## 1.6 Problems

Problem 1.1. The parity of an integer is 0 if it is even and 1 if it is odd. Which operations preserve parity:
(a) Multiplying by an even.   (b) Multiplying by an odd.   (c) Raising to a positive integer power.

Problem 1.2. What's wrong with this comparison: Google's nett worth in 2017, about $700 billion, exceeds the GDP of many countries, e.g. Argentina's 2016-GDP was about $550 billion. (Look up nett worth and GDP.)

Problem 1.3. Consider 2-contact EBOLA on a grid. You have one immunization vaccine. We show two different immunization scenarios, where you immunize the green square. Show the final infection in each case and determine which person you prefer to immunize? How many vaccines are needed to ensure that nobody else gets infected?
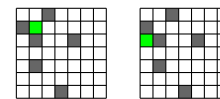
Problem 1.4. For the speed-dating problem with 16 people, $A, B, \ldots, P$ and four tables, arrange the rounds so that:
(a) In two rounds, everyone meets 6 people.
(b) In three rounds, everyone meets 9 people.
(c) In four rounds, everyone meets 12 people.
(d) In five rounds, everyone meets 15 people?

Problem 1.5 (Social Golfer Problem). 32 golfers form 8 groups of 4 each week. Each group plays a round of golf. No two golfers can be in the same group more than once. For how many weeks can this golfing activity go on?
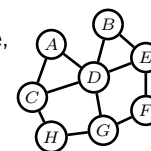(a) "Prove" that this golfing activity cannot go on for more than 10 weeks.
(b) Try to create a scheduling of players for as many weeks as you can. (10 is possible.)
(c) How is this problem related to the speed-dating problem?
In general you must schedule g groups of golfers each of size s for w weeks so that no two golfers meet more than once in the same group. Given (g, s, w), can it can be done and what is the schedule? This is a hard problem.

Problem 1.6. Students $A, \ldots, H$ form a friendship network (right). To advertise a new smartphone, you plan to give some students free samples. Here are two models for the spread of phone-adoption.
Model 1 (WEAK MAJORITY): People buy a phone if at least as many friends have the phone as don't.
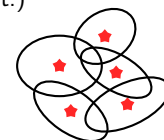Model 2 (STRONG MAJORITY): People buy a phone if more friends have the phone than don't
(a) Use your intuition and determine the most "central" of the people in this friend-network.
(b) If you give a phone only to this central node, who ultimately has a phone in: (i) Model 1 (ii) Model 2?
(c) How many phones must you distribute, and to whom, so that everyone switches to your phone in Model 2?
(d) Repeat part (c), but now you cannot give a phone to the central node.
(A slight change to a model can have a drastic impact on the conclusions. A good model is important.)

Problem 1.7. Five radio stations (red stars) broadcast to different regions, as shown. The FCC assigns radio-frequencies to stations. Two radio stations with overlapping broadcast regions must use different radio-frequencies so that the common listners do not hear garbled nonsense.
What is the minimum number of radio-frequencies the government needs?

> Discrete math problems are like childhood puzzles. Tinker like crazy until the light shines.

Problem 1.8. Two players take turns placing identical circular quarters on a circular table. Coins cannot overlap and must remain on the table. The last person to play wins. Do you want to go first or second? *[Hint: symmetry.]*

Problem 1.9. A chocolate-bar has 50 squares (5×10). How many breaks are necessary to break the bar into its 50 individual squares? You may only break a piece along a straight line from one side to the other. No stacking allowed. *[Hint: Define the invariant $\Delta = \#pieces - \#breaks$. What happens to Δ with each break?]*

Problem 1.10. A single-elimination tournament has 57 players. Players may receive byes in some rounds. How many matches are played before a winner is declared? Does it depend on how the tournament is configured? *[Hint: Define the invariant $\Delta = \#players\ remaining + \#matches\ played$. What happens to Δ after a match?]*

Problem 1.11. Five pirates must share 100 indivisible coins. The senior pirate proposes a division. If at least half the pirates agree, it's done. If not, the proposer is killed and the process continues with four pirates, and so on. A pirate values his life more than wealth. What does the senior pirate propose? *[Hint: Start with a smaller problem.]*

Problem 1.12. Can you color squares of a 9×9 grid blue or red so that every square has one opposite color neighbor (neighbors are left, right, up or down).

Problem 1.13. 57 security guards are positioned so that no two pairs of guards are the same distance apart. Every guard watches the guard closest to him. Is there an arrangement of the guards so that every guard is being watched?

Problem 1.14. 10 trucks each have 100 gallons of fuel and use 1 gallon of fuel per mile. How far can you deliver a chest that fits in one truck? (You can transfer the chest and/or fuel from truck to truck.)

Problem 1.15. A camel owner has 300 bananas to sell at a market 100 miles away. The camel carries up to 100 bananas, but eats a banana for every mile walked. How many bananas make it to the market?

Problem 1.16. Show that fewer than n initial infections cannot infect the whole $n \times n$ grid in 2-contact EBOLA. *[Hint: For a square, define 4-outgoing links (N,S,E,W) to its 4 neighbors. Pretend boundary-squares have neighbors. For an infected square, remove all outgoing links to infected neighbors. Let Δ, the "wavefront" of the infected area, be all remaining outgoing links for infected squares. Can Δ increase? What is Δ when all squares are infected?]*

Problem 1.17 (Chomp). In the grid of chocolate, if you eat the top-left square, you lose. Each player takes turns to eat a square plus all the chocolate below it and to the right. We show a possible first move and the chocolate that removed in blue. Do you want to go first or second? *[Hint: Either eating the bottom right piece wins or not. If not, what should you do?]*
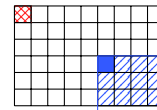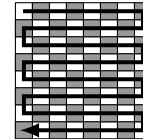
Problem 1.18. A man has a boat which can carry him and one other thing. How can the man get a fox, a chicken and a bag of corn across the river, if, when unattended, the fox eats the chicken and the chicken eats the corn.
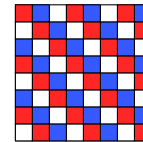
Problem 1.19. Tasks involving covering an area using different shaped tiles are a treasure trove of interesting puzzles.
  (a) Remove the top left and bottom right squares on an 8×8 chess board. Can you tile the remaining 62 squares with 31 dominos? *[Hint: Show that #black squares − #white squares is an invariant when you place a domino?]*
  (b) On an 8×8 chess board, show that if you remove any two squares of different colors, you can tile the remainder of the board with dominos. *[Hint: See illustration on the right. We show a path starting from the top-left. You can tile the board by placing dominos along this path. You may assume that the first square removed is white (why?). Show that you can still tile the remaining board along the path.].*
  (c) On a 8×8 chess board, show that if you remove any corner square, you cannot tile the remainder of the board with straight triominos (▭▭▭). It is possible to tile the board with triominos after removing one square. Can you identify which squares can be removed (there are 4)? *[Hint: See illustration on the right. We have colored the squares on the chess board so that a triomino must cover one square of each color.].*
  (d) Can you cover a 10×10 chessboard with 25 straight tetrominos (▭▭▭▭). If yes, how?

Problem 1.20. There are 13 purple, 15 red and 17 green chameleons. When chameleons of different colors meet they both transform to the third color. Will all 45 chameleons ever be the same color? *[Hint: Consider $\Delta = \#purple - \#red.$]*

Problem 1.21. A building has 1000 floors. You wish to determine the highest floor from which you can drop an egg without the egg breaking. If you had 1000 identical eggs, you could drop one from each floor and see which eggs survive. How many egg drop trials do you need if you have: (a) One egg.   (b) Two identical eggs.

Problem 1.22. Four boys take 1min, 2min, 7min and 10min to cross a bridge. The bridge only holds two boys at a time. It is dark and there is only one flashlight, which is needed to cross the bridge. Two boys cross at the speed of the slower boy who holds the flashlight. All four boys must get across the bridge. If the fastest boy acts as chauffeur for the other three, all four can cross in 21 min. Can all four get across the bridge faster?

Problem 1.23. Two consecutive positive numbers n and $n + 1$ are given to you and a friend. One player gets n and the other gets $n + 1$, at random. You look at your number and shout out your opponents number if you know it, otherwise you pass the turn to your opponent. Will this game ever stop?

Problem 1.24. A gold chain has 63 links. You can cut some links to obtain a set of links of different sizes. You wish to represent any number of links from 1 to 63 as a collection of some of your pieces.

Problem 1.25. Ants a, b, c are on the vertices A, B, C of a triangle. Each ant randomly picks one of the other vertices and walks to it. What are the chances that no ants colide on an edge or at a destination vertex? What if there are four ants a, b, c, d on the vertices A, B, C, D of a tetrahedron?

Problem 1.26. Two players alternately pick numbers without replacement from the set $\{1, 2, 3, \ldots, 9\}$. The first player to obtain three numbers that sum to 15 wins. What is your strategy?

Problem 1.27. A maharaja has 100 amphoras of wine. A traitor poisons one amphora. The poison kills in exactly one month. The maharaja uses tasters to tell if wine is safe, depending on whether the taster lives or dies after a month.

  (a) The maharaja wants to safely drink wine in a month, what is the minimum number of tasters he needs.
  (b) The maharaja wants to use all safe amphoras to throw an orgy in a month. What is the minimum number of tasters he needs. A simple solution is 100 tasters, one on each amphora. You can do much better though.

Problem 1.28. Two players take turns picking a number from one end of a line of 20 numbers. The highest total wins. In the example, if player 1 always takes from the left and player 2 from the right, player 1 gets 80, and player 2 wins with 146. Do you want to play first or second?

$$\text{③} \quad \text{⑦} \quad \text{④} \quad \text{⑲} \quad \text{⑬} \quad \text{②} \quad \text{⑭} \quad \text{⑦} \quad \text{⑤} \quad \text{⑥} \quad \text{⑦} \quad \text{⑪} \quad \text{⑧} \quad \text{②} \quad \text{㉜} \quad \text{㊼} \quad \text{⑪} \quad \text{⑥} \quad \text{⑨} \quad \text{⑬}$$

Problem 1.29. To weigh sugar, you have a comparison scale that can compare weights (illustrated). Give the fewest weights that are needed to measure out $1, 2, \ldots, 121$ pounds of sugar.

For example, to measure 3 pounds of sugar with 2 and 5 pound weights, place the sugar and 2 pounds on the one side, and 5 pounds on the other side. The sugar weighs 3 pounds if the scale balances.

Problem 1.30. More than half of 99 processors are good and the rest are bad. You may ask a processor to evaluate another processor. A good processor always gives the correct answer and a bad one gives the wrong answer. How many times must you ask some (any) processor to evaluate another before you can identify a good processor?

Problem 1.31. A plane has fuel capacity to fly half way around the world. A plane can refuel from another plane in mid-air. All planes are at the airport. How many planes and tanks of gas are needed for one plane to fly around the world? All planes must return to the airport.

Problem 1.32. 25 horses have different speeds. You can race up to 5 horses at a time and observe the order in which the horses finish. You have no stop-watch. Show that 7 races suffice to determine the fastest 3 horses.

Problem 1.33. 100 prisoners will be lined up with a red or blue hat on each head (randomly chosen). A prisoner sees only the hats ahead of them. The last in line shouts the color of his hat (everyone hears). If he is right, he is pardoned. The second-last prisoner then shouts, and so on until the first in line. No other communication is allowed. Find a better than random strategy for the prisoners. For your strategy, what are the chances each prisoner is pardoned?

Problem 1.34. At a puzzle-party with 32 guests, the host will shuffle a 52-card deck and paste a card on each guest's forhead. A guest will see every other guest's card but not their own card. After the cards are pasted on forheads, each guest, one by one, must shout out a card (e.g. 4♠). At the end the number of guests who correctly shouted out their card is multiplied by $1,000 to get a prize amount which is split evenly among all guests.

Intense discussion breaks out among the guests as they arrive. A philosopher suggests breaking into 16 pairs. In each pair, the first to shout says their partner's card so the partner can guess correctly. This strategy guarantees $16,000. A FOCS-student claims, "I can guarantee we will share $31,000." Can you come up with a strategy to guarantee $31,000?

Problem 1.35. Three friends A, B, C each have tokens a, b, c. At every step a random pair of friends is picked to swap whatever tokens they currently have. If the first pair picked is (A, B) and then (A, C) then the tokens are distributed c, a, b after the two swaps. What are the chances each friend has their own token after 2015 swaps?

Problem 1.36. On a table are some red and blue cards. Two players take turns picking two cards. If the two cards picked are the same color, both cards are replaced by one red card. If the two cards picked are different colors, both cards are replaced by one blue card. When one card remains, you win if it is blue and your opponent wins if it is red.

  (a) Must the game always end, or can it go on forever?
  (b) Who wins if there are 8 blue and 11 red cards to start? Does it matter who starts? *[Hint: Parity of blue.]*

Problem 1.37. Dad normally picks Sue from school which ends at 3pm. School ended early at 2pm, so Sue started walking home and dad picked her up on the way, returning home 20min earlier than usual. For how long did Sue walk?

Problem 1.38. Pick any six kids. Show that either 3 of them know each other or 3 of them do not know each other.

Problem 1.39. Fifteen houses are in a row. A thief robs a house. On each subsequent night, the thief robs a neighbor of the house robbed the previous night. The thief may backtrack and rob the same house. A policeman can watch any one house per night. Can the policeman guarantee catching the thief?

Problem 1.40. Three boys start at home and need to travel 50 miles to the same office. Their motorbike seats two and goes at 50mph. They walk at 5mph. Find the shortest time to get all boys to work.

Problem 1.41. To dig a hole, Bob takes 40min and Jim takes 60min. How long does the task take if both dig?

Problem 1.42. 5 of 10 coins are showing heads. You can move coins to form two sets, and you can flip over any coins you wish. Can you guarantee that both sets have the same number of heads showing, blindfolded?

Problem 1.43. Baniaz and her twin kids pass a gumball machine with 2 red, 3 blue and 4 green gumballs. Gumballs cost 1¢ each and come out randomly. Baniaz buys gumballs until she can give each of her kids one gumball of the same color. In the worst case, how much must Baniaz be willing to spend? What if she had quadruplets instead?

Problem 1.44. Two 1 meter strings burn non-uniformly in 60 sec. How do you measure 45 seconds?

> Here come hard problems that take you to the boundaries of mathematics and computing.

Problem 1.45 (Collatz/$3n+1$ Problem). Given an integer $n > 1$, repeat as follows until you reach 1:

$$n \longrightarrow \begin{cases} n/2 & \text{if } n \text{ is even;} \\ 3n+1 & \text{if } n \text{ is odd;} \end{cases}$$

Example: $6 \to 3 \to 10 \to 5 \to 16 \to 8 \to 4 \to 2 \to 1$. Do you reach 1 for every n? This "simple" problem is unsolved!

Problem 1.46 (Subset Sum). Below is a set of one hundred 27-digit numbers. Find two distinct subsets for which the sum of the numbers in each subset match. (Problem idea was from course 6.042J at ocw.mit.edu)

1:	571982539356796134655815 5629	35:	879435317221317761293977 6215	69:	754968465673294145694563 2221
2:	548794588284315869672157984	36:	298969424582747976915231 3629	70:	239787667534997199495857 9984
3:	476776653175425487422425 7763	37:	611745442798775113146758 9412	71:	467584425785737879299188 9317
4:	185592435975773212586623 9784	38:	276185448591976356844233 9436	72:	283251524138293749861467 6246
5:	428977642458919764751364 7977	39:	688421474699798597643369 5787	73:	875544277295326329936838 2378
6:	796713196176885488959421 7186	40:	867182921838175741753686 2814	74:	983366282573462445573663 8328
7:	257296727766613378922576 4888	41:	943115683724476832646893 8597	75:	529867125342542345461115 2788
8:	129458714192195263969363 9381	42:	478844866467488588358518 4169	76:	985751287918118642182341 7538
9:	476441363532391136169918 3586	43:	362475724773741477271137 2622	77:	147122614433134114478786 5593
10:	147434364182347692266715 4474	44:	936181976428624318212196 3365	78:	354543937432166165138573 5599
11:	257864976368491316342932 5833	45:	989331551615642258152935 4454	79:	673536761691562646227221 1264
12:	516159698522656868197793 8754	46:	591362598985397528956215 8982	80:	214166575414547524965493 8214
13:	224263269898168551523336 1879	47:	831389154856967281469285 8479	81:	848174725733251375828694 7416
14:	747418961456741236751683 3398	48:	226586513851837911487461 3969	82:	996121723625357695279739 7966
15:	621185567334594947174816 1445	49:	347718428896342435821175 2214	83:	994123799644582721866522 2824
16:	494271623349877221925184 8674	50:	632134961252249624151588 3378	84:	624217749346348486191586 5966
17:	551626435967275383653986 1178	51:	179643969482421326695886 8393	85:	434484351178291287584363 2652
18:	585476271961854917768925 747	52:	636625253175995567694449 6585	86:	756884256274813651861511 7797
19:	531369117196395251812473 5471	53:	854545854563689897436593 8274	87:	277662155988214612511447 3423
20:	673769175424123146975371 7635	54:	336229118621152231856685 2576	88:	617429919744784387314545 7215
21:	429238861445414672824619 8812	55:	846447386637547496734777 2855	89:	538758413152578761561756 3371
22:	446846371586674625897652 344	56:	289285756435526221994569 4217	90:	531769335337257228458824 2963
23:	263862173182236237162811 879	57:	429669393766126671538224 1936	91:	661214251555259366395596 6562
24:	125892226372929658978541 8839	58:	863476461726572471638977 5433	92:	131492858771329249361662 5427
25:	448227972726479782765489 9397	59:	841523424318278753412389 4858	93:	244682766728745168593917 3534
26:	874985532228537116298641 1895	60:	226735325445487261618224 2154	94:	978669387873198453492455 8138
27:	111659945796197179668393 6952	61:	468991184757874147318633 7883	95:	292671883874263477477871 3813
28:	387921327359632273599332 9751	62:	442876678796483437179456 5542	96:	379142627449759664196914 2899
29:	921235913157415965716819 6759	63:	714629518676416726843323 8125	97:	283172771517629990687749 51996
30:	335122318381871267369197 7472	64:	227382381357296857746938 8278	98:	328128735346372529227191 6883
31:	885583532281251286889644 9976	65:	668613272133686445763522 3349	99:	995474459492238676673551 9674
32:	433285948687125592255541 8653	66:	316151829657648815899714 6221	100:	341433914354532429885324 8718
33:	242875158237196445338175 1663	67:	191761142573992828514775 8625		
34:	673848186686689517878842 76161	68:	351643153734338713535723 7754		

Problem 1.47 (Verifier for "Hello World"). Write a program in your pet language to solve this problem.

    Input: <u>Any</u> C^{++} program F.cpp (an ASCII text file).

   Output: *Yes* if: when you compile and run F.cpp, it prints "Hello World", and eventually stops.

          No if: when you compile and run F.cpp, the program loops forever or stops without printing "Hello World".

Would you have guessed that a solver for the domino puzzle (Section 1.4) can be used to build a Hello-World-verifier?

2.5 Problems

Problem 2.1. What is the difference between a Theorem, a Conjecture and an Axiom?

Problem 2.2. List the elements in the following sets (E is the set of even numbers).
(a) $A = \{n \mid -4 \le n \le 15; \; n \in E\}$.
(b) $B = \{x \mid x^2 = 9; \; x \in \mathbb{Z}\}$.
(c) $C = \{x \mid x^2 = 6; \; x \in \mathbb{Z}\}$.
(d) $D = \{x \mid x = x^2 - 1; \; x \in \mathbb{R}\}$.

Problem 2.3. Give formal definitions of these sets using a variable.
(a) $A = \{0, 1, 4, 9, 16, 25, 36, \ldots\}$.
(b) $B = \{0, 4, 16, 36, 64, 100, \ldots\}$.
(c) $C = \{1, 2, 4, 7, 11, 16, 22, \ldots\}$.
(d) $D = \{\ldots, 1/8, 1/4, 1/2, 1, 2, 4, 8, \ldots\}$.

Problem 2.4. On the x–y plane, sketch the points in the sets:
(a) $A = \{(x, y) \mid x \in [0, 1], y \in [0, 1]\}$.
(b) $B = \{(x, y) \mid x, y \in \mathbb{R}, x^2 + y^2 = 1\}$.
(c) $C = \{(x, y) \mid x, y \in \mathbb{R}, x^2 + y^2 \le 1\}$.
(d) $D = \{(x, y) \mid x \ge 1, y \in \mathbb{R}\}$.
(e) $E = \{(x, x^2) \mid x \in \mathbb{R}\}$.
(f) $F = \{(x, x + y) \mid x \in \mathbb{R}, y \in \mathbb{Z}\}$.

Problem 2.5. Express the shaded region using unions, intersections and complements.

(a) (b) (c) (d) (e) (f)

Problem 2.6. Give two sets A, B for which $A \not\subseteq B$ and $B \not\subseteq A$.

Problem 2.7. Complement depends on the universal set $\mathcal{U}$. Let $X = \{a, e\}$. What is $\overline{X}$ when:
(a) $\mathcal{U} = \{$lower case vowels$\}$.   (b) $\mathcal{U} = \{$lower case letters$\}$

Problem 2.8. True or False: (a) $\mathbb{N} \subseteq \mathbb{Z}$ (b) $\mathbb{N} \subset \mathbb{Z}$ (c) $\mathbb{Z} \subseteq \mathbb{Q}$ (d) $\mathbb{Z} \subset \mathbb{Q}$

Problem 2.9. For each case, find $\bigcup_{i=1}^{\infty} A_i = A_1 \cup A_2 \cup A_3 \cup \cdots$ and $\bigcap_{i=1}^{\infty} A_i = A_1 \cap A_2 \cap A_3 \cap \cdots$.
(a) $A_i = \{n \mid n \in \mathbb{N}, n \ge i\}$.   (b) $A_i = \{0, i\}$.   (c) $A_i = \{x \mid x \in \mathbb{R}, 0 < x < i\}$.

Problem 2.10. Let $A_i = \{(x, y) \mid x \in [0, 1], y \in [1/(i + 1), 1/i]\}$. On the x–y plane, sketch:
(a) A_1 and A_2.   (b) $A_1 \cup A_2$.   (c) $A_1 \cup A_5$.   (d) $A_1 \cup A_2 \cup \cdots \cup A_n = \bigcup_{i=1}^{n} A_i$.   (e) $A_1 \cup A_2 \cup \cdots = \bigcup_{i=1}^{\infty} A_i$.

Problem 2.11. Let $B = \{\{a, b\}, a, b, c\}$. List the power set $\mathcal{P}(B)$ (it has 16 elements)?

Problem 2.12. List all subsets of $\{a, b, c, d\}$ that contain c but not d.

Problem 2.13. (a) Find $|M \cap V|$ and $|\mathcal{P}(M \cap V)|$ for $M = \{m, a, l, i, k\}, V = \{a, e, i, o, u\}$?   (b) What is $|\mathbb{N}|$?

Problem 2.14. $|A| = 7$ and $|B| = 4$. What are the possible values for $|A \cap B|$ and $|A \cup B|$?

Problem 2.15. What is the set $\mathbb{Z} \cap \overline{\mathbb{N}} \cap S$, where $S = \{z^2 \mid z \in \mathbb{Z}\}$ is the set perfect squares.

Problem 2.16 (Cartesian Product). Let $A = \{1, 2, 3\}$ and $B = \{a, b, c, d\}$. The Cartesian product $A \times B$ is the set of pairs formed from elements of A and elements of B,
$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$
(a) List the elements in $A \times B$. What is $|A \times B|$? ($|X|$ is the number of elements in X.)
(b) List the elements in $B \times A$. What is $|B \times A|$?
(c) List the elements in $A \times A = A^2$. What is $|A \times A|$?
(d) List the elements in $B \times B = B^2$. What is $|B \times B|$?
Generalize the definition of $A \times B$ to a Cartesian product of three sets $A \times B \times C$.

Problem 2.17. Sketch the Cartesian products $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$, $\mathbb{R} \times \mathbb{N}$, $\mathbb{N} \times \mathbb{R}$, $\mathbb{N} \times \mathbb{N} = \mathbb{N}^2$. (See Problem 2.16.)

Problem 2.18. List as a set all the 4-bit binary sequences. How many did you get? Now, list all the 4-bit binary sequences in which 00 does not occur. How many did you get?

Problem 2.19. How many binary sequences are of length 1,2,3,4,5? Guess the pattern.

Problem 2.20. A sequence $s_0, s_1, s_2, s_3, \ldots$ is described below. Give a "simple" formula for the nth term s_n in the sequence, for $n = 0, 1, 2, 3, \ldots$. Your answer should be of the form $s_n = f(n)$ for some function $f(n)$.

(a) $0, 1, 2, 3, 4, 5, 6 \ldots$

(b) $1, -1, 1, -1, 1, -1, \ldots$

(c) $0, 1, -2, 3, -4, 5, -6, \ldots$

(d) $2, 0, 2, 0, 2, 0, \ldots$

(e) $1, 2, 4, 8, 16, \ldots$

(f) $1, 3, 5, 7, 9, \ldots$

(g) $1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, \ldots$

(h) $0, 3, 8, 15, 24, 35, 48, 63, \ldots$

(i) $1, 2, 1/3, 4, 1/5, 6, 1/7, 8, 1/9, 10, 1/11, 12, \ldots$

(j) $1, 1/2, 4, 1/8, 16, 1/32, 64, 1/128, \ldots$

Problem 2.21. For each case in Problem 2.20, use a variable as in (2.1) to formally define the set of numbers.

Problem 2.22. Draw a picture of each graph representing friendships among our 6 friends $V = \{A, B, C, D, E, F\}$.

(a) $E = \{(A, B), (B, C), (C, D), (D, E), (E, F), (F, A)\}$.

(b) $E = \{(A, B), (A, C), (A, D), (A, E), (A, F)\}$.

(c) $E = \{(A, D), (B, D), (C, D), (A, E), (B, E), (C, E), (A, F), (B, F), (C, F)\}$.

(d) $E = \{(A, B), (B, C), (A, C), (D, E), (E, F), (D, F)\}$.

You should recognize familiar social structures in your pictures.

Problem 2.23. How do you get the conflict graph from the affiliation on page 18?

Problem 2.24. Model the relationship between radio-stations in Problem 1.7 using a graph.

(a) Would you use friendship networks, affiliation graphs or conflict graphs?

(b) Draw a picture of your graph for the 5 radio stations.

(c) Show that 3 radio frequencies $(1, 2, 3)$ suffice for no listener to hear garbled nonsense.

Problem 2.25 (Internet Exercise). Research these settings and explain how they can be represented by graphs:

(a) Infectious disease spread.

(b) Collaborations between academic authors.

(c) Niche overlap in ecology.

(d) Protein interactions in human metabolism.

Problem 2.26. True or false and why? (a) Every multiple of 4 has a square which is a multiple of 4. (b) Every square which is a multiple of 4 came from squaring a multiple of 4.

Problem 2.27. Do you believe this method for amplifying money? Explain why or why not.
$$1¢ = \$0.01 = (\$0.1)^2 = (10¢)^2 = 100¢ = \$1.$$

Problem 2.28 (Quotient Remainder Theorem). Given are $n \in \mathbb{Z}$ and a divisor $d \in \mathbb{N}$.

    Theorem. There are a unique quotient $q \in \mathbb{Z}$ and remainder $r \in \mathbb{Z}$, with $0 \le r < d$, such that $n = qd + r$.

Suppose $n = 27$ and $d = 5$; compute q and r. Can you think of a way to prove the theorem?

Problem 2.29. Mimic the method we used to prove $\sqrt{2}$ is irrational and prove $\sqrt{3}$ is irrational. Now use the same method to try and prove $\sqrt{9}$ is irrational. What goes wrong?

Problem 2.30 (Simple Continued Fractions).

For $n \ge 1$, a non-terminating continued fraction x is shown on the right.

Can you think of a way to show that x is irrational, for any $n \in \mathbb{N}$? (Tinker with $n = 1$ first.)

$$x = \cfrac{1}{n + \cfrac{1}{n + \cfrac{1}{n + \cfrac{1}{n + \cfrac{1}{n + \cfrac{1}{\cdots}}}}}}$$

Problem 2.31 (Ramsey). Prove a crude generalization of the 6-person party theorem. Specifically, in any n-person party, there is either a friend-clique or war with more than $(\log_2 n)/2$ people. Here is a "constructive" proof. Make three sets C (for clique), W (for war) and V. Sets C and W are initially empty and V has all the people. We run a process in steps and continue until no one is left in V. At each step, pick any person x from V and:

- Place x in C if x is friends with more than half of V. Discard from V all the enemies of x.
- Place x in W if x is enemies with at least half of V. Discard from V all the friends of x.

(a) Show that at every step in the process, everyone in C are mutual friends and everyone in W are mutual enemies.

(b) Show that at each step in the process, the size of V shrinks from $|V|$ to no less than $(|V| - 1)/2$.

(c) Show that the process continues for at least $\log_2 n$ steps, where in each step a person is added to either C or W.

(d) Show that either C or W has more than $(\log_2 n)/2$ people at the end. Are we done?

3.5   Problems

Problem 3.1. Determine T/F. If you think a statement is not a valid proposition, explain why.

(a) "2+7=10."

(b) "There are no wild killer bees in Alaska."

(c) "Miami is not in Florida."

(d) "Where is the train station?"

(e) "$2x > 5$."

(f) "$2^n < 100$."

(g) "There is a lot of pollution in Mumbai."

(h) "The answer to this question is F."

Problem 3.2. True or False: "The function f equals 5?" Explain.

Problem 3.3. True or False: "IF God exists, THEN the square of any real number is non-negative." Explain

Problem 3.4. Let p = "Ifar is a CS major" and q = "Ifar is a hockey player". Write each claim using $p, q, \wedge, \vee, \neg$.

(a) Ifar is a hockey player and CS major.

(b) Ifar either plays hockey or is a CS major.

(c) Ifar plays hockey, but he is not a CS major.

(d) Ifar neither plays hockey nor is a CS major.

(e) Ifar is a CS major or a hockey player, not both.

(f) Ifar is not a hockey player, but is a CS major.

Problem 3.5. What is the negation of these statements?

(a) Jan is rich and happy.

(b) If Kilam was born yesterday, then pigs fly.

(c) Niaz was born yesterday and pigs can't fly.

(d) Kilam's phone has at least 8GB of RAM.

(e) If Kilam is in pajamas, then all lights are off.

(f) Every student is a friend of another student.

(g) Some student is a friend of another student.

(h) All Kilam's friends are big and strong.

Problem 3.6. Kilam's has 2GB of RAM Liamsi has 4GB of RAM. Which propositions are true?

(a) IF Kilam has more RAM than Liamsi THEN pigs fly.

(b) IF Liamsi has more RAM than Kilam THEN pigs fly.

(c) Kilam has more RAM than Liamsi AND pigs fly.

(d) Kilam has more RAM than Liamsi OR pigs fly.

(e) Liamsi has more RAM than Kilam AND pigs fly.

(f) Liamsi has more RAM than Kilam OR pigs fly.

Problem 3.7. There are 3 spoons, 4 forks and 4 knives. How many utensils are:

(a) Forks or knives.   (b) Forks and knives.   (c) Neither Forks nor knives.

Problem 3.8. Rewrite each sentence in "IF..., THEN..." form.

(a) You pass the FOCS-final exam only if you studied this book for at least one week.

(b) Attending class is necessary for passing the course.

(c) For a quadrilateral to be square, it is sufficient that it have four equal angles.

(d) For a quadrilateral to be square, it is necessary that it have four equal sides.

(e) A natural number can't be an odd prime unless it is greater than 2.

(f) The giant flies come out whenever it is hot.

(g) All roads lead to Rome.

Problem 3.9. If the blind-spot indicator lights up, there is car in your blind spot and it's not safe to switch lanes. The blind-spot indicator is not lit. Is it safe to switch lanes or should you look first?

Problem 3.10. Ifar's parents always told him: "If you don't eat your peas, you can't have ice-cream." Naturally, Ifar always ate his peas and eagerly expected his ice-cream to come. Are Ifar's parents obliged to give him ice-cream? What statement did Ifar think he heard, and is that logically equivalent to what his parents actually said.

Problem 3.11. What's the difference between these marketing slogans? Which is the more impressive claim?

"If you didn't buy your car from FOCS-Auto, then you paid too much."

"If you bought you car from FOCS-Auto, then you didn't pay too much."

Problem 3.12. Trolls are knights who are honest or knaves who are liars. Troll 1 says: "If we are brothers, then we are knaves." Troll 2 says: "We are brothers or knaves." (a) Can both trolls be knights?   (b) Can both trolls be knaves?

Problem 3.13. On the Isle-of-FOCS are Saints who always tell the truth and Sinners who always lie.

(a) Two people, A and B, made these statements. Which (if any) of them must be Saints?

   A: "Exactly one of us is lying." B: "At least one of us is telling the truth."

(b) Three people, A, B, C, made these statements. Which (if any) of them must be Saints?

   A: "Exactly one of us speaks the truth." B: "We are all lying." C: "The other two are lying."

Problem 3.14. If it rains on a day, it rains the next day. Today it didn't rain. On which days must there be no rain?
(a) Tomorrow.   (b) All future days.   (c) Yesterday.   (d) All previous days.

Problem 3.15. For p = "You're sick", q = "You miss the final", r = "You pass FOCS". Translate into English:
(a) $q \to \neg r$.   (b) $(p \to \neg r) \vee (q \to \neg r)$.   (c) $(p \wedge q) \vee (\neg q \wedge r)$.

Problem 3.16. Here is a logic puzzle from a pshchology experiment studying how humans perform deductive analysis. You have before you the cards (only the top is visible). Each card has a number on one side and a letter on the other.

$$\boxed{\text{S}} \quad \boxed{5} \quad \boxed{\text{P}} \quad \boxed{\text{T}} \quad \boxed{3} \quad \boxed{4}$$

Rule: If a card has a P on it, then the other side must be a 5.

To verify that the rule is not been broken, which are the fewest cards that you need to turn over, and why?

Problem 3.17. Here is a logic puzzle from a bar setting.
　　　Law: If you are drinking beer, then you must be 21 or older.
Which of the following should the bar check to abide by the law.
(a) A's age.   (b) B's age.   (c) C's drink.   (d) D's drink.

> A is drinking a beer;
> B is drinking a coke;
> C is drinking something and looks under 21;
> D is drinking something and looks over 50.

Problem 3.18. Here's what we know about Kilam.

> 1: Kilam eats Italian or French each night.
> 2: He eats French or wears dress shoes.
> 3: Whenever he eats Italian and wears a coat, he does not wear a bow tie.
> 4: He never eats French unless he also wears a coat or dress shoes.
> 5: If he wears dress shoes, he wears a coat.

(a) Will Kilam ever be without a coat? (b) Today, Kilam is in a bow tie. What else did he wear? What did he eat?

Problem 3.19 (Converse, Contrapositive). The converse of $p \to q$ is $q \to p$. The contrapositive is $\neg q \to \neg p$. For each implication, give the converse & contrapositive, and determine which, if any, are true.
(a) If a/b and b/c are in $\mathbb{Z}$, then $a/c \in \mathbb{Z}$.
(b) $x^2 = 1 \to x = 1$.
(c) If $x^2 = x + 1$, then $x = (1 \pm \sqrt{5})/2$.
(d) If $p > 2$ is prime, then p is odd.
(e) $ab = 0 \to a = 0$ or $b = 0$.
(f) If $n \in \mathbb{N}$ ends in 3, then 3 divides n.
(g) For $n \in \mathbb{Z}$, $3n = 9 \to n^2 = 9$.
(h) For $n \in \mathbb{Z}$, $n^2 > 9 \to n > 3$.
(i) For $n \in \mathbb{N}$, $n^2 > 9 \to n > 3$.
(j) If $n \in \mathbb{N}$ is odd then $n^2 + n - 2$ is even.
(k) Every connected graph G has 32 vertices.
(l) Honk if you love FOCS.

Problem 3.20. Mathematically formulate the usual meaning of each sentence using p, q, r.
(a) p : "you will succeed at this job"; q : "you know Java"; r : "you know Python".
　　　Sentence: IF you know Java or Python, you will succeed at this job."
(b) p : "you buy a lunch entree"; q : "you can have soup"; r : "you can have salad".
　　　Sentence: IF you buy a lunch entree, you can have soup or salad."
(c) p : "you may enter the US"; q : "you have a job"; r : "you have a green-card".
　　　Sentence: IF you have a job or green-card, you may enter the US."

Problem 3.21. How many rows are in the truth table of $\neg(p \vee q) \wedge \neg r$? Give the truth table.

Problem 3.22. How many rows are in the truth-table of the proposition $(p \vee q) \to (r \to s)$.

Problem 3.23. Give the truth-tables for: $p \wedge \neg p$; $p \vee \neg p$; $p \to (p \vee q)$; $((p \to q) \wedge (\neg q)) \to \neg p$.

Problem 3.24. Show that $(p \to q) \vee p$ is ALWAYS true. This is called a tautology.

Problem 3.25. Let $q \to p$ be F and $q \to r$ be T. Answer T orF: (a) $p \vee q$ (b) $p \to q$ (c) $p \wedge q \wedge r$.

Problem 3.26. Give pseudocode for a program that takes the input $n \in \mathbb{N}$ and outputs all the possible truth values (rows in the truth table) for the statements $p_1, p_2, \ldots, p_n$. The correct output for $n = 1$ and $n = 2$ are shown. We suggest you either use recursion or a while loop.

p_1
F
T

	p_1	p_2
	F	F
	F	T
	T	F
	T	T

Problem 3.27. Show that $(p \to q) \vee (q \to p)$ is always true for arbitrary statements p, q.

Problem 3.28. True or false (use truth tables): (a) $(p \to q) \to r \overset{\text{eqv}}{\equiv} p \to (q \to r)$ (b) $(p \wedge \neg q) \vee q \overset{\text{eqv}}{\equiv} p \vee q$.

Problem 3.29. Use truth-tables to verify the rules in Figure 3.1 on page 29. Derive the logical equivalence
$$\neg((p \wedge q) \vee r) \overset{\text{eqv}}{\equiv} (\neg p \wedge \neg r) \vee (\neg q \wedge \neg r).$$

Problem 3.30 (DNF). Use $\neg, \wedge, \vee$ to give compound propositions with these truth-tables. *[Hints: Consider only rows which are T and use OR of AND's. This is known as the disjunctive normal form (DNF).]*

(a)

q	r	
T	T	F
T	F	T
F	T	F
F	F	F

(b)

q	r	
T	T	F
T	F	T
F	T	F
F	F	T

(c)

p	q	r	
T	T	T	F
T	T	F	F
T	F	T	F
T	F	F	F
F	T	T	F
F	T	F	T
F	F	T	F
F	F	F	F

(d)

p	q	r	
T	T	T	F
T	T	F	T
T	F	T	F
T	F	F	F
F	T	T	T
F	T	F	T
F	F	T	F
F	F	F	F

NOT-AND-OR formulas using only $\neg, \wedge, \vee$ can realize any truth table. In fact, an OR of AND's suffices (DNF).

Problem 3.31. Given the information, answer the question true, false or I don't know.
  (a) IF you ace the quiz and final, THEN you get an A. You aced the final. Did you get an A?
  (b) IF you ace the quiz or final, THEN you get an A. You aced the final. Did you get an A?
  (c) IF you ace the quiz and final, THEN you get an A. You got an A. Did you ace the final?
  (d) IF you ace the quiz or final, THEN you get an A. You got an A. Did you ace the final?
  (e) IF you ace the quiz and final, THEN you get an A. You got a B. Did you ace the final?
  (f) IF you ace the quiz or final, THEN you get an A. You got a B. Did you ace the final?

Problem 3.32. Given the information, answer the question true, false or I don't know.
  (a) IF it rains, THEN Kilam brings an umbrella. It did not rain. Did Kilam bring an umbrella?
  (b) EVERYONE who eats apples is healthy. Kilam is healthy. Does Kilam eat apples?
  (c) EVERYONE who eats apples is healthy. Kilam is not healthy. Does Kilam eat apples?
  (d) EVERYONE who eats apples is healthy. Kilam eats apples. Is Kilam healthy?
  (e) You can have cake OR ice-cream. You had cake. Can you have ice-cream?
  (f) Lights are turned on in the night. Lights are off. Is it day?
  (g) Lights are turned on in the night. It is day. Are the lights on?
  (h) IF you are a singer, THEN you don't eat cheese. You don't eat cheese. Are you a singer?

Problem 3.33. It rains on Tuesdays. When it rains, Kilam does not run. When it's dry, Kilam either runs or goes to work early. When Kilam runs, he must eat breakfast. All people have coffee with breakfast. Answer T/F/I don't know.
  (a) Today is Wednesday, so Kilam had coffee.
  (b) Today, Kilam went to work early, so it did not rain.
  (c) Today, Kilam did not go for a run, so either it is Tuesday or Kilam went early to work.
  (d) On Friday, Kilam did not go to work early, so he must have had coffee.
  (e) On Friday, Kilam did not go to work early, so either it rained or Kilam had coffee.

Problem 3.34. On your back bumper is a sticker saying "Honk if you love FOCS." What can you conclude about the driver in the car behind you if: (a) You hear honking? (b) You don't hear any honking?

Problem 3.35. For each pair of implications, determine which one is likely to be true in practice.
  (a) If I was in the rain, then my hair is wet.   (b) If you have a CS-degree, then you took FOCS.
      If my hair is wet, then I was in the rain.   If you took FOCS, then you have a CS-degree.

Problem 3.36. Sherrif Suzie and Big Mike debate the implication

<div style="text-align:center">If $n \in \mathbb{N}$ is odd, then $n^2 + 4$ is prime.</div>

Suzie tries to convince Mike it's false by giving a counterexample (right).

(a) Why is Sherrif Suzie only trying odd n to find a counterexample?

(b) Are you convinced the implication is true? If not, why not?

(c) Find a counterexample to show that the implication is false.

> SS: Perhaps 1 is a counterexample.
> BM: Nope: $1^2 + 4 = 5$, which is prime.
> SS: What about 3?
> BM: Nope: $3^2 + 4 = 13$, which is prime.
> SS: Let's try 5?
> BM: No again: $5^2 + 4 = 29$, a prime.
> SS: You win. The implication seems true.
> BM: Phew! I'm tired. Let's have a drink.

Problem 3.37 (Satisfiability). Assign T or F to each of p, q, r, s so that every clause below is true, i.e. satisfied.

$$(\bar{p} \vee q) \qquad (\bar{q} \vee r) \qquad (\bar{r} \vee s) \qquad (\bar{s} \vee q)$$

Problem 3.38. Assign T or F to p, q, r, s to make the compound proposition true (if possible).

(a) $(p \to q) \wedge (q \leftrightarrow \neg p)$.   (b) $(p \vee \neg r) \wedge (r \wedge s) \wedge (\neg s \wedge \neg p) \wedge (p \wedge (q \to r))$.   (c) $(p \leftrightarrow q) \to \neg(p \to q)$.

Problem 3.39. Using statements p, q, r, s, we list eight clauses. Each clause is an OR of 3 terms, where a term is a statement or its negation. A proposition appears at most once in a clause.

$$(p \vee q \vee r) \quad (\bar{q} \vee r \vee s) \quad (\bar{p} \vee q \vee s) \quad (\bar{p} \vee q \vee r) \quad (p \vee r \vee \bar{s}) \quad (\bar{p} \vee \bar{q} \vee s) \quad (\bar{p} \vee \bar{r} \vee s) \quad (\bar{p} \vee q \vee \bar{s})$$

(a) Give a truth assignment (T or F) to each of p, q, r, s so that every clause is true (satisfied).

(b) Construct eight clauses for which no truth assignment to p, q, r, s can satisfy all eight clauses.

(c) Show that one can always satisfy at least 7 of the 8 clauses, if each clause has exactly three terms.

Problem 3.40. For the domain of all students, use the predicates $S(x) = $ "x is a student", $I(x) = $ "x is a smart" and $F(x, y) = $ "x is a friend of y" to formulate the following statements.

(a) Kilam is a student.

(b) All students are smart.

(c) No student is a friend of Kilam.

(d) Every student is a friend of some other student.

(e) There is a student who is a friend of every other student.

(f) All smart students have a friend.

Problem 3.41. What is the negation of each statement. You are being asked to "translate" a negation like IT IS NOT THE CASE THAT(Kilam is a student) into "normal" English.

(a) Kilam is a student.

(b) All students are smart.

(c) No student is a friend of Kilam.

(d) Every student is a friend of some other student.

(e) There is a student who is a friend of every other student.

(f) All smart students have a friend.

Problem 3.42. Use predicates and connectors to precisely state each interpretation of "Every American has a dream."

(a) There is a single dream, the "American dream," and every American has that same special dream.

(b) Every American has their own personal dream (possibly a different one for each person).

(c) Every American has one (and only one) personal dream (possibly a different one for each person).

Problem 3.43. Give the negation of each claim in sensible English. Start with IT IS NOT THE CASE THAT($\cdot$) and then take the negation inside the quantifiers.

(a) There is a constant C for which $n^3 \le Cn^2$ for all $n \in \mathbb{N}$.

(b) For some $x > 0$, there is a constant C for which, for all $n \in \mathbb{N}$, $n^{2+x} \le Cn^2$.

Problem 3.44. Give the negation of each claim. Simplify your statement so that the negation, $\neg$, is not to the left of any quantifier. Determine which of the original statement or the negation is T. (Can both be T? Can neither be T?)

(a) $\forall x \in \mathbb{Z} : (\exists y \in \mathbb{Z} : x + 2y = 3)$.   (b) $\exists x > 0 : (\forall y > 0 : xy < x)$.   (c) $\exists (x, y) \in \mathbb{Z}^2 : (x + y = 13) \wedge (xy = 36)$.

Problem 3.45. For $x \in \{1, 2, 3, 4, 5\}$ and $y \in \{1, 2, 3\}$, determine T/F with short justifications.

(a) $\exists x : x + 3 = 10$ (b) $\forall y : y + 3 \le 7$ (c) $\exists x : (\forall y : x^2 < y + 1)$ (d) $\forall x : (\exists y : x^2 + y^2 < 12)$

Problem 3.46. For $x, y \in \mathbb{Z}$, determine T/F with short justifications.

(a) $\forall x : (\exists y : x = 5/y)$ (b) $\forall x : (\exists y : y^4 - x < 16)$ (c) $\forall x : (\forall y : \log_2 x \ne y^3)$

Problem 3.47. Let $P(x, h) = $ "Person x has hair h" and $M(h) = $ "Hair h is grey". Formulate:

(a) Kilam has some grey hair.

(b) Someone has all grey hair.

(c) Nobody is bald.

(d) Kilam does not have all grey hair.

<div style="text-align:center">38</div>

Problem 3.48. Formulate appropriate predicates with domains and give the "math" version of each statement.

(a) Every person has at most one job.
(b) Kilam has some grey hair.
(c) Everyone has some grey hair.
(d) Everyone is a friend of someone.
(e) All professors consider their students as a friend.
(f) No matter what integer you choose, there is always an integer that is larger.
(g) Every natural number has a prime factorization.
(h) Two courses which have the same student cannot have exam times that overlap.
(i) No student has won a TV game-show.
(j) There is a soul-mate for everyone.
(k) 15 is a multiple of 3. (In your predicate you must define what a multiple is.)
(l) 15 is not a multiple of 4.
(m) 16 is a perfect square. (In your predicate you must define what a perfect square is.)
(n) Every student in FOCS has taken a course in calculus and a course in programming.
(o) Every CS-major who graduates has taken FOCS.
(p) Between any two rational numbers there is another rational number.
(q) Between any rational number and larger irrational number is another irrational number.
(r) Between any rational number and larger irrational number is another rational number.

Problem 3.49. Use quantifiers to precisely formulate the associative and distributive laws of arithmetic.

Problem 3.50. For the predicates $F(x)=$"x is a freshman" and $M(x)=$"x is a math major', translate into English:

(a) $\exists x : M(x)$ (b) $\neg\exists x : F(x)$ (c) $\forall x : (M(x) \to \neg F(x))$ (d) $\neg\exists x : (M(x) \wedge \neg F(x))$

Problem 3.51. What is the difference between $\forall x : (\neg\exists y : P(x) \to Q(y))$ and $\neg\exists y : (\forall x : P(x) \to Q(y))$?

Problem 3.52. P and Q are predicates. Are these pairs of statements equivalent. Explain.

(a) $\forall x : (\neg\exists y : P(x) \to Q(y))$ and $\neg\exists x : (\exists y : P(x) \to Q(y))$.
(b) $\forall x : (\neg\exists y : P(x) \to Q(y))$ and $\neg\exists y : (\forall x : P(x) \to Q(y))$.

Problem 3.53. Let $P(x)$ and $Q(y)$ be predicates. Verify that these quantified compound propositions are equivalent. (To show that quantified predicates are equivalent, show that when one is true, the other is true and *vice versa*.)
$$\forall x : (\neg\exists y : P(x) \to Q(y)) \qquad \text{and} \qquad \neg\exists x : (\exists y : P(x) \to Q(y)).$$

Problem 3.54. Let $P(x)$ and $Q(x)$ be arbitrary predicates. Prove or disprove:

(a) $\forall x : (P(x) \wedge Q(x)) \overset{\text{eqv}}{\equiv} (\forall x : P(x)) \wedge (\forall x : Q(x))$ (b) $\forall x : (P(x) \vee Q(x)) \overset{\text{eqv}}{\equiv} (\forall x : P(x)) \vee (\forall x : Q(x))$

Problem 3.55. The input domain of predicates P and Q is empty. If you can, determine the truth values of:

(a) $\forall x : P(x)$ (b) $\exists y : P(y)$ (c) $(\forall x : P(x)) \vee (\exists y : P(y))$ (d) $(\forall x : P(x)) \vee P(y)$

Problem 3.56. Determine if each quantified compound statement is always true. If no, give a counterexample (specify the predicate and domain). If yes, explain why. (a) $(\exists x : P(x)) \to (\forall x : P(x))$ (b) $(\forall x : P(x)) \to (\exists x : P(x))$.

Problem 3.57. x and y are integers. Answer true or false, explaining your reasoning.

(a) $\forall x : (\exists y : 2x - y = 0)$ (c) $\exists x : (\forall y : 2x - y = 0)$ (e) $\exists x : (\forall y : x2^y = 0)$
(b) $\forall y : (\exists x : 2x - y = 0)$ (d) $\exists y : (\forall x : 2x - y = 0)$ (f) $\exists y : (\forall x : x2^y = 0)$

Problem 3.58. In which (if any) of the domains $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ are these claims T. (x and y can have different domains.)

(a) $\exists x : x^2 = 4$ (b) $\exists x : x^2 = 2$ (c) $\forall x : (\exists y : x^2 = y)$ (d) $\forall y : (\exists x : x^2 = y)$

Problem 3.59. True or false. A counterexample to "ALL ravens are black" must be: (a) Non-raven. (b) Non-black.

Problem 3.60 (Induction and Hempel's Paradox). Consider the claim "ALL ravens are black."

(a) You observe a black raven. Does that strengthen your belief that "ALL ravens are black?" Is it a proof?
(b) You observe a white sock. Does that strengthen your belief that "ALL non-black things are not ravens?"
(c) Show that "ALL ravens are black." is logically equivalent to "ALL non-black things are not ravens." So, does in- ductive logic suggest that observing a white sock strengthens your belief that "ALL ravens are black?" Hmm...

Problem 3.61 (Closure). A set $\mathcal{S}$ is closed under an operation if performing that operation on elements of $\mathcal{S}$ returns an element in $\mathcal{S}$. Here are five examples of closure.

$$
\begin{array}{rcl}
\mathcal{S} \text{ is closed under addition} & \rightarrow & \forall (x,y) \in \mathcal{S}^2 : x + y \in \mathcal{S}. \\
\mathcal{S} \text{ is closed under subtraction} & \rightarrow & \forall (x,y) \in \mathcal{S}^2 : x - y \in \mathcal{S}. \\
\mathcal{S} \text{ is closed under multiplication} & \rightarrow & \forall (x,y) \in \mathcal{S}^2 : xy \in \mathcal{S}. \\
\mathcal{S} \text{ is closed under division} & \rightarrow & \forall (x, y \neq 0) \in \mathcal{S}^2 : x/y \in \mathcal{S}. \\
\mathcal{S} \text{ is closed under exponentiation} & \rightarrow & \forall (x,y) \in \mathcal{S}^2 : x^y \in \mathcal{S}.
\end{array}
$$

Which of the five operations are the following sets closed under? (a) $\mathbb{N}$.   (b) $\mathbb{Z}$.   (c) $\mathbb{Q}$.   (d) $\mathbb{R}$.

**Problem 3.62.** Compute the number of positive divisors of the following integers:

$$6, 8, 12, 15, 18, 30 \qquad\qquad 4, 9, 16, 25, 36$$

State a precise conjecture that relates a property of the number of divisors of n to a property of n (proof not needed). (You may define convenient notation, for example let $\phi(n)$ be the number of positive divisors of n).

Problem 3.63. Use dominos to tile an 8×8 chessboard with two opposite-color squares removed. Tinker. Formulate a precise conjecture about whether the board with missing squares can be tiled. You don't have to prove your conjecture.

Problem 3.64. In the Ebola model, a square is infected if at least two (non-diagonal) neighbors are infected.
 (a) An initial infection is shown. Show the final state of the grid, i.e., who is ultimately infected.
 (b) Are there 5 initial infections that can infect the whole 6×6 square. What about with 6 initial infections? Also try the 4×4 and 5×5 grids.
 (c) For the $n \times n$ grid, $n \in \mathbb{N}$, formulate a conjecture for the fewest initial infections required to infect the whole square. You do not have to prove your claim, but be **precise** in your statement.
 (d) **[Hard]** Can you think of a way to justify your conjecture?
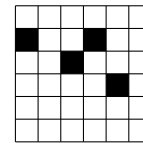
Problem 3.65. For n numbers $x_1, \ldots, x_n$, define the average $\mu = (\sum_{i=1}^n x_i)/n$ and the average of squares $s^2 = (\sum_{i=1}^n x_i^2)/n$. Tinker with some numbers and $n = 2, 3$, computing μ^2 and s^2. Make a conjecture that relates μ^2 and s^2. You don't have to prove your conjecture.

Problem 3.66 (Josephus Problem). From n children, a winner is to be picked by standing the children in a circle and then proceeding around the circle removing every other child until one remains (the winner). (Variants of this method are popular: 1 potato, 2 potato, 3 potato, 4; 5 potato, 6 potato, 7 potato, more and Eeny, meeny, miny, moe.) Number the children $1, \ldots, n$, in order as they stand in the circle (the process starts at child 1, and child 2 is the first to be removed). Let $J(n)$ be the winner when there are n children.
 (a) For $n = 8$, in what order are the children removed? Who is the winner (what is $J(8)$).
 (b) Compute $J(2), J(4), J(8), J(16), J(32)$. Can you guess $J(64)$?
 (c) Compute $J(3), J(6), J(12), J(24), J(48)$. Can you guess $J(96)$?
 (d) Formulate a conjecture for $J(2^k)$ for $k \geq 0$. You don't have to prove it.
 (e) Formulate a conjecture for $J(q2^k)$ in terms of $J(q)$, for $k \geq 0$. You don't have to prove it.
 (f) **[Hard]** Tinker like crazy and formulate a conjecture for $J(n)$. You don't have to prove it.
(In one version of the legend, Jewish historian Flavius Josephus and 40 other Jews are trapped in a cave by Romans. Instead of surrender, they stood in a circle, picking every seventh person to die at the hand of the next person picked (the last man standing commits suicide). Josephus determined where he and a friend should stand to be the last two men standing, at which point they promptly surrendered. Can you figure out where they stood?)

Problem 3.67 (Internet task). The function $f : A \mapsto B$ maps A to B. Lookup definitions of 1-to-1 (injection), onto (surjection), invertible (bijection) and give examples of each type of function when A and B are given by:
 (a) $A = \{1, 2\}$, $B = \{a, b\}$ (b) $A = \{1, 2\}$, $B = \{a, b, c\}$ (c) $A = \{1, 2, 3\}$, $B = \{a, b\}$.
(If you think it can't be done for specific cases, explain why.)

4.6 Problems

Problem 4.1. The six (or seven) "C's" of a good proof. Explain why each is important.

(a) Correct.   (c) Complete.   (e) Continuous (moving forward).

(b) Clear.   (d) Concise.   (f) Coordinated (well organized).

The seventh "C", which many mathematicians value dearly is Clever (elegant or beautiful).

Problem 4.2. What's wrong with this proof of "If n is even, then n^2 is even"? What is proved?

1: Suppose n^2 is even.

2: Let n have a prime factorization $n = p_1^{q_1} p_2^{q_2} \cdots p_k^{q_k}$.

3: Then, $n^2 = p_1^{2q_1} p_2^{2q_2} \cdots p_k^{2q_k}$. (Each prime appears an even number of times.)

4: Since n^2 is even, 2 is a prime factor, $p_1 = 2$). So, $n^2 = 2^{2q_1} p_2^{2q_2} \cdots p_k^{2q_k}$, with $q_1 > 0$.

5: So, $n = 2^{q_1} p_2^{q_2} \cdots p_k^{q_k}$, with $q_1 > 0$. That means 2 is a factor of n and, so n is even as claimed. ∎

Problem 4.3. Usinig $0 = 0$ and standard algebra, we prove $7 = 7$. Which proofs are valid? Why or why not?

(a) 1. $7 = 7$ (b) 1. Assume $7 \neq 7$ (c) 1. $0 = 0$

   2. $7 - 7 = 7 - 7$ 2. $7 - 7 \neq 7 - 7$ 2. $0 + 7 = 0 + 7$

   3. $0 = 0$ ☺   3. $0 \neq 0$ **!FISHY**   3. $7 = 7$ ☺

   $\rightarrow$ $7 = 7$ ✓ $\rightarrow$ $7 = 7$ ✓ $\rightarrow$ $7 = 7$ ✓

Problem 4.4. What is wrong with this bad proof that $4 = 7$?

1: $\mathbf{4 = 7}$ (what we are trying to prove)

2: $7 = 4$ ($a = b$ implies $b = a$)

3: $4 + 7 = 7 + 4$ ($a = b$ and $c = d$ implies $a + c = b + d$)

4: $\mathbf{11 = 11}$ ✓   (a known fact, hence our first step must be valid)

Problem 4.5. Here are two proofs that $2 = 1$. In each case, what went wrong?

(a) Let $a = 1$ and $b = 1$. Then,   (b) We use the fact that $-2 = -2$.

   1: We know $a = b$.   1: Hence, $4 - 6 = 1 - 3$,

   2: So, $2a^2 = a^2 + a^2 = a^2 + ab$.   2: So, $4 - 6 + 9/4 = 1 - 3 + 9/4$.

   3: So, $2a^2 - 2ab = a^2 - ab$.   3: That is, $(2 - 3/2)^2 = (1 - 3/2)^2$.

   4: Or, $2 \cdot (a^2 - ab) = 1 \cdot (a^2 - ab)$.   4: So, $2 - 3/2 = 1 - 3/2$.

   5: Dividing by $a^2 - ab$ gives $2 = 1$ ∎   5: Which means $2 = 1$.   ∎

Problem 4.6. Determine the true implications. If true, prove it. If false, give a counterexample. $\mathcal{H}$ is a set of horses.
[Hint: Consider separately the cases where $\mathcal{H}$ has fewer than 11 horses and $\mathcal{H}$ has at least 11 horses separately.]

(a) IF all 10-horse subsets of $\mathcal{H}$ have only gray horses, THEN all 11-horse subsets of $\mathcal{H}$ have only gray horses.

(b) IF some 10-horse subset of $\mathcal{H}$ has a black horse, THEN some 11-horse subset of $\mathcal{H}$ has a black horse.

Problem 4.7. Give direct proofs of each claim.

(a) $x, y \in \mathbb{Q} \rightarrow xy \in \mathbb{Q}$.   (c) For all $x, y \in \mathbb{Z}$, $x^2 + y^2$ is even $\rightarrow x + y$ is even.

(b) $n \in \mathbb{Z} \rightarrow n^2 + n$ is even.   (d) For all $a, b, c \in \mathbb{Z}$, (a divides b AND b divides c) $\rightarrow a$ divides c.

Problem 4.8. Give the contrapositive of each statement.

(a) If p is prime, then p is odd.   (c) If $n \in \mathbb{N}$ has remainder 2 or 3 when divided by 4, then n is not square.

(b) For $n \in \mathbb{Z}$, $n/(n+1) \notin \mathbb{Z}$.   (d) If $n \in \mathbb{N}$ is composite, then n has a prime divisor that is at most $\sqrt{n}$.

Problem 4.9. You may assume n is an integer. Give direct and contraposition proofs of:

(a) $(n^3 + 5$ is odd$) \rightarrow (n$ is even$)$.   (b) $(3$ does not divide $n) \rightarrow (3$ divides $n^2 + 2)$.

Problem 4.10. You may assume n is an integer. Prove by contraposition (explicitly state the contrapositive).

(a) x is irrational $\rightarrow \sqrt{x}$ is irrational.   (h) For $x, y > 0$, $y^3 + x^2 y \leq x^3 + xy^2 \rightarrow y \leq x$.

(b) $n^2 + 4n + 2$ is even $\rightarrow n$ is even.   (i) d doesn't divide $mn \rightarrow d$ doesn't divide m or n.

(c) $2^n - 1$ is prime $\rightarrow n$ is prime.   (j) $x^5 + 7x^3 + 5x \geq x^4 + x^2 + 8 \rightarrow x \geq 0$.

(d) n^3 is odd $\rightarrow n$ is odd.   (k) 3 divides $n - 2 \rightarrow n$ is not a perfect square.

(e) n^2 is not divisible by $4 \rightarrow n$ is odd.   (l) If $p > 2$ is prime, then $p^2 + 1$ is composite.

(f) If $p > 2$ is prime, then p is odd.   (m) For $x, y \in \mathbb{Z}$, $x^2 + y^2$ is even $\rightarrow x + y$ is even.

(g) If $2^n - n$ is prime, then n is odd.   (n) If xy is even, then x is even or y is even.

Problem 4.11. For $x, y \in \mathbb{N}$, which statements below are contradictions (cannot possibly be true). Explain.
(a) $x^2 < y$ (b) $x^2 = y/2$ (c) $x^2 - y^2 \leq 1$ (d) $x^2 + y^2 \leq 1$ (e) $2x + 1 = y^2 + 5y$ (f) $x^2 - y^2/2 = 1$ (g) $x^2 - y^2 = 1$.

Problem 4.12. Prove by contradiction:

(a) $\sqrt[3]{2}$ is irrational.

(b) $\sqrt{6}$ is irrational.

(c) $\log_2 9$ is irrational.

(d) $\forall(x, y) \in \mathbb{Z}^2 : 9x - 15y \neq 2$.

(e) $3 + 5\sqrt{2}$ is irrational.

(f) $\sin x + \cos x \geq 1$, where $x \in [0, \pi/2]$.

(g) There is no $q \in \mathbb{Q}$ for which $q - 1 = 1/q$.

(h) $(x, y) \in \mathbb{Z}^2 \rightarrow x^2 - 4y - 3 \neq 0$.

(i) For all real, positive x, y: $x + y \geq 2\sqrt{xy}$.

(j) $\forall(a, b, c) \in \mathbb{Z}^3 : (a^2 + b^2 = c^2) \rightarrow (a$ or b is even$)$.

(k) For $k \in \mathbb{N}$, $\sqrt{k} + \sqrt{k+1} < \sqrt{4k+2}$.

(l) There are no $x, y \in \mathbb{Q}$ for which $x^2 + y^2 = 3$.

(m) If 4 kids share 29 toys, someone gets at least 8 toys.

(n) Every prime number $p \geq 5$ is of the form $6k \pm 1$, where $k \in \mathbb{N}$.

Problem 4.13. Prove by contradiction:

(a) For real numbers a and b, $\lfloor a + b \rfloor \geq \lfloor a \rfloor + \lfloor b \rfloor$, where the floor $\lfloor \cdot \rfloor$ rounds down.

(b) In a right triangle with integer sides, the two shorter sides cannot both be odd.

(c) Given \$1, \$10, \$100 and \$1,000 bills, you can't get a value of 2^{n+1} using 2^n bills, for $n \in \mathbb{N}$.

(d) Let x, y, a be positive with $x \leq y$. Then, $(x + a)/(y + a) \geq x/y$.

(e) Let $a_1, a_2, \ldots, a_{10}$ be integers with $1/a_1 + 1/a_2 + \cdots + 1/a_{10} = 1$. Then, at least one of the a_i is even.

(f) If all points in the plane are red or blue, then between points of one color, all positive real distances are realized.

(g) Suppose, for $n > 3$, $a_1 + a_2 + \cdots + a_n \geq n$ and $a_1^2 + a_2^2 + \cdots + a_n^2 \geq n^2$. Then, $\max(a_1, a_2, \ldots, a_n) \geq 2$.

(h) The fraction $(21n + 4)/(14n + 3)$ is irreducible.

(i) If you cover an 8×8 chessboard with 32 dominos, some pair of adjacent dominos must form a 2×2 square.

Problem 4.14. Prove: If $a, b, c \in \mathbb{Z}$ are odd, then for all $x \in \mathbb{Q}$, $ax^2 + bx + c \neq 0$. (Contradiction in a direct proof.)

Problem 4.15. Determine the type of proof and prove. Tinker, tinker, tinker.

(a) The product of any two odd integers is odd.

(b) $\sqrt{5} + \sqrt{22} < \sqrt{48}$. (No calculators allowed!)

(c) If $3n + 2$ is odd then n is odd. Here, $n \in \mathbb{Z}$.

(d) For real numbers a, b with $a \neq b$, $a^2 + b^2 > 2ab$.

(e) For $n \in \mathbb{Z}$, $n^2 + 3n + 4$ is even. (Try cases).

(f) For $n \in \mathbb{N}$, $\sqrt{n(n+1)} \leq n + 1/2$.

(g) If n is odd, then $n^2 - 1$ is divisible by 8.

(h) For all positive real x, $x^2 + x^{-2} \geq 2$.

(i) $k > 0$ is odd. If $\sqrt{3}$ is irrational, then $\sqrt{3^k}$ is irrational.

(j) Every odd number is the difference of two squares.

(k) If mn is odd, then both m and n are odd. Here, $m, n \in \mathbb{Z}$.

(l) If $n^2 - 4n + 5$ is even then n is odd. Here, $n \in \mathbb{Z}$.

(m) If $2^n - 1$ is prime, then n is prime. Here, $n \in \mathbb{N}$.

(n) There exist integers m and n for which $2m + 3n = 13$.

(o) If $n \in \mathbb{Z}$, then $n^2 - 3$ is not divisible by 4. Here, $n \in \mathbb{N}$.

(p) If $x + y$ is irrational, then x is irrational or y is irrational.

Problem 4.16. Determine the type of proof and prove. Tinker, tinker, tinker.

(a) There is no fixed constant C for which $n^3 \leq Cn^2$ for all $n \in \mathbb{N}$.

(b) For any positive rational x, there is another positive rational $y < x$.

(c) Every nonzero rational number is a product of two irrational numbers.

(d) If $m - n$ is divisible by d, then $m^2 - n^2$ is divisible by d. Here, $m, n, d \in \mathbb{Z}$.

(e) If m is divisible by d and $m + n$ is divisible by d then n is divisible by d. Here, $m, n, d \in \mathbb{N}$.

(f) When dividing n by d, the quotient q and remainder $0 \leq r < d$ are unique. Here, $n, d, q, r \in \mathbb{Z}$.

(g) For $n \geq 2$, prove that none of $n! + 2$, $n! + 3, \ldots, n! + n$ are prime. Here, $n \in \mathbb{N}$.

(h) A perfect square number has remainder 0 or 1 when divided by 4.

(i) The numbers $m = 3^{2017} + 25$ and $n = 3^{2017} + 26$ cannot both be perfect squares.

(j) If a and b are positive real numbers with $ab < 10,000$, then $\min(a, b) < 100$.

(k) A right triangle with integer sides can't be isoceles. *[Hint: Pythagoras and $\sqrt{2}$ is irrational.]*

Problem 4.17. Determine true or false for each statement. Explain.
(a) Joy is sleeping if and only if Joy is snoring.   (b) It is raining if and only if it is cloudy.

Problem 4.18. Determine true or false for each claim. Prove your answer. (m, n are integers and x, y are reals.)

(a) n is an even prime if and only if $n = 2$.

(b) $m^2 - n^2$ is even if and only if $m - n$ is even.

(c) $2^n - 1$ is prime if and only if n is prime.

(d) n^2 is even if and only if n^2 is a multiple of 4.

(e) 4 divides n^2 if and only if 4 divides n.

(f) $m^2 + n^2$ is even if and only if $m + n$ is even.

(g) mn is even if and only if both m and n are even.

(h) mn is odd if and only if both m and n are odd.

(i) 6 divides n if and only if both 2 and 3 divide n.

(j) $x + y$ is irrational if and only if both x and y are irrational.

Problem 4.19. Prove these if and only if claims. You must prove two implications. (Break the proof into cases.)

(a) Prove: 4 divides $n \in \mathbb{Z}$ IF AND ONLY IF $n = 1 + (-1)^k(2k - 1)$ for $k \in \mathbb{N}$. (Try $n < 0, n = 0, n > 0$; k even/odd.)

(b) The natural numbers w, x, y, z satisfy $z^2 = w^2 + x^2 + y^2$. Prove that z is even IF AND ONLY IF w, x, y are all even. (Try w, x, y being even/odd.)

Problem 4.20. Assume any natural number n has a unique factorization into primes. Let p be any prime. Prove:

(a) n is divisible by p IF AND ONLY IF n^2 is divisible by p.   (b) $\sqrt{p}$ is irrational. (Contradiction.)

Problem 4.21. Prove or disprove. Tinker, tinker, tinker.

(a) For all $n \in \mathbb{Z}$, $n/(n+1) \notin \mathbb{Z}$.

(b) For all $n \in \mathbb{N}$, $n/(n+1) \notin \mathbb{N}$.

(c) If $\sqrt{r}$ is irrational, then r is irrational.

(d) If r is irrational, then $\sqrt{r}$ is irrational.

(e) For every $n \in \mathbb{N}$, $3^n + 2$ is prime.

(f) For every $n \in \mathbb{N}$, $n^2 + n$ is even.

(g) If $x \in \mathbb{R}$ then $x \leq x^2$.

(h) For $n \in \mathbb{N}$, $\lfloor n/2 \rfloor + \lceil n/2 \rceil = n$.

(i) If x, y are rational, then y^x is rational.

(j) $x \in \mathbb{Q}$ and $y \notin \mathbb{Q} \to xy \notin \mathbb{Q}$.

(k) $x \in \mathbb{Q}$, $x \neq 0$ and $y \notin \mathbb{Q} \to xy \notin \mathbb{Q}$.

(l) Every even square number is a multiple of 4.

(m) For all integers m, n, if $m < n$ then $m^2 < n^2$.

(n) For any two sets A and B, $A \nsubseteq B \to B \subseteq A$.

(o) There exist integers m, n for which $2m^2 + 5n^2 = 14$.

(p) For $n \in \mathbb{Z}$, if 3 divides n^2, then 3 divides n.

(q) For $n \in \mathbb{Z}$, if 4 divides n^2, then 4 divides n.

(r) For $n \in \mathbb{Z}$, if 6 divides n^2, then 6 divides n.

Problem 4.22. Prove or disprove. Tinker, tinker, tinker.

(a) There exist integers m, n for which $\sqrt{m+n} = \sqrt{m} + \sqrt{n}$.

(b) The product of four consecutive positive integers can never be a perfect square.

(c) If x, y are irrational, then y^x is irrational. [Hint: $(\log_2 9, \sqrt{2})$ or $(\sqrt{2}, \sqrt{2}^{\sqrt{2}})$.]

(d) For $x \in \mathbb{R}$ and $x \geq 0$, $\lfloor x \rfloor + \lfloor x + 1/3 \rfloor + \lfloor x + 2/3 \rfloor = \lfloor 3x \rfloor$.

(e) For some real $x > 0$, there is a constant C for which $n^{2+x} \leq Cn^2$ for all $n \in \mathbb{N}$.

(f) If $n \geq 2$ is not prime, then $2n + 13$ is not prime. Here, $n \in \mathbb{N}$.

(g) If d divides the product mn, then d divides m or d divides n. Here, $m, n, d \in \mathbb{N}$.

(h) n is odd if and only if $n^2 - 1$ is divisible by 8. Here, $n \in \mathbb{Z}$.

Problem 4.23. Let x be rational and let y be irrational, with $x < y$. Prove or disprove.

(a) Between x and y is some irrational number. [Hint: Average]   (b) Between x and y is some rational number.

Problem 4.24. Prove this complicated implication:
$$(\neg \exists (x, y) \in \mathbb{Q}^2 : x^2 + y^2 = 3) \to (\text{for all odd } k, \ \neg \exists (v, w) \in \mathbb{Q}^2 : v^2 + w^2 = 3^k).$$

Problem 4.25 (Cyclic shift). A binary number $\mathbf{b} = b_m b_{m-1} \cdots b_2 b_1 b_0$, where $b_i \in \{0, 1\}$ and $b_m = 1$ represents the integer $n(\mathbf{b}) = b_0 2^0 + b_1 2^1 + \cdots + b_m 2^m$. The cyclic shift of $\mathbf{b}$ moves the leftmost bit b_m to the rightmost to give $\mathbf{b}_c = b_{m-1} \cdots b_2 b_1 b_0 b_m$ (b_{m-1} could be 0), corresponding to the integer $n(\mathbf{b}_c)$.

(a) For $\mathbf{b} = 101001$, what is the cyclic shift $\mathbf{b}_c$? Compute $n(\mathbf{b})$ and $n(\mathbf{b}_c)$.

(b) Given $\mathbf{b} = b_m b_{m-1} \cdots b_2 b_1 b_0$, what is $n(\mathbf{b}_c)$ as a sum?

(c) Prove that $n(\mathbf{b}_c) \leq n(\mathbf{b})$ for all $\mathbf{b}$. When does $n(\mathbf{b}_c)$ equal $n(\mathbf{b})$? (Assume $2^0 + 2^1 + 2^2 + \cdots + 2^k = 2^{k+1} - 1$.)

Problem 4.26. A number n is triangular if $n = 1 + 2 + \cdots + k = k(k+1)/2$ for some $k \in \mathbb{N}$. (You may use the formula for the sum without proof.) A number n is square if $n = k^2$ for some $k \in \mathbb{N}$.

(a) List the first 10 triangular and square numbers. Compare with $k(k+1)/2$ for $k = 1, 2, \ldots, 10$.

(b) Prove: if n is triangular, then so too are $9n + 1$, $25n + 3$, $49n + 6$ and $81n + 10$.

(c) Prove: n is triangular if and only if $8n + 1$ is square.

Problem 4.27. A triangle is drawn on the plane. The vertices of the triangle have integer coordinates. Prove that the triangle cannot be equilateral. *[Hints: You must prove something does not exist – what proof method would you pick? Pythagoras' Theorem will be useful, as will irrational numbers. Persevere.]*

Problem 4.28. A comparison scale can only compare weights.

(a) You have 3 balls, one is heavier. Can you can determine which ball is heavier in one weighing? Prove it. Repeat for 9 balls and two weighings.

(b) You have 4 balls, one is heavier. Can you can determine which ball is heavier in one weighing? Prove it. Repeat for 10 balls and two weighings.

Problem 4.29. The points in the plane are colored red, blue or green. Prove by contradiction.
(a) If there are no green points, then there is an equilateral triangle of side 1 or $\sqrt{3}$ with monochromatic vertices.
(b) There are two points of the same color a distance 1 apart.
(c) Fix any 16×9 rectangular grid. One can form a rectangle using monochromatic points on the grid.

Problem 4.30. Basketball Bob's cumulative free throw percentage early in the season was below 80%. Later, in the season it was above 80%. Must it have been exactly 80% at some point in the season?

Problem 4.31. A 5×5 board is missing a square (black). Cover the remaining squares with L-shaped tiles, ▟. You may rotate tiles, but tiles cannot overlap or hang off the board. Don't be upset if you fail. Prove there is no L-tiling of this deficient board. As a hint, we have shaded in some squares gray.

Problem 4.32. Explain how to prove and disprove the following statements.
(a) $\neg P(n) \to Q(n)$
(b) $\neg (P(n) \to Q(n))$
(c) $\forall n : (P(n) \to Q(n))$
(d) $\forall x : ((\forall n : P(n)) \to Q(x))$
(e) $\exists n : (P(n) \to Q(n))$
(f) $\exists x : ((\exists n : P(n)) \to Q(x))$

Problem 4.33. For $(a, b) \in \mathbb{R}^2$, which mathematical claim below do you think is true?
(a) If $(\forall (a, b) : ax + b = 0)$, then $x = 0$.
(b) $\forall (a, b) : ($if $ax + b = 0$, then $x = 0)$.

Problem 4.34. Let $\mathcal{D} = \{n \mid P(n)$ is T$\}$. Prove $(\forall n \in \mathcal{D} : Q(n)) \leftrightarrow (P(n) \to Q(n))$.
(a) $(\forall n \in \mathcal{D} : Q(n)) \to (P(n) \to Q(n))$.
(b) $(P(n) \to Q(n)) \to (\forall n \in \mathcal{D} : Q(n))$.

Problem 4.35. Suppose $p \to q$ is true. Show $(p \wedge r) \to q$ is true, the stronger assumption p and r also implies q.

Problem 4.36. Recall $p \leftrightarrow q \overset{eqv}{\equiv} (p \to q) \wedge (q \to p)$. Show that $p \leftrightarrow q \overset{eqv}{\equiv} (p \wedge q) \vee (\neg p \wedge \neg q)$:
(a) Use truth-tables.
(b) Use the rules in Figure 3.1 on page 29. *[Hints: $p \wedge \neg p \overset{eqv}{\equiv}$ F and $x \vee$ F $\overset{eqv}{\equiv} x$.]*

Problem 4.37. In 1637, Pierre de Fermat made a claim (Fermat's Last Theorem) that was only proved 357 years later by Andrew Wiles. You may assume Fermat's Last Theorem:
$$\text{If } a, b, c, n \text{ are natural numbers with } n > 2, \text{ then } a^n + b^n \neq c^n.$$
Use contradiction to show that $2^{1/p}$, p-th root of 2 is irrational for integer $p > 2$.

Problem 4.38. Prove $p \to p$ is true for any statement p.

Problem 4.39. "q is necessary and sufficient for p" is another way to say $p \leftrightarrow q$.
(a) For p to be true, it is necessary that q be true. Which of the statements below must be true:
$$p \to q; \qquad q \to p; \qquad p \leftrightarrow q.$$
(b) For p to be true, it is sufficient that q be true. Now, which statements must be true.

Problem 4.40. Given that every natural number is either prime or divisible by a prime, prove by contradiction that there are infinitely many primes. *[Hint: For $x_1, x_2, \ldots, x_n \geq 2$, $x_1 x_2 \cdots x_n + 1$ is not divisible by any of $x_1, x_2, \ldots, x_n$.]*

Problem 4.41. Prove $\overline{A \cap B \cap C} = \overline{A} \cup \overline{B} \cup \overline{C}$. (a) Using Venn diagrams. (b) Show: $x \in \overline{A \cap B \cap C} \leftrightarrow x \in \overline{A} \cup \overline{B} \cup \overline{C}$.
(c) Derive $\overline{A} \cup \overline{B} \cup \overline{C}$ from $\overline{A \cap B \cap C}$ using the rules in Figure 2.1 on page 17.

Problem 4.42. Give "proof" by pictures using Venn diagrams for each set relationship:
(a) $\overline{A \cap B} = \overline{A} \cup \overline{B}$.
(b) $\overline{A \cup B} = \overline{A} \cap \overline{B}$.
(c) $A \cap \overline{A} = \varnothing$.
(d) $A \cap B \subseteq A$.
(e) $(A \cap B) \cup (A \cap \overline{B}) = A$.
(f) $(A \cup B) \cap \overline{A} = B \cap \overline{A}$.
(g) $(\overline{A \cup B}) \cap A = \varnothing$.
(h) $(\overline{A \cap B}) \cap A = A \cap \overline{B}$.
(i) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
(j) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
(k) $A \cap (B \cap C) = (A \cap B) \cap C$.
(l) $|A| + |B| = |A \cup B| + |A \cap B|$.

Problem 4.43. Give formal proofs for each equality in Problem 4.42.

Problem 4.44. The set difference $A - B$ contains the elements in A that are not in B.
(a) Give $A - B$ and $B - A$ for (i) $A = \{1, 2, 3, 4\}$, $B = \{2, 4, 6, 8, 10\}$. (ii) $A = \{3k \mid k \in \mathbb{N}\}$, $B = \{p | p \in \mathbb{N}$ is prime$\}$.
(b) Give an expression for $A - B$ in terms of A and B using only intersection, union and complements.
(c) Use Venn diagrams to prove or disprove: $A \cup (B - C) = (A \cup B) - C$.

Problem 4.45. $A = \{(x, y) \in \mathbb{R}^2 \mid y = x^2\}$; $B = \{(x, y) \in \mathbb{R}^2 \mid y = 2 - x\}$. What is $A \cap B$?

Problem 4.46. Prove that $A = B$, where A and B are the sets defined below.

(a) $A = \{x \mid x = 2k + 1, k \in \mathbb{Z}\}$ $\qquad\qquad$ $B = \{x \mid x = 2m - 17, m \in \mathbb{Z}\}$

(b) $A = \{(i, j) \mid 1 \le i \le n \text{ and } 1 \le j \le i\}$ $\qquad$ $B = \{(i, j) \mid j \le i \le n \text{ and } 1 \le j \le n\}$

Problem 4.47. In each case, prove (or disprove) a relationship between the sets.

(a) $A = \{2k, k \in \mathbb{N}\}$, $B = \{3k, k \in \mathbb{N}\}$, and $C = \{6k, k \in \mathbb{N}\}$. Prove $A \cap B = C$.

(b) $A = \{7k, k \in \mathbb{N}\}$ and $B = \{3k, k \in \mathbb{N}\}$. Prove $A \cap B \ne \varnothing$.

(c) $A = \{4k - 3, k \in \mathbb{N}\}$ and $B = \{4k + 1, k \in \mathbb{N}\}$. Prove or disprove $A = B$.

(d) $A = \{4k + 1, k \in \mathbb{Z}\}$ and $B = \{4k + 5, k \in \mathbb{Z}\}$. Prove or disprove $A = B$.

(e) $A = \{12m + 21n, m, n \in \mathbb{Z}\}$. Prove or disprove $A = \mathbb{Z}$.

(f) $A = \{12m + 25n, m, n \in \mathbb{Z}\}$. Prove or disprove $A = \mathbb{Z}$.

Problem 4.48. Prove the following facts about the power set of A and B.

(a) $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$. $\qquad$ (b) $\mathcal{P}(A) \subseteq \mathcal{P}(B) \leftrightarrow A \subseteq B$.

Problem 4.49. Prove that there exists a unique set A for which $A \cup B = B$ for all sets B.

Problem 4.50 (Closure). A set system is a collection of sets, $\mathcal{C} = \{\mathcal{A}_1, \mathcal{A}_2, \ldots\}$, where $\mathcal{A}_i$ are sets of elements from a universal set $\mathcal{U}$. The set system $\mathcal{C}$ is closed under a set-operation if performing the operation on sets in $\mathcal{C}$ produces only sets in $\mathcal{C}$. Here are examples of closure:

- **Closed under finite union.** If $\mathcal{A}_1, \mathcal{A}_2 \in \mathcal{C}$, then $\mathcal{A}_1 \cup \mathcal{A}_2 \in \mathcal{C}$.
- **Closed under finite intersection.** If $\mathcal{A}_1, \mathcal{A}_2 \in \mathcal{C}$, then $\mathcal{A}_1 \cap \mathcal{A}_2 \in \mathcal{C}$.
- **Closed under complement.** If $\mathcal{A}_1 \in \mathcal{C}$, then $\overline{\mathcal{A}_2} \in \mathcal{C}$.

(a) Let $\mathcal{C} = \{\mathcal{A}\}$ have one set $\mathcal{A}$. Show that $\mathcal{C}$ is closed under union and intersection. What about complement?

(b) Let $\mathcal{C} = \{\varnothing, \mathcal{A}, \overline{\mathcal{A}}, \mathcal{U}\}$. Show that $\mathcal{C}$ is closed under union, intersection and complement.

(c) Prove that if $\mathcal{C}$ is closed under union and complement, then $\mathcal{C}$ is closed under intersection.

(d) Give a set system $\mathcal{C}$ containing at least 4 sets that is closed under union and intersection, but not closed under complement. (Make sure to specify the universal set.)

Problem 4.51. Study these definitions of convergence and prove or disprove the claims. (In all cases, $n \in \mathbb{N}$.)

> **Definition.** $f(n) \to \infty$ if for every $C > 0$, there is n_C such that for all $n \ge n_C$, $f(n) \ge C$.
> **Definition.** $f(n) \to a$ if for every $\varepsilon > 0$, there is n_ε such that for all $n \ge n_\varepsilon$, $|f(n) - a| \le \varepsilon$.

(a) $f(n) = (2n^2 + 3)/(n + 1)$. (i) $f(n) \to \infty$. (ii) $f(n) \to 1$. (iii) $f(n) \to 2$.

(b) $f(n) = (n + 3)/(n + 1)$. $\quad$ (i) $f(n) \to \infty$. (ii) $f(n) \to 1$. (iii) $f(n) \to 2$.

(c) $f(n) = n \sin^2(n\pi/2)$. $\quad\quad$ (i) $f(n) \to \infty$. (ii) $f(n) \to 1$. (iii) $f(n) \to 2$.

Problem 4.52 (Without Loss Of Generality (wlog)). Consider the following claim.

> If x and y have opposite parity (one is odd and one is even), then $x + y$ is odd.

Explain why, in a direct proof, we may assume that x is odd and y is even? Prove the claim.
(Such a proof starts "Without loss of generality, assume x is odd and y is even. Then, ...")

Problem 4.53. Use the concept of "without loss of generality" to prove these claims.

(a) If d does not divide mn, then d does not divide m or n. (Use contraposition.)

(b) For integers x, y, if xy is not divisible by 5 then x and y are both not divisible by 5.

(c) For any nonzero real number x, $x^2 + 1/x^2 \ge 2$.

(d) For non-negative x, y, $\max(x, y) \le x + y$.

(e) **Triangle Inequality.** For all $x, y \in \mathbb{R}$, $|x + y| \le |x| + |y|$.

(f) **Schur's Inequality.** For $a, b, c \ge 0$ and $r > 0$, $a^r(a - b)(a - c) + b^r(b - a)(b - c) + c^r(c - a)(c - b) \ge 0$.

(g) Points in $\mathbb{R}^2$ are colored red or blue. Prove there are two points of the same color a distance d apart, for $d > 0$.

(h) No right triangle has sides which are Fibonacci numbers $(1, 1, 2, 3, 5, 8, 13, \ldots$, each number being the sum of the previous two). *[Hint: Triangle inequality; contradiction.]*

5.3 Problems

Problem 5.1. Is $2^p - 1$ prime for the primes $p = 2, 3, 5, 7$? Is $2^p - 1$ prime whenever p is prime?

Problem 5.2. Is $n^2 + n + 41$ prime for $n = 1, 2, \ldots, 10$. Is $n^2 + n + 41$ prime for all $n \in \mathbb{N}$?

Problem 5.3. For which n is $P(n)$ true? Explain by showing the "chain" of implications.
 (a) $P(2)$ is true and $P(n) \to P(n+1)$ for $n \geq 0$.
 (b) $P(1)$ is true and $P(n) \to (P(2n) \wedge P(2n+1))$ for $n \geq 1$.
 (c) $P(2)$ is true and $P(n) \to (P(n^2) \wedge P(n-2))$ for $n \geq 2$.
 (d) $P(1), P(2), P(3)$ are true and $P(n) \to P(n+4)$ for $n \geq 1$.
 (e) $P(0), P(1)$ are true and $P(n) \to P(n+2)$ for $n \geq 0$.
 (f) $P(0), P(1), P(2)$ are true and $P(n) \to P(3n)$ for $n \geq 1$.

Problem 5.4. Which, if any, is a valid way to prove $P(n) \to P(n+1)$. (Compare with the **BAD** proof on page 59.)
 (i) Let's see what happens if $P(n+1)$ is true.   (ii) Let's see what happens if $P(n+1)$ is F.
    $\vdots$ (valid derivations) $\vdots$ (valid derivations)
    Look! $P(n)$ is true.   ✓   Look! $P(n)$ is F.   ✓

Problem 5.5. Let us use induction to prove the conjecture: "If every person in an n-person social network has at least one friend, then everyone is linked to everyone else by a chain of friendships. Such a network is connected."

> When $n = 2$ the claim holds. For $n \geq 2$, assume any n-person network with people $p_1, \ldots, p_n$ is connected. Now add a person p_{n+1} to get an $(n+1)$-person network. Recall $p_1, \ldots, p_n$ are linked to each other. The new person p_{n+1} has a friend (say) p_j. Since p_j is linked to $p_1, \ldots, p_n$, this means p_{n+1} is linked to everyone else. Thus everyone is linked to everyone else, and the claim holds for $n+1$. ∎

Show that the conjecture is not true, and explain what is wrong with the induction proof above.

Problem 5.6. Prove by induction: $2 \times 2^1 + 3 \times 2^2 + 4 \times 2^3 + \cdots + (n+1) \times 2^n = n \times 2^{n+1}$, for $n \geq 1$.

Problem 5.7. Determine for which n the claim is true and use induction to prove it.
 (a) $2^0 + 2^1 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$.
 (b) $1 + 3 + 5 + \cdots + (2n-1) = n^2$.
 (c) $\dfrac{1}{1 \cdot 2} + \dfrac{1}{2 \cdot 3} + \dfrac{1}{3 \cdot 4} + \cdots + \dfrac{1}{n \cdot (n+1)} = \dfrac{n}{n+1}$.
 (d) $0 \cdot 1 + 1 \cdot 2 + \cdots + n \cdot (n+1) = n(n+1)(n+2)/3$.
 (e) $1/2 + 2/4 + 3/8 + \cdots + n/2^n = 2^{-n}(2^{n+1} - n - 2)$.
 (f) $\left(1 - \dfrac{1}{2}\right)\left(1 - \dfrac{1}{3}\right)\left(1 - \dfrac{1}{4}\right) \cdots \left(1 - \dfrac{1}{n}\right) = \dfrac{1}{n}$.

Problem 5.8. Prove by induction, for $n \geq 2$, $\left(1 - \dfrac{1}{1+2}\right)\left(1 - \dfrac{1}{1+2+3}\right) \cdots \left(1 - \dfrac{1}{1+2+\cdots+n}\right) = \dfrac{n+2}{3n}$.

Problem 5.9. Prove by induction, for $n \geq 1$,
 (a) $1 + \dfrac{1}{\sqrt{2}} + \dfrac{1}{\sqrt{3}} + \cdots + \dfrac{1}{\sqrt{n}} \geq \sqrt{n}$ (b) $1 + \sqrt{2} + \sqrt{3} + \cdots + \sqrt{n} \leq n\sqrt{n}$ (c) $\dfrac{1 \times 3 \times 5 \times \cdots \times (2n-1)}{2 \times 4 \times 6 \times \cdots \times 2n} \leq \dfrac{1}{\sqrt{n+1}}$.

Problem 5.10. Determine for which n the claim is true and use induction to prove it.
 (a) 5 divides $11^n - 6$.
 (b) 7 divides $n^7 - n$.
 (c) 24 divides $5^{2n} - 1$.
 (d) 8 divides $3^{2n} - 1$.
 (e) 5 divides $2^{3n} - 3^n$.
 (f) 7 divides $5^{2n+1} + 2^{2n+1}$.
 (g) 6 divides $17n^3 + 103n$.
 (h) 5 divides $4 \cdot 3^n + (-2)^n$.
 (i) 3 divides $5^n + 2 \cdot 11^n$.
 (j) 3 divides $n^3 + 5n + 6$.
 (k) 3 divides $n^3 + 2n$.
 (l) 6 divides $n^3 - n$.
 (m) 4 divides $n^4 - n^2$.
 (n) 5 divides $6^n + 4$.
 (o) 3 divides $2^{2n-1} + 1$.
 (p) 9 divides $4^{3n} + 8$.
 (q) 80 divides $3^{4n} - 1$.
 (r) 10 divides $13^n - 3^n$.
 (s) 12 divides $5 \cdot 9^n + 3$.
 (t) 8 divides $7^n - (-1)^n$.

Problem 5.11. Use induction to prove these facts about divisibility.

 (a) For positive odd n (i) 8 divides $n^2 - 1$ (ii) 16 divides $n^4 - 1$.
 (b) 3 divides $2^{3n} + 2^{n+1}$ for $n \geq 0$.
 (c) 3^{n+1} divides $2^{3^n} + 1$ for $n \geq 0$.
 (d) 15 divides $4^{2n+1} + 5^{2n+1} + 6^{2n+1}$ for $n \geq 0$.

Problem 5.12. For $n \geq 1$, prove by induction:

 (a) $4n \leq 2^{n+1}$.
 (b) $n^2 \leq 2^{n+1}$.
 (c) $n! \geq 2^{n-1}$.
 (d) $3^n > n^2$.
 (e) $n! \leq n^n$.
 (f) $1 + 2 + \cdots + n \leq n^2$.
 (g) $1^2 + 2^2 + \cdots + n^2 > n^3/3$.
 (h) $10^0 + 10^1 + \cdots + 10^n < 10^{n+1}$.
 (i) $n! \geq n^n e^{-n}$.   *[Hint:* $(1 + 1/n)^n \leq e.]$
 (j) Bernoulli's inequality: $(1 + x)^n \geq 1 + nx$ for $x \geq -1$.

Problem 5.13. Determine for which n the claim is true and prove it by induction.

(a) k is odd implies k^n is odd.

(b) $\sqrt[n]{n} \leq 2 - 1/n$.

(c) $2^{1/2^n}$ is not rational.

(d) 5 divides $(x - 2)$ implies 5 divides $x^n - 2^n$.

(e) For $x > 0$, (i) $(1 + x)^n \leq 1 + nx + n^2 x^2$ (ii) $(1 - x)^n \leq 1 - nx + n^2 x^2/2$.

(f) **[Challenging!]** $\mathrm{Re}[(\cos x + i \sin x)^n] = \cos nx$.

Problem 5.14. Prove by induction that the last digit of 3^{4n} is 1, for $n \geq 0$.

Problem 5.15. Prove: 9 divides $10^n - 1$ for $n \geq 0$. Hence, show: 9 divides x if and only if 9 divides x's digit-sum.

Problem 5.16. Prove that $(3^{2^n} - 1)/2^{n+2}$ is an odd integer for $n \geq 1$.

Problem 5.17. Prove $1 + \dfrac{1}{2} + \dfrac{1}{3} + \cdots + \dfrac{1}{2^k} \geq 1 + \dfrac{k}{2}$, for $k \geq 0$ and hence $1 + \dfrac{1}{2} + \dfrac{1}{3} + \cdots + \dfrac{1}{n} \geq \dfrac{1}{2}(1 + \log_2 n)$.

Problem 5.18. The nth Harmonic number is $H_n = 1 + 1/2 + 1/3 + \cdots + 1/n$, for $n \geq 1$. Prove:

(a) $H_1 + H_2 + \cdots + H_n = (n + 1)H_n - n$.

(b) $1 + (\ln n)/2 \leq H_n \leq 1 + \ln n$.   *[Hint: For $0 \leq x \leq 1/2$, $-2x \leq \ln(1 - x) \leq -x$.]*

Problem 5.19. Let $x_1, \ldots, x_n$ be positive and sum to $1/2$, $x_1 + x_2 + \cdots + x_n = 1/2$. Prove:

$$\frac{1 - x_1}{1 + x_1} \times \frac{1 - x_2}{1 + x_2} \times \frac{1 - x_3}{1 + x_3} \times \cdots \times \frac{1 - x_n}{1 + x_n} \geq \frac{1}{3}.$$

Problem 5.20. Prove, by induction, that every $n \geq 1$ is a sum of distinct powers of 2.

Problem 5.21. Let A be a finite set of size $n \geq 1$, prove by induction that $|\mathcal{P}(A)| = 2^n$.

Problem 5.22. Prove each case by induction. Then, guess the general pattern and prove your guess by induction.

(a) $\sum_{i=1}^n i = 1 + 2 + \cdots + n = n(n + 1)/2$

(b) $\sum_{i=1}^n i(i + 1) = 1 \cdot 2 + 2 \cdot 3 + \cdots + n \cdot (n + 1) = n(n + 1)(n + 2)/3$

(c) $\sum_{i=1}^n i(i + 1)(i + 2) = 1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + \cdots + n \cdot (n + 1) \cdot (n + 2) = n(n + 1)(n + 2)(n + 3)/4$

Problem 5.23. After determining for which n the claim holds, prove it by induction:

(a) $\left(1 - \dfrac{1}{\sqrt{2}}\right)\left(1 - \dfrac{1}{\sqrt{3}}\right)\left(1 - \dfrac{1}{\sqrt{4}}\right) \cdots \left(1 - \dfrac{1}{\sqrt{n}}\right) \leq \dfrac{2}{n^2}$.

(b) $\left(1 - \dfrac{1}{2}\right)\left(1 - \dfrac{1}{4}\right)\left(1 - \dfrac{1}{8}\right) \cdots \left(1 - \dfrac{1}{2^n}\right) \geq \dfrac{1}{4} + \dfrac{1}{2^{n+1}}$.

(c) $1 - \dfrac{1}{n + 1} < 1 + \dfrac{1}{4} + \dfrac{1}{9} + \cdots + \dfrac{1}{n^2} \leq 2 - \dfrac{1}{n}$.

(d) $\dfrac{1}{n + 1} + \dfrac{1}{n + 2} + \cdots + \dfrac{1}{2n} > \dfrac{11}{18}$.

Problem 5.24. Prove by induction on n: $\overline{A_1 \cup A_2 \cup A_3 \cup \cdots \cup A_n} = \overline{A_1} \cap \overline{A_2} \cap \overline{A_3} \cap \cdots \cap \overline{A_n}$.

Problem 5.25. Use the method of differences to guess a formula for $S(n)$. Prove your guess.

(a) $S(n) = 1 + 4 + 7 + \cdots + (3n - 2)$ (b) $S(n) = \sum_{i=1}^n i(i + 1)^2$ (c) $S(n) = \sum_{i=1}^{2n} (-1)^i i^2$.

Problem 5.26. In each problem, compute a formula for the quantity of interest. Use the following strategy: (i) Tinker with small values of n, for example $n = 1, 2, 3, 4, 5$. (ii) Guess a solution. (iii) Prove your guess by induction.

(a) The product $\Pi(n) = (1 - 1/2)(1 - 1/3) \cdots (1 - 1/(n + 1))$, for $n \geq 1$.

(b) The product $\Pi(n) = (1 - 1/4)(1 - 1/9) \cdots (1 - 1/n^2)$, for $n \geq 2$.

(c) The sum $S(n) = \sum_{i=1}^{2n} (-1)^i i$, for $n \geq 1$.

(d) The sum $S(n) = 1 \cdot 3 + 3 \cdot 5 + 5 \cdot 7 + \cdots + (2n - 1)(2n + 1)$, for $n \geq 1$.

(e) The sum $S(n) = 1/(1 \cdot 2) + 1/(2 \cdot 3) + 1/(3 \cdot 4) + \cdots + 1/(n(n + 1))$, for $n \geq 1$.

(f) The sum $S(n) = 1/2! + 2/3! + 3/4! + \cdots + n/(n + 1)!$, for $n \geq 1$.

(g) The sum $S(n) = 1/2 + 2/3 + 3/4 + \cdots n/(n + 1)$.

(h) The product $\Pi(n) = \cos \theta \times \cos(2\theta) \times \cos(4\theta) \times \cdots \times \cos(2^n \theta)$, for $n \geq 0$. *[Hint: Multiply by $\sin \theta$; $\sin 2A =?$.]*

(i) The product $\Pi(n) = (1 + 1/3)(1 + 1/3^2)(1 + 1/3^4) \cdots (1 + 1/3^{2^n})$, for $n \geq 0$. *[Hint: $(1 - 1/3) \times \Pi(n)$.]*

(j) The nth derivative of $x^2 e^x$, that is $\dfrac{d^n}{dx^n}(x^2 e^x)$, for $n \geq 1$.

(k) The integral $\Gamma(n) = \int_0^\infty dx \, x^{n-1} e^{-x}$, for $n \geq 1$.

(l) The sum $S(n) = \sum\limits_{\substack{\mathcal{A} \subseteq [n] \\ \mathcal{A} \neq \varnothing}} \prod_{x \in \mathcal{A}} 1/x$, for $n \geq 1$. (The index $\mathcal{A}$ is over the non-empty subsets of $[n] = \{1, \ldots, n\}$.)

Problem 5.27. Place n circles on the plane, dividing the plane into regions. Prove that you can color the regions red and blue so that no two regions which share a boundary at a circle have the same color.

Problem 5.28. Prove each claim by induction for $n \geq 3$.
 (a) There is a set with n numbers $x_1, \ldots, x_n$ such that each x_i divides the sum $s = x_1 + \cdots + x_n$.
 (b) There is a convex polygon having n sides and at least 3 acute internal angles.
 (c) There are n distinct positive numbers whose reciprocals sum to 1.

Problem 5.29. Prove by induction that the derivative of x^n is nx^{n-1}, for $n \geq 1$. *[Hint: $(fg)' = f'g + fg'$.]*

Problem 5.30. Prove that the nth derivative of x^n is $n!$, for $n \geq 1$.

Problem 5.31 (Nested Roots). Let $x_1 = \sqrt{1}$, $x_2 = \sqrt{1 + \sqrt{1}}$, $x_3 = \sqrt{1 + \sqrt{1 + \sqrt{1}}}$, and so on. We can get x_{n+1} from x_n using $x_{n+1} = \sqrt{1 + x_n}$. Prove that: (a) $x_n \leq 2$.   (b) x_n is monotonically increasing.
By monotone convergence (calculus), x_n converges. Make a conjecture for $\lim_{n \to \infty} x_n$.

Problem 5.32 (A Formula of Ramanujan). The math prodigy Ramanujan derived the remarkable formula:

$$2 = \sqrt{1 + 1\sqrt{1 + 2\sqrt{1 + 3\sqrt{1 + 4\sqrt{1 + \cdots}}}}}. \tag{5.1}$$

 (a) Numerically verify (5.1) by computing the RHS to a high accuracy using many terms.
 (b) Assume Ramanujan's formula is valid. Generalize the formula by proving, for all $n \geq 1$:

$$n + 1 = \sqrt{1 + n\sqrt{1 + (n+1)\sqrt{1 + (n+2)\sqrt{1 + (n+3)\sqrt{1 + \cdots}}}}}.$$

Problem 5.33. Prove, for $n \geq 3$, that every convex n-gon has $n(n-3)/2$ diagonals (that are not sides).

Problem 5.34. Prove that the sum of interior angles of a convex polygon with n sides is $(n-2)\pi$. You may assume the result is true for triangles ($n = 3$), and that one can cut a convex n-gon into a convex $(n-1)$-gon and a triangle as shown. (A convex polygon has all interior angles smaller than π.)
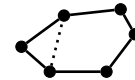
**Problem 5.35.** Suppose $a, b \geq 0$ (non-negative reals). Prove by induction:
 (a) $(a+b)^n \geq a^n + b^n$, for $n \geq 1$.
 (b) $(a+b)^n \geq a^n + b^n + 2ab(a+b)^{n-2}$, for $n \geq 2$.
 (c) $(a+b)^n \geq a^n + b^n + nab(a^{n-2} + b^{n-2})$, for $n \geq 2$.

Problem 5.36. Suppose $|x_i|, |y_i| \leq M$. Prove: $\left| \prod_{i=1}^{n} x_i - \prod_{i=1}^{n} y_i \right| \leq M^{n-1} \sum_{i=1}^{n} |x_i - y_i|$.

Problem 5.37. Prove that n lines through the origin create $2n$ regions in the plane.

Problem 5.38. $M(n)$ is the maximum number of regions into which n lines can divide a plane.
 (a) Tinker. Three lines are shown on the right, creating regions $R_1, \ldots, R_6$. What is the maximum number of regions possible with three lines?
 (b) Continue to tinker. Compute $M(n)$ for small values of n.
 (c) Make a conjecture for $M(n)$.
 (d) Prove your conjecture using induction.
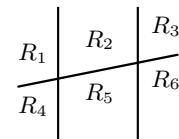
Problem 5.39. Prove you can make any postage greater than 12¢ using only 4¢ and 5¢ stamps.

Problem 5.40. A cap of a disk is a region subtended by a cord. We show three caps, which do not cover the disk. Suppose n caps do cover the entire disk. Prove by induction on n that one can cover the disk using at most 3 of the caps. *[Hint: Consider the complements of the caps and show that if every 3 cap-complements have nonempty intersection then all n complements have nonempty intersection which contradicts the caps covering the disk. (A special case of Helly's Theorem.)]*

Problem 5.41. Choose any $n + 1$ numbers from $\{1, 2, \ldots, 2n\}$. For the numbers chosen, prove by induction that:
 (a) Two are consecutive.   (b) One of the numbers is a multiple of another.

Problem 5.42. For $x_1, \ldots, x_n$, let $\mu = (\sum_{i=1}^{n} x_i)/n$ and $s^2 = (\sum_{i=1}^{n} x_i^2)/n$. Prove that $\mu^2 \leq s^2$ by induction on n.

66

Problem 5.43 (Binomial Theorem). For integers k, n, the binomial coefficient $\binom{n}{k} = n!/k!(n-k)!$ ($0! = 1$).
  (a) Show that $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$, for $1 \le k \le n$. Hence prove that $\binom{n}{k}$ is an integer for $0 \le k \le n$.
  (b) Prove, for $n \ge 1$, $(1+x)^n = \sum_{i=0}^{n} \binom{n}{i} x^i = \binom{n}{0} x^0 + \binom{n}{1} x^1 + \cdots + \binom{n}{n} x^n$.
  (c) Use (b) to give the expansions of $(1+x)^2$, $(1+x)^3$, $(1+x)^4$.
  (d) Prove the Binomial Theorem, $(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}$.

Problem 5.44 (Central Binomial Coefficient). Prove by induction that $\dfrac{4^n}{n+1} < \binom{2n}{n} < 4^{n-1}$ for $n \ge 5$.

Problem 5.45 (Binomial Coefficients are Integers). Let k be a positive integer.
  (a) Prove by induction on k that the product of k consecutive positive numbers is divisible by $k!$. *[Hint: Let $P(k)$ be the claim that $n(n+1) \cdots (n+k-1)$ is divisible by $k!$ for all $n \ge 1$. To prove $P(k+1)$, use induction on n. Also, $(n+1)(n+2) \cdots (n+k-1)(n+k) = n(n+1)(n+1) \cdots (n+k-1) + k(n+1)(n+2) \cdots (n+k-1)$ is a product of k consecutive numbers plus k times a product of $k-1$ consecutive numbers.]*
  (b) Prove that the binomial coefficient $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ is an integer, where $0 \le k \le n$.

Problem 5.46 (Fermat's Little Theorem). Prove, by induction: if p is prime, then p divides $n^p - n$ for $n \ge 1$.
[Hint: Show p divides $\binom{p}{i}$ for $0 < i < p$. Use the Binomial Theorem.]

Problem 5.47. For $n \ge 1$, prove by induction that $\dfrac{(2n-1)!!}{(2n)!!} \le \dfrac{1}{\sqrt{2n+1}}$, where the double factorials are:

$$(2n)!! = 2 \times 4 \times 6 \times \cdots \times 2n; \qquad\qquad (2n-1)!! = 1 \times 3 \times 5 \times \cdots \times (2n-1).$$

Problem 5.48. Prove by induction that for $n \ge 1$, $\dfrac{1}{\pi} \displaystyle\int_0^\pi dx \; \sin^{2n} x = \dfrac{(2n-1)!!}{(2n)!!}$.
[Hint: Show, using integration by parts, that $\int_0^\pi dx \; \sin^k x = \frac{k-1}{k} \int_0^\pi dx \; \sin^{k-2} x$.]

Problem 5.49. Prove that the regions created by n lines on a plane can be colored with two colors so that no two regions which share a side have the same color.

Problem 5.50. Let A be the 2×2 matrix $\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$. Compute the n-term matrix product A^n.
  (a) Tinker. Compute the matrix products A^2, A^3, A^4. ($\mathrm{A}^n = \mathrm{A} \times \mathrm{A} \times \cdots \times \mathrm{A}$ with n terms.)
  (b) Formulate a guess about A^n and prove it by induction.

Problem 5.51. For two sequences $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$, let $A = a_1 + \cdots + a_n$ and $B = b_1 + \cdots + b_m$ be the sums. Let S be the sum of all pairwise products $a_i b_j$. Prove by induction that $S = AB$. That is,

$$S = a_1 b_1 + \cdots + a_1 b_m + a_2 b_1 + \cdots + a_2 b_m + \cdots + a_n b_1 + \cdots + a_n b_m = (a_1 + \cdots + a_n)(b_1 + \cdots + b_m).$$

Problem 5.52. The comparison scale on the right can compare weights. Show that using weights $1, 3, 3^2, 3^3, \ldots, 3^k$ (pounds), you can measure any weight of sugar from $\{1, 2, \ldots, (3^{k+1} - 1)/2\}$.
E.g., to weigh 5 pounds with weights $1, 3, 3^2$, place sugar on one side with 1 and 3 pound weights, and place the 9 pound weight on the other side. The sugar weighs 5 pounds if the scale balances.

Problem 5.53. For 6 people A, B, C, D, E, F, we show friendship networks, G_1 and G_2.
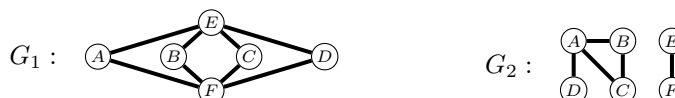
Two people are connected if they can reach each other using friendship links. In G_1, A and D can connect via E. The friendship network is connected if every pair of people can connect.
 (a) Determine whether G_1 and G_2 are connected.
  (b) Two people who are not friends are enemies. Give the enemy networks $\overline{G}_1$ and $\overline{G}_2$ ($\overline{G}$ for complement, because the enemy edges are the complement of the friend edges).
  (c) Determine whether $\overline{G}_1$ and $\overline{G}_2$ are connected.
  (d) Is it possible for both the friendship and enemy networks to be connected?
  (e) Prove, by induction on the number of people: For any friendship network G, either G or $\overline{G}$ is connected.

Problem 5.54. Each of n friends shake hands with everyone else. Prove that the number of handshakes is $n(n-1)/2$.

Problem 5.55. A round-robin tournament has n players $p_1, p_2, \ldots, p_n$. There is a match between every pair of players. Prove by induction that the number of matches played is $n(n-1)/2$.

Problem 5.56. At a party are n people. Some people shake hands with others, No one shakes another's hand more than once. Use well-ordering to prove that there are two people who make the same number of handshakes. *[Hint: Assume the claim is false for a smallest possible party size of n_* which makes a smallest possible number of total handshakes k_*. Show that someone in this party make no handshakes, and derive a contradiction.]*

Problem 5.57. Everyone plays everyone in the 4-person tournament shown. The arrow $A \longrightarrow B$ means A beat B.

tournament   a ranking   inconsistencies
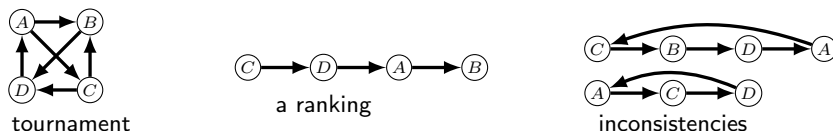
A ranking orders players so that the first player beats the second, the second beats the third and so on. An example ranking is shown. An inconsistency is a sequence of players where the first beats the second, the second beats the third, and so on up to the last who beats the first. We show 4-person and 3-person inconsistencies.

(a) Prove by induction on the number of people: Every tournament has a ranking.
(b) Prove: Every tournament has a ranking with the first player having the most wins. *[Hint: Consider the longest ranking that starts with the player having the most wins.]*
(c) Give a tournament with 5 people that has no inconsistency.
(d) Prove by induction: If there is no inconsistency, someone beats everyone else and someone loses to everyone else.
(e) Prove by induction: Every tournament with an inconsistency has a 3-person inconsistency. (Carefully define $P(n)$.)

Problem 5.58. Let S_n be the points with integer coordinates (x, y) where $x, y \geq 0$ and $x + y \leq n$. Show that S_n cannot be covered by the union of n lines. At least $n + 1$ lines are required.


S_0 S_1 S_2 S_3
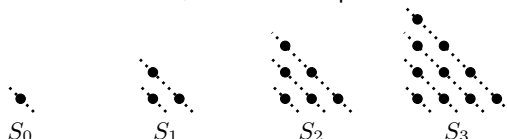
Problem 5.59. Three friends A, B, C each have tokens a, b, c. At every step a random pair of friends swaps their tokens. If the first pair picked is (A, B) and then (A, C) then the token are distributed c, a, b. Prove that it is not possible for each friend to have their own token after 2015 such swaps. *[Hint: Consider any odd number of swaps.]*

Problem 5.60. A robot has a repetoire of moves on an infinite grid as shown in the figures.

(a) The robot moves one diagonal step at a time. Prove that no sequence of moves takes the robot to the shaded square. *[Hint: Let (x, y) be the robot's position. Consider $x + y$.]*

(b) One of the moves changed. Now prove that any square (m, n) can be reached by a finite sequence of moves.
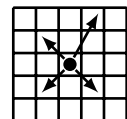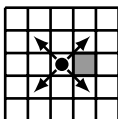

Problem 5.61. A knight's possible moves are shown by the arrows on the right. The knight starts at position $(0, 0)$ on an infinite board. Prove that the knight can move to any square (m, n) using at most $3(|m| + |n|)$ moves. *[Hint: First show the knight can move one square up, down, left or right.]*
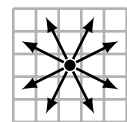
Problem 5.62. There are n squares shaded on an infinite grid.

(a) Compute the perimeter of the shaded area as highlighted by the thick line.
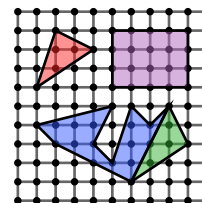(b) Prove by induction that the perimeter of the shaded area is even for all $n \geq 1$.
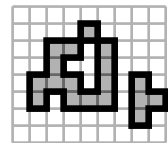
Problem 5.63. Prove a famous result in geometry: the n-polygon with maximum area incribed in a circle is regular (has equal sides). Let $\theta_1, \ldots, \theta_n$ be the angles subtended by the sides of the polygon at the center, $0 < \theta_i \leq \pi$.

(a) For $0 \leq \lambda \leq 1$ and $0 \leq x, y \leq \pi$, show that $\lambda \sin x + (1 - \lambda) \sin y \leq \sin(\lambda x + (1 - \lambda)y)$.
(b) Prove $\sin \theta_1 + \cdots + \sin \theta_n \leq n \sin\left(\frac{\theta_1 + \cdots \theta_n}{n}\right)$. Hence, prove the result. *[Hint: Area(isocelles triangle) $= \frac{1}{2} r^2 \sin \theta$.]*

Problem 5.64 (Josephus Problem). Label n objects in a circle 1 to n, clockwise. Starting at 1, repeatedly remove every other object (object 2 is removed first). Prove that for $n = 2^k$, object 1 is removed last ($k \geq 0$).

Problem 5.65 (Pick's Theorem). Five polygons are shown on a grid: red; purple; blue; green; and, blue-union-green. The vertices of each polygon are grid points.
  (a) Compute the areas of these five polygons.
  (b) For a polygon, let B be the number of grid points on the boundary and I the number of grid points inside. For each polygon, compute $I + B/2 - 1$. Do you see a pattern?

Pick's Theorem. Area(polygon with vertices at grid points) $= I + B/2 - 1$.
  (c) Prove Pick's Theorem for axis aligned rectangles (purple).
  (d) Prove Pick's Theorem for triangles (red). *[Hint: Start with right-triangles. Enclose the triangle in a rectangle.]*
  (e) A polygon P with vertices on grid points satisfies Pick's Theorem (blue). P is joined at a face to a triangle whose third vertex is a grid point (green). Show that the area of the new polygon satisfies Pick's Theorem.
  (f) A polygon P with vertices at grid points is obtained by repeatedly joining n triangles at common faces. Prove by induction that P satisfies Pick's Theorem. (Fact: Any polygon can be built by joining triangles.)

Problem 5.66. A roll of two 6-faced dice has 36 possible outcomes, one for each pair of outcomes (dice 1, dice 2):

$$(1,1) \cdots (1,6), (2,1) \cdots (2,6), (3,1) \cdots (3,6), (4,1) \cdots (4,6), (5,1) \cdots (5,6), (6,1) \cdots (6,6).$$

For indistinguishable dice, the outcomes $(1,6)$ and $(6,1)$, are the same (we can't distinguish which dice rolled 6).
  (a) How may of the 36 outcomes are distinguishable?
  (b) For n indistinguishable dice, prove by induction that the number of distinguishable outcomes is

$$\binom{n+5}{5} = \frac{1}{5!}(n+1)(n+2)(n+3)(n+4)(n+5).$$

  [Hints: Let $Q_k(n) = $ # distinguishable outcomes for n dice with k sides. Induction on k. Problem 5.22]

Problem 5.67 (Quotient-remainder Theorem). Use well-ordering to prove: Given $n \in \mathbb{Z}$ and a divisor $d \geq 0$, there are a unique quotient $q \in \mathbb{Z}$ and unique remainder $r \in \mathbb{Z}$, with $0 \leq r < d$, such that $n = qd + r$.

Problem 5.68 (The number e). One of the most important mathematical constants is $e \approx 2.71828 \cdots$.
  (a) Prove that $1 + k/n \leq (1 + 1/n)^k < 1 + k/n + k^2/n^2$ for $k \leq n$. Hence prove that $2 < (1 + 1/n)^n < 3$, for $n \geq 1$.
  (b) Prove that for $m > n \geq 2$,

$$\left(1 + \frac{1}{n}\right)^n < \left(1 + \frac{1}{m}\right)^m \qquad \text{and} \qquad \left(1 + \frac{1}{n}\right)^{n+1} > \left(1 + \frac{1}{m}\right)^{m+1}.$$

  That is, the sequence $(1 + 1/n)^n$ is increasing and bounded above by 3. Therefore it converges. The limit is defined as e. The sequence $(1 + 1/n)^{n+1}$ is decreasing and converges to the same value. Therefore for any $n \geq 2$,

$$\left(1 + \frac{1}{n}\right)^n < e < \left(1 + \frac{1}{n}\right)^{n+1}.$$

  (c) Prove that, for $n > 6$, $(n/3)^n < n! < (n/2)^n$.
  (d) Prove that, for $n \geq 1$, $(n/e)^n < n! < n(n/e)^n$.

Problem 5.69. Define a polynomial in x, $P_n(x)$ as

$$P_n(x) = 1 + \frac{x}{1!} + \frac{x(x+1)}{2!} + \frac{x(x+1)(x+2)}{3!} + \cdots + \frac{x(x+1)(x+2)\cdots(x+n-1)}{n!}.$$

  (a) Show that $P_n(-n) = (-1)^0 \binom{n}{0} + (-1)^1 \binom{n}{1} + (-1)^2 \binom{n}{2} + \cdots (-1)^n \binom{n}{n}$, and hence $P_n(-n) = 0$.
  (b) Use part (a) and the Binomial Theorem to prove that $-n$ is a root of $P_n(x)$.
  (c) What is the degree of $P_n(x)$? Prove by induction that the roots of $P_n(x)$ are $-1, -2, -3, \ldots, -n$.
  (d) Deduce a formula of the form $P_n(x) = c(x + r_1)(x + r_2) \cdots (x + r_n)$ and prove it by induction.

Problem 5.70. The positive numbers $x_1, \ldots, x_n$ and $y_1, \ldots, y_m$ have equal sum at most mn. Prove that one can cancel terms from the equation $x_1 + \cdots + x_n = y_1 + \cdots + y_m$ and still maintain equality. *[Hint: Induction on $n + m$.]*

Problem 5.71. Distinct numbers $x_1, \ldots, x_n$ must be placed in n boxes separated by $<$ and $>$ signs so that all inequalities are obeyed between consecutive numbers. For example, $5, 7, 3, 8$ can be placed in $\square < \square > \square < \square$ as follows, $\boxed{5} < \boxed{8} > \boxed{3} < \boxed{7}$. Prove this can always be done no matter what the numbers and inequalities are.

Problem 5.72. The sequence $x_1, x_2, \ldots$ is defined by: $x_1 = 1$; $x_{2n} = x_n + 1$; $x_{2n+1} = 1/x_{2n}$. Prove:

(a) Every number in the sequence is rational. *[Hint: Use well-ordering.]*

(b) Every positive rational r equals some x_n for a unique n. ($x_1, x_2, \ldots$ is a "list" of the positive rationals.)
   [Hints: Let $r = a/b$ (a and b have no common divisor). Use well-ordering w.r.t. $a + b$.]

Problem 5.73. A circle has $2n$ distinct points, n are red and n are blue. By examining the proof by induction in Example 5.4 on page 62, construct a method to find a blue point x such that a clockwise trip starting from x will always have passed as many blue points as red.

Problem 5.74. For $n+2$ statements $p, r_1, \ldots, r_n, q$ ($n \geq 1$), prove that you can conclude $p \leftrightarrow q$ from a chain of IF AND ONLY IF's or a chain of implications. Specifically, prove the following are true:

(a) $\big((p \leftrightarrow r_1) \wedge (r_1 \leftrightarrow r_2) \wedge \cdots \wedge (r_{n-1} \leftrightarrow r_n) \wedge (r_n \leftrightarrow q)\big) \to (p \leftrightarrow q)$.

(b) $\big((p \to r_1) \wedge (r_1 \to r_2) \wedge \cdots \wedge (r_{n-1} \to r_n) \wedge (r_n \to q) \wedge (q \to p)\big) \to (p \leftrightarrow q)$.

Problem 5.75. Use the well-ordering principle to prove these principles of induction.

(a) $P(1)$ and $P(n) \to (P(2n) \wedge P(2n+1))$ implies $P(n)$ for all $n \geq 1$.

(b) $P(1)$ and $P(n) \to (P(2n) \wedge P(n-1))$ implies $P(n)$ for all $n \geq 1$.

Problem 5.76 (Telescoping Sum/Product). For a function f, and $n \geq 1$, prove by induction:

(a) $\sum_{i=1}^{n}(f(i+1) - f(i)) = f(n+1) - f(1)$, and more generally $\sum_{i=1}^{n}(f(i+k) - f(i)) = \sum_{i=1}^{k}(f(n+i) - f(i))$.

(b) $\prod_{i=1}^{n} f(i+1)/f(i) = f(n+1)/f(1)$, and more generally $\prod_{i=1}^{n} f(i+k)/f(i) = \prod_{i=1}^{k} f(n+i)/f(i)$.

Problem 5.77. Find a formula in each case. Prove it. *[Hints: Induction; partial fractions; telescoping sum/product.]*

(a) $S(n) = \dfrac{1}{1 \cdot 2} + \dfrac{1}{2 \cdot 3} + \dfrac{1}{3 \cdot 4} + \cdots + \dfrac{1}{n(n+1)}$.

(d) $S(n) = \dfrac{1}{1 \cdot 2 \cdot 3} + \dfrac{1}{2 \cdot 3 \cdot 4} + \cdots + \dfrac{1}{n(n+1)(n+2)}$.

(b) $S(n) = \dfrac{1}{2!} + \dfrac{2}{3!} + \dfrac{3}{4!} + \cdots + \dfrac{n}{(n+1)!}$.

(e) $S(n) = \dfrac{1}{2 \cdot 5} + \dfrac{1}{5 \cdot 8} + \dfrac{1}{8 \cdot 11} + \cdots + \dfrac{1}{(3n-1)(3n+2)}$.

(c) $\Pi(n) = \left(1 + \dfrac{k}{1}\right)\left(1 + \dfrac{k}{2}\right)\left(1 + \dfrac{k}{3}\right) \cdots \left(1 + \dfrac{k}{n}\right)$.

(f) $\Pi(n) = \left(1 - \dfrac{1}{1+2}\right)\left(1 - \dfrac{1}{1+2+3}\right) \cdots \left(1 - \dfrac{1}{1+2+\cdots+n}\right)$.

Problem 5.78. Define the sum of the first n numbers raised to the pth power as $S_p(n)$,

$$S_p(n) = \sum_{i=1}^{n} i^p = 1^p + 2^p + \cdots + n^p.$$

(a) What is $S_0(n)$?

(b) Show that $\sum_{i=1}^{n}((i+1)^{p+1} - i^{p+1}) = (n+1)^{p+1} - 1$.   *[Hint: Problem 5.76.]*

(c) Use the Binomial Theorem to show that $\sum_{i=1}^{n}((i+1)^{p+1} - i^{p+1}) = \sum_{j=0}^{p} \binom{p+1}{j} S_j(n)$.

(d) Use (b) and (c) to show that $S_p(n) = \big((n+1)^{p+1} - 1 - \sum_{j=0}^{p-1} \binom{p+1}{j} S_j(n)\big)/(p+1)$.
   (A formula for the sum of the pth powers using sums for lower order powers.)

(e) Start with (a) and use (d) to get explicit formulas for $S_1(n)$, $S_2(n)$, $S_3(n)$, $S_4(n)$.

(f) Prove your formula for $S_4(n)$ by induction.

Using this approach, you can continue the derivation and obtain an explicit formula

$$S_p(n) = \frac{1}{p+1} \sum_{j=0}^{p} \binom{p+1}{j} B_j n^{p+1-j},$$

where B_j are the Bernoulli numbers, the first few being $B_0 = 1$; $B_1 = -1/2$; $B_2 = 1/6$; $B_3 = 0$; $B_4 = -1/30$; ...

Problem 5.79. Assume the principle of induction and prove the well-ordering principle.

Suppose $\mathcal{B}$ is a non-empty set of natural numbers. Then, $\mathcal{B}$ has a minimum element.

[Hints: Define $P(n) : \mathcal{B}$ does not contain any of $1, 2, \ldots, n$. Prove IF $\mathcal{B}$ has no minimum, THEN $P(n)$ is true for all $n \geq 1$. Hence, $\mathcal{B} = \varnothing$. That is, prove the contraposition. Note that $P(n)$ makes a claim for all of $1, 2, \ldots, n$. Induction with such predicates is called strong induction. Can you prove the claim using the simpler predicate "$P(n) : \mathcal{B}$ does not contain n." What goes wrong? Choosing the right predicate is a skill learned through practice.]

6.5   Problems

Problem 6.1. We proved the strong claim that a $2^n \times 2^n$ grid missing any square can be L-tiled. The induction proof constructively tiles the $2^n \times 2^n$ from four smaller problems on $2^{n-1} \times 2^{n-1}$ grids. You can therefore build an algorithm using the ideas in the proof. Use the algorithm suggested by the proof to obtain an L-tiling of the 8×8 grid shown, which is missing a square at position $(3, 3)$.
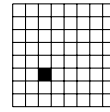
Problem 6.2. Prove: (a) $1+1/\sqrt{2}+1/\sqrt{3}+\cdots+1/\sqrt{n} > 2\sqrt{n+1}-2$.   (b) $1+\sqrt{2}+\sqrt{3}+\cdots+\sqrt{n} \le 2(n+1)\sqrt{n}/3$.

Problem 6.3. Strengthen the claim and prove by induction, for $n \ge 1$:
(a) The sum of the first n odd numbers is a square. *[Hint: Strengthen to a specific square.]*
(b) (Uses complex numbers) $\text{Re}[(\cos x + i \sin x)^n] = \cos nx$. *[Hint: Im$[(\cos x + i \sin x)^n]$ =?.]*

Problem 6.4. Consider the product $\Pi(n) = (1/2) \times (3/4) \times (5/8) \times \cdots \times (2n-1)/2n = (2n-1)!!/(2n)!!$.
(a) Use induction to show: (i) $\Pi(n) \le 1/\sqrt{2n}$. What goes wrong?   (ii) $\Pi(n) \le 1/\sqrt{2n+1}$.
(b) Is (a)(ii) a stronger claim than (a)(i)? Is (a)(i) true? Why is (a)(ii) easier to prove than (a)(i)?
(c) Use induction to prove an even stronger claim that $\Pi(n) \le 1/\sqrt{3n+1}$.

Problem 6.5. (i) Identify the weaker claim and prove it by induction. If you can't, why? (ii) Prove the stronger claim.
(a) Let $\Pi(n) = (1+1^{-3})(1+2^{-3})(1+3^{-3})\cdots(1+n^{-3})$. Claim $\Pi(n) < 3$ or $\Pi(n) < 3 - 1/n$, for $n \ge 1$.
(b) Let $\Pi(n) = (1+2^{-1})(1+2^{-2})(1+2^{-3})\cdots(1+2^{-n})$. Claim $\Pi(n) < 5/2$ or $\Pi(n) < 5(1-2^{-n})/2$, for $n \ge 2$.
(c) Claim $\sqrt[n]{n} \le 2$ or $\sqrt[n]{n} \le 2 - 1/n$, for $n \ge 1$.

Problem 6.6. Let $H_n = 1/1 + 1/2 + \cdots + 1/n$, the nth Harmonic number, and $S_n = H_1/1 + H_2/2 + \cdots + H_n/n$.
(a) Prove $S_n \le H_n^2/2 + 1$ by induction. What goes wrong?
(b) Prove the stronger claim $S_n \le H_n^2/2 + (1/1^2 + 1/2^2 + \cdots + 1/n^2)/2$. Why is this stronger?

Problem 6.7. Prove $\sqrt{2\sqrt{3\cdots\sqrt{n}}} \le 3$ by induction. Did it work? Prove a tighter bound *[Hint: Try $3/n^{1/2^{n-2}}$.]*

Problem 6.8. Prove $n^7 < 2^n$ for $n \ge 37$. (a) Use induction. (b) Use leaping induction.

Problem 6.9. What is wrong with this bad proof by strong induction that $3^k = 1$ for $k \ge 0$.

> **Base Case:** $3^0 = 1$. ✓
> **Induction:** Assume $3^k = 1$ for $k = 0, \ldots n$ and show $3^{n+1} = 1$.
> $3^{n+1} = 3^n \times 3^n/3^{n-1} = 1 \times 1/1 = 1$ (by the induction hypothesis, $3^n = 3^{n-1} = 1$)
> Therefore, by induction, $3^n = 1$ for $n \ge 0$. ✓

Problem 6.10. Let $P(m, n)$ be a predicate (claim) with two inputs $m, n \ge 1$.
(a) Determine if $P(m, n)$ is true for all $m, n \ge 1$ by showing pictorially the "grid" of implications when:
    (i) $P(1, 1)$ is true; AND   (ii) $P(m, n) \to (P(m, n+1) \wedge P(m+1, n))$ is true for $m, n \ge 1$.
(b) Use the well-ordering principle to prove the following principle of double induction.

> **Principle of Double Induction.** Let $P(m, n)$ be a predicate for $m, n \ge 1$.
>   (i) If $P(1, 1)$ is true; AND
> (ii) $P(m, n) \to (P(m, n+1) \wedge P(m+1, n))$ is true for $m, n \ge 1$.
> Then, $P(m, n)$ is true for all $m, n \ge 1$.

(c) Use double induction to prove that $4^m - 4^n$ is divisible by 3, for $m, n \ge 1$.

Problem 6.11. Let $P(m, n)$ be a predicate (claim) with two inputs $m, n \ge 1$. Suppose
 (i) $P(1, 1)$ is true;
 (ii) $P(1, n) \to P(1, n+1)$ for $n \ge 1$ and $P(m, 1) \to P(m+1, 1)$ for $m \ge 1$;
(iii) $P(m, n) \to P(m+1, n+1)$ for $m, n \ge 1$.
Show the grid of implications that is created. Is $P(m, n)$ true for all $m, n \ge 1$?

Problem 6.12. Consider the "double sum" of $i \times j$ over all pairs (i, j) with $1 \leq i \leq m$ and $1 \leq j \leq n$,

$$S(m, n) = (1 \times 1 + 1 \times 2 + \cdots + 1 \times n) + (2 \times 1 + 2 \times 2 + \cdots + 2 \times n) + \cdots + (m \times 1 + m \times 2 + \cdots + m \times n).$$

(a) Compute $S(3, 2)$.   (b) Prove $S(m, n) = mn(m + 1)(n + 1)/4$, for $m, n \geq 1$.

Problem 6.13. Prove the following claims.
  (a) Any postage greater than 11¢ can be made using 4¢ and 5¢ stamps.
  (b) Infinitely many postages cannot be made using 4¢ and 6¢ stamps.

Problem 6.14. For what n can n students be broken into teams of 4 or 7? Prove it.

Problem 6.15. Prove that there are $2^{\lceil n/2 \rceil}$ distinct n-bit binary palindromes (strings that equal their reversal).

Problem 6.16. A grill has space for two pancakes and cooks one side of a pancake in 1 minute. How long does it take to cook n pancakes (both sides of each pancake must be cooked)? Prove your answer.

Problem 6.17. Prove that a square can be cut exactly into n squares of possibly distinct positive sizes for $n \geq 6$.

Problem 6.18. Prove that $\lfloor 1/2 \rfloor + \lfloor 2/2 \rfloor + \lfloor 3/2 \rfloor + \cdots + \lfloor n/2 \rfloor = \begin{cases} n^2/4 & n \text{ even;} \\ (n^2 - 1)/4 & n \text{ odd.} \end{cases}$ ($\lfloor \cdot \rfloor$ rounds down.)

Problem 6.19. For $n \geq 1$, show that $n = \pm 1^2 \pm 2^2 \pm 3^2 \cdots \pm k^2$ (for some k and appropriate choice of each $\pm$). [Hint: What is $(k + 4)^2 - (k + 3)^2 - (k + 2)^2 + (k + 1)^2$?]

Problem 6.20. Prove by strong induction that $n \leq 3^{n/3}$ for $n \geq 0$.

Problem 6.21. Prove that, for $n \geq 1$, there is $k \geq 0$ and ℓ odd such that $n = 2^k \ell$.

Problem 6.22. Prove by strong induction that the kth prime number $p_k \leq 2^{2^{k-1}}$.

Problem 6.23. For $x \in \mathbb{R}$, suppose $x + 1/x \in \mathbb{Z}$. Prove $x^n + 1/x^n \in \mathbb{Z}$ for $n \geq 1$.

Problem 6.24. If $\cos x + \sin x$ is rational, prove that $\cos^n x + \sin^n x$ is rational for any $n \geq 1$.

Problem 6.25. For $n \geq 1$, prove by induction that $F_n = (\phi_+^n - \phi_-^n)/\sqrt{5}$ is a natural number, where $\phi_\pm = (1 \pm \sqrt{5})/2$. [Hint: Use induction. First show that $F_n = F_{n-1} + F_{n-2}$.]

Problem 6.26. Use strong induction to prove, for all $n \geq 1$, that $n/q \neq \sqrt{2}$ for any $q \in \mathbb{N}$. What does it mean?

Problem 6.27. Prove the uniqueness of binary representation (Theorem 6.4). Suppose

$$n = 2^{i_1} + 2^{i_2} + \cdots + 2^{i_r} = 2^{j_1} + 2^{j_2} + \cdots + 2^{j_\ell}, \qquad \text{where } i_1 < i_2 < \cdots < i_r \text{ and } j_1 < j_2 < \cdots < j_\ell.$$

  (a) Prove that $i_1 = j_1$. [Hint: If $i_1 < j_1$, divide both sides by 2^{i_1}. The LHS will be odd.]
 (b) Prove by induction on k that $2^{i_k} = 2^{j_k}$.

Problem 6.28. Use strong induction together with a greedy algorithm to prove that any $n \geq 0$ is a sum of distinct powers of 2 in a unique way. [Hint: Let i_1 be the highest power of 2 that is at most n, so $n = 2^{i_1} + k$, where $k < 2^{i_1}$.]

Problem 6.29. At one end of a line containing only boys and girls is a boy and at the other end is a girl. Prove that the number of boy–girl pairs who are standing next to each other is odd.

Problem 6.30. Problem 5.57 used induction to prove every tournament has a ranking. Show it by strong induction. [Hint: Remove any player v and consider two sub-tournaments: those players who lost to v; and those players who beat v.]

Problem 6.31. Between every pair of major US cities is a one-way flight (the direction is not known). Washington DC has the most out-going flights to major US cities. The president starts in Washington DC and visits each major city once in some sequence, flying from one city to the next. Prove that the president's city-tour is always possible.

Problem 6.32. We are back in L-tile land.
  (a) This time the potted plant needs more room than just one square. For $n \geq 1$, a $2^n \times 2^n$ grid-patio is missing a (large) 2×2 square in a corner as shown in the figure. Prove that the remainder of the patio can be L-tiled, for $n \geq 1$.
  (b) We are no longer sure what the size of the potted plant is. The size may be $2^k \times 2^k$, and so a $2^k \times 2^k$ square will be missing from the corner of the $2^n \times 2^n$ grid-patio. Prove that the remainder of the patio can always be L-tiled, for $k \geq 1$ and $n \geq k$. [Hint: Tinker: try $k = 2; n = 3$ and $k = 2; n = 4$ to figure out what is going on.]

**Problem 6.33.** Consider the $5^n \times 5^n$ patio with the top-left square removed.
(a) Prove that the number of remaining squares is divisible by 3.
(b) For $n \geq 1$, prove by induction that the rest of the patio can be L-tiled.

Problem 6.34. For which n can these grids be L-tiled: (a) $3^n \times 3^n$ (b) $5^n \times 5^n$ (c) $6^n \times 6^n$?

Problem 6.35. Prove that a $(3n+1) \times (3n+1)$ grid missing one square can be L-tiled, for $n \geq 1$. Use 2-leaping induction and the figure to the right as a guide to the proof.
(a) What are the base cases? Prove them.
(b) Prove that a $2k \times 3r$ grid can be tiled for $k, n \in \mathbb{N}$.
(c) Prove that A, B, C, D can be tiled and prove the claim.
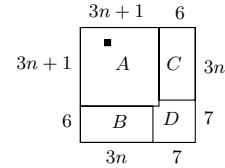
Problem 6.36. We wish to L-tile a grid that is missing its top-right quadrant (we show $k = 3$). Prove that this is always possible for $k \geq 1$. Prove $P(k)$ for $k \geq 1$, where $P(k)$ is defined as

$$P(k) : \text{The } 3/4\text{-grid missing the top right } k \times k \text{ quadrant can be } L\text{-tiled.}$$

(a) Prove $P(k)$ for $k = 1, \ldots, 4$.
(b) Prove $P(k_1) \wedge P(k_2) \rightarrow P(k_1 k_2)$.
(c) Prove $P(k)$ for $k \geq 1$. *[Hint: For $k \geq 5$, either $k = 3r, 3r + 2$ or $3r + 4$ for $r \in \mathbb{N}$.]*
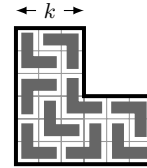
Problem 6.37 (Local Minimum). For $n = 2^k$, n^2 distinct values are concealed in each square of an $n \times n$ grid. A local minimum is a square whose value is lower than its four neighbors (up, down, left, right). Revealing a square's value is costly. Prove that you can find a local minimum by revealing at most $8n$ values.
(a) Break the $2^{k+1} \times 2^{k+1}$ grid into 4 smaller subgrids as shown. Reveal the values in the shaded strips. Among these revealed values, consider the minimum (red).
   (i) How many values are revealed?
   (ii) Prove that the subgrid with the minimum value (red) has a local minimum.
(b) Let $R(k)$ be the number of squares revealed to find a local minimum in the $2^k \times 2^k$ grid. Show that $R(k) \leq R(k-1) + 2^{k+2} - 4$. Why is it inequality, not equality?
(c) Unfold the recursion and prove that $R(n) \leq 8n - 4(\ln n + 2)$.
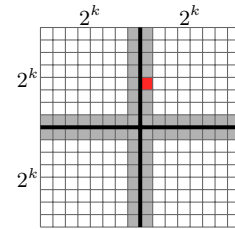
Problem 6.38. A stack of n boxes is given. Splitting a stack of k boxes into two stacks of k_1, k_2 earns $\$k_1 k_2$ (the product). You must reduce the stack of n boxes to n stacks of one box while maximizing your earnings.
(a) Tinker with different ways of unstacking 4 and 5 boxes.
(b) Make conjectures for the number of splits needed and the maximum $\$$ you can earn. Prove them by induction.

Problem 6.39. The general version of Nim has k piles with $n_1, \ldots, n_k$ coins in each pile. In 1902, Charles Bouton discovered an optimal strategy for Nim. Represent n_i in binary. For three piles of 6, 7 and 23 coins, $n_1 = 6 = 00110$, $n_2 = 7 = 00111$ and $n_3 = 23 = 10111$ (equalize the lengths of the binary numbers by front-padding with zeros). The "Nim-sums" $s_1, s_2, \ldots$ are obtained by summing each column of digits, so $s_1 = 2$, $s_2 = 3$, $s_3 = 3$, $s_4 = 0$ and $s_5 = 1$, as shown on the right.

$$n_1: 0\,0\,1\,1\,0$$
$$n_2: 0\,0\,1\,1\,1$$
$$n_3: 1\,0\,1\,1\,1$$
$$s: \mathbf{1\,0\,3\,3\,2}$$

(a) If every Nim-sum is even, show that any move will make at least one Nim sum odd.
(b) Prove: if any Nim-sum is odd, there is a move to make every Nim-sum even.
(c) Prove: if one of the Nim-sums is odd, the first player can force a win.
(d) What is your move for the (6,7,23)-pile Nim game in our example?

Problem 6.40. For $x_i > 0$, the arithmetic mean AM, the geometric mean GM and the harmonic mean HM are

$$\text{AM} = \frac{x_1 + x_2 + \cdots + x_n}{n}, \qquad \text{GM} = (x_1 x_2 \cdots x_n)^{1/n} \qquad \text{and} \qquad \text{HM} = \frac{n}{1/x_1 + 1/x_2 + \cdots + 1/x_n}.$$

(a) Prove GM $\leq$ AM. What is your induction claim $P(n)$? Here is Cauchy's famous proof using backward induction.
   (i) What is the base case? Prove it. *[Hint: $(\sqrt{x_1} - \sqrt{x_2})^2 \geq 0$.]*
   (ii) Prove that $P(2) \wedge P(n) \rightarrow P(2n)$.
   (iii) Prove $P(n) \rightarrow P(n-1)$. *[Hint: $(x_1 + \cdots + x_{n-1})/(n-1) = (x_1 + \cdots + x_{n-1} + \frac{x_1 + \cdots + x_{n-1}}{n-1})/n$.]*
   (iv) Collect everything together into a full proof by induction.
(b) Prove HM $\leq$ GM using part (a) with the numbers $\{1/x_1, 1/x_2, \ldots, 1/x_n\}$.

Problem 6.41 (Jensen's Inequality). A function f is concave if every chord of f is entirely below f. That is,

$$\text{for all } \alpha_1, \alpha_2 \geq 0 \text{ with } \alpha_1 + \alpha_2 = 1: \qquad f(\alpha_1 x_1 + \alpha_2 x_2) \geq \alpha_1 f(x_1) + \alpha_2 f(x_2).$$

(a) Prove that $f(\text{weighted average}) \geq \text{weighted average}(f)$. That is, for $\alpha_i \geq 0$ with $\alpha_1 + \cdots + \alpha_n = 1$,

$$f(\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n) \geq \alpha_1 f(x_1) + \alpha_2 f(x_2) + \cdots + \alpha_n f(x_n).$$

(b) Show that if $f''(x) < 0$, then $f(x)$ is concave. Use this to show that $\log(x)$ is concave.

(c) Prove the AM-GM inequality (see Problem 6.40). *[Hint: Take the $\log$.]*

Problem 6.42. In a line are n disks. A disk has a black face and a white one. In each step you remove a disk showing black and flip its neighbors, if they are still there. The goal is to remove all disks. Here is a sample game.

(a) Tinker. Determine when you can win, and when you can't. *[Hint: Consider the parity of black disks.]*

(b) Give an optimal strategy. Prove that your strategy wins all winnable games, and if it fails, the game is not winnable.

Problem 6.43. A sliding puzzle is a grid of 9 squares with 8 tiles. The goal is to get the 8 tiles into order (the target configuration). A move slides a tile into an empty square. Below we show first a row move, then a column move.

Prove that no sequence of moves produces the target configuration. *[Hint: The tiles form a sequence going left to right, top to bottom. An inversion is a pair that is out of order. Prove by induction that the number of inversions stays odd.]*

Problem 6.44. Generalize Problem 1.45(k). An $m \times n$ rectangular grid has at least two squares on each side ($m, n \geq 2$) and one side is even (the total number of squares is even). Two opposite color squares are removed. Prove by strong induction that the remaining squares can be tiled by dominos.

Problem 6.45. For $x \in \mathbb{R}$, one can write $x = k + \alpha$ where $k \in \mathbb{Z}$ is the integer part and $0 \leq \alpha < 1$ is the fractional part. The rounding operation $\{x\}$ is defined as follows. If $\alpha \geq 1/2$, $\{x\} = k + 1$, and if $\alpha < 1/2$, $\{x\} = k$. Note that $1/2$ is rounded up. For $n \geq 1$, a problem from an old Russian mathematics olympiad asks to compute

$$f(n) = \sum_{i=1}^{\infty} \left\{ \frac{n}{2^i} \right\} = \left\{ \frac{n}{2} \right\} + \left\{ \frac{n}{4} \right\} + \left\{ \frac{n}{8} \right\} + \left\{ \frac{n}{16} \right\} + \cdots$$

(a) Compute the sum without rounding, $n \cdot 2^{-1} + n \cdot 2^{-2} + n \cdot 2^{-3} + \cdots$. *[Hint: What is $1/2 + 1/4 + 1/8 + \cdots$?]*

(b) Compute $f(n)$ for $n = 1, 2, 3, 4, 5$, and make a conjecture for $f(n)$.

(c) Prove your conjecture. *[Hint: Exponential induction. Show $\{n/2^k + 1/2^{k+1}\} = \{n/2^k\}$.]*

Problem 6.46. We prove, using well-ordering, that every natural number has a description of 13 words or less.

Assume some numbers cannot be described in 13 words or less. By well-ordering, there is a smallest such n_*. Here is a description of n_* using 13 words or less, a contradiction:

"The smallest natural number that cannot be described in thirteen words or less"

Do you think this proof is correct? If no, why not? If yes, is anything unsatisfying about the proof?

Problem 6.47. Here is another proof of the first part of the fundamental theorem of arithmetic.

(a) Prove by strong induction that every number greater than 1 is divisible by a prime.

(b) Use (a) to prove by strong induction that every $n > 1$ is a product of primes, $n = p_1 p_2 \cdots p_k$.

Problem 6.48. What's wrong with this proof of part (ii) of the Fundamental Theorem of Arithmetic, Theorem 6.3?

$$Q(n) : \text{each of } 2, 3, \ldots, n \text{ have a unique factorization into a product of primes..}$$

[Base case] $Q(2)$ is true because 2 is a product of one prime, and that is unique.

[Induction step] Assume $Q(n) : 2, 3, \ldots, n$ have a unique factorization into primes. If $n + 1$ is prime, then there is no problem. If $n + 1$ is composite, then $n + 1 = k\ell$. Each of k and ℓ have a unique factorization into primes and taking the product gives the unique factorization of $n + 1$. Therefore, $Q(n + 1)$ is true. By induction, $Q(n)$ is true $\forall n \geq 2$.

Problem 6.49.[Hard] Prove part (ii) of the Fundamental Theorem of Arithmetic (uniqueness of prime factorization). If n is prime, there is nothing to prove. Let $n = p_1 p_2 \cdots p_r$. Suppose $n = q_1 q_2 \cdots q_\ell$ is an alternate prime factorization. To prove that the q_is are the same as the p_is, you will need Euclid's Lemma:

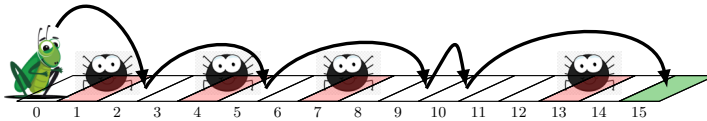**Lemma 6.6** (Euclid's Lemma). IF a prime p divides the product $a_1 a_2$, THEN either p divides a_1 p or p divides a_2.

(a) Argue that n is divisible by p_1.

(b) Generalize Euclid's lemma: IF $a_1 a_2 \cdots a_\ell$ is divisible by a prime p, THEN one of the a_i's is divisible by p. *[Hint: Use induction on ℓ; Euclid's Lemma is the base case.]*

(c) Show that one of the q_i's is divisible by p_1 and hence that $p_1 = q_i$ for one of the q_i's.

(d) Prove that the primes in $q_1 \cdots q_\ell$ all appear in $p_1 \cdots p_r$ and *vice versa*. (Strong induction on n.)

(e) Prove Euclid's Lemma. Suppose p divides $a_1 a_2$, but not a_1. Show that p divides a_2.
  (i) Prove Bézout's identity: there exist integers x and y for which $px + a_1 y = 1$.
      [Hint: Let d be the smallest positive integer for which $px + a_1 y = d$. Show that d divides both p and a_1.]
  (ii) Use Bézout's identity to prove that a_2 is divisible by p. *[Hint: Multiply by a_2.]*

Problem 6.50. Here are some interesting/challenging problems for you to prove by induction. Tinker, tinker.

(a) There is a one-way flight between every pair of cities. Prove that there is at least one special city that can be reached from every other city either directly or via one stop.

(b) For $n \geq 0$, there are integers x, y for which $x(21n + 4) + y(14n + 3) = 1$.

(c) Let $x_1, x_2, \ldots, x_n$ be any sequence of positive real numbers. Prove that
$$(x_1^2 + 1)(x_2^2 + 1) \cdots (x_n^2 + 1) \geq (x_1 x_2 + 1)(x_2 x_3 + 1)(x_3 x_4 + 1) \cdots (x_{n-1} x_n + 1)(x_n x_1 + 1).$$

(d) Enough gas for a car to travel around a circle is spread among n gas stations on the circle. Prove that the car can start at one of the gas stations and make it around the circle.

(e) Prove $\binom{j}{j} + \binom{j+1}{j} + \binom{j+2}{j} + \cdots + \binom{n}{j} = \binom{n+1}{j+1}$, for $n \geq j$. The binomial coefficient is $\binom{n}{i} = n!/i!(n-i)!$.

(f) Compute a formula for $S_n = \binom{n}{0} - \binom{n-1}{1} + \binom{n-2}{2} - \binom{n-3}{3} \cdots + (-1)^i \binom{n-i}{i} + \cdots$, where the binomial coefficient is $\binom{n}{i} = n!/i!(n-i)!$ if $n \geq i$ and zero for $n < i$. *[Hint:$\binom{n}{i} = \binom{n-1}{i} + \binom{n-1}{i-1}$.]*

(g) Given n positive numbers $x_1 < x_2 < \cdots < x_n$ with sum $s = x_1 + \cdots + x_n$ and $n-1$ positive numbers $M = \{a_1 < a_2 < \cdots < a_{n-1}\}$ with $s \notin M$, show that one can arrange the x_i into a sequence so that no prefix-sum is in M. *[Hint: Induction on n. In the induction step, consider $(s - x_{n+1}) \in M \setminus a_n$ and $(s - x_{n+1}) \notin M \setminus a_n$.]*

(h) The picture shows a cricket making jumps of sizes 2,3,4,1 and 5 to reach a destination at square 15, while avoiding spiders who lie in wait at squares 1,4,7,13.

A cricket makes n jumps of distinct positive integer sizes $a_1, \ldots, a_n$ to reach the destination $s = a_1 + \cdots + a_n$. Along the way are $n-1$ spiders at positions $x_1, \ldots, x_{n-1}$. Prove that the cricket can always reorder the jump sizes and reach the destiniation while avoiding all spiders, providing no spider is at the destination.

(i) The numbers $\{1, \ldots, n\}$ are painted on the $2n$ faces of n cards (each number is used twice). Show that it is always possible to place the cards on a table so that the numbers $1, \ldots, n$ are facing up.

(j) You have n slabs, each with a positive integer weight in $\{1, 2, \ldots, n\}$. The slabs have a total weight less than $2n$. Prove that some combination of the slabs has a total weight of exactly n.

(k) For $n \in \mathbb{N}$ and $x > 0$, prove Hermite's identity: $\lfloor x \rfloor + \lfloor x + 1/n \rfloor + \lfloor x + 2/n \rfloor + \cdots + \lfloor x + (n-1)/n \rfloor = \lfloor nx \rfloor$.
  (i) Suppose x satisfies Hermite's identity, prove that $x + k/n$ satisfies Hermite's identity for $k \in \mathbb{N}$.
  (ii) Show that $x \in [0, \frac{1}{n})$ satisfies Hermite's identity. Hence prove Hermite's identity for all $x > 0$.

(l) We arranged n^2 numbers in a square $n \times n$ table as shown on the right. The number in the ith row and jth column of the table is given by

$$a_{ij} = \frac{1}{i + j - 1}.$$

$\frac{1}{1}$	$\frac{1}{2}$	$\frac{1}{3}$	$\cdots$	$\frac{1}{n}$
$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{4}$	$\cdots$	$\frac{1}{n+1}$
$\vdots$	$\vdots$	$\vdots$		$\vdots$
$\frac{1}{n}$	$\frac{1}{n+1}$	$\frac{1}{n+2}$	$\cdots$	$\frac{1}{2n-1}$

Prove: sum(any n numbers no two of which are in the same row or column) ≥ 1.

(m) For $a, n \in \mathbb{N}$ with $a \leq n!$, prove that a is a sum of at most n distinct divisors of $n!$. For example, for $a = 23, n = 4$, the divisors of $n! = 24$ are $\{1, 2, 3, 4, 6, 8, 12, 24\}$ and $a = 12 + 8 + 3$. *[Hint: Quotient-remainder theorem.]*

(n) Let m and n be integers. Prove that, for $k \in \mathbb{N}$, $m^k - n^k$ is even if and only if $m - n$ is even.

(o) The product of any seven consecutive natural numbers is divisible by 7!.

(p) No right-triangle with positive integer sides has an area which is a perfect square. *[Hint: Problem 10.74.]*

7.4 Problems

Problem 7.1. $f(n) = f(n-1) + 1$ for $n \geq 1$ and $f(n) = 0$ otherwise. Why isn't it "circular" to define f using f?

Problem 7.2. $f(1) = 1$. For $k \geq 1$, $f(2k) = f(k)$ and $f(2k+1) = f(5k-2)$. Is $f(n)$ defined for all $n \in \mathbb{N}$?

Problem 7.3. Give a recursive definition of the function $f(n) = n! \times 2^n$, where $n \geq 1$.

Problem 7.4. Guess a formula for A_n and prove it by induction. Tinker. The method of differences can be helpful.
(a) $A_0 = 0$ and $A_n = A_{n-1} + 1$ for $n \geq 1$.   (c) $A_0 = 1, A_1 = 2$ and $A_n = A_{n-1} + 2A_{n-2}$ for $n \geq 2$.
(b) $A_0 = 1$; $A_n = \alpha A_{n-1} + 1$ for $n \geq 1$ (d) $A_0 = 1$; $A_1 = 2$; $A_n = 2A_{n-1} - A_{n-2} + 2$ for $n \geq 2$.

Problem 7.5. $A_n = 2A_{n-1} - 1$ for $n > 1$. Find a formula for A_n and prove it when (a) $A_1 = 1$ (b) $A_1 = 2$.

Problem 7.6. For each recurrence, (i) Write a program and compute T_{20}. (ii) Tinker. Unfold the recurrence and get a formula for T_n. Verify your formula for T_{20}. (iii) Prove your formula by induction.
(a) $T_0 = 2$ and $T_n = T_{n-1} + 3n$ for $n \geq 1$.   (c) $T_0 = 3$ and $T_n = 2T_{n-1} + n$ for $n \geq 1$.
(b) $T_0 = 3$ and $T_n = 2T_{n-1}$ for $n \geq 1$.   (d) $T_0 = 0$ and $T_n = 4 - T_{n-1}$ for $n \geq 1$.

Problem 7.7. Define f by $f(1) = 0$ and $f(n) = f(\lfloor n/2 \rfloor) + f(\lceil n/2 \rceil) + 1$ for $n > 1$. ($\lceil \ \rceil$ and $\lfloor \ \rfloor$ round up/down.)
(a) Is f a well defined function? Explain. (b) Tinker, guess a formula for $f(n)$ and prove it.

Problem 7.8. Define f by $f(1) = 1$, $f(n) = f(n/2) + 1$ for $n > 1$ even, and $f(n) = f(3n+1)$ for $n > 1$ odd.
(a) Compute $f(3), f(5), f(6)$.   (b) Is f defined for all $n \in \mathbb{N}$? (See the Collatz conjecture, Problem 1.45.)

Problem 7.9. Give a recurrence for A_n ($n \in \mathbb{N}$), and prove A_n solves the recurrence. Don't forget base cases.
(a) $A_n = 3 \cdot 2^n$.   (b) $A_n = 3^n - 2$.   (c) $A_n = 2 \cdot 3^n - 1$.   (d) $A_n = 2^{2n}$.
(e) $A_n = (n!)^2$.   (f) $A_n = n^3$.   (g) $A_n = n + (-1)^n$.   (h) $A_n = 2^{n^2}$.

Problem 7.10. $G_0 = 0, G_1 = 1$ and $G_n = 7G_{n-1} - 12G_{n-2}$ for $n > 1$. Find G_5. Show $G_n = 4^n - 3^n$ for $n \geq 0$.

Problem 7.11. $A_1 = 1, A_2 = 2, A_3 = 3$ and $A_n = A_{n-1} + A_{n-2} + A_{n-3}$, for $n > 3$. Prove $(9/5)^n/2 < A_n < 2^n$.

Problem 7.12. In each case tinker. Then, guess a formula that solves the recurrence, and prove it.
(a) $P_0 = 0, P_1 = a$ and $P_n = 2P_{n-1} - P_{n-2}$, for $n > 1$.   (b) $G_1 = 1$; $G_n = (1 - 1/n) \cdot G_{n-1}$, for $n > 1$.

Problem 7.13. Tinker to guess a formula for each recurrence and prove it. In each case $A_1 = 1$ and for $n > 1$:
(a) $A_n = 10A_{n-1} + 1$.   (b) $A_n = nA_{n-1}/(n-1) + n$.   (c) $A_n = 10nA_{n-1}/(n-1) + n$.

Problem 7.14. Analyze these very fast growing recursions. *[Hint: Take logarithms.]*
(a) $M_1 = 2$ and $M_n = aM_{n-1}^2$ for $n > 1$. Guess and prove a formula for M_n. Tinker, tinker.
(b) $L_1 = 2, L_2 = 2$ and $L_n = L_{n-1}L_{n-2}$ for $n > 2$. Prove bounds of the form $2^{a^n} \leq L_n \leq 2^{b^n}$. Tinker, tinker.

Problem 7.15. You have wealth $W_0 = \$100$ in the bank. At the end of every year, the bank gives you 5% interest and you add an extra \$100 in savings. Let W_n be your wealth at year n.
(a) Give a recursion for your wealth in the form $W_n = (?)W_{n-1} + (?)$. Compute W_{10}, W_{20}, W_{30}.
(b) Unfold your recursion to guess a formula for W_n and prove it by induction.

Problem 7.16 (Mortgage). You borrow a principal P at monthly interest r (e.g. in a 6% mortgage, $r = 0.5\%$ or 0.005). Every month your debt increases by a factor $1 + r$ and you pay X. Let P_n be your debt after the nth month.
(a) Show that $P_0 = P$ and $P_n = (1+r)P_{n-1} - X$ for $n \geq 1$. Unfold the recursion, make a guess for P_n and prove it.
(b) Show that the monthly payment $X = rP/(1 - (1+r)^{-N})$ will payoff your mortgage after N payments.
(c) What monthly payment X pays off a \$300,000 mortgage in 15 years, for monthly interest (i) 0.5%   (ii) 0.75%?

Problem 7.17. Let $x_1 = 1$ and $x_{n+1} = \sqrt{1 + 2x_n}$ for $n \geq 1$. Prove, for $n \geq 1$, that $x_n < 4$.

Problem 7.18. Define $f(x) = 0$ for $x \leq 0$ and $f(x) = f(x-1) + 2x - 1$ for $x > 0$. Prove $f(x) = \lceil x \rceil (2x - \lceil x \rceil)$, for $x \geq 0$. (The ceiling, $\lceil x \rceil$, is x rounded up.) *[Hint: Let $0 < \alpha \leq 1$. Prove $f(n + \alpha) = n^2 + 2n\alpha + 2\alpha - 1$ for $n \geq 0$.]*

Problem 7.19. Define a polynomial $f_n(x)$: $f_0(x) = 0$, $f_1(x) = x$ and $f_n(x) = xf_{n-1}(x) + (1 - x)f_{n-2}(x)$ for $n \geq 2$. Prove $f_n(x) = x((x-1)^n - 1)/(x-2)$.

Problem 7.20. On month 1 a baby Q is born. A baby grows into an adult in 1 month. An adult produces a baby in a month. Qs don't die. Let A_n, B_n and F_n be the respective number of adult Q, baby Q and all Qs on month n.
  (a) For $n = 1, \ldots, 10$, find A_n, B_n and F_n.   (b) Show that A_n, B_n and F_n all satisfy the Fibonacci recurrence.

Problem 7.21. The Fibonacci numbers are $F_1, F_2 = 1$;, and $F_n = F_{n-1} + F_{n-2}$ for $n > 2$.
  (a) Compute $F_1, \ldots, F_{10}$ and verify that $F_n < (7/4)^{n-1}$, for $n \geq 1$. Now prove the bound for all $n \geq 1$.
  (b) Let $\phi_\pm = (1 \pm \sqrt{5})/2$. Prove that $F_n = (\phi_+^n - \phi_-^n)/\sqrt{5}$ for $n \geq 1$.
  (c) Prove that $F_{n-1}F_{n+1} - F_n^2 = (-1)^n$, for $n \geq 2$.
  (d) Prove that every third Fibonacci number, F_{3n}, is even.
  (e) (Sum) Prove: $F_1 + F_2 + F_3 + \cdots + F_n = F_{n+2} - 1$, for $n \geq 1$.
  (f) (Sum of odd terms) Prove: $F_1 + F_3 + F_5 + \cdots + F_{2n-1} = F_{2n}$, for $n \geq 1$.
  (g) (Sum of even terms) Prove: $F_2 + F_4 + F_6 + \cdots + F_{2n} = F_{2n+1} - 1$, for $n \geq 1$.
  (h) (Alternating sum) Prove: $F_1 - F_2 + \cdots + (-1)^n F_{n+1} = (-1)^n F_n + 1$, for $n \geq 1$.
  (i) (Linear weighted sum) Prove: $F_1 + 2F_2 + 3F_3 + \cdots + nF_n = nF_{n+2} - F_{n+3} + 2$, for $n \geq 1$.
  (j) (Consecutive products) Prove: $F_1F_2 + F_2F_3 + \cdots + F_{2n-1}F_{2n} = F_{2n}^2$, for $n \geq 1$.
  (k) Prove that F_n and F_{n+1} have no common factor larger than 1, for $n \geq 1$.
  (l) Prove that F_{2n} is divisible by F_n, for $n \geq 1$, and more generally that F_{kn} is divisible by F_n, for $n, k \geq 1$.
  (m) Prove that $\gcd(F_m, F_n) = F_{\gcd(m,n)}$.
  (n) Prove $F_{m+n+1} = F_m F_n + F_{m+1}F_{n+1}$ for $m, n \geq 1$. Hence, show that $F_n^2 + F_{n+1}^2 = F_{2n+1}$.

Problem 7.22. Let $U_n = F_{2n}/F_n$ (F_n are Fibonacci numbers). Tinker. Compute $U_1, \ldots, U_5$. Do you see a pattern?
  (a) Prove that $U_n = F_{n-1} + F_{n+1}$. Hence, prove that F_n divides F_{2n}. *[Hint: Problem 7.21(n).]*
  (b) Prove that U_n satisfies the Fibonacci recursion and compute a formula for U_n

Problem 7.23. Show that every $n \geq 1$ is a sum of distinct Fibonacci numbers, e.g. $11 = F_4 + F_6$; $20 = F_3 + F_5 + F_7$. (There can be many ways to do it, e.g. $6 = F_1 + F_5 = F_2 + F_3 + F_4$.) *[Hints: Greedy algorithm; strong induction.]*

Problem 7.24. A linear kth order recurrence is: $T_n = a_0 + a_1 T_{n-1} + a_2 T_{n-2} + \cdots + a_k T_{n-k}$, for $n > k$ (T_n uses k previous terms). Given base cases $T_1, \ldots, T_k$, prove that T_n is uniquely defined for $n \geq 1$. (Induction or well-ordering.)

Problem 7.25. Suppose $T_n = a + br^n$ is an exponential sequence.
  (a) Show that $T_{n+2} = (r+1)T_{n+1} - rT_n$.
  (b) Find a formula for T_n where $T_0 = 1, T_1 = 2$ and $T_{n+2} = 4T_{n+1} - 3T_n$. *[Hint: Use T_0, T_1 to find a, b.]*
  (c) Are there any other possible formulas for T_n in (b)? *[Hint: Problem 7.24.]*

Problem 7.26. Suppose, $r \neq s$ and $T_n = ar^n + bs^n$ is a sum of exponential sequences. (Problem 7.25 sets $s = 1$.)
  (a) Show that $T_{n+2} = (r+s)T_{n+1} - rsT_n$.
  (b) Find a formula for T_n where $T_0 = 1, T_1 = 2$ and $T_{n+2} = 3T_{n+1} - 2T_n$. *[Hint: Use T_0, T_1 to find a, b.]*
  (c) Find a formula for T_n where $T_0 = 1, T_1 = 2$ and $T_{n+2} = T_{n+1} + 6T_n$.
  (d) Are there any other possible formulas for T_n in (b) and (c)? *[Hint: Problem 7.24.]*

Problem 7.27. Suppose, $T_n = (a + bn)r^n$ is a product of a polynomial with an exponential.
  (a) Show that $T_{n+2} = 2rT_{n+1} - r^2 T_n$. (This is the case $r = s$ in Problem 7.26(a).)
  (b) Find a formula for T_n where $T_0 = 1, T_1 = 4$ and $T_{n+2} = 4T_{n+1} - 4T_n$. *[Hint: Use T_0, T_1 to find a, b.]*
  (c) Are there any other possible formulas for T_n in (b)? *[Hint: Problem 7.24.]*
Problems 7.26–7.27 give a complete "dictionary" approach to 2nd-order linear recurrences (one can extend to kth-order).

Problem 7.28. For a general 2nd-order linear recurrence $T_n = a_1 T_{n-1} + a_2 T_{n-2}$, with T_0, T_1 given and $a_1, a_2 \neq 0$, guess a solution of the form $T_n = (\alpha + \beta n)\phi^n$ for constants α, β, ϕ. Determine α, β, ϕ from a_1, a_2, T_0, T_1.
  (a) If $T_0 = T_1 = 0$, what is the solution? From now, assume T_0 and T_1 are not both zero. Can α and β both be zero?
  (b) To satisfy the recurrence for $n \geq 2$, show that $\beta(\phi^2 - a_1\phi - a_2) = 0$ and $\alpha(\phi^2 - a_1\phi - a_2) + \beta(a_1\phi + 2a_2) = 0$.
  (c) By considering $\beta = 0$ and $\beta \neq 0$, show that $\phi^2 - a_1\phi - a_2 = 0$, hence $\phi = (a_1 \pm \sqrt{a_1^2 + 4a_2})/2$.
  (d) There are two cases to consider: (i) $a_1^2 + 4a_2 \neq 0$ (ii) and, $a_1^2 + 4a_2 = 0$. Analyze these two cases.
      (i) $a_1^2 + 4a_2 \neq 0$. Show by contradiction that $a_1\phi + 2a_2 \neq 0$. Hence show that $\beta = 0$ and there are two possible solutions that satisfy the recurrence: $T_n = \alpha_+ \phi_+^n$ and $T_n = \alpha_- \phi_-^n$, where $\phi_\pm = (a_1 \pm \sqrt{a_1^2 + 4a_2})/2$.
      More generally, show that the sum of the two possibilities, $T_n = \alpha_+ \phi_+^n + \alpha_- \phi_-^n$ satisfies the recurrence.
      (ii) $a_1^2 + 4a_2 = 0$. Show that $a_1\phi + 2a_2 = 0$, hence the solution of the recurrence is $T_n = (\alpha + \beta n)(a_1/2)^n$.
  (e) Solve these recurrences. *[Hint: Use T_0 and T_1 to determine $\alpha_\pm$ in (d)(i) or α, β in (d)(ii).]*
      (i) $T_0 = 1, T_1 = 6, a_1 = 6, a_2 = -9$. (ii) $T_0 = 1, T_1 = 3, a_1 = 8, a_2 = -12$. (iii) $T_0 = T_1 = 1, a_1 = a_2 = 1$.

Problem 7.29 (Akra-Bazzi). Suppose $T(n)$ satisfies $T(n) = \sum_{i=1}^{k} a_i T(b_i n + h_i) + g(n)$ where $a_i > 0$, $0 < b_i < 1$, $|h_i| \leq C$ and $|g(n)| \leq$ polynomial(n). Let p satisfy $\sum_{i=1}^{k} a_i b_i^p = 1$. Then, $T(n)$ is asymptotically approximated by:

$$T(n) \sim f(n) = n^p + n^p \int_1^n dx \, \frac{g(x)}{x^{p+1}}. \qquad (T(n) \sim f(n) \text{ means } T(n)/f(n) \overset{n \to \infty}{\longrightarrow} \text{ constant.})$$

In each case, determine $a_i, b_i, C, g(n)$, compute the approximation $f(n)$, and plot $T(n)$ and $f(n)$ versus n.

(a) $T(0) = 0$, $T(1) = 1$ and $T(n) = T(\lfloor n/2 \rfloor) + T(\lceil n/2 \rceil) + n^k$, where: (i) $k = 0$.   (ii) $k = 1$.   (iii) $k = 2$.

(b) Example 7.1 on page 87.

Problem 7.30 (Change of Variable). A recursion can be easier to solve after you change variables from A_n to $B_n = f(A_n)$, providing the recursion for B_n is easy to solve and $f(\cdot)$ is easy to invert so you can solve for $A_n = f^{-1}(B_n)$.

(a) Solve each recursion using an appropriate change of variable.
    (i) $A_1 = 1$, $A_n = 10 A_{n-1} + 1$ for $n > 1$. (Change variable to $B_n = A_n + 1/9$.)
    (ii) $A_1 = 1$, $A_n = n A_{n-1}/(n-1) + n$. (Divide both sides by n and change variable.)
    (iii) $A_1 = 1$, $A_n = 10 n A_{n-1}/(n-1) + n$.

(b) Suppose $A_1 = a$, $A_n = g(A_{n-1})$ for $n > 1$. Change variable to $B_n = f(A_n)$ and show that B_n satisfies

$$B_1 = f(a), \qquad B_n = f \circ g \circ f^{-1}(B_{n-1}) \text{ for } n > 1.$$

    Use this formula to obtain recursions for each change of variable you made in part (a).

Problem 7.31. One can use recurrences to define a sequence of strings. Define A_n as follows:

$$\begin{aligned} A_0 &= a; \\ A_n &= a \bullet A_{n-1} \bullet ba \qquad \text{for } n \geq 1. \end{aligned} \qquad (x \bullet y \text{ is concatenation, e.g. } ab \bullet ba = abba.)$$

(a) What are $A_1, \ldots, A_{10}$.   (b) Prove $A_n = a^{\bullet n} b(ab)^{\bullet n}$, where $x^{\bullet k}$ is k copies of the string x concatenated together.

Problem 7.32. Give recurrences to generate these string-sequences. ($x^{\bullet k}$ is k copies of x concatenated together.)

(a) $A_k = a^{\bullet k}$. $A_1 = a, A_2 = aa, \ldots$ (c) $A_k = a^{\bullet k} b^{\bullet k}$. $A_1 = ab, A_2 = aabb, \ldots$
(b) $A_k = a^{\bullet k} bb$. $A_1 = abb$, $A_2 = aabb, \ldots$ (d) $A_k = a^{\bullet k} b^{\bullet 2k}$. $A_1 = abb, A_2 = aabbbb, \ldots$

Problem 7.33. Define the sequence of strings $A_1, A_2, A_3, \ldots$ by $A_1 = a$, and

$$A_n = \begin{cases} A_{n/2} \bullet a & n \text{ even;} \\ A_{(n-1)/2} \bullet b & n \text{ odd.} \end{cases} \qquad (\text{for } n > 1) \qquad (x \bullet y \text{ is concatenation, e.g. } ab \bullet ba = abba.)$$

(a) What are $A_1, \ldots, A_{10}$? Prove that A_n is a string that always begins with a.

(b) **[Harder]** Prove that every string begining with a appears in the sequence $A_1, A_2, A_3, \ldots$.

Problem 7.34. Prove $\lceil \log_2(n+1) \rceil = \lceil \log_2(n+2) \rceil$ for even $n \geq 2$. *[Hints: Let $k = \lceil \log_2(n+2) \rceil$, so $n + 2 = 2^k - x$ where $x \in \{0, 2, 4, \ldots, 2^{k-1} - 2\}$. Also note, $\lceil \log_2(2^k - x) \rceil = k$ for $0 \leq x < 2^{k-1}$.]*

Problem 7.35. Analyze Example 7.1 using a different method of induction.

(a) Assume $P(1) \wedge P(2)$ are T and $P(n) \to P(2n-1) \wedge P(2n)$ for $n \geq 2$. Prove $P(n)$ for $n \geq 1$. *[Hint: Well-ordering.]*

(b) Use the method of induction in (a) to prove that $f(n) = 1 + \lceil \log_2 n \rceil$ in Example 7.1.

Problem 7.36. $f(1) = 1$ and $f(n) = 2f(\lfloor n/2 \rfloor)$ for $n > 1$. Tinker. Guess $f(n)$. Prove it by exponential induction.

Problem 7.37. Let $x_1 = 1$ and $x_{n+1} = x_n/n + n/x_n$ for $n \geq 1$. Prove $\lfloor x_n^2 \rfloor = n$ for $n \geq 4$. *[Hints: You must show $\sqrt{n} \leq x_n < \sqrt{n+1}$. Show $x/n + n/x$ is decreasing for $x \leq n$. Prove by induction that $\sqrt{n} \leq x_n \leq n/\sqrt{n-1}$. Use this to prove $x_n \geq (n-1)/\sqrt{n-2}$, and finally that $x_{n+1} < \sqrt{n+2}$.]*

Problem 7.38. Let $x_0 = 0$ and for $n \geq 1$, $x_n = \sqrt{x_{n-1} + 6}$. Tinker. Compute x_1, x_2, x_3. Now, prove that x_n is monotonically increasing in n. Also prove that $x_n < 3$.

Problem 7.39. $A_1 = 1/2$ and $A_n^{-1} = 2n + A_{n-1}^{-1}$ for $n > 1$. Tinker. Guess and prove a formula for $S_n = A_1 + \cdots + A_n$.

Problem 7.40. Let $I_n = \int_0^{\pi/2} dx \, \sin^n x$. Compute a formula for I_n.

(a) Compute I_0, I_1, I_{10}, I_{11}. *[Hint: Use integration by parts to show $I_n = (n-1)I_{n-2}/n$ for $n \geq 2$.]*

(b) Show that $I_{2k} = (\pi/2) \cdot (2k)!/(2^{2k}(k!)^2)$ and $I_{2k+1} = (2^{2k}(k!)^2)/(2k+1)!$ for $k = 0, 1, 2, \ldots$.

Problem 7.41 (Continued Fractions). A continued fraction for 2 is shown.
The recurrence $S_0 = 1; S_n = 1 + 2/S_{n-1}$ for $n \geq 1$ produces the continued fraction:

$$1 + \cfrac{2}{1 + \cfrac{2}{1 + \cfrac{2}{1 + \cfrac{2}{1 + \cfrac{2}{1 + \cfrac{2}{1 + \cdots}}}}}}$$

$$S_0 = 1, \quad S_1 = 1 + \frac{2}{1}, \quad S_2 = 1 + \frac{2}{1 + 2/1}, \quad S_3 = 1 + \frac{2}{1 + \frac{2}{1+2/1}}, \ldots$$

Prove $S_n = \dfrac{2^{n+2} + (-1)^{n+1}}{2^{n+1} + (-1)^n}$ and $\lim_{n \to \infty} S_n = 2$.

Problem 7.42. Linear algebra is a powerful tool for analyzing recurrences. From Problem 7.41, let $S_n = a_n/b_n$.
(a) What are a_0, b_0? Show that $a_n = a_{n-1} + 2b_{n-1}$ and $b_n = a_{n-1}$ for $n \geq 1$.
(b) Define the vector $x_n = \begin{bmatrix} a_n \\ b_n \end{bmatrix}$. What is x_0? Show that $x_n = Ax_{n-1}$ where $A = \begin{bmatrix} 1 & 2 \\ 1 & 0 \end{bmatrix}$.
(c) Show that $x_n = A^n x_0$. The rest of the problem develops a method to compute A^n.
(d) Show that $AQ = QD$, where $Q = \begin{bmatrix} 2 & -1 \\ 1 & 1 \end{bmatrix}$ and $D = \begin{bmatrix} 2 & 0 \\ 0 & -1 \end{bmatrix}$. (Q has the eigenvectors of A and D the eigenvalues).
(e) Since Q is invertible, show that $A = QDQ^{-1}$. Prove by induction that $A^n = QD^nQ^{-1}$. What is D^n?
(f) Derive the formula $S_n = (2^{n+2} + (-1)^{n+1})/(2^{n+1} + (-1)^n)$.

Problem 7.43. Refer to the pseudocode on the right.
(a) What is the function being implemented?
(b) Prove that the output is correct for every valid input.
(c) Give a recurrence for the runtime T_n, where $n = j - i$.
(d) Guess and prove a formula for T_n.

```
out=S([arr],i,j)
if(j<i) out=0;
else
  out=arr[j]+S([arr],i,j-1);
```

Problem 7.44. Give pseudocode for a recursive function to compute 3^{2^n} on input n. (Make it efficient.)
(a) Prove that your function correctly computes 3^{2^n} for every $n \geq 0$.
(b) Obtain a recurrence for the runtime T_n. Guess and prove a formula for T_n.

Problem 7.45. A recursive function takes input of size $n = 2^k$, reduces the problem to two of size $n/2$ and does additional work of at most n to compute the output. The runtime $T(n)$ depends only on n. Show that: (a) $T(n) \leq 2T(n/2) + n$. (b) $T(n) \in \Theta(n \log n)$. *[Hint: Induction. Show $n \log_2 n \leq T(n) \leq 2n \log_2 n$.]*

Problem 7.46. We give two implementations of `Big(n)` from page 90 (`iseven(n)` tests if n is even).

(a)
```
out=Big(n)
  if(n==0) out=1;
  elseif(iseven(n))
     out=Big(n/2)*Big(n/2);
  else out=2*Big(n-1)
```

(b)
```
out=Big(n)
  if(n==0) out=1;
  elseif(iseven(n))
     tmp=Big(n/2); out=tmp*tmp;
  else out=2*Big(n-1)
```

(i) For each, prove that the output is 2^n and give a recurrence for the runtime T_n. (`iseven(n)` is two operations.)
(ii) For each, compute runtimes T_n for $n = 1, \ldots, 10$. Compare runtimes with Exercise 7.10 on page 90.

Problem 7.47. Give a recursive definition for each set.
(a) $\{0, 3, 6, 9, 12, \ldots\}$, the multiples of 3.
(b) $\{1, 2, 3, 4, 6, 7, 8, 9, 11, \ldots\}$, the non-multiples of 5.
(c) $\{3k \mid k$ is odd$\}$.
(d) All binary strings with the same number of 0's as 1's.
(e) All binary strings with an even number of 0's.
(f) All binary strings of even length.

Problem 7.48. What is the recursively defined set $\mathcal{A}$?
By default, nothing else is in $\mathcal{A}$ (minimality).
① $1 \in \mathcal{A}$.
② $x, y \in \mathcal{A} \to x + y \in \mathcal{A}$ AND $x - y \in \mathcal{A}$.

Problem 7.49. What is the recursively defined set $\mathcal{A}$?
By default, nothing else is in $\mathcal{A}$ (minimality).
① $3 \in \mathcal{A}$.
② $x, y \in \mathcal{A} \to x + y \in \mathcal{A}$ AND $x - y \in \mathcal{A}$.

Problem 7.50. A set $\mathcal{S}$ is defined recursively as shown.
By default, nothing else is in $\mathcal{S}$ (minimality).
Give a derivation of $\neg((p \wedge q) \vee (\neg p \wedge r))$.
① $p, q, r \in \mathcal{S}$.
② $P, Q \in \mathcal{S} \to (P \wedge Q) \in \mathcal{S}$ AND $(P \vee Q) \in \mathcal{S}$;
$P \in \mathcal{S} \to \neg P \in \mathcal{S}$.

Problem 7.51. There are 5 rooted binary trees (RBT) with 3 vertices. How many have 5 vertices?

Problem 7.52. Let T_n be the number of RBTs of height n. Show that T_n satisfies the recurrence $T_0 = 1, T_1 = 3$ and $T_n = T_{n-1}^2 + 2T_{n-1}(1 + \sum_{k=0}^{n-2} T_k)$ for $n > 1$. Hence, show that the number of RBT of height 3 is 651.

Problem 7.53 (Rooted Ternary Trees (RTT)). Rooted ternery trees have a recursive definition.
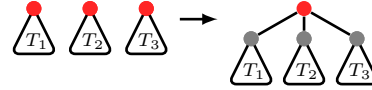
① The empty tree ε is an RTT.
② If T_1, T_2, T_3 are disjoint RTTs with roots r_1, r_2, r_3, then
linking r_1, r_2, r_3 to a new root r gives a new RTT.

(a) Give all RTT's with at most 5 nodes.   (b) Which of your RTT's in (a) are also RTT's?

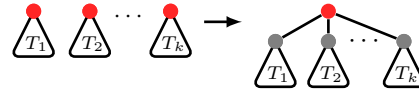**Problem 7.54 (Rooted Full Ternary Trees (RFTT)).** Rooted full ternery trees have a recursive definition.

① A single root-node ● is an RFTT.
② If T_1, T_2, T_3 are disjoint RFTTs with roots r_1, r_2, r_3, then
linking r_1, r_2, r_3 to a new root r gives a new RFTT.

(a) Give all RFTT's with at most 5 nodes.   (b) Which of your RFTT's in (a) are also RBT's?

Problem 7.55 (Rooted Trees (RT)). The rooted trees (RT) have the recursive definition.

① The empty tree ε is an RT.
② If $T_1, \ldots T_k$ are disjoint RTs with roots $r_1, \ldots, r_k$, then
linking $r_1, \ldots, r_k$ to a new root r gives a new RT.

(a) Give all RT's with at most 5 nodes.   (b) Which trees in (a) are RBT's. Which are RTTs?

Problem 7.56. The simple continued fractions $\mathcal{F}$ are recursively definined:

$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cfrac{1}{\cdots + \cfrac{1}{a_n}}}}}$$

① $1 \in \mathcal{F}$.
② $x \in \mathcal{F} \to n + 1/x \in \mathcal{F}$ for $n \in \{0, 1, 2, \ldots\}$.

(a) For $a_i \in \mathbb{N}$, the tuple $(a_1, a_2, \ldots, a_n)$ represents the continued fraction shown.
What is $(4, 3, 2, 1)$ as a fraction a/b in lowest terms?
(b) Start at the base case and repeatedly apply the constructor to derive $(4, 3, 2, 1)$.

Problem 7.57. Recursion is powerful for computing determinants.

(a) Let D_n be the determinant of an $n \times n$ matrix with diagonal a, superdiagonal b and subdiagonal c.
D_4 is shown. Show that $D_n = aD_{n-1} - bcD_{n-2}$. For $a = 1, b = -1, c = -1$, what is D_{10}?

$$\begin{vmatrix} a & b & 0 & 0 \\ c & a & b & 0 \\ 0 & c & a & b \\ 0 & 0 & c & a \end{vmatrix}$$

(b) An $n \times n$ matrix A has entries $A_{ij} = a^{|i-j|}$, and D_n is its determinant. D_4 is shown. Derive
a recursion for D_n in terms of D_{n-1}. Make a guess for D_n and prove it by induction.

$$\begin{vmatrix} 1 & a & a^2 & a^3 \\ a & 1 & a & a^2 \\ a^2 & a & 1 & a \\ a^3 & a^2 & a & 1 \end{vmatrix}$$

Problem 7.58 (Pascal's recursion). Recursion can involve many variables. Let $n, k \in \mathbb{Z}$.

(a) $f(0, 0) = 1$ and $f(0, k) = 0$ for $k \neq 0$. For $n > 0$, $f(n, k) = f(n - 1, k) + f(n - 1, k - 1)$.
    (i) Show: $f(n, k)$ is a well defined for $n \geq 1$.   (ii) Prove: $f(n, k) = \binom{n}{k} = n!/k!(n - k)!$, for $n \geq 1, 0 \leq k \leq n$.
(b) (Generalize (a)) $g(0, 0) = 1$ and $g(0, k) = 0$ for $k \neq 0$. For $n > 0$, $g(n, k) = 2g(n - 1, k) + 3g(n - 1, k - 1)$.
Tinker. Guess and prove a formula for $g(n, k)$ for $n \geq 1, 0 \leq k \leq n$. *[Hint: kth term of the binomial $(2 + 3)^n$.]*

Problem 7.59 (Catalan recursion). Let M_n be the number of ways to match n pairs of parentheses to get a
well formed arithmetic expression. There are the 5 ways for $n = 3$: [ ] [ ] [ ], [ ] [[ ]], [[ ]] [ ], [[ ] [ ]], [[[ ]]].

(a) What are M_0, M_1, M_2, M_3, M_4? Give the matched sequences for $n = 4$.
(b) Show $M_n = M_0 M_{n-1} + M_1 M_{n-2} + M_2 M_{n-3} + \cdots + M_{n-2} M_1 + M_{n-1} M_0$. Compute M_{10}.

Problem 7.60. A stick is 100 units long. You wish to cut it into 100 unit-length pieces. You can stack multiple
pieces and cut them all with one cut. What is the minimum number of cuts you need?

(a) Let n be the length of the longest piece you have. Argue that the number of cuts depends only on n.
(b) Let $C(n)$ the number of cuts needed. What is $C(1)$? Show $C(n) = C(\lceil n/2 \rceil) + 1$ for $n > 1$.
(c) Solve the recursion to get a formula for $C(n)$. How many cuts do you need for the 100-unit stick?

Problem 7.61. A building has n floors. You have k eggs and wish to find the highest safe floor from which you can
drop an egg without the egg breaking (Problem 1.21). Let $M(n, k)$ be the number of egg-drops needed. Let $Q(k, d)$
be the largest number of floors n for which you can find the highest safe floor with k eggs using at most d egg-drops.

(a) What are $M(0, k)$, $M(n, 1)$. What is $M(n, n)$? *[Hint: Binary search.]*
(b) If the first drop is at floor x, how many drops are needed if: (i) The egg breaks? (ii) The egg survives?
(c)   (i) Give a recursion for $M(n, k)$. Program your recursion to get $M(n, 3)$ for $n = 7, 8, 9, \ldots$ (high as you can).
    (ii) Give a more efficient algorithm that is based on the same recursion and compute $M(1000, 3)$.
(d) Give a recursion for $Q(k, d)$ and prove $Q(k, d) = \sum_{i=0}^{k} \binom{d}{i} - 1$. How large an n can 4 eggs and 6 drops handle?

Problem 7.62. Let T_n be the number of prefix-heavy n-bit binary sequences. A sequence is prefix-heavy if every non-empty prefix has more 1's than 0's. Let $F_{n,k}$ be the number of n-bit prefix-heavy sequences ending in $k \geq 1$ zeros.
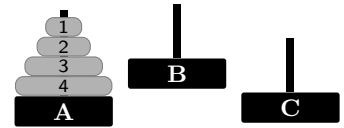   (a) What are $T_1, \ldots, T_7$? Give all the sequences corresponding to T_7.
   (b) What are $F_{7,1}, \ldots, F_{7,7}$. Give all the sequences corresponding to $F_{7,2}$.
   (c) Show that $F_{n,1} = T_{n-2} + F_{n,2}$. What are $F_{n,k}$ for $k = \lfloor (n-1)/2 \rfloor$ and $k > \lfloor (n-1)/2 \rfloor$.
   (d) Prove that $F_{n,k} = F_{n,k+1} + F_{n-2,k-1}$ for $1 < k < \lfloor (n-1)/2 \rfloor$.
   (e) Prove that $T_n = T_{n-1} + T_{n-2} + F_{n-2,1} + F_{n-2,2} + \cdots + F_{n-2,n-2}$. Hence, compute the number of prefix-heavy 10-bit sequences. *[Hint: Consider the possible ways to terminate the sequence: $1, 10, 100, 1000, \ldots$]*

Problem 7.63 (Foraging Bushman). A bushman foraging in the Kalahari can carry up to 1 gallon of water. He drinks 1 gallon of water per mile walked. On any hike, he must save enough water to walk back to the village (with 1 gallon, he can hike out $1/2$-mile and back). He can also place water along his route to increase his range.
   (a) The village has 2 gallons of water. Show how the bushman can hike out $3/4$-mile and make it back.
   (b) Let $M(n)$ be the bushman's maximum range when the village has n gallons of water. Show:
      (i) $M(n) \leq n/2$.   (ii) $M(2n) \geq M(n) + 1/4$.   (iii) Use part (ii) to show $M(n) \geq 1/2 + \lfloor \log_2 n \rfloor/4$.
Can you improve the gap between the bounds in (i) and (iii)? Which bound do you think is tighter?

Problem 7.64 (Towers of Hanoi). Here is a puzzle with n disks and 3 bases. All disks are on base A (smallest on top). You can move a disk from the top of one base to the top of another if all disks on the destination base are larger. The goal is to move all disks from A to C using the fewest moves.
   (a) Give a sequence of 16 legal moves to move the 4 disks from A to C.
   (b) Let T_n be the fewest moves needed for the task with n disks.
      (i) Show that to move disk-n from A to C, the smallest $n - 1$ disks must first be moved from A to B.
      (ii) Prove that $T_n = 2T_{n-1} + 1$. What is T_1?
      (iii) Tinker. Guess a formula for T_n and prove it by induction.

Problem 7.65 (Zeno's Paradox). A tortoise starts at 1 and moves right at 1 unit per minute. A hare that's twice as fast starts at 0 and chases the tortoise. In 1 minute, the hare catches the tortoise at position 2. Zeno says the hare never catches the tortise. He argues that when the hare reaches the tortoise's prior position, the tortise has moved forward. This argument iterates. At iteration n, the hare is behind the tortoise. At iteration $n + 1$ the hare moves to the tortoise's position at iteration n. But the tortoise has moved, so the hare remains behind at iteration $n + 1$.
   (a) Zeno concludes, by induction, that the hare is behind the tortise for all iterations. Is the argument correct?
   (b) Let t_n be the time the hare takes to execute iteration n. What is t_1? Show that $t_{n+1} = t_n/2$.
   (c) Guess and prove a formula for t_n. Show that Zeno's paradox is resolved if $1/2 + 1/2^2 + 1/2^3 + 1/2^4 + \cdots = 1$.

Problem 7.66 (Trash Compactor). A trash bin has unit volume. The trash compactor has compression factor $r > 1$. If you fill the bin with 1 unit of uncompacted trash, the compactor squashes the trash to $(1/r)$-units of compacted trash. For example, if $r = 3$, the 1 unit (uncompacted) becomes $(1/3)$-unit compacted. Now $(2/3)$-unit is free. You can refill and compact again. However, you can't further compress the initial $(1/3)$-unit of compacted trash; you can only compress the new $(2/3)$-unit down to $(2/9)$-unit, which gives a total of $(5/9)$-unit of compacted trash. Each time you use the compactor you create space for new trash, you compact the new trash and keep going like this forever.
Let the step $n = 0, 1, \ldots$ be the number of times the compactor has been used. At step n, let c_n be the amount of compacted trash in the bin and s_n the free space to be filled with new trash and compacted at the next step.
   (a) What are c_0 and s_0? For $r = 3$, compute c_n and s_n for $n = 1, 2, 3$.
   (b) Show that c_n and s_n satisfy the following recurrences with base cases c_0 and s_0 given in part (a):
$$rc_n = 1 + (r - 1)c_{n-1} \quad (n \geq 1); \qquad rs_n = (r - 1)s_{n-1} \quad (n \geq 1).$$
   (c) Guess a formula for s_n and prove it by induction.
   (d) Explain why the total amount of trash put into the bin is $s_0 + s_1 + s_2 + s_3 + s_4 + \cdots$.
   (e) If one continues to compact forever, why must the total trash put into the bin approach r, the compression ratio.
   (f) Use (c), (d) and (e) to prove the following infinite geometric sum for any $r > 1$,
$$1 + \left(\frac{r-1}{r}\right) + \left(\frac{r-1}{r}\right)^2 + \left(\frac{r-1}{r}\right)^3 + \left(\frac{r-1}{r}\right)^4 + \cdots = r.$$

Substitute $t = (r - 1)/r$ and prove the formula for an infinite geometric sum, $1 + t + t^2 + t^3 + \cdots = 1/(1 - t)$.

Problem 7.67 (Josephus Problem). In the Josephus problem (Problems 3.66, 5.64), objects $1, \ldots, n$ are in a circle. Starting at 1, every other object is removed (object 2 is removed first). Let $J(n)$ be the last object removed.

(a) Prove that $J(n)$ satisfies the recursion $J(1) = 1$ and $J(n) = \begin{cases} 2J(n/2) - 1 & n \text{ even}; \\ 2J((n-1)/2) + 1 & n \text{ odd}. \end{cases}$

(b) Use well-ordering (minimum counterexample) to show that $J(n)$ is defined for $n \geq 1$.

(c) Use (a) to compute $J(n)$ for $n \in \{1, \ldots, 32\}$.

(d) Guess a pattern for $J(n)$ based on the data in (c) and predict $J(77), J(78)$.

(e) Guess a formula for $J(n)$ and prove your guess by induction.

Problem 7.68. A cyclic shift transforms a binary number $\mathbf{b} = b_m b_{m-1} \cdots b_0$ with $b_m = 1$ by shifting the leftmost bit to the right, giving $\mathbf{b}_c = b_{m-1} \cdots b_0 b_m$. Problem 4.25 studied some properties of this operation.

(a) Use the data from Problem 7.67(c) to give a table with the binary representations of n and $J(n)$ for $n \in \{1, \ldots, 32\}$. Also include the cyclic shift of the binary representation of n.

(b) Guess at the relationship between the binary representations of n and $J(n)$, and prove it.

Problem 7.69. Generalize the Josephus problem to objects $1, \ldots, n$ with every kth object being removed, $k \geq 1$. Let $J(n, k)$ be the last object to be removed. The Josephus numbers from the previous two problems are $J(n, 2)$.

(a) What is $J(n, 1)$? What is $J(1, k)$?

(b) What is $J(5, 4)$? Use $J(5, 4)$ to deduce $J(6, 4)$. Use $J(6, 4)$ to deduce $J(7, 4)$.

(c) Find a recursion for $J(n, k)$ that uses $J(n-1, k)$. Program your recursion and fill out the following table.

k	n										
	1	2	3	4	5	6	7	8	9	10	100
1											
2											
3											
4											

(d) Where should Josephus stand to be the last one remaining in a band of 41 when every seventh person is removed.

(e) Is the recursion in part (d) or the one from Problem 7.67(a) faster for computing $J(n, 2)$? Informally explain why?

(f) Find a recursion for $J(n, k)$ that would be much more efficient than the one in part (d).

Problem 7.70 (Josephus Permutation). Update the recursion from Problem 7.69 so that instead of computing just the position of the last object to be removed, it computes the entire order in which the objects are removed.

(a) What is the order in which objects are removed when $n = 5$ and $k = 3$?

(b) Use (a) to determine the order in which objects are removed when $n = 6$ and $k = 3$?

(c) Give a recursive function to compute the order of removal for n objects, skipping every k.

(d) Implement your recursion in a program. Determine the order of twenty-six girls with last initials $A, B, \ldots, Z$ in a circle so that when every seventh girl is removed they come off alphabetically.

Problem 7.71 (Fibonacci Tiles). Recursive structures can produce interesting geometric objects. Start with a square of side 1. At each step, attach a square to the longest side of the current rectangle (the side-length of the square is the length of that longest side). We show the rectangle growing with squares numbered by the step at which they were added. Let S_n be the side-length of the square added at step n.

(a) What are $S_1, S_2, S_3, S_4, S_{10}$? [Hint: Recurrence.]

(b) Show that $S_n = F_n$ (Fibonacci numbers).

To get the Fibonacci spiral, join a quater-circle in each square (blue curve). This approximates a golden spiral satisfying the polar equation $r = a\varphi^{2\theta/\pi}$ (red curve), where $\varphi \approx 1.618$.

The golden spiral is a logarithmic spiral, $r = ae^{b\theta}$. Such spirals approximate the growth of many structures in Nature, e.g.: Nautilus shell and Aloe (Wikipedia); Storm clouds (NASA); Galaxy (ESA/Hubble). A logarithmic spiral allows growth without changing shape.

8.6   Problems

Problem 8.1. The recursive function on the right has a non-negative integer as input. Tinker and make a conjecture for what the function does and prove your conjecture by induction.

> UP(x) :
> 1: If $x = 0$, **return** 1.
> 2: If x is odd, **return** $2 \times$ UP$(\lfloor x/2 \rfloor)$.
> 3: If x is even, **return** $x + 1$

Problem 8.2. The recursive function on the right takes an integer $0 \leq j \leq n$, an array $A = [A_0, A_1, \ldots, A_n]$, a real number x, and implements Horner's method to compute the polynomial

$$A_0 + A_1 x + A_2 x^2 + \cdots + A_n x^n.$$

Prove that H$(0, A, x)$ correctly evaluates the desired polynomial.

> H(j, A, x) :
> 1: If $j = n$, **return** A_n.
> 2: **return** $A_j + x * H(j + 1, A, x)$

Problem 8.3. We show a triangle of numbers similar to Pascal's triangle. Row zero has just a 1 (all other numbers in row zero are 0). The numbers in each row are obtained by summing the three numbers above, as illustrated. Let $T_{i,j}$ be the jth entry of row i. $T_{0,0} = 1$, $T_{0,j} = 0$ for $j \neq 0$ and

$$T_{i,j} = T_{i-1,j-1} + T_{i-1,j} + T_{i-1,j+1}.$$

(a) Tinker. Make a conjecture for the sum of a row and prove it.
(b) Give a formula for the number of non-zeros in row i. Prove it.

0	0	0	0	0	**1**	0	0	0	0	0
0	0	0	0	**1**	**1**	**1**	0	0	0	0
0	0	0	**1**	**2**	**3**	**2**	**1**	0	0	0
0	0	**1**	**3**	**6**	**7**	**6**	**3**	**1**	0	0
0	**1**	**4**	**10**	**16**	**19**	**16**	**10**	**4**	**1**	0

$\cdots$

Problem 8.4. Equation (8.1) lists strings in $\mathcal{M}$ as they are created using the constructor. Give an algorithm to systematically create this list. Program your algorithm and list the first 20 strings in $\mathcal{M}$.

Problem 8.5. For the set $\mathcal{A} = \{0, 4, 8, \ldots\}$ defined on page 101, prove by induction that $4n \in \mathcal{A}$ for integer $n \geq 0$.

Problem 8.6. Give a recursive definition for the set $\mathcal{A} = \{1, 2, 2^2, \ldots\}$, the non-negative powers of 2. Prove
(a) Every element of your set is a non-negative power of 2.   (b) Every non-negative power of 2 is in your set.

Problem 8.7. Prove that every non-empty string in the set $\mathcal{M}$ of matched parentheses begins with an opening parenthesis [. Prove that][$\notin \mathcal{M}$. Is every string that begins with an opening parenthesis in $\mathcal{M}$?

Problem 8.8. For any string x, show that $x \bullet x^{\text{R}}$ is a palindrome.

Problem 8.9. The set $\mathcal{P}_{\text{o}}$ of binary strings has a recursive definition.
(a) Show that every string in $\mathcal{P}_{\text{o}}$ is a palindrome. Is every palindrome in $\mathcal{P}_{\text{o}}$?
(b) Show that every non-empty string in $\mathcal{P}_{\text{o}}$ has odd length.
(c) Is every palindrome with odd length in $\mathcal{P}_{\text{o}}$? Prove your answer.

> ① $\varepsilon \in \mathcal{P}_{\text{o}}$.
> ② $x \in \mathcal{P}_{\text{o}} \rightarrow x \bullet 0 \bullet x \in \mathcal{P}_{\text{o}}$
> $x \in \mathcal{P}_{\text{o}} \rightarrow x \bullet 1 \bullet x \in \mathcal{P}_{\text{o}}$

Problem 8.10. Recursively define all binary palindromes of even length and nothing else. Prove your answer.

Problem 8.11. Palindromes are defined on page 104. Let T_n be the number of palindromes of length n. Show that $T_0 = 1$, $T_1 = 2$ and $T_n = 2T_{n-2}$ for $n \geq 2$. Guess and prove a formula for the number of palindromes of length n.

Problem 8.12. A set $\mathcal{P}$ of parenthesis strings has a recursive definition (right).
(a) Determine if each string is in $\mathcal{P}$ and give a derivation if it is in $\mathcal{P}$.
   (i) [[[]]]] [(ii) [][[]][[]]   (iii) [[][][]
(b) Give two derivations of [][][[]] whose steps are not a simple reordering of each other.
(c) Prove by structural induction that every string in $\mathcal{P}$ has even length.
(d) Prove by structural induction that every string in $\mathcal{P}$ is balanced.
(e) For a string $x \in \mathcal{P}$, define the inbalance as follows. Start on the left of x and move right. Add $+1$ for every [you encounter, and add -1 for every] you encounter.
   (i) After you traverse x, what is the imbalance?
   (ii) Give an upper bound on the imbalance at any point in x.
   (iii) Prove by structural induction that at any point in x, imbalance ≥ 0.
(f) In the text we defined the set $\mathcal{M}$ of balanced and matched parentheses. Prove that $\mathcal{P} = \mathcal{M}$
   (i) Prove by structural induction that every $x \in \mathcal{P}$ has a derivation using the rules for $\mathcal{M}$.
   (ii) Prove by structural induction that every $x \in \mathcal{M}$ has a derivation using the rules for $\mathcal{P}$.

> ① $\varepsilon \in \mathcal{P}$
> ② $x \in \mathcal{P} \rightarrow [x] \in \mathcal{P}$
> $x, y \in \mathcal{P} \rightarrow xy \in \mathcal{P}$

Problem 8.13. [Hard] Recursively define the set $\mathcal{A}$ of all binary strings that contain more 0's than 1's. Prove:
(a) Every string in $\mathcal{A}$ has more 0's than 1's.   (b) Every string which has more 0's than 1's is in $\mathcal{A}$.

Problem 8.14. A set $\mathcal{A}$ is defined recursively. ① $3 \in \mathcal{A}$.   ② $x, y \in \mathcal{A} \to x + y \in \mathcal{A}$ AND $x - y \in \mathcal{A}$.
(a) Prove that every element of $\mathcal{A}$ is a multiple of 3.   (b) Prove that every multiple of 3 is in $\mathcal{A}$.

Problem 8.15. A set $\mathcal{B}$ is defined recursively. ① $1 \in \mathcal{B}$, $2 \in \mathcal{B}$.   ② $x, y \in \mathcal{B} \to xy + 1 \in \mathcal{B}$.   Prove that $\mathcal{B} = \mathbb{N}$.

Problem 8.16. A set $\mathcal{S}$ of points on the 2-D plane has a recursive definition.   ① $(1, 0) \in \mathcal{S}$
(a) On a 2-D xy-plot, show the points in $\mathcal{S}$ (you can't show all of $\mathcal{S}$).   ② $(x, y) \in \mathcal{S} \to (x+1, y+2) \in \mathcal{S}$
(b) Prove that every point $(x, y) \in \mathcal{S}$ satisfies $y = 2x - 2$.

Problem 8.17. Assume a bee produces only one offspring. A male bee (blue) has only a female (red) parent. A female bee has a male and female parent. We show an ancestry tree of a male bee on the right. Let m_n be the number of ancestor bees at level n. Level 1 contains just the one male bee. For example $m_4 = 3$.
(a) What are $m_1, m_2, \ldots, m_7$?
(b) Get a recurrence for m_n and show $m_n = F_n$. (F_n are the Fibonacci numbers.)
(c) Suppose a hive has m_1 male bees and f_1 female bees in the current generation (level 1).
Show that, for the entire hive, there are $m_1 F_n + f_1 F_{n+1}$ ancestor-bees at level n.

Problem 8.18. We reproduce the recursive definition of simple continued fractions from Problem 7.56.
(a) Prove that every element in $\mathcal{F}$ is a positive rational number.
(b) (Harder) Prove that every positive rational number is in $\mathcal{F}$. Let $x = a/b$ where $a, b \in \mathbb{N}$. Show that $x \in \mathcal{F}$ by strong induction on b.
    ① $1 \in \mathcal{F}$.
    ② $f \in \mathcal{F} \to n + 1/f \in \mathcal{F}$
    for $n \in \{0, 1, 2, \ldots\}$.
  (i) Base case, $b = 1$. Prove that for all $a \in \mathbb{N}$, $a \in \mathcal{F}$.
  (ii) Induction step. Assume $a/b \in \mathcal{F}$ for $b \in \{1, \ldots, n\}$ and $a \in \mathbb{N}$. Prove that $a/(n + 1) \in \mathcal{F}$ for $a \in \mathbb{N}$. [Hint: Quotient remainder theorem.]

> Problems 8.19–8.28 rely on the recursive definitions of RBT and RFBT; RTT and RFTT (ternary trees); and, RT (rooted trees), which are in Chapter 7 and Problems 7.53–7.55.

Problem 8.19. Recursively define rooted binary trees (RBT) and rooted full binary trees (RFBT).
(a) Give examples, with derivations, of RBTs and RFBTs with 5,6 and 7 vertices.
(b) Prove by structural induction that every RFBT has an odd number of vertices.

Problem 8.20. In a tree (RBT or RFBT), a leaf-vertex has two empty children; a half-full-vertex has one empty child (the other is non-empty); a full-vertex has two non-empty children. Let L, H and F be the number of leaves, half-full and full vertices respectively. The total number of vertices is $n = L + H + F$. Prove by structural induction:
(a) In any RFBT, all vertices are either full or leaves: $H = 0$.
(b) In any RBT, $n = 2L + H - 1$ and $F = L - 1$.
(c) In any RFBT, $n = 2F + 1$. Hence prove that every RFBT has an odd number of vertices.

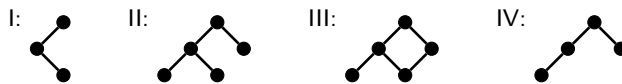**Problem 8.21.** The height and size of trees are defined recursively in Exercise 8.10. Prove:
(a) $\text{size}(T) \geq \text{height}(T) + 1$, where T is any rooted binary tree (RBT).
(b) $\text{size}(T) \geq 2 \times \text{height}(T) + 1$, where T is any rooted full binary tree (RFBT).

Problem 8.22. Consider these graphs: I: II: III: IV:
(a) Which are RBTs? Explain your answers.
(b) Which are RFBTs? Explain your answers.

Problem 8.23. Prove that every RBT is connected (there is a chain of links from every vertex to every other vertex).

Problem 8.24. Answer T or F with with explanations.
(a) Every rooted binary tree (RBT) is a rooted ternary tree (RTT).
(b) Every every rooted full binary tree (RFBT) is a rooted ternary tree (RTT).
(c) Every rooted full binary tree (RFBT) is a rooted full ternary tree (RFTT).
(d) Every rooted binary tree (RBT) is a rooted tree (RT). (What about RTT?)
(e) Every every rooted full binary tree (RFBT) is a rooted tree (RT). (What about RFTT?)

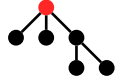**Problem 8.25.** Prove the following by structural induction.

(a) The degree of the root in any RBT is at most 2.   (c) The degree of the root in any RTT is at most 3.

(b) The degree of the root in any RFBT is 2.   (d) The degree of the root in any RFTT is 3.

Problem 8.26. Prove by structural induction a rooted full ternary tree (RFTT) has $3k - 2$ vertices, for $k \in \mathbb{N}$.

Problem 8.27. Prove the following about the rooted tree on the right.

(a) (i) It is a rooted tree (RT).   (ii) It is a rooted ternary tree (RTT).

(b) (i) It is not a rooted full ternary tree (RFTT).   (ii) It is not a rooted binary tree (RBT).

Problem 8.28. Define size and height (see Exercise 8.10) for rooted ternery trees (RTT) and rooted trees (RT).

(a) Prove: For any rooted ternary tree (RTT) T, $\text{size}(T) \leq (3^{\text{height}(T)+1} - 1)/3$. Find such a bound for the size of a rooted tree (RT) in terms of its height or explain why there isn't one.

(b) Prove: For any rooted ternary tree (RTT), $\text{size}(T) \geq \text{height}(T) + 1$. Find such a bound for the size of a rooted tree (RT) in terms of its height or explain why there isn't one.

(c) Prove: For any rooted full ternary tree (RFTT), $\text{size}(T) \geq 3 \times \text{height}(T) + 1$.

Problem 8.29 (Kraft Inequality). In an RBT or RFBT, the depth ℓ of a vertex is its distance to the root.

(a) Give an RBT with one vertex at depth 0, two at depth 1 and 4 at depth 2. Is your tree an RFBT?

(b) A leaf is a vertex with no children. Let $\ell_1, \ldots, \ell_L$ be the depths of the leaves in an RFBT. Prove that $\sum_{\ell_i} 2^{-\ell_i} = 1$.

(c) Prove, more generally, that in an RBT, $\sum_{\ell_i} 2^{-\ell_i} \leq 1$. (For the empty tree ε, this sum is empty and equals 0.)

Problem 8.30 (Tree Merging). Start with n isolated trees: ①② $\cdots$ ⓝ, each just a root (a collection of trees is a forest). To merge two trees, make one root a child of the other root. Here is a sequence of merges:

(a) Start with 8 roots ①② $\cdots$ ⑧ and construct the tree on the right using merges.

(b) Start with n roots. Let T_k be the number of disjoint trees in the forest after k merges. What is T_0? Show that $T_k = n - k$.

(c) Prove that any tree with n vertices can be obtained from n roots using $n - 1$ merges.

Problem 8.31 (Rooted Short Trees, RST). When merging trees (Problem 8.30), if we always make the smaller tree's root a child of the larger tree's root, we get short trees. The size of a tree is the number of vertices it has. Here is the recursive definition of RST.

① A single root-node ● is in RST.

② Let T_1, T_2 be disjoint RSTs with roots r_1 and r_2 and $\text{size}(T_1) \geq \text{size}(T_2)$. Then making r_2 a child of r_1 gives another RST with root r_1.

(a) Is every tree in RST a rooted tree? Is RST $\subseteq$ RBT? Which of these trees are in RST?

(i)   (ii)   (iii)   (iv)   (v)   (vi)   (vii)

(b) Report size and height for each tree in (a). The height is the longest path-length from the root to a leaf.

(c) Prove: for every RST T, $\text{height}(T) \leq \log_2(\text{size}(T))$. (Hence short tree. Union-find algorithms use short trees.)

Problem 8.32. (Requires use of matrices.) Let F_n be the Fibonacci numbers with $F_0 = 0$ and define $A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$.

(a) Prove that $A^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}$ and give a $\log n$-algorithm to compute F_n.

(b) Take the determinant of A^n and hence prove: $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$.

Problem 8.33 (Computing Fibonaccis). Algorithm F(n) computes the nth Fibonacci number for $n \in \mathbb{N}$.

(a) Let T_n be the time to compute $F(n)$. Get a recurrence for T_n.

(b) Show that $T_n \geq cF(n)$ for a constant c. Is this runtime impressive? Explain.

(c) Give another algorithm with linear runtime, $T_n \leq Cn$.

(d) Find an algorithm with logarithmic runtime, $T_n \leq C \log_2 n$. Prove the correctness and runtime of your algorithm. *[Hint: Problems 8.32, 7.46.]*

```
out=F(n)
 if(n<3) out=1;
 else
  out=F(n-1)+F(n-2);
```

Problem 8.34. You start at $x = 0$ and at step i you can move up or down i. So a possible path is $0, 1, 3, 0, 4$.
  (a) Prove that every $n \in \mathbb{N}$ can be reached.
  (b) Let $T(n)$ be the minimum number of steps to reach n. Prove that $T(n) \leq 3\sqrt{2n}$.

Problem 8.35 (Nested roots). Define the sequence of nested roots $\sqrt{m}$, $\sqrt{m + \sqrt{m}}$, $\sqrt{m + \sqrt{m + \sqrt{m}}}$, ... by the recurrence $x_1 = \sqrt{m}$ and $x_{n+1} = \sqrt{m + x_n}$ for $n \geq 1$. Prove that $x_n < \sqrt{m + 1/4} + 1/2$. Evaluate the upper bound for $m = 1$ and $m = 6$ and compare with the actual limits (you may numerically estimate the limits).

Problem 8.36. Let $A_0, A_1, A_2, \ldots$ be a sequence. The differencing operator for sequences is like differentiation for functions. The kth difference is recursively defined as follows:
$$\Delta^{(0)} A_n = A_n; \qquad \Delta^{(k)} A_n = \Delta^{(k-1)} A_n - \Delta^{(k-1)} A_{n-1}, \text{ for } k \geq 1.$$
Show that $\Delta^{(1)} A_n = A_n - A_{n-1}$ and $\Delta^{(2)} A_n = A_n - 2A_{n-1} + A_{n-2}$. For what n are $\Delta^{(1)} A_n$ and $\Delta^{(2)} A_n$ defined?

Problem 8.37. Let A_n and B_n be two sequences. The differencing operator is defined in Problem 8.36.
  (a) Prove by induction on k that $\Delta^{(k)}$ is linear, $\Delta^{(k)}(aA_n + bB_n) = a\Delta^{(k)} A_n + b\Delta^{(k)} B_n$.
  (b) Use (a) and induction on k to prove that $\Delta^{(k)} A_n = \Delta^{(1)}(\Delta^{(k-1)} A_n)$.

Problem 8.38. In this problem you analyze how the differencing operator affects polynomials.
  (a) Let $A_n = n^k$. Show that $\Delta^{(1)} A_n$ is a polynomial of degree $k - 1$.
  (b) If $A_n = a_0 + a_1 n + a_2 n^2 + \cdots + a_k n^k$ is a degree k polynomial in n, show that $\Delta^{(1)} A_n$ has degree $k - 1$.
  (c) Prove by induction on i that if A_n is a degree k polynomial in n, then $\Delta^{(i)} A_n$ has degree $k - i$, for $0 \leq i \leq k$.
  (d) Show that if A_n is a polynomial in n of degree k, $\Delta^{(k)} A_n$ is a constant. (This justifies the method of differences.)

Problem 8.39 (Slow Ant). An ant is on the left end of a 1 meter rug. Each minute the ant moves 1cm right. The rug then stretches uniformly by 1 meter. After 1 minute, the ant moves to 1cm, then the rug stretches to 2 meters (stretch by a factor 2) putting the ant at 2cm. After the 2nd minute, the ant moves to 3cm, then the rug stretches to 3 meters (stretch by a factor 1.5) putting the ant at 4.5cm, and so on. Can the ant reach the right end of the rug? After minute n let x_n be the ant's position in meters and suppose that the ant never reaches the right end of the rug.
  (a) What is x_0? Show that $x_{n+1} = (n + 1)(x_n + 0.01)/n$. Where is the right end of the rug after minute n?
  (b) Solve the recurrence for x_n and derive a contradiction. What do you conclude?
  (c) Estimate how long it takes the ant to reach the right end of the rug.

Problem 8.40. 1 meter rectangualar planks have mass 100g and center of mass in the middle. You stack planks to make a diving board for a massless ant to walk out 10 meters beyond the edge of the table (see figure). Is it possible? Number the planks $1, \ldots, n$. Plank i rests on plank $i + 1$, which is displaced $1/2i$ meters to the right of plank i ("plank" $n + 1$ is the table).

  (a) Assume the structure is stable for a massless ant. Show that the ant can walk out to $H_n/2$ meters beyond the edge of the table (H_n is the nth Harmonic number). Estimate the number of planks needed to reach 10 meters.

Prove that the structure is stable. The structure is stable if the center of mass of the group of planks $\{1, \ldots, i\}$ is above plank $i + 1$, for each $i \in \{1, \ldots, n\}$. For two groups of objects with total masses m_1 and m_2 and centers of mass x_1 and x_2, the center of mass of all objects combined is at $(m_1 x_1 + m_2 x_2)/(m_1 + m_2)$.
  (b) Let x_i be the center of mass of the group of planks $1, \ldots, i$. What is x_1? Show that $x_{i+1} = (ix_i + \frac{1}{2}(H_i+1))/(i+1)$.
  (c) Prove that $x_i = H_i/2$ and hence that the structure is stable. (To derive this formula, use Problem 5.18(a).)
  (d) What if the ant has mass 100g (a fat ant)? Can the ant still make it out to 10 meters?

Problem 8.41 (Hadamard Matrices).   This problem requires knowledge of matrices. The Sylvester-Walsh recursive definition for a set of matrices $\mathcal{H} = \{H_0, H_1, H_2, \ldots\}$ is given by
$$H_0 = [1]; \qquad H_k = \frac{1}{\sqrt{2}} \begin{bmatrix} H_{k-1} & H_{k-1} \\ H_{k-1} & -H_{k-1} \end{bmatrix} \qquad \text{for } k \geq 1.$$
  (a) What are H_1 and H_2? Prove that H_k is a symmetric $2^k \times 2^k$ matrix with all entries $\pm 2^{-k/2}$.
  (b) Prove that (i) $H_k H_k^{\mathsf{T}} = I$, where I is the $2^k \times 2^k$ identity matrix. (ii) $\operatorname{trace}(H_k) = 0$ for $k \geq 1$.

Problem 8.42. The Hadamard matrix in Problem 8.41 is used in the Hadamard transform (signal processing, fast-matrix-algorithms, coding theory, quantum computing, etc). Let $\mathbf{x}$ be a vector of length 2^k. This problem investigates an efficient algorithm for computing the matrix vector product $\mathbf{y} = H_k \mathbf{x}$. Let $n = 2^k$ be the size of $\mathbf{x}$.

(a) Show that standard matrix multiplication uses n^2 multiplications and $n(n-1)$ additions to compute $\mathbf{y}$.

(b) Partition $\mathbf{x}$ $\mathbf{y}$ into top and bottom halves. So $\mathbf{x} = \begin{bmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \end{bmatrix}$ and $\mathbf{y} = \begin{bmatrix} \mathbf{y}_1 \\ \mathbf{y}_2 \end{bmatrix}$. Show that

$$\begin{aligned} \mathbf{y}_1 &= H_{k-1}\mathbf{x}_1 + H_{k-1}\mathbf{x}_2 \\ \mathbf{y}_2 &= H_{k-1}\mathbf{x}_1 - H_{k-1}\mathbf{x}_2 \end{aligned}$$

(c) Let T_k be the number of operations (multiplies and adds) to compute $H_k\mathbf{x}$. Show that

$$T_0 = 1 \qquad \text{and} \qquad T_k = 2T_{k-1} + 2^k \qquad \text{for } k \geq 1.$$

(d) Show that $T_k = n(1 + \log_2 n)$. (Multiplication by a Hadamard is fast compared to general matrix multiplication.)

Problem 8.43 (Generating Functions). Generating functions are useful for deriving formulas for complicated recursions, instead of guessing formulas to prove by induction. Let $T_0, T_1, T_2, \ldots$ be the infinite sequence produced by the recurrence $T_0 = 0$ and $T_n = T_{n-1} + 2n - 1$ for $n \geq 1$. The generating function $G(s)$, for the sequence $T_0, T_1, T_2, \ldots$, is defined by the "formal" power series

$$G(s) = T_0 s^0 + T_1 s^1 + T_2 s^2 + \ldots = \sum_{i=0}^{\infty} T_i s^i.$$

(a) Let $G^{(n)}(s)$ be the nth derivative of G. Show that $T_n = G^{(n)}(0)/n!$.

(b) Show $G(s) = \sum_{i=0}^{\infty} T_i s^i = s \cdot \sum_{i=1}^{\infty} T_{i-1} s^{i-1} + 2\sum_{i=1}^{\infty} i s^i - \sum_{i=1}^{\infty} s^i$. Show that the first sum is $sG(s)$.

(c) Prove by induction that $\sum_{i=1}^{n} i s^i = s(1 + ns^{n+1} - (n+1)s^n)/(1-s)^2$. What is $\sum_{i=1}^{\infty} i s^i$ for $0 < s < 1$?

(d) Show that $G(s) = (1-s)^{-1} - 3(1-s)^{-2} + 2(1-s)^{-3}$.

(e) Compute $G^{(1)}(s)$, $G^{(2)}(s)$, $G^{(3)}(s)$ and conjecture a formula for $G^{(n)}(s)$. Prove it.

(f) Compute a formula for $T_n = G^{(n)}(0)/n!$. Prove it by induction.

We met the sum of the odd numbers many times. You can guess the solution and prove it by induction, so generating functions are overkill here. But when there is no easy guess, generating functions are the powertool of choice.

Problem 8.44. Find a formula for T_n where $T_0 = 1, T_1 = 4$ and $T_{n+2} = 4T_{n+1} - 4T_n$. In Problems 7.27, we guessed the solution. Generating functions remove the guesswork.

(a) Show that $G(s) = 1 + 4s + \sum_{n=2}^{\infty} T_n s^n$.

(b) Use the recurrence to show that $\sum_{n=2}^{\infty} T_n s^n = 4sG(s) - 4sT_0 - 4s^2 G(s)$.

(c) Hence, show that $G(s) = (1 - 2s)^{-2}$.

(d) Show that $G^{(k)}(s) = 2^k(k+1)!(1-2s)^{-(k+2)}$ (the kth derivative).

(e) Use Problem 8.43(a) to show that $T_n = (1+n)2^n$.

Problem 8.45. Derive the generating function for the Fibonacci numbers F_n, and use it to get a formula for F_n. Recall that $F_1 = 1, F_2 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 3$. Define the generating function

$$G(s) = F_1 s + F_2 s^2 + F_3 s^3 + \cdots = \sum_{n=1}^{\infty} F_n s^n.$$

(a) Use the recursion $F_n = F_{n-1} + F_{n-2}$ for $n \geq 3$ to show that

$$\sum_{n=3}^{\infty} F_n s^n = s \sum_{n=2}^{\infty} F_n s^n + s^2 \sum_{n=1}^{\infty} F_n s^n.$$

(b) Use (a) to show $(1 - s - s^2)G(s) = s$ and hence $G(s) = s/(1 - s - s^2)$.

(c) Use $G(s)$ to derive the formula $F_n = \left((1 + \sqrt{5})^n - (1 - \sqrt{5})^n\right)/2^n\sqrt{5}$. (See Problems 8.46 or 8.47 for hints.)

Problem 8.46. Let $G(s) = (1 - s - s^2)^{-1}$. For $|s| < (\sqrt{5} - 1)/2 \approx 0.618$, the Taylor series for $G(s)$ converges,

$$G(s) = A_0 + A_1 s + A_2 s^2 + A_3 s^3 + A_4 s^4 + \cdots = \sum_{k=0}^{\infty} A_k s^k.$$

(a) Show that $G(s) = 1 + s(1 + s) + s^2(1 + s)^2 + s^3(1 + s)^3 + \cdots + s^i(1 + s)^i + \cdots$.

(b) Show that the coefficients in the series expansion of $G(s)$ are $A_n = \sum_{i=\lceil n/2 \rceil}^{n} \binom{i}{n-i}$.

(c) Compute $A_0, \ldots, A_6$. Show $A_k = A_{k-1} + A_{k-2}$ for $k \geq 2$, and hence $A_k = F_{k+1}$ (F_n are the Fibonacci numbers).

(d) Why are Fibonacci numbers in the leading digits of $1/0.9899 = 1.010203050813213455 \cdots$?

The function $G(s) = (1 - s - s^2)^{-1}$ is related to the generating function for the Fibonacci numbers.

Problem 8.47. One can analyze $G(s) = (1 - s - s^2)^{-1}$ in Problem 8.46 by using partial fractions. Show:
$$G(s) = \frac{1}{1 - s - s^2} = \frac{1}{\phi_- \sqrt{5}} \cdot \frac{1}{1 - s/\phi_-} - \frac{1}{\phi_+ \sqrt{5}} \cdot \frac{1}{1 - s/\phi_+},$$
where $\phi_\pm = -(1 \pm \sqrt{5})/2$. ($\phi_\pm$ are the roots of the quadratic $1 - s - s^2$.) Using $1/(1-x) = 1 + x + x^2 + \cdots$, show:
$$G(s) = \frac{1}{\sqrt{5}} \left[1 \cdot \left(\frac{1}{\phi_-} - \frac{1}{\phi_+} \right) + s \cdot \left(\frac{1}{\phi_-^2} - \frac{1}{\phi_+^2} \right) + s^2 \cdot \left(\frac{1}{\phi_-^3} - \frac{1}{\phi_+^3} \right) + s^3 \cdot \left(\frac{1}{\phi_-^4} - \frac{1}{\phi_+^4} \right) + \cdots \right].$$
Hence, prove that the A_n in Problem 8.46 are given by $A_n = (\rho_+^{n+1} - \rho_-^{n+1})/\sqrt{5}$, where $\rho_\pm = (1 \pm \sqrt{5})/2$.

Problem 8.48. Solve these recurrences and give a formula for A_n. Tinker. The techniques available to you are: guess and prove; methods for linear recurrences, Problems 7.24–7.27; generating functions, Problems 8.46–8.44.

(a) $A_0 = 0$ and $A_n = A_{n-1} + n$.

(b) $A_0 = 1$ and $A_n = \alpha A_{n-1} + \beta$.

(c) $A_0 = 1$ and $A_n = \alpha A_{n-1} + \beta n$.

(d) $A_0 = 1$ and $A_n = 2n A_{n-1}$.

(e) $A_1 = 1; A_2 = 3/4$ $A_n = A_{n-1}/2 + A_{n-2}/4$.

(f) $A_0 = 3; A_1 = 8$ and $A_n = 5A_{n-1} - 6A_{n-2}$.

(g) $A_0 = 3; A_1 = 5; A_2 = 17$ and $A_n = 2A_{n-1} - 4A_{n-3}$.

(h) $A_0 = 2; A_1 = 2$ and $A_n = 2A_{n-1} - 2A_{n-2}$.

(i) $A_0 = 1; A_1 = -1$ and $A_n = 2A_{n-1} - 3A_{n-2}/4$.

(j) $A_0 = 2; A_1 = 6$ and $A_n = 4A_{n-1} - 4A_{n-2}$.

Problem 8.49. Solve the following challenging recurrence without guessing. $P_0 = 1$, $P_n = 1 - P_{n-1}/2$ for $n > 0$.

(a) Use generating functions to derive a formula for P_n. *[Hint: Use partial fractions to analyze the generating function.]*

(b) Write $P_n = a_n/b_n$ and use the methods from Problem 7.42 to solve the joint recursion for a_n, b_n.

Problem 8.50 (Catalan Numbers). Let C_n be the number of RBTs with n vertices. Find a formula for C_n.

(a) What are C_0, C_1, C_2, C_3, C_4? Is there any obvious pattern?

(b) Show the recursion $C_n = \sum_{i=0}^{n-1} C_i C_{n-1-i}$, for $n \geq 1$. Compute C_5 and C_6.

(c) Show that the generating function satisfies $G(s) = 1 + \sum_{n=1}^{\infty} \left(\sum_{i=0}^{n-1} C_i C_{n-1-i} \right) s^n$.

(d) Show that $\sum_{n=1}^{\infty} \sum_{i=0}^{n-1} f(n, i) = \sum_{i=0}^{\infty} \sum_{n=i+1}^{\infty} f(n, i)$. (Assume absolute convergence.)

(e) Show that $G(s) = 1 + sG(s)^2$. Solve the quadratic and show $G(s) = (1 - \sqrt{1 - 4s})/2s$.

(f) Let a_k be the kth derivative of $\sqrt{1 - 4s}$ at $s = 0$. Show that $a_k = -2^k \times 1 \cdot 3 \cdot 5 \cdot (2k - 3)$.

(g) Explain why $C_n = a_{n+1}/2(n+1)!$ and hence derive $C_n = (2n)!/n!(n+1)!$.

(h) Prove by induction that $C_n = (2n)!/n!(n+1)!$. C_n are known as the Catalan numbers.

Problem 8.51. [**Principle of structural induction**] Define a recursive set $\mathcal{S}$ as follows:

① [**Base case**] $s_1 \in \mathcal{S}$.

② [**Constructor**] $s, s' \in \mathcal{S} \to f(s, s') \in \mathcal{S}$.

The constructor f combines s and s' to create $f(s, s') \in \mathcal{S}$. For predicate $P(s)$, suppose
$$P(s_1) \text{ is true and } P(s) \wedge P(s') \to P(f(s, s')).$$

(a) What is s_2, the second string in $\mathcal{S}$? What are the next three strings s_3, s_4, s_5?

(b) For $s \in \mathcal{S}$, define the depth $\delta(s)$ to be the minimum number of uses of the constructor needed to derive s. What are the depths of s_1, s_2, s_3, s_4, s_5? Why is depth well defined.

(c) Is there any string other than s_1 with a depth less than 1?

(d) To prove $P(s)$ is true for all $s \in \mathcal{S}$, assume there is some $s \in \mathcal{S}$ for which $P(s)$ is false.

   (i) Let s_* be a string of minimum depth for which $P(s)$ is false. Why must s_* exist? Show that $\delta(s_*) > 0$.

   (ii) Consider any derivation of s_* with depth $\delta(s_*)$. The last step constructs s_* from two strings s', s'' which appear earlier in the derivation, $s_* = f(s', s'')$. Prove that $\delta(s') < \delta(s_*)$ and $\delta(s'') < \delta(s_*)$.

   (iii) Show that $s_* \in \mathcal{S}$, a contradiction.

(A "natural" ordering of a recursive set is by increasing depth. The same proof idea works for more complicated sets.)

9.4 Problems

For all problems, assume basic operations take 1 time-unit $(+, -, \times, \div, \lfloor \cdot \rfloor, \lceil \cdot \rceil, \text{assign}, \text{compare}, \max, \min)$.

Problem 9.1. Compute the following sums.

(a) $\sum_{i=1}^{5} 1$

(b) $\sum_{i=1}^{5} i$

(c) $\sum_{i=1}^{5} i^2$

(d) $\sum_{i=1}^{5} (4-i)$

(e) $\sum_{i=1}^{5} 2$

(f) $\sum_{i=1}^{5} 2^i$

(g) $\sum_{i=1}^{5} (2^i)^2$

(h) $\sum_{i=1}^{5} 2^{i^2}$

(i) $\sum_{i=1}^{5} \ln i$

(j) $\sum_{i=1}^{5} \ln i^2$

(k) $\sum_{i=1}^{5} (\ln i)^2$

(l) $\sum_{i=1}^{5} 2^{\log_2 i}$

(m) $\sum_{i=1}^{3} \sum_{j=1}^{3} 2$

(n) $\sum_{i=1}^{3} \sum_{j=1}^{3} (i-j)$

(o) $\sum_{i=1}^{3} \sum_{j=1}^{i} 2$

(p) $\sum_{i=1}^{3} \sum_{j=1}^{i} (i-j)$

(q) $\sum_{i=1}^{3} \sum_{j=1}^{3} \sum_{k=1}^{3} 2$

(r) $\sum_{i=1}^{3} \sum_{j=1}^{3} \sum_{k=1}^{3} 2^{i+j+k}$

(s) $\sum_{i=1}^{3} \sum_{j=1}^{3} \sum_{k=1}^{3} (i+j)$

(t) $\sum_{i=1}^{3} \sum_{j=1}^{3} \sum_{k=1}^{3} ijk$

Problem 9.2. Tinker and then compute formulas that do not contain a sum for the following:

(a) $\sum_{i=1}^{n} 3i$

(b) $\sum_{i=1}^{n} (3i+2j)$

(c) $\sum_{i=1}^{2n} (1+2i)$

(d) $\sum_{i=1}^{n} (3i+2i^2)$

(e) $\sum_{i=1}^{n} (i+1)^2$

(f) $\sum_{i=0}^{n} 2^{3+i}$

(g) $\sum_{i=1}^{n} ij$

(h) $\sum_{i=0}^{n} (i+j)^2$

(i) $\sum_{i=1}^{n} (-1)^i i$

(j) $\sum_{i=0}^{n} (-1)^i i^2$

Problem 9.3. Compute formulas that do not contain a sum for the following:

(a) $\sum_{i=1}^{n} \sum_{j=1}^{m} (i+j)$

(b) $\sum_{i=1}^{n} \sum_{j=1}^{i} (i+j)$

(c) $\sum_{i=0}^{n} \sum_{j=0}^{n} (2^i + 2^j)^2$

(d) $\sum_{i=1}^{n} \sum_{j=1}^{i} (i+j)^2$

(e) $\sum_{i=0}^{n} \sum_{j=0}^{m} 2^{i+j}$

(f) $\sum_{i=0}^{n} \sum_{j=0}^{i} (2^i + 2^j)^2$

(g) $\sum_{i=0}^{n} \sum_{j=0}^{i} 2^{i+j}$

(h) $\sum_{i=0}^{n} \sum_{j=i}^{n} (i+j)$

(i) $\sum_{i=0}^{n} \sum_{j=0}^{i} (2^j + i)^2$

(j) $\sum_{i=0}^{n} \sum_{j=0}^{i} 2^i$

(k) $\sum_{i=0}^{n} \sum_{j=0}^{i} i2^j$

(l) $\sum_{i=1}^{n} \sum_{j=1}^{n} \ln(ij)$

Problem 9.4. Compute a formula for: (a) $\sum_{i=0}^{n} (2^i)^2$ (b) $\sum_{i=0}^{n} i2^i$ (c) $\sum_{i=0}^{n} i^2 2^i$.

Problem 9.5. Compute a formula for $\sum_{n=0}^{\infty} \sum_{i=0}^{n} y^n x^i$. You may assume $|x|, |y| < 1$.

Problem 9.6. Compute formulas for (a) $\sum_{i=1}^{n} \sum_{j=1}^{n} \sum_{k=1}^{n} (i+j+k)$ (b) $\sum_{i=1}^{n} \sum_{j=1}^{i} \sum_{k=1}^{j} (i+j+k)$.

Problem 9.7. Compute a formula for the sum $4 + 44 + 444 + 4444 + \cdots + 44 \cdots 4$ (the last term has n fours).

Problem 9.8. Find a formula for the sum of first n positive integers, excluding the multiples of 3.

Problem 9.9. Estimate these sums. (a) $\sum_{i=1}^{10} \sum_{j=1}^{20} 2^{i+j}$ (b) $2^1 \times 2^2 \times 2^3 \times \cdots \times 2^{20} = \prod_{i=1}^{20} 2^i$.

Problem 9.10. Let $\boldsymbol{a} = [1, 2, 3, 4, \ldots]$ and $\boldsymbol{b} = [1, 2, 4, 8, \ldots]$. Compute $\sum_{i=1}^{20} \sum_{j=1}^{10} a_i b_j$.

Problem 9.11. Here are errors in the use of asymptotic notation. Explain why they are errors.

(a) $2n^2 + n = \Theta(n^2)$.

(b) $4^n \in \Theta(2^n)$ because 4 and 2 are constants.

(c) $O(1) + O(1) = O(1)$.

(d) Your runtime $T \in O(n^2)$, which is slower than linear.

(e) My runtime $T \in o(n^3)$, which is super fast, linear.

(f) $f \in O(g)$ (i.e. "$f \le g$"). Taking exponents, $2^f \in O(2^g)$.

Problem 9.12. Someone said $f = O(n)$, that is "f equals $O(n)$". Why is this bad?

Problem 9.13. Plot these functions on a log-log plot to get a feeling for their behavior.

$\log n$ n $n \log n$ n^2 n^3 $n^{\log n}$ 2^n $n!$ n^n

Problem 9.14. Explain what $T(n) \in \Theta(1)$, $T(n) \in O(1)$ and $T(n) \in \Omega(1)$ mean.

Problem 9.15. Determine which of these functions is in $\Theta(n)$, in $\Theta(n^2)$, or neither.

(a) 10

(b) $3n + 9$

(c) $\lfloor n \rfloor$

(d) $\lceil n/2 \rceil$

(e) $n^2 + n + 1$

(f) $\lfloor n \rfloor \cdot \lceil n/2 \rceil$

(g) $5n \log n$

(h) 2^n

(i) $n^2 + 3n$

(j) $n^2 \log n$

(k) $3^{\log_2 n}$

(l) $4^{\log_2 n}$

Problem 9.16. Determine the order-relationships between 2^{n+1}, 2^n, 2^{2n}, 2^{n^2}, e^n, $n!$.

Problem 9.17. Determine the order-relationship between $\ln n$, $\ln(n^2 + 1)$, $\ln(2n)$.

Problem 9.18. Use big-Oh to order these functions. (F_n are Fibonacci numbers and H_n are Harmonic numbers.)
$$F_n, \ H_n, \ n^{n^2}, \ (1.5)^n, \ \sqrt{n}, \ n^{100}, \ n!, \ 2^n, \ (\ln n)^n, \ n^{\ln n}, \ \ln^3 n, \ n^2, \ n \ln n, \ n^3, \ n^2 2^n, \ n^{2^n}, \ F^2_{\lceil H_n \rceil}, \ H_{F_n}.$$

Problem 9.19. Answer true or false.
(a) $\sqrt{n} \ln n \in O(n)$ (b) $2n^2 + 1 \in O(n^2)$ (c) $\sqrt{n} \in O(\ln n)$ (d) $\ln n \in O(\sqrt{n})$ (e) $3n^3 + \sqrt{n} \in \Theta(n^3)$
(f) $\ln n \in \Theta(\log_2 n)$ (g) $2^{n+1} \in O(2^n)$ (h) $2^{2n} \in O(2^n)$ (i) $3^n \in O(2^n)$ (j) $3n^3(1 + \sqrt{n}) \in \Theta(n^3)$
(k) $\ln n^2 \in \Theta(\ln n)$ (l) $2^n \in \Theta(3^n)$ (m) $\ln^2 n \in \Theta(\ln n)$ (n) $2^n \in O(3^n)$ (o) $\ln(2^n) \in \Theta(\ln(3^n))$
(p) $2^{2\log_2 n} \in \Theta(n^2)$ (q) $2^{2\ln n} \in \Theta(n^2)$ (r) $2^{2\ln n} \in O(n^2)$ (s) $n! \in \Theta(n^n)$ (t) $n! \in O(n^n)$
(u) $\sum_{i=1}^{n} i^2 \in \Theta(n^3)$ (v) $\sum_{i=1}^{n} \sqrt{i} \in \Theta(n^2)$ (w) $\sum_{i=1}^{n} 2^i \in \Theta(2^n)$ (x) $\sum_{i=1}^{n} 3^i \in \Theta(3^n)$ (y) $\sum_{i=1}^{n} 3^i \in \Theta(2^n)$

Problem 9.20. For each expression $f(n)$, give as simple a function $g(n)$ as you can for which $f(n) \in \Theta(g(n))$.
(a) $3n^2 + \sqrt{n}$ (b) $2^{3n} + 4^n$ (c) $\ln(n^2) + \ln^2 n$ (d) $(0.9)^n + n^2$ (e) $(1.1)^n + n^{17}$ (f) $n + n \ln n + \sqrt{n}$
(g) $\sum_{i=1}^{n} i^3$ (h) $\sum_{i=1}^{n} \sqrt{i}$ (i) $\sum_{i=1}^{n} 1/i$ (j) $\sum_{i=1}^{n} 2^i$ (k) $\sum_{i=1}^{n}(2^i + 5^i)$ (l) $(n + n^2)(1 + 2^n)$
(m) $\ln n!$ (n) $\ln^2 n!$ (o) $\ln 3^n$ (p) $\ln^2 2^n$ (q) $\ln 2^{n^2}$ (r) $(1 + n)(1 + n^2)$
(s) $\ln(2^n)^2$ (t) $2^{n^2 + 2n}$ (u) $\ln(2^{n^2 + 2n})$ (v) $\sum_{i=1}^{n} \ln i$ (w) $n^2(1 + \sqrt{n})$ (x) $(n + a)^b$, $a, b > 0$

Problem 9.21. Prove/disprove: (a) $\dfrac{n^3 + 2n}{n^2 + 1} \in \Theta(n)$; (b) $(n + 1)! \in \Theta(n!)$; (c) $n^{1/n} \in \Theta(1)$; (d) $(n!)^{1/n} \in \Theta(n)$.

Problem 9.22. Let $f(n) = \sum_{i=1}^{n} i$. How is $f(n)$ asymptotically related to n, n^2, n^3?

Problem 9.23. For $k \in \mathbb{N}$, prove $1^k + 2^k + \cdots + n^k \in \Theta(n^{k+1})$. (Prove upper and lower bounds Cn^{k+1} and cn^{k+1}).

Problem 9.24. Prove by contradiction: (a) $n^3 \notin O(n^2)$ (b) $2^n \notin \Theta(3^n)$ (c) $3^{\lfloor \log_2 n \rfloor} \notin \Theta(n)$.

Problem 9.25. Show that $n^1 + n^2 + n^3 + \cdots + n^n = \sum_{i=1}^{n} n^i \in \Theta(n^n)$.

Problem 9.26. How many digits are written in 1,2,3,...,n? For example 1,2,3,4,5,6,7,8,9,10 is eleven digits.

Problem 9.27. Moore's law says CPU capability doubles every two years. In 2015, a standard desktop executes 10^9 operations per second (multiplications and additions). Let T_n be the runtime (number of operations) on a computing problem of size n. Complete the table below, which shows the maximum sized problem that can be solved in a second.

year		Maximum sized problem solvable given an algorithm's runtime					
	$T_n = 10^5 n$	$T_n = 10^4 n \log_2 n$	$T_n = 10n^2$	$T_n = n^3$	$T_n = 2^n$	$T_n = n!$
2015	$n_{\max} = 10^4$	?	?	?	?	?
2025	$n_{\max} \approx 3 \times 10^5$	?	?	?	?	?
2035	$n_{\max} \approx 10^7$	?	?	?	?	?

Problem 9.28 (Estimate). Estimating properties of your algorithms is a fine art. Asymptotic analysis is very useful for quick and dirty sanity-checks. Practice your mental-math estimation skills (no electronic devices allowed).
(a) Are there more than a million pages in all the books of your library? What about the Library of Congress?
(b) How many hours in one million seconds. What about days? What about Years?
(c) Your algorithm sorts one thousand numbers in 1 second. How long does it take for one million numbers if the runtime is in (i) $\Theta(n)$,   (ii) $\Theta(n \log_2 n)$,   (iii) $\Theta(n^2)$? Give your answers in seconds, days and years.
(d) For the US, estimate the number of: (i) Cities.   (ii) Gas stations.   (iii) Miles of road.   (iv) Miles driven per year.
(e) How many instructions can your 2GHz CPU execute in one year? What about arithmetic operations?

Problem 9.29. $f(0) = 1$; $f(n) = nf(n - 1)$. Asymptotically compare $f(n)$ with: (a) 2^n (b) n^n.

Problem 9.30. $f(0) = 0$; $f(n) = f(n-1) + \sqrt{n}$. Asymptotically compare $f(n)$ with (a) n (b) $n\sqrt{n}$ (c) n^2.

Problem 9.31. Compare these functions: $n^{1/\log_2 n}$; $n^{2/\log_2 n}$; $n^{1/\log_3 n}$; $n^{1/2^{\log_2 \log_2 n}}$; $n^{1/2^{2\log_2 \log_2 n}}$.

Problem 9.32. Give the asymptotic big-Theta behavior of the runtime T_n, where
(a) $T_0 = 1$; $T_n = T_{n-1} + n^2$ for $n \geq 2$.
(b) $T_0 = 1$; $T_1 = 2$; $T_n = 2T_{n-1} - T_{n-2} + 2$ for $n \geq 2$.
(c) $T_0 = 1$; $T_n = 2T_{n-1} + 1$ for $n \geq 1$.
(d) $n = 2^k$ and $T_1 = 1$; $T_n \leq 2T_{n/2} + n$ for $k \geq 1$. *[Hint: Prove $n\log_2 n \leq T_n \leq 2n\log_2 n$.]*

Problem 9.33. In each case, give the most accurate order relation between T_n and (i) n;   (ii) 2^n;   (iii) $2^{n!}$.

(a) $T_1 = 2$; $T_n = T_{n-1}^2$ for $n > 1$.   (d) $T_1 = 2$; $T_n = (T_{n-1})^{1+2^{-n}}$ for $n > 1$.
(b) $T_1 = 2$; $T_n = 2 + 2T_{n-1}$ for $n > 1$.   (e) $T_1 = 2$; $T_n = (T_{n-1})^{1+1/n}$ for $n > 1$.
(c) $T_1 = 2$; $T_n = 2nT_{n-1}$ for $n > 1$.   (f) $T_1 = 2$; $T_n = (T_{n-1})^{\sqrt{n}}$ for $n > 1$.

Problem 9.34. A postage machine has 4¢ and 7¢ stamps. Give algorithms with $O(1)$ runtime to solve these tasks.
(a) A user inputs postage n. Determine if the postage n can be dispensed (yes or no), and
(b) If yes, compute numbers n_4 and n_7 for which $n = 4n_4 + 7n_7$. That is, compute how to dispense the postage.

Problem 9.35. An internet startup must engage users and convince them to create accounts. The 1-minute user gets bored after 1 minute and leaves. Similarly, there's the 2-minute, 3-minute, etc. users. There are half as many 2-minute users as 1-minute; half as many 3-minute users as 2-minute; and so on. The boss says you must tailor the webpage exclusively to the 1-minute user: focus on converting as many 1-minute users into accounts. Explain why.

Problem 9.36. Give order relationships between the pairs of functions. (a) $n^2!$ and $(n!)^2$ (b) $\ln(n^2!)$ and $(\ln n!)^2$.

Problem 9.37. Let $T(n) = 2^{\lfloor \log_2 n \rfloor}$. Is $T(n)$ monotonic? Plot n, $n/2$ and $T(n)$ versus n.
(a) Show that the limit of $T(n)/n$ as $n \to \infty$ does not exist.
(b) Show that there are constants c, C for which $c \cdot n \leq T(n) \leq C \cdot n$, for $n \geq 1$.

Problem 9.38. A recursive algorithm has a runtime $T(n)$ that depends only on n, the input of size. $T(1) = 1$ and for an input-size n, the algorithm solves two problems of size $\lfloor n/2 \rfloor$ and does extra work of n to get the output.
(a) Argue that $T(n)$ satisfies the recursion $T(n) = 2T(\lfloor n/2 \rfloor) + n$.
(b) Prove $T(n) \in \Theta(n \log n)$. *[Hint: Induction to show $n\log_2 n \leq T(n) \leq 2n\log_2 n$ for $n = 2^k$ and monotonicity.]*

Problem 9.39. For $f(n)$ in (a)–(f) and $g(n)$ in (i)–(v), determine if $f \in O(g)$, $g \in O(f)$, both, or neither.

	(a) n^3	(b) 2^n	(c) $n!$	(d) $\sum_{i=1}^{n} i^2$	(e) $\sum_{i=1}^{n}\sum_{j=1}^{n} 2^{i+j}$	(f) $\sum_{i=1}^{n} i\sqrt{i}$
(i)	$n^2 \log_2^2 n$	3^n	n^n	n^2	2^n	n^2
(ii)	$n^3 + n^2$	$2^{\sqrt{n}}$	$n^{n/2}$	$n^2 \log_2 n$	2^{2n}	$n^2 \log_2 n$
(iii)	$n^{3.5}$	2^{2n}	$(n+1)!$	n^3	2^{3n}	$n^{3\sin(n\pi/2)}$
(iv)	$2^{2+3\log_2 n}$	$2^{n+\log_2 n}$	$2^{n\log_2 n}$	$4^{\log_2 n}$	2^{n^2}	$4^{\log_2 n}$
(v)	$2^{\log_2^2 n}$	$2^{n+4} + 2^{\sqrt{n}}$	2^{n^2}	$8^{\log_2 n}$	$\sum_{i=1}^{n}\sum_{j=1}^{i} 2^{i+j}$	$8^{\log_2 n}$

Problem 9.40. Use the rule of thumb for nested sums on the bottom of page 119 to obtain the asymptotic growth rate for the following sums, and verify by exact computation. If the rule does not work, why not?

(a) $\sum_{i=1}^{n}\sum_{j=1}^{i} j$.   (b) $\sum_{i=1}^{n}\left(i^2 + \sum_{j=1}^{n} j\right)$.   (c) $\sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{j=1}^{n}(i^2 + ijk)$.   (d) $\sum_{i=1}^{n}\sum_{j=1}^{i^2} j$.

Problem 9.41. Give rough and dirty asymptotic analysis (growth rates) of these nested sums using big-Oh notation. The rule of thumb for nested sums on the bottom of page 119 won't work, but modified versions of the rule can work.

(a) $\sum_{i=1}^{n}\sum_{j=1}^{\lfloor\sqrt{i}\rfloor} i^3 j^2$.   (b) $\sum_{i=1}^{n}\sum_{j=1}^{i^2} i^3 j^2$.   (c) $\sum_{i=1}^{n}\sum_{j=1}^{i^2} i \log_2 j^3$.   (d) $\sum_{i=1}^{n}\sum_{j=1}^{i^2} i^2 2^j$.

Problem 9.42 (Bounding Terms). Let $f(x)$ be a positive increasing function.

(a) Show that $\sum_{i=1}^{n} f(i) \leq n f(n)$. Use this to get an upper bound on (i) $\sum_{i=1}^{n} i^k$.   (ii) $\sum_{i=1}^{n} 2^i$.

(b) Show that $\sum_{i=1}^{n} f(i) \geq (k+1)f(n-k)$ for $0 \leq k < n$. Use this to get a lower bound on (i) $\sum_{i=1}^{n} i^k$.   (ii) $\sum_{i=1}^{n} 2^i$.

(c) Refine the bound in (a) to $\sum_{i=1}^{n} f(i) \leq (n-r)f(n-r) + rf(n)$, for $0 \leq r \leq n$, and show $\sum_{i=1}^{n} 2^i \in O(2^n \log n)$.

Problem 9.43. Suppose $f(x)$ is positive and $f(i+1)/f(i) \leq r$, where $0 < r < 1$. Show that $\sum_{i=1}^{n} f(i) \in \Theta(1)$.

Problem 9.44. You can use techniqes for sums to compute products. Show that

$$\log\left(\prod_{i=1}^{n} f(i)\right) = \sum_{i=1}^{n} \log f(i), \qquad \text{and} \qquad \log\left(\prod_{i=1}^{n}\prod_{j=1}^{m} f(i,j)\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} \log f(i,j).$$

Compute the products: (a) $\prod_{i=0}^{n} 2^i$ (b) $\prod_{i=1}^{n} 2^{2i-1}$ (c) $\prod_{i=1}^{n} i 2^i$ (d) $\prod_{i=0}^{n}\prod_{j=0}^{m} 2^{i+j}$ (e) $\prod_{i=0}^{n}\prod_{j=0}^{m} 2^i 3^j$.

Problem 9.45. Use integration to estimate $S_n = \sum_{i=1}^{n} r^i$. Compare with the exact formula.

Problem 9.46. Give upper and lower bounds and the asymptotic (big-Theta) behavior for

(a) $\sum_{i=1}^{n} \dfrac{i^2}{i^3 + 1}$ (b) $\sum_{i=1}^{n} i \ln i$ (c) $\sum_{i=1}^{n} i e^{2i}$. *[Hint: Integration by parts.]*

Problem 9.47. Use integration to get upper and lower bounds for $S_n = \sum_{i=1}^{n} \dfrac{1}{1+i^2}$.

(a) How tight are your bounds for S_{1000} (tightness is |upper bound − lower bound|).

(b) Write $S_{1000} = \sum_{i=1}^{10} \dfrac{1}{1+i^2} + \sum_{11}^{1000} \dfrac{1}{1+i^2}$.   Compute the left sum. Bound the right sum with integration. What are your new bounds. How tight are they?

(c) Generally, for $n > k$, $S_n = \sum_{i=1}^{k} \dfrac{1}{1+i^2} + \sum_{k+1}^{n} \dfrac{1}{1+i^2}$.   Use integration to bound the right sum. Show that the tightness of the bound is in $O(1/k^2)$.

Problem 9.48. Use integration to approximate: (a) $\sum_{i=1}^{\infty} i^{-3/2}$ to within $1/100$.   (b) $\ln(10^9!)$.

Problem 9.49. Give upper and lower bounds for $(2n)!/(2^{2n} \times (n!)^2)$. *[Hint: Bounds for $n!$.]*

Problem 9.50. Give a big-Theta analysis of $\sum_{i=0}^{n}\sum_{j=0}^{n} 2^{ij}$. *[Hint: Get tight upper and lower bounds. Integration.]*

Problem 9.51. Use integration to bound $\dfrac{(2i-1)!!}{(2i)!!} = \dfrac{1}{2}\cdot\dfrac{3}{4}\cdot\dfrac{5}{6}\cdots\dfrac{2i-1}{2i} = \prod_{i=1}^{n}\dfrac{2i-1}{2i}$. Compare with Problem 6.4.

Problem 9.52. For $f(x) = e^x \cdot e^{e^x}$, show: (a) $\sum_{i=1}^{n} f(i) \in \omega\left(\int_0^n f(x)\right)$ (b) $\sum_{i=1}^{n} f(i) \in o\left(\int_1^{n+1} f(x)\right)$.

(This function grows too quickly for the integration method. If your algorithm's runtime is $T(n) = e^n \cdot e^{e^n}$, good luck!)

Problem 9.53. Show that $\sum_{i=1}^{n}\sum_{j=1}^{n} i = \sum_{i=1}^{n}\sum_{j=1}^{n} j$. What about $\sum_{i=1}^{n}\sum_{j=1}^{i} i = \sum_{i=1}^{n}\sum_{j=1}^{i} j$?

Problem 9.54. For any function f show these equalities between two sums.

(a) $\sum_{i=1}^{n} f(i) = \sum_{i=0}^{n-1} f(i+1)$ (b) $\sum_{i=0}^{n} f(i) = \sum_{i=0}^{n} f(n-i)$ (c) $\sum_{i=1}^{n}\sum_{j=1}^{n} f(i)f(j) = \left(\sum_{i=1}^{n} f(i)\right)^2$

Problem 9.55. Show that: (a) $\sum_{i=1}^{n}\sum_{j=1}^{i} f(j) = \sum_{i=1}^{n}\sum_{j=i}^{n} f(i) = \sum_{i=1}^{n} f(i)(n+1-i)$ (b) $\sum_{i=1}^{n}\sum_{j=1}^{n} f(i,j) = \sum_{i=1}^{n}\sum_{j=i}^{n} f(j,i)$.

Problem 9.56. Recall $H_n = 1 + 1/2 + 1/3 + \cdots + 1/n = \sum_{i=1}^{n} 1/i$. Let $S_n = \sum_{i=1}^{n} H_i$.

(a) Use the integration method to approximate S_n.

(b) Show that $S_n = \sum_{i=1}^{n}\sum_{j=1}^{i} 1/j$, and use Problem 9.55 to show that $S_n = \sum_{i=1}^{n}\sum_{j=i}^{n} 1/i$.

(c) Compute a formula for the double sum in (b) and prove it by induction. Compare to your approximation in (a).

Problem 9.57. Show that $\sum_{i=0}^{n-1} \frac{i}{n-i} = \sum_{i=1}^{n} \frac{n-i}{i}$. Hence, show $\frac{0}{n} + \frac{1}{n-1} + \frac{2}{n-2} + \cdots + \frac{n-2}{2} + \frac{n-1}{1} = nH_n - n$.

Problem 9.58. For any function f, show that $\sum_{i=1}^{n} \sum_{j=1}^{i} f(i,j) = \sum_{j=1}^{n} \sum_{i=j}^{n} f(i,j)$. Hence, compute these Harmonic sums.

(a) $\sum_{i=1}^{n} H_i$ (b) $\sum_{i=1}^{n} iH_i$ (c) $\sum_{i=1}^{n} i^2 H_i$.

Problem 9.59. Let $S(n) = \sum_{i=1}^{n} \frac{1}{2i-1}$. Show $S(n) = H_{2n} - H_n/2$, hence $S(n) \approx (\ln 4n + \gamma)/2$, where $\gamma \approx 0.577$.

Problem 9.60 (Telescoping). Compute $\sum_{i=1}^{n}(f(i+1) - f(i))$ and $\prod_{i=1}^{n} f(i+1)/f(i)$, for any function f.

Problem 9.61. Find a formula in each case. *[Hints: Partial fractions; telescoping sum/product.]*

(a) $S(n) = \sum_{i=1}^{n} \frac{1}{i(i+1)}$

(c) $S(n) = \sum_{i=1}^{n} \frac{i}{(i+1)!}$

(e) $\Pi(n) = \prod_{i=1}^{n} \left(1 + \frac{k}{i}\right)$

(b) $S(n) = \sum_{i=1}^{n} \frac{1}{i(i+1)(i+2)}$

(d) $S(n) = \sum_{i=1}^{n} \frac{1}{(3i-1)(3i+2)}$

(f) $\Pi(n) = \prod_{i=2}^{n} \left(1 - \frac{1}{1+2+\cdots+i}\right)$

Problem 9.62. Differentiation can be used to compute sums.

(a) Give the formula for the geometric sum, $G(r) = \sum_{i=0}^{n} r^i$, and compute its derivative $\frac{dG}{dr}$.

(b) Show that $\frac{dG}{dr} = \sum_{i=0}^{n} ir^{i-1}$ and hence that $\sum_{i=0}^{n} ir^i = \frac{r}{(1-r)^2}(1 + nr^{n+1} - (n+1)r^n)$.

(c) Use the second derivative $\frac{d^2G}{dr}$ to prove the formula below for the sum $\sum_{i=0}^{n} i^2 r^i$,

$$\sum_{i=0}^{n} i^2 r^i = \frac{r(1+r)}{(1-r)^3} + \frac{(2n^2 + 2n - 1)r^{n+2} - n^2 r^{n+3} - (n+1)^2 r^{n+1}}{(1-r)^3}.$$

(d) When $-1 < r < 1$, use the result in part (c) to give formulas for the infinite sums $\sum_{i=0}^{\infty} ir^i$ and $\sum_{i=0}^{\infty} i^2 r^i$.

Problem 9.63. Use differentiation to show that $\sum_{i=1}^{\infty} 2^{-i}/i = \ln 2$.

(a) Let $S(\lambda) = \sum_{i=1}^{\infty} 2^{-\lambda i}/i$. Get a formula for $\frac{d}{d\lambda} S(\lambda)$. *[Hint: Derivative and sum commute.]*

(b) Get a formula for $S(\lambda)$ by integrating $\frac{d}{d\lambda} S(\lambda)$. For the constant of integration, try $\lambda \to \infty$.

(c) What should you set for λ in $S(\lambda)$ to get $\sum_{i=1}^{\infty} 2^{-i}/i$. What's the answer? What is $\sum_{i=1}^{\infty} 3^{-i}/i$?

Problem 9.64 (Abel's Summation by Parts). Analogous to integration by parts, $\int f dg = fg - \int g df$, prove the formula for summation by parts:

$$\sum_{i=m}^{n} f_i(g_{i+1} - g_i) = (f_n g_{n+1} - f_m g_m) - \sum_{i=m+1}^{n} g_i(f_i - f_{i-1}).$$

(a) For $\sum_{i=0}^{n} i2^i$, show that you can choose $f_i = i$ and $g_i = 2^i$. Hence show that $\sum_{i=0}^{n} i2^i = (n-1)2^{n+1} + 2$.

(b) Use summation by parts to compute a formula for $\sum_{i=0}^{n} i^2 2^i$.

(c) Using summation by parts, show $\sum_{i=1}^{n} H_i = (n+1)H_n - n$. *[Hint: $H_i = H_i \times 1$.]*

(d) Use summation by parts to show $\sum_{i=1}^{n} \frac{H_{i+1}}{i(i+1)} = 2 - \frac{1 + H_{n+1}}{n+1}$. Hence show that $\sum_{i=1}^{\infty} \frac{H_{i+1}}{i(i+1)} = 2$.

Problem 9.65.(Basel Problem) Compute exactly $\zeta(2) = \sum_{i=1}^{\infty} 1/i^2 \approx 1.645$. Basel is the hometown of Euler who announced this sum in 1735. Weierstrass proved Euler's method rigorous 100 years later.) Follow in Euler's steps.

(a) Use the Taylor series for $\sin x$ to give an infinite polynomial expansion for $(\sin x)/x$.

(b) What are the roots of $(\sin x)/x$? Show that $(\sin x)/x = A \cdot \prod_{i=1}^{\infty}(1 - x^2/\pi^2 i^2)$. What is A?

(c) Compare the coefficient of the x^2 term in (a) and (b) and deduce the value of $\sum_{i=1}^{\infty} 1/i^2$.

(d) Compute $\sum_{i=1}^{\infty} 1/(2i-1)^2$.

Problem 9.66 (Taylor Series and Infinite Sums). What is the Taylor series for $-\ln(1-x)$? Compute:

(a) $\sum_{i=1}^{\infty} (-1)^i/i$.   (b) $\sum_{i=1}^{\infty} (-1)^i/(i+1)$.   (c) $\sum_{i=1}^{\infty} r^{3i}/i$, where $0 < r < 1$.

Problem 9.67 (Accelerating convergence). Let $a_i = (-1)^{i+1}/i$ for $i = 1, 2, \ldots$ and $S_n = \sum_{i=1}^{n} a_i$. The partial sums S_n converge to $S = 1 - 1/2 + 1/3 - 1/4 + 1/5 - \cdots$. Use a Taylor expansion of $\ln(1+x)$ to guess S.

(a) Compute the partial sum S_{20} and compare with the value of the full infinite sum S.

(b) The Shank transform $S^{(1)} = \Phi(S)$ is given by $S_i^{(1)} = (S_{i-1}S_{i+1} - S_i^2)/(S_{i-1} - 2S_i + S_{i+1})$. One can iterate the Shank transform and define $S^{(2)} = \Phi(S^{(1)})$, $S^{(3)} = \Phi(S^{(2)})$, and so on. Compute $S_{10}^{(4)}$ and compare with S.

(c) What values of a_i are needed to compute $S_{10}^{(4)}$ versus S_{20}. What is the conclusion?

(d) Justify the Shank transform as a way to accelerate the convergence of the sequence using the model $S_n = S + aB^n$.

Problem 9.68 (Divergent sums). Consider the sum $S = 2^0 + 2^1 + 2^2 + 2^3 + \cdots$.

(a) [Analytic Continnuation] Let $\phi(z) = \sum_{i=0}^{\infty} 2^i z^i$. When does the sum converge?
 (i) Give a closed form for $\phi(z)$. (ii) Is the closed form defined at $z = 1$? (iii) What does this give for S?
 (It's bizzare to evaluate this sum as negative. You need a course in complex analysis to see why it's okay.)

(b) [Axiomatic summation] Define a sum operator $\Phi(\mathbf{a})$ which assigns a value to an infinite sequence $\mathbf{a} = (a_1, a_2, \ldots)$ that we would like to interpret as the infinite sum. Any such operator should be incremental and linear,
$$\Phi(a_1, a_2, a_3, \ldots) = a_1 + \Phi(a_2, a_3, a_4, \ldots) \quad \text{and} \quad \Phi(\beta a_1, \beta a_2, \beta a_3, \ldots) = \beta \Phi(a_1, a_2, a_3, \ldots).$$
Let $x = \Phi(1, 2, 4, 8, \ldots)$. Show that $x = 1 + 2x$ and hence $x = -1$. An infinite sum of positives is negative!? 😐

Problem 9.69. Sharpen your canines on these tricky sums. Tinker. Find patterns. Guess. Use induction if needed.

(a) Get formulas for these sums. (i) $\sum_{i=1}^{n} i\sqrt{2^i}$. (ii) $\sum_{i=1}^{n} i\ln(1 + 1/i)$.

(b) Get a formula for $\binom{n}{0} + \frac{1}{2}\binom{n}{1} + \frac{1}{3}\binom{n}{2} + \cdots + \frac{1}{n+1}\binom{n}{n}$, where $\binom{n}{i} = \frac{n!}{i!(n-i)!}$.

(c) Get a formula for $\cos\theta + \cos 2\theta + \cos 3\theta + \cdots + \cos n\theta$. [Hint: $e^{i\theta} = \cos\theta + i\sin\theta$.]

(d) Show that: $\dfrac{1}{\log_2 k} + \dfrac{1}{\log_3 k} + \dfrac{1}{\log_4 k} + \cdots + \dfrac{1}{\log_n k} = \dfrac{1}{\log_{n!} k}$.

(e) Get a formula for $\binom{m}{0} + \binom{m}{1}\cos\theta + \binom{m}{1}\cos 2\theta + \cdots + \binom{m}{m}\cos m\theta$. [Hint: $e^{i\theta}$; Binomial Theorem.]

(f) Get a formula for $\sum_1^n iF_i = F_1 + 2F_2 + 3F_3 + \cdots + nF_n$. ($F_n$ are the Fibonacci numbers,)

(g) Get a formula for $\sum_1^n i^2 F_i = F_1 + 4F_2 + 9F_3 + \cdots + n^2 F_n$. ($F_n$ are the Fibonacci numbers,)

(h) Get a formula for this sum of ratios of Fibonacci numbers: $\sum_{i=2}^{\infty} \dfrac{F_i}{F_{i-1}F_{i+1}}$. [Hint: Telescoping, see Problem 9.60.]

(i) Using summation by parts, show $\sum_{i=1}^{n} \dfrac{H_i}{i} = \frac{1}{2}H_n^2 + \frac{1}{2}\sum_{i=1}^{n}\dfrac{1}{i^2}$. (Problem 6.6 proves this by induction).

(j) Get a formula involving the Harmonic numbers for the sum $\sum_{k=1}^{n} \dfrac{1}{(2k-1)(k+1)}$.

(k) Get a formula involving the Harmonic numbers for $\sum_{i=1}^{n} \dfrac{1}{1 + 1/i}$.

(l) Compute the infinite sum $\sum_{i=2}^{\infty} \dfrac{1}{i^4 - i^2}$. [Hint: Partial fractions and telescoping. Basel problem.]

(m) Compute the sum $S(n) = \sum_{i=1}^{n} \dfrac{3i+8}{i(i+2)} \cdot \left(\dfrac{1}{2}\right)^i$ and $\lim_{n\to\infty} S(n)$. [Hint: Partial fractions and telescoping.]

(n) Find the sum of the numbers which do not contain the digit 5 in $\{0, 1, 2, \ldots, 10^n - 1\}$. For $n = 1$, the sum is 40.

(o) (Kempner, 1914) Let S be the sum of the reciprocals of all numbers which do not contain the digit 5.
 (i) Show that S is finite.   (ii) Estimate S to within 1.

(p) Let $S_k = \sum_{i=1}^{\infty} i^k/2^i$. (i) Show that S_k is an integer for $k = 0, 1, 2, \ldots$.   (ii) Compute S_5.

(q) **(Open problem)** Compute Apéry's constant $\zeta(3) = \sum_{i=1}^{\infty} 1/i^3$ in terms of known constants $\pi, e, 1, 2$, etc. As a start, estimate Apéry's constant to within 1/1000. (cf. Basel problem, Problem 9.65.)

Problem 9.70. Array $[a_1, \ldots, a_n]$ is input to the `MaxSubstringSum` algorithm below.

```
MaxSum ← 0;
for i, j = 1 to n do
    CurSum ← 0;
    for k = i to j do
        CurSum ← CurSum + a_k;
    MaxSum ← max(CurSum, MaxSum);
return MaxSum;
```

For $i \leq j$, the algorithm considers all starting points i and ending points j, and computes the sum of the terms from a_i to a_j in CurSum. MaxSum is the maximum such sum. This algoirthm is known as "exhaustive brute force": consider all possible substrings $[i, j]$ and find the one with maximum sum.

Show that the runtime $T(n) = 2 + \sum_{i=1}^{n} \left[2 + \sum_{j=i}^{n} \left(5 + \sum_{k=i}^{j} 2 \right) \right]$. Hence, show $T(n) = 2 + 31n/6 + 7n^2/2 + n^3/3$.

Problem 9.71. Here is a more efficient algorithm than the one in Problem 9.70.

```
MaxSum ← 0;
for i = 1 to n do
    CurSum ← 0;
    for j = i to n do
        CurSum ← CurSum + a_j;
        MaxSum ← max(CurSum, MaxSum);
return MaxSum;
```

The algorithm in Problem 9.70 repeats a lot of computation. The innermost loop (over k) computes a sum from i to j; this sum was available earlier when the sum from $i - 1$ to j was computed. We can get all substring sums starting from i in one pass from i to n.

(It helps to implement and test this and the brute-force algorithm from the previous problem on some sample sequences.)

Show that the runtime is $T(n) = 2 + \sum_{i=1}^{n} \left(3 + \sum_{j=i}^{n} 6 \right)$. Hence, show $T(n) = 2 + 6n + 3n^2$.

Problem 9.72. Here is an algorithm for `MaxSubstringSum` based on recursion.

```
function S(ℓ, r)
if ℓ = r, return max(0, a_ℓ);
mid = ⌊(ℓ + r)/2⌋;
(LMax, RMax) = (S(ℓ, mid), S(mid + 1, r));
MidL, MidLmax ← a_mid;
for i = mid − 1 to ℓ do
    MidL ← MidL + a_i;
    MidLmax ← max(MidLmax, MidL);
MidR, MidRmax ← a_mid+1;
for j = mid + 2 to r do
    MidR ← MidR + a_j;
    MidRmax ← max(MidRmax, MidR);
return max(LMax, RMax, MidLmax + MidRmax);
```

The idea is to identify 3 cases for the max-substring: it lies entirely within the left half of the sequence (LMax); the right half of the sequence (RMax); or, it crosses over from the left to the right (MidMax). The final output is the maximum of the three cases.

The function computes the max-substring-sum from $[a_\ell, \ldots, a_r]$, so the desired max-substring sum is $S(1, n)$.

Let $T(n)$ be the running time on a sequence of size n. Show that $T(1) = 3$.

(a) If n is even, show that $T(n) = 2T(n/2) + 21 + \sum_{i=1}^{mid-1} 6 + \sum_{i=mid+2}^{n} 6 = 2T(n/2) + 6n + 9$.

(b) If n is odd, show that $T(n) = T((n + 1)/2) + T((n − 1)/2) + 6n + 9$.

(c) Tinker and compute $T(n)$ for $n = 1, 2, 3, 4, \ldots, 10$ to verify the table (you need to fill in the value for 10):

n	1	2	3	4	5	6	7	8	9	10
$T(n)$	3	27	57	87	123	159	195	231	273	?

(d) Use induction to prove that $T(2^n) = (6n + 12) \cdot 2^n − 9$.

(e) Prove that $3n(\log_2 n + 1) − 9 \leq T(n) \leq 12n(\log_2 n + 3) − 9$ and compare the bounds with your table in part (c).
    [Hint: Argue by monotonicity that $T(2^{\lfloor \log_2 n \rfloor}) \leq T(n) \leq T(2^{\lceil \log_2 n \rceil})$.]

Problem 9.73. Here is a very efficient `MaxSubstringSum` algorithm.

```
CumSum, CumMin, MaxSum ← 0;
for i = 1 to n do
    CumSum ← CumSum + a_i;
    CumMin ← min(CumSum, CumMin);
    MaxSum ← max(MaxSum, CumSum − CumMin);
return MaxSum;
```

The algorithm computes the cumulative sum CumSum from $i = 1$ to n. The max-substring-sum ending at i is CumSum(i) minus the minimum cumulative sum up to i, CumMin (CumMin starts at 0, the sum of the empty sequence). The algorithm maintains CumSum, CumMin and the maximum of (CumSum − CumMin).

Show that the running time is $T(n) = 5 + \sum_{i=1}^{n} 10$. Compute the sum and show $T(n) = 5 + 10n$.

10.4   Problems

Problem 10.1. Prove the quotient-remainder theorem. Given n, d. Let R be the possible non-negative remainders:
$$R = \{x | x = n - qd;\ q \in \mathbb{Z};\ q \le n/d\}.$$

(a) Is R empty? Show that R has a minimum element $r = n - qd$ with $0 \le r < d$. *[Hint: If $r \ge d$, then $r - d \in R$.]*

(b) [Uniqueness] Let $n = q_1 d + r_1 = q_2 d + r_2$, with $0 \le r_1, r_2 < d$. Prove $q_1 = q_2$. *[Hint: $(q_1 - q_2)d = r_2 - r_1$.]*

Problem 10.2 (Generating Primes: Sieve of Erasothenes).
The algorithm gives a method to output all the primes up to n.

1: List $1, \ldots, n$ and delete 1.
2: **while** numbers are on the list **do**
3:     Let x be the smallest.
4:     Output x as prime.
5:     Delete x and its multiples.

(a) Use the algorithm to output all primes up to 50.

(b) Prove that every number output is prime.

(c) Prove that every prime up to n is output.

Efficiently implementing the sieve is not trivial. Near-linear time is possible.

Problem 10.3. Kilam has 72 red and 90 blue crayons. He distributes *all* crayons into packets. A packet has crayons of one color, and all packets are the same size. Packets are as large as possible. How many packets are made?

Problem 10.4. What is the smallest positive multiple of 7 that has remainder 1 when divided by 2, 3, 4 and 5.

Problem 10.5. Kilam runs every 12th day and Liamsi every 8th. Both ran today. When do they next run together?

Problem 10.6. What are the possible remainders when a square n^2 is divided by 3? What about 4?

Problem 10.7. Prove that $2^{50}3^{100}5^{25} - 1$ is not prime. *[Hint: $1 + x + x^2 + \cdots + x^{n-1} = (x^n - 1)/(x - 1)$.]*

Problem 10.8. What natural numbers are relatively prime to 2, 3 and 6?

Problem 10.9. How many zeros are at the end of 1000!?

Problem 10.10. For any $m, n, x \in \mathbb{Z}$, prove that $\gcd(m, n) = \gcd(m, n - mx)$.

Problem 10.11. Use Euclid's algorithm and the remainders generated to solve these problems.

(a) Compute $\gcd(1200, 2250)$ and find $x, y \in \mathbb{Z}$ for which $\gcd(1200, 2250) = 1200x + 2250y$.

(b) Find x, y as in (a), but with the additional requirement that $x \le 0$ and $y \ge 0$.

Problem 10.12. Find $\gcd(356250895, 802137245)$. Write it as $356250895x + 802137245y$ for $x, y \in \mathbb{Z}$. Show work.

Problem 10.13. Let $d = \gcd(m, n)$, where $m, n > 0$. Bezout gives $d = mx + ny$ where $x, y \in \mathbb{Z}$. Prove or disprove:

(a) It is always possible to choose: (i) $x > 0$.   (ii) $x < 0$.

(b) It is possible to find another $x, y \in \mathbb{Z}$ for which $0 < mx + ny < d$.

(c) It is always possible to find $a, b \in \mathbb{Z}$ for which $ax + by = 1$.

Problem 10.14. How can you make \$6.27 using 5¢ and 8¢ stamps, using the maximum number of 8¢ stamps?

Problem 10.15. Prove.

(a) If a divides bc and $\gcd(a, b) = 1$ then a divides c.

(b) For any prime p, if $p | a_1 a_2 \cdots a_n$ then p divides one of the a_i.

(c) The gap between consecutive primes can be arbitrarily large. *[Hint: Is $n! + 2$ prime?]*

Problem 10.16. Prove, for $n, q \in \mathbb{N}$, $2^{qn} - 1$ is divisible by $2^n - 1$.

Problem 10.17. Prove $\gcd(2^a, 2^b - 1) = 1$ for $a, b \in \mathbb{N}$ by finding $x, y \in \mathbb{Z}$ for which $2^a \cdot x + (2^b - 1) \cdot y = 1$. *[Hints: If $a \le b$, the problem is easy (let $x = 2^{b-a}$). If $a > b$, what is $2^a + 2^{b-a}(2^b - 1)$? How is this helpful?]*

Problem 10.18. The Fibonacci numbers are: $F_1 = F_2 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for $n > 2$. Prove:

(a) $\gcd(F_n, F_{n+1}) = 1$ (F_n and F_{n+1} are coprime).   (c) $F_{m+n} = F_m F_{n+1} + F_{m-1} F_n$.

(b) $F_m | F_{mn}$ for $n \ge 1$.   (d) $\gcd(F_m, F_n) = F_{\gcd(m,n)}$ for $m, n \ge 1$.

Problem 10.19. Let $\ell > 0$ be an integer linear combination of m and n. Prove that ℓ is a multiple of $\gcd(m, n)$.

Problem 10.20. For $m, n, d > 0$, if d is a common divisor of m, n and $d = mx + ny$ for $x, y \in \mathbb{Z}$, prove $d = \gcd(m, n)$.

Problem 10.21. The GCD of three numbers m, n, k is their largest common divisor.
(a) Prove that $\gcd(m, n, k) = \gcd(\gcd(m, n), k)$.
(b) Prove a Bezout Theorem: $\gcd(m, n, k) = mx + ny + kz$, the smallest possible positive integer linear combination.

Problem 10.22. You may find Bezout's identity useful for answering these questions.
(a) Prove that consecutive integers n and $n + 1$ are relatively prime.
(b) For which positive n are the pair n and $n + 2$ relatively prime? Prove your answer.
(c) Let p be a prime and $n > 0$. When are n and $n + p$ coprime. Prove your answer. *[Hint: When is $\gcd(n, p) = 1$?]*
(d) For $k \in \mathbb{Z}$, prove that $2k + 1$ and $9k + 4$ are relatively prime.
(e) As a function of $k \in \mathbb{Z}$, compute $\gcd(2k - 1, 9k + 4)$.

Problem 10.23. Suppose x^2 is a multiple of y for integers $x, y > 1$. Prove that $\gcd(x, y) > 1$ in two ways:
(a) Use Bezout's identity.   (b) Use prime factorization.

Problem 10.24 (Chicken Nugget Theorem). McFOCS sells nuggets in boxes of 9 or 20. Find the largest quantity of nuggets you can't buy (no throwing nuggets away). Use these two steps. Let $m, n > 0$ with $\gcd(m, n) = 1$.
(a) Show that any $a \in \mathbb{Z}$ is an integer linear combination $a = mx + ny$, with $0 \le x < n$. Show that x, y are unique. Hence prove that $mn - m - n \ne ms + nt$ with non-negative integers s, t.
(b) For $k \ge 1$ prove by induction that there are non-negative integers s, t such that $mn - n - m + k = ms + nt$.

Problem 10.25. In each case, prove or disprove.
(a) $\mathbb{Z} \subseteq \{2x + 3y \mid x, y \in \mathbb{Z}\}$.   (b) $\mathbb{Z} \subseteq \{2x + 3y \mid x, y \in \mathbb{Z}, x > 0\}$.   (c) $\mathbb{Z} \subseteq \{4x + 6y \mid x, y \in \mathbb{Z}\}$.

Problem 10.26. In each case, prove or disprove whether infinitely many integer pairs $(x, y) \in \mathbb{Z}^2$ are a solution to:
(a) $3x + 4y = 5$.   (b) $12x + 18y = 4$.   (c) $12x + 18y = 6$.

Problem 10.27. Build an efficient algorithm to compute Bezout coefficients for $m, n > 0$. Bezout coefficients are any $x, y \in \mathbb{Z}$ for which $\gcd(m, n) = mx + ny$.
(a) Let $r_0 = n$ and $r_1 = m$. Euclid's gcd-algorithm starts by computing $r_2 = \text{rem}(n, m)$. Show that $r_2 = r_0 - \lfloor r_0 / r_1 \rfloor r_1$ and $\gcd(m, n) = \gcd(r_1, r_0) = \gcd(r_2, r_1)$.
(b) As Euclid's algorithm computes remainders $r_2, r_3, r_4, \ldots$. Let $q_i = \lfloor r_{i-2} / r_{i-1} \rfloor$. Show that $r_i = r_{i-2} - q_i r_{i-1}$ and $\gcd(m, n) = \gcd(r_i, r_{i-1})$ for $i \ge 2$. (Induction)
(c) Give the sequence of remainders $r_0, r_1, r_2, r_3, \ldots$, when $m = 14$ and $n = 10$.
(d) Suppose the first remainder which is 0 is r_{k+1}. What is $\gcd(m, n)$?
(e) Compute Bezout coefficients x_i, y_i for each remainder r_i. That is express $r_i = x_i m + y_i n$.
　　(i) What are x_0, y_0 and x_1, y_1?
　　(ii) For $i \ge 2$, show that $x_i = x_{i-2} - q_i x_{i-1}$ and $y_i = y_{i-2} - q_i y_{i-1}$, where $q_i = \lfloor r_{i-2} / r_{i-1} \rfloor$.
　　(iii) For $m = 14, n = 10$ compute the Bezout coefficients $x_0, x_1, \ldots$ and $y_0, y_1, \ldots$ and verify $r_i = mx_i + ny_i$.
　　(iv) Program an efficient algorithm that, given m, n, computes $\gcd(m, n)$ and Bezout coefficients x, y. (Your need to use r_i, x_i, y_i.) Compute the GCD and Bezout coefficients for $m = 49, 332, 470$ and $n = 172, 535, 181$.
This algorithm that also computes Bezout coefficients is called the extended Euclid Algorithm.

Problem 10.28. The Extended Euclid Algorithm (Problem 10.27) gives remainders $r_0, r_1, r_2, \ldots$. Prove $r_i \le r_{i-2}/2$ for $i > 2$. *[Hints: For $i > 2$, show $r_{i-1} \le r_{i-2}$, and consider $r_{i-1} \le r_{i-2}/2$ and $r_{i-1} > r_{i-2}/2$ separately.]*
(If you are so inclined, use this fact to prove that the runtime of Euclid's algorithm is in $O(\log_2 m + \log_2 n)$.)

Problem 10.29. Solve each measuring problem, or explain why it can't be done. (You have unlimited water.)
(a) Using 6 and 15 gallon jugs, measure (i) 3 gallons (ii) 4 gallons (iii) 5 gallons.
(b) Using 5 and 11 gallon jugs, measure (i) 6 gallons (ii) 7 gallons.

Problem 10.30. Consider the Die-Hard problem with 3 and 6 gallon jugs, and an unlimited supply of water. Prove by induction that the amount of water in both jugs will always be a multiple of 3. Hence, you can't measure 4 gallons.

Problem 10.31. Find b/a where $a = 2 \cdot 11$ and $b = 2^3 \cdot 7 \cdot 11^3 * 13^2$.

Problem 10.32. Let $n = 2^{a_2} 3^{a_3} 5^{a_5} 7^{a_7} \cdots$ for integers $a_i \ge 0$. Give conditions on the a_i equivalent to n being:
(a) even   (b) odd   (c) prime   (d) a square   (e) a cube   (f) square-free (no square except 1 divides n).

Problem 10.33. For positive integers m and n, prove: (a) $m^2|n^2 \to m|n$.   (b) $10|m^2 \to 10|m$.

Problem 10.34. Find the smallest positive integer n such that $2n$ is a square and $3n$ is a cube.

Problem 10.35. Suppose the distinct primes $p_1, \ldots, p_k$ divide $n \in \mathbb{N}$. Prove that $\prod_{i=1}^{k} p_i \le n$.

Problem 10.36. Show that 2^a and $2^b - 1$ are relatively prime using their prime factorizations.

Problem 10.37. For $k \in \mathbb{N}$, show that $2^k - 1$ and $2^k + 1$ are relatively prime.

Problem 10.38. Prove by induction that $2^{2^n} - 1$ has at least n distinct primes as factors, for $n \ge 1$.

Problem 10.39. Prove that $\gcd((a^p - 1)/(a - 1), a - 1) = \gcd(p, a - 1)$. What happens when p is prime? *[Hint:* $a^p - 1 = (a - 1)(1 + a + a^2 + \cdots + a^{p-1})$ *and* $a^k = (1 + a - 1)^k = 1 + \alpha a$ *(what is α?).]*

Problem 10.40. Let $n = \prod_{p_i} p_i^{a_i}$. Prove: the number of divisors of n is $\tau(n) = \prod_{p_i}(1 + a_i)$.

Problem 10.41. When does a positive integer n have an odd number of positive divisors?

Problem 10.42. If m and n are coprime and mn is a square, prove that both m and n are squares.

Problem 10.43. Use the Fundamental Theorem of Arithmetic to prove that for every $n \in \mathbb{N}$, if $\sqrt{n} \notin \mathbb{N}$ then $\sqrt{n}$ is irrational. (There is no irreducible fraction whose square is an integer.)

Problem 10.44 (Least Common Multiple (LCM)). The least common multiple $\operatorname{lcm}(m, n)$ is the smallest positive integer that is divisible by both m and n. Assume $m, n > 0$.
 (a) Compute the LCM for the pairs: $(2, 3)$; $(3, 5)$; $(6, 8)$.
 (b) Compute: (i) $\gcd(12, 16)$,   (ii) $\operatorname{lcm}(12, 16)$,   (iii) $\gcd(12, 16) \times \operatorname{lcm}(12, 16)$,   (iv) 12×16.
 (c) Prove the $\operatorname{lcm}(m, n) \cdot \gcd(m, n) = mn$.
     (i) Let $m = k \cdot \gcd(m, n)$ and $n = k' \cdot \gcd(m, n)$. Prove $\operatorname{lcm}(m, n) \le kk' \gcd(m, n)$.
     (ii) Prove $mn|\operatorname{lcm}(m, n)\gcd(m, n)$, hence $\operatorname{lcm}(m, n)\gcd(m, n) \ge mn$. *[Hint: Bezout.]*
     (iii) Use (i) and (ii) to prove $\operatorname{lcm}(m, n) = kk' \gcd(m, n)$ and $\operatorname{lcm}(m, n) \cdot \gcd(m, n) = mn$.

Problem 10.45. Let $n = \prod_{p_i} p_i^{a_i}$ and $m = \prod_{p_i} p_i^{b_i}$. Show:
 (a) $\gcd(m, n) = \prod_{p_i} p_i^{\min(a_i, b_i)}$ and $\operatorname{lcm}(m, n) = \prod_{p_i} p_i^{\max(a_i, b_i)}$.
 (b) Compute 72×108 and $\gcd(72, 108) \times \operatorname{lcm}(72, 108)$. Show that $mn = \gcd(m, n)\operatorname{lcm}(m, n)$ for $m, n > 0$.
(Euclid's method is more efficient as an algorithm, but (a) gives a "formula" for GCD which is useful in derivations.)

Problem 10.46. Prove or disprove.
 (a) $\gcd(m^k, n^k) = \gcd(m, n)^k$.   (c) $\gcd(m, n) = 1$ AND $\gcd(n, k) = 1 \to \gcd(m, k) = 1$.
 (b) $m^k \equiv n^k \to m \equiv n \pmod{d}$.   (d) $\gcd(m, n) \ne 1$ AND $\gcd(n, k) \ne 1 \to \gcd(m, k) \ne 1$.

Problem 10.47. Generalize GCD-fact (v) on page 132. Prove $xk \equiv yk \pmod{d} \to x \equiv y \pmod{d/\gcd(k, d)}$.

Problem 10.48. Prove these facts. Part (a) is called transitivity
 (a) $a \equiv b \pmod{d}$ and $b \equiv c \pmod{d} \to a \equiv c \pmod{d}$.   (b) $a \equiv b \pmod{d} \to \gcd(a, d) = \gcd(b, d)$.

Problem 10.49. Use modular arithmetic to solve these problems.
 (a) Compute the remainder when: (i) 2200^{2200} is divided by 3   (ii) 2014^{2014} is divided by 5.
 (b) What is the last digit of: (i) $3^{2016} + 4^{2016} + 7^{2016}$ (ii) $3^{1000} \times 5^{2000} + 7^{3000} \times 9^{4000}$ (iii) $2^{70} + 3^{70}$?
 (c) Prove that $2^{70} + 3^{70}$ is divisible by 13.
 (d) What is the last digit of 102^{1211}. What is the second last digit?
 (e) Prove that $102^{1211} - 3^{1211}$ is divisible by 99.
 (f) A number x after multiplying by 7 and adding 5 has a remainder 2 when divided by 11. What is $\operatorname{rem}(x, 11)$?
 (g) What is the remainder when (i) $5^n + 2 \cdot 11^n$ is divided by 3?   (ii) $4^{2n+1} + 5^{2n+1} + 6^{2n+1}$ is divided by 15?
 (h) Prove that every $n \ge 1$ is congruent to the sum of its digits modulo 9. For example, $952 \equiv 16 \pmod{9}$.
 (i) It's now 3pm. Where is the hour hand after: (i) 233 hours   (ii) 14×233 hours   (iii) 233^{233} hours.

Problem 10.50. Ayfos counts from 1 to n using her five left-fingers. Label her fingers T, F, M, R, L (thumb, fore, middle, ring, little). She starts by calling T one, then F two, M three, R four, L five. She then retraces calling R six, M seven, F eight, T nine. Then F ten, and so on. What finger will Ayfos be on when she reaches (a) 1,000   (b) 10^{2015}?

Problem 10.51. Prove that $3|n \leftrightarrow 3|$sum of n's digits. Is this true for 9? *[Hint: Show $10^k \equiv 1 \pmod 3$ for $k \geq 1$.]*

Problem 10.52. Prove there is no square in the sequence $11, 111, 1111, 11111, \ldots$. *[Hint: $x^2 \equiv ?? \pmod 4$.]*

Problem 10.53. For a prime p, prove: $x^2 \equiv y^2 \leftrightarrow x \equiv y$ or $x \equiv -y \pmod p$. What if p is not prime?

Problem 10.54. For any prime p and $a \in \mathbb{N}$, prove that $a^{p^j} \equiv a \pmod p$ for $j \geq 1$. (Use Fermat's Little Theorem.)

Problem 10.55. Use Fermat's Little Theorem (or explain why you can't) to help calculate these remainders.
  (a) $\text{rem}(3^{2015}, 7)$ (b) $\text{rem}(2^{2015}, 23)$ (c) $\text{rem}(2^{2015}, 13)$ (d) $\text{rem}(7^{81}, 15)$.

Problem 10.56. Prove: $(n-1)^2 | n^{n-1} - 1$. *[Hint: $n^k = (n-1+1)^k$; Binomial Theorem.]*

Problem 10.57. Compute these modular inverses, or explain why you can't.
  (a) $6^{-1} \pmod 7$ (c) $5^{-1} \pmod{12}$ (e) $1265^{-1} \pmod{88179}$
  (b) $6^{-1} \pmod 8$ (d) $12^{-1} \pmod 5$ (f) $31870410^{-1} \pmod{58642669}$

Problem 10.58. Find all solutions for x in each case. If there aren't any, explain why.
  (a) $1 \equiv (x \times -17) \pmod 4$ (b) $x \equiv -17 \pmod 4$ (c) $1 \equiv (x \times -12) \pmod 4$ (d) $x \equiv -12 \pmod 4$
  (e) $84x - 38 \equiv 79 \pmod{15}$ (f) $7x \equiv 12 \pmod{13}$ (g) $341x \equiv 2941 \pmod 9$ (h) $20x \equiv 23 \pmod{14}$
  (i) $4x \equiv 5 \pmod 6$ (j) $6x \equiv 3 \pmod 9$ (k) $x^2 \equiv 2 \pmod 4$ (l) $x^2 \equiv 2 \pmod 7$

Problem 10.59. For prime p, show that $p | \binom{p}{i}$ for $0 < i < p$. ($\binom{p}{i} = p!/i!(p-i)!$ is an integer, see Problem 5.45.)

Problem 10.60. For prime p and $x, y \in \mathbb{Z}$, show $(x+y)^p \equiv x^p + y^p \pmod p$. (Binomial Theorem; Problem 10.59)

Problem 10.61. Use Problem 10.60 to show that, for a prime p, if $k^p \equiv k \pmod p$, then $(k+1)^p \equiv k+1 \pmod p$. Hence, prove Fermat's Little Theorem by induction.

Problem 10.62. Prove that $b_n = 1^1 + 2^2 + \cdots + n^n$ has a periodic last digit with period 100, $b_n \equiv b_{n+100} \pmod{10}$.

Problem 10.63. Prove there are infinitely many primes of the form $3n + 2$ for $n \geq 1$.
  (a) Suppose $x_i \equiv 1 \pmod 3$ for $i = 1, \ldots, k$. Prove $x_1 x_2 \cdots x_k \equiv 1 \pmod 3$.
  (b) Let $p_i = 3n_i + 2$ for $i = 1, \ldots, k$ and $n_i \geq 1$. Let $N = 3p_1 \cdots p_k + 2$. Prove that N is odd and $N \equiv 2 \pmod 3$.
  (c) Prove there is a prime factor q of N of the form $q = 3n + 2$ for $n \geq 1$. *[Hint: Part (a).]*
  (d) Prove by contradiction that there are infinitely many primes of the form $3n + 2$ for $n \geq 1$.

Problem 10.64. Use the ideas in Problem 10.63 to prove that there are infinitely many primes of the form $4n - 1$. *[Hint: For primes $p_1, \ldots, p_k$ show that $N = 4p_1 p_2 \cdots p_k - 1$ cannot have all its prime factors of the form $4p + 1$.]*

Problem 10.65 (Chineese Remainder Theorem). If the remainders of x modulo pairwise relatively prime divisors $d_1, d_2, \ldots, d_k$ are known, then x modulo the product $d_1 d_2 \cdots d_k$ is unique. Do these examples.
  (a) Find x, where $x \equiv 2 \pmod 5$ and $x \equiv 3 \pmod 7$. Give two solutions x_1, x_2 and their remainders modulo 35.
  (b) If x_1 and x_2 both satisfy the requirements in (a), prove that $x_1 \equiv x_2 \pmod{35}$.
  (c) $x \equiv 4 \pmod 8$ and $x \equiv 1 \pmod{15}$. What is $\text{rem}(x, 120)$?

Problem 10.66. Let $d_1, d_2, \ldots, d_k$ be pairwise relatively prime, that is $\gcd(d_i, d_j) = 1$. Suppose x has remainder r_i when divided by d_i, $x \equiv r_i \pmod{d_i}$. Prove the Chineese Remainder Theorem (Problem 10.65) using these steps.
  (a) Suppose $d_1 | n$, $d_2 | n$. Then, $d_1 d_2 | n$.
  (b) Suppose that $d_i | n$ for $i = 1, \ldots, k$. Then, $d_1 d_2 \cdots d_k | n$. (Induction)
  (c) Suppose x_1 and x_2 are two solutions for x. Prove that $d_i | x_1 - x_2$ for $i = 1, \ldots, k$.
  (d) For x_1, x_2 as in (c), show $x_1 \equiv x_2 \pmod{d_1 d_2 \cdots d_k}$. That is, x modulo the product of divisors $d_1 \cdots d_k$ is uniquiely determined by its remainders modulo each individual divisor.

Problem 10.67 (Euler's Totient Function). Define $\phi(n)$, the number of positive integers up to n that are coprime to n, $\phi(n) = \sum_{d=1}^{n} [\![\gcd(n, d) = 1]\!]$. (The indicator function $[\![\cdot]\!]$ is 1 if its argument is true and 0 otherwise.)
  (a) Plot $\phi(n)$ versus n for $n = 1, \ldots, 20$. ($\phi(n)$ is a very erratic function.)
  (b) What is $\phi(p)$ for a prime p. Show that $\phi(p^k) = p^k(1 - 1/p)$.
  (c) Show that if $\gcd(m, n) = 1$ then $\phi(mn) = \phi(m)\phi(n)$.
  (d) Show that $\phi(n) = n \prod_{p|n}(1 - 1/p)$. (The product is over primes which divide n.)
  (e) (Due to Gauss) Compute $\sum_{d|n} \phi(d)$ for $n = 1, \ldots, 20$. Make a conjecture and prove it.
  (f) Prove Euler's Extension of Fermat's Little Theorem: If $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod n$.

Problem 10.68. Show: if $2^n - 1$ is prime, then n is prime. *[Hint: $1 + 2^x + 2^{2x} + \cdots + 2^{x(y-1)} = ?$]*
(Primes of the form $2^p - 1$ are Mersenne primes. We don't know if there are infinitely many Mersenne primes.)

Problem 10.69. Show: if $2^p - 1$ is prime then $2^{p-1}(2^p - 1)$ is perfect. *[Hint: The divisors are 2^i and $2^i(2^p - 1)$.]*

Problem 10.70. Show, using the following steps, that every even perfect number has the form $2^{p-1}(2^p - 1)$ with $2^p - 1$ prime. Define $\sigma(n)$ to be the sum of the divisors of n that include n.
  (a) Show: n is perfect if and only if $\sigma(n) = 2n$.
  (b) Suppose $\gcd(m, n) = 1$. Show: $\sigma(mn) = \sigma(m)\sigma(n)$.
  (c) Suppose x is even. Show: for some $k \geq 2$, $x = 2^{k-1}y$, where y is odd.
  (d) What is $\gcd(2^{k-1}, y)$ when y is odd?
  (e) Now, suppose x is an even perfect number.
     (i) Show: $2x = \sigma(x) = \sigma(y)(2^k - 1)$, and hence that $\sigma(y) = 2^k y/(2^k - 1)$.
     (ii) Show: $2^k - 1 | y$ (use Euclid's lemma), hence that $y = m(2^k - 1)$.
     (iii) Show: $\sigma(y) = y + 1$ if and only if y is prime.
     (iv) Show: if $y = m(2^k - 1)$ and $\sigma(y) = 2^k y/(2^k - 1)$, then $m = 1$ and $2^k - 1$ is prime.
     (v) Conclude: $x = 2^{k-1}(2^k - 1)$ where $2^k - 1$ is prime.
(Are there infinitely many even perfect numbers? Is there an odd perfect number? We don't know.)

Problem 10.71. Alice sends the location of Charlie's party to Bob. The message is: *MyHouse*
  (a) Convert the message to binary using the ASCII code and evaluate the binary number to get an integer message M.
  (b) How can you ensure that your message is a prime number, while allowing Bob to understand the message?

Problem 10.72. Let $p = 14251$ and $q = 14519$ be two primes. Find choices for e and d in the RSA algorithm and compute the encryption M_* of the message $M = 19$. Show that your private key d decrypts M_* correctly.

Problem 10.73 (One Time Pad). Alice and Bob have shared a private key $k = k_1 k_2 \cdots k_8$ (8 bits). The message $M = m_1 m_2 \cdots m_8$ (same length as k). Alice sends the message $M_* = m_{1*} m_{2*} \cdots m_{8*}$ where each bit m_{i*} is the addition modulo 2 of the corresponding bits in k and M, $m_{i*} = m_i + k_i \pmod 2$. This is the XOR one time pad.
  (a) Set $k = 11010011$. (i) $M = 10110101$, what is M_*? (ii) $M* = 11100111$, what was M?
  (b) If k is random, justify the statement "There is no way to recover M from M_*."
  (c) (Plain text attack) Alice uses the same key k to encode $M_1 = 10111100$ and M_2. The encoded messages are $M_{1*} = 11111111$ and $M_{2*} = 00001111$. What is M_2?
  (d) (Prior attack) Alice uses the same key k to encode M_1 and M_2. The encoded messages are $M_{1*} = 11111111$ and $M_{2*} = 00001111$. Can we discern anything about M_1, M_2. As a hint, here is a visual example of this attack.
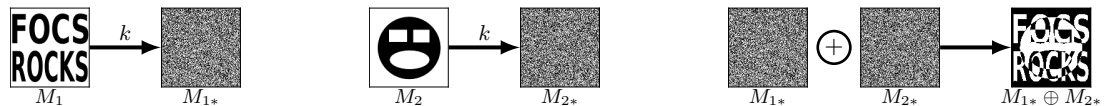
Problem 10.74 (Pythagorean Triples). Pythagoras' Theorem for the sides of a right triangle is $x^2 + y^2 = z^2$. Find all possible right triangles with integer sides. Such sides are called Pythagorean triples.
  (a) Show that $(3, 4, 5)$, $(6, 8, 10)$ and $(5, 12, 13)$ are Pythagorean triples.
  (b) In a primitive Pythagorean triple, $\gcd(x, y, z) = 1$. Which triples in (a) are primitive?
  (c) [Euclid's formula] For $m > n$, show that $(m^2 - n^2, 2mn, m^2 + n^2)$ is a Pythagorean triple.
  (d) If m, n are not both odd and $\gcd(m, n) = 1$, show that Euclid's formula generates a primitive Pythagorean triple.
  (e) [Harder] Show: every primitive Pythagorean triple can be generated by Euclid's formula.
  (f) Is there an infinite sequence $a_1, a_2, \ldots$ where $a_1^2 + a_2^2 + \cdots + a_n^2$ is a square for $n \geq 1$? *[Hint: $3, 4, \ldots$]*

Problem 10.75 (Fermat's Last Theorem). Prove $x^4 + y^4 \neq z^4$ for $x, y, z \in \mathbb{Z}$. *[Hint: Problem 6.50(p).]*

Problem 10.76. Let $\nu_p(x)$ be the largest power of prime p that divides x, so $x = \prod_{\text{primes } p} p^{\nu_p(x)}$.
  (a) Show that $\nu_p(xy) = \nu_p(x) + \nu_p(y)$ and, assuming y divides x, $\nu_p(x/y) = \nu_p(x) - \nu_p(y)$.
  (b) Show that $\nu_p(n!) = \sum_{i=1}^{\infty} \lfloor n/p^i \rfloor = \lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \lfloor n/p^3 \rfloor + \cdots$.
  (c) In base-p, let $n = a_0 + a_1 p + a_2 p^2 + \cdots + a_k p^k$. Show that $\nu_p(n!) = (n - \sum_{i=0}^{k} a_k)/(p - 1)$.
  (d) Prove that $n!$ is not divisible by 2^n.
  (e) Prove that $n!$ is divisible by 2^{n-1} if and only if $n = 2^k$.

Problem 10.77. Prove that if $2n/3 < p \leq n$, then $\nu_p(n!) = 1$ and $\nu_p((2n)!) = 2$. Show $\nu_p\left(\binom{2n}{n}\right) = 0$, and hence p does not divide $\binom{2n}{n}$. *[Hint: Compute $\lfloor n/p^i \rfloor$.]*

Problem 10.78. Show: $\nu_p\left(\binom{2n}{n}\right) = \nu_p((2n)!) - 2\nu_p(n!) = \sum_{i=1}^{\lfloor \log_p(2n) \rfloor} \lfloor 2n/p^i \rfloor - 2\lfloor n/p^i \rfloor \leq \log_p(2n)$.

Problem 10.79. Prove that $\binom{2n}{n} \geq 4^n/(2n+1)$. *[Hint: $(1+1)^{2n} = \sum_{i=0}^{2n} \binom{2n}{i}$.]*

Problem 10.80. Prove that $\prod_{\text{primes } p \leq n} p \leq 4^n$. The variable p denotes a prime. Follow these steps.

(a) Show $\displaystyle\prod_{p \leq 2m+1} p = \prod_{p \leq m+1} p \times \prod_{m+2 \leq p}^{p \leq 2m+1} p$ and $\displaystyle\prod_{m+2 \leq p}^{p \leq 2m+1} p \leq \binom{2m+1}{m}$. *[Hint: If $p \in [m+2, 2m+1]$ then p divides $\binom{2m+1}{m}$.]*

(b) Prove the claim using strong induction. *[Hint: Use the binomial expansion of $(1+1)^{2m+1}$ to show $\binom{2m+1}{m} \leq 2^{2m}$.]*

Problem 10.81. Use Problems 10.76–10.80 to prove the rhyme first proved by Chebyshev:

> *Chebyshev said it and I say it again,*
> *There is always a prime between n and $2n$*   *–Joseph Bertrand's Postulate*

Assume for some n there is no prime p with $n < p \leq 2n$. Follow 19-year-old Paul Erdős' approach (Erdős' first paper).

(a) Show that at most $\sqrt{2n}$ prime factors of $\binom{2n}{n}$ are at most $\sqrt{2n}$, and each of these factors contributes a factor at most $2n$ in the prime factorization of $\binom{2n}{n}$.

(b) Show that for $p \geq \sqrt{2n}$, $\nu_p(\binom{2n}{n}) \leq 1$.

(c) Show that $\binom{2n}{n} \leq (2n)^{\sqrt{2n}} \times \prod_{\sqrt{2n} \leq p \leq 2n/3} p \leq (2n)^{\sqrt{2n}} \times \prod_{p \leq 2n/3} p \leq (2n)^{\sqrt{2n}} 4^{2n/3}$.

(d) Show that $(2n)^{\sqrt{2n}} 4^{2n/3} \geq 4^n/(2n+1)$.

(e) Show that this is impossible if $n \geq 468$, and prove Bertrand's postulate.

Problem 10.82 (Euler Product). Use Euler's method to show that the product $\prod_{\text{primes } p}(1 - 1/p^2) = 6/\pi^2$.

(a) Compute a formula for $1 + 1/p^2 + 1/p^4 + 1/p^6 + \cdots + 1/p^{2i} + \cdots = \sum_{i=0}^{\infty} 1/p^{2i}$.

(b) What integers x_i appear in the sum $\sum_i 1/x_i$ obtained by expanding out each product?

(i) $\left(1 + \dfrac{1}{3} + \dfrac{1}{3^2} + \dfrac{1}{3^3} + \cdots\right)\left(1 + \dfrac{1}{7} + \dfrac{1}{7^2} + \dfrac{1}{7^3} + \cdots\right)$ (ii) $\left(1 + \dfrac{1}{3^2} + \dfrac{1}{3^4} + \cdots + \dfrac{1}{3^{2i}} + \cdots\right)\left(1 + \dfrac{1}{7^2} + \dfrac{1}{7^4} + \cdots + \dfrac{1}{7^{2i}} + \cdots\right)$

(c) Use Problem 9.65 to compute the product $\prod_{\text{primes } p}(1 - 1/p^2)$ by showing

$$\prod_{\text{primes } p} \frac{1}{1 - 1/p^2} = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \frac{1}{5^2} + \frac{1}{6^2} + \cdots . \tag{10.2}$$

Problem 10.83. Here are a few famous open problems from number theory. The internet sprawls with more.

(a) The Euler-Mascheroni constant is $\gamma = \lim_{n \to \infty}(H_n - \ln n) \approx 0.5772156649$. Is γ rational or irrational?

(b) Is every even number greater than 2 a sum of two primes? (Goldbach's conjecture)

(c) Are there odd perfect numbers? Are there infinitely many even perfect numbers (or, Mersenne Primes)?

(d) Are there infinitely many twin primes, primes p where $p + 2$ is also prime?

(e) (Collatz or $3n + 1$ conjecture). For a number n, define $f(n) = n/2$ if n is even and $3n + 1$ otherwise. Does the sequence $n, f(n), f^2(n), \ldots$ eventually become 1 for every $n \in \mathbb{N}$?

(f) A prime q is called a Sophie-Germain prime if $p = 2q + 1$ is prime. The prime p is called safe. Can you find a Sophie-Germain prime larger than 100? We don't know if there are infinitely many Sophie-Germain primes.

(g) What is the exact value (in terms of known constants) of $\zeta(3) = 1 + 1/2^3 + 1/3^3 + 1/4^3 + 1/5^3 + \cdots$.

(h) **(Riemann Hypothesis)** Equation (10.2) relating primes and integers generalizes to any complex power s,

$$\prod_{\text{primes } p} \frac{1}{1 - 1/p^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \frac{1}{6^s} + \cdots = \zeta(s). \tag{10.3}$$

The summation is absolutely convergent for $Re(s) > 1$ and $\zeta(s)$ has a unique analytic continuation to the complex plane. The Riemann Hypothesis is that all zeros of $\zeta(s)$ with $0 < Re(s) < 1$ have $Re(s) = 1/2$. That's the burning question in number theory with implications to the distribution of prime numbers and more.

11.7 Problems

Problem 11.1. Draw all graphs that have the vertex set $V = \{a, b, c\}$.

Problem 11.2. Draw pictures of K_1, K_2, K_3, K_4, K_5, K_6 and $K_{4,4}$. (Use filled in circles for vertices.)

Problem 11.3. Give the degree sequences of K_{n+1}, $K_{n,n}$, L_n, C_n, S_{n+1} and W_{n+1}.

Problem 11.4. Prove: if a graph has degree sequence $[5, 1, 1, 1, 1, 1]$, then it must be S_5.

Problem 11.5. A graph is regular if every vertex has the same degree. Which of these graphs are regular:
   (a) K_6;   (b) $K_{4,5}$ (c) $K_{5,5}$ (d) L_6 (e) S_6 (f) W_4 (g) W_5?

Problem 11.6. Give a graph (no loops or parallel edges) satisfying the constraints or explain why it doesn't exist.
   (a) The graph has 5 vertices each of degree 3.   (c) The graph has 4 vertices of degrees 1,2,3,4.
   (b) The graph has 4 edges and vertices of degrees 1,2,3,4.   (d) The graph has 6 vertices of degrees 1,2,3,4,5,5.

Problem 11.7. For graphs G and H: (i) Give adjacency lists and adjacency matrices. (ii) Give degree distributions. (iii) Determine if G and H are isomorphic.

   (a) G: H: (b) G: H:

Problem 11.8. Is there a friend network with 7 friends, each of who know 3 friends?

Problem 11.9. Among 7 people, 6 have exactly 2 friends. How many friends can the 7th person have?

Problem 11.10. Give simple graphs with these degree sequences, or explain why you can't. Recall $2|E| = \sum_{i=1}^{n} \delta_i$.
   (a) $[5, 3, 3, 2, 1]$ (b) $[3, 2, 1, 1, 1]$ (c) $[3, 3, 2, 1]$ (d) $[3, 3, 3, 3, 3]$ (e) $[3, 3, 3, 3, 3, 3]$ (f) $[3, 3, 2, 2, 2]$
   (g) $[4, 4, 4, 4, 4]$ (h) $[4, 4, 3, 2, 1]$ (i) $[4, 3, 3, 2, 2]$ (j) $[3, 3, 3, 2, 2]$ (k) $[3, 3, 3, 3, 2]$ (l) $[5, 3, 2, 2, 2]$

Problem 11.11. In a graph only the two vertices u, v have odd degree. Prove there is a path from u to v.

Problem 11.12. All vertex-degrees in a 9-vertex graph are 5 or 6. Prove that at least 5 vertices have degree 6 OR at least 6 vertices have degree 5.

Problem 11.13. FOCSbook has n people and each person has $n - 2$ friends. Find all n where it is possible?

Problem 11.14. Compute the number of edges in the following graphs: (a) K_n (b) $K_{n,\ell}$ (c) W_n

Problem 11.15. Model Manhattan's road network as an (n, ℓ) rectangular grid of vertices. We show a $(4, 6)$-grid.
   (a) How many vertices and edges are in the $(4, 6)$-grid on the right?
   (b) Compute the number of vertices and edges in the (n, ℓ)-grid.
   (c) Compute the degree distribution for the (n, ℓ)-grid.
   (d) How long is a shortest path from the vertex at (x, y) to the vertex at (w, z)?
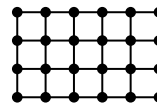
Problem 11.16. A graph is r-regular if every vertex has the same degree r. Show:
   (a) If r is even and $n > r$, there is an r-regular graph with n vertices. (Tinker!)
   (b) If r is odd and n is odd, there is no r-regular graph with n vertices.
   (c) If r is odd and $n > r$ is even, there is an r-regular graph with n vertices.
   (d) An r-regular graph with $4k$ vertices must have an even number of edges.

Problem 11.17. What is $|E|$ for a simple graph with degrees $[9, 5, 2, 2, 0]$. What about a multigraph?

Problem 11.18. A graph G has n vertices and m edges. Answer each of the following and prove your answer.
   (a) G is not connected. What is the maximum m?   (b) G is connected. What is the minimum m?

Problem 11.19. At a party with 10 people, in any group of four, someone knows the other three people. Prove that someone at the party knows everyone else at the party. *[Hint: Consider the person with maximum degree.]*

Problem 11.20. Baniaz and her partner organize a party with 4 other couples. People shake hands, but no one shakes hands with their partner. Baniaz asks each of the other nine people how many people they greeted, and receives 9 different answers. How many people did Baniaz greet and how many people did her partner greet?

Problem 11.21 (Complement Graph). For graph G, the complement $\overline{G}$ has the same vertices, but edges in $\overline{G}$ are the complement of edges in G: distinct vertices u and v are adjacent in $\overline{G}$ if and only if they are not adjacent in G. Give the complements of (a) The graph shown. (b) K_n. (c) $K_{n,m}$. (d) S_{n+1}.
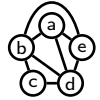
Problem 11.22. Answer the following questions about a graph and its complement defined in Problem 11.21.
  (a) If G is regular, prove that $\overline{G}$ is also regular. (In a regular graph, all vertices have the same degree.)
  (b) Give a connected graph G for which the complement $\overline{G}$ is: (i) Connected. (ii) Not conected.
  (c) Prove that either G or $\overline{G}$ must be connected.
  (d) Suppose G is a tree. Give necessary and sufficient conditions for $\overline{G}$ to be connected.
  (e) Give 4 and 5-vertex graphs which are isomorphic to their complement. Such graphs are self-complemetary. Show that there is no self-complementary graph with 3 or 6 vertices.
  (f) Prove that there is an n-vertex self-complementary graph if and only if $n = 4k$ or $n = 4k + 1$

Problem 11.23 (Friends Paradox). Don't despair because your friends have, on average, more friends than you do. This is typical in any social network. Let δ_i be vertex v_i's degree and define vertex v_i's friend-degree κ_i as the average degree of vertex v_i's friends. Let $\bar{\delta} = (\sum_{i=1}^{n} \delta_i)/n$ be the average of the vertex-degrees and $\bar{\kappa} = (\sum_{i=1}^{n} \kappa_i)/n$ be the average of the friend-degrees. You may assume every vertex has positive degree.
  (a) Compute $\bar{\delta}$ and $\bar{\kappa}$ for: K_3, $K_{2,3}$, S_5, L_4, W_5.
  (b) Let $N(i)$ be the neighborhood (friends) of v_i, and δ_i the degree of v_i. Justify the steps:

$$\bar{\kappa} \overset{(i)}{=} \frac{1}{n} \sum_{i=1}^{n} \frac{1}{\delta_i} \sum_{j \in N(i)} \delta_j \overset{(ii)}{=} \frac{1}{n} \sum_{i=1}^{n} \frac{1}{\delta_i} \sum_{j \in N(i)} (\delta_j - \delta_i + \delta_i) \overset{(iii)}{=} \bar{\delta} + \frac{1}{n} \sum_{i=1}^{n} \frac{1}{\delta_i} \sum_{j \in N(i)} (\delta_j - \delta_i).$$

  (c) Show that the edge (v_i, v_j) contributes $(\delta_i - \delta_j)(1/\delta_j - 1/\delta_i)$ to the double sum in the last term.
  (d) Prove that $\bar{\kappa} \geq \bar{\delta}$ and characterize when $\bar{\kappa} = \bar{\delta}$. (On average, your friends have more friends than you do.)

Problem 11.24 (Graphical Sequence). A sequence $\delta_1, \delta_2, \ldots, \delta_n$ is graphical if there is a simple graph whose n vertices $v_1, v_2, \ldots, v_n$ have these degrees, $\delta_1, \delta_2, \ldots, \delta_n$.
  (a) Determine if these degree sequences are graphical: (i) [4,4,2,1,1]   (ii) [4,4,2,2,1,1]
  (b) Suppose $\delta_1 \geq \delta_2 \geq \cdots \geq \delta_n \geq 0$ is graphical. Prove there is a graph having these degrees with its highest-degree vertex v_1 of degree δ_1 adjacent to the δ_1 next highest-degree vertices $v_2, v_3, \ldots, v_{\delta_1+1}$. *[Hint: If v_1 is not adjacent to all these vertices, "rewire" two edges so that v_1 becomes adjacent to one more of these vertices.]*
  (c) **[Havel-Hakimi]** Prove: $\delta_1 \geq \delta_2 \geq \cdots \geq \delta_n \geq 0$ is graphical if and only if $\delta_2 - 1, \delta_3 - 1, \ldots, \delta_{\delta_1+1} - 1, \delta_{\delta_1+2}, \ldots, \delta_n$ is graphical. The second degree sequence corresponds to removing the highest-degree vertex (which is linked to the next highest-degree vertices).
  (d) Are these sequences graphical: (i) [6,5,5,5,4,4,2,1]   (ii) [8,7,6,6,5,3,2,2,2,1]

Problem 11.25 (Connected Components). For a graph G and a vertex v, the component containing v, $C(v)$, is the set of vertices which are connected to v (v is in $C(v)$).
  (a) For the graph G on the right, give vertex and edge sets, (V, E).
  (b) What are $C(b)$, $C(e)$, $C(f)$, $C(i)$? Explain why $C(a) = C(c)$ (same component).
  (c) How many distinct components are in G and what are they?
  (d) How many components are in a connected graph?
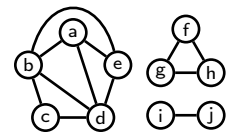
Problem 11.26. How many edges must be added to make the graph in Problem 11.25 connected? Prove: a graph with n vertices and e edges has at least $n - e$ components. Use induction on e.

Problem 11.27. A graph is 2-regular. Prove that each connected component is a cycle.

Problem 11.28. Every vertex degree in a graph is at least 2. Prove that there is at least one cycle.

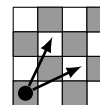**Problem 11.29.** Conjecture: A graph with all vertices of positive degree must be connected.
  (a) You add a vertex of positive degree to a connected n-vertex graph. Is the resulting $(n+1)$-vertex graph connected?
  (b) Using part (a), here is a sketch of a proof by induction that a graph with positive degrees is connected.

  > The base case, $n = 2$, is easy to check. Assume any n vertex graph with positive degrees is connected.
  > Add a vertex of positive degree to get $n + 1$ vertices. By (a), this $n + 1$ vertex graph is connected.

  Give the formal proof, or disprove the claim and explain what's wrong with the induction.

Problem 11.30. The diameter of a graph is the distance between the two vertices that are furtherest apart. Compute the diameters of: (a) K_n (b) $K_{n,m}$ (c) C_n (d) L_n (e) W_n.

Problem 11.31. A standard chess-knight's move is a $(1,2)$-L, 1 squares in one direction and then 2 squares in an orthogonal direction. The knight starts at the bottom-left of a 4×4 chessboard.
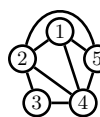 (a) How many moves are needed to reach each square. *[Hint: Start with 0 moves, then 1, then 2,...]*
  (b) Can the knight visit every square exactly once and return to the bottom left.

Problem 11.32. Prove the following facts of any graph $G = (V, E)$ with n vertices.
  (a) There are at least two vertices with the same degree (degree twins).
  (b) One can partition V into two sets so that every vertex in a set has at least half its neighbors in the other set.
  (c) If every vertex has degree at least $\delta \geq 2$, there is a cycle of length at least $\delta + 1$.
  (d) If every vertex has degree at least $n/2$, the graph is connected.
  (e) If the degrees of non-adjacent vertices sum to at least $n - 1$, the graph is connected.
  (f) If every subset S of at most $n/2$ vertices has an edge from inside S to outside, then G is connected.

Problem 11.33. Give the adjacency matrix A for the graph on the right.
  (a) For $k = 1, 2, 3$, compute matrices D_k whose (i, j) entry is the number length-k paths from i to j.
  (b) Compute A^k for $k = 1, 2, 3$ and compare with D_k.
  (c) For a general graph, prove by induction that $D_k = A^k$ for $k \geq 1$. (A^k counts length-k paths.)

Problem 11.34. In a weighted graph, the weighted degree of a vertex is the sum of edge-weights incident to the vertex. Prove that the sum of the weighted degrees equals twice the sum of the edge weights.

Problem 11.35 (Euler Paths). Trace each picture by placing a pencil on a vertex and drawing over each edge <u>once</u> without lifting the pencil. A path using each edge once is an Euler path. Vertices can be used multiple times.

(a)   (b)   (c)   (d)   (e)

If the path starts and ends at the same vertex, it is an Euler cycle. Do any of the graphs have both an Euler path and Euler cycle? Formulate conjectures about when a graph has an Euler path and when it has an Euler cycle.

Problem 11.36. For a connected graph G, prove the following claims.
  (a) G has an Euler cycle if and only if every vertex has even degree.
  (b) G has an Euler path (not a cycle) if and only if all vertices but two have even degree.
  (c) One can transform any graph G into a graph G' having an Euler cycle by adding at most one vertex and edges only from this new vertex to the other vertices. Similarly, one can get an Euler path.

Problem 11.37. For the graph shown, what is the minimum number of edges you must add so that the resulting graph has an Euler cycle (parallel edges allowed). What if parallel edges are not allowed?
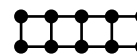
Problem 11.38. For which r, s does $K_{r,s}$ have an Euler cycle?

Problem 11.39 (Hypercube). The n-hypercube H_n has 2^n vertices, one for each n-bit string $b_1 \cdots b_n$, which is the label of the vertex. There is an edge between two vertices if and only if their labels differ in just one of the bits.
  (a) Give drawings of H_1, H_2 and H_3, and determine the number of edges in each graph.
  (b) How many edges are in H_n and what is the degree sequence? When is there an Euler path or cycle?
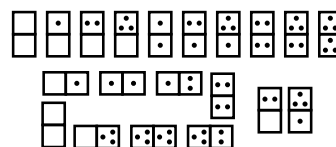
Problem 11.40 (Chineese Postman). A neighborhood G has 10 streets and 7 intersections. We show the time in minutes for a postman to walk along each street.
  (a) How quickly can a postman enter G at $@$, deliver mail along every street and exit at $@$?
  (b) Can the time be reduced if the postman enters and exits at another intersection, e.g. b?
  (c) Can the time be reduced if the postman enters and exits from different intersections?
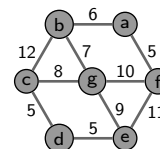
Problem 11.41. We show the 10 dominos using pairs of numbers in $\{0, 1, 2, 3\}$ (0 is blank). We placed some of the dominos in a ring so that touching dominos meet at the same number. The ring does not include all the 10 dominos.
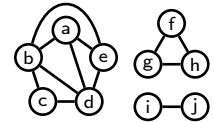 (a) Can you place all the dominos in a ring?
  (b) How many dominos are there for pairs of numbers in $\{0, \ldots, n\}$?
  (c) For which n can you place all the dominos in a ring? *[Hints: Make each number a vertex. Problem 11.35.]*

Problem 11.42 (Ramsey Numbers). Remarkably, a social network with 6 people must have a 3-clique or 3-war. No matter how random the network, there must be some structure. We can get more structure by increasing the size.
  (a) Show that any social network with 10 people has a 4-clique or a 3-war.
  (b) Show that any social network with 9 people has a 4-clique or a 3-war. *[Hints: Assume no 3-war and prove there is a 4-clique by contradiction. To get a contradiction, show that every vertex has 3 enemies and 5 friends.]*
  (c) Prove Ramsey's result that any amount of structure can be guaranteed. For integers $k, s > 0$ there is a smallest number $R(k, s)$ for which any graph with $R(k, s)$ vertices has a k-clique or an s-war. $R(3, 3) \le 6$ and $R(4, 3) \le 9$.
      (i) Prove that $R(k, s) = R(s, k)$ and $R(k, s) \le R(k - 1, s) + R(k, s - 1)$. Why does this prove Ramsey's result, that there is as much structure as you wish in large enough graphs.
      (ii) What is $R(k, 1)$? Prove by induction that $R(k, s) \le (k + s - 2)!/((k - 1)! \times (s - 1)!)$.

Aliens give us a year to compute Ramsey(5,5) or face extinction. We could marshal the world's best minds and fastest computers, and within a year we might have the value. If, instead, the demand was Ramsey(6,6), we should preemptively attack. – Paul Erdős

Problem 11.43 (Induced Subgraph). The subgraph induced by some of the vertices is obtained by removing all other vertices and also the edges to any of those removed vertices. For the graph on the right, what are the subgraphs induced by the vertices:
  (a) $\{a, b, c\}$ (b) $\{a, b, d\}$ (c) $\{a, b, e\}$ (d) $\{a, c, e\}$ (e) $\{a, g, i\}$

Problem 11.44. A subgraph is a subset of edges and all vertices at endpoints of those edges. Note the difference between general subgraphs and induced subgraphs which are a subset of vertices and all edges linking those vertices. For the graph shown, which of these are subgraphs and which are induced subgraphs?
  (a) K_3 (b) C_4 (c) L_4 (d) S_4 (e) S_5 (f)

Problem 11.45. The subgraph induced by removing a vertex is a "card". An n-vertex graph has n cards. We show the 4-card "deck" of a 4-vertex graph. What are the decks of: (a) K_n (b) $K_{n,m}$ (c) C_n (d) S_{n+1}?
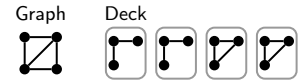
Problem 11.46. Determine the graph from its deck. (a)   (b)

Conjecture (Kelly and Ulam): A graph with at least three vertices is uniquely specified up to isomorphism by its deck.

Problem 11.47. Prove: If $|E| \ge |V|\delta/2$, then some induced subgraph has minimum degree at least $\delta/2$.

Problem 11.48. A cut-vertex in a connected graph is a vertex whose removal results in the remaining graph being disconnected. Identify all the cut vertices in the graph on the right.
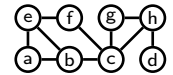
Problem 11.49. A graph has n vertices. The shortest path between two vertices u, v has length greater than $n/2$. Prove that one can disconnect u from v by removing a single other vertex. Such a vertex is called a (u, v)-cut-vertex.

Problem 11.50 (Menger's Theorem). Prove there is no (u, v)-cut-vertex (see Problem 11.49) if and only if at least two paths from u to v share no vertices other than u and v. Such paths are disjoint. (Menger showed that disconnecting u from v requires removal of at least k vertices if and only if there are k disjoint paths from u to v.)

Problem 11.51. Use Menger's Theorem to prove the result in Problem 11.48.

Problem 11.52. Similar to a cut-vertex, an edge e is a cut-edge in G if the removal of e disconnects G. Prove that e is a cut-edge if and only if e is not on any cycle of G.

Problem 11.53. A connected graph has no cycles. Prove that some vertex has degree-1. *[Hint: A longest path.]*

Problem 11.54. A tree has 17 vertices. How many edges does it have. If the maximum degree is 16, draw the tree.

Problem 11.55. Prove that a tree with n vertices and maximum degree Δ has at least Δ leaves.

Problem 11.56. A tree with n vertices has diameter 2. What is the tree (give a drawing)?

Problem 11.57. Give all non-isomophic 7-vertex trees with 3 or more degree-1 and 2 or more degree-3 vertices.

Problem 11.58. A graph G with n vertices and $n - 1$ edges is not a tree. Show that G has at least one connected component which is a tree and at least one connected component which is not a tree.

Problem 11.59. Label the edges of K_n with $1, 2 \ldots, \binom{n}{2}$. A monotonic path is one with labels increasing along the path. Prove that there is a monotonic path of length at least $n - 1$.

Problem 11.60 (Spanning Tree). Is the graph on the right a tree? If not, why not?

(a) Give two different trees using all vertices and a subset of the edges. Such trees are spanning trees. A spanning tree is a minimal subset of the edges which maintains connectivity.

(b) Prove: Any connected graph has a spanning tree. *[Hint: Remove an edge from a cycle; induction.]*

(c) Which graphs have exactly one spanning tree?
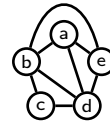
Problem 11.61 (BFS-tree). Let G be connected. Start at (say) vertex ⓐ, the level-0 vertex. Draw the edges to neighbors of ⓐ, the level-1 vertices which are distance 1 from ⓐ. Now process each level-1 vertex drawing the edges to all neighbors that have not already been linked to – these are level-2 vertices. Continue processing level-2, then level-3, etc. We illustrate the steps with G.

Building a BFS-tree for G
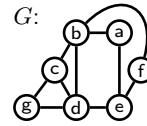
(a) Give different BFS-trees, with roots ⓐ and ⓔ.

(b) Show: when G is connected, the result is a tree with all vertices of G.

(c) Prove there are no edges of G between vertices at levels i and $(i+2)$ in the BFS-tree.

(d) Prove that the shortest path in G from the start vertex (in this case ⓐ) to any level-i vertex is i.

(e) True or False: the number of levels in the BFS-tree doesn't depend on which vertex is the root.

level-0
level-1
level-2
level-3
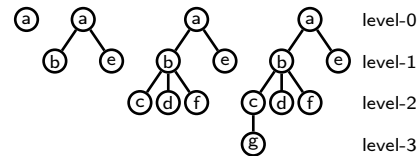
Problem 11.62. Recursively define rooted trees. Generate 3 rooted trees which are not rooted binary trees (RBTs). Give a recursive function to compute the height of a rooted tree.

Problem 11.63. Prove or disprove:

(a) A connected graph is a tree if and only if the average degree of its vertices is less than 2.

(b) Every graph with n vertices and $n-1$ edges is a tree.

(c) There is a tree with degrees $\delta_1 \geq \delta_2 \geq \cdots \geq \delta_n > 0$ if and only if $\sum_{i=1}^{n} \delta_i = 2n - 2$.

Problem 11.64. Give planar drawings of these graphs and verify Euler's formula. (a) ⬡ (b) ✶
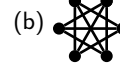
**Problem 11.65.** A graph G has degree sequence $[5, 4, 4, 3, 2, 2]$.

(a) How many edges does G have?   (b) Could G be planar? If yes, how many faces does G have. If not, why?

Problem 11.66. Prove that every subgraph of a planar graph is planar.

**Problem 11.67.** This problem builds on Exercise 11.7. Prove the following.

(a) If G and $\overline{G}$ are planar then $2 \leq |V| \leq 10$. *[Hint: Exercise 11.7(h).]*

(b) For a planar graph with C components, $F + V - E = 1 + C$. (Euler's invariant for disconnected graphs.)

(c) Every 5-regular graph with 10 vertices is not planar.

Problem 11.68. Euler was intrigued by regular polyhedra, convex solids bounded by finitely many polygonal faces (Platonic solids). A polyhedron is a graph whose edges are intersections between faces. The octohedron and its planar drawing are shown. (See also Exercise 11.7 on page 150.)
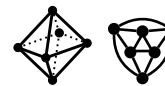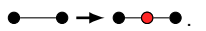
(a) Why is a polyhedron graph planar? *[Hint: Project onto an in-sphere.]*

(b) A polyhedron is regular if every face has the same number of sides s and every vertex is the intersection of the same number of faces d. In the octohedron, the polygons are triangles, so $s = 3$, and four triangles intersect at every vertex so $d = 4$. Show that the graph of a regular polyhedron is regular and the vertex-degree is d.

(c) Let V be the number of vertices, E the number of edges and F the number of faces of the polyhedron. Show that $Vd = 2E$ and $Fs = 2e$, hence that $Vd = Fs$.

(d) Use Euler's invariant to show: $1/s + 1/d - 1/2 = 1/E$ and hence $3 \leq s, d \leq 5$. Find all possible choices for s, d.

Problem 11.69. Color-code each country (region labeled $A, B, C, \ldots$) so that a minimum number of colors is used and countries that share a border have different color-codes.

(a)

(b)
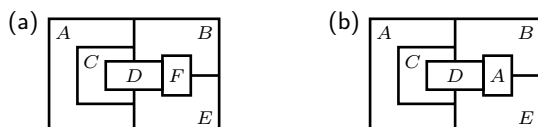
(The 4-color theorem says any map should be 4-colorable. What goes wrong in (b)? What assumption on the countries is needed?)

158

Problem 11.70. Subdividing an edge breaks the edge in two and adds a vertex in the middle: ●——● → ●—●—●. You can continue subdividing edges of a graph to get a subdivision of a graph.

(a) Formally define subdivision. Show that C_n can be obtained by repeated subdivision of K_3.

(b) Show that a sequence of subdivisions adds degree-2 vertices without changing other degrees.

(c) Show that a graph is planar if and only if any subdivision of the graph is planar.

(d) Can a subgraph of the Petersen graph (see Problem 12.53) be obtained by repteaded subdivision of $K_{3,3}$? What about K_5? Is the Petersen graph planar? Explain your answers. *[Hint: Exercise 11.7 (g,h).]*

(Kuratowski's Theorem: Every non-planar graph has a subdivision of $K_{3,3}$ or K_5 as a subgraph.)

Problem 11.71 (Topological Sort). Let G be an acyclic directed graph.

(a) Prove: there is a vertex with in-degree zero and also one with out-degree zero.

(b) For the graph on the right, order the vertices so that if u preceeds v, then there is no v-to-u path. Prove that this is always possible. Such an ordering is a topological sort.
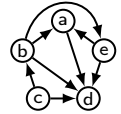
Problem 11.72. Prove that in any tournament which does not contain a cycle, some vertex beats every other vertex.

Problem 11.73. In any ordering of $[1, 2, \ldots, n^2 + 1]$, there is a monotonic subsequence of length $n + 1$. For example, $[5, 1, 2, 4, 3]$ has the monotonic subsequences $[5, 4, 3]$, $[1, 2, 4]$ and $[1, 2, 3]$. Prove this result using directed graphs and partial orders. Let the sequence be $n^2 + 1$ vertices on a line. Add a directed edge from a number (vertex) to every higher number (vertex) on the right. We show the line of vertices for $[5, 1, 2, 4, 3]$, together with the directed edges.

(a) Show: a chain is an increasing subsequence and an antichain is a decreasing subsequence.

(b) Suppose the maximum chain has size at most n. Prove that there is an antichain of size at least $n + 1$ and hence prove the result. *[Hint: Example 11.6, Dilworth's Theorem.]*

(c) Find a permutation of of $[1, 2, \ldots, n^2]$ with no monotonic subsequence of length $n + 1$. (The result is tight.)

**Problem 11.74.** Solve each problem by first finding the appropriate graph representation.

(a) Show that you can't draw 9 line segments on the plane so that each intersects with exactly 3 others.

(b) Three cups have sizes 3,5,8 ounces. The 8 ounce cup is filled with wine. How many pours are needed to split the wine into two cups? If it can't be done, explain why. *[Hint: The start "configuration" (vertex) is $(0, 0, 8)$.]*

(c) 4 canibals and 4 pacifists must cross a river using a row-boat with space for two. If canibals outnumber pacifists on the banks or boat, pacifists are eaten. What is the minimum number of river crossings to transport the people?

(d) A queen covers a square if that square is on the same row, column or diagonal as the queen. What is the minimum number of queens required to cover the 8×8 chessboard?

(e) The friendships between seven people A, B, C, D, E, F, G are shown below. Can the people sit around a circular table so that no two enemies sit next to each other? What if we add one more friendship between C and D?

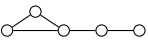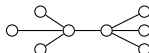|	A	B	C	D	E	F	G
friends with	B, F	A, C, E	B, F, G	F, G	B, F, G	A, C, E	C, D, E

(f) Place n points on a plane so that any two points are at least distance 1 from each other. A good pair of points are distance exactly 1 from each other. Prove that there are at most $3n$ good pairs.

Problem 11.75. A chessboard is infinite in all directions. A (p, q)-knight moves $\pm p$ steps parallel to one axis and $\pm q$ steps parallel to the other axis. A standard knight is a $(2, 1)$-knight. The infinite chess-board is a graph. Each square is a vertex. Two vertices are linked if a (p, q)-knight can, in one move, reach one square from the other. For what p and q is the graph connected, e.g. is $(0, 0)$ connected to $(4, 1)$ by the $(5, 3)$-knight?

(a) What is the degree distribution (does it depend on p and q)?

(b) Prove that a $(5, 3)$-knight which starts at $(0, 0)$ can't reach $(4, 1)$, the red square.

(c) Prove the graph is connected for the $(2, 1)$-knight. (Induction)

(d) When is the graph connected for the $(p, 1)$-knight. (Induction)

(e) For what p and q is the (p, q)-knight's graph connected. *[Hints: The "obvious" necessary conditions are sufficient. Reduce the (p, q)-knight to an $(r, 1)$-knight. Prove the fact: if $\gcd(a, b) = 1$ and a is odd, then $\exists x, y \in \mathbb{N}$ for which $ax - by = 1$ with y even.]*

(f) Prove that if the infinite-in-all-directions board is connected, then the infinite-positive-quadrant board is also connected.
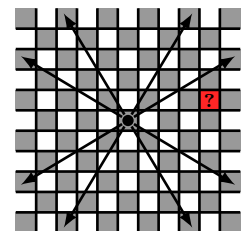
Problem 11.76 (Graceful Labeling). A connected graph has vertices $v_1, \ldots, v_n$ and m edges. Label vertex v_i with $\ell(v_i) \in \{0, \ldots, m\}$. The vertex labels must be distinct. An edge $e = (v_i, v_j)$ inherits the label $|\ell(v_i) - \ell(v_j)|$. The labeling is graceful if all the edge labels are different.

(a) Give graceful labelings of (i) (ii) (iii) The paths L_{10} and L_{11}. (iv) The star S_{10}.

(b) Will there always be enough vertex labels? What will the set of edge labels in any graceful labeling be?

(c) Prove that no graph with m edges can be gracefully labeled with vertex labels from $\{1, \ldots, m\}$.

The Graceful Tree conjecture due to Rosa, Ringel and Kotzig is that every tree can be gracefully labeled.

Problem 11.77 (Sperner's Lemma). Sperner's Lemma is an application of the Handshaking Theorem. We show barycentric subdivisions of a triangle with red, green and blue vertices. The task: color all other vertices, but on an outer side use only the colors at that side's end-points (there are red-green, green-blue and red-blue sides).
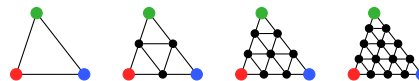
We show a valid coloring of a barycentric subdivision on the right. The three gray-shaded triangles are tricolored (have vertices of all three colors). Prove Sperner's Lemma.
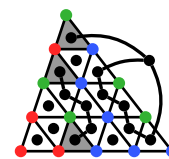
Sperner's Lemma: There is always a tricolored triangle.

Construct a graph (see figure) with vertices for subdivision triangles and an external vertex. Place edges between vertices if the boundaries of the vertex-traingles share a blue-green side.

(a) For any valid coloring of any subdivision, prove that the external vertex has odd degree.

(b) Prove that there is an odd number of odd degree vertices among the internal triangles.

(c) What are the possible degrees of internal-triangle vertices? Which triangles have odd degree?

(d) Prove Sperner's Lemma (actually you proved a stronger result than Sperner's Lemma).

(The proof works for any triangular subdivision, not just barycentric subdivisions. Sperner's Lemma generalizes to $d > 2$ dimensions: a tricolored triangle becomes a $(d+1)$-colored simplex.)

Problem 11.78 (Applications of Sperner's Lemma).

(a) **[Brouwer Fixed Point Theorem]** A map of a country is somewhere inside the country. Prove that some point on the map is directly above the point in the country that it represents. (Assume the country is triangular.)

More generally, let T be a triangle, the convex hull of the vertices $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$. Any continuous mapping $f : T \mapsto T$ has a fixed point $\mathbf{x}_* \in T$ for which $f(\mathbf{x}_*) = \mathbf{x}_*$.

(i) Show that every point $\mathbf{v} \in T$ has a unique representation $\mathbf{v} = x_1 \mathbf{v}_1 + x_2 \mathbf{v}_3 + x_3 \mathbf{v}_3$, where $x_i \geq 0$ and $x_1 + x_2 + x_3 = 1$. (x_1, x_2, x_3) are called the barycentric coordinates of $\mathbf{v}$.

(ii) The mapping f takes $\mathbf{x} = (x_1, x_2, x_3)$ to $(f_1(\mathbf{x}), f_2(\mathbf{x}), f_3(\mathbf{x}))$. Define the color of a point $\mathbf{v}$ as red if $f_1(\mathbf{x}) < x_1$; green if $f_1(\mathbf{x}) \geq x_1$ and $f_2(\mathbf{x}) < x_2$; and blue if $f_1(\mathbf{x}) \geq x_1$, $f_2(\mathbf{x}) \geq x_2$ and $f_3(\mathbf{x}) < x_3$. In the diagram, color v according to the color of the region into which f maps v.

- If f does not have a fixed point, show that every $\mathbf{v} \in T$ has a well defined color.
- What colors are the vertices of T? What colors are points on the sides of T?

(iii) Let $\mathbf{x} = (x_1, x_2, x_3)$ and $\mathbf{y} = (y_1, y_2, y_3)$. Show that if $y_i \leq x_i$ then $\mathbf{x} = \mathbf{y}$.

(iv) Consider a barycentric subdivision of T whose vertices are colored by f as in (ii). What can you deduce about f from a tricolored triangle as the subdivision gets finer?

(v) Prove the Brouwer Fixed Point Theorem. Facts from calculus: T is compact so any infinite sequence has a convergent subsequence. f is continuous which means if $\mathbf{x} \to \mathbf{x}_*$ and $f_1(\mathbf{x}) < x_1$, then $f_1(\mathbf{x}_*) \leq x_{1*}$.

(b) **[Envy-Free Resource Allocation]** Users a, b, c share a resource during a time interval $[0, 1]$: the interval is split into pieces of lengths x_1, x_2, x_3; each user gets one piece. Users value pieces differently, e.g. b and c might prefer earlier and a prefers later. An example allocation is: $\underset{x_1}{\underline{b}} \,\underset{x_2}{\underline{c}} \,\underset{x_3}{\underline{a}}$. Assume a piece of length 0 has no value and users value pieces in a continuous manner. Given three pieces, (x_1, x_2, x_3), a user will have a favorite piece (ties are allowed). Treat (x_1, x_2, x_3) as barycentric coordinates.

(i) Show that one can assign an "owner" a, b or c to each vertex so that every subdivision triangle has vertices with different owners. See the example on the right.

(ii) Color each vertex (allocation) using its owner's favorite piece: red for x_1, green for x_2 and blue for x_3. Prove: There is always a tricolored traingle.

(iii) Prove: There is a resource allocation with every user geting their favorite piece. Such a sharing is envy-free (no user is jealous of any other).
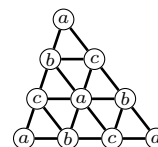
12.4 Problems

Problem 12.1. Identify which graphs are bipartite and redraw them with left and right vertices.

(a) (b) (c) (d) (e) (f) (g)
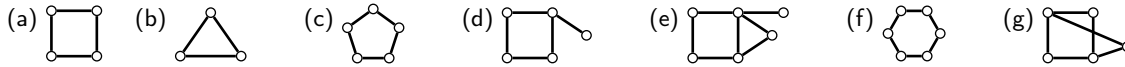
Problem 12.2. An r-regular bipartite graph G with $r \geq 1$ has left and right vertex sets V_1 and V_2. Prove $|V_1| = |V_2|$.

Problem 12.3. Bipartite matching pairs objects of one type with another type, e.g. men with women. Instead, one can match objects with each other. For example, assigning roommates when people are not compatible with everyone (one defines a compatibility graph). A perfect matching pairs up all vertices. Which graphs have perfect matchings
(a) K_n (b) C_n (c) P_n (d) S_{n+1} (e) W_{n+1}?

Problem 12.4. Show that these graphs with an even number of vertices, have no perfect matching. Show also that you can add one edge, and get a perfect matching in each case. (Problem 12.3 defines perfect matchings.)

(a) (b)

Problem 12.5. A maximum matching maximizes the number of edges in the matching. A matching is maximal if it cannot be increased by adding another edge. For each graph, find maximal and maximum matchings of the given sizes.

(a) maximal:2 maximum:3 (b) maximal:1 maximum:2
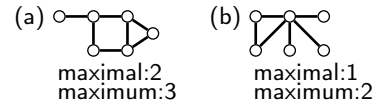
Problem 12.6. Find a maximum matching in each graph.

(a) (b) (c) (d)

Problem 12.7. Five women A, B, C, D and E are each willing to marry a subset of the men V, W, X, Y and Z (chart on the right). Find a matching of the women to men they are willing to marry. Only one woman can marry a man. If you think it can't be done, prove it using Hall's Theorem.

| A: V, W |
| B: V, X, Y |
| C: V, Z |
| D: W, Z |
| E: V, Z |

Problem 12.8. A company has system admins P, Q, R, S. Admins have areas of expertise, but may only cover one area. Can the four different areas be covered? If yes, assign the admins to areas. If no, prove it using Hall's Theorem.

| P: mac, wireless, email |
| Q: linux, wireless |
| R: wireless, email |
| S: linux, mac |

Problem 12.9. In a regular bipartite graph every vertex has the same degree. Prove:
(a) The number of left and right-vertices are equal. (b) Some matching covers the left-vertices. *[Hint: Hall's theorem.]*

Problem 12.10. Prove or disprove.
(a) K_3 is bipartite.
(b) Every graph with a perfect matching is connected.
(c) Every tree has at most one perfect matching. *[Hint: To which vertex must a leaf match?]*
(d) Any maximal matching is at least half the size of a maximum sized matching.

Problem 12.11. The gray edges form a bipartite graph and the black edges are a matching.
(a) Show that the matching is maximal. Find an augmenting path which starts and ends at unmatched vertices, doesn't repeat vertices, and alternates between using non-matching and matching edges.
(b) Prove: if there is an augmenting path, you can increase the size of the matching.
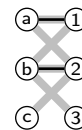
Problem 12.12. Show that a graph G is bipartite if and only if it has no cycle of odd length.
(a) Prove that if there is a cycle of odd length, the graph cannot be bipartite.
(b) Use a BFS-tree (Problem 11.61) to color even level vertices red and odd level vertices blue. Show that the 2-coloring is valid if and only if no edge connects vertices in the same level.
(c) Prove that if an edge exists between vertices in the same level, there is an odd cycle.
(d) Show that a graph has chromatic number 2 if and only if it has no cycle of odd length.

Problem 12.13. Use Problem 11.33 to prove that a bipartite graph has no cycle of odd length. *[Hint: The adjacency matrix of a bipartite graph for a suitable ordering of the vertices has the form $\mathrm{A} = \begin{bmatrix} \mathbf{0} & \mathrm{B} \\ \mathrm{B}^{\mathsf{T}} & \mathbf{0} \end{bmatrix}$. What is the form of A^{2k+1}?]*

Problem 12.14. Jobs $J_1, \ldots, J_n$ are performed on servers $S_1, \ldots, S_m$. Server S_i has capacity for $\ell_i \geq 0$ jobs. Each job can run on a subset of the servers. Give necessary and sufficient conditions for being able to do all the jobs.

Problem 12.15. Each of m children $\epsilon_1, \ldots, \epsilon_m$ like a subset of the camps in $\{C_1, \ldots, C_n\}$. Camp C_i has space for $c_i \geq 0$ children. Give necessary and sufficient conditions for being able to fill all the camps to capacity.

Problem 12.16. From m committees $C_1, \ldots, C_m$ we choose distinct representatives $r_1, \ldots, r_m$, one from each committee. Prove this is possible if and only if for every subset $S \subseteq \{1, \ldots, m\}$, $|\cup_{i \in S} C_i| \geq |S|$.

Problem 12.17. Two players alternately choose distinct vertices on a graph G. Player 1 starts with any vertex, and each subsequent new vertex picked must be adjacent to the previous one picked. The two players together follow a path on G. The last player to pick a vertex wins. Prove that player 2 can win if and only if G has a perfect matching.

Problem 12.18. Ayfos was born on Jan. 5,6,9 or Feb. 7,8 or Mar. 4,6 or Apr. 4,5,7. Ayfos reveals the month to Kilam and the day to Niaz. The possible birthdays are represented as a bipartite graph with months on the left and days on the right. Here is the conversation between Kilam and Niaz
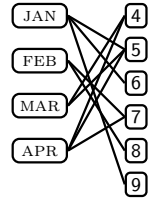
 (a) *Kilam (to Niaz)*: I know that you can't figure out the month.
 (b) *Niaz (to Kilam)*: Well, I can now figure out the month.
 (c) *Kilam (to Niaz)*: Ahh, I can now figure out the day.
Use each statement to remove edges. Only one edge will remain. When was Ayfos born?

Problem 12.19. A non-negative matrix Q with row and column-sum 1 is called doubly stochastic.

 (a) A permutation matrix is a matrix of 0s and 1s with one 1 in each column and row. Prove that a square nonnegative integer matrix is a sum of n permutation matrices if and only if every row and column sums to n. For example,

$$\begin{pmatrix} 1 & 3 & 0 \\ 2 & 1 & 1 \\ 1 & 0 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

 (b) Prove, by induction on the number of non-zeros, that a doubly stochastic matrix Q is a linear combination of permutation matrices, $Q = c_1 P_1 + \cdots + c_m P_m$, where $\sum_i c_i = 1$ and $c_i > 0$. For example,

$$\begin{pmatrix} 0.5 & 0.2 & 0.3 \\ 0 & 0.3 & 0.7 \\ 0.5 & 0.5 & 0 \end{pmatrix} = \frac{3}{10} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} + \frac{1}{5} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} + \frac{1}{2} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Problem 12.20. For the given preferences of 3 boys b_1, b_2, b_3 and 3 girls g_1, g_2, g_3, find stable marriages using the dating ritual when:
 (a) Boys woo and girls decide.   (b) Girls woo and boys decide.
A person's regret is how far from their top choice they married (e.g. if b_1—g_3 is a marriage, then regret$(b_1) = 2$ and regret$(g_3) = 1$). Compute the regrets in (a) and (b).
(FYI: Girls have maximum regret when boys propose and minimum regret when girls propose. **Make the first move!**)

	b_1	b_2	b_3		g_1	g_2	g_3
1.	g_2	g_1	g_1		b_1	b_2	b_3
2.	g_1	g_3	g_2		b_3	b_3	b_1
3.	g_3	g_2	g_3		b_2	b_1	b_2

Problem 12.21. The dating ritual finds a stable matching in a complete bipartite graph $K_{n,n}$. If, instead, the underlying graph is complete, K_{2n}, then any pair of vertices can be matched. Each person now has a preference list over $2n - 1$ people. For $n = 2$, on the right are preference lists for four friends **A**lice, **B**arb, **C**harlie and **D**unce. **A**, **B** and **C** form a "love triangle" with **A** liking **B** who likes **C** who likes **A**. **D** is a misfit in this group. Prove there is no stable matching.

	A	**B**	**C**	**D**
1.	B	C	A	A
2.	C	A	B	B
3.	D	D	D	C

Problem 12.22. For bipartite graphs, there is always a stable matching for any set of preferences (Gale & Shapley). Is there also always an unstable matching for any set of preferences? Prove:
> Every set of preferences for n boys and n girls ($n \geq 3$) has an unstable matching.

Problem 12.23 (Greedy Matching). A greedy algorithm for stable marriage is to process the boys in an arbitrary order, giving each boy their top-choice among all available girls at the time the boy's match is made.
 (a) Prove that every boy will be matched. (b) Give an example to show that the resulting matching may not be stable.

Problem 12.24. Courses $C_1, \ldots, C_k$ are available to n students. Course C_i has capacity c_i, where $\sum_i c_i = n$. Students submit preferences ranking the k courses. Each student is placed in one course. An assignment of students to courses is stable if no pair of students wish to exchange seats. Prove or disprove: The greedy algorithm which sequentially places students into their top-choice among the available courses at that time produces a stable assignment.

Problem 12.25. Ten years before the dating algorithm, the National Resident Matching Program was matching medical residents to hospitals. Each candidate submits preferences over hospitals and each hospital submits preferences over candidates. Each hospital could have multiple openings for residents. Give a dating algorithm for stable matching of residents to hospitals and prove it. *[Hint: Model a hospital with multiple openings as multiple identical hosiptals.]*

Problem 12.26 (Proof of Theorem 12.5). In the dating ritual with boys proposing, prove that the stable outcome is the best possible for boys and worst possible for girls. Let the final marriages be $M = \{b_1-g_1, \ldots, b_n-g_n\}$.

(a) For only this part, suppose the top choices of all the boys are distinct. How happy is b_1? What about g_1?

(b) Prove there is no stable matching where any b_i marries a girl he likes more than g_i.

    (i) For another stable matching with marriages $M' = \{b_1-g'_1, \ldots, b_n-g'_n\}$. Suppose $b_i : [g'_i > g_i]$ (this notation means b_i prefers g'_i to g_i). Show that at some time in the dating ritual, b_i woos g'_i and gets rejected.

    (ii) Among the boys who are better off in M', let b_* be the first to be rejected by his prefered mate g'_*, who rejects b_* for b (b marries g in M and g' in M'). Prove:

$$g'_* : [b > b_*]; \qquad b : [g'_* \geq g]; \text{ (Who did } b \text{ woo first?)} \qquad b : [g' > g'_*] \ (M' \text{ is stable}).$$

    Therefore, prove that b is also happier in M'.

    (iii) Prove that b was rejected before b_* was rejected. Prove the claim by contradiction.

(c) Prove there is no stable matching where any g_i marries a boy she likes less than b_i. *[Hints: Contradiction. Assume g_* marries b_* in M but b in M', and $g_* : [b_* > b]$. Use stability of M' to show that b_* is happier in M' than M.]*

Problem 12.27 (König-Egerváry Theorem). Use Hall's Theorem to prove that the sizes of a maximum matching and minimum vertex cover are equal in bipartite graphs. Consider a bipartite graph as shown. Let Q be a minimum vertex cover with left-vertices X and right-vertices Y, so $Q = X \cup Y$. The left-vertices not in X are $\bar{X}$ and the right-vertices not in Y are $\bar{Y}$. Let $S \subseteq X$ be a subset of left-vertices in X. The neighbors of S are some vertices in Y (gray edges) and some vertices in $\bar{Y}$. Let the neighbors in $\bar{Y}$ by $\bar{N}(S)$.
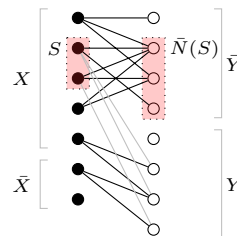
(a) Prove that Q remains a vertex cover if S is replaced with $\bar{N}(S)$.

(b) Prove that $|S| \leq |\bar{N}(S)|$. *[Hint: Q is a minimum vertex cover.]*

(c) Prove there is a matching from X into $\bar{Y}$ that covers X. *[Hint: Hall's Theorem.]*

(d) Similarly, prove there is a matching from $\bar{X}$ into Y that covers Y.

(e) Prove there is a matching whose size is $|Q|$ and explain why this concludes the proof.

For a direct proof of this deep result, see "A short proof of König's Theorem" by R. Rizzi, 2000.

Problem 12.28. Prove Hall's Theorem using the König-Egerváry Theorem. *[Hint: If all left-vertices can't be matched, the left-vertices not in a minimum vertex cover violate Hall's condition.]*

Problem 12.29. In graph G, C is a vertex cover and M is a matching. Prove:

(a) If you add a vertex u to G, with some edges to u, then $C \cup \{u\}$ is a vertex cover for $G \cup \{u\}$.

(b) Each vertex in C can cover at most one edge in M.

(c) $|M| \leq |C|$. Hence prove: size(maximum matching) $\leq$ size(minimum vertex cover).

Problem 12.30. Color C_3, C_4, C_5, C_6 using the fewest colors. Make a conjecture and prove it.

Problem 12.31. Find the minimum number of colors, $\chi(G)$, needed to color each graph.

(a) (b) (c) (d) (e) (f) (g) K_n (h) $K_{n,m}$ (i) C_n (j) W_{n+1}.

Problem 12.32. What can you say about $\chi(G)$ if G has K_n as a subgraph?

Problem 12.33. For any graph G, show that Greedy coloring uses $\chi(G)$ colors for some vertex-ordering.

Problem 12.34. Describe a method for coloring the tree on the right using the fewest colors. Your method should work for any tree. Explain why your method works for any tree.
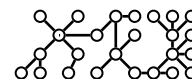
Problem 12.35. Consider Greedy coloring with the vertices ordered $1, 2, \ldots$

(a) How many colors does Greedy use for the graph on the right?

(b) Show that the chromatic number of the graph on the right is 2.

(c) Generalize. Show that there is a graph G with n vertices for which $\chi(G) = 2$, but Greedy uses $\Omega(n)$ colors for some vertex-order.
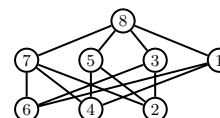
Problem 12.36. For any $M \geq 2$, prove that there is a tree and an ordering of its vertices for which Greedy coloring needs at least M colors. Tinker! *[Hint: ○–○–○–○ and recursion.]*

Problem 12.37 (4×4 **Sudoko**). A completed 4×4 Sudoko is shown on the right. Each quadrant, row and column must contain the digits $1, 2, 3, 4$. Treating the numbers as colors, a valid solution to the Sudoko puzzle gives a 4-coloring of a particular graph. What is that graph?

2	3	1	4
1	4	2	3
3	1	4	2
4	2	3	1

Problem 12.38. A graph G with n vertices has maximum degree $\Delta \geq 1$. Prove:
  (a) $\chi(G) \leq \Delta + 1$, and give a graph for which the bound cannot be improved.
  (b) If at most Δ vertices have the maximum degree Δ, then $\chi(G) \leq \Delta$.
  (c) If at least κ vertices have degree at most δ, then $\chi(G) \leq \max\{n - \kappa, \delta + 1\}$.
  (d) If G is connected and at least one vertex has degree strictly less than Δ, then $\chi(G) \leq \Delta$.
  (e) $\chi(G \setminus v) \leq \chi(G) \leq \chi(G \setminus v) + 1$, where $G \setminus v$ is G with the vertex v removed.
  (f) $\chi(G)\chi(\overline{G}) \geq n$, where $\overline{G}$ is the complement graph of G.

Problem 12.39. Graph G has maximum degree k and is not regular. Prove or disprove: G is k-colorable.

Problem 12.40. Prove by induction that every connected acyclic graph (i.e., a tree) is bipartite as follows.
 (a) Show there is a degree-1 vertex. *[Hint: End of a longest path.]*   (b) Remove a degree-1 vertex and use induction.

Problem 12.41. Computing χ and finding a χ-coloring are in a sense equivalent. Show how a blackbox that computes the chromatic number χ for any graph. can be used to find a minimum coloring of a graph G.
  (a) If u, v are non-adjacent, the contraction $G_{u,v}^-$ merges u, v into one vertex whose neighbors are those of u and v. The augmentation $G_{u,v}^+$ adds the edge (u, v). Give $G_{u,v}^-$ and $G_{u,v}^+$ for the graph shown.
  (b) Show: if some minimum coloring in G gives u and v the same color, then $\chi(G) = \chi(G_{u,v}^-)$. In this case, how can you get a minimum coloring of G from a minimum coloring of $G_{u,v}^-$?
  (c) Show: if every optimal coloring of G gives different colors to u, v then $\chi(G) = \chi(G_{u,v}^+)$. In this case, how do you get an optimal coloring of G from an optimal coloring of $G_{u,v}^+$?
  (d) Show how to optimally color G using $O(n^2)$ blackbox-calls plus $O(n)$ extra work, where n is the number of vertices.

Problem 12.42 (**5-Color Theorem**). Let G be a planar graph with n vertices. Prove by induction on n that G can be 5-colored. Let v be a minimum-degree vertex in G. By Exercise 12.10(a), $\deg(v) \leq 5$.
  (a) Why can you assume that $G \setminus v$ can be 5-colored?
  (b) Suppose $\deg(v) \leq 4$. Prove that G can be 5-colored.
  (c) Suppose $\deg(v) = 5$. Let $v_1, \ldots, v_5$ be the neighbors of v. Prove that $G \setminus v$ can be 5-colored while using at most 4 colors for $v_1, \ldots, v_5$.
    (i) Prove there are two neighbors of v who are not linked. *[Hint: Exercise 11.7(g).]*
    (ii) Suppose v_1 and v_2 are not linked by an edge. Merge them into a super-vertex v_1v_2 as shown on the right (every edge to v_1 or v_2 becomes an edge to the super-vertex v_1v_2). Prove that $G \setminus v$ with this super-vertex is planar and also that it can be 5-colored.
    (iii) Prove that a 5-coloring of $G \setminus v$ is obtained from the 5-coloring in (ii) by giving both v_1 and v_2 the color of the supervertex v_1v_2. How many colors are used for $v_1, \ldots, v_5$?
 (d) Complete the proof that G is 5-colorable.
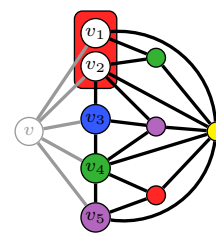
Problem 12.43. In Section 12.3 on page 168 are the graph problems: (a) Connected components (b) Spanning tree (c) Euler cycle (d) Hamiltonian cycle (e) K-center (f) Vertex cover (g) Dominating set (h) Network flow. Give a "formal" problem specification for each task (you don't need to solve the task). Your formal specification should include:
  (i) A formal specification of the input (e.g. a graph $G = (V, E)$).
  (ii) A formal specifcation of the output (e.g. a subset $S \subseteq V$).
  (iii) The property the output must have (e.g. S is a largest subset with pairwise adjacent vertices).

Problem 12.44. Draw a graph with chromatic number at least 6, and prove it. Make the drawing planar if you can.

Problem 12.45. Find the desired object for the graph shown. (There's no efficient solution for general graphs.)
  (a) [MAXCLIQUE] A largest vertex set of pairwise adjacent vertices (each pair of vertices is adjacent).
  (b) [MAXINDEPENDENTSET] A largest vertex set of pairwise non-adjacent vertices.
  (c) [MINVERTEXCOVER] A smallest vertex set such that every edge has at least one endpoint in the set.
  (d) [MINDOMINATINGSET] A smallest vertex set such that every other vertex has a neighbor in the set.
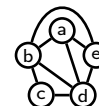
Problem 12.46. Solve each problem (a)–(c) for each graph (i)–(iii).
  (a) Does the graph have an Euler cycle, an Euler path, both or neither?
  (b) Color the graph using a minimum number of colors. What is the chromatic number?
  (c) Find a minimum dominating set and a minimum vertex cover.
  (d) Find a maximum clique and a maximum independent set.

(i)
(ii)
(iii)
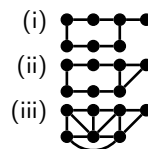
Problem 12.47 (Hamiltonian Cycle). A Hamiltonian path visits every node once. A Hamiltonian cycle, in addition, returns to the start. Find Hamiltonian paths and cycles in these graphs. If you think it's impossible, explain why.

  (a)   (b)   (c)   (d)   (e)

Can a graph have both a Hamiltonian path and a Hamiltonian cycle?

Problem 12.48. A tournament is a graph with a directed edge between every pair of vertices. Prove that every tournament has a directed Hamiltonian path, a path visiting every vertex once.

Problem 12.49. For what n, m does $K_{n,m}$ have: (a) An Euler path or cycle   (b) A Hamiltonian path or cycle?

Problem 12.50. Sir William Hamilton's "Voyage around the world" puzzle on the right is a planar drawing of a dodecahedron which represents the world with 19 cities as vertices of the dodecahedron. The puzzle is to determine whether one can start at a city and visit each city once along the edges of the dodecahedron, returning to the original city. Can you find a Hamiltonian cycle?

Problem 12.51. A graph has a Hamiltonian cycle. You add an edge. Must the graph continue to have a Hamiltonian cycle? Repeat for: Hamiltonian path; Euler cycle; Euler path.

Problem 12.52 (Dirac's Theorem). A graph G has $n \geq 3$ vertices and minimum degree at least $n/2$. Prove that G has a Hamiltonian cycle using the following steps.
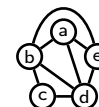 (a) Prove that G is connected.
  (b) Let $P = u_1 u_2 \cdots u_k$ be a longest path in G. Prove that all edges of u_1 and u_k are to other vertices in P.
  (c) If (u_1, u_k) is an edge, then P is a cycle. If not, show that there are consecutive vertices u_j, u_{j+1} for which (u_1, u_j) and (u_{j+1}, u_k) are edges. Construct a cycle with all vertices of P.
  (d) Show that the cycle in (c) is Hamiltonian (no vertex is left out). *[Hint: P is a longest path.]*
  (e) Dirac's Theorem is a special case of Ore's Theorem which only requires non-adjacent vertices to have degree-sum at least n. Use the same general idea to prove Ore's Theorem.

Problem 12.53 (Petersen Graph). Give the degree sequence for the Petersen graph on the right.
  (a) Show that the Petersen graph is not bipartite and give a 3-coloring.
  (b) Show that there is a Hamiltonian path, but no Hamiltonian cycle.
  (c) Show that if you remove any vertex, the graph has a Hamiltonian cycle.
  (d) Is there an Euler cycle or Euler path?
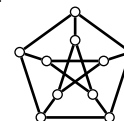
Problem 12.54 (Line Graph). For graph G, the line graph $L(G)$ has a node for every edge in G. Two vertices in $L(G)$ are adjacent if and only if their corresponding edges in G have a common endpoint. Give the line graphs of: (a) The graph on the right.   (b) K_4 (c) $K_{1,3}$ (d) C_5 (e) P_5 (f) S_5.

Problem 12.55. Prove the following properties about a graph G and its line graph $L(G)$.
  (a) If G is connected, $L(G)$ is connected. Is the converse true?
  (b) If G has an Euler cycle, $L(G)$ has a Hamiltonian cycle. Is the converse true?
  (c) If G_1 and G_2 are isomorphic, $L(G_1)$ and $L(G_2)$ are isomorphic.
  (d) If G has degree sequence $[\delta_1, \ldots, \delta_n]$, $L(G)$ has $(\sum_{i=1}^{n} \delta_i)/2$ vertices and $\sum_{i=1}^{n} (\delta_i^2 - \delta_i)/2$ edges.

Problem 12.56. To virally market a product, you give it for free to sponsors – primary adopters. A sponsor convinces their friends to buy the product – secondary adopters. We show a graph in which the red sponsors convert the blue vertices, but there are some non-adopters (black). If the red sponsors can convert all the remaining vertices to blue, then the sponsors are a dominating set. Every vertex is either in the dominating set or linked to at least one vertex in the dominating set.
  (a) Find a minimum sized set of sponsors that converts the whole network in the example, a minimum dominating set. (Finding a minimum dominating set for a general graph is [HARD].)
  (b) Show that a minimum dominating set has at least $n/(\Delta + 1)$ vertices. (Δ = maximum degree)
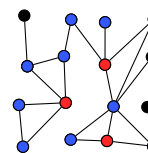
Problem 12.57. A graph has n vertices and every node has positive degree. Show that a minimum dominating set has at most $n/2$ vertices using the following approach.

(a) A weak 2-coloring is a 2-coloring such that every vertex is adjacent to at least one vertex of opposite color. Show that there exists a weak 2-coloring. *[Hint: BFS, Problem 11.61]*

(b) Show that vertices of the same color in a weak 2-coloring form a dominating set.

(c) Show that there are at least two disjoint dominating sets and complete the proof.

Problem 12.58. An independent set is maximal if you cannot increase its size by adding a vertex. Prove that any maximal independent set is a dominating set. When is the complement of a maximal independent set also dominating?

Problem 12.59. Use Problem 12.58 to show that if all vertices have positive degree, then there are two disjoint dominating sets. Hence, one has at most half the vertices. *[Hint: Largest independent set and its complement.]*

Problem 12.60. In a graph with n vertices, every group of size $\lceil n/2 \rceil$ has a common neighbor outside the group. Prove: Some vertex has degree $n - 1$. *[Hint: Complement graph, contradiction and Problem 12.59.]*

Problem 12.61. Prove: S is a vertex cover if and only if its complement $\overline{S}$ is an independent set. Hence that

$$\text{size(largest independent set)} + \text{size(smallest vertex cover)} = \text{number of vertices.}$$

Problem 12.62. Prove: A graph with n vertices and max. degree Δ has an independent set of size at least $n/(\Delta+1)$.

Problem 12.63. For a graph G with n vertices, $\alpha(G)$ is the maximum size of an independent set and $\chi(G)$ is the minimum number of colors needed to color G. Prove: $\chi(G) \geq n/\alpha(G)$.

Problem 12.64. A zoo wants to place as many different species in an exhibit as possible. Two species are incompatible if they compete for food or one eats the other, which defines an incompatibility graph with species as vertices. The zoo needs a largest subset of pairwise compatible species, a maximum independent set in the incompatibility graph.

(a) If a species is incompatible with no more than Δ other species, show that you can place at least $n/(\Delta+1)$ species in the exhibit. (Δ is the maximum degree of the incompatibility graph.)

(b) (Turán) If, on average, a species is incompatible with d other species, show that you can place at least $n/(d+1)$ species in the exhibit. (The graph's average degree is d.) Use the following steps.

   (i) Show that the set I created in the following way is an independent set.
      1. Pick an ordering of the n vertices.
      2. Place v_i into I if and only if v_i preceeds all its neighbors in the ordering.
     Create an independent set for each of the $n!$ orderings $I_1, \ldots, I_{n!}$. The independent sets may not be distinct.

   (ii) Show that v_i belongs to $n!/(\delta_i + 1)$ of the the $n!$ independent sets $I_1, \ldots, I_{n!}$.

   (iii) Show $\sum_{k=1}^{n!} |I_k| = n! \sum_{i=1}^{n} 1/(\delta_i + 1)$, and thus the average size of $I_1, \ldots, I_{n!}$ is $\sum_{i=1}^{n} 1/(\delta_i + 1)$.

   (iv) Show that the maximum independent set has size at least $\sum_{i=1}^{n} 1/(\delta_i + 1)$.

   (v) Show that $\sum_{i=1}^{n} 1/(\delta_i + 1) \geq n/(d + 1)$. *[Hint: AM-HM inequality, see Problem 6.40.]*

Problem 12.65. In Problem 12.54, we defined the line graph. Prove that the edges in a matching of G are an independent set in the line graph $L(G)$. So, a maximum matching in G gives a maximum independent set in $L(G)$.

Problem 12.66 (Interval Graph). Given intervals on a line, to get the interval graph, treat intervals as vertices and add edges between intervals if they overlap. Intervals $[x_1, y_1]$ and $[x_2, y_2]$ overlap if and only if $\max(x_1, x_2) \leq \min(y_1, y_2)$.
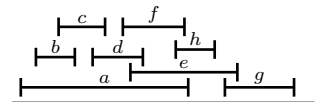
(a) Give the interval graph for the intervals $a, b, \ldots, h$ shown.

(b) The intervals are durations over which tasks $a, b, \ldots, h$ are to be performed. Only one person is available. Show that the largest number of tasks which can be performed is a largest independent set in the interval graph. What are these tasks?

(c) What is the minimum number of people needed to do all the tasks?

(d) We show the temperature range for storing a set of drugs $D_1, \ldots, D_7$ on the right.

   (i) At what temperature do you set a fridge to store the largest number of drugs? *[Hint: Formulate a graph and identify a largest clique.]*

   (ii) To store all drugs, how many fridges do you need, and at what temperatures?

(e) Which of these graphs can be an interval graph: (i) K_n (ii) C_n (iii) $K_{n,m}$ (iv) S_{n+1}.

Drug	Temp
D_1	[25,37]
D_2	[29,43]
D_3	[36,50]
D_4	[49,52]
D_5	[51,55]
D_6	[36,51]
D_7	[50,54]

Problem 12.67. From intervals $[a_i, b_i]$, $i = 1, \ldots, n$, you repeatedly choose the interval with leftmost b and throw away all intervals which overlap it. Prove that the intervals chosen are a maximum independent set in the interval graph.

Problem 12.68 (Maximum Cut). A cut is a division of the vertices into two sets S_1 and S_2. The cut-size is the number of edges crossing from S_1 to S_2. A sad vertex doesn't have more neighbors in its own set than the other set.
  (a) Show that there is a cut in which every vertex is sad. *[Hint: Consider the maximum cut.]*
  (b) Show that any cut in which every vertex is sad has size at least half the size of the maximum cut.

Problem 12.69 (Metric K-Center and Greedy). To service 10 points on the plane, are 3 warehouses, each warehouse is at a point. The roads form a grid. A point p's service distance δ_p is the distance along roads to its nearest warehouse. The maximum service distance Δ is the furthest a point is from its warehouse, $\Delta = \max_p \delta_p$. We must place the warehouses to minimize Δ.
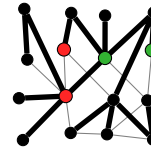 (a) Compute Δ for the 3 warehouses boxed in red.
  (b) Find Δ^*, the optimal Δ by writing a program to try all choices for 3 warehouses.
  (c) Here is a greedy algorithm to find k warehouses. Pick the first warehouse arbitrarily.
      1: **while** number of warehouses $< k$ **do**
      2:    Pick the next warehouse as the point with largest service distance to the current set of warehouses.
      Let Δ be the maximum service distance for the three warehouses returned by the greedy algorithm.
    (i) Use the algorithm starting from each point. Report Δ_{best} and Δ_{worst} for the best and worst 3 warehouses found.
    (ii) Show that any two warehouses is at least Δ apart and some point is at least Δ away from every warehouse.
    (iii) Consider the 3 warehouses and the point which is at least Δ away from all warehouses in the optimal solution (4 points). Show that at least two of these points are serviced by the same warehouse in the optimal solution.
    (iv) Show that the two points serviced by the same warehouse in the optimal solution are at most $2\Delta^*$ apart.
    (v) Prove that $\Delta \le 2\Delta^*$. That is, the greedy algorithm is a 2-approximation to optimal.
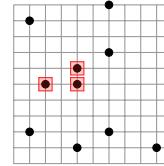
Problem 12.70 (Low Stretch Spanners). Spanning trees can be highways in road networks. On the right, the thick black edges are a spanning tree highway system. The other edges are non-highways. The highway-only path between the green vertices has length 2, and there's no shorter path using all edges. For the red vertices, the shortest path-length is 1, but the highway-only path has length 3. The path-stretch is the ratio of the highway-only to shortest path-lengths. The path stretch is 1 for the green vertices and 3 for the red vertices.
  (a) The stretch is the maximum path-stretch over all vertex-pairs. Compute the stretch of the spanning tree above.
  (b) Find a "best" spanning tree, having minimum stretch. (In general, this task is [HARD].)
  (c) What is worst case path stretch for a minimum stretch spanning tree. *[Hint: C_n.]*
  (d) Prove that the stretch of a spanning tree is at least 2 unless the graph is a already a tree.
  (e) Give a minimum stretch spanning tree for K_n. What is the stretch?

Problem 12.71 (Minimum Spanning Tree, MST). In a weighted graph, it is often important to have a spanning tree whose edges have the minimum total weight, a minimum weight spanning tree, MST. In a highway system, such a tree contains the widest highways with shortest transit times.
  (a) For the weighted graph shown, construct an MST.
  (b) Prove or disprove. Every connected weighted graph has at least one MST.
  (c) Prove or disprove. If all edge weights are distinct then all spanning trees have different total weight.
  (d) Prove or disprove. If edge e has strictly minimum weight, every MST contains edge e.
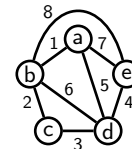
Problem 12.72 (Prim's Greedy Algorithm for Minimum Spanning Tree, MST). For a weighted connected graph G with n nodes, Prim's algorithm uses a greedy approach to construct a tree as follows.
  1: Initialize sets S and T to empty sets. Add any vertex v_1 into S.
  2: **while** $S \ne V$ **do**
  3:    Find a lowest weight edge $e = (u, v)$ connecting a vertex $u \in S$ to a vertex v in $\overline{S}$. Add e into T and v into S.
The tree constructed by Prim's algorithm consists of the edges in T. Let T_* be the edges of any MST.
  (a) Use Prim's greedy algorithm to construct a spanning tree for the graph in Problem 12.71.
  (b) Prove that the edges in T constructed by Prim's algorithm are a spanning tree for any connected graph G.
  (c) Label the vertices as they are added into S as $v_1, \ldots, v_n$. The edges in T are (v_i, v_{i+1}) for $i < n$. Let (v_k, v_{k+1}) be the first edge in T that is not in T_*. Prove there is some edge $w = (v_i, v_j) \in T_*$ where $i \le k$ and $j > k$.
  (d) Prove that replacing w in T_* with (v_k, v_{k+1}) gives a spanning tree with total weight no larger than weight(T_*)
  (e) Prove that the spanning tree T produced by Prim's algorithm is an MST.

Problem 12.73 (Traveling Salesman and MST). A traveling salesman (red) visits 8 clients (black) and returns home (red). The salesman drives along the road network which is a grid.
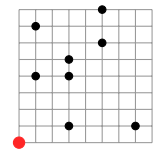
(a) What order for visiting clients minimizes the distance driven? How far must the salesman drive?

(b) Prove that the distance driven is further than the weight of any minimum spanning tree of an appropriately defined graph. You must define the graph.

(c) Use a minimum spanning tree rooted at the home vertex (red) to construct a path that visits each client and uses each edge of the tree at most twice. *[Hint: Pre-order traversal.]*

(d) Prove that the tree constructed in (c) is a 2-approximation to optimal.

Problem 12.74. Solve each problem by first formulating it using graphs.

(a) Four knights on a 3×3 chessboard must use standard knight moves to go from the left configuration to the right one. Show how to do it or explain why it can't be done.
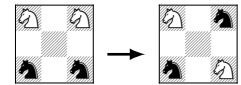
(b) In the neighborhood on the right, black regions are streets and gray regions contain houses on both sides of the streets. A mailman delivers mail to all the houses. To avoid crossing the street back and forth, he walks at least twice along every street, once on each side.
  (i) Construct a path for the mailman so that each side of the street is traversed once.
  (ii) Can you construct a path as in (i) for any neighborhood? Explain.

(c) Six friends play each other in chess. Each game is 1 hour. At least how long will the round robin take?

(d) Radio frequencies $1, 2, \ldots$ are assigned to stations A through F. Two stations cannot be assigned the same frequency unless they are at least 100 miles apart. Pairs of stations which are within 100 miles of each other are highlighted with a red dot in the table. Assign frequencies to the stations using the minimum number of frequencies. Prove that you used the minimum number of frequencies.

	A	B	C	D	E	F
A		•			•	•
B	•		•		•	
C		•		•		
D			•			
E	•	•				•
F	•				•	

(e) Wrapping from back to front, the 3-bit substrings of 00011101 are $000, 001, 011, 111, 110, 101, 010, 100$. Find a 16 bit sequence whose 4-bit substrings are all 4-bit sequences. Is there a 2^d sequence that produces all d-bit sequences as substrings. (Efficient storage of all 2^d d-bit sequences.)

(f) Students A through F are each taking three courses indicated by blue dots in the table. The available courses are C_1 through C_8. Assign the minimum number of exam slots to the courses so that every student can take their exams. Two courses cannot have the same exam slot if a student is in both courses. Prove that you used the minimum number of exam slots.

	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8
A	•	•	•					
B	•	•		•				
B			•	•		•		
D		•		•		•		
E			•		•		•	
F				•		•		•

(g) Four east-coast teams a, b, c, d play four west-coast teams at cities w, x, y, z over four consecutive weeks. On each week each east-coast team plays one west-coast team. An east-coast team flies round-trip into a west-coast city. While on the west-coast, the team drives around playing its matches and then drives back to its first city to take the return flight home. Teams want to minimize their driving. We show the driving distances between the west-coast cities. What cities should each team fly into and what are each teams schedules (who plays whom on each week)? *[Hint: Latin square; TSP.]*

	w	x	y	z
w	0	180	140	100
x	180	0	45	90
y	140	45	0	60
z	100	90	60	0

(h) A zoo needs habitats to house **A**ntelope, **B**aboon, **C**obra, **D**onkey, **E**lephant, **F**lamingo, **G**iraffe, **H**yena, **I**guana, **J**aguar, **K**angaroo, **L**ion and **M**onkey. But, some animals don't get along with others (shown on the right). What is the maximum number of animals that can go into one habitat? What is the minimum number of habitats you need?

1. **C** scares all but **B,E,I,M**.
2. **L,H,J** eat **A,D,K**.
3. **A,E,G** will fight for food.
4. **E,G** will trample **C,I**.
5. **F** is afraid of **E,G,H,J,L**.
6. **B,M** annoys **J,L**.

(i) Color a polyhedron's faces so that faces sharing an edge have different colors. How many colors are needed for the: (i) cube   (ii) tetrahedron   (iii) octahedron?

(j) A house for sale has the floorplan shown. Can a realtor who shows the house:
  (i) Start in a room and return to the room after passing through every door once?
  (ii) Start in a room and return to the room after passing through every room once?
  (iii) Remodel the house so every room has an odd number of internal doors?
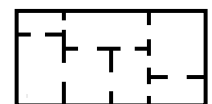
(k) Deal 52 cards of a standard deck into 13 piles of 4. Can you pick a card from each pile and get all values A,K$\cdots$2?

(l) The towns $a, \ldots, g$ each need a hospital or access to one at another town by road. A hospital costs $\$H$ and a road costs $\$R$. The feasible unbuilt roads are shown (dotted). Find the minimum cost of hospital access for all towns if (i) $R = 1, H = 2$. (ii) $R = 2, H = 1$.

(m) We show a friendship network. The vertices are people and the edges are the friendship links. If possible, find a way for the people to be seated at a round table:
  (i) Harmoniously, so that every person has a friend to their left and their right?
 (ii) Sadistically, so that every person has an enemy to their left and their right?

(n) For the same friendship network in part (m), find a smallest set of people D for which every one else is either a friend or friend of a friend (foaf) of someone in the set D.

(o) Color the squares on a 4×4 chess board so that a standard chess knight on any square cannot attack a square of the same color. What if the piece is a king instead of a knight? Generalize to an $n \times n$ board.
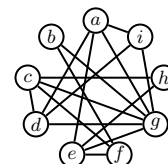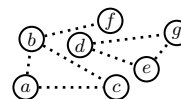
Problem 12.75. Community integration is a social issue. We show a grid-community with offices (brown), parks (green) and houses (white). A house can neighbor up to 8 other houses (vertical, horizontal and diagonal). Black links show the neighbors of each house. An occupant of a house is red or blue. A house is integrated if at least half its neighbor-houses are the opposite color. The community is integrated if every house is integrated.
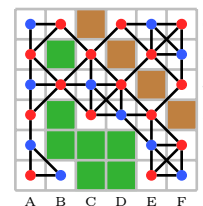
(a) We assigned colors to occupants. Identify all houses which are not integrated.
(b) **Proposition DMC23:** The community must be integrated.
    Reassign colors to houses (you may change the number of red houses) so that the community is integrated.
(c) **Opposition DMC24:** Some communities can't be integrated, depending on how parks and offices are situated. Strike down Opposition DMC24 by proving that one can always integrate a community. Prove:

  Theorem. For any graph, one can assign red or blue to each vertex so that every vertex is integrated.

  [Hint: maximize $\sum_v$ #(opposite color neighbors of v) $-$ #(same color neighbors of v).]

(d) Characterize the communities that can be totally integrated (all neighbors of a house must have opposite color).
(e) The viscinity of a vertex is its neighbors and neighbors of neighbors. Can one always ensure a node's viscinity has at least half the vertices of opposite color. [Hint: Define a "2-hop" neighborhood graph.]

Problem 12.76. MM is a bipartite graph. NF is a directed graph obtained by adding a source s linked it to all left-vertices, and by linking all right-vertices to a sink t. The weight (capacity) of each link is 1 (in black).

(MM)   (NF)
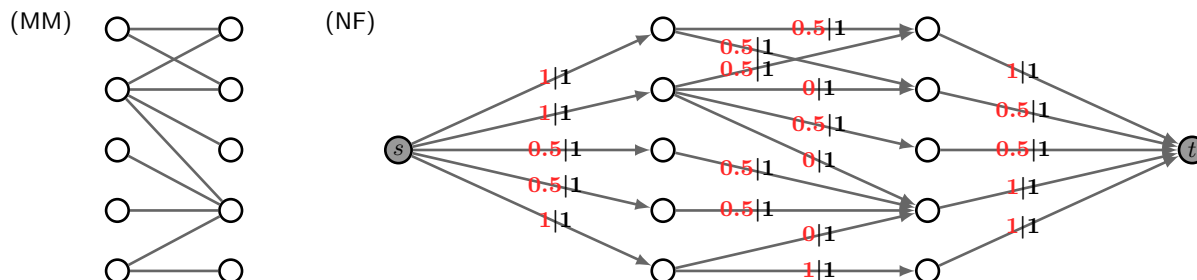
(a) Using Hall's Theorem, show there is no complete matching for the graph MM. Find a maximum matching.
(b) A flow from s to t in NF sends "stuff" from s to t along each edge. We show a flow along each edge in red, and edge capacities in black. 4 units leave s (the size of the flow). Two constraints must be satisfied:
  - [Capacity constraint] The flow on any edge cannot exceed the edge's capacity.
  - [Flow conservation] Except for s, t, everything going into a vertex must leave the vertex.

  (i) For the flow shown in red, verify that all the constraints are satisfied.
  (ii) Show that the maximum matching from (a) also corresponds to a flow.
  (iii) Show that the flow in NF is the maximum possible flow from s to t.
  (iv) Convert the flow in NF to an integral flow, with integral amounts flowing on each edge.
  (v) Show that a maximum integral flow corresponds to a maximum matching.

When link capacities are integers, there is always an integral maximum flow (look up Ford-Fulkerson), from which we get a maximum matching. Using one problem to solve another is a theme in computer science. Network flow has many such uses, from finding disjoint paths to designing surveys to airline scheduling to image segmentation.

13.5   Problems

It is common practice to use $[n]$ as a shorthand for the set $\{1, 2, \ldots, n\}$.

Problem 13.1. Prove: if $A_1, \ldots, A_n$ are disjoint, then $|A_1 \cup \cdots \cup A_n| = |A_1| + \cdots + |A_n|$.

Problem 13.2 (Transitivity). For finite sets A, B, C, prove that injection, surjection and bijection are transitive.
 (a) Prove: IF $A \overset{\text{INJ}}{\mapsto} B$ and $B \overset{\text{INJ}}{\mapsto} C$, THEN $A \overset{\text{INJ}}{\mapsto} C$. ($\overset{\text{INJ}}{\mapsto}$ means "maps injectively to (1-to-1)")
 (b) Prove: IF $A \overset{\text{SUR}}{\mapsto} B$ and $B \overset{\text{SUR}}{\mapsto} C$, THEN $A \overset{\text{SUR}}{\mapsto} C$. ($\overset{\text{SUR}}{\mapsto}$ means "maps surjectively to (onto) ")
 (c) Prove: IF $A \overset{\text{BIJ}}{\mapsto} B$ and $B \overset{\text{BIJ}}{\mapsto} C$, THEN $A \overset{\text{BIJ}}{\mapsto} C$. ($\overset{\text{BIJ}}{\mapsto}$ means "maps bijectively to")
What does each transitivity statement above imply for comparing the sizes of the relevant sets.

Problem 13.3. How many 10-bit binary numbers begin with: (a) 1   (b) 1 or 01   (c) 1 or 01 or 001   (d) 000.

Problem 13.4. We show sample California (left) and West Virginia (right) license plates. Give a plausible counting-based explanation for why these states have different formats.

Problem 13.5. The choices for breakfast (B), lunch (L) and Dinner (D) are shown. You can't have two hot or cold meals in a row. How many daily menus can you create?

> B $\in$ {hot sausages, hot eggs, cold cereal, cold fruit}
> L $\in$ {hot pasta, hot burger, cold sandwich}
> D $\in$ {hot steak, hot pizza, cold salad, cold beer}

Problem 13.6. In how many ways can 6 chess players be organized into 3 pairs for the first round of a tournament. What if the chess boards on which they play are numbered 1,2,3?

Problem 13.7. The set $A = \{1, 2, 3, 4, 5, 6\}$. How many subsets of A are there:
 (a) in all   (b) having $\{1, 2, 3\}$ as a subset   (c) having at least 1 odd number   (d) having exactly 1 even number?

Problem 13.8. A word is a 5-letter string using the characters $a, b, c, \ldots, z$. How many words
 (a) in all   (b) with no repeated letters   (c) begin abc?   (d) begin abc or end xyz (e) begin abc or end cde?

Problem 13.9. Every day, you rest or walk one mile. In how many ways can you walk 12 miles in 20 days?

Problem 13.10. From 10 students, in how many ways can you choose a president and vice-president? What if two students are identical twins in every possible way? What if three students are identical triplets in every possible way?

Problem 13.11. Just as we counted binary numbers, count ternary numbers (digits are 0,1,2).
 (a) (i) How many 10-trit (**tr**inary dig**it**) numbers are there?   (ii) How many 10-trit numbers have four 1's?
 (b) Explain, without explicit calculation, the equality $2^{10}\binom{10}{0} + 2^9\binom{10}{1} + 2^8\binom{10}{2} + \cdots + 2^1\binom{10}{9} + 2^0\binom{10}{10} = 3^{10}$.
 (c) (i) How many 10-trit numbers have four 1's and three 2's.   (ii) How many 10-trit numbers have no 2's.

Problem 13.12. We show the 28 dominos in a standard domino set. Each tile is distinct and uses two numbers from $\{0, \ldots, 6\}$. How many tiles are there if the numbers are in $\{0, \ldots, 8\}$.
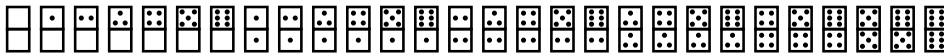
Problem 13.13. An exam has 4 T/F questions; 6 four-choice questions and a long answer question whose answer is an integer between -5 and 5 inclusive. How many possible ways are there to answer the exam?

Problem 13.14. How many binary palindromes have n bits. (A palindrome is a string that equals its reversal.)

Problem 13.15. How many different functions are there which map the given domain to the given range.
 (a) domain = $\{a, b, c, d\}$, range = $\{1, 2, 3, 4, 5\}$ (b) domain = $\{1, 2, 3, 4, 5\}$, range = $\{a, b, c, d\}$.

Problem 13.16. 300056400 has prime factorization $2^4 \times 3^7 \times 5^2 \times 7^3$. How many divisors does 300056400 have?

Problem 13.17. Sets A and B have sizes 3 and 8 respectively. How many functions of each type are there?
 (a) 1-to-1 from A to B (b) 1-to-1 from B to A (c) Onto from A to B (d) Onto from B to A.

Problem 13.18. How many bijections map $\{a, b, c, d, e, f\}$ to: (a) $\{1, 2, \ldots, 6\}$ (b) $\{1, 2, \ldots, 7\}$ (c) $\{1, 2, \ldots, 5\}$?

Problem 13.19. US dollar-bills have 8 digit serial numbers, e.g. 62655681. A bill is defective if a digit repeats. What fraction of bills are defective? *[Hint: Count the non-defective bills.]*

Problem 13.20. How many different squares can a king reach with 100 moves on an infinite chessboard? (Moves are left, right, up, down or diagonal.)

Problem 13.21. How many subsets of $X = \{x_1, \ldots, x_6\}$: (a) Contain x_1.   (b) Contain x_1 and x_2 but not x_4?

Problem 13.22. How many types of skates have: (a) One extra?   (b) Any number of extras? Skate options are:

    Colors: White, Beige, Pink, Yellow, Blue.   **Sizes:** 4,5,6,7,8.   **Extras:** Tassels, Stripes, Bells.

Problem 13.23. T-shirts come in 4 colors and 5 students need to be assigned shirts.
  (a) In how many ways can shirts be assigned? (Students can have the same color shirt.)
  (b) What if no two students can get the same color shirt?
  (c) What if the students line up, and students next to each other cannot get the same color?

Problem 13.24. 50 runners compete. How many possible outcomes are there when:
  (a) We care about the order of all finishers.
  (b) We are only interested in who gets gold, silver and bronze.
  (c) We only care about the top-10 finishers, who will qualify for the final.

Problem 13.25. Count the sleeping arrangements for 5 girls and 1 boy who stay over at a math contest in four rooms (max. two per room). Boys can't room with girls. (a) Rooms are identical? (b) Rooms are numbered $1, 2, 3, 4$?

Problem 13.26. You take two socks from a drawer with 50 different socks and put one on each foot. In how many ways can you do this? What if the drawer has 25 different *pairs* of socks?

Problem 13.27. In how many ways can 20 tennis players form 10 pairs for the first round of a tennis tournament?

Problem 13.28. A US Social Security number has 9 digits. The first digit may be zero.
  (a) How many SS numbers are there? How many are even? How many have only even digits?
  (b) How many are palindromes (e.g. 342151243)?
  (c) How many have no 8? How many have at least one 8? How many have exactly one 8?

Problem 13.29. In each case, count.
  (a) The stacks of 5 poker chips that can be made from 12 chips of different colors.
  (b) The stacks of 5 poker chips that can be made from 3 red chips and 9 blue chips.
  (c) The 7-letter words that have no two consecutive letters the same?
  (d) The 2-dozen bouquets that can be formed using red, pink, peach and white roses?
  (e) The subsets of $\{a, b, c, d, e, f, g\}$ that contain: (i) a and g (ii) a or g.
  (f) The ways to pick 10 books to read from you collection of 100 books.
  (g) The different 13-card bridge hands possible from a deck of 52 cards.
  (h) The ways to choose 3 pizza toppings from 11 available toppings?
  (i) The orders in which a travelling salesman can visit the 50 states?
  (j) The poker hands with a card in every suit?
  (k) The ways to misspell "triangle", assuming you started with "t".
  (l) The cell phone numbers (ten digits not starting with 0).
  (m) The graphs on the 6 vertices Ⓐ Ⓑ Ⓒ Ⓓ Ⓔ Ⓕ.
  (n) The graphs on the 6 vertices Ⓐ Ⓑ Ⓒ Ⓓ Ⓔ Ⓕ which have the edges Ⓒ–Ⓓ and Ⓓ–Ⓔ.
  (o) The graphs on the 6 vertices Ⓐ Ⓑ Ⓒ Ⓓ Ⓔ Ⓕ with 2 edges.
  (p) The boy-girl patterns in which 2 boys and 4 girls can stand in a circle (rotations of the same pattern are identical).
  (q) The ways ten distinguishible boys can join hands for a circle dance. (rotations of the same pattern are identical).
  (r) The ways 6 boys and 6 girls in a dance class can be partnered into boy-girl couples.
  (s) The binary 10×10 matrices in which the entries in row i sum to i.
  (t) The 10×12 matrices whose entries are ± 1 and the product of the entries in every row and column is -1. What about the number of 10×11 such matrices? Tinker.

Problem 13.30. Estimate the number of possible friendship networks with 10 people. What about 100 people?

Problem 13.31. A social network has 6 people Ⓐ Ⓑ Ⓒ Ⓓ Ⓔ Ⓕ. Adding up each person's friends gives 26. How many *different* graphs could represent this social network? (Graphs differ if they don't have the same edges.)

Problem 13.32. Alice (A) and Bob (B) repeatedly play a game. A wins 4 times and B wins 3 times. In how many ways can you arrange the outcome of the games so that at some point A and B were tied?

Problem 13.33. How many quadrilaterals can be formed with vertices as the points shown? How many are: (a) squares   (b) rectangles   (c) parallelograms   (d) trapezoids?
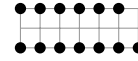
Problem 13.34. In how many ways can 50 students be split into 5 teams of ten for intramurals? *[Hint: Start small.]*

Problem 13.35. With 22 soccer players, in how many ways can you build two 11-person teams for a scrimmage? What if you had 32 players for an 11-on-11 scrimmage? Be careful. Tinker (start with two players).

Problem 13.36. In how many ways can Ayfos choose 6 bridesmaids, one of whom is maid of honor, from 15 friends?

Problem 13.37. A company's 5 executives and 15 employees have a golf outing.
  (a) In how many ways can one choose the 1st foursome that goes out onto the golfcourse?
  (b) In how many ways can one choose the 1st, 2nd, 3rd, 4th, 5th foursomes?
  (c) If an executive must be in each foursome, in how many ways can one choose the 1st, 2nd, 3rd, 4th, 5th foursomes?
  (d) If all that matters is who people play golf with, not when they play, in how many ways can we choose the foursomes?

Problem 13.38. An NBA team has 8 players. In how many ways can you choose 5 players to start the game?

Problem 13.39. There are 100 runners. In each case count the ways to construct the outcome.
  (a) The runners run a race and we are interested in the order in which they finish.
  (b) The runners run a race and we are interested in the order of the top-10 finishers.
  (c) The State-team which is the top-10 finishers of the race.
  (d) The State-team which is the top-10 finishers of the race with a captain and vice-captain from those top-10.
  (e) 10 end-of-season awards which are given to the runners (a runner may get more than one award).

Problem 13.40. Count 5-card poker: (a) Straights (multi-suit sequence)   (b) Straight flushes (one-suit sequence)?

Problem 13.41. WikiX has about 40 million articles (about 6 million in English). For a natural language processing task, you compute "edit distances" between all pairs of articles and store them in a symmetric 40million × 40million matrix of 64-bit double precision entries. About how much RAM is needed to store the distances between distinct pairs?
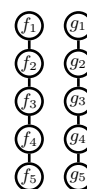
Problem 13.42. To determine if a graph G with 50 vertices is 3-colorable, you test all possible 3-colorings. Your computer checks a million 3-colorings per second. Estimate how long it is going to take, in the worst case.

Problem 13.43. A bank password card has 200 *different* strings of length 3 (right). Each string contains letters $A \cdots Z$ or digits $0 \cdots 9$. To login, the bank picks 4 *different* numbers (for example 1,40,22,181) and the user must input the strings corresponding to those numbers as the password (in the example: 'AQ1' '3E9' 'D1E' 'FEX').
  (a) Compute the number of different password *cards*.
  (b) For a fixed card, how many different passwords are there if:
    (i) The order of strings matters?   (ii) The order of strings does not matter?

Password Card		
1. AQ1	**21.** 3DE	$\cdots$ **181.** FEX
2. AAD	**22.** D1E	$\cdots$ **182.** Q7P
$\vdots$		
20. TR7	**40.** 3E9	$\cdots$ **200.** 0T4

Problem 13.44 (Counting genotypes and phenotypes). Here's a simple model for genetics. A person has two sets of 5 genes: father genes $f_1, \ldots, f_5$ and mother genes $g_1, \ldots, g_5$. A given gene-position is a trait (e.g. eye-color) and each gene can be one of four types (called alleles). For example, the eye-color gene could have alleles green, blue, brown, black. The alleles for gene 1 are $\{a_1, a_2, a_3, a_4\}$; the alleles for gene 2 are $\{b_1, b_2, b_3, b_4\}$; and so on. The entire genome is a list of 5 ordered pairs. For example, $(a_1, a_1)(b_3, b_2)(c_2, c_2)(d_2, d_3)(e_4, e_1)$ means the father-alleles are $a_1 b_3 c_2 d_2 e_4$ and the mother-alleles are $a_1 b_2 c_2 d_3 e_1$ (the father and mother genes can be the same allele). Your genes are your genotype.
  (a) How many different genotypes are there? What if father and mother genes are indistinguishable?
  (b) The phenotype is the physical expression of the genotype. If a single allele of a gene is present, that allele is the trait. If two alleles are present, the trait is a combination of the two, independent of which allele is the father's. For example: the trait for (a_1, a_1) is a_1; (a_1, a_2) and (a_2, a_1) have the same trait, some mix of a_1 and a_2. The phenotype is the list of traits expressed by each gene. How many different phenotypes are possible?

Problem 13.45. There are 7 flavors of donut and you must pick a dozen. There is a bijection between packages of 12 donuts and binary sequences of length 18 with _?fill in?_ 1's. More generally, for k types of donuts, there is a bijection between packages of n donuts and binary sequences of length _?fill in?_ with _?fill in?_ 1's.

Problem 13.46. There are 10 sundae toppings from which you select 4. How many sundaes are possible if:
  (a) You do not repeat a topping and the order in which the toppings are added does not matter to you?
  (b) You do not repeat a topping and the order in which the toppings are added matters to you?
  (c) You may repeat toppings and the order in which the toppings are added does not matter to you?
  (d) You may repeat toppings and the order in which the toppings are added matters to you?

Problem 13.47. Count the ways to split 20 identical $1-bills among 3 children? What if each child gets at least $2?

Problem 13.48. In Yahtzee you roll five 6-sided dice. How many rolls are possible (order does not matter)?

Problem 13.49. Unlike a set, a multiset may contain the same element many times (order does not matter). Using the numbers $\{1, \ldots, 20\}$, in how many ways can you form: (a) A *set* of size 5? (b) A *multiset* of size 5?
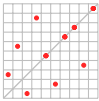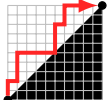
Problem 13.50. How many 7-digit phone-numbers are non-decreasing (each digit is not less than the previous one.)

Problem 13.51. How many functions $f : \{1, \ldots, 5\} \mapsto \{1, \ldots, 10\}$ are: (a) Strictly increasing? (b) Non-decreasing?

Problem 13.52. How many integer solutions are there to $x_1 + x_2 + x_3 + x_4 = 10$ if
  (a) x_i are positive?   (b) x_i are non-negative?   (c) $x_1 \geq -3, x_2 \geq -2, x_3 \geq 1, x_4 \geq 2$?

Problem 13.53. Solve with build-up counting. Tinker, tinker, tinker. Invent appropriate notation.
  (a) How many 20-bit binary strings contain 00 as a substring. *[Hint: Count strings not containing 00.]*
  (b) How many 10-digit numbers do not have 3 consecutive digits the same. *[Hint: Count those starting with a 0.]*
  (c) A word has one or more vowels (a,e,i,o,u). Vowels cannot be consecutive. How many 10 letter words are there?
  (d) How many of the 6 digit numbers 000000 through 999999 have digits which sum to 27?
  (e) In how many ways can 10 non-attacking castles be placed symmetrically about the diagonal on a 10×10 board. Castles are non-attacking if no pair is on the same row or column. In a symmetric arrangement, if there is a castle at (x, y) there must be one at (y, x).
  (f) How many outcomes of the roll of 4 distinguishible dice have a sum 16?
  (g) How many 10-vertex rooted binary trees (RBT) are there? (1 vertex: one; 2 vertices: two; 3 vertices: five)
  (h) The streets in a neighborhood form a rectangular grid. A child starts at home and walks to school which is 10 blocks east and 10 blocks north. How many shortest paths are there?
  (i) On a grid, how many "diagonally dominant" up-and-right paths are there from $(0, 0)$ to $(10, 10)$. A diagonally dominant path never drops below the line $y = x$, e.g. red path. Such paths remain in the white region of the grid, never dropping into the black region.
  (j) Integers z_1, z_2, z_3 satisfy $0 \leq z_1 \leq z_2 \leq z_3 \leq 10$. How many such sequences are there?
  (k) How many 20-bit binary strings have exactly six 1's and at least four consecutive 0's.
  (l) A binary string is prefix-heavy if every prefix has *more* 1s than 0s. How many 10-bit strings are prefix-heavy?
  (m) How many ways can 20 be represented as a sum of: (i) 5 non-negative integers. (ii) 5 positive integers.
  (n) Start at $(0, 0)$ on a grid and keep rolling two dice. If the roll is (i, j), move i steps right and j steps up. In how many ways can you reach the grid point $(9, 7)$?
  (o) How many subsets of $\{1, 2, \ldots, 20\}$ have a subset-sum which is divisible by 3?

Problem 13.54 (Stirling Numbers of the Second Kind). Let $A = \{a, b, c, d, e\}$.
  (a) In how many ways can one partition A into (i) two sets labeled S_1, S_2 (ii) three sets labeled S_1, S_2, S_3?
  (b) How many of the partitions in (a) have all sets in the partition being non-empty?
  (c) The ordered Stirling number $\begin{bmatrix} n \\ k \end{bmatrix}$ is the number of ways to partition n elements into k non-empty subsets labeled $S_1, \ldots, S_k$. What are: (i) $\begin{bmatrix} 1 \\ k \end{bmatrix}$ (ii) $\begin{bmatrix} n \\ 1 \end{bmatrix}$ (iii) $\begin{bmatrix} n \\ n \end{bmatrix}$ (iv) $\begin{bmatrix} 5 \\ 2 \end{bmatrix}$ (v) $\begin{bmatrix} 5 \\ 3 \end{bmatrix}$ (vi) $\begin{bmatrix} n \\ 2 \end{bmatrix}$?
  (d) Show $\begin{bmatrix} n \\ k \end{bmatrix} = k \left(\begin{bmatrix} n-1 \\ k \end{bmatrix} + \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} \right)$. *[Hint: Consider two cases, x_1 on its own and x_1 not on its own.]*
  (e) Repeat (a) and (b) for unlabeled (identical) subsets. So, $\{a, b\}\{c, d, e\}$ and $\{c, d, e\}\{a, b\}$ are the same partition.
  (f) The unordered Stirling number $\left\{ \begin{matrix} n \\ k \end{matrix} \right\}$ is the number of ways to partition n elements into k unlabeled (identical) sets. What are: (i) $\left\{ \begin{matrix} 1 \\ k \end{matrix} \right\}$ (ii) $\left\{ \begin{matrix} n \\ 1 \end{matrix} \right\}$ (iii) $\left\{ \begin{matrix} n \\ n \end{matrix} \right\}$ (iv) $\left\{ \begin{matrix} 5 \\ 2 \end{matrix} \right\}$ (v) $\left\{ \begin{matrix} 5 \\ 3 \end{matrix} \right\}$ (vi) $\left\{ \begin{matrix} n \\ 2 \end{matrix} \right\}$?
  (g) How is $\left\{ \begin{matrix} n \\ k \end{matrix} \right\}$ related to $\begin{bmatrix} n \\ k \end{bmatrix}$. Use the relationship to show $\left\{ \begin{matrix} n \\ k \end{matrix} \right\} = k \left\{ \begin{matrix} n-1 \\ k \end{matrix} \right\} + \left\{ \begin{matrix} n-1 \\ k-1 \end{matrix} \right\}$.
  (h) Use build-up counting to compute the number of ways to partition 10 senators into 5 non-empty named committees.

Problem 13.55. How many King-Queen positions are possible in Example 13.3 on page 186, without row/column restrictions. Here are two arguments. Which one is correct and why? How are the answers related?

  (i) There are 64 choices for the King and then 63 for the Queen. The product rule gives $64 \times 63 = 4032$ positions.

 (ii) We count the sequences $c_K r_K c_Q r_Q$ as in Example 13.3, but now without the restriction that $c_Q \neq c_K$ and $r_Q \neq r_K$. By the product rule there are $8 \times 8 \times 8 \times 8 = 4096$ positions.

Problem 13.56. Here are some counting problems on chessboards.

  (a) We highlighted different squares (at different locations or of different sizes) on an 8×8 chess board. How many squares are there? What if it was an $n \times n$ board.

  (b) In how many ways can m identical castles be placed on an $n \times n$ board so that no two are on the same row or column?
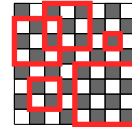
Problem 13.57. The Towers of Hanoi puzzle (Problem 7.64, page 99) has n disks on 3 bases A, B, C. Valid configurations have the disks on a base ordered from smallest on top to largest on the bottom. How many valid configurations are possible for:

  (a) Distinguishable bases A, B, C.   (b) Unlabeled, indistinguishible, bases.
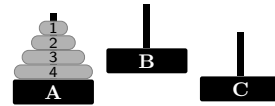
Problem 13.58. List the 2 and 3 element subsets of $\{1, 2, 3, 4, 5\}$. Pair each 2-subset with its complement (a 3-subset) to verify that there are an equal number of 2 and 3-subsets.

Problem 13.59 (Bank security). A bank has 5 VPs. No two VPs can have access to the vault. However, any 3 VPs can have access. How many vault-locks are needed and how should their keys be distributed among the VPs?

  (a) How many different pairs of 2 VPs are there? Call this number m

  (b) Suppose ℓ locks $L_1, \ldots, L_\ell$ suffice, with each person getting some subset of the ℓ keys. Prove that $\ell \geq m$.

   (i) Consider the VP-subsets $S_1, \ldots, S_m$. Prove that if the VPs in subset S_i combined their keys, they must be missing the key to at least one lock, call it $L(S_i)$. If they are missing the keys to multiple locks, pick one.

   (ii) Prove that the mapping $S_i \mapsto L(S_i)$ is 1-to-1. *[Hint: Contradiction: any 3 VPs can access the vault.]*

  (c) Prove that m locks suffice by showing how to distribute keys of the locks to the 5 VPs.

  (d) Generalize to n VPs where no subset of k has access to the vault but every subset of $k + 1$ can access the vault.

Problem 13.60. Compte these binomial expressions. Don't use the $\binom{n}{k}$ formula. Instead, reason about the meaning.

  (a) $\binom{6}{0}$ (b) $\binom{6}{9}$ (c) $\binom{6}{6}$ (d) $\binom{6}{1}$ (e) $\binom{6}{5}$ (f) $\binom{6}{4} - \binom{6}{2}$ (g) $\binom{10}{2}\binom{8}{4} - \binom{10}{4}\binom{6}{2}$ (h) $\binom{10}{6}\binom{6}{2} - \binom{10}{2}\binom{8}{4}$.

Problem 13.61. In Example 13.4 we proved the Binomial Theorem using counting. Prove it by induction.

  (a) Prove $(1+x)^n = \sum_{i=0}^{n} \binom{n}{i} x^i$ by induction on n. Hence, prove $(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}$. *[Hint: Pascal's identity.]*

  (b) Expand $(1+1)^n$ and $(1-1)^n$ and show (i) $\sum_{i=1}^{n} \binom{n}{i} = 2^n$ (ii) $\sum_{i=1}^{n} (-1)^i \binom{n}{i} = 0$.

Problem 13.62. What is the coefficient of x^3 in: (a) $(1+x)^6$.   (b) $(3-2x)^6$.   (c) $(2x+1)^{10} - (3-2x)^5$.

Problem 13.63. What are the coefficients of x^3, x^4, x^5, x^6, x^7 in the expansion of $(\sqrt{x} + 2x)^{10}$?

Problem 13.64 (Parity of $\binom{n}{k}$). Prove that $\binom{n}{k} \equiv 0 \pmod 2$ if n is even and k is odd. Otherwise (n is odd or k is even), show that $\binom{n}{k} \equiv \binom{\lfloor n/2 \rfloor}{\lfloor k/2 \rfloor} \pmod 2$. *[Hint: Consider the 4 cases for n and k being even/odd.]*

Problem 13.65 (Binomial Sums). Identify the valid ranges for the variables and prove each "Binomial Identity" using the formula for the Binomial coefficient, $\binom{n}{k} = n!/k!(n-k)!$. Use induction where appropriate.

  (a) Symmetry: $\binom{n}{k} = \binom{n}{n-k}$

  (b) Pascal's Identity: $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$

  (c) Absorbtion: $k\binom{n}{k} = n\binom{n-1}{k-1}$

  (d) Absorbtion: $\binom{k}{i}\binom{n}{k} = \binom{n}{i}\binom{n-i}{k-i}$

  (e) Sum: $\sum_{k=0}^{n} \binom{n}{k} = 2^n$

  (f) Alternating sum: $\sum_{k=0}^{n} \binom{n}{k}(-1)^k = 0$

  (h) First moment: $\sum_{k=0}^{n} k\binom{n}{k} = n2^{n-1}$

  (i) Upper sum: $\sum_{k=m}^{n} \binom{k}{m} = \binom{n+1}{m+1}$

  (j) Diagonal sum: $\sum_{k=0}^{n} \binom{m+k}{k} = \binom{m+n+1}{n}$

  (k) Vandermonde Convolution: $\sum_{k=0}^{\ell} \binom{n}{k}\binom{m}{\ell-k} = \binom{m+n}{\ell}$

  (l) Exponential Upper-Lower Sum: $\sum_{k=0}^{n} \binom{n+k}{k} 2^{-k} = 2^n$

Problem 13.66 (Combinatorial proofs). By counting objects in different ways, one can derive combinatorial relationships without knowing $\binom{n}{k}$. This can reveal important structure in a counting problem. Here is an example. A k-subset of n elements uniquely determines its complement subset with $n - k$ elements. This proves $\binom{n}{k} = \binom{n}{n-k}$ without using a formula for $\binom{n}{k}$. Give combinatorial proofs for each identity (Problem 13.65 asked for algebraic proofs).

(a) $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$. (To get a k-subset you either pick the first element or not.)

(b) $\sum_{i=0}^{n} \binom{n}{i} = 2^n$. (To get all subsets of an n-set, count subsets of size $0, 1, \ldots, n$.)

(c) $\sum_{i=k}^{n} \binom{i}{k} = \binom{n+1}{k+1}$. $\left(\begin{array}{l}\text{To choose } k+1 \text{ objects from } n+1, \text{ let the last object}\\ \text{chosen be at position } i+1, \text{ where } i \in \{k, k+1, \ldots, n\}.\end{array}\right)$

(d) $\sum_{i=0}^{n}(-1)^i\binom{n}{i} = 0$. $\left(\begin{array}{l}\text{For } S \subseteq X = \{x_1, \ldots, x_n\}, \text{ let } f(S) = S \cup x_1 \text{ if } x_1 \notin S \text{ and } S \setminus x_1\\ \text{otherwise. Show that } f \text{ is a bijection from even to odd-sized subsets.}\end{array}\right)$

(e) $k\binom{n}{k} = n\binom{n-1}{k-1}$. $\left(\begin{array}{l}\text{To choose a } k\text{-committee with a head: (i) Choose the committee and}\\ \text{a head from within; or, (ii) Choose the head plus } k-1 \text{ other members.}\end{array}\right)$

(f) $\binom{k}{i}\binom{n}{k} = \binom{n}{i}\binom{n-i}{k-i}$. (Generalize (e) to a k-committee with i executive members.)

(g) $\sum_{k=0}^{\ell} \binom{n}{k}\binom{m}{\ell-k} = \binom{m+n}{\ell}$. $\left(\begin{array}{l}\text{Choose } \ell \text{ hats from } m \text{ red and } n \text{ blue hats? Consider}\\ \text{separately 1 blue or 2 blue or, } \ldots, \text{ or } \ell \text{ blue hats.}\end{array}\right)$

Problem 13.67. Give a combinatorial proof of $k\binom{n}{k} = n\binom{n-1}{k-1}$ and show $\binom{n}{k} = \frac{n \times (n-1) \times (n-2) \times \cdots \times (n-k+1)}{k \times (k-1) \times (k-2) \times \cdots \times 2 \times 1}$.

Problem 13.68. Consider the k-subsets of $x_1, \ldots, x_n$ where the ℓth element of the k-subset is x_i (the first $\ell - 1$ elements are from $x_1, \ldots, x_{i-1}$ and the remaining $k - \ell$ elements are from $x_{i+1}, \ldots, x_n$).
(a) What are the possible cases for i? For a given i, how many such constrained k-subsets are there?
(b) Prove the combinatorial identity $\sum_{i=\ell}^{n+\ell-k} \binom{i-1}{\ell-1}\binom{n-i}{k-\ell} = \binom{n}{k}$, for $1 \le \ell \le k$.

Problem 13.69. Give a combinatorial proof for the summation in Problem 13.65(g), $\sum_{k=1}^{n} k\binom{n}{k} = n2^{n-1}$.
(a) Show that the number of length-n sequences of 0s, 1s and a single x is $n2^{n-1}$.
(b) Show that $k\binom{n}{k}$ sequences from (a) have $(k-1)$ 0s. Sum over $k = 1, \ldots, n$ to prove the claim.

Problem 13.70. The ith factorial power is $k^{\underline{i}} = k(k-1)\cdots(k+1-i) = k!/(k-i)!$. Prove: $\sum_{k=i}^{n} k^{\underline{i}}\binom{n}{k} = n^{\underline{i}}2^{n-i}$. Give the explicit formulas for $i = 1, 2$. *[Hint: Problems 13.66(e),(b).]*

Problem 13.71. Use a counting argument to prove the result in Problem 13.70 as follows.
(a) How many n-trit (**tri**nary di**git**) strings have k ones? How many n-trit strings have k ones and j twos?
(b) Show that $\binom{n}{k}2^{n-k} = \sum_{j=0}^{n-k} \binom{n}{j}\binom{n-j}{k}$. Show that this is equivalent to the result in Problem 13.70.

Problem 13.72. Prove that $\sum_{i=0}^{m} i^{\underline{k}}\binom{n+i}{i} = k!\binom{n+k}{n}\binom{n+m+1}{m-k}$, where the factorial power $i^{\underline{k}} = i!/(i-k)!$. Give explicit formulas for $k = 0, 1, 2$. *[Hint: Show $i^{\underline{k}}\binom{n+i}{i} = k!\binom{n+k}{n}$ and use the diagonal sum in Problem 13.65(j).]*

Problem 13.73. Let $A_1, \ldots, A_n$ be subsets of $X = \{1, 2, \ldots, M\}$ with no A_i a subset of another. Let $|A_i| = \ell_i$ and let E_i be the orderings of X in which the first ℓ_i elements are in A_i.
(a) Let $M = 4$, $A_1 = \{1, 4\}$ and $A_2 = \{1, 2\}$. What are E_1 and E_2? Show that $E_i \cap E_j = \varnothing$.
(b) Show that $|E_i| = \ell_i!(M - \ell_i)!$, and hence that $\sum_{i=1}^{n} \ell_i!(M - \ell_i)! \le M!$.
(c) Prove the Lubell-Yamamoto-Meshalkin inequality: $\sum_{i=1}^{n} 1/\binom{M}{\ell_i} \le 1$, and that it's tight.

Problem 13.74. Give three proofs that the product of n consecutive natural numbers is divisible by $n!$.
(a) Induction.   (b) Use the binomial coefficient $\binom{n+k}{k}$.   (c) Using the number of times a prime p divides $x!$.

Problem 13.75. In the generalized Binomial coefficient $\binom{r}{k}$ the upper index r can be real.

$$\binom{r}{k} = \frac{r(r-1)\cdots(r-k+1)}{k(k-1)\cdots 1} = \frac{r^{\underline{k}}}{k!} \qquad \text{(for integer } k \ge 0 \text{ and 0 otherwise).}$$

(a) When r is a positive integer n, show that you recover the regular Binomial coefficient $\binom{n}{k}$.
(b) When r is negative, prove the negation formula, $\binom{r}{k} = (-1)^k\binom{k-r-1}{k}$.
(c) Which identities in Problem 13.65 still hold for generalized Binomial coefficients?

193

Problem 13.76. A set of n integers sums to s. There are ℓ subsets each with sum less than $s/2$, and e subsets each with sum $s/2$. Show that $\ell + e/2 = 2^{n-1}$. *[Hint: Map subsets with sum $> s/2$ to those with sum $< s/2$.]*

Problem 13.77. How many rolls of 4 distinguishible dice sum to 6? *[Hint: Bijection to 9-bit sequences.]* What if the sum is 7? *[Hint: Sum rule.]* What if the dice are indistinguishible?

Problem 13.78. How many possible rolls are there for n distinguishible k-sided dice. What if the dice are indistinguishible? *[Hint: Bijection to binary sequences; see also Problem 5.66.]*

Problem 13.79. Show a bijection between 20-bit binary sequences with 10 ones and shortest paths on a grid from $(0,0)$ to $(10,10)$. Hence, compute the number of shortest paths from $(0,0)$ to $(10,10)$. Compare with Problem 13.53(e).

Problem 13.80. Let $P(m,n)$ be the number of shortest paths on a grid from $(0,0)$ to (m,n).
(a) Show: $P(m,n) = P(m-1,n) + P(m,n-1)$ for $m, n > 0$. What are $P(m,0)$ and $P(0,n)$?
(b) Give a bijection between the shortest paths and binary sequences of a particular type.
(c) Use your bijection to give a formula for the number of shortest paths from $(0,0)$ to (m,n).
(d) Prove, by induction, that your formula solves the recurrence derived in (a).

Problem 13.81. In the grid, ● is home, ● is work and ● is the grocery. Two shortest paths from ● to ● are in bold, one through the grocery and one not. All shortest paths from ● to ● make 8 steps.
(a) How many different shortest paths are there from ● to ●?
(b) How many shortest paths from ● to ● use ●? How many avoid ●?
(c) Repeat (a),(b) if ● moves to m steps right and n steps north of ●
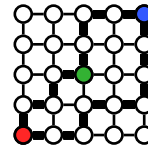
Problem 13.82. Prove that $\binom{n}{0}^2 + \binom{n}{1}^2 + \binom{n}{2}^2 + \cdots + \binom{n}{n-1}^2 + \binom{n}{n}^2 = \binom{2n}{n}$ in three different ways.
(a) Induction on n. *[Hint: Prove the stronger statement $\sum_i \binom{n}{i}\binom{n}{r-i} = \binom{2n}{r}$. Why is this stronger?]*
(b) Use $(1+x)^{2n} = (1+x)^n (1+x)^n$, and consider the coefficient of x^n on both sides.
(c) Count shortest paths on a grid from $(0,0)$ to (n,n) going through $(n,0)$ or $(n-1,1)$ ... or $(1,n-1)$ or $(0,n)$.

Problem 13.83. Tickets have 6 digit codes (000000 through 999999). How many codes have the sum of their first 3 digits equal to the sum of their last 3 digits? *[Hint: Bijection with codes that sum to 27. Problem 13.53(d).]*

Problem 13.84. A sequence is non-decreasing if $0 \le z_1 \le z_2 \le \cdots \le z_k \le n$. Count non-decreasing sequences using a bijection to non-negative solutions of $x_1 + x_2 + \cdots + x_k \le n$.

Problem 13.85. How many different rectangles are on a 5×4 grid (we shaded two).
(a) Carefully count the rectangles as a summation and evaluate your sum.
(b) We show 6 squares arranged vertically along the y-axis and 5 circles arranged horizontally along the x-axis. Show a bijection between sets containing two distinct squares and two distinct circles and the rectangles on the grid. Hence compute the number of rectangles and verify with (a).
(c) Give a formula for the number of different rectangles in the $m \times n$ grid.
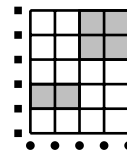
Problem 13.86. How many different triangles can be formed using line segments of the lines in the picture (no two lines are parallel, no three meet at a point). The vertices of the triangle must be intersection points of the lines. We show one such triangle in gray.
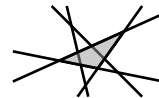
Problem 13.87. In how many ways can n knights sit on a round table. (Rotations of the same pattern are equivalent).

Problem 13.88. In how many ways can you choose k students from n students in a line in such a way that between every pair of choosen students, there are at least 2 students left behind. *[Hint: Bijection to binary sequences. Tinker.]*

Problem 13.89. A composition of n is a *sequence* of *positive* integers adding to n, e.g., $(6,4)$, $(4,6)$ and $(2,4,2,2)$ are different compositions of 10. Count the compositions of n.
(a) Tinker. If you see a pattern, make a guess and prove it by induction.
(b) Use a bijection between compositions and binary sequences to get the answer.
  (i) Consider the 9-bit sequence 001110100. Start a number at 1 and process the sequence from left to right. When you encounter a 0, start a new number at 1; when you encounter a 1, add 1 to the current number. We get the sequence $(1,1,4,2,1,1)$. Show that this procedure gives a composition of 10 for any 9-bit sequence.
  (ii) Prove that the procedure in (i) gives a composition of n for any $(n-1)$-bit sequence. Prove that the procedure is a bijection, and determine the number of compositions of n.

Problem 13.90 (Superpermutation). The sequence $s = aba$ is a superpermutation for the two distinguishible objects $\{a, b\}$ because every permutation of $\{a, b\}$ occurs in s as a substring.
   (a) Give superpermutations of shortest length for: (i) $\{a, b, c\}$ (length 9).   (ii) $\{a, b, c, d\}$ (length 33).
   (b) Prove that the shortest superpermutation of n objects has length between $n! + n - 1$ and $n \times n!$.

Problem 13.91. The number of diagonally dominant paths from $(0, 0)$ to (n, n) is the nth Catalan number C_n (see Problem 13.53(g)). Use bijection to compute C_n as follows. On the left is a non-diagonally dominantpath p. Such a path touches the line $y = x - 1$. The green dot is the first time the path contacts with $y = x - 1$.
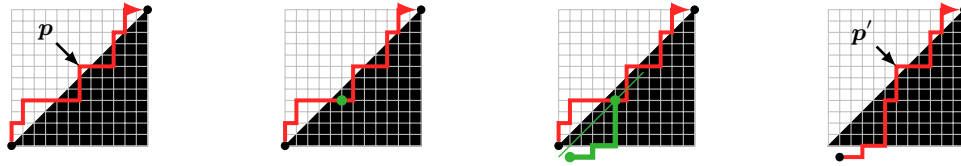
Reflect the path p *up to* the green dot using $y = x - 1$ as mirror (green) and then continue along p after the green dot, to get the path p' (rightmost figure). This path p' is a shortest path from $(1, -1)$ to (n, n).
   (a) Prove that our construction that maps p to the reflected p' is a bijection between the set of non-diagonally dominant paths from $(0, 0)$ to (n, n)) and the set of shortest paths from $(1, -1)$ to (n, n).
   (b) How many shortest paths are there from: (i) $(0, 0)$ to (n, n)?   (ii) $(1, -1)$ to (n, n)?
   (c) Show that the number of diagonally dominant paths from $(0, 0)$ to (n, n) is $C_n = \binom{2n}{n} - \binom{2n}{n-1} = \frac{1}{n+1}\binom{2n}{n}$.
   (d) Compute $C_1, C_2, \ldots, C_{10}$ and compare with Problem 13.53(g).

Problem 13.92. Let C_n be the number of ways to match n pairs of parentheses in the usual arithmetic sense (you never close an unopened parenthesis). For example "()()" and "(())" are matched but "())(" is not.
   (a) Compute C_3 and C_4, listing all the corresponding sequences of matched parentheses.
   (b) Prove: C_n is the nth Catalan number. *[Hint: Map to diagonally dominant paths: "(" moves up, ")" moves right.]*

Problem 13.93. Let C_n be the number of rooted binary trees on n vertices.
   (a) Compute C_3 and C_4, listing all the corresponding trees.
   (b) Prove: C_n is the nth Catalan number (cf. Problem 8.50). *[Hint: Use depth first search to map rooted binary trees to matched parentheses: when DFS moves down, open a parenthesis; when DFS moves up, close a parenthesis.]*

Problem 13.94 (Count Walks). A walker at $(0, 0)$ takes n steps right. At each step he moves up or down. If the walker hits the water at $y \leq -1$ (blue), he drowns: $y = -1$ is an absorbing barrier. Compute $Q(n)$, the number of paths that do not get absorbed.
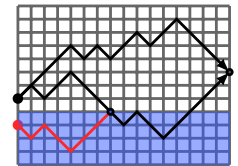
We show two black paths ending at $(n, 2)$. One is absorbed. We reflected the absorbed path about the barrier $y = -1$ up to when it first enters the blue region (red path). The red path plus the rest of the absorbed path gives a path from $(0, -1)$ to $(n, 2)$.
   (a) What is the smallest k_* for which there is a non-absorbed path to (n, k_*). How many up moves i_* are made?
   (b) How many paths are there from $(0, 0)$ to (n, k_*) in total (ignoring the absorbing river)?
   (c) How many paths are there from $(0, -2)$ to (n, k_*) in total (ignoring that these paths start in the river)?
   (d) Prove a bijection between absorbed paths from $(0, 0)$ to (n, k_*) and all paths from $(0, -2)$ to (n, k_*).
   (e) Show that the number of non-absorbed paths ending at (n, k_*) is $\binom{n}{i_*} - \binom{n}{i_*+1}$.
   (f) Show that the number of non-absorbed paths is $Q(n) = \binom{n}{\lceil n/2 \rceil} = n!/(\lceil n/2 \rceil! \lfloor n/2 \rfloor!)$.
   (g) Generalize to a barrier at $-b$. Show that $Q(n, b) = \binom{n}{x} + \binom{n}{x+1} + \cdots + \binom{n}{x+b-1}$, where $x = \lceil (n - b + 1)/2 \rceil$.

Problem 13.95. Counting walks with absorbing barriers, Problem 13.94, has many applications. In each case find a link between the objects in question and paths on a grid with an absorbing barrier. Then apply Problem 13.94.
   (a) Show that the number of n-bit sequences that are prefix-heavy (*more* 1s in every prefix) is $T_n = \binom{n-1}{\lceil (n-1)/2 \rceil}$.
   (b) Show that the number of n-bit prefix-heavy sequences ending in k zeros is $F_{n,k} = \binom{n-k-1}{\lceil (n-1)/2 \rceil}$, for $k \geq 1$.
   (c) Show that the number of ways to match n pairs of parentheses (Problem 13.92) is $C_n = \frac{1}{n+1}\binom{2n}{n}$.
   (d) Alice (A) and Bob (B) repeatedly play a game n times. A wins more times than B. In how many ways can you arrange the outcome of the games so that: (i) At some point A and B were tied? (ii) A is always ahead of B?

Problem 13.96. The 2nd-order polynomial in two variables x_1, x_2 is $a_0 + a_1 x_1 + a_2 x_2 + a_3 x_1^2 + a_4 x_1 x_2 + a_5 x_2^2$. There are 6 coefficients $a_0, \ldots, a_5$. How many coefficients are in the Qth-order polynomial with d variables?

Problem 13.97. Compute h_n, the number of perfect matchings in K_{2n}.
(a) Show $h_n = (2n-1)!! = (2n-1) \times (2n-3) \times \cdots \times 3 \times 1$. *[Hint: Show $h_n = (2n-1)h_{n-1}$.]*
(b) Construct a matching using consecutive pairs of vertices in a permutation of $1, \ldots, 2n$.
   (i) Show that $2^n n!$ different permutations give the same matching.
   (ii) Show $h_n = (2n)!/2^n n!$, and that this matches with (a). *[Hint: Multiplicity rule.]*

Problem 13.98. In how many ways can you choose a k-tuple of sets $\mathcal{S} = (S_1, S_2, \ldots, S_k)$, where $S_i \subseteq \{x_1, \ldots, x_n\}$ and $S_1 \cap S_2 \cap \cdots \cap S_k = \varnothing$. *[Hint: In how many ways can x_1 be placed into the sets? What about x_2? Product rule.]*

Problem 13.99. Prove Fermat's Little Theorem: when p is prime, $p|(a^p - a)$. For $a = 4$, $p|(4^p - 4)$. Consider a length-p sequence using 4 symbols a, b, c, d, e.g., $ababacd$ ($p = 7$). Joining the ends of a sequence gives a necklace. Multiple sequences can give the same necklace up to rotation. For $ababacd$, the duplicates are:

$ababacd$ $dababac$ $cdababa$ $acdabab$ $bacdaba$ $abacdab$ $babacda$

(All 7 sequences give the same necklace. Each successive sequence
is obtained by removing the last symbol and adding it to the front)

(a) Show that the number of sequences which contain more than one symbol is $4^p - 4$.
(b) You get up to p distinct sequences by repeatedly rotating the last symbol to the front. If you get fewer than p distinct sequences, show that one of the sequences is an integer repetition of some shorter sequence.
(c) Can a sequence with prime length and more than one symbol be repetitions of a shorter sequence? Explain.
(d) Prove that every distinct necklace with more than one symbol is created by p distinct sequences and hence there are $(4^p - 4)/p$ distinct necklaces with more than one symbol.
(e) Explain why you have proved Fermat's Little Theorem for $a = 4$. Generalize to arbitrary a.

Problem 13.100. In how many ways can 10 boys and 13 girls form a circle? (Rotations of the same pattern are equivalent.) *[Hint: $10 + 13$ is prime. The methods from Problem 13.99 might be useful.]*

Problem 13.101 (Cayley's formula and Prüfer codes). We show a labeled tree. Repeatedly remove the leaf with the lowest label, listing the labels of the removed leaf's neighbor.
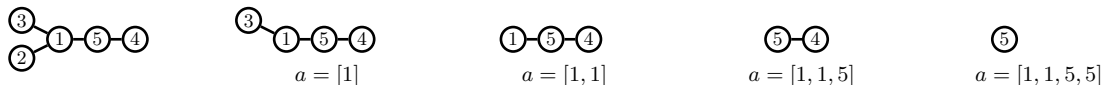
The sequence of neighbors of removed leafs is $a = [1, 1, 5, 5]$. This is the Prüffer code for the tree.
(a) Prove that the last entry in the Prüffer code must be n.
(b) Reconstruct the sequence of node removals b ($(b[i], a[i])$ are the edges). Start with $b = a$ and replace $b[1]$ with the smallest label not in b; then replace $b[2]$ with the smallest label not in b; and so on up to $b[n-1]$:

$$[1, 1, 5, 5] \quad \to \quad [2, 1, 5, 5] \quad \to \quad [2, 3, 5, 5] \quad \to \quad [2, 3, 1, 5] \quad \to \quad [2, 3, 1, 4].$$

(c) Prove that there are n^{n-2} labeled trees on n vertices. *[Hint: Bijection to Prüffer codes.]*

Problem 13.102. Show: there are $(n+1)^{n-1}$ labeled rooted forests on n vertices. *[Hint: Bijection from labeled trees on $n+1$ vertices to labeled rooted forests on n vertices by removing the root; Cayley's formula.]*

Problem 13.103 (Parking Functions). There are n parking spots $1, \ldots, n$ in a row and n cars $C_1, \ldots, C_n$ arrive in sequence. Car C_i prefers parking spot a_i, will drive up to spot a_i, park there if the spot is available or else park in the next available spot if one exists. The sequence $(a_1, \ldots, a_n)$ is a *parking function* if every car finds a spot. List all parking functions for $n = 2, 3$. Prove that the number of parking functions is $(n+1)^{n-1}$ as follows.
(a) Instead of parking in a row, consider the parking algorithm on a circle with one additional spot $n+1$, also allowing $a_i = n+1$. Now all n cars can park for any $(a_1, \ldots, a_n)$ and there will be one empty spot. Prove that $(a_1, \ldots, a_n)$ is a parking function for the original row with n spots if and only if spot $n+1$ is left empty on the circle.
(b) Prove, for the circle, that if $(a_1, \ldots, a_n)$ results in C_i parking at space p_i, then $(a_1 + j, \ldots, a_n + j) \pmod{n+1}$ results in C_i parking in space $p_i + j \pmod{n+1}$.
(c) For $i = 0, \ldots, n$, and any $(a_1, \ldots, a_n)$, prove that exactly one of $(a_1 + i, \ldots, a_n + i) \pmod{n+1}$ is a parking function for the row. That is, every row-parking function maps to $n+1$ distinct circle parking functions.
(d) How many circle parking functions are there? Prove the claim.

14.3　Problems

It is common practice to use $[n]$ as a shorthand for the set $\{1, 2, \ldots, n\}$.

Problem 14.1. How many different words can you form using the letters: (a) ABC　(b) AAA　(c) AARDVARK?

Problem 14.2. How many different words can you form using the letters:
(a) REARRANGE　　(b) BOOKKEEPER　　(c) DISCRETE　　(d) PARALLEL　　(e) SUCCESS　　(f) MISSISSIPPI.

Problem 14.3. Using the letters in the word PEPPERONI, how many different words are there:
(a) In all?　　(b) That begin and end with P?　　(c) That have all three P's together?

Problem 14.4. The word MISSISSIPPI is scrambled into two possibly nonsensical words, e.g. IPIM SSISSIP. How many such two word anagrams are there? The order of the two words matters.

Problem 14.5. In each case, determine the number of ways the task can be performed.
(a) 10 identical candies must be distributed among 4 children.
(b) A 15-letter sequence must be made up of 5 A's, 5B's and 5C's.
(c) 10 identical rings must be placed on your 10 fingers. (A finger can get more than one ring.)
(d) 3 red, 3 green and 3 blue flags are to be arranged in some order along the street for the parade.

Problem 14.6. For each word, alphabetically sort all words that can be formed from the letters. Give the word's rank (x out of y) in this alphabetic list. (a) TURING.　　(b) JACKASS.

Problem 14.7. Find the coefficients of x^3 and x^{17} in: (a) $(1 + \sqrt{x} + x + x^2)^{10}$　　(b) $(x^{1/2} + x^{3/2} + x^{7/2})^{10}$.

Problem 14.8. What is the coefficient of x^i in $(1 + 1/x + x)^n$? How is your answer related to $T_{n,i}$ in Problem 8.3?

Problem 14.9. A shelf holds up to 100 books. In how many ways can you arrange 100 books on 8 shelves?
(a) Find the number of ways if the order of the books on each shelf (i) matters　　(ii) does not matter.
(b) Repeat (a) if in addition each bookshelf must have at least one book.

Problem 14.10. A class has 25 boys and 25 girls. How many groups of 25 students have more girls than boys? What if there are 50 boys and 50 girls, how many groups of 50 have more girls than boys?

Problem 14.11. You can put any combination of 10 toppings on a pizza. You will make 3 pizzas.
(a) Show that there are 2^{10} different pizzas that are possible.
(b) Ifar says there are $(2^{10})^3/3!$ ways to make 3 pizzas. He argues as follows: each pizza has 2^{10} choices. Hence, by the product rule, for 3 pizzas, there are $(2^{10})^3$ ways. Since order does not divide this by the 3! orderings. You smelled a rat. What is the remainder when $(2^{10})^3$ is divided by 6. What's the problem?
(c) Explain in words Ifar's error. Find the correct answer. It will be $x/3!$. What is $\text{rem}(x, 3!)$?

Problem 14.12. In each case, count the number of objects/arrangements of the given type:
(a) n-letter words, if letters are used at most once. (26 letter alphabet.)
(b) n-letter words, if letters can be reused. (26 letter alphabet.)
(c) m different colored balls are in n distinguishible urns (an urn can have 0 to m balls).
(d) m identical balls are in n distinguishible urns (an urn can have 0 to m balls).
(e) m different colored balls are in n distinguishible urns, with at most one ball in each urn.
(f) US Social-Security numbers (see Problem 13.28) with digits in strictly increasing order.
(g) US Social-Security numbers with digits in non-decreasing order.

Problem 14.13. A campus with four majors has M students of which: 1,000 are in each major; 100 are in each double-major; 10 are in each triple-major; and, 1 is in all majors. What is M?

Problem 14.14. At XYZ-College, every student takes either the SAT or the ACT. If 79.7% of students take the SAT and 41% of students take the ACT, what percentage of students take both?

Problem 14.15. XYZ-College offers only CS and MATH majors. There are 70 students. 50 are CS majors and 50 are math majors. How many students are dual CS-MATH majors.

Problem 14.16. Two proof-readers A and B read a document. A finds a typos and B finds b typos. There were c typos in common. How many typos in all were found?

Problem 14.17. How many 8-bit sequences (a) begin or end in 1? (b) begin in 1 or have 101 starting at position 4?

Problem 14.18. Consider the binary strings consisting of 10 bits.
  (a) How many contain fewer 1's than 0's?
  (b) How many contain (i) 5 or more consecutive 1's   (ii) 5 or more consecutive 0's?
  (c) How many contain 5 or more consecutive 0's OR 5 or more consecutive 1's?

Problem 14.19. How many of the numbers $1, 2, \ldots, 1{,}000{,}000$ are:
  (a) Divisible by 2 or 5?   (b) Not divisible by 2,3 or 5?   (c) Divisible by 4 or 6?

Problem 14.20. A 5-card poker hand is monochromatic if all cards are the same color; it is a flush if all cards are the same suit. How many hands are either a flush or monochromatic?

Problem 14.21. Sets A, B, C have sizes $2, 3, 4$. What are the min and max for $|A \cup B \cup C|$?

Problem 14.22. $|A_1| = 115$, $|A_2| = 125$, $|A_3| = 120$, $|A_1 \cap A_2| = 70$, $|A_1 \cap A_3| = 75$, $|A_2 \cap A_3| = 80$, $|A_1 \cap A_2 \cap A_3| = 40$. Compute the number of elements: (a) Only in A_1. (b) Only in A_2. (c) Only in A_3. (d) In all.

Problem 14.23. Determine whether the following statements are true and if so, give proofs.
  (a) $|A \cup B| = |A| + |B|$ if and only if $A \cap B = \varnothing$.
  (b) $|A \cup B \cup C| = |A| + |B| + |C|$ if and only if $A \cap B \cap C = \varnothing$.
  (c) $|A \cup B \cup C| = |A| + |B| + |C|$ if and only if $A \cap B = \varnothing$ and $A \cap C = \varnothing$ and $B \cap C = \varnothing$.

Problem 14.24. Write out in full the inclusion-exclusion expansion of $|A_1 \cup A_2 \cup A_3 \cup A_4 \cup A_5|$.

Problem 14.25. Of 41 students in Algebra, Bio or Chem., the number failing each combination of courses is shown. How many passed all three courses?

A	B	C	AB	AC	BC	ABC
12	5	8	2	6	3	1

Problem 14.26. How many 7-digit telephone numbers are non-monotonic. A telephone number is monotonic if it's digits are either non-decreasing or non-increasing.

Problem 14.27. How many of the billion numbers $0, \ldots, 999999999$ contain a 1? Solve this problem in three ways:
  (a) Compute how many do not contain a 1 and subtract from ____?____?
  (b) Compute how many contain 1 one, 2 ones, ..., 9 ones and then ____?____?
  (c) Let $A_i = \{\text{numbers in which the } i\text{th digit is one}\}$. Compute $|A_1 \cup A_2 \cup A_3 \cup \cdots \cup A_9|$.

Problem 14.28. There are 10^k k-digit strings (digits can repeat). How many of those strings use each digit at least once? *[Hint: How many do not contain 1? How many do not contain 1 and 2?]*

Problem 14.29. You list the numbers from 0 to 9999999. How many times does a 1 appear in the list?

Problem 14.30. Count the integer solutions to $\sum_{i=1}^{6} x_i = 27$ satisfying $0 \le x_i \le 9$. Use these steps.
  (a) Find the number of solutions satisfying $x_i \ge 0$.
  (b) Let A_i be the solutions with $x_i \ge 10$. How is the answer you seek related to part (a) and $|A_1 \cup A_2 \cup A_3 \cup \cdots \cup A_6|$.
  (c) Compute $|A_1 \cup A_2 \cup A_3 \cup \cdots \cup A_6|$ using inclusion-exclusion and solve the problem. *[Hint: Show $|A_1 \cup A_2 \cup A_3| = 0$.]*
  (d) How is your answer related to Problem 13.53(d).

Problem 14.31. Use inclusion-exclusion to count the integer solutions to $x_1 + x_2 + x_3 = 20$ with $-2 \le x_1 \le 10$, $2 \le x_1 \le 8$ and $0 \le x_1 \le 15$.

Problem 14.32. w, x, y, z are non-negative integers satisfying $w + x + y + z \le 100$.
  (a) How many possible solutions are there for w, x, y, z?   (b) How many of those solutions have $x > 1$ OR $y > 1$?

Problem 14.33. A menu has three \$1-items. Count the ways to spend \$10. What if there's a limit of four per item?

Problem 14.34. How many passwords of length 8 have a lowercase letter, an uppercase letter and a special character. Passwords use letters $\{a,b,\ldots,z,A,B,\ldots,Z\}$, digits $\{0,1,\ldots,9\}$ or special characters $\{!,@,\#,\$,\%,\hat{~},\&,*,(,)\}$.

Problem 14.35. How many integers in $\{1, \ldots, 2015\}$ are not divisible by any of $\{8, 12, 20\}$. *[Hints: How many are divisible 8 or 12 or 20; inclusion-exclusion.]*

Problem 14.36. How many permutations of $\{1, 2, 3, 4, 5, 6\}$ contain any of the sub-sequences 12, 23 or 56?

Problem 14.37. How many numbers in $[1000]$ are divisible by (a) 2 or 4? (b) 2 or 5?

Problem 14.38. Pokemon have 4 digit serial numbers, e.g. 0255. A pokemon is defective if a digit is repeated (e.g. 0255 is defective). Approximate the fraction of defective serial numbers?

Problem 14.39. Count the shortest paths from $(0,0)$ to $(4,4)$ on a grid. Such pathes move up or right.
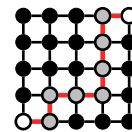 (a) Use build up counting. Let $P(n,m)$ be the number of paths from $(0,0)$ to (n,m). Show that
      $P(n,m) = P(n-1,m) + P(n,m-1)$.
  (b) What are $P(0,m)$ and $P(n,0)$?
  (c) Using (a),(b) compute $P(4,4)$, the number of paths from $(0,0)$ to $(4,4)$.
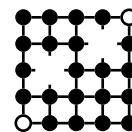 (d) Explain why $P(n,m) = \binom{n+m}{n}$.
A terrorist attack has taken out the two nodes $(1,2)$ and $(3,3)$, as shown.
  (e) Modify your build up counting to compute the number of paths from $(0,0)$ to $(4,4)$ that remain.
  (f) Use inclusion-exclusion to show that the number of paths remaining equals:

$$\binom{8}{4} - \binom{3}{1}\binom{5}{2} - \binom{6}{3}\binom{2}{1} + \binom{3}{1}\binom{3}{1}\binom{2}{1}$$

Problem 14.40. You roll 8 distinguishible dice. In each case, how many outcomes:
  (a) Don't contain a 1.   (b) Don't contain a 1 or 2.   (c) Contain all 6 numbers.*[Hint: Inclusion-exclusion.]*
How is your answer to (c) related to the onto functions from $[8]$ to $[6]$?

Problem 14.41. How many permutations of $\{1,\ldots,6\}$ keep: (a) One element fixed? (b) Two elements fixed?

Problem 14.42 (Derangements). The n people who checked in their hats each left with someone else's hat. Show that this can be done in: $D_n = n! \sum_{i=0}^{n} (-1)^i / i!$ ways. *[Hint: Use inclusion-exclusion for $|B_1 \cup B_2 \cup \cdots \cup B_n|$ where B_i contains the arrangements for which person i has his hat. The answer is $n! - |B_1 \cup B_2 \cup \cdots \cup B_n|$, why?]*
Prove the formula satisfies the derangement recursion: $D_1 = 0; D_2 = 1$ and $D_n = (n-1)(D_{n-1} + D_{n-2})$. (Induction.)

Problem 14.43. Recall the number of dearrangements of n objects, $D_n = n! \sum_{i=0}^{n} (-1)^i / i!$. Let $D_{n,k}$ be the number of arrangements of n objects so that k are in their correct position.
  (a) Prove that $\sum_{k=0}^{n} D_{n,k} = n!$.
  (b) Show that $D_{n,k} = \binom{n}{k} D_{n-k}$, hence $\sum_{k=0}^{n} \binom{n}{k} D_{n-k} = n!$. (A combinatorial proof.)
  (c) Show $\sum_{k=0}^{n} \binom{n}{k} D_k = n!$. *[Hint: Show $\sum_{k=0}^{n} \binom{n}{k} D_{n-k} = \sum_{k=0}^{n} \binom{n}{k} D_k$. Note $D_{n-k} \neq D_k$.]*
  (d) Use (a) and (b) to show that $\sum_{k=0}^{n} \sum_{\ell=0}^{n-k} (-1)^\ell / (k!\ell!) = 1$. (A combinatorial proof.)
  (e) Prove (d) by induction. *[Hint: Show $\sum_{k=0}^{n} \sum_{\ell=0}^{n-k} (-1)^\ell / (k!\ell!) = 1 + \sum_{s=1}^{n} 1/s! \sum_{k=0}^{s} \binom{s}{k} (-1)^k$.]*

Problem 14.44. Joey Goofit argues that to choose a k-subset from n elements, choose an r-subset, $r \geq k$, then a k subset from the r-subset. Hence, by the product rule, $\binom{n}{k} = \binom{n}{r}\binom{r}{k}$. Explain Joey's error. Give a combinarorial proof of the correct identity, $\binom{r}{k}\binom{n}{r} = \binom{n}{k}\binom{n-k}{r-k}$. *[Hint: Choose a team of r with k starters from n players in two ways: choose the team, then the starters; choose the starters, then the rest of the team. Explain why your proof works.]*

Problem 14.45. Prove that $(n!)^2$ divides $(n^2)!$. Prove it: algebraically (induction); combinatorially (multinomial coefficient); number theoretically *[Hint: number of times prime p divides $x!$].*

Problem 14.46. For a prime p, prove that $(n_1 + n_2 + \cdots + n_k)^p \equiv n_1^p + n_2^p + \cdots + n_k^p \pmod{p}$.
[Hints: Multinomial theorem. Show that, when p is prime, p divides $\binom{p}{i_1, i_2, \ldots, i_k}$ if $i_1, i_2, \ldots, i_k$ are all less than p.]

Problem 14.47. Use the Binomial Theorem and the identity $(1+x)^m (1+x)^n = (1+x)^{m+n}$ to prove the Vandermonde convolution identity in Problem 13.65(k), $\sum_{k=0}^{\ell} \binom{n}{k}\binom{m}{\ell-k} = \binom{m+n}{\ell}$.

Problem 14.48. A drawer has 10 red and 10 blue socks. What is the minimum number of socks you must pull out to guarantee: (a) getting a pair of the same color? (b) getting a pair of blue socks?

Problem 14.49. How many guests ensure that two are born in: (a) The same month? (b) May?

Problem 14.50. Pick any 51 different numbers from 1,...,100. Prove that two are consecutive.

Problem 14.51. For any 11 numbers, prove that two have a difference that is divisible by 10.

Problem 14.52. ID-number format is {uppercase letter}{2 bits}{uppercase letter}{2 decimal digits}, e.g. $J01E38$.
 (a) How many possible ID-numbers are there?
 (b) 40,000 students get IDs. At least how many of the student IDs must satisfy each criterion:
   (i) Have the same first letter?   (ii) Have the same first letter and last digit?   (iii) Start with J?

Problem 14.53. Bridge, Hearts and Majong each require 4 players to play. Ten students each know to play one of these three games. Prove that at least one of the games can be played.

Problem 14.54. You have 10 numbers $x_1, \ldots, x_{10}$ where $x_i \in [1, 104]$. Show that there are two distinct subsets of the numbers that have the same subset sum. **Challenge:** What about 9 numbers in $[1, 100]$?

Problem 14.55. A comparison scale which you can use at most twice can only compare weights.
 (a) You have 9 balls. One is heavier. Show how to determine which ball is heavier.
 (b) If you had 10 balls (one being heavier), prove that you cannot guarantee finding the heavier ball.

Problem 14.56. Let S be a set of $n + 1$ distinct numbers chosen from the set $\{1, 2, \ldots, 2n\}$.
 (a) Estimate the number of ways to choose S when $n = 100$. *[Hint: $\log n! = \sum_{i=1}^{n} \log i$.]*
 (b) Show that there are two numbers $x, y \in S$ with $\gcd(x, y) = 1$. *[Hint: $\gcd(k, k + 1) = 1$.]*

Problem 14.57. June has 30 days. I brushed my teeth 50 times in June, at least once each day. Show that there is a string of days $i, i + 1, i + 2, \ldots, i + k$ where I brushed my teeth exactly 14 times in total. *[Hint: Exercise 14.10(b).]*

Problem 14.58. Solve these problems using the pigeonhole principle, by identifying the right pigeons and pigeonholes.
 (a) How many students are needed to guarantee that at least two have the same first two initials.
 (b) A drawer has 43 white, 2 black, 23 blue and 8 red socks. How many socks must you grab to guarantee:
   (i) A matching pair?   (ii) A white pair?   (iii) A black pair?
 (c) The format of 250 million 10-digit phone-numbers is (aaa)-xxx-xxxx. How many area codes (aaa) are needed.
 (d) Five points are inside an equilateral triangle of side-length 2cm. Show that two points are at most 1cm apart.
 (e) A drawer has 1 sock of color C_1, 2 of color C_2, ..., 20 of color C_{20}. How many socks should you pull out to ensure getting at least 10 socks: (i) of one color   (ii) of color C_{20}.
 (f) For any 17 points inside an 8×8 square, show that at least two points are at most $\sqrt{8}$ apart.
 (g) Color points on the plane red or blue. Prove that two points of the same color are exactly 1 mile apart.
 (h) Let $n \in \mathbb{N}$. Prove that some multiple of n has only the digits 0 and 5. *[Hint: $5, 55, 555, \ldots \pmod{n}$.]*
 (i) Prove that some multiple of 2019 has only the digit 7 (a number of the form $7777 \cdots$).
 (j) 25 castles are placed on an 8×8 chessboard. Prove that 4 do not attack each other (castles on the same row or column attack each other). Arrange 24 castles so that no 4 are mutually non-attacking (prove it).
 (k) Pick any 101 numbers from the set $1, \ldots, 200$. Prove that some number is a multiple of another. *[Hint: Any number x has a unique representation $x = 2^k y$ where y is odd.]* (For a proof by induction, see Problem 5.41.)
 (l) Show that you can translate a 2-D shape S with area$(S) > 1$ so at least two of its points have integer coordinates.
 (m) For any set of n integers, there is a subset whose sum is divisible by n.
 (n) Eleven grid points in a 5×4 grid are colored green. Show that some rectangle on the grid has four green vertices.
 (o) In a friendship network with more than 200 people, everyone has at least 1 friend and no one has more than 100 friends. Show that at least 3 people have the same number of friends.
 (p) Six points are placed on a unit circle. Show that two are a distance at most 1 apart.
 (q) Using a comparison scale, you wish to measure any integer number of pounds of sugar from $1, 2, \ldots, M$. Prove that with k weights, $M \leq (3^k - 1)/2$. (Problem 5.52 shows how to achieve this bound.)
 (r) $x_1, x_2, \ldots, x_n$ is a permutation of $1, 2, \ldots, n$, where n is odd. Show that $(x_1 - 1)(x_2 - 2) \cdots (x_n - n)$ is even.
 (s) A 100-vertex graph has 1000 edges labeled $1, \ldots, 1000$. Show that edge labels increase along a path of length at least 20. *[Hint: Start tokens at each vertex. Process edges ordered by label, swapping the tokens along the edge.]*
 (t) Pick any 67 distinct numbers from $\{1, 2, \ldots, 99\}$. Prove that 3 numbers must be consecutive.

Problem 14.59. Find a bijection $f : \mathbb{N} \mapsto \mathbb{N}$ with $f(n) \leq n$ for all n and $f(n) < n$ for some n. *[Hint: Well-ordering; pigeonhole.]* ("No-free-lunch": lossless file compression that strictly compresses some files must expand others. ☹)

Problem 14.60. Prove that $\max(x_1, \ldots, x_n) \geq \mathrm{average}(x_1, \ldots, x_n)$. Hence, prove the pigeonhole principle.

Problem 14.61. Let $S = \{1, 2, \ldots, 2n\}$ and let $L \subset S$ be a subset of size $n + 1$.
(a) In how many ways can you select L. Simplify your answer using Stirling's approximation.
(b) Show that every choice for L contains two numbers that are relatively prime. [Hint: $(1, 2)(3, 4) \cdots (2n - 1, 2n)$.]
(c) Show that every choice for L contains two numbers with one being a multiple of the other.

Problem 14.62 (Bins with Capacities). Count the ways to place n indistinguishable balls into k bins with bin-capacity m balls ($n \leq mk$). Only the number of balls in each bin matters. Use inclusion-exclusion to show:

$$\# \text{ ways } = F(n, k, m) = \sum_{i=0}^{\lfloor k/(m+1) \rfloor} (-1)^i \binom{k}{i} \binom{n - i(m+1) + k - 1}{k - 1}.$$

[Hint: If A_i are ways for bin i to have more than m, $F(n, k, m) = \binom{n+k-1}{k-1} - |A_1 \cup A_2 \cup \cdots \cup A_k|$.]

Problem 14.63 (Generating Functions). Count integer solutions to $z_1 + z_2 + z_3 = 30$ where $0 \leq z_1 \leq 10$, $0 \leq z_2 \leq 15$ and $0 \leq z_3 \leq 20$.
(a) Pick z_1 as a term from $(x^0 + x^1 + \cdots + x^{10})$, z_2 from $(x^0 + x^1 + \cdots + x^{15})$ and z_3 from $(x^0 + x^1 + \cdots + x^{20})$. The polynomials are the generating functions for z_1, z_2, z_3. The generating function for the sum is the product,

$$G(x) = (x^0 + x^1 + \cdots + x^{10})(x^0 + x^1 + \cdots + x^{15})(x^0 + x^1 + \cdots + x^{20}).$$

Prove that the coefficient of x^{30} in $G(x)$ is the solution to the problem we seek.
(b) Prove that $G(x) = (1 - x^{11})(1 - x^{16})(1 - x^{21})(1 - x)^{-3}$.
(c) Let c_k be the coefficient of x^k in the expansion of $(1 - x)^{-3}$. Show that $c_k = (k + 1)(k + 2)/2$.
(d) Prove that the coefficient of x^{30} in $G(x)$ is $c_{30} - c_{19} - c_{14} - c_9 + c_3$. (Cf. Exercise 14.5(c))
(e) Solve the same problem with the constraints $-3 \leq x_1 \leq 7$, $2 \leq x_2 \leq 17$ and $1 \leq x_3 \leq 21$.

Problem 14.64. Let $Q(k, s)$ count the k-digit strings with digit-sum s. Find $Q(k, s)$ using a generating function.
(a) Pick each digit as a term from $(x^0 + x^1 + \cdots + x^9)$. Show that the coefficient of x^s in $G(x)$ is the answer, where

$$G(x) = (x^0 + x^1 + \cdots + x^9)^k.$$

(b) Show that $G(x) = (1 - x^{10})^k (1 - x)^{-k}$.
(c) Show that $(1 - x^{10})^k = \sum_{i=0}^{k} (-1)^i \binom{k}{i} x^{10i}$ and $(1 - x)^{-k} = \sum_{j=0}^{\infty} \binom{k+j-1}{j} x^j$, hence that

$$G(x) = \left(\sum_{i=0}^{k} (-1)^i \binom{k}{i} x^{10i} \right) \cdot \left(\sum_{j=0}^{\infty} \binom{k+j-1}{j} x^j \right).$$

(d) Find the coefficient of x^s in (c). Consider term i in the first sum and term $s - 10i$ in the second to show:

$$\text{coefficient of } x^s = \sum_{i=0}^{\lfloor s/10 \rfloor} (-1)^i \binom{k}{i} \binom{k + s - 10i - 1}{k - 1}.$$

(e) Relate (d) to Problem 14.62. Use (d) to compute $Q(6, 27)$. Compare with Problems 14.30 and 13.53(d).

Problem 14.65. How many subsets of $[n]$ have a sum divisible by 3. [Hint: $(1 + x)(1 + x^2) \cdots (1 + x^n)$.]

Problem 14.66. A walker at $(0, 0)$ takes n steps right. At each step she moves up, down or stays at the same level (trinomial walk). Contrast this with the (binomial) walker in Problem 13.94 who only moves up or down. The walker ends at position (n, i), $-n \leq i \leq n$? Hany different paths are possible? How is your answer related to Problem 14.7.

Problem 14.67. Here are some counting problems on graphs to challenge you. In each case count:
(a) Simple (no self-loops) graphs on n vertices that are (i) undirected (ii) directed.
(b) (i) Tournaments on n vertices. (ii) Tournaments on n vertices with no cycles [Hint: Problem 11.72.]
(c) Hamiltonian cycles in (i) K_n (ii) $K_{n,n}$.
(d) Perfect matchings in $K_{n,n}$.
(e) Spanning trees in (i) K_n [Answer: n^{n-2}] (ii) $K_{2,n}$ (iii) $K_{n,m}$.

15.5 Problems

Problem 15.1. In the context of this chapter, define, as carefully as you can:
  (a) Experiment.   (b) Sample Space.   (c) Probability Space.   (d) Event.   (e) Probability.

Problem 15.2. A sample space Ω has four outcomes: $\omega_1, \omega_2, \omega_3, \omega_4$. What is x in each case?
  (a) $P(\omega_1) = P(\omega_2) = P(\omega_3) = 1/10, P(\omega_4) = x$.   (b) $P(\omega_i) = i \times x$.

Problem 15.3. Which of these numbers cannot be a probability?
  $0, \quad 1, \quad 0.5, \quad 2/3, \quad 3/2, \quad -10^{-10}, \quad 10^{-10}, \quad 21\%, \quad 100\%, \quad \pi, \quad 1/\pi, \quad 1/\sqrt{2}, \quad \sqrt{2}-1.$

Problem 15.4. The mathematician D'Alembert was asked: "In two coin flips, what are the chances an H appears?" He reasoned: if the first flip is H, stop; otherwise flip again. In two of the three possible outcomes in $\{H, TH, TT\}$ an H appears, so his answer was $2/3$. What is wrong with D'Alembert's reasoning. What is the correct probability?

Problem 15.5 (Galton's Paradox). Flip 3 coins. What is the probability that all three coins match?

We argue that at least two coins *must* match (pigeonhole principle). The remaining coin is equally likely to be H or T, and so will match the two matching coins half the time. Hence, all three coins match half the time. Do you agree?

Problem 15.6. Roll a pair of fair dice. Compute these probabilities:
  (a) $\mathbb{P}[\text{sum exceeds 6}]$ (e) $\mathbb{P}[\text{sum exceeds 6 AND even}]$ (i) $\mathbb{P}[\text{sum exceeds 6 OR even}]$
  (b) $\mathbb{P}[\text{sum at most 6}]$ (f) $\mathbb{P}[\text{sum at most 6 AND even}]$ (j) $\mathbb{P}[\text{sum at most 6 OR even}]$
  (c) $\mathbb{P}[\text{sum is even}]$ (g) $\mathbb{P}[\text{sum exceeds 6 AND odd}]$ (k) $\mathbb{P}[\text{sum exceeds 6 OR odd}]$
  (d) $\mathbb{P}[\text{sum is odd}]$ (h) $\mathbb{P}[\text{sum at most 6 AND odd}]$ (l) $\mathbb{P}[\text{sum at most 6 OR odd}]$

Problem 15.7. In Problem 15.6, use sets to explain the relationship between the answers to part (g) and part (j).

Problem 15.8. Roll two dice. Compute the probability of: (a) One 6   (b) A sum of 6   (c) A sum divisible by 3.

Problem 15.9. Roll 3 dice. Compute the probability of: (a) No 1.   (b) No 2.   (c) No 1 or 2.   (d) At least one 1.

Problem 15.10. Flip a fair coin 4 times. Compute the probabilities of these events:
  (a) $A = \{\text{Equal number of H and T}\}$.   (b) $B = \{\text{First 2 flips are H}\}$.   (c) A AND B.   (d) A OR B.

Problem 15.11. You and a friend each flip two *fair* coins. Compute $\mathbb{P}[\text{you get \textit{more} heads}]$.

Problem 15.12. Roll a fair die 5 times. What is the probability: (a) some number repeats (b) you get no sixes?

Problem 15.13. How may fair die rolls repeats a number with probability at least: (a) 30%   (b) 50%   (c) 100%.

Problem 15.14. Over 1,000 days, 600 had rain, 400 had sunshine and 800 had either rain or sunshine. On a random day, find the chances of: (a) Rain and sunshine.   (b) Rain but no sunshine.   (c) Neither rain nor sunshine.

Problem 15.15. Among 400 students, 150 are in math, 120 are in bio and 50 are math-bio duals. What are the chances a random student is in: (a) math or bio   (b) bio and not math   (c) neither math nor bio?

Problem 15.16. A box contains 10 coins. 9 are *fair* and 1 has *two heads*. You pick a coin at random and flip it three times. What is the probability of flipping three heads (HHH)?

Problem 15.17. Two dice have probabilites $p_1, \ldots, p_6$ to roll $1, \ldots, 6$. Show: $\mathbb{P}[\text{doubles}] \geq 1/6$.

Problem 15.18. A bag has 2 blue, 2 red, 2 green and 2 pink balls. You randomly pick 4 balls. What is the probability that the number of different colors you get is (a) 4   (b) 3   (c) 2   (d) 1.
Repeat your calculations when you pick with replacement: after you pick each ball you replace it back into the bag.

Problem 15.19. Randomly throw 4 balls into 4 buckets. Each bucket can hold up to 2 balls. What is the probability that the number of non-empty buckets is: (a) 4   (b) 3   (c) 2   (d) 1. Use Monte-Carlo to verify your answers.

Problem 15.20. Three graduates throw their hats in the air. The hats fall randomly back to the graduates. Compute the probability that no graduate gets their hat back. What about if there were four graduates?

Problem 15.21. Four boys board a 4-seater bus with assigned seats. The first boy randomly sits. Thereafter each boy takes their assigned seat if possible, or else a random open seat. What are the chances the last boy gets his seat?

Problem 15.22 (Gift Exchange). Four guests place gifts for each other under the tree. The gifts are randomly assigned to guests. Compute the probability that: (a) No guest gets their gift back. (b) One guest gets their gift back.

Problem 15.23. Six cups are placed randomly on six saucers, two each of red, blue and green. What is the probability that no cup is upon a saucer of the same color?

Problem 15.24. Are these dice non-transitive? A: $\{$ 🎲 🎲 🎲 $\}$ B: $\{$ 🎲 🎲 🎲 $\}$ C: $\{$ 🎲 🎲 🎲 $\}$.

Problem 15.25. Three biased coins have a value on each side with corresponding probabilities to flip each value:

$$\text{coin } A = \left\{\begin{matrix} \mathbf{10} & \mathbf{2} \\ 0.6 & 0.4 \end{matrix}\right\} \qquad \text{coin } B = \left\{\begin{matrix} \mathbf{5} & \mathbf{4} \\ 0.6 & 0.4 \end{matrix}\right\} \qquad \text{coin } C = \left\{\begin{matrix} \mathbf{3} & \mathbf{20} \\ 0.6 & 0.4 \end{matrix}\right\} \qquad \begin{matrix} \leftarrow \text{values} \\ \leftarrow \text{probabilities} \end{matrix}$$

You and a friend each pick different coins and flip. The higher value wins. Do you want to pick first or second?

Problem 15.26. A class has 10 boys and 5 girls. Three children are picked randomly, one after another. Compute:

(a) The probability the first two are boys.   (b) The probability both sexes are represented.

Problem 15.27. 10 boys and 5 girls randomly line up. What are the chances a girl is last in line?

Problem 15.28. In 6-shooter Russian water-bullet-roulette, do you prefer to go first or second if:

(a) The bullet wheel is not respun for each shot.   (b) The bullet wheel is respun for each shot.

Problem 15.29. In the grid shown, 🔴 is home, 🔵 is work and 🟢 is the grocery. Two shortest paths from 🔵 to 🔴 are in bold, one goes through the grocery and one does not. All shortest paths from 🔵 to 🔴 have length 8. You randomly choose a shortest path from 🔵 to 🔴, with each shortest path being equally likely. What are the chances you can pick up groceries on your way home from work?
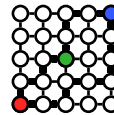
Problem 15.30. Answer Chevalier de Méré's 1654 problem: "Should you bet even money on the occurence of at least one 'double-six' during 24 rolls of a pair of dice?" What about 25 rolls?

Problem 15.31. Show that a six in 4 dice rolls is more likely than not. How about a double-six in 24 rolls of two dice? A double-six from 2 dice is 6-times less likely than a six from one die. Cardano's ($\sim$1525) *rule of proportion* says you need k times as many tries to get at least one success if your odds drop by a factor k, hence the 24 rolls of two dice in de Méré's gamble. Is Cardano's rule reasonable. Did Cardano's rule work for de Méré? If not, why?

Problem 15.32. Gamblers in de Méré's time had trouble dividing the stake in an incomplete gamble. Gamblers A and B each bet \$1. A coin is flipped repeatedly until 3 heads appear (A wins \$2) or 3 tails appear (B wins \$2). The game stops midway with the sequence of flips HHT. Suggest a way to fairly divide the \$2 between A and B.

Problem 15.33. 13-cards are dealt randomly from a standard 52-card deck. Compute probabilities to get one, two, three and four Aces. Use Monte Carlo to corroborate your answers.

Problem 15.34. Which randomly dealt 5-card poker hand (see Exercise 13.15 and Problem 13.40) should win:

(a) Four-of-a-kind or straight-flush?   (b) Straight or Three-of-a-kind?

Problem 15.35. Draw two cards randomly from a 52-card deck. Compute the probabilities:

(a) The first is a K and the second a picture (A, K, Q, J).   (b) At least one card is a picture.

Problem 15.36. Draw two cards randomly from a 52-card deck. Compute the probabilities:

(a) Both are ♠.   (b) One is ♠.   (c) One is ♠ and one is ♥.   (d) One is ♠ or one is ♥.

Problem 15.37. On the internet, the chances a packet transmission is successful (reaches the destination) is 60%. Compute the probability that more than 10 tries are needed to send a packet.

Problem 15.38. Eight pawns are placed randomly on different squares of a chessboard. Compute these probabilities.

(a) The pawns are in a straight line (including diagonals).   (b) No two pawns are in the same row or column.

Problem 15.39. You are stationed for 2 years in the Congo. If you take a monthly Malaria profilactic, the chances of Malaria that month in the Congo is 5%. What are your chances to get Malaria sometime during your stay?

Problem 15.40. A bag contains 10 identical envelopes each with some money. You and a friend randomly draw different envelopes. Do you want to go first or second, or does it not matter?

Problem 15.41. In a bag are 12 balls, 2 balls in each of 6 colors. You randomly pick 5 balls without replacement. Compute $\mathbb{P}[i]$, the probability that you get i colors in your sample, for $i = 1, \ldots, 6$.

Problem 15.42. Give the probability space for the outcome of each of these "experiments."
 (a) A fair coin is flipped and a fair die is rolled.
 (b) Pick a random lower-case letter from all written English text. What if you always pick the first letter of a word?
 (c) A bag contains numbers $1,\dots,20$. 5 numbers are randomly drawn without replacement.
 (d) A bag contains numbers $1,\dots,20$. 5 numbers are randomly drawn with replacement.
 (e) A pair of red and blue socks are in a drawer. You pick two socks out at random.
 (f) Six cups are placed randomly on six saucers, two each of red, blue and green.
 (g) A random 10-bit sequence is picked.
 (h) A 10-bit sequence is picked by randomly picking the first bit and repeating that bit 9 times.
 (i) A biased coin (probability p of H) is flipped 3 times.
 (j) A biased coin (probability p of H) is flipped until a H is flipped.
 (k) Randomly pick from $1,\dots,20$: (i) A number. (ii) An odd number. (iii) A prime number.
 (l) Roll a pair of identical dice. What if one die is red and the other is blue? What if you just record the sum?
 (m) An unfair die has $\mathbb{P}[6] = 1/2$ and other numbers are equally likely. Roll twice. What if you just record the sum?
 (n) Flip a coin until you get H. What if you only counted the number of flips?
 (o) There are 10 pizza toppings. You pick 3 toppings randomly for your pizza. Consider these cases.
       (i) A topping can be reused. (ii) A topping can't be reused (iii) Repeat if the order of toppings matters.
 (p) A knock-out tournament (e.g. Wimbledon) begins with 2^n players and has n rounds. The initial table of draws is specified: in the first round, player $2i-1$ draws player $2i$ for $i = 1,\dots,2^{n-1}$. The outcome of a match is random. Consider two cases: (i) Only the tournament winner matters.   (ii) The outcome of every match matters.
 (q) Each pair from {Adam, Barb, Charlie, Doris} randomly decides whether or not to be friends.

Problem 15.43. For a probability space (Ω, P) and any two events A and B, show:
 (a) If $A \subseteq B$ then $\mathbb{P}[A] \le \mathbb{P}[B]$.   (e) $\mathbb{P}[A \cup B] + \mathbb{P}[A \cap B] = \mathbb{P}[A] + \mathbb{P}[B]$.
 (b) $\mathbb{P}[A \cup \overline{A}] = 1$ and $\mathbb{P}[A \cap \overline{A}] = 0$.   (f) $\mathbb{P}[A \cup B] \le \mathbb{P}[A] + \mathbb{P}[B]$.
 (c) $\mathbb{P}[A \cap B] + \mathbb{P}[A \cap \overline{B}] = \mathbb{P}[A]$.   (g) If $\mathbb{P}[A] > 1/2$ and $\mathbb{P}[B] \ge 1/2$, then $\mathbb{P}[A \cap B] > 0$.
 (d) $\mathbb{P}[A \cap B] \le \min(\mathbb{P}[A], \mathbb{P}[B])$.   (h) $\mathbb{P}[A \text{ OR } B \text{ but not both}] = \mathbb{P}[A] + \mathbb{P}[B] - 2\mathbb{P}[A \cap B]$ (EXCLUSIVE-OR)

Problem 15.44. For events A and B, $\mathbb{P}[A] = 3/4$ and $\mathbb{P}[B] = 1/3$. Show that $1/12 \le \mathbb{P}[A \cap B] \le 1/3$. Give examples to show that both extremes are possible. Find corresponding bounds for $\mathbb{P}[A \cup B]$.

Problem 15.45 (Gossip). The probability space in Problem 15.42(q) defines friendships of 4 people. If someone hears a rumor, they tell it to their friends. Adam got a juicy piece of gossip. What are the chances Barb hears it?

Problem 15.46 (Random Permutation). On the right is an experiment, a randomized algorithm run on a list (a_1, a_2, a_3) which is initialized to $(1, 2, 3)$.
 (a) Give the probability space for this experiment.
 (b) Generalize the algorithm to a list of size n.
 (c) Prove that the probability space is uniform over the permutations of $1,\dots,n$.

```
1: for i = 1,...,3 do
2:     Randomly pick list position
       j from {i, i + 1,...,3}.
3:     Swap a_i with a_j.
```

Problem 15.47. A fair coin is flipped 20 times giving a sequence of H and T. Compute these probabilities:
 (a) The first H is at flip 20.   (b) The number of H and T are equal.   (c) Exactly two H.   (d) At least two H.

Problem 15.48. Two girls repeatedly roll an n-sided die. What are the chances the first to roll gets a 1 first?

Problem 15.49. A drunk leaves the bar at position 1, and takes random steps: left with probability $2/3$ or right with probability $1/3$. What is the probability the drunk reaches home (at position 0) before reaching the lockup (at position 3)?
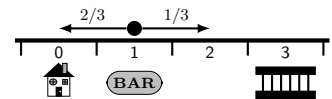
Problem 15.50. Three monkeys A, B, C have a 6-shooter pistol loaded with 2 bullets. Starting with A, each spins the bullet-wheel and shoots their foot. Compute probabilities p_A, p_B, p_C for each monkey to be the first shot.

Problem 15.51. You randomly throw 4 balls into 4 buckets. If a bucket has more than 2 balls, empty the buckets and restart. If all buckets have at most 2 balls, you stop. What is the probability that the number of non-empty buckets is:
 (a) 4   (b) 3   (c) 2   (d) 1.   (Use Monte-Carlo simulation to verify your answers.)

Problem 15.52. Repeatedly flip a fair coin. Show that any fixed sequence of H and T occurs with probability 1.

Problem 15.53. Repeatedly roll a die. What is the probability two 5s are rolled before four even numbers are rolled?

Problem 15.54. A random cut on a circular pizza picks two random points on the circumference and cuts along the chord joining the two points. You make two random cuts. What is the probability to get 4 pieces of pizza?

Problem 15.55. An urn has m blue and n red balls. Randomly pick balls one by one and lay them in a line. Show that the probability the first k balls are blue and the $(k+1)$st ball is red is

$$\binom{m+n-k-1}{n-1} \Big/ \binom{m+n}{n}.$$

(a) Prove the answer by justifying these steps:
   (i) In the outcome tree, $\mathbb{P}[\text{ball-1 is blue}] = m/(m+n)$ and $\mathbb{P}[\text{ball-1 is red}] = n/(m+n)$.
   (ii) We are only concerned with the branch where ball-1 is blue.
   (iii) From the "ball-1-blue" branch, $\mathbb{P}[\text{ball-2 is blue}] = (m-1)/(m+n-1)$.
   (iv) Continue by showing that the probability the first k balls are blue and the $(k+1)$st ball is red is

$$\frac{m}{m+n} \times \frac{m-1}{m+n-1} \times \frac{m-2}{m+n-2} \cdots \times \frac{m-k+1}{m+n-k+1} \times \frac{n}{m+n-k}.$$

   (v) Show that the answer in (iv) equals the desired answer.

(b) Use a uniform probability space. Label the blue balls $b_1, \ldots, b_m$ and the red balls $r_1, \ldots, r_n$.
   (i) Show that the number of ordrings of the labeled balls is $(m+n)!$.
   (ii) Show that the number of ways to choose the first k balls from $b_1, \ldots, b_m$, the $(k+1)$st ball from $r_1, \ldots, r_n$, and finally an ordering of the remaining balls is

$$\frac{m!}{(m-k)!} \times n \times (m+n-k-1)!.$$

   (iii) Hence, show the answer is $(m! \times n \times (m+n-k-1)!)/((m-k)! \times (m+n)!)$, as desired.

(c) Obtain the answer directly, again using a uniform probability space.
   (i) Show the number of arrangements of m blue and n red balls is $\binom{m+n}{n}$.
   (ii) Fix the first $k+1$ balls to k blue and 1 red. Show that the number of arrangements of the remaining $m+n-k-1$ balls is $\binom{m+n-k-1}{n-1}$ and conclude the anwer.

Problem 15.56. A bag has mk balls of k colors (m of each color). Randomly pick $n \leq mk$ balls without replacement. Show that the probability to get ℓ different colors ($\ell \leq \min(n, k)$) is

$$P(n, k, m, \ell) = \binom{k}{\ell} \frac{(m!)^\ell}{(mk)!} \sum_{\substack{n_1 + \cdots + n_\ell = n \\ 1 \leq n_i \leq m}} \binom{mk-n}{\delta_{n_1}, \delta_{n_2}, \ldots, \delta_{n_\ell}} \binom{n}{n_1, n_2, \ldots, n_\ell}$$

where $\delta_{n_i} = m - n_i$. Compute $P(n, k, m, \ell)$ for picking $n = 5$ balls when there are $k = 6$ colors and $m = 3$ balls of each color. Use Monte-Carlo simulation to verify your answer.

Problem 15.57. (**Inclusion-Exclusion**) Derive a formula for the probability of a union (similar to size of a union):

$$\mathbb{P}\left[\bigcup_{i=1}^n \mathcal{E}_i\right] = \sum_{k=1}^n (-1)^{k+1} \cdot (\text{sum of probabilities of all } k\text{-way intersections})$$

Problem 15.58. In the outcome-tree, we multiply edge probabilities to get the outcome-probabilities. Prove by induction that the resulting outcome-probabilities are a valid probability space, that is the probabilities sum to 1.

Problem 15.59. (**Principle of Restricted Choice**) Someone picks A or B in one of three settings.

   Setting 1. Their choice is *unrestricted* and they will pick randomly.

   Setting 2. Their choice is restricted to A.

   Setting 3. Their choice is restricted to B.

If A is picked, restricted choice says that setting 3 is ruled out and setting 2 becomes more likely (relative to setting 1). Not picking B suggests their choice was restricted to A. Use restricted choice to explain why switching is better in the Monty Hall game. (See also Problem 16.70. Restricted choice applies when some random action *may* have been under a constraint. If the action is consistent with the constraint, then the odds tilt toward the constraint being true.)

16.5   Problems

Problem 16.1. What is $\mathbb{P}[\text{Heads} \mid \text{Coin is flipped fairly}]$? (A conditional probability can be "obvious", yet not computable from the definition because the probabilities needed are not available.)

Problem 16.2. Planes are considered safer than cars: 5 deaths per billion miles driven versus 0.08 deaths per billion miles flown. Use conditioning to suggest ways to improve your driving odds.

Problem 16.3. On your friend's social media account, 80% of her posts are exciting. You conclude 80% of her life is exciting. You compare with your life and get depressed. What conditional probability trap did you fall into?

Problem 16.4. Professional researchers can easily fall into conditional probability traps. An IZA Institute of Labor Economics article "Health, Height and the Household at the Turn of the 20th Century" found that:

> In a study of British army recruits, the average height of British men (of average age of 20), was about 5 feet 6 inches (168 centimeters) at the turn of the century (1911), whereas British army recruits now (2014) stand on average at about 5 feet 10 inches (178 cm). The increase of 10cm can be attributed, most likely, to improved nutrition, health services and hygiene,...

It is reasonable to guess that British army recruits tend to be the taller and stronger members of society.
  (a) What conditional probability trap did the researchers fall into? Be specific.
  (b) For fixed army size and a larger population, will the average height of army recruits be larger or smaller?
  (c) For fixed population size, and a larger army, will the average height of the army recruits be larger or smaller?
  (d) The male population of England and Wales in 1911 was about 17,000,000 and in 2014 it was about 29,000,000. Meanwhile, the British armed forces dropped from about 500,000 in the 1900s to about 180,000 in 2014. Explain the results in the quoted study without relying on nutrition, health and hygeine? (Assume all recruits are men.)
  (e) Assume men have random heights from 140cm to 180cm (a better model would use a Bell curve). Use Monte Carlo to build a population of 17,000,000 men for 1911 and a separate population of 29,000,000 men for 2014. Build an army by starting from the tallest person and accepting them into the army with probability 5%, continuing with the next tallest person and so on until you get an army of the desired size.
   (i) Why do you start from the tallest person?
   (ii) Report the average height in each population and the average height of each army.

Conditioning killeth. Beware of convenient data in statistical studies rather than correct randomly sampled data.

Problem 16.5. Two worlds have 1 million birds each. World 1 has 100 black ravens and the rest are other birds. World 2 has 1000 black ravens, 1 white raven and the rest are other birds. You enter a randomly picked world.
  (a) What are the chances that all ravens are black in your world?
  (b) You see a random bird and it's a black raven. Now, what are the chances that all ravens are black in your world? (In this case, observing a black raven decreases your belief that "ALL ravens are black." See also Problem 3.60)

Problem 16.6. There are **5,000** students: **1,000** CS; **100** MATH; and, **80** dual CS-MATH. A randomly picked student is in CS or MATH. Compute the probability the student is in CS.

Problem 16.7. Chances are 6% a random day is a rainy Sunday. Today is Sunday. What are the chances of rain?

Problem 16.8. A bag has 3 red and 4 blue marbles. You draw two marbles.
  (a) What are the chances the second marble is red?
  (b) One of the marbles is red. What are the chances the second marble is red?
  (c) The first marble, it's red. What are the chances the second marble is red?

Problem 16.9. An urn has 10 black balls. A random number of balls are painted white.
  (a) Randomly pick 2 balls with replacement. What are the chances both are white?
  (b) Randomly pick 2 balls with replacement. What are the chances the second is white if the first is (i) white (ii) black?
  (c) Randomly pick a ball with replacement until it is white. It took two tries. Replace the ball and randomly pick a new ball. What is the probability it is white? What is your best guess for the number of white balls in the urn?
  (d) Describe Monte Carlo simulations you could run to verify your answers to (a), (b) and (c).

Problem 16.10. In "Let's Make a Deal," Monty prefers door-3 and will always open it when possible. If Monty opens door-3, should you switch or stay? What about if he opens door 2?

Problem 16.11. Flip 3 fair coins. At least one flip is heads. What is the probability at least two flips are heads?

Problem 16.12 (Galton's paradox). You fliped 3 fair coins and two match. The remaining flip matches those matching flips with probability $1/2$, hence $\mathbb{P}[3 \text{ match} \mid 2 \text{ match}] = 1/2$. Do you agree? What is $\mathbb{P}[3 \text{ match} \mid 2 \text{ match}]$?

Problem 16.13. Draw cards from a shuffled 52-card deck. What are the chances the 5th card drawn is the ♠A.

Problem 16.14. For events A and B, prove: (a) $\mathbb{P}[A \mid A \cup B] \geq \mathbb{P}[A]$ (b) $\mathbb{P}[A \mid A \cap B] = 1$.

Problem 16.15. Prove or disprove.
  (a) $\mathbb{P}[\overline{A} \mid B] = 1 - \mathbb{P}[A \mid B]$.   (b) $\mathbb{P}[A \mid \overline{B}] = 1 - \mathbb{P}[A \mid B]$.   (c) $\mathbb{P}[A \cup B] = 1 - \mathbb{P}[\overline{A} \mid \overline{B}]\mathbb{P}[\overline{B}]$.

Problem 16.16. Prove or disprove: $\mathbb{P}[A \mid B] = 1$ if and only if $B \subseteq A$.

Problem 16.17 (Conditioning and Inclusion-Exclusion). Prove or disprove.
  (a) $\mathbb{P}[A \cup B \mid C] = \mathbb{P}[A \mid C] + \mathbb{P}[B \mid C] - \mathbb{P}[A \cap B \mid C]$.   (b) $\mathbb{P}[A \mid B \cup C] = \mathbb{P}[A \mid B] + \mathbb{P}[A \mid C] - \mathbb{P}[A \mid B \cap C]$.

Problem 16.18. Bag 1 has two black balls, Bag 2 has a black and a white ball. Randomly pick a bag and randomly take a ball from it. The ball is black. What are the chances the second ball in the same bag is black?

Problem 16.19. Compute the probability the sum of two fair dice is even given the dice have different values.

Problem 16.20. We show the number of students taking various extracurriculars.
  (a) What are the chances Ayfos (a random student) is doing Ballet?
  (b) What are the chances Ayfos is in 6th grade?
  (c) What are the chances the 7th grader Need (i) Skates (ii) Does ballet or skates?
  (d) Baniaz is doing chess. What are the chances she's a 6th grader?

Grade	Chess	Ballet	Skating
6th	65	55	30
7th	85	55	70
8th	60	75	45

Problem 16.21. We show weekly texting patterns (number of students).
  (a) What are the chances Niaz has 21 or more texts?
  (b) What are the chances Niaz is in 11th grade?
  (c) Niaz is in 11th grade. What are the chances he has 50 or fewer texts?
  (d) Need has 50 or fewer texts. What are the chances he is in 11th grade?

	Number of texts		
Grade	$0 - 20$	21-50	Over 50
9th	25	55	30
10th	5	60	50
11th	1	40	70

Problem 16.22. We show blood groups versus race. O can donate blood to anyone; A can donate to A or AB; B can donate to B or AB; and, AB can donate only to AB. (O is a universal donor and AB a universal recipient.) You (a random person) are travelling in a land (Caucasia, Africa, Asia or South Asia) and are involved in an accident. You need a blood transfusion. A random local donor is picked.

Race	O	A	B	AB
Caucasian	9.5%	9%	2%	1%
African	9%	6.5%	4.5%	1.5%
Asian	13.5%	8%	5.5%	1.5%
South Asian	8%	6%	11.5%	3%

  (a) What are your chances of survival?
  (b) Give a table of your survival chances depending on your land of origin and the land you are travelling in.

Problem 16.23. A box has 6 fair and 4 two-headed coins. You pick a random coin, flip it, and get H. What is the probability you picked a fair coin, $\mathbb{P}[\text{fair coin} \mid \text{you got H}]$?

Problem 16.24. One-in-20 men and one-in-400 women are color blind. Assume an equal number of men and women.
  (a) You randomly pick a person. What is the probality they are color blind?
  (b) You randomly pick a person. They are color blind. What is the probability you picked a male?

Problem 16.25. Niaz must place 50 red and 50 blue marbles into two jars in any way he wishes, as long as both jars are non-empty. Baniaz will pick a jar randomly and then pick a marble from that jar. Niaz wins if Baniaz picks a red marble. How should Niaz distribute the marbles into the jars, and what is the probability that Niaz wins?

Problem 16.26. Kilam throws two darts at a dartboard. The second dart lands farther from the center than the first. What are the chances a third dart lands farther from the center than the first? (Kilam's skill stays constant.)

> Ayfos argues: Kilam throws 3 independent darts and the 3rd dart will be closer than the first only when the third dart is the best throw. Each dart has an equal chance of being the best throw, so the probability for the third dart to be the best throw is $1/3$. Hence, the third dart is worse than the first with probability $2/3$.

> Niaz argues: The second dart is irrelevant. All that matters is the first and third darts. The third dart has a 50-50 shot at beating the first one. So, the third dart will be worse than the first with probability $1/2$.

It's easy to come up with seemingly intuitive but wrong arguments. When in doubt, use the outcome-tree. Compute the correct probability and determine which (if any) of Ayfos and Niaz are correct. Give an intuition for your answer.

Problem 16.27. Randomly draw 5 cards from a 52-card deck and reveal one. Compute the probability of two aces if the revealed card is: (a) ♥A (b) an Ace   (c) ♥K (d) not an Ace?

Problem 16.28 (Spam). Spam is 40% of email. "Great deal" is in the subject of 1% of spam emails and 0.2% of non-spam emails. What are the chances an email with "Great deal" in the subject is spam. *[Hint: Bayes Theorem.]*

Problem 16.29. FOCS has sections A (20 female, 14 male) and B (14 female, 18 male).
  (a) What are the chances a random FOCS student is female?
  (b) What are the chances a random student picked from a random FOCS section is female?
  (c) What are the chances a randomly picked FOCS student who is female is in section A?

Problem 16.30. A storm produces hail 20% of the time. One-in-1000 storms is a mega-storm, producing hail 80% of the time. It is hailing. What are the chances that it's a mega-storm?

Problem 16.31. It rains half the time. If it's rains, chances of heavy traffic are 75% but otherwise 25%. In heavy traffic I am late for work, otherwise I'm late 50% of the time. I was late for work. What are the chances it's raining?

Problem 16.32. Randomly draw two balls from a bag with 3 black and 3 white balls. Compute these probabilities.
  (a) Ball 1 is black.   (b) Ball 2 is black.   (c) Balls 1 and 2 are black.   (d) Ball 2 is black if ball 1 is black.

Problem 16.33. At a house with two kids, you are ushered in by a girl. What are the chances both kids are girls?

Problem 16.34. Sally has two children. One is a son Mag. What are the chances Mag has a brother? Susie also has two children. You randomly meet one in the super-market, his name is Tom. What are the chances Tom has a brother?

Problem 16.35. Niaz, who has two children, either goes alone on a walk with probability $1/2$ or takes a random child. You met him walking with a boy. What are the chances he has two boys?

Problem 16.36. Baniaz has two kids. What are the chances both are girls in each of the situations below?
  (a) Baniaz confirms that one of her children is a girl.
  (b) Baniaz confirms one of her children is a girl named Leilitoon (a rare name, assuming names are randomly picked).
  (c) Baniaz confirms one of her children is a girl who was born on a Sunday.

Problem 16.37. A parent picks a boy's name as Beta with probability $0 < \beta < 1$. Baniaz has two children with different names. What is the probability Baniaz has two boys if:
  (a) Baniaz has a boy   (b) Baniaz has a boy named Beta   (c) Baniaz does not have a boy named Beta?

Problem 16.38. There are two beavers, brown and black. What are the chances both are male? What if you know:
  (a) one is male   (b) one is male and one is born on a Tuesday   (c) one is a male born on a Tuesday?
Verify answers with Monte Carlo simulation. How strange, the birthday of a beaver changes the probability of two males.

Problem 16.39. You are at door 1 in a 4-door version of the Monty Hall game. Monty opens a door as follows. He starts at door 2. He flips a fair coin. If the flip is H, he opens the door if it is empty. Otherwise, he moves up one door and repeats the process until he opens a door. (From door 4, he moves to door 2). You only see the final door opened, not the whole process. Find the optimal strategy and probability to win. (The strategy depends on the door opened.)

Problem 16.40. A bag has 3 coins: a 2-headed coin, a 2-tailed coin and a regular fair coin. Randomly pick a coin and place it on the table. You can see a heads facing up. What is the probability the side facing down is heads?

Problem 16.41. Cards with distinct values $v_1, \ldots, v_m$ are dealt in random order. The k'th card is largest among the cards already dealt. What is the probability it is the largest in the pack?

Problem 16.42. Cards are drawn randomly from a 52-card deck until a ♠ is drawn. What are these probabilities?
  (a) No ♥ have been drawn?   (b) No ♥ or ♢ have been drawn?   (c) No ♥, ♢ or ♣ have been drawn?
Verify your answers using a Monte Carlo. Report the exact and Monte Carlo results.

Problem 16.43. Five out of 100 coins are two-headed. You randomly pick a coin and flip it "fairly" twice (each side is equally probable). What is the probability to get (a) 2 heads   (b) 2 tails   (c) matching flips?

Problem 16.44. A box has 6 fair coins and 4 two-headed coins. You pick a coin randomly. What are the chances you picked a fair coin if (a) You flip and get H.   (b) You flip again and get H.   (c) You flip yet again and get H.

Problem 16.45. A box has three coins: fair, two-headed and two-tailed. You pick a random coin. What are the chances you have the two-headed coin if (a) You flip it and get H? (b) You flip the same coin again and get H?

Problem 16.46. Alice, Bob and Carol take turns rolling a die in the order $A, B, C, A, B, C, \ldots$. Compute the probability that A gets a 6 first, B second and C third.

Problem 16.47. A class has 10 boys and 5 girls. Three children are selected one after another. Compute the probability that the first two are boys if both sexes are represented.

Problem 16.48. A cab was in a hit and run accident at night. Two companies, Green and Yellow, operate cabs.
- 85% of the cabs in the city are Green and 15% are Yellow.
- A witness identified a Yellow cab. In dim light, a witness correctly identifies cab-color 80% of the time.

With no additional evidence, which cab company do you think is responsible and why?

Problem 16.49. In NYC, 1-in-50 people in a bar are born there. 3-in-4 people born in NYC and 1-in-10 people not born in NYC support the Yankees. What are the chances a NYC-bar-patron supporting the Yankees is born in NYC?

Problem 16.50. Students understand 80% of the material. On a 5-choice problem, a student who understands the topic gets it correct 95% of the time, and otherwise guesses correctly 20% of the time. Compute the probability that:
  (a) A student answers correctly?   (b) A student who answers correctly understands the topic?

Problem 16.51. A box has 10 coins, 9 are fair and 1 is two-headed. You pick a coin at random, flip it three times and get HHH. What is the probability that the coin you picked is fair?

Problem 16.52. One out of n coins is 2-headed. A random coin is picked and flipped k times. All flips were H.
  (a) What is the probability that the coin flipped is 2-headed.
  (b) For $n = 10^6$, how high should one pick k to be 99.9% sure the 2-headed coin was flipped?

Problem 16.53. Kilam and Liamsi take an oral exam. 20 questions are in a hat. Kilam can answer 10 of them. Each student draws a question from the hat (without replacement) and passes if they get it correct. Kilam argues with the professor that he must draw first to have a higher chance of getting a question he knows. If he draws second, then Liamsi might have already drawn one of the questions that he knows. Explain why Kilam is wrong using two methods:
  (a) Use a uniform probability space to compute Kilam's probability to get an A if he draws second.
  (b) Use total probability with two cases defined by whether or not Liamsi gets a question Kilam can answer.
(The professor says none of this matters anyway because students should be prepared to answer to all questions.)

Problem 16.54. Adam, Barb, Charlie and Doris each choose a random number in $\{1, 2, 3, 4, 5\}$. What are the chances that some pair chooses the same number? What if there are k people and n numbers?

Problem 16.55. In June 2015, 23 Fortune 500 companies listed women CEOs (4.6%). Since about 50% of people are women, this is evidence of gender bias in the workplace, when it comes to promoting women to CEO. That is,
$$\mathbb{P}[\text{NamedCEO} \mid \text{Woman}] \ \ll \ \mathbb{P}[\text{NamedCEO} \mid \text{Man}].$$
What is wrong with this reasoning? What is the correct reasoning?

Problem 16.56. In the random gossip network of Problem 15.45, what is the probability that Barb will hear Adam's gossip if Charlie and Doris are not friends?

Problem 16.57. 1 in 1000 drivers is driving drunk. The breathalyzer never fails to detect a drunk person, but is wrong 5% of the time on a sober person. On New Year's eve, there is a random sobriety checkpoint at which drivers are stopped randomly and given the breathalyzer. What are the chances that a driver who fails the brethalyzer is drunk? Is the brethalyzer test doomed? Explain why/how it's not so bad in practice.

Problem 16.58. Three monkeys A, B, C have a 6-shooter pistol loaded with two bullets. Starting with A, each takes turns spinning the bullet-wheel and shooting their foot. Compute the probabilities:
  (a) p_A, p_B, p_C that each monkey escapes unscathed.   (b) q_A, q_B, q_C that each monkey is the first to be injured.

Problem 16.59. A biased coin is flipped repeatedly. How likely is a run of m heads before a run of n tails?

Problem 16.60. Randomly pick a card from a well shuffled deck. What is the probability that:
  (a) The card is a king given it is a spade.   (b) The card is a spade given it is a king.

Problem 16.61. You randomly deal a 5-card poker hand from a 52-card deck (Exercise 13.15). What is the probability of a full house if the first two cards are queens? What if the first two cards are ♠Q and ♥Q in that order?

Problem 16.62. A plane has n seats assigned to n passengers, who randomly choose an available seat on boarding. What is the probability the last passenger gets her assigned seat? What if the first passenger chooses the wrong seat?

Problem 16.63. The US Social-Security Admin tracks survival probabilities that a newborn lives to a given age.

Age (years)	10	20	30	40	50	60	70	80	90	100	110	120
% Survivors (males)	99.2	98.7	97.5	95.9	92.8	86.0	73.5	50.3	17.4	0.9	0.001	0

For example, 86% of newborn males live to 60. For random 10, 30 and 50 year-olds,
  (a) Compute the probability that: (i) each lives to 80   (ii) each dies between 70 to 80.
  (b) For any survival curve, prove: $\mathbb{P}[\text{live till 80} \mid \text{lived till 17}] < \mathbb{P}[\text{live till 80} \mid \text{lived till 25}]$.

Problem 16.64. About 1 in a 1000 people have Coeliac disease. The test for Coeliac makes a mistake on 1 in 10 people who have it (90% accuracy if you have Coeliac) and on 1 in 100 people who do not have it (99% accuracy if you do not have Coeliac). You got tested, and the result was positive. What are the chances that you have Coeliac?

Problem 16.65 (Texas Holdem Poker). In Texas Holdem you get two cards, and then 5 more. You choose a hand of 5-cards from these seven cards. Your first two cards are the same rank. What are the chances you can make:
  (a) a flush?   (b) a full house?   (c) a four-of-a-kind?   (d) a straight?
What are the chances if, instead, your first two cards are of the same suit?

Problem 16.66 (Positive Predictive Value, PPV). The PPV of a medical test is the probability a random person has the condition if the test says YES. PPV quantifies how much you can trust the test.

$$\text{PPV} = \mathbb{P}[\text{person has medical condition} \mid \text{test says YES}].$$

Suppose a fraction p of the population has the condition and let $\gamma = p/(1-p)$ be the ratio of people with the condition to people without the condition. The true positive rate TP is the probability the test says YES if you have the condition; the false positive rate FP is the probability the test says YES if you do not have the condition. Show that

$$\text{PPV} = \frac{1}{1 + (FP/TP)/\gamma}.$$

The test is useful if $FP/TP \ll \gamma$. Doctors often don't tell you the PPV. Make sure to ask.

Problem 16.67 (Prosecutor's Fallacy). One person commits a crime in a town of 10,000 people. Everyone will take a lie-detector test. One person, Kilam, fails the lie-detector. Here are the properties of the lie-detector. If guilty, you fail 90% of the time. If not guilty, you pass 99.9% of the time. Prosecutor Paul argues:

  "Were Kilam innocent, he fails the lie detector **0.1%** of the time. So, beyond a reasonable doubt, he's guilty!"

  (a) What conditional probability trap did the prosecutor fall into?
  (b) Explain to Prosecutor Paul why he should compute $\mathbb{P}[\text{Person found is guilty} \mid \text{One person is found by lie-detector}]$.
  (c) Compute the conditional probability in (b) using the following steps.
      (i) Show that $\mathbb{P}[\text{One person is found by lie-detector}] = 0.9 \times (0.999)^{9999} + 0.1 \times 9999 \times 0.001 \times (0.999)^{9998}$.
      (ii) Show that the left term in the sum is $\mathbb{P}[\text{person found is guilty AND one person is found by lie-detector}]$.
      (iii) Show that $\mathbb{P}[\text{Person found is guilty} \mid \text{One person is found by lie-detector}] \approx 47\%$. That's reasonable doubt! The one person found as guilty is more likely to be innocent.
  (d) Repeat part (c) for a town with 100,000 people.
Moral: If you search for something among many, e.g. 10,000, you might "find" it, even when it's not there.

Problem 16.68 (Meiosis). Recall the genetics model in Problem 13.44. In meiosis, one set of genes (gamete) is produced from the father and mother-genes. Think of a biological robot or enzyme (blue square) which randomly picks one set of genes and one-by-one replicates each gene as it iterates through the set. The robot can get confused and randomly "crossover" to the other gene-set after transcribing k genes in the starting gene-set ($k = 1, \ldots, 5$). After crossing-over, the enzyme continues by transcribing the genes in the other gene-set. In the example, the crossover happens after f_2 and the resulting gamete is $f_1 f_2 g_3 g_4 g_5$.
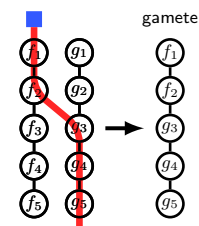
  (a) Assume a single crossover at a random location. Give the probability space.
  (b) What are $\mathbb{P}[f_1 \in \text{gamete}]$, $\mathbb{P}[f_2 \in \text{gamete}]$ and $\mathbb{P}[f_1 \in \text{gamete} \mid f_2 \in \text{gamete}]$?

Problem 16.69 (Simpson's Paradox). Approximate admissions data at a famous university are:

	Engineering		Humanities	
	# Applicants	#Admitted	# Applicants	#Admitted
Male	825	533	273	16
Female	108	81	352	34

(a) For a random applicant, compute $\mathbb{P}[\text{Admitted} \mid \text{Male}]$ and $\mathbb{P}[\text{Admitted} \mid \text{Female}]$. Is there a case for gender bias?

(b) Revisit the case for gender bias by considering the disciplines separately and computing:

$\mathbb{P}[\text{Admitted} \mid \text{Male Applying to Engineering}]$ $\mathbb{P}[\text{Admitted} \mid \text{Female Applying to Engineering}]$

$\mathbb{P}[\text{Admitted} \mid \text{Male Applying to Humanities}]$ $\mathbb{P}[\text{Admitted} \mid \text{Female Applying to Humanities}]$

(Simpsons paradox arises when you look at conditional probabilities by breaking into cases. The full and by-discipline conditional probabilities lead to opposite conclusions. Conditional probability is subtle. Our numbers are approximate. Nevertheless, our conclusions mimic the real-life investigation. The critical issue is why significantly fewer female students applied to engineering.)

Problem 16.70 (Principle of Restricted Choice). Kilam picks between the two choices A and B in one of three situations, and you do not know which situation Kilam is in.

1. His choice is unrestricted and he will pick randomly. (*A priori* probability p_1 for case 1.)
2. His choice is restricted to A. (*A priori* probability p_2 for case 2.)
3. His choice is restricted to B. (*A priori* probability p_3 for case 3.)

Suppose that he picks option A. Prove that the *a posteriori* probabilities are given by

$$p_1' = \frac{p_1}{p_1 + 2p_2}; \qquad p_2' = \frac{2p_2}{p_1 + 2p_2}; \qquad p_3' = 0.$$

(Situation 3 can't be and situation 2 is now twice as likely relative to situation 1 than it was, that is $p_2'/p_1' = 2p_2/p_1$.)

Problem 16.71. Use restricted choice to explain the difference between the cases of Ayfos and Need on page 228

Problem 16.72. A box has 6 fair coins and 4 biased coins with probability of heads $2/3$.

(a) Pick a single random coin and flip it 3 times. What is $\mathbb{P}[2 \text{ heads}]$?

(b) Flip 3 times, each time fliping a random coin and then replacing it. What is $\mathbb{P}[2 \text{ heads}]$?

Problem 16.73. A randomly shuffled 52-card deck is face down. At each step, you may take the top card (before seeing it) and stop, or reveal and discard the top card. You win if you take a red card. Otherwise you lose.

(a) If you decide to take the 1st card, what is the probabilty that you win?

(b) Prove that no strategy wins with higher probability. *[Hint: Prove a more general claim by induction: with k red and ℓ black cards, the maximum win probability is $k/(k + \ell)$.]*

Problem 16.74 (First Ballot Theorem (Bertrand, 1887)). Voters sequentialy vote randomly for A or B. Assume that $n = 2k + 1$ votes are cast (odd number). Show that the probability A was always ahead of B is:

(a) Δ/n if A wins by Δ votes. *[Hint: Problems 13.94 and 13.95(d).]*   (b) $2^{-2k}\binom{2k}{k} \approx 1/\sqrt{k}$ if A wins.

Problem 16.75. Alice, Barb and Claire each flip a fair die in that order until someone gets a 6 and wins. Compute the probabilities each player wins. Generalize to n players. Compute the probabilities $p_1, \ldots, p_n$ that each player wins.

Problem 16.76. A jar has one amoeba. Every minute, every amoeba turns into 0, 1, 2, or 3 amoebae, each with probability $1/4$ (dies, does nothing, splits in 2, or splits in 3). Assume that amoebae act independently. Compute the probability that the amoeba population eventually dies out. You may assume that the probability is strictly less than 1.

Problem 16.77. Alice and Bob take turns answering questions. The probability of a correct answer is α for Alice and β for Bob. Show that the probability Alice is first to answer correctly is

(a) $\alpha/(\alpha + \beta - \alpha\beta)$ if Alice goes first.   (b) $\alpha(1 - \beta)/(\alpha + \beta - \alpha\beta)$ if Bob goes first.

Give two derivations for each answer using: (i) The infinite outcome-tree method.   (ii) The law of total probability.

Problem 16.78. Alice and Bob play a tennis game. Alice wins a point with probability α. The first person to win at least 4 points with a margin of at least 2 points wins the game. What is the probability that Alice wins the game? Verify your result with Monte Carlo for $\alpha \in \{1/3, 2/5, 3/7, 4/9\}$. Report the fraction of wins in simulation for Alice.

Problem 16.79 (More efficient fair flip from biased coin). Recall Example 16.3 on page 232. We show another algorithm to get a fair flip from a biased coin. The algorithm may output a result after 2, 3, or 4 flips. In some cases, after 4 flips it restarts. Lower case 'h' and 't' are the flips of the coin, with the probability of 'h' being p. The algorithm keeps flipping until the output is either H or T. Show that

$$\mathbb{P}[\text{H}] = 1/2.$$

(a) Use the law of total probability.
(b) Sum probabilities on an infinite outcome-tree.
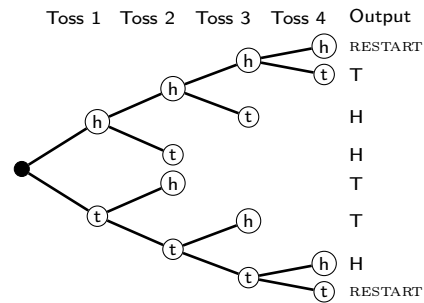
Problem 16.80. Teams A and B play in a world series. The winner is the first to win 4 games. Joe has $\$1024$ and wants to place an even money bet on A to win the series. If A wins the series, he gets back $\$2048$, otherwise $\$0$. One can only place even money bets on individual games. Find a way for Joe to simulate his bet on A to win the series.

Problem 16.81 (Clinical tests). Chances are 80% that an untreated person gets acne during a month's observation. Chances are 40% an acne drug works. If the drug works, 90% of acne cases are suppressed. Patients arrive (one per month), are randomly either given the drug (treated group) or not (control group), and then observed for a month.

(a) What are the chances the first patient to develop acne is a control patient?
(b) What are the chances the drug works if the first patient to develop acne is a control patient?
(c) What are the chances the drug works if the first patient to develop acne is a treated patient?

Problem 16.82 (Monte Carlo Roulette). A roulette wheel has a zero 0 (green) and the numbers $1, \ldots, 36$ half of which are red and the other half are black. You bet on red and the wheel is spun coming to rest on a number. The game is summarized in the algorithm to the right. Use the law of total probability to compute the probability that you win.

1: Spin: red wins; black loses; 0 goes to HOLD.
2: If you're in HOLD, spin:
   red wins; black loses; 0 goes to JAIL.
3: If you're in JAIL, spin:
   red goes back to hold (step 2); black or 0 loses.

Problem 16.83. A fair 5-sided die generates a number in $\{1, 2, 3, 4, 5\}$ with probability $1/5$ each. Give, with proof, an algorithm to simulate a fair 7-sided die which generates a number in $\{1, 2, 3, 4, 5, 6, 7\}$ with probability $1/7$ each.

Problem 16.84. Continually flip a biased coin with probability of heads p. Show that the probability for the first head to occur on an even numbered flip is $(1 - p)/(2 - p)$.

(a) Use the outcome-tree method (infinite probability space).   (b) Use the law of total probability.

Problem 16.85. To fairly decide which of three children A, B, C will inherit his throne, a king flips a fair coin until either HH or TT appear. If HH appears on an even flip, A inherits. If TT appears on an even flip, B inherits. If HH or TT appear on an odd flip, C inherits. Is the king's process fair?

Problem 16.86. Show that the algorithm in Example 16.3 makes $2k$ flips with probability $2p(1-p)(p^2 + (1-p)^2)^{k-1}$.

Problem 16.87. Flip twice a biased coin with heads-probability p. HH is a win, TT is a loss, and otherwise restart. Find the win-probability.

Problem 16.88. Dirty Harry and Ugly Sam play two-bullet Russian Roulette: a 6-cylinder revolver is randomly loaded with two bullets and the cylinder is spun. Ugly Sam and Dirty Harry take turns shooting their big-toe until someone gets hurt. This is what you do if you fail FOCS and drop out. The cylinder moves one shell forward after each shot.

(a) What is the probability that Ugly Sam is shot on the first trigger-pull?
(b) What is the probability that Dirty Harry is shot on the second trigger-pull?
(c) What is the probability that Ugly Sam is the one to get hurt.
(d) The bullets are loaded into consecutive shells before spinning. Repeat parts (a)-(c).

Problem 16.89. Let P_n be the probability of at least 2 heads in n fair coin flips.

(a) What is P_2? What is the probability of no heads in n coin flips?
(b) Use the law of total probability to show that $P_n = (P_{n-1} + 1)/2 - 2^{-n}$ for $n > 2$.
(c) Prove by induction that $P_n = 1 - (n + 1)2^{-n}$.   (Binomial distribution, see Chapter 18).

Problem 16.90 (Total Probability for More than 2 Cases). Events $C_1, \ldots, C_k$ are a partition of Ω if no two can co-occur and at least one must occur ($\cup_{i=1}^{k} C_i = \Omega$ and $C_i \cap C_j = \varnothing$).

(a) If $C_1, \ldots, C_k$ are a partition of Ω, show that $C_1 \cap A, \ldots, C_k \cap A$ are a partition of A.

(b) Prove the Law of Total Probability for the k "cases" in a partition $C_1, \ldots, C_k$ of Ω:
$$\mathbb{P}[A] = \sum_{i=1}^{k} \mathbb{P}[A \mid C_i] \cdot \mathbb{P}[C_i] = \mathbb{P}[A \mid C_1] \cdot \mathbb{P}[C_1] + \cdots + \mathbb{P}[A \mid C_k] \cdot \mathbb{P}[C_k].$$

Problem 16.91. Use the law of total probability to solve these problems.

(a) Repeatedly roll two fair dice. What is the probability to roll a sum of 6 before a sum of 8. Give some intuition.

(b) Repeatedly roll two fair dice. What is the probability to roll a sum of 6 before a sum of 10.

(c) Repeatedly roll two fair dice. What is the probability to roll a sum of 12 before rolling two consecutive sums of 7.

(d) Repeatedly flip a biased coin with probability of heads p. Show that the probability to observe two consecutive H before two consecutive T is $p^2(2 - p)/(1 - p(1 - p))$.

Problem 16.92. Prove formulas for a "conditional" law of total probability,

(a) $\mathbb{P}[A \cap C \mid B] = \mathbb{P}[A \mid B \cap C] \cdot \mathbb{P}[C \mid B]$

(b) Suppose $C_1, \ldots, C_k$ are a partition of Ω. Prove that
$$\mathbb{P}[A \mid B] = \mathbb{P}[A \mid B \cap C_1] \cdot \mathbb{P}[C_1 \mid B] + \cdots + \mathbb{P}[A \mid B \cap C_k] \cdot \mathbb{P}[C_k \mid B].$$
(Weight each of k cases C_i and B by the probability of C_i given B and add.)

Problem 16.93. Suppose $C_1, \ldots, C_k$ are a partition of Ω. Prove or disprove:
$$\mathbb{P}[A] = \mathbb{P}[A \mid B \cap C_1] \cdot \mathbb{P}[C_1 \cap B] + \cdots + \mathbb{P}[A \mid B \cap C_k] \cdot \mathbb{P}[C_k \cap B].$$
$$\mathbb{P}[A \mid B] = \mathbb{P}[A \mid B \cap C_1] \cdot \mathbb{P}[C_1 \cap B] + \cdots + \mathbb{P}[A \mid B \cap C_k] \cdot \mathbb{P}[C_k \cap B].$$
$$\mathbb{P}[A \text{ AND } B] = \mathbb{P}[A \mid B \cap C_1] \cdot \mathbb{P}[C_1 \cap B] + \cdots + \mathbb{P}[A \mid B \cap C_k] \cdot \mathbb{P}[C_k \cap B].$$

> **Build-up Probability.** When it's hard to get a formula, you can often compute a probability by starting simple and building up just as we did in build-up counting.

Problem 16.94. Let $Q(n)$ be the probability of an even number of heads in n coin flips with probability p of heads.

(a) What are $Q(1), Q(2), Q(3)$? Show that $Q(n + 1) = p + (1 - 2p)Q(n)$.

(b) When $p = 1/2$, what is the solution to this recurrence?

(c) Prove by induction that $Q(n) = (1 + (1 - 2p)^n)/2$. (To solve recurrences, see for example Problem 8.43.)

Problem 16.95. Find the probability of no HH in 20 fair coin flips. Let $Q(n)$ be the probability of no HH in n flips.

(a) What are $Q(1), Q(2), Q(3)$ and $Q(4)$? Show that $Q(n) = Q(n - 1)/2 + Q(n - 2)/4$.

(b) Use the recurrence to compute $Q(20)$. How is the answer related to Problem 13.53(a)?

(c) Prove that $Q(n) = (\phi_+^n - \phi_i^n + (\phi_+^{n-1} - \phi_-^{n-1})/4)/(\phi_+ - \phi_-)$, where $\phi_\pm = (1 \pm \sqrt{5})/4$.
   [Hints: Induction; show $4\phi_\pm^2 = 2\phi_\pm + 1$.]

(d) Generalize these results to the case when the coin is biased with probability p of H.

Problem 16.96. On Mars, girls are twice as likely as boys. A Martian couple has children until two boys *in a row*. Find the probability to have 20 children. *[Hint: Let $R(n) = \mathbb{P}[n \text{ children}]$. Relate $R(n)$ to $Q(n)$ in Problem 16.95(d).]*

Problem 16.97. Let $B(n, k)$ be the probability of k heads in n flips of a biased coin with probability p of heads.

(a) What are $B(1, 0), B(1, 1), B(2, 0), B(2, 1), B(2, 2)$?

(b) Show that $B(n, k) = pB(n - 1, k - 1) + (1 - p)B(n - 1, k)$. Use this recursion to construct a triangle like Pascal's Triangle for $B(n, k)$ with $p = 1/3$. What is $B(10, 4)$ for $p = 1/3$?

(c) When $p = 1/2$, what is the solution to this recurrence?

(d) Prove by induction that $B(n, k) = \binom{n}{k} p^k (1 - p)^{n-k}$.   (Binomial distribution, see Chapter 18).

Problem 16.98. Flip a coin with heads-probability p until you get TT. Find P_n, the probability to flip n times.

(a) What are P_2 and P_3? Use total probability to show: $P_n = pP_{n-1} + p(1 - p)P_{n-2}$ for $n > 2$.

(b) Solve the recurrence and show $P_n = a(\phi_+^{n-1} - \phi_-^{n-1})$. (What are a, ϕ_+, ϕ_-?) Verify with Monte Carlo simulation.

Problem 16.99. You keep flipping a coin and score 1 point for each H and 2 points for each T. Compute the probability that you will at some point have a total score of 20.

(a) Let P_n be the probability that your score will hit n. What are P_0, P_1, P_2?

(b) Explain why $\mathbb{P}[\text{score} = n \text{ OR score} = n + 1] = 1$.

(c) Use (b) to show that $1 = P_n + P_{n+1} - \mathbb{P}[\text{score} = n \text{ AND score} = n + 1]$, and hence prove $P_{n+1} = 1 - P_n/2$.

(d) Compute P_{20}, and verify with Monte Carlo simulation.

(e) Solve the recursion and obtain a formula for P_n, and verify with Monte Carlo simulation. *[Hint: Problem 8.49]*.

Problem 16.100. Start with \$5 and flip a biased coin up to 20 times (probability of H is p). On each flip, you may bet an integer number of dollars up to how much money you have. On the first flip you may bet $0, 1, \ldots, 5$ dollars. If you flip H, you win the amount bet. If you flip T, you lose the amount bet. You target is \$20 and hence you wish to maximize the probability to have at least \$20 at the end. What is your first bet when:

(a) $p = 0.5$ (b) $p = 0.7$ (c) $p = 0.3$?

Problem 16.101. On Mars, boys are twice as likely as girls. A Martian couple has children until they have two boys in a row. Compute the probability the couple will have 10 children.

(a) Let $Q(n)$ be the probability to have n children. What are $Q(2)$ and $Q(3)$?

(b) Show that $Q(n) = Q(n-1)/3 + 2Q(n-2)/9$ for $n > 3$ and hence compute $Q(n)$.

(c) Get a formula for $Q(n)$ and prove it by induction.

Problem 16.102. A three-sided die has face-values 1,2,3. Roll the die 10 times and compute the sum. What is the probability the sum is 15. *[Hint: Let $Q(n, s) = \mathbb{P}[\text{sum of } s \text{ in } n \text{ rolls}].]*

Problem 16.103. Revisit problem 15.21 with n boys and prove that chances are 50% that the last boy gets his seat.

Problem 16.104. Flip 25 biased coins with heads-probability $1/3$. Find $\mathbb{P}[\text{number of heads is divisible by 3}]$.

(a) Relate $A(n), B(n), C(n)$ to $A(n-1), B(n-1), C(n-1)$ and compute $A(25)$, where:

$$\begin{aligned} A(n) &= \mathbb{P}[\text{number of heads in } n \text{ flips has remainder 0 when divided by 3}] \\ B(n) &= \mathbb{P}[\text{number of heads in } n \text{ flips has remainder 1 when divided by 3}] \\ C(n) &= \mathbb{P}[\text{number of heads in } n \text{ flips has remainder 2 when divided by 3}] \end{aligned}$$

(b) Use Monte Carlo to estimate the probability and compare with your answer in (a).

Problem 16.105. Solve the recurrences in Problem 16.104 to get a formula for the probability that 3 divides the number of heads in n coin flips, with probability p of heads. *[Hint: Adapt Problem 7.42 on page 97.]*

Problem 16.106. Three friends A, B, C each have tokens a, b, c. At every step a random pair swaps whatever tokens they currently have. If the first pair picked is (A, B) and then (A, C), the token are distributed c, a, b.

(a) After 10 swaps, compute the probability that each friend has their own token.

(b) After 11 swaps, compute the probability that each friend has their own token.

(c) Tinker further and make a conjecture for the probability that each friend has their own token after n swaps.

(d) Prove your conjecture by induction.

(e) Repeat parts (a)-(d) if initially the tokens are distributed randomly to the friends.

Problem 16.107. There is one amoeba on day 0. Each day, an amoeba dies with probability $1/4$ or splits into two.

(a) Compute the probability the species is extinct on day 10. *[Hint: Let $Q(n, t) = \mathbb{P}[n \text{ amoeba on day } t].]*

(b) Compute the probability the species goes extinct at some time.

Problem 16.108. You plant six seeds in the ground on day 0. Each subsequent day (day 1,2,3,...), each seed may sprout or remain a seed, sprouting with probability $1/3$. Find the probability that all seeds have sprouted by day 10. *[Hint: Let $Q(n, k)$ be the probability that if you have k seeds, they have all sprouted by day n.]*

17.3   Problems

Problem 17.1. Prove the following important facts:
   (a) The events Ω and $\varnothing$ are independent of any event E.
   (b) If events A and B are independent, then each of the pairs of events $(A, \bar{B}), (\bar{A}, B)$ and $(\bar{A}, \bar{B})$ are independent.
   (c) If an event A is independent of *every* event E, then $\mathbb{P}[A]$ is either 0 or 1. *[Hint: A is independent of A.]*

Problem 17.2. If (A, B) and (B, C) are independent, must (A, C) be independent? (Transitivity of independence)

Problem 17.3. Prove or disprove: If $A \cap B = \varnothing$ then A and B are independent.

Problem 17.4. Does A and B being independent imply that $\mathbb{P}[A \cap B \mid C] = \mathbb{P}[A \mid C]\mathbb{P}[B \mid C]$?

Problem 17.5. For the probability space given, compute $\mathbb{P}[A]$ and $\mathbb{P}[A \mid B]$ to determine if the events are independent.
   (a) $A = \{1, 2, 3\}$ and $B = \{2, 3, 4\}$.   (f) $A = \{1, 2, 3\}$ and $B = \{4, 5\}$.
   (b) $A = \{2, 3, 4\}$ and $B = \{1, 2, 3\}$.   (g) $A = \varnothing$ and $B = \{1, 5\}$.
   (c) $A = \{1, 5\}$ and $B = \{1, 2, 5\}$.   (h) $A = \{1, 5\}$ and $B = \varnothing$.
   (d) $A = \{1, 2, 5\}$ and $B = \{1, 5\}$.   (i) $A = \{1, 2, 3, 4, 5\}$ and $B = \{1, 2\}$.
   (e) $A = \{1, 2, 3\}$ and $B = \{1, 2, 3\}$.   (j) $A = \{1, 2\}$ and $B = \{1, 2, 3, 4, 5\}$.

Ω	1	2	3	4	5
P	0.1	0.1	0.2	0.2	0.4

Problem 17.6. Two biased coins have heads-probability 0.01 and 0.99. Randomly pick one and flip twice. Define events $A_1 = \{$1st flip is H$\}$ and $A_2 = \{$2nd flip is H$\}$. Find $\mathbb{P}[A_1], \mathbb{P}[A_2]$ and $\mathbb{P}[A_1 \cap A_2]$. Are A_1 and A_2 independent?

Problem 17.7. Compute the probability that a random 10-bit sequence starts with 111.

Problem 17.8. Randomly roll two independent dice. Compute these probabilities.
   (a) $\mathbb{P}[$both are odd$]$ (b) $\mathbb{P}[$one is odd$]$ (c) $\mathbb{P}[$at least one is odd$]$ (d) $\mathbb{P}[$sum is even$]$.

Problem 17.9. When drawing cards from a 52-card deck, is the second event independent of the first? Explain.
   (a) Randomly draw a card, it's an ace. Randomly draw a second card and ask if it's also an ace.
   (b) Randomly draw a card, it's an ace. Randomly draw a second card and ask if it's a two.
   (c) Randomly draw a card, it's a club. Randomly draw a second card and ask if it's a spade.
   (d) Randomly draw a card, it's an ace. Replace the card, randomly draw a second card and ask if it's also an ace.

Problem 17.10. Label the rows and columns $1, \ldots, 8$ on a standard 8×8 chessboard with alternating black and white squares. Pick a random square. Are these events relating to properties of the square independent?
   (a) $A = \{$white$\}$, $B = \{$black$\}$.   (b) $A = \{$even row$\}$, $B = \{$even column$\}$.   (c) $A = \{$white$\}$, $B = \{$even column$\}$.

Problem 17.11. You have a well shuffled deck. Are the events A and B independent?
   (a) Draw one card. $A = $ "The card is a king" and $B = $ "The card is a spade".
   (b) Draw two cards. $A = $ "Both cards have the same suit" and $B = $ "Both cards have the same rank".

Problem 17.12. A survey shows that 65% of children dislike vegetables. Four children are chosen at random with replacement. What is the probability that all four dislike vegetables?

Problem 17.13. For two fair dice, show that "sum is 7" and "first roll is odd" are independent.

Problem 17.14. A jar contains 10 red, 10 green and 10 blue balls. Randomly pick two balls. Are their colors independent if you pick (a) With replacement?   (b) Without replacement?

Problem 17.15. A jar has 8 red, 5 green and 6 blue balls. Pick two balls. Compute $\mathbb{P}[$both balls are green$]$ and $\mathbb{P}[$balls have different colors$]$ if you pick (a) Without replacement.   (b) With replacement.

Problem 17.16. Roll two independent dice D_1 and D_2. In each case, are the events A and B independent?
   (a) $A = \{D_1$ is odd$\}$, $B = \{D_2$ is even$\}$.
   (b) $A = \{D_1 + D_2 = 10\}$, $B = \{D_1$ and D_2 are both odd$\}$.
   (c) $A = \{D_1 + D_2 = 9\}$, $B = \{D_1 \leq 3, D_2 \geq 4\}$.

Problem 17.17. Ayfos has three independent children. Each sex is equally likely. Define the three events:

$$A = \{\text{all three of same sex}\} \qquad B = \{\text{at most one boy}\} \qquad C = \{\text{there's a boy and a girl}\}.$$

Which pairs of events are independent? What if each sex is not equally likely? Repeat for four children.

Problem 17.18. Use independence, when applicable, to compute these probabilities.
(a) Toss two fair coins and two dice. What is $\mathbb{P}$[two heads and die sum of 9]?
(b) Randomly pick 10 digits independently from $\{0, 1, \ldots, 9\}$. What is $\mathbb{P}$[no 0s]?
(c) A jar contains 90 red and 10 blue balls. Pick 10 balls randomly (without replacement). What is $\mathbb{P}$[all red]?
(d) Flip a fair coin 10 times. What is $\mathbb{P}$[all heads occurr at the end]?
(e) Independently pick 10 bits $b_1 b_2 \cdots b_{10}$ with probability $3/4$ for 1. What is $\mathbb{P}$[sequence is non-decreasing]?
(f) I try each of 10 keys in a random order until the door opens. What are the chances I enter by the 3rd attempt?

Problem 17.19. There are two roads from A to B, from B to C and from A to C. In winter, each road is independently blocked by snow, with probability p. Compute these probabilities:
(a) (i) There is a route from A to B.   (ii) There is a route from A to C.
(b) There is a route from A to B if, from A to C: (i) There is no route.   (ii) There is a route.

Problem 17.20. You are a tourist in a foreign park, where there are twice as many tourists as locals. Locals hate the tourists and will always answer a question incorrectly. Tourists are random and answer repeated questions independently, giving the correct answer with probability $2/3$. You meet a random passer by and ask whether the exit is left or right.
(a) The answer is left. What are the chances the exit is left?
(b) You ask the same person and get left again. Now, what are the chances the exit is left?
(c) You ask a 3rd time and get left again. Now, what are the chances the exit is left?
(d) You ask a 4th time. What are the chances the exit is left if: (i) The answer is left?   (ii) The answer is right?

Problem 17.21. I randomly pick a number x from $\{1, \ldots, n\}$, with probability p_i that x is i. I randomly pick a second number r from $\{1, \ldots, M\}$ and reveal to you $z = x + r \pmod{M}$.
(a) Does knowing z help you to predict x? Explain.
(b) You have access to a fair coin. Give an algorithm to produce z assuming the p_i have finite binary expansions, $p_i = \sum_{j=1}^{k} b_{ij} 2^{-j}$ and M is a power of 2, $M = 2^{\ell}$.

Problem 17.22. Los Angeles has about 6,500 miles of road and 20 million people. Estimate the chances a random person, in their lifetime, is in a car accident with a drunk. *[Hints: Chances of no accident on Friday's or Saturday's.]*

Problem 17.23. Use the Fermi-method to estimate:
(a) The number of piano tuners in USA.
(b) The number of passenger cars that are sold each year in USA.
(c) The dollar amount New York state spends on K-12 education a year.
(d) The number of people airborne over USA at any given moment.
(e) The average savings per flight if airlines asked passengers to urinate before boarding.
(f) The number of correct consecutive letters from Macbeth somewhere in the typings of 1 million monkeys typing randomly on 1 million typewriters for a year.
(g) The number of insects living on planet Earth.
(h) The total amount of time spent by US college students studying for finals in a semester.
(i) The computer memory usage by all college students in USA.
(j) The number of cities in USA with population above 10,000.

Problem 17.24. In each case, give a probability space and events that are:
(a) 2-way, 3-way but not 4-way independent.   (b) 3-way, 4-way but not 2-way independent.

Problem 17.25. Suppose that A and B are independent.
(a) Which of these pairs are independent: (i) $A, \overline{B}$ (ii) $\overline{A}, \overline{B}$ (iii) $\overline{A}, B$ (iv) $A, \overline{A} \cap B$ (v) $A, \overline{A} \cup B$.
(b) Show that: (i) $\mathbb{P}[A \mid \overline{B}] = \mathbb{P}[A]$.   (ii) $\mathbb{P}[\overline{A} \mid \overline{B}] = \mathbb{P}[\overline{A}]$.
(c) If A and B have positive probability, can they be disjoint events.
(d) Can $\mathbb{P}[A] = 0$?
(e) Show that $\mathbb{P}[\overline{A \cup B}] = \mathbb{P}[\overline{A}] \times \mathbb{P}[\overline{B}]$.

Problem 17.26. Transistors fail independently with probability p. Chip A has 2 transistors, and chip B has 4. A chip fails if more than half its transistors fail. Both chips fail with the same probability. What could p be?

Problem 17.27. Projects are independent and take 1,2 or 3 days to complete, each equally likely. You and your spouse each start a project on day 1. On any night, if you and your spouse are in sync and have just finished a project that day, you will have dinner together. Otherwise, if just one of you finish a project, you will start a new project. What is the probability that the next time you have dinner with your spouse will be on the 3rd night?

Problem 17.28. A jar contains 6 red balls, 3 green balls, 5 white balls and 7 yellow balls. Two balls are chosen from the jar, with replacement. What is the probability that:
  (a) Both balls chosen are green?   (b) Both balls are the same color?   (c) The balls are different color?

Problem 17.29. A 100-sided die with faces $1, \ldots, 100$ is rolled 5 times. Find $\mathbb{P}[\text{all rolls are different}]$.

Problem 17.30. How many times must you roll a 100-sided die so that the chances of rolling some number more than once is at least: (a) 30%   (b) 50%   (c) 100%.

Problem 17.31. On page 248, we computed a table with the chances to find a FOCS-twin by the kth student when the class size is 200. Recompute the table for a class of size 300.

Problem 17.32. If some birthdays are more likely than others, show that the probability of FOCS-twins with N students increases. Index the days $1, \ldots, B$. Let p_i be the probability of a birthday on day i. Show:

$$Q(p_1, \ldots, p_B) \stackrel{\text{def}}{=} \mathbb{P}[\text{student } s_1 \text{ has no FOCS-twin}] \leq \left(\frac{B-1}{B}\right)^{N-1}.$$

  (a) Show that $Q(p_1, \ldots, p_B) = \sum_{i=1}^{B} p_i (1 - p_i)^{N-1}$.
  (b) Show that Q is maximized when all p_i are equal. To do so, suppose that $p_1 > p_B$ and define

$$\Delta Q(\delta) = Q(p_1 - \delta, p_2, \ldots, p_{B-1}, p_B + \delta) - Q(p_1, p_2, \ldots, p_{B-1}, p_B).$$

   (i) Show that $\lim_{\delta \to 0} \Delta Q/\delta = (1 - p_1)^{N-1}(2p_1 - 1) + (1 - p_B)^{N-1}(1 - 2p_B)$.
   (ii) Show that the expression in (i) is positive.
   (iii) Explain why this proves that $Q(p_1, \ldots, p_B)$ is maximized when all the p_i are equal.

Problem 17.33. A movie theater gives a free ticket to the first in line whose birthday matches that of someone who already bought a ticket. Assume birthdays are independent and random throughout the year.
  (a) What position in line gives you the greatest chance of winning the free ticket?
  (b) What is the probability that you will get the free ticket?

Problem 17.34. Independently generate a 10-bit binary sequence $b_1 \cdots b_{10}$ with $\mathbb{P}[b_i = 0] = 1/2$. Compute the probability the sequence is sorted from low to high, e.g. 0000111111 is sorted.

Problem 17.35. 3 independent bits are sent over a channel, and $\mathbb{P}[\text{bit=1}] = 3/4$. The channel is noisy, independently flipping each bit with probability $1/4$. The signal received is 101. We are interested in the original message.
  (a) What are the possible original messages and what are their posterior probabilities.
  (b) Which message would you decode the received signal 101 as? What is your probability of error?
  (c) We also send over the channel the number of ones in the message (a size hint) as a separate 2-bit string. For each possible size received (00,01,10,11) find the most likely messages and the probability of a decoding-error.
  (d) What is the posterior over the 4 digit messages for the signal 1111 and received size hint 011?
  (e) Verify your results with a Monte-Carlo simulation.

Problem 17.36. You have $100 and bet $1 at a time on red in roulette. What are your chances win $50 before ruin.

Problem 17.37. A $1 column bet in roulette has 12 numbers and wins $2 if you get one of those numbers, with probabilitly 12/38. A red bet wins $1 if the outcome is red, with probability 18/38. You start with $20. What are your chances of winning at least $10 before ruin if: (a) All bets are on red.   (b) All bets are on a column.

Problem 17.38. L people at a circular table pass bread around (see Exercise 17.11). Number the seats $0, 1, \ldots, L-1$ counter-clockwise. A person passes right with probability p and left with probability $1 - p$, where $0 < p < 1$. The bread starts at seat 0. What is the probability P_k that the person at seat k is the last to receive the bread?
  (a) With $p = 1/3$ and $L = 10$, run a Monte-Carlo simulation to compute $P_1, \ldots, P_9$.
  (b) Compute P_k for general L and p and compare with your Monte-Carlo simulation.

Problem 17.39. Prove Theorem 17.4 by using the methods in Problem 7.28 to solve the gambler's ruin recurrence

$$P_k = pP_{k-1} + (1-p)P_{k+1} \text{ for } 0 < k < L; \qquad P_0 = 1 \text{ and } P_L = 0.$$

Problem 17.40. Solve the gambler's ruin recurrence in Problem 17.39 using generating functions.
(a) Define a polynomial $G(s) = \sum_{k=0}^{L} P_k s^k$, the generating function for the sequence $\{P_k\}$. Let $\alpha = 1/(1-p)$ and $\beta = p/(1-p)$. Use the recursion to show that

$$G(s) = \frac{1 + (P_1 - \alpha)s + \beta P_{L-1}s^{L+1}}{1 - \alpha s + \beta s^2},$$

(b) Show that $1 - \alpha s + \beta s^2 = (1 - a_+ s)(1 - a_- s)$, where $a_\pm = (\alpha \pm \sqrt{\alpha^2 - 4\beta})/2$.
(c) For $a_+ \neq a_-$, i.e. $p \neq \frac{1}{2}$, show $\dfrac{1}{1 - \alpha s + \beta s^2} = \dfrac{a_+}{(a_+ - a_-)(1 - a_+ s)} - \dfrac{a_-}{(a_+ - a_-)(1 - a_- s)}$. (Partial fractions.)
(d) P_k is the coefficient of the s^k in $G(s)$. Show, for $1 \leq k \leq L$, that

$$P_k = \frac{a_+^{k+1} - a_-^{k+1} + a_+^k(P_1 - \alpha) - a_-^k(P_1 - \alpha)}{a_+ - a_-}.$$

(e) Use $P_L = 0$ to show that $P_1 - \alpha = -(a_+^{L+1} - a_-^{L+1})/(a_+^L - a_-^L)$.
(f) Show that $P_k = (a_+^L a_-^k - a_+^k a_-^L)/(a_+^L - a_-^L)$ for $p \neq 1/2$. Prove that this matches Theorem 17.4 on page 252.
(g) What happens when $p = 1/2$? *[Hint: $(1-s)^{-2} = 1 + 2s + 3s^3 + \cdots + (k+1)s^k + \cdots$].*

Problem 17.41 (Kolmogorov Zero-One Law). Let $s_1, s_2, s_3, \ldots$ be an infinite sequence of independent random signs (± 1). Define the event $A_p = \{s_1, s_2, \ldots \mid \sum_{i=1}^{\infty} s_i/i^p \text{ converges}\}$.
(a) Using Monte-Carlo or otherwise, estimate $\mathbb{P}[A_p]$ for $p \in \{1/4, 1/2, 3/4, 1, 2\}$. Some creativity is required.
(b) Let B_n be any event defined using only $s_1, \ldots, s_n$. Show that $\mathbb{P}[A_p \mid B_n] = \mathbb{P}[A_p]$.
    (A_p is an example of a tail-event because it is independent of any finite prefix $s_1, \ldots, s_n$.)
(c) Kolmogorov's law is that $\mathbb{P}[A_p] = 0$ or 1. Here is the intuition. Define B_n by

$$B_n = \{s_1 \cdots s_n x \mid s_1 \cdots s_n \text{ is the prefix of a sequence in } A_p \text{ and } x \text{ is any } \pm 1 \text{ sequence}\}.$$

B_n "is" A_p as $n \to \infty$. So, by (a), A_p is independent of A_p. Deduce Kolmogorov's law.
(d) Make a conjecture for $\mathbb{P}[A_p]$, depending on p. (Lookup Rademacher, Paley & Zygmund.)
The 0-1 law holds for any tail-event. The formal proof needs measure theory because the sample space is uncountable. The 0-1 law is the root of phase transitions in physical systems (water/ice; percolation/no percolation; connected/disconnected infinite graph, etc.)

> **Randomized Algorithms** are a modern tool using probability to design algorithms. An algorithm that works with some (usually large) probability is better than no algorithm.

Problem 17.42 (The "ATM"-Test). Here is an application of probability to security. You want to authenticate yourself at the ATM without revealing your password. After all, who knows what another "bank's" ATM might do with your password? We faced a similar problem in Section 14.2 on page 202, to convince you that a solution to the subset sum problem exists without revealing it. In cryptography, such proofs are called "zero-knowledge" because they do not convey any information about the solution. Here is one strategy for the ATM situation.

> **for** $t = 1, \ldots, T$ **do**
>   The ATM tests you. Each test is independent.
>   **if** You know the password **then**
>   You answer correctly and reveal no password-information.
>   **else if** You are an imposter and don't know the password **then**
>   You can only answer the test correctly with probability at most $1/2$.
> You access the account only if you pass all T tests.

Compute T, the number tests, so that an imposter can access your account with probability at most 10^{-100}. (For a test that you can answer without revealing your password, but an imposter cannot, see Problem 29.57.)

Problem 17.43 (Approximate median). You have an array of 1000 distinct numbers. The median has rank 500. You wish to choose a number in the middle 20% with rank in $\{401, \ldots, 600\}$: [▬▬▬▬ good ▬▬▬▬] . A deterministic approach sorts the numbers and then picks one in the middle, What is the asymptotic runtime?

(a) Pick a number randomly. What are the chances of success? What is the runtime?

(b) Continue to pick a number independently and randomly until success. What are the chances you need k draws to succeed? What is the maximum number of draws you may need? How do you test for success?

(c) Continue to pick a number randomly without replacement until success. What are the chances you need k draws to succeed? What is the maximum number of draws you may need?

Part (a) is a Monte-Carlo algorithm with a fixed runtime and some probability of failure. Parts (b) and (c) are Las Vegas algorithms which guarantee success but have a nondeterministic runtime.

Problem 17.44 (Contention Resolution). Pam and Sam try to access a database at time steps $1, 2, 3, \ldots$. If both try to access the database, both get locked out for that time step.

(a) Pam and Sam try in every time step to access the database. Will they ever succeed?

(b) Pam and Sam implement a randomized algorithm. Each independently attempts to access the database with probability p (independently at every time step). Let $P(i) = \mathbb{P}[\text{Pam gains access to the database at time step } i]$. Similarly define $S(i)$ for Sam. Let $B(i)$ be the probability that one of them gains access at time step i.
  (i) Compute $P(i)$, $S(i)$ and $B(i)$. Set p to the value that maximizes $P(i)$.
  (ii) Show that $\mathbb{P}[\text{Pam waits } k \text{ steps for access}] = (3/4)^{k-1} \times (1/4)$.
  (iii) Show that $\mathbb{P}[\text{First successful access is after } k \text{ steps}] = (1/2)^k$.

(c) Repeat the problem for three people Pam, Sam and Ram all accessing the same database.

Problem 17.45 (Min-Cut). A graph cut separates the vertices into sets A and B. The cut-value is the number of edges from A to B. To find a cut with minimum value we try repeatedly merging sets of vertices until we have two sets. Each merge happens at an edge. Here is an example.
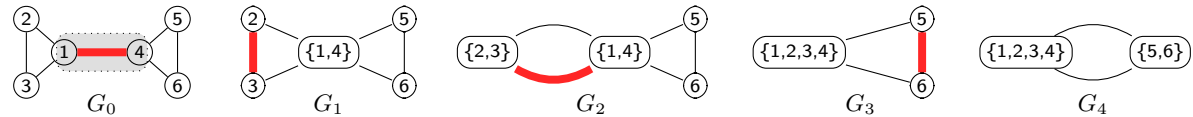
G_0 : Original graph, 1st contraction. Two vertices are contracted at the red edge into a super-vertex $\{1, 4\}$, giving G_1.

G_1 : 2nd contraction. The super-vertex maintains edges to all vertices connected to either vertex 1 or 4. The super-vertex is a set of vertices. Contract again on the red edge in G_1 to get a super-vertex $\{2, 3\}$, producing G_2.

G_2 : 3nd contraction merging super-vertices. The super-vertex $\{2, 3\}$ keeps all edges to neighbors of vertices 2 or 3: the two edges to super-vertex $\{1, 4\}$ result in a multigraph with parallel edges. Contract on the red edge to get G_3.

G_3 : 4th contraction. Contract on the red edge to get G_4.

G_4 : Only two super-vertices remain, identifying the cut $A = \{1, 2, 3, 4\}$, $B = \{5, 6\}$ with cut-value 2.

(a) Is the cut in the example above a min-cut? Give a sequence of edge contractions that does give a min-cut.

(b) What property must every contraction-edge satisfy for the result to be a min-cut.

Randomized algorithm for min-cut: For contraction $i + 1$, choose the contraction-edge independently and randomly from all available edges in G_i, the multi-graph after contraction i. Compute the probability that this algorithm produces a min-cut. Suppose the min-cut has size k and there are M cuts $(A_1, B_1), \ldots, (A_M, B_M)$ with this minimum size.

(c) Prove that $|E(G_i)| \geq (n - i)k/2$, where $|E(G)|$ is the number of edges in graph G. *[Hints: Every cut in G_i is a cut in G_0. If the min-cut size is k, can the minimum degree be less than k? Handshaking Theorem.]*

(d) Fix a min-cut, for example (A_1, B_1). Prove by induction that all the edges in the cut (A_1, B_1) remain in G_i with probability at least $\left(1 - \frac{2}{n}\right)\left(1 - \frac{2}{n-1}\right) \cdots \left(1 - \frac{2}{n-i+1}\right)$.

(e) Prove that $\mathbb{P}[\text{algorithm returns cut } (A_1, B_1)] \geq 2/n(n - 1)$. *[Hint: What should i be in the product of part (e)?]*

(f) Prove that $\mathbb{P}[\text{return a min-cut}] \geq 2M/n(n - 1)$. *[Hint: The algorithm returns one cut.]*

(g) Independently repeat the algorithm ℓ times and return the cut of minimum value. Show:

$$\mathbb{P}[\text{return a min-cut}] \geq 1 - \left(1 - \frac{2M}{n(n - 1)}\right)^{\ell} \geq 1 - e^{-2M\ell/n(n-1)}.$$

Show that the algorithm succeeds with probability at least $1 - \epsilon$ for $2M\ell \geq n(n - 1)\log(1/\epsilon)$.

> **Probabilistic Method.** The probabilistic method is a modern technique that uses probability and independence to prove results about a deterministic setting.

Problem 17.46. The surface of a sphere is arbitrarily painted red and blue with 90% of the surface painted red. Prove that it is possible to inscribe a cube whose vertices are all red.
  (a) Consider a randomly inscribed cube with vertices $v_1, \ldots, v_8$. Show that $\mathbb{P}[v_i \text{ is blue}] = 0.1$.
  (b) Show that $\mathbb{P}[v_1 \text{ OR } v_2 \text{ OR } \cdots \text{ OR } v_8 \text{ is blue}] \leq 0.8$.
  (c) Hence show that $\mathbb{P}[\text{all 8 vertices are red}] \geq 0.2 > 0$.
  (d) What does it mean if a probability is positive?

Problem 17.47. The sets $S_1, \ldots, S_m$ are subsets of a universal set $S = \{1, \ldots, n\}$. The task is to color the vertices in S red or blue so that none of the S_i are monochromatic, i.e. contain vertices of only one color. Here is an example of a valid coloring of 5 sets $S_1, \ldots, S_5$ using vertex colors ①②③④⑤.

$$S_1 : \{①②③\} \qquad S_2 : \{①②④\} \qquad S_3 : \{①③④\} \qquad S_4 : \{②③④\} \qquad S_5 : \{①②⑤\}.$$

  (a) Prove that the following collections of sets are not 2-colorable.
      (i) $\{①②\}$ $\{①③\}$ (ii) $\{①②③\}$ $\{①③④\}$ $\{②③④\}$ $\{①③⑤\}$
          $\{②③\}$ $\{②④⑤\}$ $\{①④⑤\}$ $\{②③⑤\}$
  (b) When there are more elements per set, one can color more sets. Suppose each set has size $|S_i| = \ell$. Let $m(\ell)$ be the maximum number of sets one can guarantee is 2-colorable. So any collection of $m(\ell)$ sets is 2-colorable; and there is some collection of $m(\ell) + 1$ sets that is not 2-colorable. Show that $m(\ell) \geq 2^{l-1} - 1$ (Erdős, 1963).
      (i) Independently color each element randomly. Compute $P_i = \mathbb{P}[S_i \text{ is monochromatic}]$.
      (ii) Show that $\mathbb{P}[\text{any } S_i \text{ is monochromatic}] \leq \sum_i P_i$.
      (iii) If $m < 2^{l-1}$, show that $\mathbb{P}[\text{any } S_i \text{ is monochromatic}] < 1$.
      (iv) Show that $\mathbb{P}[\text{all } S_i \text{ are not monochromatic}] > 0$.
      (v) Conclude that there must be a valid 2-coloring, hence prove that $m(\ell) \geq 2^{l-1} - 1$.
(Erdős also showed $m(\ell) \in O(\ell^2 2^\ell)$. Beck (in 1978) and Spencer (in 1981) showed $m(\ell) > \ell^{1/3-o(1)} 2^\ell$; Radhakrishnan and Srinivasan (in 2000) improved this to $m(\ell) > c 2^\ell \sqrt{\ell/2 \ln \ell}$ for $c = 1 - o(1)$.)

Problem 17.48. Prove these results on the number of distinct min-cuts in a graph with n vertices.
  (a) If the graph is a cycle, then it has $n(n-1)/2$ distinct min-cuts.
  (b) No graph has more than $n(n-1)/2$ distinct min-cuts. *[Hint: Problem 17.45(g); a probability is at most 1.]*

Problem 17.49. In a tournament, every player plays every other player and wins or loses (there is directed edge between every pair). A tournament is k-dominated if every subset of k players is beaten by some other player. Show that there is a tournament with 25 players that is 2-dominated.
  (a) Construct a tournament by independently and randomly choosing each edge-direction.
      (i) A set S of 2 players is dominated if another player beats everyone in S. Show that
$$\mathbb{P}[S \text{ is not dominated}] = (1 - 1/4)^{n-2}.$$
      (ii) Let $S_1, \ldots, S_M$ be the different subsets of 2 players. What is M?
      (iii) Show that $\mathbb{P}[\text{None of the } S_i \text{ are dominated}] \leq M \times (1 - 1/4)^{n-2}$.
      (iv) For $n = 25$, show that $\mathbb{P}[\text{None of the } S_i \text{ is dominated}] < 1$
      (v) Explain why there must be some tournament with 25 vertices that is 2-dominated.
  (b) Show that there is a k-dominated tournament with n vertices if $2^{-k}(n-k) > \ln \binom{n}{k}$. Hence, show that there is a $(1-\epsilon) \log_2 n$–dominated tournament (asymptotic in n, for any $\epsilon > 0$). *[Hint: Show $\mathbb{P}[\text{no } k\text{-subset is dominated}] \leq \binom{n}{k} \times (1 - 2^{-k})^{n-k}$ and use $1 - x \leq e^{-x}$.]*

Problem 17.50. [Lubell-Yamamoto-Meshalkin inequality, Problem 13.73] $A_1, \ldots, A_n$ are subsets of $\{1, 2, \ldots, M\}$, with no A_i a subset of another and $\ell_i = |A_i|$. Use probability to prove $\sum_{i=1}^n 1/\binom{M}{\ell_i} \leq 1$. *[Hint: Let X_σ be a random permutation of X and E_i the event that A_i is a prefix of X_σ. Compute $\mathbb{P}[E_1 \cup \cdots \cup E_n]$. What is $E_i \cap E_j$?]*

18.6   Problems

Problem 18.1. $\mathbf{X}$ and $\mathbf{Y}$ are random variables on the same sample space Ω. Are $\mathbf{X} + \mathbf{Y}$, $\mathbf{XY}$ and $\min(\mathbf{X}, \mathbf{Y})$ random variables? If yes, define how to compute them for an outcome $\omega \in \Omega$.

Problem 18.2. For probability space (Ω, P), is P a random variable? What about $P \ln P$?

Problem 18.3. For each PDF, show that the sum of the probabilities is 1.
(a) $P_{\mathbf{X}}(k) = 1/n$ for $k = 1, 2, \ldots, n$.
(b) $P_{\mathbf{X}}(k) = B(k; n, p)$ for $k = 0, 1, \ldots, n$.
(c) $P_{\mathbf{X}}(k) = p(1-p)^{k-1}$ for $k = 1, 2, 3 \ldots$.
(d) $P_{\mathbf{X}}(k) = e^{-\lambda}\lambda^k/k!$ for $k = 0, 1, 2, \ldots$.

Problem 18.4. For what values of a constant A are the following a valid normalized PDF.
(a) $P_{\mathbf{X}}(k) = Ak$ for $k = 0, \ldots, 5$.
(b) $P_{\mathbf{X}}(k) = Ak$ for $k = 0, \ldots, n$.
(c) $P_{\mathbf{X}}(k) = A$ for $k = 0, \ldots, \infty$.
(d) $P_{\mathbf{X}}(k) = Ak^2$ for $k = 0, \ldots, 5$.
(e) $P_{\mathbf{X}}(k) = A2^{-k}$ for $k = 0, \ldots, 5$.
(f) $P_{\mathbf{X}}(k) = A/k$ for $k = 1, \ldots, \infty$.
(g) $P_{\mathbf{X}}(k) = A/k^2$ for $k = 1, \ldots, \infty$.
(h) $P_{\mathbf{X}}(k) = A2^{-k}$ for $k = 0, \ldots, \infty$.
(i) $P_{\mathbf{X}}(k) = A/k!$ for $k = 0, \ldots, \infty$.
(j) $P_{\mathbf{X}}(k) = A\lambda^k/k!$ for $k = 1, \ldots, \infty$.
(k) $P_{\mathbf{X}}(k) = Ak\lambda^k$ for $k = 1, \ldots, \infty$.
(l) $P_{\mathbf{X}}(k) = A\lambda^k/k$ for $k = 1, \ldots, \infty$.

Problem 18.5. A random variable $\mathbf{X}$ has a PDF from Problem 18.4(a)–(l). In each case compute:
(a) $\mathbb{P}[\mathbf{X} > 1]$.   (b) The most probable value of $\mathbf{X}$.   (c) $\mathbb{P}[\mathbf{X}$ is even$]$.

Problem 18.6. Random variables $\mathbf{X}$ and $\mathbf{Y}$ are independent and have a uniform distribution on $\{1, \ldots, 10\}$. What is the PDF of $\mathbf{X} + \mathbf{Y}$? Give a plot of the histogram.

Problem 18.7. A biased die rolls values in $\{1, 2, 3, 4, 5, 6\}$ with probabilities $p_1, p_2, p_3, p_4, p_5, p_6$ respectively. Can one choose p_i so that the PDF of the sum of two independent rolls is uniform on $\{2, \ldots, 12\}$?
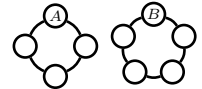
Problem 18.8.
(a) Give the CDF for the PDF:

x	0	1	2	3	4
$P_{\mathbf{X}}(x)$	0.2	0.1	0.2	0.4	0.1

(b) Give the PDF for the CDF:

x	$(-\infty, 0)$	$[0, 1)$	$[1, 2)$	$[2, 3)$	$[3, 4)$	$[4, \infty)$
$F_{\mathbf{X}}(x)$	0	0.1	0.15	0.5	0.8	1

Problem 18.9. A LAN has two disjoint parts (right), with two special nodes A, B. Randomly pick two different nodes in the network (every pair of nodes has equal probability of being picked).
(a) Add a new link between the two nodes picked. Find the probability there is a path from A to B.
(b) Let $d(A, B)$ be the length of the shortest path between A and B after adding the new link. If the network is not connected $d(A, B) = \infty$. Give the PDF of $d(A, B)$.

Problem 18.10. Let $\mathbf{F}$ be the indicator random variable equal to 0 if a couple's first child is a boy and 1 if it is a girl. Let $\mathbf{X}$ be the number of children they have (waiting time) until they have at least 1 boy and 1 girl. Let p be the probability of a boy (different children are independent). Are $\mathbf{F}$ and $\mathbf{X}$ independent: (a) If $p = 1/2$? (b) If $p = 1/3$?

Problem 18.11. Flip a coin 10 times and define random variables $\mathbf{X}_T$, the number of tails flipped, and $\mathbf{X}_H$, the number of heads flipped. Are $\mathbf{X}_T$ and $\mathbf{X}_H$ independent?

Problem 18.12. Flip a coin until until a given string appears. For each string, find the PDF for the number of flips.
(a) H.   (b) HH.   (c) HHH.   (d) HT.   (e) Any string with at least 3 H's.

Problem 18.13. The independent random variables $\mathbf{X}$ and $\mathbf{Y}$ are ± 1, each with probability $1/2$. Let $\mathbf{Z} = \mathbf{XY}$. Show that $\mathbf{X}$, $\mathbf{Y}$ and $\mathbf{Z}$ are pairwise independent. Are they independent?

Problem 18.14. Flip 3 biased coins with probability of heads $3/5$. Let $\mathbf{X}$ be the number of heads and let $\mathbf{Y}$ be an indicator for whether the last two flips match. Give the joint PDF $P_{\mathbf{XY}}(x, y)$ as a joint PDF table.
(a) Are $\mathbf{X}$ and $\mathbf{Y}$ independent?   (b) Find $P_{\mathbf{X}}(2)$, $P_{\mathbf{Y}}(1)$ and $\mathbb{P}[\mathbf{X} = 2 \mid \mathbf{Y} = 1]$.

Problem 18.15. In a dice game, if you roll 1, the game stops and you win \$1. For any other roll, you must decide whether to stop and win the value rolled, or continue rolling. One strategy is to stop if the roll is τ or larger. For this strategy, give the PDF of your winnings for the six different choices of the threshold τ, where $\tau \in \{2, 3, \ldots, 6\}$.

Problem 18.16. Let $\mathbf{X}_1, \mathbf{X}_2, \mathbf{X}_3$ be uniform random variables on $\{1, \ldots, 10\}$. Let $\mathbf{Z}$ be the sum, $\mathbf{Z} = \mathbf{X}_1 + \mathbf{X}_2 + \mathbf{X}_3$.
(a) Give the PDF of $\mathbf{Z}$.   (b) You observe $\mathbf{Z} = 10$. Give the conditional PDF for $\mathbf{X}_1$, $\mathbb{P}[\mathbf{X}_1 = x \mid \mathbf{Z} = 10]$.

Problem 18.17. X_1 and X_2 are independent uniform random variables on $\{1, 2, \ldots, 10\}$.
  (a) Give the PDFs of: (i) The sum, $Y = X_1 + X_2$.   (ii) The maximum, $Z = \max(X_1, X_2)$.
  (b) Repeat if there are three independent uniform random variables X_1, X_2, X_3.

Problem 18.18. A biased die has probability $p_i = Ai$ to roll i, for $i \in \{1, \ldots, 6\}$, where A is a constant.
  (a) Give the PDF of the sum of two rolls.   (b) Give the PDF of the sum of three rolls.

Problem 18.19. Let X and Y be waitings times with success probabilities p and q. Give the PDF of $Z = X + Y$.

Problem 18.20. $X_1, \ldots, X_5$ are independent uniform random variables on $\{1, 2, \ldots, 10\}$. Give the PDFs of the minimum Y and the maximum Z. Use Monte Carlo to verify your answer. *[Hint: Find $\mathbb{P}[Y \geq i]$ and $\mathbb{P}[Z \leq i]$.]*

Problem 18.21. X and Y are independent with the same PDF, $P(k) = 2^{-k}$ for $k = 1, 2, \ldots$. For $m, n \in \mathbb{N}$, find:
  (a) $\mathbb{P}[\min(X, Y) \leq m]$.   (d) $\mathbb{P}[X = Y]$.   (g) $\mathbb{P}[mX = nY]$.
  (b) $\mathbb{P}[\max(X, Y) \leq m]$.   (e) $\mathbb{P}[X > mY]$.   (h) $\mathbb{P}[mX > nY]$.
  (c) $\mathbb{P}[X \text{ divides } Y]$.   (f) $\mathbb{P}[X \geq mY]$.   (i) $\mathbb{P}[mX \geq nY]$.

Problem 18.22. The Alphas and Omegas play in a best of seven game world series. A team wins a game with probability $1/2$ and games are independent. The superstar on the Alphas is Epsilon. In a game, Epsilon gets $0, 1, 2, 3, 4$ hits with probabilities $1/2, 1/8, 1/8, 1/8, 1/8$. Give the PDF for the number of hits Epsilon gets in the series.

Problem 18.23. You draw a 5 card poker hand from a shuffled 52-card deck. Give the PDF for the number of Aces.

Problem 18.24. You and a friend are randomly placed in a line with eight other people (ten people in line). Give the PDF for the number of people between you and your friend. Verify with Monte Carlo.

Problem 18.25 (Derangements). Ten graduates throw up their hats which land randomly on heads. Give the PDF for the number of graduates getting back their own hat. *[Hint: Problem 14.43.]*

Problem 18.26 (Rock, paper, scissors). Ifar and Niaz each privately choose one of $\{R, P, S\}$. R beats S, S beats P and P beats R. Show that if Ifar chooses randomly using a uniform distribution, Niaz wins with probability $1/3$, no matter what his strategy. If Ifar uses a non-uniform strategy, show that Niaz can increase his probability to win.

Problem 18.27. For the guessing game in Example 18.2 on page 266, I choose L uniformly on $\{1, 2, 3\}$ and set $H = L + 1$. What are your chances to win using the strategy in Example 18.2? Prove that you cannot do better?

Problem 18.28. Let X be a random variable taking values in $\{1, \ldots, n\}$ with unknown PDF. Let R be a uniform random variable on $\{1, \ldots, M\}$, and $Y = X + R \pmod{M}$. Show that X and Y are independent.

Problem 18.29 (Secure Multiparty Computation (MPC)). One can use Problem 18.28 to privately share a sum in a multiparty computation. Alice, Bob and Charlie wish to share their average salary without revealing individual salaries. Let X_1, X_2, X_3 be the salaries. Effectively, they wish to privately share the sum, $X_1 + X_2 + X_3$.
  (a) Let M be a sufficiently large integer, $M \gg X_1 + X_2 + X_3$. Alice generates R_1 uniformly on $\{1, \ldots, M\}$ and sends $Y_1 = X_1 + R_1 \pmod{M}$ to Bob using Bob's public key. Explain why Bob cannot infer Alice's salary.
  (b) Bob generates R_2 uniformly on $\{1, \ldots, M\}$ and sends $Y_2 = Y_1 + R_2 \pmod{M}$ to Charlie using Charlie's public key. Explain why Charlie cannot infer Bob or Alice's salary.
  (c) Charlie generates R_3 uniformly on $\{1, \ldots, M\}$ and sends $Y_3 = Y_2 + R_3 \pmod{M}$ to Alice using Alice's public key. Explain why Alice cannot infer Bob or Charlie's salary.
  (d) Now, Alice sends $Y_4 = Y_3 - R_1$ to Bob. Can Bob infer any salaries.
  (e) Bob sends $Y_5 = Y_4 - R_2$ to Charlie. Charlie computes and sends $Y_6 = Y_5 - R_3$ to Alice and Bob. What is Y_6?
  (f) Explain why the sum has been privately shared. What does Alice know about the salaries of Bob and Charlie?

Problem 18.30. A random cut on a circular pizza picks two random points on the circumference and cuts along the chord joining the two points. Give the PDF for the number of pieces produced when you make three random cuts.

Problem 18.31. Let X be the number of flips of a fair coin until H appears. Give the PDF and CDF of X.

Problem 18.32. Give a formula for the CDF $F_X(k)$ where the distribution of X is:
  (a) Uniform on $\{1, \ldots, n\}$. Give a plot of F_X for $n = 20$.
  (b) Binomial with n trials and success probability p (leave it as a sum). Give a plot of F_X for $n = 20, p = 0.25$.
  (c) The waiting time to success with probability 0.25. Give a plot of F_X.

Problem 18.33. A die roll is $\{1, 2, \ldots, 6\}$ with probabilities $\{p_1, p_2, \ldots, p_6\}$. Give the CDF for the maximum out of 10 rolls of the die. From your CDF, obtain the PDF for the maximum.

Problem 18.34. Which random variables (measurements) are Binomial? The number of successes is Binomial if:

> (i) The experiment counts successes in a fixed number of binary (succeed/fail) trials.
> (ii) Each trial has the same fixed probability p of success.
> (iii) The trials are independent of each other.

(a) Randomly answer 20 multiple-choice questions (5 choices each). Count the number correct.
(b) Flip a biased coin (probability p of H) and count the number of heads in 100 flips.
(c) Flip a biased coin until 2 heads appear (probability p of H) and count the number of flips.
(d) The number of students sampled when you randomly sample from 1,000 students until four are from NY-state.
(e) The number of students from NY-state when you randomly sample 100 students without replacement from 1,000.
(f) The number of students from NY-state when you randomly samples 100 students with replacement from 1,000.
(g) The number of SUV-owners in a Gallup poll that randomly samples 1,000 Americans (without replacement).
(h) The number of darts you throw until you hit the bulls-eye.
(i) The number of darts hitting the bulls-eye if you throw 3 darts.
(j) Hats of 100 men are given back to the men randomly. Count how many men get their hat back.
(k) The number of cut edges from A to B when each vertex of a graph with m edges is randomly placed into A or B.
(l) Draw 10 cards from a shuffled deck and count the number of aces.
(m) You have 10 shuffled decks. Draw one card from each deck and count the number of aces.
(n) Let $\mathbf{X}$ be the number of 1s in the BITWISE-OR of two 10-bit sequences of independent random bits (1/0 are T/F). For example, 0001110010 BITWISE-OR 1000111000 = 1001111010.
(o) Flip 20 fair coins and re-flip just once all coins which flipped H.
    (i) Count the coins showing heads at the end.   (ii) Count the total number of heads flipped in the experiment.
(p) Your total winnings in 100 fair coin flips when you win $2 per H and lose $1 per T.
(q) A box has 50 bulbs in a random order, with 5 being defective. Of the first 5 bulbs, count the number defective.

Problem 18.35. Let a and b be two random 10-bit sequences, and let $c = a \oplus b$ be their BITWISE-OR, where 0 is F and 1 is T. For example, $0001110010 \oplus 1000111000 = 1001111010$. Compute $\mathbb{P}[c$ has five 1s$]$.

Problem 18.36. Plot the PDF for the number of heads in 10 biased coin flips with probability of heads $3/5$. Use a Monte Carlo with 10,000 trials to get a histogram for the number of heads. Compare. (Look up histogram on the www.)

Problem 18.37. In a flight, airplane engines independently fail with probability p. An airplane crashes if more than half its engines fail. For what values of p is a 2-engine airplane safer than a 4 engine airplane?

Problem 18.38. A big hospital delivers 1000 babies and a small hospital delivers 100. Boys and girls are equally likely. Which hospital (big or small) has a higher chance of having the same number of boys as girls?

Problem 18.39. Flip 101 independent fair coins. Find: (a) $\mathbb{P}[0$ heads$]$ (b) $\mathbb{P}[1$ or more heads$]$ (c) $\mathbb{P}[$Majority heads$]$. Repeat for a biased coins with probability $2/3$ of heads.

Problem 18.40 (Voting). A smurf gets a yes/no question right with probability p. Find the smallest p if the chances are 99% that a majority vote of 1001 independent smurfs is correct. What about 10001 smurfs?

Problem 18.41. For 20 fair coin flips, define events $A = \{$equal number of H and T$\}$ and $B = \{$first 3 flips are H$\}$. Compute the probabilities: (a) A occurs.   (b) B occurs.   (c) A AND B occur.   (d) A OR B occur.

Problem 18.42. Which is more likely: n sixes in $6n$ dice or $n+1$ sixes in $6(n+1)$ dice?

Problem 18.43. Flip a fair coin n times. What is the probability of an equal number of H and T? Recompute the probability given the new information that the first flip is H.

Problem 18.44. Roll 10 independent dice. Compute these probabilities:
(a) There's no 1.   (b) There's no 2.   (c) There's no 1 or 2.   (d) There's at least one 1.

Problem 18.45. Compute these probabilities.

(a) Independently flip 5 fair coins. What is $\mathbb{P}[\text{you get 4 or more heads}]$?

(b) You roll 4 independent fair dice. What is $\mathbb{P}[\text{exactly one 2 and one 4}]$?

(c) Independently generate 4 random bits $b_1 b_2 b_3 b_4$. Compute $\mathbb{P}[\sum_{i=1}^{4} b_i = 2]$.

(d) Independently generate 10 random bits $b_1 b_2 \cdots b_{10}$. What is the probability $b_1 \leq b_2 \leq \cdots \leq b_{10}$.

Problem 18.46. A 101-sided die is fair. Die faces are $1, \ldots, 101$. Compute these probabilities:

(a) In 10 rolls at least one 101 is rolled.   (c) The sum of two rolls equals k for $k \in \{2, \ldots, 202\}$.

(b) A pair of rolls match.   (d) Some number is rolled more than once in n rolls.

Problem 18.47. A 101-sided die is not fair (die faces are $1, \ldots, 101$). The probability to roll 101 is 100 times the probability of any other roll. All rolls other than 101 are equaly likely.

(a) Give the PDF for: (i) A single roll.   (ii) The sum of two rolls.

(b) Give the probability of: (i) At least one 101 in 10 rolls.   (ii) Doubles in a pair of rolls.

(c) What is the probability for some number to be rolled more than once (i) in three rolls?   (ii) in n rolls?

Problem 18.48. Let $\mathbf{X}$ be the number of father-genes in the gamete produced by the meiosis process in Problem 16.68. Give the PDF for $\mathbf{X}$. Does $\mathbf{X}$ have a Binomial distribution? Explain why or why not.

Problem 18.49. Passengers miss flights 10% of the time. FOCS-air has 9 seats and books 10 passengers; DMC-air has 18 seats and books 20 passengers. Which flight is over-booked more often?

Problem 18.50. A 500 student course with 28 lectures is taught in a lecture hall with 460 seats. Students attend lecture 90% of the time. Assume students are independent and independently attend each lecture.

(a) What are the chances a student won't have a seat in the first lecture. *[Hint: Problem 18.70 may be useful.]*

(b) What are the chances that in all 28 lectures, every student who attends lecture has a seat.

(c) How many seats are needed for at least a 99% chance that all lectures can accomodate all students who attend.

Problem 18.51. A hair-gene can be {a,a}, {b,b}, {a,b} or {b,a}. The pair {a,a} gives blonde hair and the other three pairs give black hair (b is "dominant"). One-third of black haired people are {b,b}. When two parents mate, an element from each parent's gene is randomly selected and combined to get the child's gene. 100 blonde men each produces a child with a random black haired women. Compute the probability of 30 blonde children.

Problem 18.52. Flip 20 fair coins. Now re-flip just once all coins which came up heads.

(a) Let $\mathbf{X}$ be the number of heads showing at the end. Give the PDF for $\mathbf{X}$, $P_\mathbf{X}$.

(b) What is the probability you end up with 5 heads showing at the end?

(c) What is the probability you flipped 5 heads in total (in both rounds of flipping)?

Problem 18.53. For independent $\mathbf{X}, \mathbf{Y}$, show: (a) $P_\mathbf{X}(x|\mathbf{Y} = y) = P_\mathbf{X}(x)$. (b) $\mathbb{P}[\mathbf{X} \leq x, \mathbf{Y} \leq y] = F_\mathbf{X}(x)F_\mathbf{Y}(y)$.

Problem 18.54. For independent $\mathbf{X}$ and $\mathbf{Y}$, let $\mathbf{U}(\omega) = f(\mathbf{X}(\omega))$ and $\mathbf{V}(\omega) = g(\mathbf{Y}(\omega))$, where f and g are arbitrary functions. Show that $\mathbf{U}$ and $\mathbf{V}$ are independent.

Problem 18.55. $\mathbf{X}$ and $\mathbf{Y}$ are random variables.

(a) Is there a joint PDF for which $\mathbf{X}$ and $\mathbf{Y}$ are independent but $\mathbf{X}^2$ and $\mathbf{Y}^2$ are not?

(b) Is there a joint PDF for which $\mathbf{X}^2$ and $\mathbf{Y}^2$ are independent but $\mathbf{X}$ and $\mathbf{Y}$ are not?

(c) If $\mathbf{X}$ can only take on 1 value, are $\mathbf{X}$ and $\mathbf{Y}$ independent?

Problem 18.56. Let $\mathbf{X}, \mathbf{Y}$ be independent random variables. Show that any two events $\mathcal{X}$ and $\mathcal{Y}$ where $\mathcal{X}$ is defined using $\mathbf{X}$ and $\mathcal{Y}$ is defined using $\mathbf{Y}$ are independent, $\mathbb{P}[\mathcal{X} \text{ AND } \mathcal{Y}] = \mathbb{P}[\mathcal{X}] \times \mathbb{P}[\mathcal{Y}]$.

Problem 18.57 (Bayes' Theorem). For random variables $\mathbf{X}, \mathbf{Y}$, show that

$$\mathbb{P}[\mathbf{X} = x \mid \mathbf{Y} = y] = \frac{P_{\mathbf{X}\mathbf{Y}}(x, y)}{P_\mathbf{Y}(y)} = \frac{P_{\mathbf{X}\mathbf{Y}}(x, y)}{\sum_x P_{\mathbf{X}\mathbf{Y}}(x, y)}$$

Problem 18.58 (Transformations). A random variable $\mathbf{X}$ has PDF $P_\mathbf{X}(x)$ and CDF $F_\mathbf{X}(x)$.

(a) For $\mathbf{Y} = a\mathbf{X} + b$ with $a > 0$, show that $F_\mathbf{Y}(y) = F_\mathbf{X}((y - b)/a)$.

(b) For $\mathbf{Y} = \mathbf{X}^2$, show that $F_\mathbf{Y}(y) = F_\mathbf{X}(\sqrt{y}) - F_\mathbf{X}(-\sqrt{y}) + P_\mathbf{X}(-\sqrt{y})$ (assume $y \geq 0$).

Problem 18.59. Let $\mathbf{X}_1, \ldots, \mathbf{X}_n$ be random variables. Define joint and conditional PDFs:

$$P(x_1, \ldots, x_n) = \mathbb{P}[\mathbf{X}_1 = x_1 \text{ AND } \mathbf{X}_2 = x_2 \text{ AND } \cdots \text{ AND } \mathbf{X}_n = x_n];$$
$$P(x_i \mid x_1 \ldots, x_{i-1}) = \mathbb{P}[\mathbf{X}_i = x_i \mid \mathbf{X}_1 = x_1, \mathbf{X}_2 = x_2, \ldots, \mathbf{X}_{i-1} = x_{i-1}]$$

(a) Show that $P(x_1, \ldots, x_n) = P(x_1) \cdot P(x_2 \mid x_1) \cdot P(x_3 \mid x_1, x_2) \cdots P(x_n \mid x_1 \ldots, x_{n-1})$.
(b) Define independence for n random variables. (Relate the joint PDF to the marginals.)

Problem 18.60. Suppose $\mathbf{X}$ and $\mathbf{Y}$ are independent, taking values in the same set V.
(a) If $\mathbf{X}$ is a uniform random variable, show that $\mathbb{P}[\mathbf{X} = \mathbf{Y}] = 1/|V|$.
(b) If $\mathbf{X}$ and $\mathbf{Y}$ have the same marginal distribution, show that $\mathbb{P}[\mathbf{X} = \mathbf{Y}] \geq 1/|V|$.
(c) In general, $0 \leq \mathbb{P}[\mathbf{X} = \mathbf{Y}] \leq 1$. Give joint distributions that achieve both bounds.

Problem 18.61 (Clinical Trials). Patients are randomly placed into control and treated groups with 50 controls and 100 treated. A placebo is given to the controls and the drug to the treated. The probability that a patient is cured is p_c for controls and p_t for treated. We don't know p_c or p_t. We know:
- p_c is either 0.4, 0.5 or 0.6 and each possibility is equally likely.
- With probability 1/2 the drug has no effect ($p_t = p_c$). With probability 3/10 the drug has a 10% positive effect ($p_t = p_c + 1/10$). With probability 1/5 the drug has a 10% detrimental side-effect ($p_t = p_c - 1/10$).

Patients are independent. In the study, 27 in the control group are cured and 63 in the treated group are cured. Find the probabilities of the 9 combinations for p_c, p_t: (a) Before the clinical trial.   (b) After the clinical trial.

Problem 18.62. You drive 500 times every year (to and from work). You speed 5% of the time. When you speed, chances of a ticket are 1%. On any given year, compute the probabilities you get $0, 1, 2$ and 3 or more tickets.
In 2014 about 41 million tickets were issued. The US population was about 317 million. About half the population commutes to work and 90% of commuters drive. Does this data reasonably match the model?

Problem 18.63. Each edge In a 10-vertex graph is independent and present with probability p.
(a) For $p \in \{0.01, 0.02, 0.03, \ldots, 0.99\}$, compute $\mathbb{P}[\text{graph has 10 edges}]$ and give a plot versus p.
(b) Use Monte Carlo to estimate the probability the graph is connected for each value of p in (a). Plot the probability to be connected versus p. (Randomly generate graphs. The fraction of connected graphs estimates the probability.)

Problem 18.64. A drunk starts a random walk (page 250) at 0 with probability $2/3$ to step left. His position $\mathbf{X} \in \{0, \pm 1, \pm 2, \ldots\}$ has PDFs after 1, 2 and 3 steps as shown below.

		-4	-3	-2	-1	0	1	2	3	4	
						drunk's position x					
1 step $P_{\mathbf{X}}(x)$	$\cdots$	0	0	0	2/3	0	1/3	0	0	0	$\cdots$
2 step $P_{\mathbf{X}}(x)$	$\cdots$	0	0	4/9	0	4/9	0	1/9	0	0	$\cdots$
3 step $P_{\mathbf{X}}(x)$	$\cdots$	0	8/27	0	4/9	0	2/9	0	1/27	0	$\cdots$

Plot the PDF for the drunk's position after the drunk has taken 10 and 20 steps. Show the result of a Monte Carlo simulation to experimentally confirm your answer. *[Hint: You could solve this problem in one of two ways: Use the build up method and relate the $(k+1)$-step $P_{\mathbf{X}}$ to the k-step $P_{\mathbf{X}}$; or, relate $P_{\mathbf{X}}$ to a Binomial distribution.]*

Problem 18.65 (Noisy Channels). A message $m_1 \cdots m_n$ of n bits is sent over a link that independently flips bits with probability $1/10$. You send each bit $2k+1$ times. The receiver "decodes" the $2k+1$ received bits per message-bit by majority vote, yielding the received message $r_1 \cdots r_n$.
(a) The message is garbled if even one bit is decoded incorrectly. What is the smallest k for which you can recover the message at least 99.9% of the time?
(b) Using error correction, you can tolerate ϵn incorrect bits (constant fraction of error). If $\epsilon = 1/10$, what is the smallest k allowing message recovery at least 99.999% of the time.

Problem 18.66. A device with 100 independent components fails if four or more components fail. The failure probability is $p = 0.01$ on a given year. Compute (a) $\mathbb{P}[\text{device fails in year 1}]$.   (b) $\mathbb{P}[\text{device lasts more than 5 years}]$.

Problem 18.67. In Roulette, a straight-up bet for \$1 wins \$35 with probability $1/38$ and otherwise loses the \$1. You start with \$105 and place 105 straight-up bets \$1. Are you more likely than not to come out ahead?

Problem 18.68. Let $\mathbf{X}$ be the number of successes in n independent trials and $\mathbf{Y}$ the number of successes in m additional trials. The success-probability is p in all trials. Let $\mathbf{Z} = \mathbf{X} + \mathbf{Y}$. Give the PDF of $\mathbf{Z}$. Hence, show that if $\mathbf{X} \sim B(n, p)$ and $\mathbf{Y} \sim B(m, p)$ are independent then $\mathbf{X} + \mathbf{Y} \sim B(n + m, p)$.

Problem 18.69 (Binomial Probabilities). Flip a coin n times, with heads-probability p. Find the probabilities:

(a) $\mathbb{P}[\text{zero H}]$ and $\mathbb{P}[\text{zero T}]$. Specialize to $p = 1/2$

(b) $\mathbb{P}[\text{at least one H}]$ and $\mathbb{P}[\text{at least one T}]$. Specialize to $p = 1/2$

(c) $\mathbb{P}[\text{number of H is even}]$. Specialize to $p = 1/2$. *[Hint: $(x + y)^n - (y - x)^n$. See also Problem 16.94.]*

Problem 18.70 (Computing Binomial Probabilities). The formula $B(k; n, p) = \binom{n}{k} p^k (1 - p)^k$ is numerically unstable. For example, $B(0; 1000, 1/3) = (1/3)^{1000}$ which is numerically 0 on most computing platforms.

(a) Fix n and p and let $L_k = \ln B(k; n, p)$. What is L_0?

(b) Show that $L_{k+1} = L_k + \ln\left(p(n - k)/(1 - p)(k + 1)\right)$ for $k = 0, \ldots, n - 1$.

(c) For $n = 1000$ and $p = 1/3$, plot $B(k; n, p) = e^{L_k}$ versus k.

Problem 18.71. For the Binomial distribution $B(k; n, p) = \binom{n}{k} p^k (1 - p)^k$, fix $p = 1/3$.

(a) For $n = 10, 20, \ldots, 100$, let k^* maximize $B(k; n, p)$. Plot k^*/n versus n. Make a guess for $k^*(n)$ and prove it.

(b) Plot the maximum probability $B(k^*; n, 1/3)/\sqrt{n}$ versus n. Make a guess for $B(k^*; n, p)$ and prove it.

Problem 18.72. For the Binomial distribution $B(k; n, p) = \binom{n}{k} p^k (1 - p)^k$, let $M(n, p)$ be the probability that a (strict) majority of at least $\ell = \lceil (n + 1)/2 \rceil$ trials are a success.

(a) Express $M(n, p)$ as a sum. Show: (i) $M(n, p)$ is increasing in p. (ii) For $p > 1/2$, $M(n, p)$ is increasing in n.

(b) Fix $p > 1/2$ and prove:

$$1 - \frac{p}{2p - 1} \binom{n}{\ell} p^{n-\ell} (1 - p)^\ell \le M(n, p) \le 1 - \binom{n}{\ell} p^{n-\ell} (1 - p)^\ell.$$

Problem 18.73. You and a friend independently and repeatedly try to access a wireless channel, randomly with probability p at each step. The channel is accessible if one of you (not both) try to access. Let $\mathbf{X}$ be how long you wait for a first access and $\mathbf{Y}$ how long your friend waits. Give the PDF of: (a) $\mathbf{X}$ (b) $\mathbf{Y}$ (c) $\mathbf{Z} = \mathbf{X} - \mathbf{Y}$.

Problem 18.74 (Multinomial). Pick 10 fruits independently with probabilities: pear $1/2$; apple $1/3$; orange $1/6$. Compute the probabilities to get: (a) 5 pears. (b) 5 pears and 2 apples. (c) At least 5 pears or at least 2 apples.

Problem 18.75 (Zipf or Power Laws). Randomly pick an English word. We plot a word's probability versus its usage rank. You get close to a power law PDF, $P(\text{rank}) = \alpha/(\text{rank})^\beta$, which is linear on a log-log scale. Here is a simple model that could explain the power law. Randomly type letters a, b or space $\sqcup$. Everytime a space appears, you have created a new word.

(a) Write a program to randomly type 100 million symbols. Collect the words and their frequencies and give a log-log plot of frequency versus rank.

(b) Show that words with rank around 2^i have probability about $(1/3)^i$. Get theoretical estimates of α and β and compare with the Monte Carlo in (a).

(c) Repeat for an alphabet of just one letter a and three letters a, b, c.

(Power laws are everywhere from city population distribution to wealth distribution.)
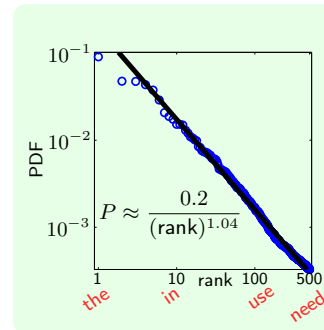
Problem 18.76 (Waiting Time is "Memoryless"). With a success-probability of p, you made τ trials with no success. Let $\mathbf{X}$ be the total trials to the first success.

(a) Compute the probability to wait an additional t trials, $\mathbb{P}[\mathbf{X} = \tau + t \mid \mathbf{X} > \tau]$.

(b) Why do we say that the waiting time is "memoryless"?

Problem 18.77 (Waiting for r Successes). Let the success-probability in a trial be p. Let $\mathbf{X}$ be the waiting time for r successes. Derive the PDF of $\mathbf{X}$, i.e. compute $\mathbb{P}[\mathbf{X} = t]$.

(a) At which step is the rth success? In how many ways can you arrange the first $r - 1$ successes?

(b) Show that $P_\mathbf{X}(t) = \binom{t-1}{r-1} p^r (1 - p)^{t-r}$.

(c) Show that (c) matches the PDF of the waiting time for one success when $r = 1$.

Problem 18.78 (Waiting for k successes and ℓ failures). Let $\mathbf{X}$ be the waiting time for k successes and ℓ failures with success probability p. Derive the PDF of $\mathbf{X}$ below. Verify using Monte Carlo for $p = 1/2, k = 2, \ell = 6$.

$$P_{\mathbf{X}}(t) = \begin{cases} 0 & t < k + \ell; \\ \binom{t-1}{k-1}p^k(1-p)^{t-k} + \binom{t-1}{\ell-1}p^{t-\ell}(1-p)^{\ell} & t \geq k + \ell. \end{cases}$$

Problem 18.79 (Successes in n Trials). A trial succeeds with probability p and you have a budget of n trials. Let $\mathbf{X}$ be the number of successes. In this problem, derive the PDF for $\mathbf{X}$ in two ways, and in so doing, you will produce a combinatorial proof of a famous combinatorial summation. You must compute $P_{\mathbf{X}}(k) = \mathbb{P}[\mathbf{X} = k]$.

(a) Show that $P_{\mathbf{X}}(k) = \binom{n}{k}p^k(1-p)^{n-k}$.
(b) Use the waiting time distribution for k successes to derive $P_{\mathbf{X}}(k)$:
   (i) Show that the trial on which the kth success occurs must be one of $k, k+1, \ldots, n$.
   (ii) Where does the $(k+1)$th success occur?
   (iii) Use the law of total probability to show that

$$\mathbb{P}[\mathbf{X} = k] = \sum_{i=k}^{n} \mathbb{P}[k\text{th success at } i] \cdot \mathbb{P}[(k+1)\text{th success after } n \mid k\text{th success at } i].$$

   (iv) Show that $\mathbb{P}[(k+1)\text{th success after } n \mid k\text{th success at } i] = (1-p)^{n-i}$.
   (v) Use Problem 18.77 to show $\mathbb{P}[\mathbf{X} = k] = p^k(1-p)^{n-k} \sum_{i=k-1}^{n-1} \binom{i-1}{k-1}$.
(c) Prove the identity $\sum_{i=m}^{n} \binom{i}{m} = \binom{n+1}{m+1}$. (Upper summation of binomial coefficients.)

Problem 18.80 (Interviewing/Optimal Dating). Here is a model for dating to find an optimal spouse. You date in a random order n candidates having distinct values $v_1, v_2, \ldots, v_n$. Here are the rules.
   I. When you date (interview) candidate i you can determine his/her value v_i.
   II. After determining v_i you must decide to accept or reject candidate i.
        If you accept, you stop dating, get married and settle down.
        If you reject, it too is final - no second chances.
   III. You must get the best candidate (or else there is potential for scandal).

What are your chances of finding the optimal spouse, getting married, and living happily ever after? One strategy is to date the first K potential partners with no intention of settling down. During this exploration phase, you learn what's out there ("playing the field"). After K candidates, you now accept any candidate that beats all previous candidates. It turns out this type of strategy is best. What is the optimal value of K and what are your chances of success?

(a) Let $\mathbf{X}$ be the position of the best spouse. What is the PDF of $\mathbf{X}$?
(b) Fix K. Compute $\mathbb{P}[\text{success} \mid \mathbf{X} = i]$. *[Hint: Where's the best of the first $i - 1$ candidates?]*
(c) For given K, let $Q(K) = \mathbb{P}[\text{success}]$. Show $Q(K) = n(H_n - H_K)/K$, where $H_n = 1 + 1/2 + \cdots + 1/n$ is the nth Harmonic number. *[Hint: Law of total probability.]*
(d) Let K^* maximize $Q(K)$. Show that $H_n - 1 \leq H_{K^*} < H_n - 1 + 1/K^*$. Hence, show that $K^* \to \infty$, and $H_{K^*} \to H_n - 1$ (for $n \to \infty$). *[Hint: Analyze $Q(K+1) - Q(K)$.]*
(e) Use $H_n \approx \ln n + 0.577$ and $H_{K^*} \to H_n - 1$ to show $K^* \to n/e$ and $Q(K^*) \to 1/e$ (for $n \to \infty$). (Surprisingly, chances of success with a million sequential suitors is about 37%)
(f) Assume people date "seriously" from age 20-40 years and at a uniform rate (e.g. 1 date per month). At what age should you stop "playing the field" and get ready to settle down if someone comes along who beats all others you have dated? (Census data: $\sim 35\%$ of marriages last 25 years; divorce is least likely when marriage-age is 28-32.)

Problem 18.81 (Hypergeometric). A crate has 50 bulbs, 10 are defective. You randomly pick 10 bulbs without replacement. Let $\mathbf{X}$ be the number of defective bulbs in the 10 you picked. Give the PDF of $\mathbf{X}$.
Generalize to the case where there are n bulbs, m are defective and you pick k bulbs. Let $\mathbf{X}$ be the number of defective bulbs in the k you picked. Give the PDF of $\mathbf{X}$, $P_{\mathbf{X}}(x; n, m, k)$.

Problem 18.82. A lake has 600 fish and 60 have been marked by a biologist in a study. A year later, the biologist randomly caught (without replacement) 60 fish. Give the PDF for the number of marked fish in the second sample. What if there is a 10% chance of a fish dying after a year? Give the new PDF.

Problem 18.83 (Mark and Recapture). The number of fish in a lake is $\mathbf{X} \in [200, 400]$, with each value of $\mathbf{X}$ being equally likely. In a study, a biologist randomly caught 40 fish (without replacement), marked them and replaced them in the lake. The next day the biologist caught 40 random fish and found 20 to be marked.

(a) What was the PDF of $\mathbf{X}$ before the biologist did anything?

(b) What is the updated PDF of $\mathbf{X}$ after finding that 20 fish in the new sample are marked (give a plot)?

(c) What is the most likely number of fish in the lake?

Problem 18.84. A box has $\mathbf{N}$ fair coins. $\mathbf{N}$ is unknown and has a Poisson PDF, $\mathbb{P}[\mathbf{N} = k] = e^{-2}2^k/k!$. You flip all the coins. What is the PDF for the number of H flipped?

Problem 18.85 (Multinomial). A fair die is rolled n times (independently). What is the probability to get:

(a) $n/2$ ones and $n/2$ fours? (Assume n is even.)

(b) k_1 ones, k_2 twos , k_3 threes , k_4 fours, k_5 fives and k_6 sixes, where $k_i \geq 0$ and $k_1 + k_2 + \cdots + k_6 = n$?

Problem 18.86 (Poisson PDF). The Binomial distribution $B(k; n, p)$ is the probability of k successes in n trials with success probability p. Let $p = \lambda/n$ for n large (many trials with vanishing success probability per trial).

(a) Show that $P_{\mathbf{X}}(k) = (\lambda^k/k!) \times (1 - \lambda/n)^{n-k} \times (n(n-1) \cdots (n - (k-1)))/n^k)$.

(b) For λ, k fixed and $n \to \infty$, show that $P_{\mathbf{X}}(k) \to e^{-\lambda}\lambda^k/k!$. (The Poisson PDF which models the number of "arrivals" in many applications: helpdesk-calls in a day; gamma-rays in an hour; insurance claims in a year; traffic at an intersection.)

Problem 18.87 (Poisson-Binomial). Give the PDF for the number of successes in 10 trials with success-probabilities in the trials being: $(\frac{1}{10}, \frac{1}{10}, \frac{3}{10}, \frac{4}{10}, \frac{5}{10}, \frac{6}{10}, \frac{6}{10}, \frac{7}{10}, \frac{8}{10}, \frac{9}{10})$. Compare with the Binomial PDF for 10 trials, each having success-probability $1/2$ (equal to the average). *[Hint: Let $Q(r, k) = \mathbb{P}[r$ successes in the first k trials].]*

Problem 18.88 (Banach's Matchbox). Kilam has two matchboxes, one in his left pocket and one in his right. The matchboxes start with 100 matches. Each time Kilam needs a match he is equally likely to use one from either pocket. The first time Kilam reaches for a match and finds the matchbox empty, let $\mathbf{X}$ be the number of matches in the other box. Give the PDF of $\mathbf{X}$ and verify it with Monte Carlo.

Problem 18.89. Pick numbers randomly from $\{1, \ldots, 100\}$ with replacement until their sum exceeds 100. Let $\mathbf{X}$ count how many numbers are picked. Give the PDF for $\mathbf{X}$ and verify it with Monte Carlo. Generalize to picking from $\{1, \ldots, n\}$ until the sum exceeds n?

Problem 18.90 (Random Graphs). A graph with n nodes $v_1, \ldots, v_n$ is a random graph if every edge (v_i, v_j) is independent and present in the graph with probability p.

(a) Compute the probability that there are k edges in the graph, as a function of n and p.

(b) Let $\mathbf{D}_i$ be the degree of node v_i. Are $\mathbf{D}_1$ and $\mathbf{D}_2$ independent?

(c) Give the joint distribution for $(\mathbf{D}_1, \mathbf{D}_2)$. You must compute $\mathbb{P}[\mathbf{D}_1 = d_1 \text{ AND } \mathbf{D}_2 = d_2]$. *[Hint: Law of total probability with the two cases: edge (v_1, v_2) is present or not.]*

Problem 18.91 (Hitting Time). A drunk starts at a bar and randomly walks left or right.

(a) His house is 10 steps to the left. Let $\mathbf{H}$ be the number of steps it takes the drunk to reach home, called the hitting time. Use Monte Carlo to estimate the PDF of $\mathbf{H}$, and give a plot.

(b) The drunk continually wanders until he comes back to the bar. Let $\mathbf{R}$ be the number of steps it takes the drunk to come back to the bar, called a return time. Use Monte Carlo to estimate the PDF of $\mathbf{R}$, and give a plot.

(c) Use the techniques from Problem 13.94 to analytically compute the PDF for the hitting time $\mathbf{H}$ and compare with your Monte Carlo simulation. *[Hint: Compute $\mathbb{P}[hitting\ time > x]$.]*

19.3   Problems

Problem 19.1. Which best describes the expected value of a random variable $\mathbf{X}$?
  (a) It is the typical observed value of $\mathbf{X}$ in an experiment.
  (b) It is the most likely value of $\mathbf{X}$ to be observed in an experiment.
  (c) It is just one of the possible values of $\mathbf{X}$ that can be observed in an experiment.
  (d) None of the above. If so, how do you explain the expected value to a lay-person?

Problem 19.2. Give examples of a random variable $\mathbf{X}$ with the following properties. You must give the PDF of $\mathbf{X}$.
  (a) $\mathbb{E}[\mathbf{X}] > 1$ but $\mathbb{P}[\mathbf{X} > 1] \approx 0$.   (b) $\mathbb{E}[\mathbf{X}] = 1$ but $\mathbb{P}[\mathbf{X} = 1] = 0$.   (c) $\mathbb{E}[\mathbf{X}] > 1$ but $\mathbb{P}[\mathbf{X} > 1] = 0$.

Problem 19.3. Suppose $\mathbb{E}[\mathbf{X}] = \mu$. Show that $\mathbb{P}[\mathbf{X} \geq \mu] > 0$ and therefore, there must be an outcome ω for which $\mathbf{X}(\omega) \geq \mu$. Similarly, there must be an outcome ω for which $\mathbf{X}(\omega) \leq \mu$.

Problem 19.4. You roll a loaded 6-sided die (values 1,...,6). Each even roll is twice as likely as each odd roll. What is the expected value of a single roll of this loaded die?

Problem 19.5. Let $\mathbf{X}$ and $\mathbf{Y}$ be two independent dice rolls. Define $\mathbf{Z} = \mathbf{X} + 2\mathbf{Y}$. Give the PDF of $\mathbf{Z}$ and $\mathbb{E}[\mathbf{Z}]$.

Problem 19.6. Compute the expected value of a random variable having each PDF in Problem 18.4.

Problem 19.7. Compute the expected value for each PDF in Figure 18.4 on page 268.

Problem 19.8. Roll a pair of fair dice until you get a sum of 6. What is the expected number of rolls?

Problem 19.9. Roll a fair die until you get a number greater than 1. Let $\mathbf{X}$ be the final roll.
  (a) How many rolls do you expect to make?   (b) What is $\mathbb{E}[\mathbf{X}]$?

Problem 19.10. Flip a fair coin. If it is H you pay $\$10$. If it is T, flip again: if the second flip is H you pay $\$10$, and if T you get $\$40$. Compute the expected gain. How much would you pay to play this game?

Problem 19.11. An artwork's value $\mathbf{X}$ is uniformly distributed on $\{\$100, \$101, \ldots, \$200\}$. If you bid b, you get the artwork if $b \geq \mathbf{X}$, and its value value doubles, so your profit is $2\mathbf{X} - b$. What bid maximizes your expected profit?

Problem 19.12. A game costs $\$x$ to play. You toss 4 fair coins. If you get more heads than tails, you win $\$10 + x$ for a profit of $\$10$. Otherwise, you lose and get nothing back, so your loss is $\$x$. What is your expected profit?

Problem 19.13. A die is rolled 3 times. After each roll, you may accept the value rolled as payoff and leave, or continue to the next roll. How much would you pay to play this game?

Problem 19.14. In a gamble, your payoff is the maximum of three fair dice rolls. How much would you pay to play?

Problem 19.15. You make 105 straight-up bets for $\$1$ in Roulette (Problem 18.67). What is your expected profit?

Problem 19.16. In a dice game, if you roll 1, the game stops and you win $\$1$. For any other roll, you must decide whether to stop and win the value rolled, or continue rolling. Your strategy is to stop if the roll is τ or larger (you may choose $\tau \in \{2, \ldots, 6\}$). How much will you pay to play? (See also Problem 18.15.)

Problem 19.17. A drive fails on year t with probability $f(t) = 2^{-t}$. The drive survived to year 2. What is the expected lifetime of the drive? What if $f(t) = t^{-1}/H_{10}$ for $t \in \{1, \ldots, 10\}$? (H_{10} is the 10th Harmonic number.)

Problem 19.18. 10% of drives are defective. A test for identifying defective drives has accuracy 90%. You tested 1000 drives and 150 failed the test. What is the expected number of defective drives among the 1000?

Problem 19.19. Children are independent and both sexes are equally likely. A randomly selected child in a family is male. Do you expect him to have an equal number of brothers and sisters?

Problem 19.20. A royal family has children until it has a boy or three children, whichever comes first. Children are independent and each sex is equally likely. Find the expected number of princes and the expected number of princesses.

Problem 19.21. A keychain has 10 similar keys. You are fumbling in the dark trying each key in a random order to open your appartment door. What is the expected number of keys you try before you unlock the door?

Problem 19.22. You randomly guess every answer on a multiple choice exam with 50 questions and 4 possible answers per question. What is the expected number of questions you answer correctly?

Problem 19.23. What is the expected number of rolls of a fair 6-sided die until you roll a 6?

Problem 19.24. How many children do you expect to sample until you find someone born on December 25th?

Problem 19.25. You may invest in a particular project. There is a 35% chance to lose $30,000$, a 40% chance to break even, and a 25% chance to make $55,000$. Based solely on this information, what should you do?

Problem 19.26. A bag has 2 red and 3 blue balls. You randomly pick balls without replacement. You win $1 for each red ball and lose $1 for each blue ball. You may stop picking at any time. How much would you pay to play?

Problem 19.27. In a race with 3 horses, horse i wins with probability $i/6$. You start with $1 and bet b_i on horse i. If horse i wins, you get back $b_i o_i$. (o_i is the payoff-odds for horse i.)
(a) If horse i wins, show that your wealth increases by $b_i o_i - \sum_{i=1}^{3} b_i$.
(b) If $(o_1, o_2, o_3) = (5, 4, 2)$, show how to guarantee a profit. In general, show this if $\sum_i 1/o_i < 1$.
(c) Let $(o_1, o_2, o_3) = (4, 7/2, 2)$. How will you place bets to maximize the expected profit.
(d) For (c), how will you place bets to maximize the expected return, where return $= \ln(\text{profit})$.

Problem 19.28. In a lottery, for $1 you pick any 5 different numbers from $\{1, \ldots, 75\}$. Then, 5 different numbers are randomly picked from $\{1, \ldots, 75\}$. If your numbers match those drawn in any order, you win $15,000,000$. Compute the probability to win and your expected winnings.

Problem 19.29. A lottery runs every month. For $1, you pick an 8-digit number, e.g. 03312014. The lottery takes 10% of the $1 and the remainder goes into the jackpot. The lottery picks a random 8-digit string and all matching tickets evenly split the jackpot. The jackpot grows until someone wins. Every month, 100 million people play the lottery.
(a) Assume everyone bets a random 8-digit number.
  (i) What is your expected winning on the first month of the lottery?
  (ii) Nobody wins on the first month. What is your expected winning on the second month?
  (iii) After how many months of unclaimed jackpot is it "profitable" to play the lottery?
(b) Assume everyone bets a valid date (birthday, anniversary, etc.) `mmddyyyy`, e.g. 03312014.
  (i) What strategy will you use to pick a number and why?
  (ii) What is your expected winning on the first month of the lottery?
  (iii) Nobody wins on the first month. What is your expected winning on the second month?
  (iv) After how many months of unclaimed jackpot is it "profitable" to play the lottery?

Problem 19.30. A drunk starts at 0 and takes independent steps left with probability $1/3$ and right with probability $2/3$. What is the expected position of the drunk after 100 steps?

Problem 19.31. You bet $1 on a fair coin toss: if H, you double your money; if T, you lose your bet. If you lose, you double your bet and play again. Compute your expected profit if:
(a) You continue betting until you win or have made n coin tosses.
(b) You continue betting until you win with no limit on the number of tosses.

Problem 19.32. You got all heads in 10 flips of a random coin from a jar with 9 fair coins and 1 two-headed coin. Compute the expected number of heads in another 100 flips of the same coin.

Problem 19.33. Toss 9 fair coins. Toss another 9 coins if and only if you got more heads than tails. Let $\mathbf{X}$ be the total number of heads you toss. What is $\mathbb{E}[\mathbf{X}]$?

Problem 19.34. Compute $\mathbb{E}[\text{number of 1s}]$ in the BITWISE-OR of two 10-bit sequences of independent random bits (1/0 are T/F). E.g.,0001110010 BITWISE-OR 1000111000 = 1001111010).

Problem 19.35. Hospitals BIG and SMALL deliver 200 and 100 babies per day respectively. A day is unusual if 60% or more of births are one sex. In a year, what is the expected number of unusual days in hospital BIG versus SMALL?

Problem 19.36. A bag has 3 white and 1 black ball and another has 1 white and 3 black balls. Pick a random bag (probability $1/2$ for each bag) and a random ball from that bag (probability $1/4$ for each ball). The ball is white. Let $\mathbf{X}$ be the number of white balls in the other bag. What is $\mathbb{E}[\mathbf{X}]$? (The **information** "the ball is white" is crucial.)

Problem 19.37. It rains 1 in 7 days and is cloudy 1 in 5 days. Assume a year has 366 days.
(a) What is the expected number of rainy days in a year?
(b) What is the expected number of rainy days on a year with: (i) 100 cloudy days   (ii) At least 50 cloudy days?

Problem 19.38. Pick a random coin from a box with 6 fair and 4 two-headed coins. What is the expected number of heads in 10 flips.

Problem 19.39. A box has 1024 fair and 1 two-headed coin. You pick a coin randomly, make 10 flips and get all H.
  (a) You flip the same coin you picked 100 times. What is the expected number of H?
  (b) You flip the same coin you picked until you get H. What is the expected number of flips you make?

Problem 19.40. Pick random numbers from $\{1, \ldots, 100\}$ with replacement until their sum exceeds 100. How many numbers do you expect to pick. Can you generalize to numbers from $\{1, \ldots, n\}$ until the sum exceeds n?

Problem 19.41. A password must be a permutation of $\{0, 1, \ldots, 9\}$. Your birthday is 12/24 (Dec. 24), so for security reasons, your password can't contain the substrings 12 or 24. For example, 0213456789 is ok, but none of $\{0\textcolor{red}{12}3456789, 013\textcolor{red}{24}56789, 987654321, 0113456789, 03\textcolor{red}{12}456789\}$ are ok.
  (a) How many possible passwords can you set?
  (b) What is the expected number of tries to get an acceptable password if you randomly generate strings using:
      (i) Independent random permutations of $\{0, \ldots, 9\}$, with each permutation being equally likely?
      (ii) Independent random 10-digit strings, with each string being equally likely?
  (c) A hacker can test 10^5 passwords a second. What is the expected time to hack your account if:
      (i) The hacker randomly generates a permutation to test, each time independently.
      (ii) The hacker randomly generates the digits of a 10-digit string to test, each time independently.
      (iii) The hacker randomly orders all valid passwords (without 12 and 24) and tries each one from first to last.
      (iv) The hacker randomly orders all permutations of $\{0, \ldots, 9\}$ and tries each one from first to last.
      (v) The hacker randomly orders all 10-digit strings and tries each one from first to last.

Problem 19.42. For two independent dice rolls $\mathbf{D}_1$ and $\mathbf{D}_2$, let $\mathbf{X} = \mathbf{D}_1 + \mathbf{D}_2$ and $\mathbf{Y} = \mathbf{D}_1 - \mathbf{D}_2$.
  (a) Show that $\mathbb{E}[\mathbf{XY}] = \mathbb{E}[\mathbf{X}]\mathbb{E}[\mathbf{Y}]$.   (b) Are $\mathbf{X}$ and $\mathbf{Y}$ independent?

Problem 19.43 (Moment Generating Function). Let $\mathbf{X}$ be the waiting time to success with success-probability p. Let $\mathbf{Z} = e^{s\mathbf{X}}$ and let $M(s) = \mathbb{E}[\mathbf{Z}] = \mathbb{E}[e^{s\mathbf{X}}]$.
  (a) Show that $M(s) = p/(e^{-s} - 1 + p)$ within a certain range of s. What is that range for s?
  (b) Let $M^{(k)}(s) = \frac{d^k}{ds^k} M(s)$. Show that $\mathbb{E}[\mathbf{X}^k] = M^{(k)}(0)$. $\mathbb{E}[\mathbf{X}^k]$ is the kth moment of $\mathbf{X}$. The derivatives of $M(s)$ at $s = 0$ give the moments of $\mathbf{X}$. For this reason, $M(s)$ is called the moment generating function of $\mathbf{X}$.)
  (c) Use the moment generating function to compute $\mathbb{E}[\mathbf{X}]$, $\mathbb{E}[\mathbf{X}^2]$ and $\mathbb{E}[\mathbf{X}^3]$.
  (d) Let $\mathbf{X}$ and $\mathbf{Y}$ be independent random variables. Let $\mathbf{Z} = \mathbf{X} + \mathbf{Y}$ be the sum. Show that the moment generating function for $\mathbf{Z}$, when it exists, is the product of the moment generating functions for $\mathbf{X}$ and $\mathbf{Y}$, when they exist.

Problem 19.44. A random variable $\mathbf{X}$ takes values in $\{0, 1, 2, \ldots\}$. Let $G_{\mathbf{X}}(x) = \mathbb{P}[\mathbf{X} > x]$.
  (a) Show that $G_{\mathbf{X}}(x) = 1 - F_{\mathbf{X}}(x)$. ($F_{\mathbf{X}}$ is the CDF)   (b) Show that $\mathbb{E}[\mathbf{X}] = \sum_{x=0}^{\infty} G_{\mathbf{X}}(x)$.

Problem 19.45. A random variable $\mathbf{X}$ takes values in $\{0, 1, \ldots, n\}$ and has CDF $F_{\mathbf{X}}$.
  (a) Show that $\mathbb{E}[\mathbf{X}] = (n+1) - \sum_{x=0}^{n} F_{\mathbf{X}}(x)$.
  (b) Show that this result is consistent with Problem 19.44(b).
  (c) What happens here when $n \to \infty$? Why does Problem 19.44(b) still work?

Problem 19.46. Prove the following properties of expectations.
  (a) (i) $\mathbf{X} \geq t \to \mathbb{E}[\mathbf{X}] \geq t$.   (ii) $\mathbb{E}[\mathbf{X}] \geq t \to \mathbb{P}[\mathbf{X} \geq t] > 0$.   (iii) $\mathbf{X} \geq \mathbf{Y} \to \mathbb{E}[\mathbf{X}] \geq \mathbb{E}[\mathbf{Y}]$.
  (b) If $a \leq \mathbf{X} \leq A$ then $a\mathbb{E}[\mathbf{Y}] \leq \mathbb{E}[\mathbf{XY}] \leq A\mathbb{E}[\mathbf{Y}]$ for any random variable $\mathbf{Y}$.
  (c) **[Markov Inequality]** Suppose $\mathbf{X}$ is non-negative, $\mathbf{X} \geq 0$. Then, $\mathbb{E}[\mathbf{X}] \geq t\mathbb{P}[\mathbf{X} \geq t]$ for any $t \geq 0$.
      (i) Let the random variable $\mathbf{Y} = 0$ if $\mathbf{X} < t$ and $\mathbf{Y} = t$ if $\mathbf{X} \geq t$. Show that $\mathbf{X} \geq \mathbf{Y}$ and compute $\mathbb{E}[\mathbf{Y}]$.
      (ii) Prove Markov's Inequality using part (a)(iii).

Problem 19.47 (Total Expectation with Many Cases). Suppose $C_1, \ldots, C_k$ are events that partition Ω. This means no two events can co-occur and at least one event must occur, $\cup_{i=1}^{k} C_i = \Omega$ and $C_i \cap C_j = \varnothing$. Prove:

$$\mathbb{E}[A] = \sum_{i=1}^{k} \mathbb{E}[A \mid C_i] \cdot \mathbb{P}[C_i] = \mathbb{E}[A \mid C_1] \cdot \mathbb{P}[C_1] + \cdots + \mathbb{E}[A \mid C_k] \cdot \mathbb{P}[C_k].$$

Problem 19.48 (Expected value from joint PDF). Let $\mathbf{Z} = f(\mathbf{X}, \mathbf{Y})$ be a function defined using random variables $(\mathbf{X}, \mathbf{Y})$ with joint PDF $P_{\mathbf{XY}}(x, y)$. The expectated value is defined from the probability space by

$$\mathbb{E}[\mathbf{Z}] = \sum_{w \in \Omega} Z(w) \cdot P(\omega) = \sum_{\omega \in \Omega} f(\mathbf{X}(\omega), \mathbf{Y}(\omega)) \cdot P(\omega).$$

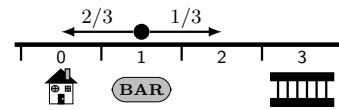Show that the expected value can be computed from the joint-PDF using a sum over all possible x and y:

$$\mathbb{E}[\mathbf{Z}] = \sum_{x \in \mathbf{X}(\Omega)} \sum_{y \in \mathbf{Y}(\Omega)} f(x, y) \cdot P_{\mathbf{XY}}(x, y).$$

Problem 19.49. Let $\mathbf{X}$ and $\mathbf{Y}$ have joint distribution $P_{\mathbf{XY}}(x, y)$. Let $\mathbf{Z} = f(\mathbf{X}, \mathbf{Y})$. Prove that

$$\mathbb{E}[\mathbf{Z}] = \sum_{x \in \mathbf{X}(\Omega)} P_{\mathbf{X}}(x) \sum_{y \in \mathbf{Y}(\Omega)} P_{\mathbf{Y}}(y \mid \mathbf{X} = x) f(x, y) = \sum_{x \in \mathbf{X}(\Omega)} P_{\mathbf{X}}(x) \mathbb{E}_{\mathbf{Y}}[f(x, \mathbf{Y}) \mid \mathbf{X} = x].$$

Problem 19.50 (Expected Hitting Time). Find the expected number of steps made by a drunk who leaves a bar at position 1 and takes independent steps: left (L) with probability $2/3$ or right (R) with probability $1/3$. The drunk stops if he reaches home (at position 0) or the lockup (at position 3).
(Home and the lockup are "barriers". The time to reach a barrier is called the hitting time.)

Problem 19.51. In Problem 19.50, find the expected hitting time if the drunk gets home (conditional expectation).

Problem 19.52. Generalize the expected hitting time in Problem 19.50 to p being the probability to move left and L the position of the lockup. Let E_k be the expected number of steps when starting at position k. Let $\beta = p/(1-p)$.
  (a) What are E_0 and E_L? Show that for $0 < k < L$, $E_k = 1 + pE_{k-1} + (1-p)E_{k+1}$.
  (b) Use (a) to show: $E_k = \dfrac{\beta+1}{\beta-1}\left(k - L\dfrac{\beta^k - 1}{\beta^L - 1}\right)$. *[Hint: $\sum_{i=0}^n i\beta^i = (n\beta^{n+1} - (n+1)\beta^{n+1} + \beta)/(\beta - 1)^2$.]*

Problem 19.53. A gambler walks into a casino with \$50 and plays roulette. The gambler bets \$1 on red (probability $18/36$ to win) and keeps betting until either going bankrupt or doubling his money. If it takes about 1 minute to play one game of roulette, how many hours of entertainment does the gampler expect to have. *[Hint: Problem 19.52.]*

Problem 19.54 (Least-Squares Fit). You summarize a random variable $\mathbf{X}$ using a single number h. The squared error h makes in approximating $\mathbf{X}$ is $(h - \mathbf{X})^2$. Define the quality of h by its expected error, $\text{err}(h) = \mathbb{E}[(h - \mathbf{X})^2]$.
  (a) Show that $\text{err}(h) = h^2 - 2h\mathbb{E}[\mathbf{X}] + \mathbb{E}[\mathbf{X}^2]$.
  (b) Show that $h^* = \mathbb{E}[\mathbf{X}]$ is optimal, i.e. minimizes $\text{err}(h)$, and that h^* has expected squared error $\mathbb{E}[\mathbf{X}^2] - \mathbb{E}[\mathbf{X}]^2$.
This is a famous result: $\mathbb{E}[\mathbf{X}]$ is the estimator of $\mathbf{X}$ with minimum expected squared error.

Problem 19.55. The expected value summarizes a random variable $\mathbf{X}$. Another popular summary of $\mathbf{X}$ is a median, which is a "midpoint" of the PDF. We say <u>a</u> midpoint because the median may not be unique. The median is any value m for which at least half of the probability of $\mathbf{X}$ is at or below m and at least half is at or above m,

$$\mathbb{P}[\mathbf{X} \le m] \ge 1/2 \qquad \text{and} \qquad \mathbb{P}[\mathbf{X} \ge m] \ge 1/2.$$

x	0	1	2	3
$P_{\mathbf{X}}(x)$	$1/8$	$3/8$	$1/4$	$1/4$

  (a) Give all the medians for a random variable with PDF on the right.
  (b) Give all medians of the waiting time with success probability $1/5$.
  (c) Give all medians of a Binomial with 20 trials and success probability $1/5$

Problem 19.56 (Least-Absolute-Error Fit). You wish to summarize random variable $\mathbf{X}$ with PDF $P_{\mathbf{X}}$ using a number h, as in Problem 19.54. The error h makes in approximating $\mathbf{X}$ is the absolute error $|h - \mathbf{X}|$. The quality of h is the expected absolute error, $\text{err}(h) = \mathbb{E}[|h - \mathbf{X}|]$. Show that to minimize $\text{err}(h)$ you should pick h as a median of $\mathbf{X}$. (This is a famous result: the least-absolute-error or robust regression estimator of $\mathbf{X}$ is a median of $\mathbf{X}$.)

Problem 19.57. Toss two coins. Roll 6 dice for each H tossed. Compute the expected number of sixes.

Problem 19.58. A Martian couple has children until they have 2 males (sexes of children are independent). Compute the expected number of children the couple will have if, on Mars, males are:
  (a) Half as likely as females.   (b) Just as likely as females.   (c) Twice as likely as females.

Problem 19.59. A Martian couple has children until they have 2 males *in a row* (sexes of children are independent). Compute the expected number of children the couple will have if, on Mars, males are:
  (a) Half as likely as females.   (b) Just as likely as females.   (c) Twice as likely as females.

Problem 19.60. A team is equally likely to win or lose its first game. In each following game, the previous result is twice as likely as the opposite result. What is the expected number of games played to get two wins.

Problem 19.61.(Hard) Couples have children (at least 1) until they get an equal number of boys and girls (balance). Let $\mathbf{X}$ be the number of children a couple has. Use these steps to compute $\mathbb{E}[\mathbf{X}]$:

(a) Show that $\mathbb{P}[\mathbf{X} > k + 1] = 2^{-k} \binom{k}{k/2}$ for k even and $\mathbb{P}[\mathbf{X} > k + 1] = 2^{-k} \binom{k}{(k-1)/2}$ for k odd.

(b) Show that $4^k / \sqrt{4k} \leq \binom{2k}{k} \leq 4^k / \sqrt{3k+1}$ and use Problem 19.44 to show that $\mathbb{E}[\mathbf{X}] = \infty$.

(c) Compute $\mathbb{E}[\mathbf{X}]$ if there is a cap of N on the number of children?

Problem 19.62 (Derivatives and Sums). Differentiating under the summation is a useful technique for computing sums, which is important because expectations involve sums.

(a) Show that $a \dfrac{\partial}{\partial a} \sum\limits_{k=0}^{n} \binom{n}{k} a^k b^{n-k} = \sum\limits_{k=0}^{n} k \cdot \binom{n}{k} a^k b^{n-k}$.

  (i) Show that $\sum\limits_{k=0}^{n} k \cdot \binom{n}{k} a^k b^{n-k} = na(a + b)^{n-1}$.

  (ii) Use a similar approach to show that $\sum\limits_{k=0}^{n} k^2 \cdot \binom{n}{k} a^k b^{n-k} = (nab + n^2 a^2)(a + b)^{n-2}$.

(b) Show that $a \dfrac{\partial}{\partial a} \sum\limits_{k=0}^{n} a^k = \sum\limits_{k=0}^{n} k a^k$.

  (i) Show that $\sum\limits_{k=0}^{n} k a^k = \dfrac{a + na^{n+2} - (n+1)a^{n+1}}{(1-a)^2}$.

  (ii) Use a similar approach to show that

$$\sum_{k=0}^{n} k^2 a^k = \frac{a(a+1) - (n+1)^2 a^{n+1} + (2n^2 + 2n - 1)a^{n+2} - n^2 a^{n+3}}{(1-a)^3}.$$

  (iii) For $|a| < 1$, prove the infinite sums $\sum\limits_{k=0}^{\infty} k a^k = \dfrac{a}{(1-a)^2}$ and $\sum\limits_{k=0}^{\infty} k^2 a^k = \dfrac{a(a+1)}{(1-a)^3}$.

Problem 19.63. Let $\mathbf{X}$ be a Binomial on n trials with success probability p.

(a) Use Problem 19.62(a)(ii) to show that $\mathbb{E}[\mathbf{X}^2] = np(1-p) + n^2 p^2$.

(b) Use Exercise 19.6(b) on page 280 and (a) to show $\mathbb{E}[\mathbf{X}^2 - \mathbf{X}] = \mathbb{E}[\mathbf{X}^2] - \mathbb{E}[\mathbf{X}]$.

Problem 19.64. Let $\mathbf{X}$ be the waiting time with success probability p. Compute $\mathbb{E}[\mathbf{X}^2]$ in two ways:

(a) Use the PDF of $\mathbf{X}$ (infinite sum plus Problem 19.62(b)(iii)).   (b) Use the Law of Total Expectation.

Problem 19.65 (Expected Wait to r Successes). Let $\mathbf{X}$ be the waiting time for r successes with success probability p. Compute $\mathbb{E}[\mathbf{X}]$. Recall the PDF of $\mathbf{X}$ is (Problem 18.77)

$$P_{\mathbf{X}}(t) = \binom{t-1}{r-1} p^r (1-p)^{t-r}.$$

(a) Show that $\mathbb{E}[\mathbf{X}] = \sum\limits_{t=r}^{\infty} t \cdot \binom{t-1}{r-1} \beta^r (1-p)^t = r\beta^r \sum\limits_{t=r}^{\infty} \binom{t}{r}(1-p)^t$, where $\beta = p/(1-p)$.

(b) Show the combinatorial identity $\sum\limits_{i=0}^{\infty} \binom{r+i}{r} \alpha^i = 1/(1-\alpha)^{r+1}$.

  (i) Show that $\binom{r+i}{r}$ is the coefficient of α^i in the product of the r+1 terms:

$$(1 + \alpha + \alpha^2 + \cdots)(1 + \alpha + \alpha^2 + \cdots) \cdots (1 + \alpha + \alpha^2 + \cdots).$$

  (ii) Show that the product is equal to $1/(1-\alpha)^{r+1}$.

  (iii) Use (i) and (ii) to prove the combinatorial identity.

(c) Use the combinatorial identity to evaluate the summation and show $\mathbb{E}[\mathbf{X}] = r/p$.

Problem 19.66 (Stock-Trading). A stock has price $\$1000$. Every day it randomly goes up or down by $\$1$, with probability $1/2$ for each. You will trade this stock using a trading strategy for 100 days.

(a) A simple "buy and hold" strategy is to buy the stock on day 0 and sell it on the 100th day.
  (i) What is the expected profit?   (ii) What is the probability that the profit is positive.

(b) Another strategy buys the stock if the price is $\$1000$. If the stock reaches $\$1001$, sell and wait (if the price comes back down to $\$1000$, buy again and repeat). On the 100th day, sell any stock owned at the current price.
  (i) What is the expected profit?   (ii) What is the probability that the profit is positive. Verify with Monte Carlo.

Problem 19.67 (Game Theory). A lion can prowl the plain or water-hole. An impala can graze the plain or drink at the water-hole. If both are at the water, the lion (very happy) drinks water and eats the impala (very sad). If both are on the plain, the lion (happy) eats the impala (very sad). If the lion is on the plain, and the impala at the water, the impala (happy) drinks and the lion (very unhappy) has nothing. If the lion is at the water and the impala on the plain, the impala (happy) eats and the lion drinks.

Depending on who does what, the payoffs to each animal are summarized in the payoff-matrix to the right. Each box is a pair of actions, one for the lion and one for the impala. The payoffs to the lion are in red and the impala's payoffs are in green. For example, in the PLAIN-PLAIN box (both on the plain), the lion's payoff is $+5$ and the impala's payoff is -10.

The impala is on the plain with probability p. The lion is on the plain with probability q. The animals may change their probabilities and we assume that both animals know p and q.

(a) The impala picks an action randomly, $p = 1/2$. The lion chooses q to maximize his expected payoff. What will the expected payoffs be for lion and impala? Can the impala do better, knowing the lions choice of q?

(b) The impala assumes the lion observes p and maximizes his (the lion's) expected payoff. Is there a value p^* for which the lion is indifferent between PLAIN and WATER?

(c) Similarly, the lion assumes the impala observes q and maximizes his (the impala's) expected payoff. Is there a value q^* for which the impala is indifferent between PLAIN and WATER?

(d) The impala and lion choose p^* and q^* respectively. Can either animal increase their expected payoff by unilaterally changing their probability?

The pair (p^*, q^*) is a Nash equilibrium from which neither animal gains by deviating. The Nobel prize winner John Nash proved that such equilibria always exist.

Problem 19.68. J. B. S. Haldane, after a back of the envelope calculation, pronounced "I would gladly give up my life for two brothers or eight cousins." Justify this statement using the following simple model for genetics. There are two types of a gene for an important trait: the rare (and precious) type A occuring with probability x and the common type a occuring with probability $1 - x$. Each person has two copies of the gene. When two people mate to produce a child, one copy of the gene from each parent is randomly passed on to the child. For example, if the parents have genes (mom:Aa, dad:Aa), then the child will be AA with probability $1/4$, Aa with probability $1/2$ and aa with probability $1/4$. You have the precious type A (so your genes are either AA or Aa).

(a) Compute $\mathbb{P}[\text{you are } AA \text{ or } Aa \mid \text{your parents are } (AA, AA)]$. Repeat for your parents being (AA, Aa), (Aa, Aa), (AA, aa), (Aa, aa), (aa, aa).

(b) Compute $\mathbb{P}[\text{your parents are } (AA, AA) \mid \text{you are } AA \text{ or } Aa]$. Repeat for your parents being (AA, Aa), (Aa, Aa), (AA, aa), (Aa, aa), (aa, aa).

(c) Show that the chances your sibling is AA or Aa if you are is $(1 + x(1-x)/4)/(2 - x)$. As $x \to 0$ (A is rare), how many siblings do you give your life for, if the expected number of people with the A-gene mustn't decrease?

(d) By a similar analysis, show that if you have an A-gene, then your cousin has an A-gene with probability $(1 + x(9 - 9x + 15x^2 - 20x^3 + 8x^5))/(8 - 4x)$, which approaches $1/8$ as $x \to 0$.

Problem 19.69 (Exchange Paradox). You are randomly given one of two identical envelopes. One envelope contains twice as much money as the other. You are given the option to switch envelopes. You reason as follows:

1: My current envelope contains an amount A. The other envelope has $B = A/2$ or $B = 2A$.

2: Each possibility has probability $1/2$ since I was given a random envelope, so

$$\mathbb{E}[B] = \tfrac{1}{2} \times (A/2) + \tfrac{1}{2} \times (2A) = 5A/4.$$

3: The other envelope has a higher expected value than my current amount A, so I switch.

4: I am back in the same situation as step 1, and end up switching forever. 😣

Explain what is wrong with the reasoning above and resolve the paradox.

20.6 Problems

Problem 20.1. Let $\mathbf{X}$ and $\mathbf{Y}$ be independent dice rolls, and $\mathbf{Z} = \mathbf{X} + 2\mathbf{Y}$. Compute $\mathbb{E}[\mathbf{Z}]$.

Problem 20.2. Is $\mathbb{E}[\mathbf{X}|\mathbf{Y}]$ a function of $\mathbf{X}$, of $\mathbf{Y}$, of both $\mathbf{X}$ and $\mathbf{Y}$ or of neither $\mathbf{X}$ nor $\mathbf{Y}$?

Problem 20.3. Compute the expected value of each random variable in Problem 18.34.

Problem 20.4. Use linearity to compute $\mathbb{E}[\mathbf{X}_2]$ for the experiment on page 295 where the first die roll $\mathbf{X}_1$ determines how many dice are summed to give $\mathbf{X}_2$. Write $\mathbf{X}_2$ as the sum of 6 random variables,
$$\mathbf{X}_2 = \mathbf{Z}_1 + \mathbf{Z}_2 + \mathbf{Z}_3 + \mathbf{Z}_4 + \mathbf{Z}_5 + \mathbf{Z}_6,$$
where $\mathbf{Z}_i$ is additional die roll i if that roll is made and zero otherwise. A possible outcome is $(4; 2, 1, 2, 6)$ for which the first roll was 4 and the additional rolls are $\mathbf{Z}_1, \mathbf{Z}_2, \mathbf{Z}_3, \mathbf{Z}_4$ equal to $2, 1, 2, 6$ respectively and $\mathbf{Z}_5 = \mathbf{Z}_6 = 0$.
 (a) What is $\mathbb{P}[\mathbf{Z}_i = 0]$? Use total expectation with the two cases $\{\mathbf{X}_1 < i\}$ and $\{\mathbf{X}_1 \geq i\}$ to compute $\mathbb{E}[\mathbf{Z}_i]$.
 (b) Use linearity of expectation to compute $\mathbb{E}[\mathbf{X}_2]$.

Problem 20.5. A box contains numbers $1, \ldots, 100$. You randomly pick 5 numbers. Compute the expected sum when you pick numbers (a) *with replacement* (b) *without replacement*. Generalize to picking k numbers from $1, \ldots, n$.

Problem 20.6. In a document with M typos, *independent* proof-readers A and B respectively find a typos and b typos, with c typos in common. Let p_A (resp. p_B) be the probability that A (resp. B) detects a specific typo.
 (a) What is the expected number of typos found by: (i) A (ii) B (iii) Both A and B?
 (b) The typos found were corrected. Estimate the number of typos which remain.

Problem 20.7. In a round of speed-dating (Section 1.2 on page 8), 16 people $A, B, \ldots, P$ are randomly assigned seats at four tables with four seats per table. Two people meet if they sit at the same table.
 (a) Compute the probability that A will meet B during an evening with 4 rounds of speed-dating.
 (b) Show that every person expects to meet 8.856 people during an evening with 4 rounds of speed-dating.

Problem 20.8. You send a random number of packets, uniform on $\{1, 2, \ldots, 10^5\}$. A packet is resent until it reaches. A packet's size is also random, uniform on $\{1, 2, \ldots, 10^5\}$. In each case, find the expected time spent sending packets.
 (a) The chances a packet reaches its destination are 90% and it takes 0.01 sec. to send a packet, independent of size.
 (b) The chances a packet reaches its destination are 90% and it takes $(0.01 \times \text{size})$ sec. to send a packet.
 (c) A packet reaches its destination with probability $(1/\text{size})$ and it takes $(0.01 \times \text{size})$ sec. to send a packet.

Problem 20.9. A file manager stores each of 4000 files on one of 4 disks, randomly selected. The total size of all files is 500MB. Compute the expected: (a) Number of files on each disk.   (b) Amount of storage used on each disk.

Problem 20.10. Let $\mathbf{X}$ be the number of trials to success with success-probability p. Use iterated expectation to compute $\mathbb{E}[\mathbf{X}^3]$. Confirm your answer from the PDF by computing an infinite sum.

Problem 20.11. Ten sailors return from shore and sleep randomly in their ten bunks (one sailor per bunk).
 (a) Let $\mathbf{X}$ be the number of sailors in the correct bunk. Compute (i) $\mathbb{P}[\mathbf{X} = 10]$ (ii) $\mathbb{P}[\mathbf{X} = 9]$ (iii) $\mathbb{P}[\mathbf{X} = 8]$.
 (b) Compute the expected number of sailors in the correct bunk, that is $\mathbb{E}[\mathbf{X}]$.

Problem 20.12. You visit $\mathbf{N} \in \{1, 2, \ldots\}$ shops ($\mathbf{N}$ is random). At the ith shop, you spend $\mathbf{X}_i$ for $i = 1, \ldots, \mathbf{N}$. The $\mathbf{X}_i$ are random, having the same expected value μ. In total you spend $\mathbf{X}$. Show that your expected spending is the expected number of shops you visit times the expected spending in each shop, $\mathbb{E}[\mathbf{X}] = \mathbb{E}[\mathbf{N}] \cdot \mu$.

Problem 20.13. Let $\mathbf{X}_1$ be a random variable which takes values greater than 1, $\mathbf{X}_1 > 1$. Let $\mathbf{X}_2$ be the waiting time to success with success probability $(\mathbf{X}_1 - 1)/\mathbf{X}_1$.
 (a) Compute $\mathbb{E}[\mathbf{X}_2 \mid \mathbf{X}_1]$. What is it a function of?   (b) Show that $\mathbb{E}[\mathbf{X}_2] = 1 + \mathbb{E}\left[1/(\mathbf{X}_1 - 1)\right]$ (iterated expectation).

Problem 20.14. A Martian couple has children until 2 males. On Mars, males are half as likely as females and children are independent. Compute the expected number of children the couple will have.

Problem 20.15. 10,000 people are to be tested for a rare disease that affects 1% of the population. (10,000 tests.)
 (a) Group people into batches of 10 and do one test on all the blood in a batch. If the test is negative, all people in the batch are negative. In any positive batch, administer individual tests. What is the expected number of tests?
 (b) What is the best batch-size and the corresponding expected number of tests? (This is called optimal pooling.)
 (c) Can you do better than in part (b). Try to decrease the expected number of tests as much as you can.

Problem 20.16. Chemical compounds $C_1, C_2, \ldots, C_n$ are placed in buckets $B_1, \ldots, B_k$, $n \geq 4$, . Compound C_i explodes if it is in the same bucket as any of the compounds $\{C_{i-3}, C_{i-2}, C_{i-1}, C_{i+1}, C_{i+2}, C_{i+3}\}$. For example, C_3 is explosive with $\{C_1, C_2, C_4, C_5, C_6\}$ (there's no C_0). We choose the number of buckets k to avoid explosions.

(a) Show that you need *at least* 4 buckets and *at most* n buckets, $4 \leq k \leq n$.
(b) Show that you can safely put the compounds into 4 buckets for all $n \geq 4$. That is, $k = 4$ suffices.
(c) You *independently* place 10 compounds randomly into 4 buckets. Each bucket has probability $1/4$. Compute:
    (i) $\mathbb{P}[C_1$ is in a bucket with an explosive partner] and $\mathbb{P}[C_4$ is in a bucket with an explosive partner].
    (ii) The expectated number of explosive pairs created. *[Hint: Sum of indicators.]*

Problem 20.17.
(a) A cereal box comes with one of 10 toys. You buy cereal until you collect all 10 toys. Compute:
    (i) $\mathbb{P}[$you buy at most 15 boxes of cereal].   (ii) $\mathbb{E}[$number of boxes bought].
(b) Let $\mathbf{X}$ be the number of fair die rolls until all values appear. Compute: (i) $\mathbb{P}[\mathbf{X} \geq 10]$.   (ii) $\mathbb{E}[\mathbf{X}]$.
(c) Find the expected sample size when you sample students until you get: (i) 40 distinct birthdays (ii) all birthdays.

Problem 20.18. A bag has 10 red balls. On each turn a random ball is painted blue if it isn't already blue, and returned to the bag. Find the expected number of turns to paint all balls blue. Generalize to n red balls.

Problem 20.19. A bag has 4 balls of different colors. At each step, pick two random balls and paint one ball the other ball's color. Replace the balls and repeat. On average, how many steps till all balls are the same color?

Problem 20.20. Solve using build-up expectation. If in doubt, verify with Monte Carlo.
(a) A couple has kids until 2 boys and 4 girls. How many children do they expect if girls are twice as likely as boys.
(b) The sequence 01001000010001010100 has seven 00's. Find the expected number of 00's in 20 random bits.
(c) A drunk starts at a bar and randomly takes independent steps left or right until reaching home or jail. Home is 20 steps to the left and jail is 20 steps to the right. Compute the expected number of steps the drunk makes.
(d) There are 100 different toys in cereal boxes and you will stop collecting toys when you have 20 of them. What is the expected number of cereal box purchases? Generalize to the case with n different toys and you stop toy-collecting when you have k of them. Show, by induction, that $n(H_n - H_{n-k})$ solves your recursion.
(e) Get a recursion for the expected number of successes in n trials with success probability p. Solve the recursion.
(f) A biased coin with probability $1/3$ of heads is flipped 10 times. In a run, all consecutive flips are the same, for example HHTHTTTTHH has five runs. Compute the expected number of runs.
(g) There is a blue jar with 10 blue balls and red jar with 10 red balls. At each step, a random ball is selected from each jar and they are swapped. After 10 such swaps, compute the expected number of red balls in the red jar.
(h) Cards are drawn randomly from a 52-card deck until a spade is drawn. What is the expected number of draws?
(i) Flip a biased coin with probability $1/3$ of H. What is the expected waiting time to ten heads in a row?
(j) 20 kids stand in line. A random pair of *adjacent* standing kids pair up and sit. This continues until no more pairs can be formed. What is the expected number of unpaired kids?
(k) **(ESP)** A deck has 26 red and 26 black cards. At each step, you guess the color of the next card (knowing how many red and blue cards went by). What is the expected number of correct guesses for optimal guessing?
(l) **(Banach's Matchbox)** Two matchboxes have 100 matches each. Kilam uses matches randomly from either box. The first time there's no match in the box he picks, how many matches do you expect in the other box?
(m) A 3-sided fair die is rolled until one 1, two 2s and three 3s appear. What is the expected number of rolls?
(n) There are 100 empty slots in a line. Doves, one by one, randomly pick an empty slot whose neighboring slots are also empty, until no viable slots remain. On average, how many slots have doves?
(o) You have 6 guesses to guess $\mathbf{X}$, a random integer in $[1, 1000]$. At each guess you are told if $\mathbf{X}$ is higher or lower. If you guess right, you win $\mathbf{X}$. What is the expected profit with optimal guessing. What is your first guess?
(p) You plant six seeds in the ground on day 0. Each subsequent day (day 1,2,3,...), each seed may sprout or remain a seed, sprouting with probability $1/3$. What is the expected wait until all seeds have sprouted.

Problem 20.21. The ends of 100 strings are randomly paired and tied. A cycle is a set of strings tied together to form a necklace. For example, if we label the ends of the strings $(x_1, y_1), (x_2, y_2), \ldots, (x_{100}, y_{100})$ and tie x_1–x_2, y_2–x_3, y_3–y_1, we get a cycle of length three formed from the first three strings. A loop occurs if both ends of the same string are tied (a cycle with one string). Compute the expected number of: (a) loops   (b) cycles.

Problem 20.22. Randomly pick numbers from $\{1, \ldots, 100\}$ with replacement until the sequence picked is not increasing. What is the expected length of the sequence?

Problem 20.23. For a fair coin, show that the expected number of flips to get n heads in a row is $2^{n+1} - 2$.

Problem 20.24. How much would you pay for this gamble? Your profit starts at $0. You repeatedly choose whether to flip a coin or cash out. If you flip and get heads, $1 is added to the profit, and if you get tails the profit resets to 0. The gamble ends if you cash out or if three tails are flipped. *[Hint: Analyze the gamble that ends after one tails.]*

Problem 20.25. Al and Joe each randomly pick 5 restaurants from 20, and must eat at a restaurant both picked.
  (a) Use indicator random variables to compute the expected number of restaurants that the boys can eat at.
  (b) Find the PDF for the number of restaurants they can eat at, and get the expected value from the PDF.

Problem 20.26. Five students independently get a random number in $\{1, \ldots, 10\}$. A score is increased for every pair of students whose numbers agree. Find the expected score when:
  (a) For every pair of students whose numbers agree, the score is increased by 1.
  (b) For every pair of students whose numbers agree, the score is increased by the number the pair has.
  (c) Generalize (a) and (b) to n students independently getting a number in $\{1, \ldots, k\}$.

Problem 20.27. A carnival game costs 50¢ to play. You roll three dice.
  (a) You win $1 if at least one roll is a six. Do you wish to play?
  (b) You win a dollar amount equal to the number of sixes rolled. Do you wish to play?

Problem 20.28. Flip a fair coin until you get two H in a row. Let $\mathbf{X}$ be the number of flips.
  (a) Show that $\mathbb{P}[\mathbf{X} = n] = (\phi_+^{n-1} - \phi_-^{n-1})/\sqrt{20}$, where $\phi_\pm = (1 \pm \sqrt{5})/4$.
  (b) Use (a) to show $\mathbb{E}[\mathbf{X}] = 6$. *[Hint: Show $\sum_{n=0}^{\infty} na^n = a/(1-a)^2$ and $\sum_{n=0}^{\infty} a^n = 1/(1-a)$.]*
  (c) Use iterated expectation or total probability to show $\mathbb{E}[\mathbf{X}] = 6$.

Problem 20.29. Flip a coin until a specific sequence of heads and tails appears. Let $\mathbf{X}$ be the number of flips.
  (a) What is the expected number of flips, $\mathbb{E}[\mathbf{X}]$, when the sequence: (i) TH   (ii) HHH   (iii) TTHH.
  (b) You want a specific sequence of length k. Prove that $\mathbb{E}[\mathbf{X}] \leq k2^k$.

Problem 20.30. Sequences HHH and TTHH compete. A coin is flipped and the sequence that appears first wins.
  (a) Find the expected number of flips until HHH appears. Repeat for TTHH.
  (b) Find the probability that HHH wins the game.
  (c) Give intuition for why TTHH wins more often against HHH, yet in isolation TTHH needs more flips to appear.

Problem 20.31. A fair 5-sided die generates a number in $\{1, 2, 3, 4, 5\}$ with probability $1/5$ each. Give an algorithm to simulate a fair 7-sided die which generates a number in $\{1, 2, 3, 4, 5, 6, 7\}$ with probability $1/7$ each. Find the expected number of rolls of the 5-sided die to get one "roll" of the 7-sided die (try to make this as small as you can).

Problem 20.32. Use linearity of expectation and indicator random variables for (a)–(d).
  (a) The concierge randomly returns coats of n men. On average, how many men get their own coat?
  (b) You flip m balls randomly into n bins. What is the expected number of bins that contain exactly k balls?
  (c) A and B are independent random subsets of $\{1, \ldots, n\}$ with $|A| = k$ and $|B| = \ell$. Find $\mathbb{E}[|A \cap B|]$ and $\mathbb{E}[|A \cup B|]$.
  (d) A street has n houses, k are red and ℓ are white. Find the expected number of neighbors painted different colors.
  (e) **[Hard]** Obtain and use the PDF of the random variable to get the expectation for parts (a)–(d) .

Problem 20.33. How many pairs of students in a class of 200 do you expect to have the same birthday? (Assume there are 365 birthdays and birthdays are random and independent.)

Problem 20.34. Flip a coin n times with heads-probability p. In a run all flips are the same, e.g. HHTHTTTTHH has five runs. Show that the expected number of runs is $1 + 2(n-1)p(1-p)$. *[Hint: $\mathbf{X}_i = 1$ if flip$(i) \neq$ flip$(i-1)$.]*

Problem 20.35. Toss 10 balls randomly into 10 bins. Find the expected number of bins with (a) 0 balls   (b) 1 ball.

Problem 20.36 (Bernoulli diffusion). One jar has n red balls, another n blue. Pick a random ball from each jar and swap them. Do this k times. Find the expected number of red balls in each jar. *[Hint: Problem 18.69(c)]*

Problem 20.37. One hundred men check their hats and coats at a restaurant. When leaving, the hats and coats are distributed independently and randomly to the men. Compute the expected number of men who leave the restaurant:
  (a) With both clothing items that are their own.   (b) With at least one clothing items that is their own.

Problem 20.38. From n elderly couples, m random people expire. How many couples remain, in expectation? *[Hint: $\mathbf{X}_i = 1$ if both members of couple i remain.]*

Problem 20.39. Projects are independent and take 1,2 or 3 nights to complete (each equally likely). You and your spouse have dinner and each start a project on night 1. On any night, if you and your spouse are in sync and have just finished a project, you will have dinner together. Otherwise, if just one of you finish a project, you will start a new project. What is the expected number of nights till you next dine with your spouse?

Problem 20.40 (St. Petersburg Paradox). Flip a fair coin until H. You win $\$2^t$ if t flips are made. How much do you pay for this gamble if: (a) You only care about money.   (b) You get $(\log_2 \mathbf{X})^k$ in utility from $\$\mathbf{X}$.

Problem 20.41 (Sampling With vs. Without replacement). An urn has 10 white and 20 black balls. You randomly pick a ball until you get a white ball. Let $\mathbf{X}$ be the waiting time (number of balls sampled).
(a) What is the expected waiting time if you pick balls *with* replacement.
(b) Suppose you pick balls *without* replacement.
   (i) Comparing to with replacement, guess whether the expected waiting time will increase or decrease, and why.
   (ii) Use build-up expectation to compute the expected waiting time and compare with (a).
   (iii) Find the PDF for the waiting time $\mathbf{X}$ and use it to compute the expected waiting time. *[Hint: Problem 13.72.]*
   (iv) Generalize to m white and n black balls. Give a formula for the expected waiting time.
   (v) Define the indicator random variable $\mathbf{B}_i = 1$ if black ball i is picked *before any white ball*. Show that $\mathbf{X} = 1 + \mathbf{B}_1 + \mathbf{B}_1 + \cdots + \mathbf{B}_{20}$ and use this to compute the expected waiting time.

Problem 20.42. In Exercise 20.8 on page 301, suppose temperature y_i is picked from $y_1 < \cdots < y_n$ with probability p_i. Let F_i be the cumulative probability $p_1 + p_2 + \cdots + p_i$. Let $r(T) = \mathbb{E}[\text{number of records broken to time } T]$.

(a) Show that $r(T) = 1 + \displaystyle\sum_{i=1}^{n-1} \frac{p_{i+1} F_i}{1 - F_i}(1 - F_i^{T-1})$.

(b) For $p_i = \lambda e^{-\alpha i}$ where $\lambda = (e^\alpha - 1)/(1 - e^{-\alpha n})$, show that as $T \to \infty$, $\Theta(n)$ records get broken. Show

$$\lim_{T \to \infty} r(T) \;=\; 1 + \lambda e^{-\alpha} \sum_{i=1}^{n-1} \frac{1 - e^{-\alpha i}}{1 - e^{-\alpha(n-i)}} \;\in\; \Theta(n).$$

Problem 20.43. For $T \ll n$ in Exercise 20.8, show that the number of records broken is logarithmic in T.

Problem 20.44. Let $\mathbf{X}$ be the waiting time to k boys and ℓ girls (see Section 20.3). Let $\mathbf{X}_b$ be the time you wait for the k boys and let $\mathbf{X}_g$ be any *additional* time you must wait to get up to ℓ girls.
(a) What are the possible values of $\mathbf{X}_b$ and $\mathbf{X}_g$. Show that $\mathbf{X} = \mathbf{X}_b + \mathbf{X}_g$. Is $\mathbf{X}_g$ independent of $\mathbf{X}_b$? Explain.
(b) Show that $\mathbb{E}[\mathbf{X}_g \mid \mathbf{X}_b] = \max(0, k + \ell - \mathbf{X}_b)/(1 - p)$.
(c) Hence show using iterated expectation, that $\mathbb{E}[\mathbf{X}] = k/p + \mathbb{E}[\max(0, k + \ell - \mathbf{X}_b)]/(1 - p)$.

Problem 20.45. Let $\mathbf{X}$ be the wait for k successes with success probability p. Compute $\mathbb{E}[\max(0, r - \mathbf{X})]$ for $r \geq k$.
(a) Let $\mathbf{X}$ have PDF $P_{\mathbf{X}}(i)$ for $i \geq k$. Show that $\mathbb{E}[\max(0, r - \mathbf{X})] = \sum_{i=k}^r (r - i) \cdot P_{\mathbf{X}}(i)$.
(b) Use Problem 18.77 to show that $P_{\mathbf{X}}(i) = \binom{i-1}{k-1} p^k (1 - p)^{i-k}$.
(c) Hence, show that $\mathbb{E}[\max(0, r - \mathbf{X})]$ is r when $k = 0$ and $\sum_{i=k}^r (r - i)\binom{i-1}{k-1} p^k (1 - p)^{i-k}$ when $k > 0$.
(d) Using Problem 20.44(d), show that the expected waiting time to k boys and ℓ girls is

$$\mathbb{E}[\text{wait to } k \text{ boys and } \ell \text{ girls}] = \frac{k}{p} + \frac{1}{1-p} \sum_{i=k}^{k+\ell}(k + \ell - i)\binom{i-1}{k-1} p^k (1 - p)^{i-k}.$$

(e) For $p = 1/3$ and $p = 1/2$, compute the expected waiting time to get 2 boys and 2 girls.
(f) **[Hard]** One can further simplify (d) using the normalized incomplete Beta function $I(x, m, n)$,

$$I(x, m, n) = \frac{\int_0^x dt \; t^{m-1}(1 - t)^{n-1}}{\int_0^1 dt \; t^{m-1}(1 - t)^{n-1}}.$$

   (i) Show that $\sum_{i=0}^m \binom{n+i}{n} x^i = (1 - I(x, m + 1, n + 1))/(1 - x)^{n+1}$.
   (ii) Show that the expected wait to k boys and ℓ girls is $kI(1 - p, \ell, k + 1)/p + \ell I(p, k, \ell + 1)/(1 - p)$.
      (Useful identities: $I(x, m, n) = I(1 - x, n, m)$. $I(x, m, n + 1) = I(x, m, n) + \binom{m+n-1}{n} x^m (1 - x)^n$.)
   (iii) For $p = 1/2$ and $k = \ell$, show that the expected wait is $(1 + \binom{2k}{k} 2^{-2k}) \cdot 2k$. Compare to waiting for k boys.

Problem 20.46. Let $W(k, \ell)$ be the expected wait for k boys and ℓ girls with the probability for a boy being p.
(a) What are $W(k, 0)$ and $W(0, \ell)$? Show that $W(k, \ell)$ satisfies the recursion
$$W(k, \ell) = 1 + pW(k - 1, \ell) + (1 - p)W(k, \ell - 1) \qquad \text{(for } k > 0 \text{ and } \ell > 0\text{)}.$$
(b) Use build-up to compute the expected wait to 2 boys and 2 girls for $p = 1/3$ and $p = 1/2$.
(c) Prove by induction that the formula in Problem 20.45(d) solves the recursion in (a).

Problem 20.47. Random variables $(\mathbf{X}_1, \dots, \mathbf{X}_k)$ have joint-PDF $P_{\mathbf{X}_1 \cdots \mathbf{X}_k}(x_1, \dots, x_k)$, where $(x_1, \dots, x_k)$ is a k-tuple in $\mathbf{X}_1(\Omega) \times \cdots \times \mathbf{X}_k(\Omega)$. Let $\mathbf{Z} = f(\mathbf{X}_1, \dots, \mathbf{X}_k)$. The expectation of $\mathbf{Z}$ is
$$\mathbb{E}[\mathbf{Z}] = \sum_{\omega \in \Omega} Z(w) \cdot P(\omega) = \sum_{\omega \in \Omega} f(\mathbf{X}_1(\omega), \dots, \mathbf{X}_k(\omega)) \cdot P(\omega).$$
(a) Show that $\mathbb{E}[\mathbf{Z}] = \sum\limits_{(x_1, \dots, x_k)} f(x_1, \dots, x_k) \cdot P_{\mathbf{X}_1 \cdots \mathbf{X}_k}(x_1, \dots, x_k)$.
(b) Use (a) with $f(\mathbf{X}_1, \dots, \mathbf{X}_k) = a_1 \mathbf{X}_1 + \cdots + a_k \mathbf{X}_k$ to prove linearity of expectation.

Problem 20.48 (Conditional Expectation is Linear). For random variables $\mathbf{X}_1, \dots, \mathbf{X}_n$ and event A, prove:
$$\mathbb{E}[\mathbf{X}_1 + \cdots + \mathbf{X}_n \mid A] = \mathbb{E}[\mathbf{X}_1 \mid A] + \cdots + \mathbb{E}[\mathbf{X}_n \mid A].$$

Problem 20.49. Is it generally true that $\mathbb{E}[1/\mathbf{X}] = 1/\mathbb{E}[\mathbf{X}]$? Is it ever true?

Problem 20.50. Let $\mathbf{X}_1$ and $\mathbf{X}_2$ be independent dice rolls. Determine if the equalities hold. Explain.
(a) $\mathbb{E}[e^{\mathbf{X}_1}] \overset{?}{=} e^{\mathbb{E}[\mathbf{X}_1]}$.
(b) $\mathbb{E}[e^{\mathbf{X}_1 + \mathbf{X}_2}] \overset{?}{=} e^{\mathbb{E}[\mathbf{X}_1]} + e^{\mathbb{E}[\mathbf{X}_2]}$.
(c) $\mathbb{E}[e^{\mathbf{X}_1 + \mathbf{X}_2}] \overset{?}{=} e^{\mathbb{E}[\mathbf{X}_1 + \mathbf{X}_2]}$.
(d) $\mathbb{E}[e^{\mathbf{X}_1 + \mathbf{X}_2}] \overset{?}{=} e^{\mathbb{E}[\mathbf{X}_1]} \cdot e^{\mathbb{E}[\mathbf{X}_2]}$.
(e) $\mathbb{E}[e^{\mathbf{X}_1 + \mathbf{X}_2}] \overset{?}{=} \mathbb{E}[e^{\mathbf{X}_1}] \cdot \mathbb{E}[e^{\mathbf{X}_2}]$.
(f) $e^{\mathbb{E}[\mathbf{X}_1 + \mathbf{X}_2]} \overset{?}{=} e^{\mathbb{E}[\mathbf{X}_1]} \cdot e^{\mathbb{E}[\mathbf{X}_2]}$.
(g) $\mathbb{E}[e^{\mathbf{X}_1 \cdot \mathbf{X}_2}] \overset{?}{=} e^{\mathbb{E}[\mathbf{X}_1]} \cdot e^{\mathbb{E}[\mathbf{X}_2]}$.
(h) $\mathbb{E}[e^{\mathbf{X}_1 \cdot \mathbf{X}_2}] \overset{?}{=} \mathbb{E}[e^{\mathbf{X}_1}] \cdot \mathbb{E}[e^{\mathbf{X}_2}]$.

Problem 20.51. Which equalities are true in general, and why? Tinker with $\mathbf{X}_1$ and $\mathbf{X}_2$ being die rolls.
(a) $\mathbb{E}[\log(\mathbf{X}_1 + \mathbf{X}_2)] = \mathbb{E}[\log \mathbf{X}_1] + \mathbb{E}[\log \mathbf{X}_1]$.
(b) $\mathbb{E}[\log(\mathbf{X}_1 + \mathbf{X}_2)] = \log(\mathbb{E}[\mathbf{X}_1] + \mathbb{E}[\mathbf{X}_1])$.
(c) $\mathbb{E}[\log(\mathbf{X}_1 \mathbf{X}_2)] = \mathbb{E}[\log \mathbf{X}_1] + \mathbb{E}[\log \mathbf{X}_1]$.
(d) $\mathbb{E}[\log(\mathbf{X}_1 / \mathbf{X}_2)] = \mathbb{E}[\log \mathbf{X}_1] - \mathbb{E}[\log \mathbf{X}_1]$.

Problem 20.52. Prove: (a) $\mathbb{E}[(\mathbf{X} + a)^2] = \mathbb{E}[\mathbf{X}^2] + 2a\mathbb{E}[\mathbf{X}] + a^2$ (b) $\mathbb{E}[(a_1 \mathbf{X}_1 + \cdots + a_n \mathbf{X}_n)^2] = \sum\limits_{i=1}^{n} \sum\limits_{j=1}^{n} a_i a_j \mathbb{E}[\mathbf{X}_i \mathbf{X}_j]$.

Problem 20.53. Show $\mathbb{E}[\mathbf{X}^2] = \mathbb{E}[\mathbf{X}]^2 + \mathbb{E}[(\mathbf{X} - \mathbb{E}[\mathbf{X}])^2]$, and hence that $\mathbb{E}[\mathbf{X}^2] \geq \mathbb{E}[\mathbf{X}]^2$.

Problem 20.54. Suppose $\mathbf{X}$ is a positive random variable, taking values $x_1, \dots, x_k$. Prove $\mathbb{E}[1/\mathbf{X}] \geq 1/\mathbb{E}[\mathbf{X}]$.

Problem 20.55. For a positive random variable $\mathbf{X}$, taking values $x_1, \dots, x_k$ with probabilities $p_1, \dots, p_k$, show $\mathbb{E}[\mathbf{X}^n] \geq \mathbb{E}[\mathbf{X}]^n$, for $n \geq 1$. Use the following steps.
(a) Show the claim for $k = 2$: $(p_1 x_1^n + p_2 x_2^n) \geq (p_1 x_1 + p_2 x_2)^n$. [Hint: Consider stationary points of the difference.]
(b) Use induction on k to prove the claim for $k \geq 2$.

Problem 20.56. Show that $\mathbb{E}[\mathbf{X}^{2n}] \geq \mathbb{E}[\mathbf{X}^2]^n$. [Hint: Problems 20.53 and 20.55.]

Problem 20.57. For random variable $\mathbf{X}$, define $f(\lambda) = \mathbb{E}[e^{\lambda \mathbf{X}}]$. Show that $\frac{d}{d\lambda} f(\lambda) = \mathbb{E}[\mathbf{X} e^{\lambda \mathbf{X}}]$. (In general, you can take a derivitive inside or pull it outside an expectation, when all quantities are absolutely convergent.)

Problem 20.58 (Expectation and exponentiation). Let $\mathbf{X}$ be a random variable taking finitely many values.
(a) Use the Taylor series of $e^{\mathbf{X}}$ to show that $\mathbb{E}[e^{\mathbf{X}}] = \sum_{i=0}^{\infty} \mathbb{E}[\mathbf{X}^i]/i!$.
(b) Prove $\mathbb{E}[e^{\mathbf{X}}] \geq e^{\mathbb{E}[\mathbf{X}]}$ when $\mathbf{X}$ is a positive random variable. [Hint: Problem 20.55.]
(c) Prove $\mathbb{E}[e^{\mathbf{X}}] \geq e^{\mathbb{E}[\mathbf{X}]}$ even if $\mathbf{X}$ can be negative. [Hint: Start with two possible values for $\mathbf{X}$. Induction.]

Problem 20.59 (Jensen's Inequality). A function f is convex if, for any $\alpha \in [0, 1]$,
$$f(\alpha x + (1 - \alpha)y) \leq \alpha f(x) + (1 - \alpha)f(y)$$
(a) If $\mathbf{X}$ takes on two possible values, prove that $\mathbb{E}[f(\mathbf{X})] \geq \mathbb{E}[f(\mathbf{X})]$.
(b) Prove by induction on the number of possible values of $\mathbf{X}$ that $\mathbb{E}[f(\mathbf{X})] \geq \mathbb{E}[f(\mathbf{X})]$.
(c) Prove that $1/x, e^x, x^2, -\ln x$ are convex on $(0, \infty), (-\infty, \infty), [0, \infty), (0, \infty)$ respectively.
(d) Prove: (i) $\mathbb{E}[1/\mathbf{X}] \geq 1/\mathbb{E}[\mathbf{X}]$. (ii) $\mathbb{E}[e^{\mathbf{X}}] \geq e^{\mathbb{E}[\mathbf{X}]}$. (iii) $\mathbb{E}[\mathbf{X}^2] \geq \mathbb{E}[\mathbf{X}]^2$. (iv) $\mathbb{E}[\ln \mathbf{X}] \leq \ln \mathbb{E}[\mathbf{X}]$.

Problem 20.60 (Covariance). Show that for any random variables $\mathbf{X}$ and $\mathbf{Y}$,
$$\mathbb{E}[\mathbf{XY}] = \mathbb{E}[\mathbf{X}] \cdot \mathbb{E}[\mathbf{Y}] + (\mathbb{E}[\mathbf{XY}] - \mathbb{E}[\mathbf{X}] \cdot \mathbb{E}[\mathbf{Y}]).$$
The expected product is the product of expectations when the covariance $\mathrm{Cov}(\mathbf{X}, \mathbf{Y}) = \mathbb{E}[\mathbf{XY}] - \mathbb{E}[\mathbf{X}] \cdot \mathbb{E}[\mathbf{Y}] = 0$. Random variables with zero covariance are *uncorrelated*. Independent implies uncorrelated (independence is stronger than uncorrelated). Give random variables $\mathbf{X}, \mathbf{Y}$ which are uncorrelated but dependent.

Problem 20.61 (Linearity and Infinite Sums). At times $t = 1, 2, \ldots$, Joe bets $b_t = 2^{t-1}$ on a fair coin flip and wins b_t if it's H, losing b_t if it's T. The game stops when Joe wins a bet. Let $\mathbf{X}$ the final profit.
  (a) Find the expected profit using the stopping time distribution. Let P_t be the probability to stop at time t.
     (i) Show that $P_t = 2^{-t}$ and that if the game stops at step t, the gambler's profit is \$1.
     (ii) Show that the expected profit is $\mathbb{E}[\mathbf{X}] = \sum_{t=1}^{\infty} P_t = 1$.
  (b) Find the expected profit using linearity of expectation. Let $\mathbf{X}_t$ be the profit at time t, where $\mathbf{X}_t \in \{0, 2^{t-1}, -2^{t-1}\}$ (zero if the game stops before time t). What are $\mathbb{P}[\mathbf{X}_t = 0]$, $\mathbb{P}[\mathbf{X}_t = 2^{t-1}]$ and $\mathbb{P}[\mathbf{X}_t = -2^{t-1}]$.
     (i) Compute $\mathbb{E}[\mathbf{X}_t]$. Show that $\mathbf{X} = \mathbf{X}_1 + \mathbf{X}_2 + \mathbf{X}_3 + \cdots$, hence use linearity of expectation to compute $\mathbb{E}[\mathbf{X}]$.
     (ii) Explain the discrepancy between this result and the result from (a).
  (c) If the game stops after T steps, show that (a) and (b) give the same expected winnings.

> **Probabilistic Method.** The probabilistic method is a modern technique that uses probability and expectations to prove results about a deterministic setting.

Problem 20.62. Show that it is possible to color each number in the set $A = \{1, \ldots, 100\}$ using blue or red so that no 10-term arithmetic progression in A is monochromatic. To do so, consider randomly coloring the numbers.
  (a) How many 10-term arithmetic progressions are there?
  (b) What is the probability that a given 10-term arithmetic progression is monochromatic?
  (c) What is the expected number of monochromatic 10-term arithmetic progressions? Hence, prove the result.

Problem 20.63. Let D_k be the number of ways to give 10 men their hats so that exactly k get their correct hat. Prove that $\sum_{k=0}^{n} kD_k = 10!$. *[Hint: Expected number of men getting their hats in a random assignment.]*

Problem 20.64 (Ramsey Numbers). Fix $k > 1$. Prove that if n satisfies $2\binom{n}{k}2^{-k(k-1)/2} < 1$, some graph with n vertices has no k-clique or k-war. So, n vertices cannot *guarantee* a k-clique or a k-war.
  (a) Let $S_1, S_2, \ldots, S_M$ be the distinct k-subsets of the n vertices. What is M?
  (b) Generate a random graph on n vertices $v_1, \ldots, v_n$ by independently adding each edge (v_i, v_j) into the edge set with probability $1/2$. Show that $\mathbb{P}[S_i \text{ is a } k\text{-clique or } k\text{-war}] = 2 \times 2^{-k(k-1)/2}$.
  (c) Let $\mathbf{X}_i = 1$ if S_i is a k-clique or k-war, and 0 otherwize. What is $\mathbb{E}[\mathbf{X}_i]$.
  (d) Let $\mathbf{X}$ be the total number of k-cliques or k-wars. Find $\mathbb{E}[\mathbf{X}]$ and prove the claim. *[Hint: Is $\mathbb{E}[\mathbf{X}] < 1$?]*
  (e) For $k \in [5, 10]$, what is the largest n for which $2\binom{n}{k}2^{-k(k-1)/2} < 1$?
  (f) If every n-vertex graph has a k-clique or k-war, show that $n \in \Omega(k2^{k/2})$. *[Hint: $\binom{n}{k} \le (ne/k)^k$.]*

Problem 20.65. Prove that every graph $G = (V, E)$ has a cut of size at least $|E|/2$. A cut partitions V into two disjoint sets A, B; its size is the number of edges crossing from A to B.
  (a) Construct the sets A, B by randomly placing vertices independently into one of the sets. Let $e = (u, v)$ be an edge in the graph. Compute $\mathbb{P}[u \text{ and } v \text{ are in different sets}]$.
  (b) Define the indicator $\mathbf{X}(e) = 1$ if u and v are in different sets. Show that the value of the cut is $\mathbf{X} = \sum_{e \in E} \mathbf{X}(e)$. Compute $\mathbb{E}[\mathbf{X}]$ and prove the claim (Problem 19.3 will help).

Problem 20.66. Problem 20.65 proved there is always a cut of size at least $|E|/2$. The *randomized algorithm* of independently placing each vertex into one of the two sets A or B (each with probability $1/2$) gives a cut with expected size $|E|/2$. Unfortunately, this algorithm will not always find a cut of size $|E|/2$, even though one exists. It is even *possible* to produce a cut of size zero, and that's unsettling. Here's one way to "derandomize" the algorithm.
  (a) For vertices $v_1, v_2, \ldots, v_n$ let $\mathbf{X}_1, \mathbf{X}_2, \ldots, \mathbf{X}_n$ indicate which set each vertex is in ($\mathbf{X}_i = 1$ if $v_i \in A$ and $\mathbf{X}_i = 0$ if $v_i \in B$). Let $\mathbf{Z}$ be the cut-size. What are: $\mathbb{E}[\mathbf{Z}]$, $\mathbb{E}[\mathbf{Z} \mid \mathbf{X}_1 = 0]$ and $\mathbb{E}[\mathbf{Z} \mid \mathbf{X}_1 = 1]$?
  (b) Suppose $\mathbf{X}_1, \mathbf{X}_2, \ldots, \mathbf{X}_k$ are fixed to $x_1, x_2, \ldots, x_k$. Show that
  $$\mathbb{E}[\mathbf{Z} \mid x_1, \ldots, x_k] = (\mathbb{E}[\mathbf{Z} \mid x_1, \ldots, x_k, \mathbf{X}_{k+1} = 0] + \mathbb{E}[\mathbf{Z} \mid x_1, \ldots, x_k, \mathbf{X}_{k+1} = 1])/2.$$
  Hence, prove that one of the conditional expectations on the RHS is at least as large as $\mathbb{E}[\mathbf{Z} \mid x_1, \ldots, x_k]$.

(c) As in (b), suppose $\mathbf{X}_1, \mathbf{X}_2, \ldots, \mathbf{X}_k$ are fixed to $x_1, x_2, \ldots, x_k$ (the first k vertices are placed in sets A or B). Let δ_A (resp. δ_B) be the number of edges from v_{k+1} to the vertices already placed in A (resp. B). Show that

$$\mathbb{E}[\mathbf{Z} \mid x_1, \ldots, x_k, \mathbf{X}_{k+1} = 1] - \mathbb{E}[\mathbf{Z} \mid x_1, \ldots, x_k, \mathbf{X}_{k+1} = 0] = \delta_B - \delta_A.$$

Set $x_{k+1} = 1$ if $\delta_B \geq \delta_A$ and $x_{k+1} = 0$ otherwise. Prove that $\mathbb{E}[\mathbf{Z} \mid x_1, \ldots, x_k] \leq \mathbb{E}[\mathbf{Z} \mid x_1, \ldots, x_k, x_{k+1}]$.

(d) (Sequential greedy) For iterations $t = 1, 2, \ldots, n$, deterministically place vertex v_t into A if v_t has at least as many edges to the vertices currently in A versus those currently in B. Prove that the cut size is at least $|E|/2$.

This technique for derandomizing an algorithm is called the method of conditional expectations.

Problem 20.67. Consider this collection of 8 logical OR-clauses (each OR has 3 variables):

$$(x \vee y \vee z) \quad (\overline{x} \vee \overline{y} \vee z) \quad (\overline{x} \vee \overline{z} \vee w) \quad (\overline{x} \vee z \vee w) \quad (y \vee z \vee w) \quad (x \vee \overline{y} \vee w) \quad (y \vee \overline{z} \vee \overline{w}) \quad (x \vee z \vee \overline{w})$$

The goal is to choose T/F for each variable so that a maximum number of OR-clauses is T. The probabilistic method gives a quick proof that at least 7 clauses can simultaneously be true.

(a) Choose each variable to be T/F randomly and independently. Show: $\mathbb{P}[\text{OR-clause is T}] = 7/8$.

(b) Let $\mathbf{X}_i = 1$ if the ith clause is satisfied and 0 otherwise. The number of satisfied clauses is $\mathbf{X} = \sum_i \mathbf{X}_i$. Compute $\mathbb{E}[\mathbf{X}]$ and prove that at least 7 clauses are simultaneously satisfiable.

(c) If there were seven (not eight) clauses, prove that one can always satisfy all seven clauses.

(d) Generalize. Suppose there are n clauses $C_1, \ldots, C_n$ and clause C_i has k_i *different* variables. Prove: One can choose T/F for each variable so that at least $\sum_i (1 - 2^{-k_i})$ clauses are T.

Problem 20.68. In Problem 20.67, randomly picking truth-values of variables satisfies 7/8-th of the clauses on average. This randomized algorithm does not guarantee a truth-assignment satisfying at least 7/8-th of the clauses. Use the method of conditional expectations (Problem 20.66) to derandomize this algorithm. Suppose there are n variables and m clauses. Let $\mathbf{X}_1, \ldots, \mathbf{X}_n$ indicate which variables are T. Let $\mathbf{Z}$ be the number of clauses satisfied.

(a) Suppose $\mathbf{X}_1, \ldots, \mathbf{X}_k$ are fixed to $x_1, \ldots, x_k$. Show that

$$\mathbb{E}[\mathbf{Z} \mid x_1, \ldots, x_k] = (\mathbb{E}[\mathbf{Z} \mid x_1, \ldots, x_k, \mathbf{X}_{k+1} = \text{T}] + \mathbb{E}[\mathbf{Z} \mid x_1, \ldots, x_k, \mathbf{X}_{k+1} = \text{F}])/2.$$

So, one of the conditional expectations on the RHS is at least as large as $\mathbb{E}[\mathbf{Z} \mid x_1, \ldots, x_k]$.

(b) Fix $\mathbf{X}_1, \ldots, \mathbf{X}_k$ to $x_1, \ldots, x_k$. Set $x_{k+1} = \text{T}$ if $\mathbb{E}[\mathbf{Z} \mid x_1, \ldots, x_k, \mathbf{X}_{k+1} = \text{T}] \geq \mathbb{E}[\mathbf{Z} \mid x_1, \ldots, x_k, \mathbf{X}_{k+1} = \text{F}]$, and $x_{k+1} = \text{F}$ otherwise. Prove that

$$\mathbb{E}[\mathbf{Z} \mid x_1, \ldots, x_k] \leq \mathbb{E}[\mathbf{Z} \mid x_1, \ldots, x_k, x_{k+1}].$$

How do you determine if $\mathbb{E}[\mathbf{Z} \mid x_1, \ldots, x_k, \mathbf{X}_{k+1} = \text{T}] \geq \mathbb{E}[\mathbf{Z} \mid x_1, \ldots, x_k, \mathbf{X}_{k+1} = \text{F}]$?

(c) Use (b) to give the details of a greedy algorithm to assign truth-values that satisfy at least 7/8-th of the clauses. Prove it, and give the asymptotic runtime of the algorithm.

Problem 20.69. A graph $G = (V, E)$ has n vertices, m edges, and degree sequence $\delta_1, \ldots, \delta_n$. Let the $n \times n$ adjacency matrix be A ($A_{ij} = 1$ if edge $(v_i, v_j) \in E$ and 0 otherwise). Let $x_1, \ldots, x_n$ be *any* sequence of n numbers with $x_i \in [0, 1]$. Let α be the size of a maximum independent set in G. Show that

$$\alpha \geq \sum_{i=1}^{n} x_i - \frac{1}{2} \sum_{i=1}^{n} \sum_{j=1}^{n} A_{ij} x_i x_j. \tag{20.7}$$

(a) Remove each vertex v_i (and its edges) independently, with probability $1 - x_i$. Let $\mathbf{X}$ be the number of vertices and $\mathbf{Y}$ the number of edges which remain in the graph. Show that:

$$\mathbb{E}[\mathbf{X}] = \sum_{i=1}^{n} x_i \qquad \text{and} \qquad \mathbb{E}[\mathbf{Y}] = \frac{1}{2} \sum_{i=1}^{n} \sum_{j=1}^{n} A_{ij} x_i x_j.$$

(b) After doing part (a), repeat until no edges remain: pick any edge and remove one of its vertices, the one with the largest number of incident (remaining) edges. Prove that you remove at most $\mathbf{Y}$ vertices.

(c) Prove there are at least $\mathbf{X} - \mathbf{Y}$ independent vertices remaining after (b). Hence, conclude there is an independent set of size at least $\mathbb{E}[\mathbf{X} - \mathbf{Y}]$ and prove (20.7).

(d) Suppose the x_i are a constant x. Show that $\alpha \geq nx - mx^2$. Maximize the RHS and show that there is an independent set of size at least $n/2\bar{\delta}$, where $\bar{\delta}$ is the average degree.

(e) Set $x_i = 1/\delta_i$ and prove that $\alpha \geq (\sum_{i=1}^{n} 1/\delta_i)/2$. [Hint:$1/ab \leq (1/a^2 + 1/b^2)/2$.]

(f) Given the optimal $x_i^* \in [0, 1]$ that maximize (20.7), show how to derandomize the algorithm using conditional expectations (see Problems 20.66 and 20.68) to deterministically get an independent set satisfying (20.7) with x_i^*.

(g) Prove that for the optimal $x_i^* \in [0, 1]$ which maximize (20.7), you get equality in (20.7).

21.4   Problems

Problem 21.1. For a random variable $\mathbf{X}$, which of the following does $\sigma(\mathbf{X})$ measure?
  (a) The average value of $\mathbf{X}$ you will observe if you ran the experiment many times.
  (b) The average number of times you run the experiment before observing the value $\mathbb{E}[\mathbf{X}]$.
  (c) The size of the deviation between the observed value of $\mathbf{X}$ and the expected value $\mathbb{E}[\mathbf{X}]$.
  (d) The probability that $\mathbf{X}$ will be larger than its expected value $\mathbb{E}[\mathbf{X}]$.
  (e) The number of possible values of $\mathbf{X}$.

Problem 21.2. Compute $\mathbb{E}[\mathbf{X}]$ and $\sigma^2(\mathbf{X})$, where $\mathbf{X}$ has the PDF shown.

x	-2	-1	0	1	2
$P_{\mathbf{X}}(x)$	$\frac{1}{10}$	$\frac{1}{10}$	$\frac{2}{10}$	$\frac{3}{10}$	$\frac{3}{10}$

Problem 21.3. Random variables $\mathbf{X}_1$ and $\mathbf{X}_2$ have the PDF's shown.
  (a) Guess which random variable has higher variance. Explain your guess.
  (b) Compute the variances and verify your guess.

x	0	1	2	3	4
$P_{\mathbf{X}_1}(x)$	$\frac{1}{11}$	$\frac{2}{11}$	$\frac{5}{11}$	$\frac{2}{11}$	$\frac{1}{11}$
$P_{\mathbf{X}_2}(x)$	$\frac{3}{11}$	$\frac{2}{11}$	$\frac{1}{11}$	$\frac{2}{11}$	$\frac{3}{11}$

Problem 21.4. The mean and variance of a sample $\{x_1, \ldots, x_n\}$, is the mean and variance of a random variable which takes those values with equal probabilities. Compute the mean and variance of these samples:
  (a) {-3,-2,-1,0,1,2,3}   (b) {0,1,2,3,4,5,6}   (c) {0,1,2,3}   (d) {1,4,7,10}

Problem 21.5. A royal family has children until they get a boy or until they have three children, whichever comes first. Let $\mathbf{B}$ be the number of princes and $\mathbf{G}$ the number of princesses. Find the mean and variance of $\mathbf{B}$ and $\mathbf{G}$.

Problem 21.6. A Poisson random variable has PDF $P(i) = e^{-\lambda}\lambda^i/i!$ for $i = 0, 1, 2, \ldots$. Show that the mean and variance are both λ. Give a plot of the PDF for $\lambda = 2$. In your plot, indicate what the mean and variance represent.

Problem 21.7. For two independent fair dice rolls $\mathbf{X}$ and $\mathbf{Y}$, let $\mathbf{Z} = \mathbf{X} + 2\mathbf{Y}$. Compute $\sigma(\mathbf{Z})$. ($\sigma^2(\mathbf{X}) = 35/12$.)

Problem 21.8 (Ternary). Find the mean and variance of a ternary random variable which takes values in $\{-1, 0, 1\}$ with probabilities p, q, r. Specialize to the case $p = q = r = 1/3$.

Problem 21.9. A random variable $\mathbf{X}$ has a symmetric PDF about μ, $P_{\mathbf{X}}(\mu + \Delta) = P_{\mathbf{X}}(\mu - \Delta)$. Show $\mathbb{E}[\mathbf{X}] = \mu$.

Problem 21.10. What is its PDF of a random variable $\mathbf{X}$ for which $\mathbb{E}[\mathbf{X}^2] = \mathbb{E}[\mathbf{X}]^2 = \mu^2$?

Problem 21.11. Let $\mathbf{X}$ be uniform on {-3,-2,-1,0,1,2,3}. Compute the PDF, mean and variance of $\mathbf{Y}$, where
  (a) $\mathbf{Y} = \mathbf{X} + 1$.   (b) $\mathbf{Y} = \mathbf{X}^2 + 1$.   (c) $\mathbf{Y} = 2\mathbf{X} + 1$.

Problem 21.12. Random variables $\mathbf{X}$ and $\mathbf{Y}$ are independent with $\mathbb{E}[\mathbf{X}] = 2, \mathbb{E}[\mathbf{Y}] = 6, \sigma^2(\mathbf{X}) = 9, \sigma^2(\mathbf{Y}) = 16$.
  (a) Compute $\mathbb{E}[\mathbf{X}^2 - \mathbf{Y}^2]$.   (b) Compute $\sigma^2(2\mathbf{X} + 3\mathbf{Y})$.

Problem 21.13. A random variable $\mathbf{X}$ has mean 100 and variance 24. Compute:
  (a) $\mathbb{E}[\mathbf{X}^2]$.   (b) $\mathbb{E}[5 - 3\mathbf{X}]$.   (c) $\mathbb{E}[-\mathbf{X}]$.   (d) $\sigma^2(-\mathbf{X})$.   (e) $\sigma^2(5 - 3\mathbf{X})$.

Problem 21.14. Prove or disprove: The variance of a sum is at most the sum of variances.

Problem 21.15. Let $\mathbf{X}$ be a random variable with mean μ and variance σ^2. Define the z-score $\mathbf{Z} = (\mathbf{X} - \mu)/\sigma$.
  (a) Is the z-score $\mathbf{Z}$ a valid random variable?   (b) Show that the mean of $\mathbf{Z}$ is zero and its variance is 1.

Problem 21.16. Let $\mathbf{X}$ be the number of heads in 36 fair coin flips. Find the mean and variance of $(\mathbf{X} - 5)/3$.

Problem 21.17. Flip a coin n times with probability p of heads. Find the mean and variance of $(\mathbf{X} - np)/\sqrt{np(1 - p)}$.

Problem 21.18. Randomly pick 3 donuts from a batch of 12 in which 4 are stale. You get $\mathbf{X}$ stale donuts.
  (a) Give the PDF of $\mathbf{X}$, the probability that 0,1,2,3 are stale.   (b) Find the mean and variance of $\mathbf{X}$.

Problem 21.19. The daily temperature has $\mu = 60F$ and $\sigma = 5F$. What are μ and σ if temperature is in °C?

Problem 21.20. If 40% of people vote republican, find μ and σ for the number of republican votes with 2000 voters.

Problem 21.21. Find σ^2 for a uniform distribution on $\{1, 2, 3, 4\}$. For $\{1, 2, \ldots, n\}$, show $\sigma^2 = (n^2 - 1)/12$.

Problem 21.22. Let $\mathbf{X}$ be the total number of heads in 20 independent coin flips, with probability p of heads.
  (a) Give the PDF of $\mathbf{X}$ and use the PDF to find $\mathbb{E}[\mathbf{X}]$ and $\text{var}[\mathbf{X}]$.
  (b) Use linearity of expectation to compute $\mathbb{E}[\mathbf{X}]$ and $\text{var}[\mathbf{X}]$.

Problem 21.23. A dealer orders a device for $100 and sells it for $200. The manufacturer repurchases unsold devices for $50. The demand for devices is a random variable $\mathbf{X}$ with a PDF $\mathbb{P}[\mathbf{X} = k] = (1 - e^{-5})e^{-5k}$ for $k = 0, 1, \ldots$.

(a) The dealer orders n devices. Compute the mean and variance of the dealer's profit.

(b) (Inventory management) Give the dealer some advice on how many devices to order.

Problem 21.24. A couple has kids until two boys. Let $\mathbf{X}$ be the number of children the couple has.

(a) Give the PDF for $\mathbf{X}$ and use the PDF to compute the mean and variance of the waiting time.

(b) Write $\mathbf{X}$ as a sum and use that to compute the mean and variance of the waiting time.

(c) Find the the mean and variance of the wait for n boys.

Problem 21.25. An urn has 10 black balls. You randomly paint $\mathbf{X}$ of the balls white, where $\mathbf{X}$ is a random variable with mean $\mu = 4$ and variance $\sigma^2 = 6$. Randomly draw two balls with replacement.

(a) What is the probability that the first ball is white?

(b) What are the probabilities: (i) The second ball is white?   (ii) The second ball is white given the first is white?

(c) What is the probability that both balls are white? When is the color of the balls independent?

Problem 21.26. For independent dice rolls $\mathbf{X}_1$ and $\mathbf{X}_2$, find $\mathrm{var}(\mathbf{X}_1 - \mathbf{X}_2)$ without using the PDF of $\mathbf{X}_1 - \mathbf{X}_2$.

Problem 21.27. For independent random variables $\mathbf{X}_1$ and $\mathbf{X}_2$, prove that $\sigma^2(\mathbf{X}_1 + \mathbf{X}_2) = \sigma^2(\mathbf{X}_1 - \mathbf{X}_2)$.

Problem 21.28. Prove or disprove these properties about the standard deviation.

(a) For any random variable $\mathbf{X}$: (i) $\sigma(\mathbf{X} + a) = \sigma(\mathbf{X})$.   (ii) $\sigma(b\mathbf{X}) = |b|\sigma(\mathbf{X})$.

(b) For independent random variables, the standard deviation of the sum is the sum of standard deviations.

(c) For independent random variables, the standard deviation of the sum is at most the sum of standard deviations.

Problem 21.29 (Spread). Let $\mathbf{X}$ be a random variable taking values $x_1, \ldots, x_n$ with probabilities $p_1, \ldots, p_n$. The mean $\mu = \sum_{i=1}^{n} p_i x_i$. The spread is the expected absolute deviation as opposed to expected squared deviation,

$$\overline{\sigma} = \mathbb{E}[|\mathbf{\Delta}|] = \sum_{i=1}^{n} p_i |x_i - \mu|.$$

What does spread measure? Is it comparable to σ or σ^2? Prove that spread is at most the standard deviation, $\overline{\sigma} \leq \sigma$.

Problem 21.30. Compute $\sigma^2(\mathbf{X})$ for $\mathbf{X}$ defined in the experiment in Problem 19.36 on page 288.

Problem 21.31. Compute the variance of the wait to 2 boys for the Martians in Problem 19.58 on page 290.

Problem 21.32. Compute the variance of a drunk's position after he makes n random steps right or left.

Problem 21.33. A Bernoulli random variable $\mathbf{X}$ has $\mathbb{E}[\mathbf{X}^2] = 1/3$.

(a) Find $\mathbb{E}[\mathbf{X}]$ and $\sigma^2(\mathbf{X})$.

(b) If $\mathbf{X}_1, \ldots, \mathbf{X}_{500}$ are independent with the same distribution as $\mathbf{X}$, compute μ and σ^2 for the average $\frac{1}{500}\sum_{i=1}^{500} \mathbf{X}_i$.

Problem 21.34. You have N to invest in N independent stocks each worth $1. Every year a stock doubles with probability $2/3$, or crashes to $0 with probability $1/3$. Each year is independent. For each investing strategy below, find the mean and variance of your profit in 2 years. Which strategy is best for your conservative grandmother?

(a) Invest all your money into one stock.

(b) Invest an equal share of your money in each stock.

(c) Strategy (i) in the 1st year and strategy (ii) in the 2nd year.

(d) Strategy (ii) in the 1st year and strategy (i) in the 2nd year.

Problem 21.35 (Averaging). Two independent thermometers show temperatures $\mathbf{X}_1$ and $\mathbf{X}_2$ whose means are the true temperature T and variances are σ_1^2 and σ_2^2. Let $\mathbf{X}$ be the average of these measurements, $\mathbf{X} = (\mathbf{X}_1 + \mathbf{X}_2)/2$.

(a) Find the mean and variance of the average. Is the average a "better" estimate of the temperature?

(b) Can you do better, knowing σ_1^2 and σ_2^2? [Hint: Consider a weighted average.]

Problem 21.36 (Sampling Without replacement). An urn has 10 white and 20 black balls. Let $\mathbf{X}_1$ be the waiting time (number of balls sampled) until a white ball appears and $\mathbf{X}_2$ the waiting time until two white balls appear. Find the mean and variance of $\mathbf{X}_1$ and $\mathbf{X}_2$ in each setting below. [Hint: Problem 20.41.]

(a) You pick with replacement.   (b) You pick without replacement.   (c) Generalize to m white and n black balls.

Problem 21.37. For the waiting time to collect n out of n coupons (Example 20.6 on page 295), show

$$\sigma^2 \;=\; n^2\sum_{i=1}^{n}\frac{1}{i^2} - nH_n \;<\; n^2\sum_{i=1}^{\infty}\frac{1}{i^2} - nH_n \;=\; \frac{\pi^2 n^2}{6} - nH_n.$$

($H_n = 1 + \frac{1}{2} + \cdots + \frac{1}{n}$ is the nth Harmonic number.) Use Monte Carlo to verify the case $n = 5$.

Problem 21.38. Find a random variable $\mathbf{X}$ with $\mu = 1$ and $\mathbb{P}[\mathbf{X} \geq 5] = 1/5$, saturating the Markov bound.

Problem 21.39. Find $\mathbb{P}[\mathbf{X} \geq t]$, where $\mathbf{X} \in \{1, \ldots, T\}$ and $P_{\mathbf{X}}(x) = A/x(x+1)$. Compare to Markov's bound.

Problem 21.40. For the sample space $\Omega = \mathbb{N} = \{1, 2, \ldots\}$, define random variables $\mathbf{X}(n) = n$ and $\mathbf{Y}(n) = n^2$.
(a) Compute $\mathbb{E}[\mathbf{X}]$ and $\mathbb{E}[\mathbf{Y}]$ and var$[\mathbf{X}]$ for the probability function $P(n) = 2^{-n}$.
  [Hints: $\sum_{n=1}^{\infty} na^n = a/(1-a)^2$ and $\sum_{n=1}^{\infty} n^2 a^n = a(a+1)/(1-a)^3$ for $0 \leq a < 1$.]
(b) How is var$[\mathbf{X}]$ related to $\mathbb{E}[\mathbf{X}]$ and $\mathbb{E}[\mathbf{Y}]$?
(c) Compute $\mathbb{P}[\mathbf{X} \geq N]$ for $N > 1$ and compare with upper bounds from the Markov and Chebyshev inequalities.
(d) For the probability function $P(n) = 6/\pi^2 n^2$, compute $\mathbb{E}[\mathbf{X}]$.

Problem 21.41. 100 hats randomly land on 100 heads and $\mathbf{X}$ is the number of people who get their hats back.
(a) Compute $\mathbb{E}[\mathbf{X}]$ and var$[\mathbf{X}]$. *[Hints: Let $\mathbf{X}_i = 1$ if person i gets their hat back. Are the $\mathbf{X}_i$ independent?]*
(b) Give an upper bound on the probability that more than half the people get their hats back.

Problem 21.42. Show that a random variable with mean $\mu = 1$ can have any variance.
(a) For any $M \geq 0$, construct a random variable with mean 1 and variance M. *[Hint: Two values.]*
(b) Can a positive random variable with mean 1 have any variance?

Problem 21.43. For independent $\mathbf{X}_1$ and $\mathbf{X}_2$ with the same PDF, which of these have the same variance as $\mathbf{X}_1$.
(a) $-\mathbf{X}_1$.   (b) $\mathbf{X}_1 + \mathbf{X}_2$.   (c) $(\mathbf{X}_1 + \mathbf{X}_2)/2$.   (d) $(\mathbf{X}_1 + \mathbf{X}_2)/\sqrt{2}$.

Problem 21.44. If $\mathbf{X}_1$ and $\mathbf{X}_2$ are independent, show:
(a) $\sigma^2(\mathbf{X}_1 + \mathbf{X}_2) = \sigma^2(\mathbf{X}_1 - \mathbf{X}_2)$.   (b) $\sigma^2(\mathbf{X}_1\mathbf{X}_2) = \sigma^2(\mathbf{X}_1)\sigma^2(\mathbf{X}_2) + \sigma^2(\mathbf{X}_1)\mathbb{E}[\mathbf{X}_2]^2 + \mathbb{E}[\mathbf{X}_1]^2\sigma^2(\mathbf{X}_2)$.

Problem 21.45. For independent $\mathbf{X}_1, \ldots, \mathbf{X}_n$ with $\mathbb{E}[\mathbf{X}_i] = 0$, show that the expected sum-squared equals the sum of expected-squares: $\mathbb{E}[(\mathbf{X}_1 + \cdots + \mathbf{X}_n)^2] = \mathbb{E}[\mathbf{X}_1^2] + \cdots + \mathbb{E}[\mathbf{X}_n^2]$.

Problem 21.46. $\mathbf{X}$ and $\mathbf{Y}$ are random variables (not necessarily independent). Prove that

$$\sigma^2(\mathbf{X} + \mathbf{Y}) = \sigma^2(\mathbf{X}) + \sigma^2(\mathbf{Y}) + 2\mathbb{E}[\mathbf{XY}] - 2\mathbb{E}[\mathbf{X}]\mathbb{E}[\mathbf{Y}].$$

Problem 21.47. Let $\mathbf{X}$ and $\mathbf{Y}$ be independent and $\mathbf{Z} = \mathbf{XY}$. Prove or disprove each formula for the variance.
(a) $\sigma^2(\mathbf{Z}) = \sigma^2(\mathbf{X})\sigma^2(\mathbf{Y})$.   (c) $\sigma^2(\mathbf{Z}) = \sigma^2(\mathbf{X})\mathbb{E}[\mathbf{Y}]^2 + \sigma^2(\mathbf{Y})\mathbb{E}[\mathbf{X}]^2$.
(b) $\sigma^2(\mathbf{Z}) = \sigma^2(\mathbf{X})\mathbb{E}[\mathbf{Y}^2] + \sigma^2(\mathbf{Y})\mathbb{E}[\mathbf{X}^2]$.   (d) $\sigma^2(\mathbf{Z}) = \sigma^2(\mathbf{X})\sigma^2(\mathbf{Y}) + \sigma^2(\mathbf{X})\mathbb{E}[\mathbf{Y}]^2 + \sigma^2(\mathbf{Y})\mathbb{E}[\mathbf{X}]^2$.

Problem 21.48. For independent random variables, prove: standard deviation(sum) $\leq$ sum(standard deviations).

Problem 21.49. For any $x_1, \ldots, x_n$, prove that $n\sum_{i=1}^{n} x_i^2 \geq \left(\sum_{i=1}^{n} x_i\right)^2$. *[Hint: Uniform on $x_1, \ldots, x_n$.]*

Problem 21.50. For any values $x_1, \ldots, x_n$, prove that $\sum_{i=1}^{n} e^{-x_i} \geq n^2/\sum_{i=1}^{n} e^{x_i}$.

Problem 21.51 (Cauchy-Schwarz, $\boldsymbol{a} \cdot \boldsymbol{b} \leq \|\boldsymbol{a}\|\|\boldsymbol{b}\|$). Let $\boldsymbol{a} = [a_1, \ldots, a_n]$ and $\boldsymbol{b} = [b_1, \ldots, b_n]$, with $b_i \neq 0$. Let $\mathbf{X}$ be a random variable taking values $x_i = a_i/b_i$ with probabilities $p_i = b_i^2/\sum_{j=1}^{n} b_j^2$. Use $\mathbb{E}[\mathbf{X}^2] \geq \mathbb{E}[\mathbf{X}]^2$ to show

$$(\boldsymbol{a} \cdot \boldsymbol{b})^2 = \left(\sum_{i=1}^{n} a_i b_i\right)^2 \leq \sum_{i=1}^{n} a_i^2 \sum_{j=1}^{n} b_j^2 = \|\boldsymbol{a}\|^2\|\boldsymbol{b}\|^2.$$

Problem 21.52. A graph with n nodes has degrees $d_1 \geq d_2 \geq \cdots \geq d_n$ and average degree $d = (d_1 + \cdots + d_n)/n$. Show that $\sum_{i=1}^{n} 1/(d_i + 1) \geq n/(d+1)$. *[Hint: Invent a random variable $\mathbf{X}$ and use $\mathbb{E}[\mathbf{X}^2] \geq \mathbb{E}[\mathbf{X}]^2$.]*

Problem 21.53. Let $\mathbf{X}_1, \ldots, \mathbf{X}_n$ be independent with means $\mu_1, \ldots, \mu_n$ and variances $\sigma_1^2, \ldots, \sigma_n^2$. The average is $\mathbf{X} = (\mathbf{X}_1 + \cdots + \mathbf{X}_n)/n$. What are $\mu(\mathbf{X})$ and $\sigma^2(\mathbf{X})$. What would formula (21.7) on page 318 be for $\mathbf{X}$?

Problem 21.54. In Figure 21.2 on page 310 we gave the PDF for the sum of 4 and 100 dice. Use the build-up method to get the PDF for the sum of n dice. Let $P(n, s)$ be the probability that the sum of n dice is s.

(a) What are the possible values for the sum of n dice?

(b) What are $P(1, s)$ and $P(n, n)$? For $s \geq n$, use total probability to show $P(n, s) = \sum_{i=1}^{\min(6, s-n+1)} P(n-1, s-i)/6$.

(c) Compute $P(5, s)$ by filling the following table using (b). We did two rows.

$P(n,s)$		1	2	3	4	5	6	7	8	9	10	11	12	13	$\cdots$	30
	1	1/6	1/6	1/6	1/6	1/6	1/6	0	0	0	0	0	0	0	$\cdots$	0
n	2	0	1/36	1/18	1/12	1/9	5/36	1/6	5/36	1/9	1/12	1/18	1/36	0	$\cdots$	0
	3	?	?	?	?	?	?	?	?	?	?	?	?	?	$\cdots$	?
	4	?	?	?	?	?	?	?	?	?	?	?	?	?	$\cdots$	?
	5	?	?	?	?	?	?	?	?	?	?	?	?	?	$\cdots$	?

(d) Write a program to compute $P(n, s)$ and find σ(average of n dice) for $n = 1, \ldots, 100$. Compare with $\sqrt{35/12n}$.

Problem 21.55. An aggressive drunk takes 10 steps $\mathbf{X}_1, \ldots, \mathbf{X}_{10}$. Each step is independent, and moves left or right with equal probability. The size of the step increases with time, $|\mathbf{X}_i| = i$.

(a) Find the PDF for the position of the drunk after the 10 steps. *[Hint: Build-up.]*

(b) Use the PDF to compute the expected value and standard deviation of the drunk's position after 10 steps.

(c) Use linearity to compute the expected value and standard deviation of the drunk's position after 10 steps.

Problem 21.56 (Bernoulli Maximizes Variance). Let $\mathbf{X}$ be a random variable taking values in $[0, 1]$ with mean μ. Suppose $\mathbf{X}$ takes values $0 = x_1 < x_2 < \cdots < x_{n-1} < x_n = 1$ with probabilties $p_1, \ldots, p_n$ and $\sum_i p_i x_i = \mu$. Prove that $\mathbb{E}[\mathbf{X}^2] \leq \mu$ and $\sigma^2(\mathbf{X}) \leq \mu(1 - \mu)$. To do so, suppose $p_k > 0$ for some $1 < k < n$.

(a) Create new probabilities $p'_1, \ldots, p'_n$ as follows. Set p_k to 0, increase p_1 and p_n and leave the other p_j unchanged:
$$p'_1 = p_1 + (1 - x_k)p_k \qquad p'_k = 0 \qquad p'_n = p_n + x_k p_k \qquad p'_j = p_j \text{ for } j \notin \{1, k, n\}.$$
Show that $p'_1, \ldots, p'_n$ are a valid PDF summing to 1 and the random variable $\mathbf{Y}$ with PDF $p'_1, \ldots, p'_n$ has mean μ.

(b) Show that $\mathbb{E}[\mathbf{Y}^2] > \mathbb{E}[\mathbf{X}^2]$, hence $\sigma^2(\mathbf{Y}) > \sigma^2(\mathbf{X})$. Complete the proof that the Bernoulli maximizes variance.

Problem 21.57. In an exam with n questions, let p_i be the probability a student answers question i correctly.

(a) What is the condition on the p_i so that the expected grade on the exam is 80%?

(b) Show that the grade-variance is maximized when $p_i = 0.8$. (Higher variance is better for differentiating students.)

Problem 21.58. Use Chebyshev's inequality to bound the probability of 2500 ± 100 heads in 5000 fair coin flips.

Problem 21.59. You are building a circuit board and need 50 transistors. About 2% of transistors are defective. Use Chebyshev's Inequality to estimate the number of transistors you should order to ensure at least a 99% chance that you will have enough non-defective transistors. Compare with the correct number you should order.

Problem 21.60. Voltage in the US has a mean of 120V and a standard deviation of 5V. A device's operating voltage is 112-128. Use Chebyshev's inequality to bound the probability that the device will not be damaged when turned on.

Problem 21.61. In a game, you win \$1 with probability 0.4 and lose \$1 with probability 0.6. You play 100 games. Compute the probability that you will not lose money and compare with the upper bound from Chebyshev's inequality.

Problem 21.62. You send 100 bits over a wireless channel that flips bits independently with probability $1/10$. Compute the probability that $4 \leq$ number of errors ≤ 16. Compare with the lower bound from Chebyshev's inequality.

Problem 21.63 (Gallup poll). In a Gallup poll, we try to predict the outcome of an election by examining the votes from a sample of 1000 voters. Let p be the population fraction voting republican versus $1 - p$ for democrat.

(a) Assume $p = 50\%$. Find the 3σ-range for the number in the sample who vote republican?

(b) Predict, giving reasons, who won the election when the number who voted republican is (i) 425 (ii) 480 (iii) 565.

Problem 21.64. On your 15 min commute to work you encounter 20 independent traffic lights. At a light, the delay is 0 or 1 minute with probabilities $1/4$ and $3/4$ respectively. Use Chebyshev to estimate your chances to get to work on time if you leave (a) 45 min before work (b) 30 min before work. Compare with the exact probabilities.

Problem 21.65. Let $\mathbf{X}$ be the waiting time with success probability p. Compute $f(n) = \mathbb{P}[\mathbf{X} \geq n]$ and $g(n)$, the Chebyshev upper bound on $\mathbb{P}[\mathbf{X} \geq n]$. Show that $f(n) \in o(g(n))$. (Chebyshev's bound can be much worse than reality.)

Problem 21.66 (Monte Carlo for Variance). Random variables $\mathbf{X}_1, \ldots, \mathbf{X}_n$ have means $\mu_1, \ldots, \mu_n$ and variances $\sigma_1^2, \ldots, \sigma_n^2$. Generate $z_1, \ldots, z_n$ independently using the distributions of $\mathbf{X}_1, \ldots, \mathbf{X}_n$. The average of $\{z_i\}$ is the sample mean, $\bar{z} = (z_1 + \cdots + z_n)/n$. The sample variance is the average squared-deviation from the sample mean,

$$s^2 = \frac{1}{n} \sum_{i=1}^{n} (z_i - \bar{z})^2.$$

(a) Show that $\mathbb{E}[\bar{z}] = (\mu_1 + \cdots + \mu_n)/n$, the average of the means.
(b) Show that $s^2 = (1/n)\sum_{i=1}^{n} z_i^2 - \bar{z}^2$, the average of the squares minus the squared-average.
(c) Show that $\mathbb{E}[s^2] = ((n-1)/n) \cdot (1/n)\sum_{i=1}^{n} \sigma_i^2 + (1/n)\sum_{i=1}^{n} \mu_i^2 - ((1/n)\sum_{i=1}^{n} \mu_i)^2$.
    (A term slightly below average$(\sigma_1^2, \ldots, \sigma_n^2)$ plus variance$(\mu_1, \ldots, \mu_n)$ which measures the spread in the μ_i.)
(d) When each $\mathbf{X}_i$ has the same mean μ and variance σ^2, show that $\mathbb{E}[\bar{z}] = \mu$ and $\mathbb{E}[s^2] = ((n-1)/n)\sigma^2$.
(e) Justify the following Monte Carlo approach to estimating $\mathbb{E}[\mathbf{X}]$ and $\sigma^2(\mathbf{X})$. Generate n values for $\mathbf{X}$ having sample mean $\bar{z}$ and sample variance s^2. Estimate $\mu = \bar{z}$ and $\hat{\sigma}^2 = (n/(n-1))s^2$.

Problem 21.67 (Failed Monte Carlo).

(a) Show that $P_\mathbf{X}$ is a valid PDF by showing it sums to 1.
(b) Run a Monte Carlo experiment to generate n $\mathbf{X}$'s independently and plot the average of the n $\mathbf{X}$'s versus n for up to $n = 10^6$ experiments. You must figure out how to "generate" $\mathbf{X}$.
(c) Does the average appear to converge? Explain your observations by computing the expectation.

Problem 21.68 (Conditional variance and total variance). Define the conditional variance,

$$\sigma^2(\mathbf{X} \mid A) = \mathbb{E}[\mathbf{X}^2 \mid A] - \mathbb{E}[\mathbf{X} \mid A]^2.$$

Suppose there are k mutually exclusive and exhaustive cases, $C_1, C_2, \ldots, C_k$. Prove the law of total variance:

$$\sigma^2(\mathbf{X}) = \sum_{i=1}^{k} \sigma^2(\mathbf{X} \mid C_i)\mathbb{P}[C_i] + \sum_{i=1}^{k} \mathbb{E}[\mathbf{X} \mid C_i]^2 \cdot P[C_i] - \left(\sum_{i=1}^{k} \mathbb{E}[\mathbf{X} \mid C_i] \cdot P[C_i]\right)^2.$$

The variance is the weighted sum of "within case spreads" plus "between case spread" (variance of case averages).

Problem 21.69 (Law of Iterated Variance). Suppose $\mathbf{Y}$ depends on $\mathbf{X}$. Use Problem 21.68 to prove

$$\sigma^2(\mathbf{Y}) = \mathbb{E}_\mathbf{X}[\sigma^2(\mathbf{Y} \mid \mathbf{X})] + \sigma_\mathbf{X}^2(\mathbb{E}[\mathbf{Y} \mid \mathbf{X}]).$$

Problem 21.70. For independent indicators $\mathbf{X}_1, \ldots, \mathbf{X}_n$ with $p_i = \mathbb{P}[\mathbf{X}_i = 1]$ and $\mathbf{X} = \mathbf{X}_1 + \cdots + \mathbf{X}_n$, prove

$$\mathbb{P}[\mathbf{X} = 0] \leq e^{-\mathbb{E}[\mathbf{X}]}.$$

(a) Show that $\mathbb{P}[\mathbf{X} = 0] = \prod_{i=1}^{n}(1 - p_i) \leq \prod_{i=1}^{n} e^{-p_i}$. Hence, prove the result. *[Hint: $1 - x \leq e^{-x}$.]*
(b) 50 million people play a lottery, each independently picking a 6-digit number. To win, the number must match a randomly picked 6-digit number. Prove that the chances someone wins the lottery is at least $1 - e^{-50}$.

Problem 21.71 (Hoeffding Lemma). A random variable $\mathbf{X}$ is in $[0, 1]$ and $\mathbb{E}[\mathbf{X}] = \mu$. For any $\lambda > 0$, prove

$$\mathbb{E}[e^{\lambda(\mathbf{X} - \mu)}] \leq e^{\lambda^2/8}.$$

(a) Show that e^x is convex: $e^{\alpha x + (1-\alpha)y} \leq \alpha e^x + (1-\alpha)e^y$, for $\alpha \in [0, 1]$.
(b) Use the convexity of e^x to show: $e^{\lambda(\mathbf{X} - \mu)} \leq (1 - \mathbf{X})e^{-\lambda\mu} + \mathbf{X}e^{\lambda(1-\mu)}$.
(c) Show that $\mathbb{E}[e^{\lambda(\mathbf{X} - \mu)}] \leq (1 - \mu)e^{-\lambda\mu} + \mu e^{\lambda(1-\mu)}$.
(d) Let $f(\lambda) = \ln\left((1 - \mu)e^{-\lambda\mu} + \mu e^{\lambda(1-\mu)}\right)$. Show: $f(0) = f'(0) = 0$ and $f''(\lambda) \leq 1/4$. *[Hint: $f''(\lambda) = xy/(x+y)^2$, where $x = (1 - \mu)e^{-\lambda}$ and $y = \mu$. Show $xy/(x+y)^2 \leq 1/4$ when $x + y \neq 0$.]*
(e) Use (d) and integration to show that $f(\lambda) \leq \lambda^2/8$ and conclude the proof.

Problem 21.72. Suppose $\mathbf{X} \in [a, b]$. For $\lambda > 0$, prove $\mathbb{E}[e^{\lambda(\mathbf{X} - \mathbb{E}[\mathbf{X}])}] \leq e^{\lambda^2(b-a)^2/8}$. *[Hint: $\mathbf{Y} = (\mathbf{X} - a)/(b - a)$ in Hoeffding's Lemma (Problem 21.71).]*

Problem 21.73 (Hoeffding Bound). Let $X_1, \ldots, X_n$ be independent, $X_i \in [0, 1]$ and $X = (\sum_i X_i)/n$. Prove:

$$\mathbb{P}\big[|X - \mathbb{E}[X]| \geq \epsilon\big] \leq 2e^{-2n\epsilon^2}.$$

(a) Show that $\mathbb{P}\big[|X - \mathbb{E}[X]| \geq \epsilon\big] = \mathbb{P}\big[X - \mathbb{E}[X] \geq \epsilon\big] + \mathbb{P}\big[\mathbb{E}[X] - X \geq \epsilon\big]$.

(b) Explain why, for any $s > 0$, $\mathbb{P}\big[X - \mathbb{E}[X] \geq \epsilon\big] = \mathbb{P}\big[e^{s(X - \mathbb{E}[X])} \geq e^{s\epsilon}\big]$.

(c) Prove that $\mathbb{P}[X - \mathbb{E}[X] \geq \epsilon] \leq e^{-s\epsilon} \prod_{i=1}^{n} \mathbb{E}[e^{s(X_i - \mathbb{E}[X_i])/n}]$. *[Hint: Markov bound plus independence.]*

(d) Use Hoeffding's Lemma to prove that $\mathbb{P}\big[X - \mathbb{E}[X] \geq \epsilon\big] \leq e^{-s\epsilon + s^2/8n}$ (for any $s > 0$).

(e) Set $s = 4n\epsilon$ in (d) to prove $\mathbb{P}\big[X - \mathbb{E}[X] \geq \epsilon\big] \leq e^{-2n\epsilon^2}$.

(f) Use a similar argument for $\mathbb{P}\big[\mathbb{E}[X] - X \geq \epsilon\big]$ and conclude the proof using the union bound.

Problem 21.74. Let $X_1, \ldots, X_n$ be independent, $X_i \in [a, b]$ and $X = (\sum_i X_i)/n$. Prove

$$\mathbb{P}\big[|X - \mathbb{E}[X]| \geq t\sigma(X)\big] \leq 2e^{-nt^2/2}.$$

[Hint: Use Hoeffding Bound with $Y = (X - a)/(b - a)$. By Problem 21.56, $\sigma(Y) \leq 1/2$.]

Problem 21.75. Use the Hoeffding bound in Problem 21.74 to analyze each case by bounding a relevant probability.

(a) (A/B-testing). Assume 10% of users will click an ad when shown webpage layout A or B. Layouts A and B are shown to 1000 web-surfers. What are the chances 10 more people click the ad in layout A than B?

(b) An average student answers a question correctly 80% of the time. What are the chances a student is above average if they score 70% on a test and the test has (i) 10 questions? (ii) 50 questions? (iii) 100 questions?

(c) FOCStel claims only 1 in a thousand drives fail. You bought 100 drives and 5 failed. What are your thoughts?

Problem 21.76. For 50 independent fair coin flips, estimate $\mathbb{P}[20 \leq \text{number of H} \leq 30]$. Compare Chebyshev's Inequality, Hoeffding's Bound, the Central Limit Theorem and the correct value from the Binomial distribution.

Problem 21.77. A couple has kids until 5 boys. Estimate $\mathbb{P}[7 \leq \text{number of children} \leq 13]$ using Chebyshev's inequality and compare with the true probability. Give an estimate using Hoeffding's Inequality or explain why you can't.

Problem 21.78 (Balls and Bins). Randomly throw n balls independently into n bins (each bin is equally likely).

(a) Let X_i indicate whether bin i is nonempty, and let $X = \sum_i X_i$ be the number of nonempty bins. Show that, asymptotically, a constant fraction of bins are nonempty.

   (i) What is the PDF of X_1? Are the X_i independent?

   (ii) Compute the mean and variance of X. Show that $\mathbb{E}[X] \to n(1 - 1/e)$ as $n \to \infty$,

(b) Let random variable Y_i be the number of balls which fall in bin i.

   (i) What is the PDF of Y_1? Are the Y_i independent?

   (ii) Let $Y = \sum_i Y_i$. Compute the mean and variance of Y.

   (iii) Give a bound on the probability that at least k balls fall in bin 1. Specifically show

$$\mathbb{P}[Y_1 \geq k] \leq \binom{n}{k}\left(\frac{1}{n}\right)^k \leq \frac{1}{k!}.$$

   [Hint: For $k \geq 2$, write $\mathbb{P}[Y_1 \geq k] = \sum_{i=k}^{n} a_i$. Show $\frac{a_{i+1}}{a_i} \leq \frac{1}{2}$, hence $\mathbb{P}[Y_1 \geq k] \leq 2\binom{n}{k}(\frac{1}{n})^k$. Now show that $\frac{a_{i+1}}{a_i} \leq \frac{n-k}{(k+1)(n-1)}$, hence that $\mathbb{P}[Y_1 \geq k] \leq \binom{n}{k}(\frac{1}{n})^k(\frac{n-1}{n})^{n-k}(1 + \frac{n-k}{nk-1})$.]

(c) Let $Z = \max_i Y_i$ be the maximum number of balls in a bin. Prove the important result that $\mathbb{E}[Z] \leq c \ln n$, for some constant $c > 0$ (you expect at most $O(\ln n)$ balls in any bin).

   (i) Use a union bound and part (b) to show that $\mathbb{P}[Z \geq k] \leq n/k!$.

   (ii) Hence show that, for any $\alpha > 0$, $\mathbb{P}[Z \geq \alpha \ln n] \to 0$ as $n \to \infty$.

   (iii) Define events $A = \{Y_1 \geq \alpha \ln n\}$ and $B = \{\max(Y_2, \ldots, Y_n) \geq \alpha \ln n\}$. Show

$$\mathbb{E}[Z] = \mathbb{E}[Z \mid A]\mathbb{P}[A] + \mathbb{E}[Z \mid \overline{A} \wedge B]\mathbb{P}[\overline{A} \wedge B] + \mathbb{E}[Z \mid \overline{A} \wedge \overline{B}]\mathbb{P}[\overline{A} \wedge \overline{B}].$$

   (iv) Hence, show that $\mathbb{E}[Z] \leq \dfrac{n}{\lceil \alpha \ln n \rceil!} + \dfrac{n(n-1)}{\lceil \alpha \ln n \rceil!} + \alpha \ln n$.

   (v) By choosing α appropriately, prove the claim that $\mathbb{E}[Z] \leq c \ln n$, for some $c > 0$.

22.4   Problems

Problem 22.1. A barber shaves *all* those and *only those* who do not shave themselves. Who shaves the barber?

Problem 22.2. YES or NO and explain. **"Is the answer to Problem 22.2 'NO'?"**

Problem 22.3. Explain the judge's inaction in the following anecdote.
> A lawyer who never won a case filed his *last* case against his law school, sueing for a tuition-refund.
> > *Lawyer to Judge:* They did such a bad job that I never won a case.
> > *Judge:* Hmm. . . reasonable. If you never win a law suit, you deserve a refund.
> Nevertheless, the judge pondered forever and never made a ruling.

Problem 22.4. A neverending stream of balls ①②③④⑤··· is placed ten at a time into a bucket (balls 1 to 10, then 11 to 20, and so on). For every ten put in, one is removed. How many balls remain in the bucket in each case?
 (a) The ball removed has lowest number in the bucket.   (b) The ball removed has highest number in the bucket.

Problem 22.5. $A = \{a, b, c\}$; $B = \{x, y, z\}$. A function f maps $a \mapsto x$; $b \mapsto x$; $c \mapsto z$. Is the function f:
 (a) An injection   (b) A surjection   (c) One-to-one   (d) A bijection   (e) Invertible?

Problem 22.6. A, B are finite and $f : A \mapsto B$ is 1-to-1 but not onto. Prove $|A| < |B|$. What if A, B are infinite?

Problem 22.7. Give a definition of a surjection similar to this formal definition of an injection:
> **Injection:** A function $f : A \mapsto B$ is an injection if $\forall a_1, a_2 \in A : f(a_1) = f(a_2) \rightarrow a_1 = a_2$.

Problem 22.8. For what values of $n \in \mathbb{Z}$ is $f(z) = z^n$ an injection from $\mathbb{Z}$ to $\mathbb{Z}$.

Problem 22.9. Determine which of {injective, surjective, bijective} apply to each function $f : A \mapsto B$.
 (a) $A = \mathbb{R}, B = \mathbb{R}, f(x) = e^x$ (d) $A = \mathbb{Q}, B = \mathbb{R}, f(x) = e^x$ (g) $A = \mathbb{R}_{\geq 0}, B = \mathbb{R}_{\geq 0}, f(x) = x^2$
 (b) $A = \mathbb{R}, B = \mathbb{R}_{>0}, f(x) = e^x$ (e) $A = \mathbb{Q}, B = \mathbb{R}_{>0}, f(x) = e^x$ (h) $A = \mathbb{R}, B = \mathbb{R}, f(x) = x(x-1)(x-2)$
 (c) $A = \mathbb{R}, B = \mathbb{R}, f(x) = x^2$ (f) $A = \mathbb{R}, B = \mathbb{R}_{\geq 0}, f(x) = x^2$ (i) $A = \mathbb{N}, B = \mathbb{N}, f(x) = \lfloor \sqrt{x} \rfloor$

Problem 22.10. Let $f : E \times O \mapsto \mathbb{N}$ be defined by $f(x, y) = xy/2$, where $E, O \subseteq \mathbb{N}$ are the even and odd numbers. Prove or disprove: (a) f is injective.   (b) f is surjective.   (c) f is bijective.

Problem 22.11. A function maps $A = \{1, 2, 3, 4\}$ to $B = \{a, b, c, d, e\}$. How many such functions are
 (a) Injective   (b) Not injective   (c) Surjective   (d) Bijective?

Problem 22.12. [**Advanced**] Prove the following. *[Hints: Axiom of choice and Zorn's lemma, see the internet.]*
 (a) There is an injection from A to B if and only if there is a surjection from B to A.
 (b) If there is no injection from A to B then there is an injection from B to A. (Total ordering.)

Problem 22.13. Let $f : A \mapsto B$ and $g : B \mapsto C$. The composition $g \circ f : A \mapsto C$ is $g \circ f(x) = g(f(x))$. Prove or disprove.
 (a) f, g are bijections $\rightarrow g \circ f$ is a bijection.   (d) $g \circ f$ is an injection $\rightarrow f, g$ are injections.
 (b) $g \circ f$ is a bijection $\rightarrow f, g$ are bijections.   (e) f, g are surjections $\rightarrow g \circ f$ is a surjection.
 (c) f, g are injections $\rightarrow g \circ f$ is an injection.   (f) $g \circ f$ is a surjection $\rightarrow f, g$ are surjections.

Problem 22.14. Let $f : A \mapsto B$ and $g : A \mapsto C$. The product $f \otimes g : A \mapsto B \times C$ is given by $f \otimes g(x) = (f(x), g(x))$.
 (a) Prove or disprove: IF f is an injection, THEN $f \otimes g$ is an injection.
 (b) Prove or disprove: IF f and g are surjections THEN $f \otimes g$ is a surjection.
 (c) Prove or disprove: IF f and g are bijections THEN $f \otimes g$ is a bijection.

Problem 22.15. What can you deduce about A if there is an injection from A to $\mathbb{N}$ but no bijection.

Problem 22.16. Give a bijection from A to B (prove that your mapping is a bijection).
 (a) $A = \{\text{squares of integers}\}$; $B = \mathbb{Z}$.   (b) $A = \{\text{positive odd numbers}\}$; $B = \mathbb{Z}$.

Problem 22.17. Answer TRUE or FALSE, with proof.
 (a) A bijection must be an injection.   (d) There is an uncountable subset of $\mathbb{N} \times \mathbb{N}$.
 (b) There is a bijection from $\mathbb{Q}$ to $\mathbb{R}$.   (e) Every infinite subset of $\mathbb{R}$ is uncountable.
 (c) There is a bijection from $\mathbb{Q}$ to $\mathbb{Z}$.   (f) The solutions to $x \equiv 0 \pmod{6}$ are countable.

Problem 22.18. Let $\mathcal{B}$ be the finite binary strings, and $\mathcal{T}$ the finite ternary strings (strings whose characters are $0, 1$ or 2). Show that $|\mathcal{B}| = |\mathcal{T}|$. *[Hint: $0 \mapsto 00; 1 \mapsto 01; 2 \mapsto 10$.]*

Problem 22.19. Suppose $f_A : A \overset{\text{INJ}}{\mapsto} \mathbb{N}$ and $f_B : B \overset{\text{INJ}}{\mapsto} \mathbb{N}$ (A and B are countable). Use f_A and f_B to construct a function $f : A \cup B \overset{\text{INJ}}{\mapsto} \mathbb{N}$ to prove that $A \cup B$ is countable. (You must prove your f is an injection.)

Problem 22.20. Prove that IF $|A| \leq |B|$ AND $|B| \leq |C|$, then $|A| \leq |C|$.

Problem 22.21. Determine if each method is a valid way to show that A is countable.
(a) Show an onto function from $\mathbb{N}$ to A.
(b) Show a 1-to-1 function from $\mathbb{N}$ to A.
(c) Show a bijection from $\mathbb{N}$ to A.
(d) Show an injection from $\mathbb{N}$ to A.
(e) Show there is no injection from $\mathbb{N}$ to A.
(f) Show a 1-to-1 function from A to $\mathbb{N}$.

Problem 22.22. To list $\mathbb{Z}$, follow the arrows (start at 0). Is the list valid? Give the first 12 numbers. What are the list-positions of $z = 2015$ and $z = -2015$.

$$-4 \leftarrow -3 \quad -2 \leftarrow -1 \quad 0 \rightarrow 1 \quad 2 \rightarrow 3 \quad 4 \rightarrow$$
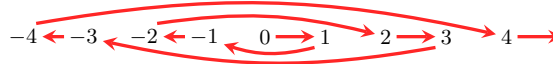
Problem 22.23. If possible, give lists for these sets. (a) Positive rationals. (b) Solutions to $\sin(x) = 0$. (c) $\mathbb{Z} \times \mathbb{Z}$.

Problem 22.24. Prove that the unweighted finite graphs are countable. What if the weights are (a) integers (b) real?

Problem 22.25. True or false. Explain your answers.
(a) The positive multiples of 5 are countable.
(b) $\mathbb{Z} \cup \mathbb{Z}^2 \cup \mathbb{Z}^3$ is countable.
(c) $|\mathbb{N}| = |\{\text{square numbers}\}|$.
(d) (i) All subsets of $\mathbb{N}$ are countable. (ii) All finite subsets of $\mathbb{N}$ are countable.
(e) (i) All finite binary strings are countable. (ii) All infinite binary strings are countable.
(f) The angles between 0 and 2π are countable.
(g) The infinite binary strings that are eventually zero (e.g. $b_1 b_2 \cdots b_\ell 0000 \cdots$) are countable.
(h) The functions from $\mathbb{N}$ to $\mathbb{N}$ are countable.
(i) There is a countable, infinite set for which all the subsets are countable.

Problem 22.26. Prove or disprove.
(a) The ordered pairs of integers, $\mathbb{Z}^2$, is countable, where $\mathbb{Z}^2 = \{(z_1, z_2) | z_1, z_2 \in \mathbb{Z}\}$.
(b) The ordered pairs of rationals, $\mathbb{Q}^2$, is countable, where $\mathbb{Q}^2 = \{(q_1, q_2) | q_1, q_2 \in \mathbb{Q}\}$.
(c) F is the set of all distinct functions from $\mathbb{N}$ to $\mathbb{N}$, $F = \{f | f : \mathbb{N} \mapsto \mathbb{N}\}$. F is countable.

Problem 22.27. Let A, B be countable. Prove the Cartesian product $A \times B = \{(a, b) \mid a \in A, b \in B\}$ is countable.

Problem 22.28. Determine, with proof, if each set of functions is finite, countable or uncountable. The functions:
(a) Map $\{0\}$ to $\mathbb{N}$ (b) Map $\mathbb{N}$ to $\{0\}$ (c) Map $\{0,1\}$ to $\mathbb{N}$ (d) Map $\mathbb{N}$ to $\{0, 1\}$.

Problem 22.29. The positive rationals are $\mathbb{Q}_+ = \{x/y \mid x, y \in \mathbb{N}\}$. Prove that $\mathbb{Q}_+$ is countable.
(a) Let $f(x, y) = 2^x 3^y$. Prove that f is an injection from $\mathbb{N}^2$ to $\mathbb{N}$. *[Hint: Fundamental Theorem of Arithmetic.]*
(b) Use (a) to show $|\mathbb{Q}_+| \leq |\mathbb{N}|$. Show that $\mathbb{Q}_+$ being countable means $\mathbb{Q}$ must be countable.

Problem 22.30. Use ideas from Problem 22.29 to prove countable sets are closed under union and Cartesian product. Let $\{p_1, p_2, \ldots\}$ be primes. Let $\{A_1, A_2, \ldots\}$ be a countable set, where each $A_i = \{a_{i,1}, a_{i,2}, \ldots, \}$ is itself countable.
(a) For $x \in \cup_i A_i$, let A_ℓ be the first set containing x, $x \in A_\ell$ and $x \notin A_j$ for $j < \ell$. Let x be the kth element in A_ℓ. Use $f(x) = p_\ell^k$ to prove that $\cup_i A_i$ is countable. That is, the union of countably many countable sets is countable.
(b) Let $x = (x_1, x_2, \ldots, x_n)$ be an ordered n-tuple from $A_1, \ldots, A_n$, so $x \in A_1 \times A_2 \times \cdots A_n$.
   (i) Let x_i be the k_i-th element in A_i. Use $f(x_1, \ldots, x_n) = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$ to prove that $A_1 \times A_2 \times \cdots \times A_n$ is countable. That is, the Cartesian product of finitely many countable sets is countable.
   (ii) Why does the argument in (i) fail for an infinite Cartesian product. In fact, prove that the Cartesian product of countably many sets is uncountable, if infinitely many of the sets have size at least 2.

Problem 22.31. Prove or disprove that each intersection of the following collection of sets is countable.
(a) Countably many countable sets. (b) Uncountably many countable sets. (c) Countably many uncountable sets.

Problem 22.32. Prove that eventually constant infinite sequences on $\mathbb{N}$ are countable.

Problem 22.33. Prove that $|\{\text{infinite increasing sequences on } \mathbb{N}\}| = |\mathbb{R}|$. What about finite increasing sequences?

Problem 22.34. Given a set $\mathcal{X}$, let $x_0 \in \mathcal{X}$ and $\mathcal{X}_0$ the *proper* subset of $\mathcal{X}$ with all elements in $\mathcal{X}$, except x_0. Prove:
(a) If $\mathcal{X}$ is infinite, $|\mathcal{X}| \leq |\mathcal{X}_0|$. *[Hint: Let $C \subseteq \mathcal{X}_0$ be countable. Start with an injection from $C \cup x_0$ to C.]*
(b) $\mathcal{X}$ is infinite if and only if $\mathcal{X}$ injectively maps to some proper subset of $\mathcal{X}$. *[Hint: Pigeonhole for finite $\mathcal{X}$.]*

Problem 22.35. Prove that $f(b) = 2^{\text{length}(b)} + \text{value}(b)$ (Example 22.5 on page 331) is an injection from finite binary strings to $\mathbb{N}$. What does this imply about $|\{\text{finite binary strings}\}|$?

Problem 22.36. Prove that $[0, 1]$ has the same cardinality as the full continuum $\mathbb{R}$.

Problem 22.37 (Algebra of Infinity). Justify these "rules" for handling $\aleph_0 = |\mathbb{N}|$ (k is a constant, e.g. 2).
(a) $\aleph_0 + k = \aleph_0$.   (b) $k \times \aleph_0 = \aleph_0$.   (c) $\aleph_0^k = \aleph_0$.   (d) $2^{\aleph_0} > \aleph_0$.

Problem 22.38. Algebraic numbers are solutions to integer-polynomial equations,

$$a_1 x^{k_1} + a_2 x^{k_2} + \cdots + a_\ell x^{k_\ell} = 0,$$

(a_i, k_i are integers and $k_1 < k_2 \cdots < k_\ell$ are positive.) A number is transcendental if it is not algebraic. Prove:

$$\begin{aligned} |\{\text{algebraic numbers}\}| &= |\mathbb{N}|; \\ |\{\text{transcendental numbers}\}| &> |\mathbb{N}|. \end{aligned} \qquad \left(\begin{array}{l} \text{The transcendentals, e.g. } \pi \text{ and } e, \text{ far} \\ \text{outnumber the algebraics, e.g. } 2, \sqrt{2}. \end{array}\right)$$

Problem 22.39 (Irrationals have cardinality $\mathfrak{c}$). Cantor went after irrationals, a messy set. Prove that irrationals have the cardinality of the continuum. (There are many more irrationals than rationals.)
(a) Show that the number $x = 0.1011011011011 \cdots = 0.1\overline{011}$ equals 5/7. Informally argue that a rational number's binary expansion has the form $0.y\overline{z}$, for finite binary strings y and z. (z could be 0.)
(b) Argue that an irrational number's binary representation is infinite without a repeating tail.
(c) Let $x \in [0, 1]$ have infinite expansion $0.b_1 b_2 b_3 \cdots$. Let $z = 0.10b_1 110b_2 1110b_3 11110b_4 \cdots$. Prove z is irrational.
(d) Show that $|\mathbb{R}| \leq |\{\text{irrational numbers}\}|$, and hence that $|\mathbb{R}| = |\{\text{irrational numbers}\}|$.
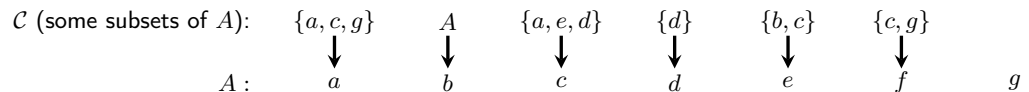
Problem 22.40 (Cardinality of the square, $\mathbb{R}^2$). Cantor was after a set with cardinality larger than the continuum. He was sure the square $\mathbb{R} \times \mathbb{R}$ would be it. After trying hard to show that there is no injection from $\mathbb{R} \times \mathbb{R}$ to $\mathbb{R}$, Cantor finally found one in 1877. His own words to Dedekind were "I see it but I do not believe it."
(a) Let (x, y) be reals with binary expansions $x = 0.a_1 a_2 a_3 \cdots$ and $y = 0.b_1 b_2 b_3 \cdots$. Define the mapping $(x, y) \mapsto z$, where $z = 0.a_1 b_1 a_2 b_2 a_3 b_3 \cdots$. Prove that this mapping is an injection from $(0, 1) \times (0, 1)$ to $(0, 1)$.
(b) What does this tell you about $|(0, 1) \times (0, 1)|$? Prove that $|(0, 1) \times (0, 1)| = |(0, 1)|$.

Problem 22.41 (Power Set and Cantor's Theorem). Among Cantor's many gems, this is the stunning result bearing his name. Recall that the power set of A, $\mathcal{P}(A)$, is the set of *all* subsets of A. Prove Cantor's Theorem.

Theorem 22.8 (Cantor, 1891). A set is smaller than its power-set. For any set A, $|A| < |\mathcal{P}(A)|$.

(a) Show $|A| \leq |\mathcal{P}(A)|$ by giving an injection from A to $\mathcal{P}(A)$.
(b) Let $A = \{a, b, \ldots, g\}$. Here is an injection from a set $\mathcal{C}$ containing subsets of A to the elements in A.

$$\mathcal{C} \text{ (some subsets of } A\text{):} \quad \{a, c, g\} \quad A \quad \{a, e, d\} \quad \{d\} \quad \{b, c\} \quad \{c, g\}$$
$$\qquad \qquad \downarrow \qquad \downarrow \qquad \downarrow \qquad \downarrow \qquad \downarrow \qquad \downarrow$$
$$A: \qquad \quad a \qquad b \qquad c \qquad d \qquad e \qquad f \qquad g$$

Element a is beautiful because the set which maps to a contains a; Element c is ugly because the set which maps to c *does not contain* c. (Some elements of A may be neither beautiful nor ugly, e.g. g, because in an injection, not all elements of A need be used.) The ugly set $\mathcal{W}$ is the set of *all* ugly elements. Find the ugly set for the injection above. Does the ugly set appear in the domain of the injection?
(c) Let f be any injection from $\mathcal{C}$ (which contains some subsets of A) to elements of A. Prove that the ugly set of f cannot be in $\mathcal{C}$ (the domain of the injection). *[Hint: Contradiction. Assume $\mathcal{W} \in \mathcal{C}$ and consider the element $x \in A$ to which $\mathcal{W}$ is mapped, $f(\mathcal{W}) = x$. Either $x \in \mathcal{W}$ or $x \notin \mathcal{W}$. Which is it?]*
(d) Set $\mathcal{C} = \mathcal{P}(A)$ and prove that, for *any* A, there is no injection from $\mathcal{P}(A)$ to A. Hence, prove Cantor's Theorem.

Problem 22.42. Prove that sets generated from recursive definitions are countable.

Problem 22.43 (Cantor Set). Construct a subset of $[0, 1]$ as follows. Start with the interval $[0, 1]$. At every step, remove the middle one-third of every interval in the set.

(a) At step i, show that the number of intervals is 2^i, the length of each interval is $(1/3)^i$ and the total length of the intervals is $(2/3)^i$. Hence, the total length of the intervals converges to 0 as $i \to \infty$. Further, the lengths of the intervals becomes 0, that is, we are left with a collection of points whose total length is zero.

(b) Let $0.t_1 t_2 t_3 \cdots$ be the base-3 representation of a number in $[0, 1]$. At step 0, all possible numbers remain. Show:

    (i) At step 1, the numbers which remain have $t_1 \in \{0, 2\}$.

    (ii) At step k, the numbers which remain have $t_1, \ldots, t_k \in \{0, 2\}$.

    (iii) At step i, for $i \to \infty$, all numbers with $t_1, t_2, \ldots \in \{0, 2\}$ remain.

(c) Prove that the Cantor set is uncountable.

The Cantor set is uncountable, yet it has measure zero. (Measure formally quantifies total "length" for subsets of $\mathbb{R}$. Rationals in $[0, 1]$ also have measure zero, but are countable.) The irrationals in $[0, 1]$ have measure 1.)

Problem 22.44 (Russell's Paradox). Let S be a collection of sets. Try to find a set S which contains itself. Start with a singleton set $S_1 = \{\bullet\}$.

(a) Is $S_1 \in S_1$?

(b) Add S_1 into itself to create $S_2 = S_1 \cup \{S_1\}$. What is S_2. Is $S_2 \in S_2$?

(c) Keep adding the set into itself: define $S_{i+1} = S_i \cup \{S_i\}$. What is S_4?

(d) Continuing forever gives a set S_∞. Show that S_∞ has a recursive definition:

    (i) $\bullet \in S_\infty$.   **[basis]**

    (ii) $x \in S_\infty \to x \cup \{x\} \in S_\infty$.   **[constructor rule]**

    (iii) Nothing else is in S_∞.   **[minimality]**

(e) Is $S_\infty \in S_\infty$? *[Hint: is any infinite set in S_∞.]*

(f) Things are looking bleak. Consider the set $\overline{T}$ containing all things that are not turtles. Does $\overline{T}$ belong to $\overline{T}$?

(g) Suppose there are sets that contain themselves and sets that don't. Define the set W, a catalog of all the sets that *do not contain themselves*, the "well-behaved sets",

$$W = \{\text{sets } S \mid S \text{ does not contain itself}\}.$$

So, $A \in W \leftrightarrow A \notin A$. If W is well defined, either $W \in W$ or $W \notin W$. Derive a contradiction for each case. (Logically, W can't exist. Further, sets can't contain *any* object. Modern set-theory uses the Zermelo–Fraenkel (ZF) axioms plus the axiom of choice (C), ZFC-set-theory.)

Problem 22.45. Here is a proof by induction of the well-ordering principle. Our claim is:

$$P(n) : \text{every set } A \subset \mathbb{N} \text{ of size } n \text{ has a minimum element.}$$

We prove $P(n)$ $\forall n \geq 1$ by strong induction.

    [Base case] $P(1)$ is T: if $|A| = 1$, the lone element in A is the minimum element.

    [Induction step] Assume $P(1), \ldots, P(n)$ and consider any set A of size $n+1$, $A = \{x_1, x_2, \ldots, x_n, x_{n+1}\}$. The set $\{x_1, x_2, \ldots, x_n\}$ has a minimum element, because $P(n)$ is T. Call this element x_*. If $x_{n+1} \leq x_*$, then x_{n+1} is a minimum element in A. Otherwise x_* is a minimum element in A. In either case, A has a minimum element. Since A was arbitrary, every set of size $n + 1$ has a minimum element.

    Therefore, $P(n + 1)$ is T, and by induction, $P(n)$ is T $\forall n \geq 1$.

This is a faulty proof of the well-ordering principle. What is wrong with it? (See also Problem 5.79.)

23.4 Problems

Problem 23.1. How is a computing problem defined in the text?
(a) Kilam says a computing problem is a subset of $\mathbb{N}$. Could Kilam be right?
(b) Ayfos says any computing problem is a function mapping $\mathbb{N}$ to $\{0, 1\}$. Could Ayfos be right?

Problem 23.2. If n and $n + 2$ are prime, n is a younger-twin-prime. List the language of younger-twin-primes.

Problem 23.3. Give languages for each computing problem. Use a binary encoding for strings.
  (a) Testing whether a number n is a multiple of 4.   (b) Given a list of bits, is it sorted (all 0s before all 1s).

Problem 23.4. Starting from n counters, two players take turns removing 1,2 or 3 counters. The person who takes the last counter wins. Given $n \in \mathbb{N}$, can the first player force a win? Give the language for this computing problem.

Problem 23.5. Which of the following tasks are formulated as decision problems.
(a) An inversion in a list of distinct numbers $x_1, x_2, \ldots, x_n$ is a pair $x_i > x_j$ with $i < j$. Find the number of inversions.
(b) Given a set of line segments, determine if there is a pair of segments that intersect.
(c) Determine the maximum possible score on level 3 of Super Mario Brothers.
(d) Is there a flight itinerary from Tokyo to Roanoke with fewer than 3 stop-overs.

Problem 23.6. Give a decision version for each task and show how to solve the task using the decision version.
(a) How many goody-bags are there with n candies of k colors? (d) How many colors are needed to color a graph G?
(b) How big is a largest independent set in a graph G?   (e) What is the largest number in a list of numbers?
(c) How big is the largest clique in a graph G.   (f) How close are two nodes in a graph G?

Problem 23.7. True or false? Explain your answers.
(a) All languages have infinitly many strings.   (d) A language must contain strings of every finite length.
(b) A language can be uncountable.   (e) The union of two languages is a language.
(c) A language can contain strings of infinite length.   (f) The complement of any language is a language.

Problem 23.8. Is the union of *uncountably* many languages a valid language?

Problem 23.9. Let $\mathcal{L}_1 = \{\varepsilon, 01\}$ and $\mathcal{L}_2 = \{1, 01, 10\}$ (a) Find $\mathcal{L}_1 \bullet \mathcal{L}_2$, $\mathcal{L}_1^{\bullet 2}$ and $\mathcal{L}_2^{\bullet 2}$.   (b) Is $\mathcal{L}_1 \bullet \mathcal{L}_2 = \mathcal{L}_2 \bullet \mathcal{L}_1$?

Problem 23.10 (Kleene star). For a language $\mathcal{L} = \{s_1, s_2, \ldots\}$, $\mathcal{L}^* = \{\varepsilon, s_1, s_2, s_1 \bullet s_1, s_1 \bullet s_2, \ldots\}$.
(a) For $\mathcal{L} = \{1, 10\}$ give the strings of length at most 6 in $\mathcal{L}^*$.
(b) For $\mathcal{L}$ in (a), prove that $1110111 \in \mathcal{L}^*$ and that $11100111 \notin \mathcal{L}^*$
(c) Prove that $\mathcal{L}_1 \subseteq \mathcal{L}_2 \rightarrow \mathcal{L}_1^* \subseteq \mathcal{L}_2^*$.
(d) Prove or disprove: (i) $\mathcal{L}^*$ is a valid language for any valid language $\mathcal{L}$.   (ii) $\mathcal{L}^*$ is always countable.

Problem 23.11. Let $\mathcal{L}_0 = \{0\}$ and $\mathcal{L}_1 = \{1\}$. Give English descriptions of (a) $\mathcal{L}_0^*$ (b) $\mathcal{L}_1^*$ (c) $(\mathcal{L}_0 \cup \mathcal{L}_1)^*$.

Problem 23.12. For any $\mathcal{L}_1, \mathcal{L}_2$, prove or disprove: (a) $\mathcal{L}_1^* \cup \mathcal{L}_2^* = (\mathcal{L}_1 \cup \mathcal{L}_2)^*$.   (b) $\mathcal{L}_1^* \cap \mathcal{L}_2^* = (\mathcal{L}_1 \cap \mathcal{L}_2)^*$.

Problem 23.13 (Wildcard vs. Kleene star). What is the difference between $1*$ and $\{1\}^*$?

Problem 23.14. In each part, determine which strings can be generated by the corresponding regular expression.
(a) Regular expression: $\{0, 01\} \bullet \{1, 10\}$.   Strings: ε; 0; 1; 00; 01; 10; 11; 0000; 0110; 1111.
(b) Regular expression: $\{1\}^* \cup \{0\}^*$.   Strings: ε; 000; 11; 000111.
(c) Regular expression: $\{1\}^* \bullet \{0\}^*$.   Strings: ε; 000; 11; 000111.
(d) Regular expression: $\overline{\{1\}^*} \cup \{0\}^*$.   Strings: ε; 000; 11; 000111.
(e) Regular expression: $\overline{\{1\}^*} \bullet \{0\}^*$.   Strings: ε; 000; 11; 000111.
(f) Regular expression: $\{0, 01\}^* \bullet \{1, 10\}^*$.   Strings: 101110; 00111; 00100; 01100.
(g) Regular expression: $\{0, 01\}^* \cap \{1, 10\}^*$.   Strings: 101110; 00111; 00100; 01100.
(h) Regular expression: $\overline{\{0, 01\}^*} \bullet \{1, 10\}^*$.   Strings: 101110; 00111; 00100; 01100.

Problem 23.15. For each regular expression, give 3 strings in the language and 3 strings not in the language.
  (a) $\{0\}^* \bullet \{1\}^*$ (b) $\{0\}^* \cup \{1\}^*$ (c) $\Sigma \bullet \{0\}^*$ (d) $\Sigma^* \bullet \{01\} \bullet \Sigma^*$ (e) $(\{0\} \bullet \{1\}^*)^*$ (f) $(\{01\} \bullet \{1\}^*)^*$.

Problem 23.16. Give a *recursive* definition of the language $L = \{001^{\bullet 2n} | n \geq 0\}$.

Problem 23.17. Give a recursive definition of $\mathcal{L}^*$ for a finite language $\mathcal{L} = \{w_1, \ldots, w_k\}$.

Problem 23.18. Prove or disporve: there is a language $\mathcal{L}$ for which $\overline{\mathcal{L}^*} = (\overline{\mathcal{L}})^*$.

Problem 23.19. Let $\mathcal{L} = \{$strings with a different number of 0s and 1s. Prove $\mathcal{L}^* = \Sigma^*$ (all finite binary strings).

Problem 23.20. For language $\mathcal{L}$, the positive concatenations $\mathcal{L}^+ = \cup_{n=1}^{\infty} \mathcal{L}^{\bullet n}$ (concatenations of at least one string).
  (a) Give the strings of length at most 4 in $\{0, 01\}^+$.
  (b) Give a string in $\{0\} \bullet \{11\}^* \cup \{01\}^*$ which is not in $\{0\} \bullet \{11\}^+ \cup \{01\}^*$.

Problem 23.21. The set of palindromes is $\mathcal{L}_{\mathsf{palindrome}} = \{u \mid u \in \Sigma^*, u = u^{\mathrm{R}}\}$. Prove that
$$\mathcal{L}_{\mathsf{palindrome}} = \{u \bullet v \bullet w \mid u \in \Sigma^*, v \in \{\varepsilon, 0, 1\}, w = u^{\mathrm{R}}\}.$$

Problem 23.22. Recursively define $\mathcal{L}_{\mathsf{palindrome}} = \{$strings which equal their reversal$\}$. (See problem 23.21.)

Problem 23.23 (Reversal). The reversal of $\mathcal{L}$, $\mathcal{L}^{\mathrm{R}}$, has the reversal of all strings in $\mathcal{L}$, $\mathcal{L}^{\mathrm{R}} = \{w^{\mathrm{R}} \mid w \in \mathcal{L}\}$.
  (a) Give regular expressions for the reversals of these languages: (i) $\{01\}^*$ (ii) $\{01\}^* \bullet \{110\}^*$ (iii) $\overline{\{01\}^*}$.
  (b) For languages $\mathcal{L}_1$ and $\mathcal{L}_2$, formally define: (i) $(\mathcal{L}_1 \cup \mathcal{L}_2)^{\mathrm{R}}$ (ii) $(\mathcal{L}_1 \cap \mathcal{L}_2)^{\mathrm{R}}$ (iii) $(\overline{\mathcal{L}_1})^{\mathrm{R}}$ (iv) $(\mathcal{L}_1 \bullet \mathcal{L}_2)^{\mathrm{R}}$ (v) $(\mathcal{L}_1^*)^{\mathrm{R}}$.
  (c) Prove or disprove:
     (i) $(\mathcal{L}_1 \cup \mathcal{L}_2)^{\mathrm{R}} = \mathcal{L}_1^{\mathrm{R}} \cup \mathcal{L}_2^{\mathrm{R}}$ (ii) $(\mathcal{L}_1 \cap \mathcal{L}_2)^{\mathrm{R}} = \mathcal{L}_1^{\mathrm{R}} \cap \mathcal{L}_2^{\mathrm{R}}$ (iii) $(\overline{\mathcal{L}_1})^{\mathrm{R}} = \overline{\mathcal{L}_1^{\mathrm{R}}}$ (iv) $(\mathcal{L}_1 \bullet \mathcal{L}_2)^{\mathrm{R}} = \mathcal{L}_2^{\mathrm{R}} \bullet \mathcal{L}_1^{\mathrm{R}}$ (v) $(\mathcal{L}_1^*)^{\mathrm{R}} = (\mathcal{L}_1^{\mathrm{R}})^*$.

Problem 23.24. Given $\mathcal{L}$, let $\mathcal{L}^{\mathrm{R}}$ be the reversal and $\mathcal{L}_{ww^{\mathrm{R}}} = \{ww^{\mathrm{R}} \mid w \in \mathcal{L}\}$. Prove or disprove: $\mathcal{L}_{ww^{\mathrm{R}}} = \mathcal{L} \bullet \mathcal{L}^{\mathrm{R}}$.

Problem 23.25. Prove or disprove: $\mathcal{L}_{\mathsf{palindrome}}^{\bullet 2} = \mathcal{L}_{\mathsf{palindrome}}$.

Problem 23.26. Is there a "nontrivial" language (not $\{\varepsilon\}$ or Σ^*) for which (a) $\mathcal{L}^{\bullet 2} = \mathcal{L}$ (b) $\mathcal{L}^* = \mathcal{L}$?

Problem 23.27. Let $\mathcal{L}_1 = 1*$ and $\mathcal{L}_2 = *110$, where the wild-card symbol $*$ can be any string in Σ^* ($1*$ is not $\{1\}^*$, the latter being Kleene-star). Informally describe each language. Explain the difference between $\mathcal{L}_1 \cap \mathcal{L}_2$ and $\mathcal{L}_1 \bullet \mathcal{L}_2$.

Problem 23.28. For each language $\mathcal{L}$, give example strings in $\mathcal{L}$ and strings not in $\mathcal{L}$.
  (a) $\mathcal{L} = \{0^{\bullet n} 1^{\bullet m} \mid n \geq 0, m \geq 1\}$.   (c) $\mathcal{L} = \{w \neq uu^{\mathrm{R}} \mid u \in \Sigma^*\} \cap \mathcal{L}_{\mathsf{palindrome}}$.   (e) $\mathcal{L} = \{1\}^* \bullet \{01\}^*$.
  (b) $\mathcal{L} = \{w = uu^{\mathrm{R}} \mid u \in \Sigma^*\}$.   (d) $\mathcal{L} = \Sigma^{\bullet 3}$, where $\Sigma = \{0, 1\}$.   (f) $\mathcal{L} = \{1\} \bullet \{01\}^*$.

Problem 23.29. Find regular expressions for $\mathcal{L}$ and its reversal $\mathcal{L}^{\mathrm{R}}$ (Problem 23.23), where strings of $\mathcal{L}$ satisfy:
  (a) The first and last bit are the same.   (d) There is exactly one occurrence of 111 as a substring.
  (b) The number of 1s is divisible by 2.   (e) There is at least one occurrence of 100 as a substring.
  (c) Every 0 is followed by at least one 1.   (f) The length of the strings is a multiple of 5.

Problem 23.30. Let $\mathcal{L}_1 = \{0^{\bullet 2}\}$ and $\mathcal{L}_2 = \{0^{\bullet 3}\}$.
  (a) Give informal English descriptions of (i) $\mathcal{L}_1^*$ (ii) $\mathcal{L}_2^*$ (iii) $(\mathcal{L}_1 \cup \mathcal{L}_2)^*$.
  (b) Generalize. Let $\mathcal{L}_1 = \{0^{\bullet x}\}$ and $\mathcal{L}_2 = \{0^{\bullet y}\}$. Give an informal English description of $(\mathcal{L}_1 \cup \mathcal{L}_2)^*$. *[Hint: $\gcd(x, y)$.]*

Problem 23.31. True or False: (a) $100 \in \{0\}^* \bullet \{1\}^* \bullet \{0\}^* \bullet \{1\}^*$ (b) $001 \in \{0\}^* \bullet \{1\}^* \bullet \{0\}^* \bullet \{1\}^*$.

Problem 23.32. True or False? Explain your answer.
  (a) Let $\mathcal{L}_1 = \{0\}^* \bullet \{1\}^*$ and $\mathcal{L}_2 = \{1\}^* \bullet \{0\}^*$. Then, $\mathcal{L}_1 \cap \mathcal{L}_2 = \varnothing$.
  (b) Let $\mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_3$ be any three languages. Then, $(\mathcal{L}_1 \bullet \mathcal{L}_2)^* \bullet \mathcal{L}_3^* = \mathcal{L}_1^* \bullet (\mathcal{L}_2 \bullet \mathcal{L}_3)^*$.
  (c) Let $\mathcal{L}_1, \mathcal{L}_2$ be any two languages. Then, $\mathcal{L}_1 \bullet (\mathcal{L}_2 \bullet \mathcal{L}_1)^* = (\mathcal{L}_1 \bullet \mathcal{L}_2)^* \bullet \mathcal{L}_1$.

Problem 23.33. Give a regular expression for each language when (i) you may and (ii) you may not use complements.
  (a) Strings with at most one 1 and at most one 0.   (b) Strings whose number of 0s is not divisible by 4.

Problem 23.34. True or False: A regular expression without any Kleene star operations describes a finite language.

Problem 23.35. Construct a state transitioning machine for the language in Pop Quiz 23.1, a push-light whose start state can be on or off (similar to the machine for $\mathcal{L}_{\mathsf{push}}$ on page 343). For an input string in the language, the final resting state of the machine should decide if the light is on or off.

Problem 23.36 (Decision vs. calculation). Formulate a decision version of the arithmetic task of calculating the product $x \times y$ of given non-negative integers x, y.

(a) How many times do you need to use the decision problem to solve the arithmetic task?

(b) What are your thoughts if x, y are positive real numbers?

Problem 23.37 (Independent set: decision vs. search). The search task is to *find* a maximum independent set in an input graph G. This *search* version is different from the optimization version which asks for the *size* of a maximum independent set, $\alpha(G)$. The decision version of maximum independent set is:

> **Problem:** INDEPENDENT-SET-K
> **Input:** Finite graph $G = (V, E)$ and target K.
> **Question:** Is there an independent set in G of size at least K.

A solver for the decision version can solve the optimization version. Show that the decision version can solve the search version to find a maximum independent. For a vertex v in G, $N(v)$ are the neighbors of v. For a subset of vertices S, $G - S$ is the induced subgraph obtained after removing S.

(a) Show how to obtain $\alpha(G)$ using INDEPENDENT-SET-K.

(b) Show that if v is in a maximum independent set of G, then $\alpha(G) = 1 + \alpha(G - \{v\} \cup N(v))$.

(c) Show that if v is not in any maximum independent set of G, then $\alpha(G) = \alpha(G - \{v\})$.

(d) Show how you can construct a maximum independent set using INDEPENDENT-SET-K.

(e) What is the maximum number of calls to INDEPENDENT-SET-K that are needed?

Problem 23.38 (Coloring: decision vs. search). The search task is to *find* a valid coloring using the fewest colors for an input graph G. The optimization version only asks for the *minimum number* of colors needed, the chromatic number $\chi(G)$. The decision version of graph coloring is:

> **Problem:** GRAPH-COLORING-K
> **Input:** Finite graph $G = (V, E)$ and target K.
> **Question:** Is there a valid coloring of G that uses at most K colors.

A solver for the decision version can solve the optimization version. Show that the decision version can also solve the search version to find an optimal coloring. Let u and v be non-adjacent vertices in G.

(a) Show how to obtain the chromatic number $\chi(G)$ using the decision version of coloring.

(b) The contraction $G_{u,v}^-$ merges u, v into one vertex w whose neighbors are all neighbors of u or v. The augmentation $G_{u,v}^+$ adds the edge (u, v). Give $G_{u,v}^-$ and $G_{u,v}^+$ for the graph shown on the right.

(c) Show: if some optimal coloring in G gives u and v the same color, then $\chi(G) = \chi(G_{u,v}^-)$. In this case, how can you get an optimal coloring of G from an optimal coloring of $G_{u,v}^-$?

(d) Show: if every optimal coloring of G gives different colors to u, v then $\chi(G) = \chi(G_{u,v}^+)$. In this case, how do you get an optimal coloring of G from an optimal coloring of $G_{u,v}^+$?

(e) Show how to get an optimal coloring of G using repeated calls to GRAPH-COLORING-K.

(f) What is the maximum number of calls to GRAPH-COLORING-K that are needed?

Problem 23.39. Ayfos forms a list $\{\mathcal{L}_1, \mathcal{L}_2, \ldots\}$ of languages. Prove that some language is not on the list.

Problem 23.40 (Finite Descriptions). A precise definition of a language such as $\{\varepsilon, 0, 11, 101, 1111, 11011, \ldots\}$ must be finite and unambiguous. For example, $\{(01)^{\bullet n} \mid n \geq 0\}$ is the language $\{\varepsilon, 01, 0101, 010101, \ldots\}$.

Assume any finite description can only use the 255 characters of the ASCII code, but it can be arbitrarily long. Prove that some languages cannot be described. *[Hint: Use a counting argument.]*

Problem 23.41. For a countable alphabet $\Sigma = \{\sigma_1, \sigma_2, \sigma_3, \ldots\}$ show that the set of all finite strings Σ^* is countable.

Problem 23.42. Let $\mathcal{L}$ be an *infinite* subset of $\{0\}^*$.

(a) Prove that some such $\mathcal{L}$ cannot be described by a finite regular expression.

(b) Prove that $\mathcal{L}^*$ can always be described by a finite regular expression. *[Hint: Problem 23.30.]*

Problem 23.43. Test your intuition. The languages $\mathcal{L}_{(01)^n}, \mathcal{L}_{0^n 1^n}, \mathcal{L}_{\text{palindrome}}, \mathcal{L}_{\text{repeated}}$ are defined in the text. Sort them in order of increasing "complexity". Explain you reasoning. (Don't cheat by reading ahead 😊.)

24.4 Problems

**Problem 24.1.** You email a friend about your fancy new DFA for a language with binary alphabet $\Sigma = \{0, 1\}$.
(a) Your DFA has 5 states, $q_0, \ldots, q_4$. Identify what you must send your friend. How many bits of information is it?
(b) Generalize (a) to an alphabet $\Sigma = \{\sigma_1, \ldots, \sigma_s\}$ with s symbols, and a DFA with k states $q_0, \ldots, q_{k-1}$.

Problem 24.2. For the finite automaton on the right:
(a) What is the start state? What is the set of accept states?
(b) What sequence of states are visited for input 0011?
(c) Give all strings of length at most 4 accepted by the machine.
(d) Give the conditions on a general automaton M under which $\varepsilon \in \mathcal{L}(M)$?
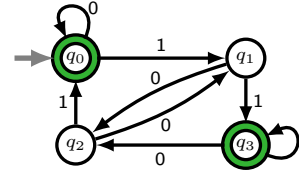
Problem 24.3. Describe in words the language accepted by each automaton, and also give a regular expression.
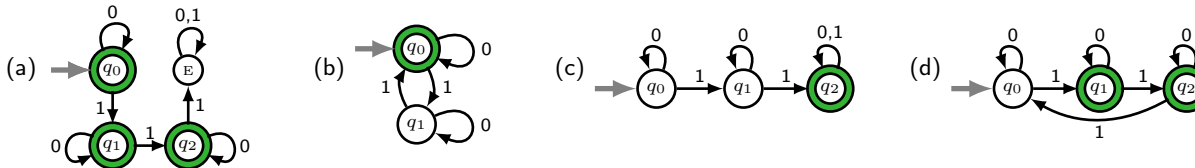
Problem 24.4. State diagrams (directed graphs) are a nice visual way to describe DFAs. One can also use a table whose rows are states. Entries in a state's row indicate where to transition for each input bit. The start state is q_0 and we use green and red for the (YES) and (NO) states. Describe in words the languages accepted by each automaton.

(a)	1	0
→ q_0	q_0	q_1
q_1	q_1	q_0

(b)	1	0
→ q_0	q_1	q_0
q_1	q_2	q_2
q_2	q_1	q_0

(c)	1	0
→ q_0	q_1	q_1
q_1	q_1	q_2
q_2	q_2	q_1

(d)	1	0
→ q_0	q_1	q_0
q_1	q_1	q_0
q_2	q_2	q_2

(e)	1	0
→ q_0	q_1	q_0
q_1	q_2	q_1
q_2	q_3	q_2
q_3	q_3	q_3

(f)	1	0
→ q_0	q_1	q_0
q_1	q_3	q_2
q_2	q_1	q_0
q_3	q_3	q_2

(g)	1	0
→ q_0	q_3	q_0
q_1	q_4	q_0
q_2	q_1	q_2
q_3	q_4	q_2
q_4	q_4	q_4

Problem 24.5. Problem 24.4 shows how to describe a DFA using a table. Give the table description of the DFAs in Problem 24.3. Instead of color coding states, you may identify accept states by just circling them.

Problem 24.6. Give the simplest automaton which accepts each language.
(a) All finite strings, Σ^*. (b) No strings, $\varnothing$. (c) Just the empty string ε. (d) All strings but the empty string ε.

Problem 24.7. Give DFA's for the following computing tasks.
(a) The DFA accepts quarters and dispenses a coke each time the machine gets 3 quarters.
(b) The DFA accepts quarters and dimes and dispenses candy when the balance is at least 50¢.
(c) (i) $\mathcal{L} = \{00010, 10111\}$ (ii) $\mathcal{L} = \{$strings with 101 as a substring$\}$ (iii) $\mathcal{L} = \{001^{\bullet 2n} | n \geq 0\}$.
(d) Fix $d \in \mathbb{N}$. (i) $\mathcal{L} = \{1^{\bullet n} \mid n$ is a multiple of $d\}$ (ii) $\mathcal{L} = \{w \mid w$ is a binary number that is a multiple of $d\}$.

Problem 24.8. What is the probability a random 10-bit-string $b_1 b_2 \ldots b_{10}$ is accepted by each automaton?
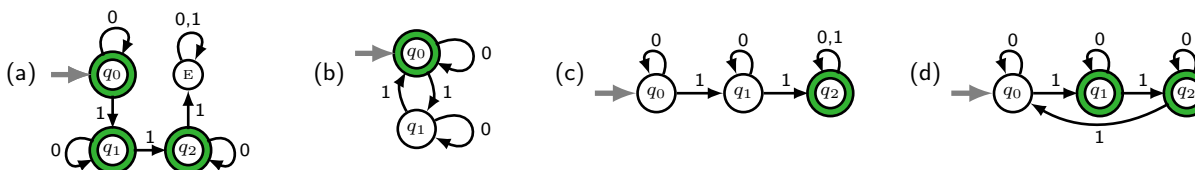
Problem 24.9. The DFA processes $b_1 \ldots b_n$, a random string of n independent bits where $b_i = 1$ with probability p. Show that $\mathbb{P}[\text{accept}] = 1 - (1-p)^n - np(1-p)^{n-1}$.
[Hint: Find a simple property of accepted strings and use the Binomial distribution.]
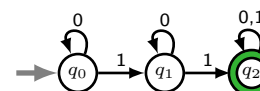
Problem 24.10. A voomba vacuum-rover ▲, when placed on one end of a dirt path, should move step by step and vacuum up all the dirt. The voomba can sense dirt in the square ahead, can rotate 90° clockwise, can move forward and transition among its internal states. Design a voomba as a DFA. In the picture, the voomba is facing north, left of the first piece of dirt.
When will your voomba succesfully vacuum all the dirt? Give an informal argument.
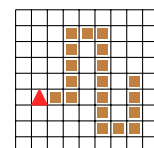
Problem 24.11. Give DFAs for the following languages, aka computing problems.

(a) Strings which end in 1.
(b) Strings which do not end in 1.
(c) Strings which begin in 1 and end in 0.
(d) Strings which do not contain any 0s.
(e) $\mathcal{L} = \{1^{\bullet 5n} \mid n \geq 0\}$.
(f) $\mathcal{L} = \{1^{\bullet 2n}01^{\bullet 2k+1} \mid n, k \geq 0\}$.
(g) Strings which begin with 10 or end with 01.
(h) Strings which begin with 10 and end with 01.
(i) Strings in which every 0 is adjacent to a 0.
(j) All strings except 10 and 100.
(k) Strings whose 3rd bit from the end is 1.
(l) Strings which begin and end in the same bit.
(m) Strings whose adjacent bits are different.
(n) Non-empty strings with an even number of 1s.
(o) Strings not of the form $0^{\bullet n}1^{\bullet k}$ for $n, k \geq 0$.
(p) Strings which contain 0101 as a substring.
(q) Strings which do not contain 001 as a substring.
(r) Strings whose even bits alternate between 0 and 1.
(s) Strings whose odd bits match the previous even bit.
(t) Strings with no 1s separated by an odd number of symbols.
(u) Strings with no 1s separated by an even number of symbols.
(v) Strings with an even number of 0s and one or two 1s.
(w) Strings whose length is divisible by 3.
(x) Strings whose length is not divisible by 2 or 3.
(y) Strings with an even number of 1s or more than two 1s.
(z) Strings with exactly two 0s and exactly two 1s.

Problem 24.12. Use DFAs for simpler languages to find a DFA for each language.

(a) Strings of even length with an odd number of 0s.
(b) Strings with an odd number of 0s that end in 1.
(c) Strings with exactly two 0s and at least two 1s.
(d) Strings which do not contain exactly two 0s.
(e) Strings with exactly two 0s and exactly two 1s.
(f) Strings with matching even bits and matching odd bits.
(g) Strings whose length is not divisible by 2 or 3.
(h) Strings which do not contain the substring 01.
(i) Strings which do not contain either 01 or 10 as substrings.
(j) Strings of odd length not in $\{0\}^* \bullet \{1\}^*$.

Problem 24.13 (Transducer). A DFA-transducer resembles everyday computing. DFAs answer (YES) or (NO). Transducers also transform the input string to an output. A schematic is on the right. At each step, the DFA reads an input bit, transitions state *and* may write a string to the output. For example, consider this instruction,

It says: "If you read 1 when in state q_0, transition to q_5 and write 01."

(a) Give the output of each transducer on: (i) 00 (ii) 111 (iii) 11101 (iv) 0010101.
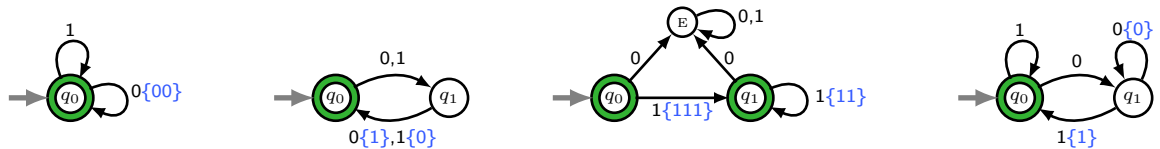
(b) Describe in words the tasks implemented by each transducer in part (a).
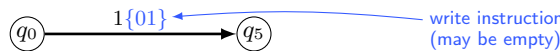(c) Give a transducer whose output is every third bit of the input string flipped. For example $0011000100 \to 011$.
(d) Prove that, for input w, no DFA-transducer writes to output: (i) w^{R} *[Hint: $w = 00$ and $w = 01$.]*   (ii) ww.

Problem 24.14 (Addition). These languages correspond to the arithmetic task of addition.

(a) Let $\mathcal{L} = \{w_1 \# w_2 \# w_3 \mid w_1 + w_2 = w_3\}$ where # is a punctuation symbol and w_1, w_2, w_3 are treated as binary numbers. For example, $101\#11\#1000 \in \mathcal{L}$ and $101\#011\#1111 \notin \mathcal{L}$. Prove that no DFA solves $\mathcal{L}$.
(b) Recall that one can define languages using any alphabet Σ. Use a new alphabet Σ_3,

$$\Sigma_3 = \left\{ \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \right\}.$$

A string in Σ_3^* has 3 rows of bits, each row defines a binary string. Define a language $\mathcal{L}_3$ for addition where a string is in $\mathcal{L}_3$ if the sum of the first two rows (binary numbers) equals the third. For example,

$$\begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}\begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} \in \mathcal{L}_3 \qquad\qquad \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}\begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} \notin \mathcal{L}_3$$

Prove that $\mathcal{L}_3$ is regular. *[Hint: Build a DFA for the reversal $\mathcal{L}_3^{\mathrm{R}}$. How does this help? See Problem 24.44.]*
(c) Convert $\mathcal{L}_3$ to a regular language $\mathcal{L}_{\mathrm{ADD}}$ over the binary alphabet $\Sigma = \{0, 1\}$. *[Hint: $001100010110 \in \mathcal{L}_{\mathrm{ADD}}.]*
(d) At a high level, explain the difference between $\mathcal{L}$ and $\mathcal{L}_{\mathrm{ADD}}$, and how come $\mathcal{L}_{\mathrm{ADD}}$ is regular but $\mathcal{L}$ is not.

The format of the input to a computer (DFA) can affect whether a problem is solvable.

Problem 24.15 (Two Input Tapes). In each setting, create a DFA to test two input strings x and y for equality.
   (a) The DFA has two read-heads and x and y are on two input tapes. The DFA alternately reads bits from x and y.
   (b) The DFA has one input tape, and the input string is xy. *[Hint: $\mathcal{L} = \{ww \mid w \in \Sigma^*\}$.]*
   (c) The DFA has one input tape, and the input string has the bits of x and y interleaved, $x_1y_1x_2y_2\cdots$.

Problem 24.16 (Hidden Markov Model (HMM)). A patient has two states, normal $\textcircled{N}$, or epileptic $\textcircled{E}$. On exposure to a sequence of light stimuli, 0 for dark and 1 for bright, the patient transitions state and emits an output of 0 for no muscle spasm or 1 for a muscle spasm. The patient is a probabilistic automaton with transducer capabilities.

1, prob=0.8 {prob(0)=0.8}
0, prob=1.0 {prob(0)=0.9}

1, prob=0.1 {prob(0)=0.4}
0, prob=0.4 {prob(0)=0.5}

1, prob=0.9 {prob(0)=0.2}
0, prob=0.6 {prob(0)=0.3}

N   E

1, prob=0.2 {prob(0)=0.7}
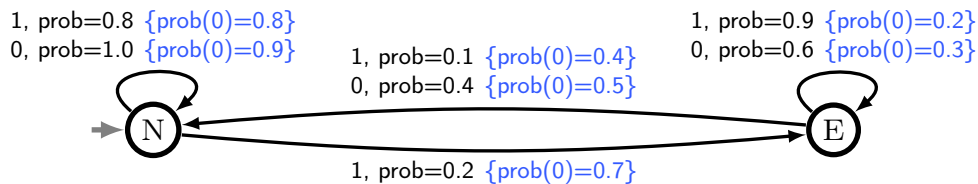
The start state is normal. The label "1, prob=0.8 {prob(0)=0.8}" on the arrow from $\textcircled{N}$ to $\textcircled{N}$ means: from state $\textcircled{N}$ with input 1, transition to $\textcircled{N}$ with probability 0.8 and output 0 with probability 0.8 or 1 with probability 0.2.
   (a) Explain in words each instruction shown in the state diagram and why they intuitively make sense.
   (b) Use build-up probability where needed to compute these probabilities.
       (i) The input is 0111. Find the probability that the final state is epileptic. (The states are "hidden" from view.)
       (ii) The input is 0111 and the output is 0110. Find the probability that the final state is epileptic.
       (iii) For a random (unknown) input, the output is 0110. Find the probability that the final state is epileptic.
In practice, one learns the HMM probabilities (the "biology") from observed outputs, a topic in machine learning.

Problem 24.17. Let $\mathcal{L} = \{$strings not containing 01 as a substring, with an even number of 0s and odd number of 1s$\}$.
   (a) $\mathcal{L}$ is related to 3 simpler languages. Use DFAs for the simpler languages and product states to get a DFA for $\mathcal{L}$.
   (b) Find a 5-state DFA for $\mathcal{L}$ by carefully analyzing $\mathcal{L}$ and describing it more simply.

Problem 24.18. Give a DFA for the language $\mathcal{H}$ containing strings that end at their first occurrence of 11,

$$\mathcal{H} = \{w \mid w = x11, x \text{ does not end in 1 or contain 11 as a substring}\}.$$

Problem 24.19. Give a DFA for the language of all strings with length at most ℓ. Use as few states as you can.

Problem 24.20. Let $\mathcal{L}_3 = \{$strings whose 3rd bit from the right is 0$\}$.
   (a) Give a regular expression for $\mathcal{L}_3$.
   (b) Give a DFA to solve $\mathcal{L}_3$ using at most 8 states and show that no DFA with fewer than 8 states solves $\mathcal{L}_3$.
   (c) Generalize to $\mathcal{L}_k = \{$strings whose kth bit from the right is 0$\}$. Show that 2^k states are needed.

Problem 24.21. Let $\mathcal{L}_3 = \{ww \mid w \text{ has length 3}\}$.
   (a) Give a DFA to solve $\mathcal{L}_3$ using at most 8 states and show that no DFA with fewer than 8 states solves $\mathcal{L}_3$.
   (b) Generalize to $\mathcal{L}_k = \{ww \mid w \text{ has length } k\}$. Show that 2^k states are needed.

Problem 24.22. Let $\mathcal{L}_1 = \{w \mid w \text{ contains } 010\}$ and $\mathcal{L}_2 = \{w \mid w \text{ begins and ends in 1}\}$. Find DFAs for:
(a) $\mathcal{L}_1$ and $\mathcal{L}_2$.   (b) $\overline{\mathcal{L}_1}$ and $\overline{\mathcal{L}_2}$.   (c) $\mathcal{L}_1 \cap \mathcal{L}_2$ and $\mathcal{L}_1 \cup \mathcal{L}_2$.   (d) $\mathcal{L}_1 \bullet \mathcal{L}_2$ and $\mathcal{L}_2 \bullet \mathcal{L}_1$.   (e) $\mathcal{L}_1^*$ and $\mathcal{L}_2^*$.

Problem 24.23. Suppose $\mathcal{L}_1$ and $\mathcal{L}_2$ are both *not* regular. Prove or disprove that these languages can't be regular:
(a) $\mathcal{L}_1 \cup \mathcal{L}_2$ (b) $\mathcal{L}_1 \cap \mathcal{L}_2$ (c) $\mathcal{L}_1 \bullet \mathcal{L}_2$ (d) $\overline{\mathcal{L}_1}$.

Problem 24.24. Two automata are the *same* if there is an isomorphism between them with $\boxed{\text{YES}}$-states mapping to $\boxed{\text{YES}}$-states and $\boxed{\text{NO}}$-states mapping to $\boxed{\text{NO}}$-states. Give two *different* automata which accept the same language.

Problem 24.25 (Count DFAs). How many different DFA's have two states, a start state q_0 and q_1. A DFA is defined by its accept states and transition instructions, which can be described by a graph with nodes q_0, q_1 and a directed edge for each instruction (accept states have double circles). Different DFA's can have the same $\boxed{\text{YES}}$-set.

Problem 24.26. Give regular expressions to describe each laguage in Problem 24.11.

Problem 24.27. For each language $\mathcal{L}$, give a DFA which accepts $\mathcal{L}$ and a regular expression that describes $\mathcal{L}$.

(a) Strings which contain 00 as a substring.   (c) Strings with at least two 0s.

(b) Strings with at most two 0s.   (d) Strings in which the number of 0s is even and 1s is odd.

Problem 24.28. Find DFAs for languages described by these regular expressions. (The wildcard $*$ stands for Σ^*).

(a) $(\{01\} \cup \{001\})^*$ (b) $\{0\}^* \bullet \overline{(\{10\} \cup \{11\})^*}$ (c) $\{0\}^* \cup \{1\}^*$ (d) $(\{01\} \bullet \{1\}^*)^*$ (e) $*101*1$.

Problem 24.29. Construct a regular expression for the $\boxed{\text{YES}}$-set of each DFA.

(a)   (b)   (c)
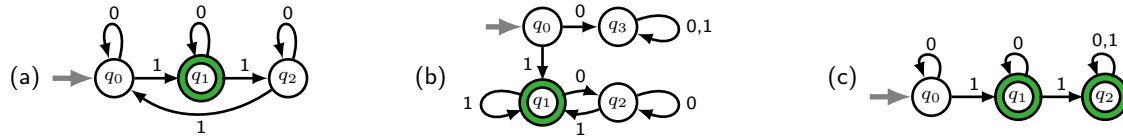
Problem 24.30 (Convert a DFA to a regular expression).

(a) For the DFA M on the right, show $\mathcal{L}(M) = \{0,1\} \bullet \{0\}^* \bullet (\{1\} \bullet \{0,1\} \bullet \{0\}^*)^*$.

(b) One can systematically convert any DFA to a regular expression. The language $\mathcal{L}$ of a DFA with states $q_0, \ldots, q_\ell$ contains all strings that take the automaton from its start state q_0 to a $\boxed{\text{YES}}$-state. Define the language $\mathcal{L}_k(i,j)$ as the set of strings that take the automaton from state q_i to state q_j visiting *only* states in $\{q_0, q_1, \ldots, q_{k-1}\}$ along the way. The strings in $\mathcal{L}_0(i,j)$ take q_i directly to q_j without visiting any other state. For strings in $\mathcal{L}_1(i,j)$, the automaton can visit q_0; for strings in $\mathcal{L}_2(i,j)$, the automaton can visit states in $\{q_0, q_1\}$; and so on.

  (i) For our DFA M, what are $\mathcal{L}_0(0,0), \mathcal{L}_0(0,1), \mathcal{L}_0(1,0), \mathcal{L}_0(1,1)$?

  (ii) The strings in $\mathcal{L}_1(i,j)$ take q_i to q_j without visiting any of the states $q_1, \ldots, q_\ell$. The only state that may be visited, if at all, is q_0. Show that $\mathcal{L}_1(i,j)$ is

$$\mathcal{L}_1(i,j) = \mathcal{L}_0(i,j) \cup \{\text{strings taking } M \text{ from } q_i \text{ to } q_j \text{ that visit } q_0 \text{ and no higher state}\}.$$

  Hence, show that $\mathcal{L}_1(i,j) = \mathcal{L}_0(i,j) \cup (\mathcal{L}_0(i,0) \bullet \mathcal{L}_0(0,0)^* \bullet \mathcal{L}_0(0,j))$.

  (iii) Use (ii) to obtain regular expressions for $\mathcal{L}_1(0,0), \mathcal{L}_1(0,1), \mathcal{L}_1(1,0), \mathcal{L}_1(1,1)$.

  (iv) Find regular expressions for $\mathcal{L}_2(0,0), \mathcal{L}_2(0,1), \mathcal{L}_2(1,0), \mathcal{L}_2(1,1)$ by first showing that

$$L_2(i,j) = \mathcal{L}_1(i,j) \cup (\mathcal{L}_1(i,1) \bullet \mathcal{L}_1(1,1)^* \bullet \mathcal{L}_1(1,j)).$$

  (v) Show that $\mathcal{L}(M) = \mathcal{L}_2(0,1)$, and hence give a regular expression for $\mathcal{L}(M)$.

(c) Does the regular expression in (b) use complement or intersection? What is the significance of your answer?

Problem 24.31. Use the method in Problem 24.30 to find regular expressions for each DFA in Problem 24.29.

Problem 24.32. Regular expressions are solved by a DFAs. Prove the converse, that computing problems solvable by DFAs can be described by regular expressions DFAs and regular expressions are "equivalent". Prove the theorem:

Theorem 24.4. The $\boxed{\text{YES}}$-set of any DFA can be described by a regular expression.

To prove it, generalize Problem 24.30 to an automaton with k states $q_0, \ldots, q_{k-1}$ whose $\boxed{\text{YES}}$-states are $q_\ell, \ldots, q_{k-1}$.

(a) Show that $\mathcal{L}_0(i,j)$ is a finite language, hence a regular expression.

(b) Show that for $k \geq 0$, $L_{k+1}(i,j) = \mathcal{L}_k(i,j) \cup (\mathcal{L}_k(i,k) \bullet \mathcal{L}_k(k,k)^* \bullet \mathcal{L}_k(k,j))$.

(c) Prove, by induction on n, that $L_n(i,j)$ can be described by a regular expression for all $i, j = 0, 1, \ldots, k-1$.

(d) Show that $\mathcal{L}(M) = \cup_{j=\ell}^{k-1} \mathcal{L}_k(0,j)$ and prove Theorem 24.4. The union is over the $\boxed{\text{YES}}$-states $q_\ell, \ldots, q_{k-1}$.

Problem 24.33. Find a regular expression that *does not* use complement to describe the language $\overline{\{0,01\}^*}$.

(a) Give a DFA for the language $\{0,01\}$.

(b) Give a nondeterministic automaton for the language $\{0,01\}^*$. *[Hint: See Exercise 24.8 on page 355.]*

(c) Use subset-states to convert your automaton in (b) into a DFA.

(d) Construct a DFA to accept the complement of the language accepted by your DFA in (c).

(e) Use the method in Problem 24.32 to find a regular expression for the DFA in (d).

Problem 24.34. Let $\mathcal{L} \subseteq \{0\}^*$ be an infinite language over a unary alphabet, and consider $\mathcal{L}^*$.

(a) Let $\mathcal{L} = \{0^{\bullet 2^n} \mid n \geq 0\}$. Do you think $\mathcal{L}$ is regular? What about $\mathcal{L}^*$?

(b) Show that $\mathcal{L}^*$ is always regular (solvable by a DFA), even if $\mathcal{L}$ is not regular. *[Hint: Problems 23.30 and 23.42.]*

(c) Prove there are *uncountably* many $\mathcal{L} \subset \{0\}^*$ which are *not* regular. *[Hint: Infinite binary strings are uncountable.]*

Problem 24.35. Give an example of languages that are not regular but whose union is regular. You must prove neither language is regular and that the union is regular. Do the same for intersection. What about complement?

Problem 24.36. You have access to the state diagrams (directed graph) of DFAs M_1 and M_2.
(a) How would you determine if $\mathcal{L}(M_1)$ is empty?   (b) How would you determine if $\mathcal{L}(M_1) \cap \mathcal{L}(M_2)$ is empty?

Problem 24.37. Let M be a DFA with k states whose language is $\mathcal{L}(M)$. Prove the following.
(a) $\mathcal{L}(M)$ is empty if and only if M accepts no string of length at most $k - 1$. *[Hint: Suppose the shortest string M accepts has length $\ell \geq k$. Use the pigeonhole principle to show that M accepts a shorter string.]*
(b) $\mathcal{L}(M)$ is infinite if and only if M accepts some string w whose length satisfies $k \leq \text{length}(w) \leq 2k - 1$.
(c) Do either of the claims in (a) or (b) depend on whether the alphabet Σ is binary?

Problem 24.38. A DFA M with at most 10 states is given as a black-box. You may run M on finitely many inputs and observe the outputs (YES) or (NO). Show how to answer these questions. Problem 24.37 may be useful.
(a) Is 010101 in $\mathcal{L}(M)$?   (b) Is $\mathcal{L}(M)$ empty?   (c) Is $\mathcal{L}(M)$ infinite?   (d) Does $\mathcal{L}(M)$ contain all strings?

Problem 24.39. DFAs M_1 and M_2 with at most k_1 and k_2 states are given as black-boxes. You can run the DFAs on inputs and observe the outputs (YES) or (NO). Show how to determine whether M_1 and M_2 solve the same problem.
(a) Let $\mathcal{L}_1 = \mathcal{L}(M_1)$ and $\mathcal{L}_2 = \mathcal{L}(M_2)$. What does it mean for M_1 and M_2 to solve the same problem?
(b) The set difference $\mathcal{L}_1 \setminus \mathcal{L}_2 = \{$strings in $\mathcal{L}_1$ that are not in $\mathcal{L}_2\}$. Is $\mathcal{L}_1 \setminus \mathcal{L}_2$ regular? *[Hint: $A \setminus B = A \cap \overline{B}$.]*
(c) Use (b) to give a method to determine if $\mathcal{L}_1 = \mathcal{L}_2$. *[Hint: Problem 24.38.]*
(d) For your solution in (c), how many times do you need to run M_1 and M_2? Does it depend on the alphabet size?

Problem 24.40 (Nondeterminism). Answer questions (i)–(iii) for each nondeterministic automaton.
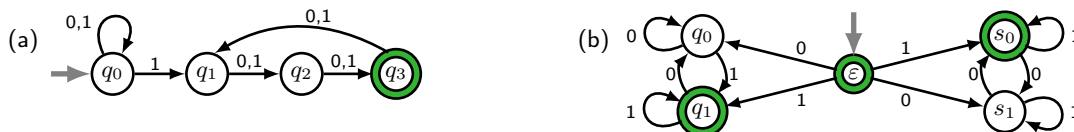
(i) At a nondeterministic step, imagine the automaton guesses how to proceed and has the luxury to always guess correctly and accept the input if possible. Use this view to describe in words the task solved by each automaton.
(ii) In a DFA, a computation traces a sequence of states. With nondeterminism, the path branches at every nondeterministic step, creating a tree of states rooted at the start state. Show the computation tree for input 11011.
(iii) Use subset states to convert each nondeterministic automaton to a DFA. For your DFA and the nondeterministic version, show the sequence of states for two (YES)-strings and two (NO)-strings.

Problem 24.41 (Nondeterminism and complement). For a DFA M accepting the language $\mathcal{L}(M)$, we saw that to solve the complement problem $\overline{\mathcal{L}(M)}$, you simply flip the (YES) and (NO) states in M.
(a) Give the automaton obtained by flipping the (YES) and (NO) states of the automaton in Problem 24.40(a).
(b) What is the output for the original automaton and the automaton with states flipped on the input 100?
(c) Articulate why flipping the states does not always solve the complement language for a nondeterministic automaton.
(d) Give a method to find the automaton for the complement language of a nondeterministic automaton?

Problem 24.42. Find DFAs for the reversal of each language, containing the reversed strings: $\mathcal{L}^{\text{R}} = \{w^{\text{R}} \mid w \in \mathcal{L}\}$.
(a) Strings which end in 1.
(b) Strings which begin in 1 or end in 0.
(c) Strings which do not contain any 0s.
(d) $\mathcal{L} = \{1^{\bullet 2n}01^{\bullet 2k+1} \mid n, k \geq 0\}$.
(e) Strings in which every 0 is adjacent to a 0.
(f) Strings whose adjacent bits are different.
(g) *Non-empty* strings with an even number of 1s.
(h) Strings *not* of the form $0^{\bullet n}1^{\bullet k}$ for $n, k \geq 0$.
(i) Strings which contain 001 as a substring.
(j) Strings which do not contain 001 as a substring.
(k) Strings whose even bits alternate between 0 and 1.
(l) Strings whose odd bits match the previous even bit.

Problem 24.43. For the DFA M, find a DFA M^{R} for the reversal of $\mathcal{L}(M)$.
(a) Follow these steps: (i) Flip the roles of two states. (ii) Change the directions of the arrows. (iii) Is the resulting automaton deterministic? What if a state has no exiting arrow for a particular input-bit? (iv) Find a DFA for $\mathcal{L}(M)^{\text{R}}$.
(b) Find a simpler DFA for $\mathcal{L}(M)^{\text{R}}$ by analyzing the language solved by M.
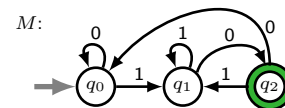
Problem 24.44. Show how to systematically go from a DFA for $\mathcal{L}$ to a DFA for $\mathcal{L}^{\text{R}}$.

M_1:

(a) We modified M from Problem 24.43 to M_1, making q_1 also a $\boxed{\text{YES}}$-state.

  (i) Does Problem 24.43(a) work for creating M_1^{R} to slove $\mathcal{L}(M_1)^{\text{R}}$?

  (ii) Modify M_1 as follows. Make q_1 and q_2 $\boxed{\text{NO}}$-states. Create two new states, one for accept, A, and one for error, E. Whenever M_1 would have transitioned to an accept state, *also* allow the new DFA to transition to A. From A, if a new bit arrives, transition to E and remain there. Using these instructions, derive the modified automaton with blue arrows, as shown.

  (iii) Is the modified automaton deterministic or nondeterministic.

  (iv) Explain why the modified automaton solves the same problem as M_1.

  (v) Use the modified automaton to find a DFA M_1^{R} for $\mathcal{L}(M_1)^{\text{R}}$.

(b) Find a simpler DFA S_1^{R} for $\mathcal{L}(M_1)^{\text{R}}$ by analyzing the language M_1 solves. On all strings of length 4, show the trajectory of states and final decision from M_1, the complex DFA M_1^{R} from part (b) and your simplified DFA S_1^{R}.

(c) If nondeterminism is allowed, prove that an automaton with just one $\boxed{\text{YES}}$-state can solve any regular language.

(d) Prove that the reversal of any regular language is also regular.
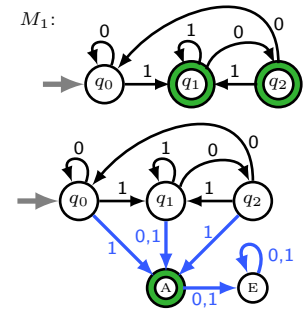
Problem 24.45. Let $\mathcal{L} = \{$strings with a 1 at some multiple of 3 bits from the end$\}$.

(a) Find a DFA M^{R} for the reversal $\mathcal{L}^{\text{R}}$ and use M^{R} to get a DFA for $\mathcal{L}$ using the methods in Problem 24.44.

(b) Find a nondeterministic automaton for $\mathcal{L}$ and use subset states to convert it to a DFA. (Problem 24.40 may help.)

Problem 24.46. In each case, a language $\mathcal{L}$ is obtained from regular languages $\mathcal{L}_1, \mathcal{L}_2$. Prove that $\mathcal{L}$ is regular. Either give a regular expression for $\mathcal{L}$ or show how to get a DFA for $\mathcal{L}$ from DFAs for $\mathcal{L}_1, \mathcal{L}_2$.

(a) $\mathcal{L} = \{$strings in $\mathcal{L}_1$ which are *not* in $\mathcal{L}_2\}$.   (Closure under set-difference.)

(b) $\mathcal{L} = \{$strings which are a prefix of some string in $\mathcal{L}_1\}$.   (Closure under prefixing.)

(c) $\mathcal{L} = \{$strings in $\mathcal{L}_1$ which are a prefix of some string in $\mathcal{L}_2\}$.   (Closure under prefixing.)

(d) $\mathcal{L} = \{$strings which are a suffix of some string in $\mathcal{L}_1\}$. *[Hint: Reversal.]*   (Closure under suffixing.)

(e) $\mathcal{L} = \{$strings in $\mathcal{L}_1$ which are a suffix of some string in $\mathcal{L}_2\}$.   (Closure under suffixing.)

(f) $\mathcal{L} = \{$strings whose bits are the odd bits of some string in $\mathcal{L}_1\}$.   (Closure under subsampling.)

(g) $\mathcal{L} = \{wx \mid xw \in \mathcal{L}_1\}$.   (Closure under flipping.)

(h) $\mathcal{L} = \{$strings in $\mathcal{L}_1$ which do not contain any string in $\mathcal{L}_2$ as a substring$\}$. (Closure under avoidance.)

(i) $\mathcal{L} = \{w \mid w = x_1 y_1 x_2 y_2 \cdots x_k y_k,$ where $x_1 x_2 \cdots x_k \in \mathcal{L}_1$ and $y_1 y_2 \cdots y_k \in \mathcal{L}_2\}$.   (Closure under interleaving.)

(j) $\mathcal{L} = \{w \mid wx \in \mathcal{L}_1$ for some x with $|x| = |w|\}$.   (Closure under truncation.)

(k) $\mathcal{L} = \{w \mid wx \in \mathcal{L}_1$ for some $x \in B\}$ (Closure under completion. B can be non-regular.)

    [Hint: You can show a DFA exists without having an method to construct it.]

Problem 24.47. Prove these problems cannot be solved by DFAs. One method is to use the pigeonhole principle.

(a) $\mathcal{L} = \{0^{\bullet n} 1^{\bullet 2^n} \mid n \geq 0\}$.   (g) $\mathcal{L} = \{0^{\bullet n^2} \mid n \geq 0\}$.

(b) $\mathcal{L}_{\mathbf{geq}} = \{0^{\bullet n} 1^{\bullet k} \mid n \geq 0, k \geq n\}$.   (h) $\mathcal{L} = \{0^{\bullet n} 1^{\bullet m} 0^{\bullet n} \mid m, n \geq 0\}$.

(c) A problem whose $\boxed{\text{YES}}$-set is the palindromes.   (i) $\mathcal{L} = \{0^{\bullet n} 1^{\bullet m} \mid m, n \geq 0, m \neq n\}$.

(d) $\mathcal{L} = \{ww^R \mid w \in \Sigma^*\}$.   (j) $\mathcal{L} = \{0^{\bullet n} 1^{\bullet n+5} \mid n \geq 0\}$.

(e) $\mathcal{L} = \{$strings with an equal number of 0s and 1s$\}$.   (k) $\mathcal{L} = \{w \in \Sigma^*$ which are not palindromes$\}$.

(f) $\mathcal{L} = \{0^{\bullet 2^n} \mid n \geq 0\}$.   (l) $\mathcal{L} = \{wxw \mid w, x \in \Sigma^*\}$.

Problem 24.48. Use closure of regular languages under set operations to prove that each language $\mathcal{L}$ is not regular.

(a) $\mathcal{L} = \{$strings with an equal number of 0s and 1s$\}$. *[Hints: Contradiction. Cosider $\mathcal{L} \cap \{0^{\bullet n} 1^{\bullet k} \mid n, k \geq 0\}$.]*

(b) $\mathcal{L} = \{0^{\bullet n} 1^{\bullet k} \mid k \geq n\}$. *[Hints: Contradiction. Show that $((\overline{\mathcal{L}} \cap (\{0\}^* \bullet \{1\}^*)) \bullet \{1\}) \cap \mathcal{L} = \{0^{\bullet n} 1^{\bullet n} \mid n \geq 1\}$.]*

Problem 24.49. Prove each claim using closure of regular languages under set operations.

(a) If a finite set is removed from or added to a regular language, the resulting language is regular.

(b) If a finite set is removed from or added to a language that is not regular, the resulting language is not regular.

Problem 24.50. Find a DFA to solve each problem, or prove that no such DFA exists.

(a) Strings where the number of 1's is a multiple of 3.   (d) Strings of the form $0^{\bullet 2^n}$ for $n \geq 0$.

(b) Strings with 3 times as many 0's as 1's.   (e) $\{0^{\bullet 2^n} \mid n \geq 0\}^*$. (Kleene star)

(c) Strings of the form $0^{\bullet n^2}$ for $n \geq 0$.   (f) $\{0^{\bullet 2^n} \mid n \geq 1\}^*$. (Kleen star)

Problem 24.51. Appearances can deceive. In each case, find DFAs for two similar looking languages, if possible.

(a) $\mathcal{L}_1 = \{$Strings with 1 at a multiple of 3 from the front$\}$ $\mathcal{L}_2 = \{$Strings with 1 at a multiple of 3 from the end$\}$.

(b) $\mathcal{L}_1 = \{1^{\bullet n} w \mid n \geq 1, w$ has n or more 1's$\}$ $\qquad\qquad$ $\mathcal{L}_2 = \{1^{\bullet n} w \mid n \geq 1, w$ has n or fewer 1's$\}$.

(c) $\mathcal{L}_1 = \{0^{\bullet n} w 0^{\bullet n} \mid n \geq 1, w \in \Sigma^*\}$ $\qquad\qquad\qquad$ $\mathcal{L}_2 = \{0^{\bullet n} 1 w 0^{\bullet n} \mid n \geq 1, w \in \Sigma^*\}$.

(d) $\mathcal{L}_1 = \{0^{\bullet n} 1 w 0^{\bullet n} \mid n \geq 1, w \in \Sigma^*\}$ $\qquad\qquad\quad$ $\mathcal{L}_2 = \{0^{\bullet n} 1 w 0^{\bullet n} \mid 5 \geq n \geq 1, w \in \Sigma^*\}$.

Problem 24.52. Suppose $\mathcal{L}$ is a regular language and $\mathcal{L}^{\text{R}}$ its reversal. Prove or disprove:

(a) $\mathcal{L} \bullet \mathcal{L}^{\text{R}}$ is regular. $\qquad$ (b) $\mathcal{L}_{ww^{\text{R}}} = \{w \bullet w^{\text{R}} \mid w \in \mathcal{L}\}$ is regular. $\qquad$ (c) If $\mathcal{L} \bullet \mathcal{L}'$ is regular, then $\mathcal{L}'$ is regular.

Problem 24.53. The language $\mathcal{L}$ distinguishes a string x from a string y iff for some w, $x \bullet w \in \mathcal{L}$ and $y \bullet w \notin \mathcal{L}$.

(a) Let $\mathcal{L}_1 = \{0^{\bullet n} 1^{\bullet k} \mid n, k \geq 0\}$ and $\mathcal{L}_2 = \{0^{\bullet n} 1^{\bullet n} \mid n \geq 0\}$. Find x, y that are distinguished by $\mathcal{L}_1$. Repeat for $\mathcal{L}_2$.

(b) If $\mathcal{L}$ distinguishes x from y, does it mean $\mathcal{L}$ distinguishes y from x?

(c) Show: If $\mathcal{L}$ is regular and distinguishes x from y, then any DFA for $\mathcal{L}$ ends at different states on inputs x and y.

(d) $\mathcal{L}$ is a distinguisher for a set of strings S iff for every pair of distinct strings $x, y \in S$, either $\mathcal{L}$ distinguishes x from y or $\mathcal{L}$ distinguishes y from x. Find an infinite set S for which $\mathcal{L}_2$ is a distinguisher. Can you do the same for $\mathcal{L}_1$?

Problem 24.54. if possible, find an infinite set S for which the language $\mathcal{L}$ is a distinguisher (see Problem 24.53).

(a) $\mathcal{L} = \{0^{\bullet n} 1^{\bullet k} \mid n \geq 0, k \geq n\}$ (b) $\mathcal{L} = \{ww \mid w \in \Sigma^*\}$ (c) $\mathcal{L} = \{w \mid w \in \Sigma^*, w = w^{\text{R}}\}$ (d) $\mathcal{L} = \{0^{\bullet 2^n} \mid n \geq 0\}$.

Problem 24.55 (Myhill-Nerode Theorem). Suppose a language $\mathcal{L}$ is a distinguisher for a set S.

(a) If $\mathcal{L}$ is regular and M is a DFA for $\mathcal{L}$, prove that M ends in a different state for every input string in S.

(b) Prove the Myhill-Nerode Theorem: S is infinite if and only if $\mathcal{L}$ is not regular. *[Hint: Contradiction.]*

(c) Prove that the languages in Problem 24.54 are not regular.

The Myhill-Nerode Theorem generalizes the method of proof in the text for showing that $\{0^{\bullet n} 1^{\bullet n}\}$ is not regular.

Problem 24.56 (Pumping Lemma). Let M be a DFA with k states and let $w \in \mathcal{L}(M)$ be any string in the $\boxed{\text{YES}}$-set having length at least k. Prove that you can represent $w = xyz$ with $y \neq \varepsilon$ and $|xy| \leq k$ such that for all $i \geq 0$, $xy^{\bullet i} z \in \mathcal{L}(M)$. That is, w can be "pumped", i.e. enlarged, to $xy^{\bullet i} z = \{xz, xyz, xyyz, xyyyx, xyyyyz, \ldots\}$.

(a) Show that as M processes the first k bits of w it visits a state twice at (say) bits i and j, with $0 \leq i < j \leq k$.

(b) Show that you can choose $y = w[i+1] w[i+1] \cdots w[j]$.

(c) Construct a DFA to solve $\{0^{\bullet 2n} 1^{\bullet 2m+1} \mid n, m \geq 0\}$.

$\qquad$ (i) How many states did you need? $\qquad$ (ii) Give a string in the language that can be pumped. Show how.

(d) Can any string in a finite language be pumped? Does this contradict the Pumping Lemma?

Problem 24.57. Prove these languages are not regular. *[Hint: Problem 24.56. Find a string that can't be pumped.]*

(a) $\mathcal{L} = \{0^{\bullet n} 1^{\bullet n} \mid n \geq 0\}$. $\qquad$ (b) $\mathcal{L} = \{$balanced strings$\}$. $\qquad$ (c) $\mathcal{L} = \{$palindromes$\}$.

Problem 24.58. Prove: A DFA for a *finite* language with a string of length ℓ has more than ℓ states. *[Hint: Pump.]*

Problem 24.59 (Punctuation). Let $\mathcal{L}_1 \# \mathcal{L}_2 = \{w_1 \# w_2 \mid w_1 \in \mathcal{L}_1, w_2 \in \mathcal{L}_2\}$. The punctuation symbol # is not in any strings of $\mathcal{L}_1$ or $\mathcal{L}_2$. If $\mathcal{L}_1$ and $\mathcal{L}_2$ are regular, show that $\mathcal{L}_1 \# \mathcal{L}_2$ is regular. Why is concatenation with punctuation easier than without?

Problem 24.60. Give a high-level d-PDA for $\mathcal{L}_{\text{balanced}} = \{$strings with an equal number of 0's and 1's$\}$.

Problem 24.61. Give a high-level d-PDA for each problem. If it can't be done, give the intuition for why. The punctuation symbol # is used to make some languages "easier".

(a) $\mathcal{L}_{\text{geq}} = \{0^{\bullet n} 1^{\bullet k} \mid n \geq 0, k \geq n\}$. $\quad$ (f) $\mathcal{L}_{2^n} = \{0^{\bullet 2^n} \mid n \geq 0\}$. $\qquad$ (f) $\mathcal{L}_{\text{punc-rep}} = \{w \# w \mid w \in \{0, 1\}^*\}$.

(b) $\mathcal{L}_{\times 3} = \{0^{\bullet n} 1^{\bullet 3n} \mid n \geq 0\}$. $\qquad$ (g) $\mathcal{L}_{n^2} = \{0^{\bullet n^2} \mid n \geq 0\}$. $\qquad$ (g) $\mathcal{L}_{\text{even-pal}} = \{w w^{\text{R}} \mid w \in \{0, 1\}^*\}$.

(c) $\mathcal{L}_{+4} = \{0^{\bullet n} 1^{\bullet n+4} \mid n \geq 0\}$. $\qquad$ (h) $\mathcal{L}_{\text{punc-pal}} = \{w \# w^{\text{R}} \mid w \in \{0, 1\}^*\}$. $\quad$ (h) $\mathcal{L}_{\text{even-rep}} = \{w w \mid w \in \{0, 1\}^*\}$.

Problem 24.62. A nondeterministic automaton accepts if one possible final state is $\boxed{\text{YES}}$. Strict nondeterminism requires all possible final states to be $\boxed{\text{YES}}$. Show that strict-nondeterministic automata solve regular languages.

Problem 24.63 (Nondeterministic PDA). Nondeterminism allows an automaton to pursue multiple paths. This effectively allows the automaton to always "guess" correctly which path to follow to accept a string in the language. Nondeterministic machines can be converted to DFA by tracking the subset of possible states during the computation. What about nondeterministic PDAs? Could a nondeterministic PDA be implemented by a deterministic PDA?

25.4 Problems

Problem 25.1. For each ambiguous sentence, (i) Give the two possible meanings. (ii) Suggest how parse trees can distinguish the two meanings. (English grammar uses punctuation to disambiguate.)
  (a) "I love to cook my family and my dog."   (b) "Having no fork makes eating a lot harder."

Problem 25.2. Give English descriptions for the languages generated by each CFG:
  (a) $S \to S$ (b) $S \to \epsilon \mid 0S \mid 1S1S$ (c) $S \to \varepsilon \mid 0 \mid 1 \mid SS$ (d) $S \to A00A$ (e) $S \to 0S1 \mid 1A \mid A0$
                                                                   $A \to \varepsilon \mid 0 \mid 1 \mid AA$ $A \to \varepsilon \mid 0A \mid 1A$

Problem 25.3. Use the descriptions of each language in Problem 25.2 to give a CFG for the complement language.

Problem 25.4. Rewrite the CFG on the right with all production rules for a variable on one line. $S \to 00S1$
  (a) Give a string in this CFL with length longer than 5 and give a string *not* in this CFL. $S \to 01$
  (b) Describe the language in words. $S \to \varepsilon$
  (c) Give a Chomsky Normal Form for the grammar (see also Exercise 25.7).

Problem 25.5. Give a Chomsky Normal Form for each grammar in Problem 25.2 (see also Exercise 25.7).

Problem 25.6. Give a parse tree and derivation of 001011001 for CFG $S \to 0S \mid 1S1S \mid \epsilon$. What is the language?

Problem 25.7. Give a DFA and CFG for each problem. (a) $\{01^{\bullet n} \mid n \geq 0\}$ (b) $\{0^{\bullet n}1^{\bullet n} \mid n \leq 5\}$ (c) $*1$.

Problem 25.8. Find a CFG for each language.
  (a) $\{0^{\bullet n}1^{\bullet n+k} \mid n, k \geq 0\}$.
  (b) Strings of the form $0^{\bullet 3n}$ for $n \geq 0$.
  (c) Strings of the form $0^{\bullet n}1^{\bullet 3n+1}$ for $n \geq 0$.
  (d) Strings with an even number of 1's.
  (e) Strings with at least three 1s.
  (f) Strings with more 0s than 1s.
  (g) Strings *not* of the form $0^{\bullet n}1^{\bullet n}$.
  (h) Strings with twice as many 0s as 1s.
  (i) $\{0^{\bullet m}1^{\bullet n} \mid m \neq n\}$.
  (j) $\{0^{\bullet n} \mid n$ is *not* a multiple of 3$\}$.
  (k) $\{0^{\bullet n}1^{\bullet m} \mid 0 \leq n \leq m \leq 2n\}$.

  (l) $\{0^{\bullet m}1^{\bullet n} \mid n \neq m$ and $n \neq 3m\}$.
  (m) Strings with a 1 before a 0, that is $*1 * 0*$.
  (n) Strings with an odd number of bits and middle bit 0.
  (o) Strings whose first and last bit are the same.
  (p) $\{0^{\bullet n}1^{\bullet m}0^{\bullet m}1^{\bullet n} \mid n, m \geq 0\} \cup \{0^{\bullet n}1^{\bullet m}0^{\bullet n+m} \mid n, m \geq 0\}$.
  (q) $\{0^{\bullet m}1^{\bullet n}0^{\bullet \ell} \mid m, n, \ell \geq 0$ and $(n \neq m$ OR $n \neq \ell)\}$.
  (r) Strings $w\#v$ where w^{R} is a substring of v.
  (s) All palindromes w where $w = w^{\text{R}}$ (not only of the form ww^{R}).
  (t) Strings which are not palindromes.
  (u) Strings not of the form ww (non-equality).
  (v) Strings in which every prefix has at least as many 0s as 1s.

Problem 25.9. Find a CFG for each language using union and/or concatenation.
  (a) $\{0^{\bullet n}1^{\bullet k}0^{\bullet m} \mid n, m \geq 0$ and $k > n + m\}$.   (c) $\{0^{\bullet n}1^{\bullet k}0^{\bullet m} \mid n, m \geq 0$ and $k > n + 1\}$.
  (b) $\overline{\{0^{\bullet n}1^{\bullet n}0^{\bullet n} \mid n \geq 0\}}$.   (d) Strings with an unequal number of 0s and 1s.

Problem 25.10. Give a CFG to generate the reversal of strings in the CFG: $S \to 00S1 \mid 1S0 \mid \epsilon$.

Problem 25.11. Suppose $\mathcal{L}_1$ and $\mathcal{L}_2$ are context free. Show that these languages are context free.
  (a) $\mathcal{L}_1 \cup \mathcal{L}_2$ (union)   (b) $L_1 \bullet \mathcal{L}_2$ (concatenation)   (c) $\mathcal{L}_1^*$ (Kleene star)   (d) $\mathcal{L}^{\text{R}} = \{w^{\text{R}} \mid w \in \mathcal{L}\}$ (reversal).
[Hint: For reversal, reverse the hybrid string on the RHS of production rules and use induction.]

Problem 25.12. Construct a CFG for $\mathcal{L} = \{$strings *not* containing 00$\}$ as follows.
  (a) Construct a DFA for $\overline{\mathcal{L}} = \{$strings containing 00$\}$, and use that to find a DFA for $\mathcal{L}$.
  (b) Use the technique in Example 25.2 on page 368 to construct a CFG for $\mathcal{L}$ using your DFA for $\mathcal{L}$.

Problem 25.13. Prove that the CFG in (25.2) on page 369 generates all strings whose number of ones $\equiv 1 \pmod 3$.

Problem 25.14. Prove that the CFG $S \to \# \mid 0S0 \mid 1S1$ generates all strings of the form $w\#w^{\text{R}}$.

Problem 25.15. Prove by induction on string length that the CFG's in (25.3) and (25.5) generate the same strings.

Problem 25.16. For each language $\mathcal{L}$, (i) Give a CFG that generates $\mathcal{L}$. (ii) Prove by induction that your CFG generates only strings in $\mathcal{L}$. (iii) Prove by induction that every string in $\mathcal{L}$ can be generated by your CFG.
  (a) $\mathcal{L} = \{$strings with an odd number of 1s$\}$ (c) $\mathcal{L} = \{$strings with *more* 1s than 0s$\}$
  (b) $\mathcal{L} = \{$strings with equal number of 0s and 1s$\}$.   (d) $\mathcal{L} = \{$strings with *more* 1s than 0s in every prefix$\}$

Problem 25.17. Consider the language $\mathcal{L} = \{\epsilon, 1, 11, 111, \ldots\} = \{1\}^*$.

(a) Show that the CFG $S \to \varepsilon \mid 1S$ generates $\mathcal{L}$. Give a derivation of 111.

(b) Show that the CFG $S \to \varepsilon \mid 1 \mid SS$ generates $\mathcal{L}$. Give two *different* derivations of 111.

(c) A *left* (*right*) derivation replaces the leftmost (rightmost) variable at every step. For the grammar in part (b), give left and right derivations of 111.

Problem 25.18. Problem 25.17(c) defines left and right derivations. For the CFG shown, give parse trees for left and right derivations of: (a) 00101   (b) 1001   (c) 00011.

1: $S \to A1B$
2: $A \to \varepsilon \mid 0A$
3: $B \to \varepsilon \mid 0B \mid 1B$

Problem 25.19. Find a CFG for each language.

(a) $\mathcal{L}_1 = \{0^{\bullet n} 1^{\bullet n} 0^{\bullet m} 1^{\bullet m} \mid n, m \geq 1\}$.   (b) $\mathcal{L}_2 = \{0^{\bullet n} 1^{\bullet m} 0^{\bullet m} 1^{\bullet n} \mid n, m \geq 1\}$.   (c) $\mathcal{L}_1 \cup \mathcal{L}_2$ and $\mathcal{L}_1 \bullet \mathcal{L}_2$.

Problem 25.20. Using your CFG for $\mathcal{L}_1 \cup \mathcal{L}_2$ in Problem 25.19(c), give two different left derivations of 00110011 and their (different) parse trees. (Your grammar is ambiguous. In fact, every grammar for this language is ambiguous.)

Problem 25.21. For CFG $S \to 0S \mid S1 \mid 0 \mid 1$, prove no string has 10 as a substring. *[Hint: Induction on length.]*

Problem 25.22. What is wrong with this proof that $0^{\bullet n} 1^{\bullet 2n} 0^{\bullet n}$ is a CFL. Let $\mathcal{L}_1 = 0^{\bullet n} 1^{\bullet n}$ and $\mathcal{L}_2 = 1^{\bullet n} 0^{\bullet n}$, both of which are CFL's. Since CFLs are closed under concatenation, $\mathcal{L}_1 \bullet \mathcal{L}_2 = 0^{\bullet n} 1^{\bullet n} 1^{\bullet n} 0^{\bullet n} = 0^{\bullet n} 1^{\bullet 2n} 0^{\bullet n}$ is a CFL.

Problem 25.23. (a) Show how a d-PDA can solve $\mathcal{L} = \{0^{\bullet n} 1^{\bullet n+m} 0^{\bullet m} \mid n, m \geq 0\}$.   (b) Find a CFG for $\mathcal{L}$.

Problem 25.24. In each case explain intuitively why a d-PDA cannot solve $\mathcal{L}$ and find a CFG for $\mathcal{L}$.

(a) $\mathcal{L} = \{0^{\bullet m} 1^{\bullet n} 0^{\bullet k} \mid n = m \text{ or } n = k\}$.   (b) $\mathcal{L} = \{w \mid w\text{'s second half has a } 1\} = \{xy \mid |x| \geq |y|, \ y \text{ has a } 1\}$.

Problem 25.25. Show that every regular language has a *right-linear* CFG, where every production rule has the form

$$A \to x \qquad \text{or} \qquad A \to xB \qquad (x \text{ is a string of terminals}).$$

The variables are replaced with strings having at most one variable that is at the rightmost end. *[Hint: Example 25.2.]* (The converse is also true, every right linear CFG generates a regular language.)

Problem 25.26. Suppose a language $\mathcal{L}_1$ is solved by a d-PDA and $\mathcal{L}_2$ is solved by a DFA. Use product states to prove that $\mathcal{L}_1 \cap \mathcal{L}_2$ is a CFL. (More generally, a CFL intersected with a regular language is a CFL.)

Problem 25.27. The CFG on the right generates the language $\mathcal{L}$. Prove that:

(a) $\mathcal{L} = \{\text{strings with an odd number of 0's}\}$.

(b) $\mathcal{L}$ is regular. (Ginsburg-Rice, 1962: CFLs on unary alphabets are regular.)

1: $S \to 0 \mid 0A$
2: $A \to 0S$

Problem 25.28 (Pumping). The CFG from Pop Quiz 25.1 is on the right, see also Exercise 25.7. There are 5 variables. The start variable S is not on the RHS of any rule. All rules have the form $A \to BC$ or $A \to t$, where A, B, C are variables and t a terminal. All derivations of a non-empty string of length ℓ have $2\ell - 1$ steps.

1: $S \to \varepsilon \mid T_0 T_1 \mid T_0 A$
2: $X \to T_0 T_1 \mid T_0 A$
3: $A \to X T_1$
4: $T_0 \to 0$
5: $T_1 \to 1$

(a) Give the parse tree for $w = 000111$. Remove all leaves (terminals) to get a binary tree whose vertices are variables. The root is Ⓢ. Explain why this binary tree is full (vertices have 0 or 2 children).

(b) There is a path in the parse tree from Ⓢ to a terminal-leaf in which the variable A appears twice. How many variables are in this path other than Ⓢ? We illustrate the situation on the right. Since $S \overset{*}{\Rightarrow} w$, the leaves of the tree rooted at S form w. We decomposed w as $w = axbyc$, where first-$A \overset{*}{\Rightarrow} xby$ and second-$A \overset{*}{\Rightarrow} b$. That is, the leaves of the subtree rooted at the first A form xby and the leaves of the subtree rooted at the second A form b. Determine a, x, b, y, c (one or more can be ε).
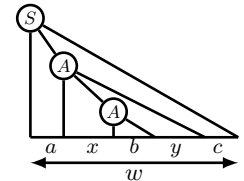
(c) Repeating a variable on a path from S to a terminal leaf is similar to a DFA looping back to the same state as it processes a string. Replace the subtree rooted at the second A with the subtree rooted at the first A to get the valid parse tree/derivation on the right.
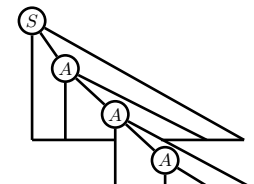
   (i) What is the string whose parse tree is on the right (in terms of a, x, b, y, c)?

   (ii) In (b), can you replace the subtree rooted at the first A with the subtree rooted at the second A? What string is derived? Why can't both x and y be empty?

   (iii) Prove that $ax^{\bullet i} by^{\bullet i} c$ can be generated for $i \geq 0$. (w can be *pumped*.)

Problem 25.29 (Pumping Lemma). Generalize Problem 25.28. For any CFG in Chomsky Normal Form, prove:

> **Pumping Lemma.** For any CFL, there is a parameter p, the pumping length, such that if w is in the language and has length $\ell \geq p$, then w can be decomposed into $w = axbyc$ such that
> (i) $\text{length}(xby) < p$;   (ii) x and y are not both ε;   (iii) $ax^{\bullet i}by^{\bullet i}c$ is in the language for $i \geq 0$.

Let S be the start variable and assume there are k additional variables. Recall, from Exercise 25.7: Only S can transition to ε, and S is not on the RHS of any rule. All rules are of the form $A \to BC$ or $A \to t$, where A, B, C are variables and t a terminal. All derivations of a non-empty string of length ℓ have $2\ell - 1$ steps.

(a) Let w be a string of length ℓ. The leaves in the parse tree are terminals each produced by a transition of a variable directly to a terminal. Remove these terminal-leaves. What remains is a binary tree of variables. Suppose $\ell > 2^k$.
   (i) Show that some path p from the root $\circledS$ to a leaf x in the remaining tree has length at least $k + 1$
   (ii) Start at x and move up toward S until a variable (say) A is repeated. Show that at most k steps are made.
   (iii) Show that the substring in w derived from the (repeated) variable from (ii) has length at most 2^k.
   (iv) Prove that w can be decomposed as $w = axbyc$ with $\text{length}(xby) \leq 2^k$ and not both x, y being ε such that $ax^{\bullet i}by^{\bullet i}c$ can be generated by the CFG for $i \geq 0$. Hence, prove the pumping lemma.

(b) Use the pumping lemma to prove that $\mathcal{L} = \{0^{\bullet n}1^{\bullet n}0^{\bullet n} \mid n \geq 0\}$ is not context free. Use these steps as a guide.
   (i) Let p be the pumping length and $w = 0^{\bullet p+1}1^{\bullet p+1}0^{\bullet p+1}$. Why are the only possibilities for xby: entirely in the left 0s; overlapping left 0s and 1s; entirely in the 1s; overlapping 1s and right 0s; entirely in the right 0s.
   (ii) Consider each case in (i) and show that w cannot be pumped, contradicting the pumping lemma.

Problem 25.30. Use the pumping lemma to show that these languages are not CFL's. Assume $k, m, n \in \mathbb{N}$.

(a) $\{0^{\bullet n}1^{\bullet m}0^{\bullet k} \mid n \leq m \leq k\}$.
(b) (i) $\{0^{\bullet m}1^{\bullet n} \mid m = kn\}$ (ii) $\{0^{\bullet m}1^{\bullet n} \mid m \neq kn\}$.
(c) (i) $\{0^{\bullet n^2}\}$ (ii) $\{0^{\bullet n}1^{\bullet n^2}\}$.
(d) Balanced palindromes.
(e) (i) $\{ww \mid w \in \{0,1\}^*\}$ (ii) $\{w\#w \mid w \in \{0,1\}^*\}$.
(f) (i) $\{0^{\bullet n}1^{\bullet 2^n}\}$ (ii) $\{0^{\bullet 2^n} \mid n \geq 0\}$.

Problem 25.31. Prove that a CFG generates an infinite language if and only if it generates some string whose length satisfies $p \leq \text{length}(w) \leq 2p$, where p is the pumping length from Problem 25.29.

Problem 25.32. Suppose a CFG generates a unary language $\mathcal{L}$, $\mathcal{L} \subseteq \{1\}^*$. Let p be the pumping length from Problem 25.29. Prove that if $1^{\bullet 0}, 1^{\bullet 1}, \ldots, 1^{\bullet p+p!}$ are all in $\mathcal{L}$, then $\mathcal{L} = \{1\}^*$. Follow these steps.

(a) For $p \leq k$, if $1^{\bullet k} \in \mathcal{L}$, use the pumping lemma to show that $1^{\bullet k+n\alpha} \in \mathcal{L}$ for some $1 \leq \alpha < p$ and $n \geq 0$.
(b) Using $\{np! \mid n \geq 0\} \subset \{n\alpha \mid n \geq 0\}$, show that $1^{\bullet k+np!} \in \mathcal{L}$ for $p \leq k \leq p!$ and $n \geq 0$. Hence, prove the claim.

Problem 25.33. In each case $\mathcal{L}_1$ and $\mathcal{L}_2$ look similar. Give a CFG for $\mathcal{L}_1$ and prove that $\mathcal{L}_2$ is not a CFL.

(a) $\mathcal{L}_1 = \{(01)^{\bullet n}(01)^{\bullet n} \mid n \geq 0\}$, $\mathcal{L}_2 = \{0^{\bullet n}1^{\bullet n}0^{\bullet n}1^{\bullet n} \mid n \geq 0\}$.
(b) $\mathcal{L}_1 = \{0^{\bullet n}0^{\bullet 2n}0^{\bullet 3n} \mid n \geq 0\}$, $\mathcal{L}_2 = \{0^{\bullet n}\#0^{\bullet 2n}\#0^{\bullet 3n} \mid n \geq 0\}$.
(c) $\mathcal{L}_1 = \{ww^{\text{R}}\}$, $\mathcal{L}_2 = \{wxw^{\text{R}} \mid \text{length}(w) = \text{length}(x)\}$.
(d) $\mathcal{L}_1 = \{\text{strings } w\#v \text{ where } w^{\text{R}} \text{ is a substring of } v\}$, $\mathcal{L}_2 = \{\text{strings } w\#v \text{ where } w \text{ is a substring of } v\}$.
(e) $\mathcal{L}_1 = \{w \mid w\text{'s mid-third has a } 1\} = \{xyz \mid |x| = |z| \geq |y|, \ y \text{ has a } 1\}$, $\mathcal{L}_2 = \{w \mid w\text{'s mid-third has two } 1\text{s}\}$.

Problem 25.34. Prove that if a d-PDA accepts $\mathcal{L}$, then there is a CFG that generates $\mathcal{L}$.

Problem 25.35 (Context sensitive grammar). In each production rule of grammars I and II below, an instance of the string on the LHS can be replaced by the string on the RHS.

For each grammar:
(a) Give derivations of three different strings.
(b) Guess the problem solved by the grammar.
(c) Informally justify your guess.
(d) Is there a contradiction with any claims in Section 25.3 on page 373?

Grammar I	Grammar II
1: $S \to \varepsilon \mid 0SBC$	1: $S \to A0B$
2: $CB \to BC$	2: $A \to \varepsilon \mid AD$
3: $0B \to 0X$	3: $D0 \to 00D$
4: $XB \to XX$	4: $DB \to B$
5: $XC \to XY$	5: $B \to \varepsilon$
6: $YC \to YY$	
7: $X \to 1$	
8: $Y \to 0$	
Variables: S, B, C, X, Y.	Variables: S, A, B, D.

26.4 Problems

Problem 26.1. Order these sets of languages using the subset relation:

DFA = {languages solved by DFA}   CFG = {languages solved by CFG}   TM = {languages solved by TM}

Problem 26.2. What is the difference between a recognizer and a decider? Which is an algorithm? Why?

Problem 26.3. Give machine-code of a Turing Machine for the language $*01$. Zig-zagging over the tape is common behavior for a Turing Machine. How many times does your machine need to scan over the tape. Informally explain why.

Problem 26.4. Find the $\boxed{\text{YES}}$-sets of Turing Machines M_1 and M_2. Which Turing Machine do you prefer and why?

Problem 26.5. In each case: (i) Give pseudocode of a Turing Machine for the problem. (ii) Give machine-code for each module in your pseudocode. (iii) Combine your modules to get machine-code of a Turing Machine for the problem.

(a) $\mathcal{L} = \{0^{\bullet n}|n \geq 0\}$ (only zeros).
(b) $\mathcal{L} = \{0^{\bullet n}1^{\bullet n}|n \geq 0\}$ (testing equality).
(c) $\mathcal{L} = \{0^{\bullet 2n}|n \geq 0\}$ (parity-check).
(d) $\mathcal{L} = \{0^{\bullet 2^n} \mid n \geq 0\}$ (exponentials).
(e) $\mathcal{L} = \{$palindromes $w = w^{\text{R}}\}$

(f) $\mathcal{L} = \{$balanced strings with an equal number of 0s and 1s$\}$.
(g) $\mathcal{L} = \{$strings with number of 0s $= 2 \times$ number of 1s$\}$.
(h) $\mathcal{L} = \{$strings with number of 0s $\neq 2 \times$ number of 1s$\}$.
(i) $\mathcal{L} = \{0^{\bullet i}\#1^{\bullet j}\#0^{\bullet k} \mid i, j > 0$ and $k = i + j\}$ (addition).
(j) $\mathcal{L} = \{w_1\#w_2\#\cdots\#w_\ell \mid w_i \neq w_j$ for $i \neq j\}$ (distinct strings).

Problem 26.6. In each case, give high level pseudocode for a Turing Machine M for the problem.

(a) Regular languages: (i) $\mathcal{L}_1 = \{*01*\}$ (ii) $\mathcal{L}_2 = \{*01\}$.
(b) Not CFL: $\mathcal{L} = \{0^{\bullet n}\#1^{\bullet n}\#0^{\bullet n}\}$ (# is punctuation).
(c) Squaring: $\mathcal{L} = \{0^{\bullet n}\#1^{\bullet n^2}, n \geq 0\}$ (# is punctuation).
(d) Exponential: $\mathcal{L} = \{0^{\bullet n}\#1^{\bullet 2^n}, n \geq 0\}$ (# is punctuation).

(e) Repetition: $\mathcal{L} = \{ww|w \in \{0, 1\}^*\}$.
(f) Palindromes: $\mathcal{L} = \{w|w \in \{0, 1\}^*, w = w^{\text{R}}\}$.
(g) Add Two: $\mathcal{L} = \{0^{\bullet n}1^{\bullet n+2}\}$.
(h) Inequality: $\mathcal{L} = \{0^{\bullet m}1^{\bullet n} \mid n \geq m^2\}$.

Problem 26.7. Which of DFA, CFG or TM can solve (a) $\{0^{\bullet n}1^{\bullet 2n} \mid n \geq 0\}$ (b) $\{0^{\bullet n} \mid n$ is prime$\}$? (Explain.)

Problem 26.8. Can a Turing Machine solve the problems $\{0^{\bullet n}\#0^{\bullet n^2} \mid n \geq 0\}$ and $\{0^{\bullet n^2} \mid n \geq 0\}$? (Show how.)

Problem 26.9. In each case, give high level pseudocode for a transducer Turing Machine M for the problem.

(a) Add Two: The input is $0^{\bullet n}$ and M halts with $0^{\bullet n+2}$ on the tape.
(b) Multiplication by 2: The input is $0^{\bullet n}$ and M halts with $0^{\bullet 2n}$ on the tape.
(c) Squaring: The input is $0^{\bullet n}$ and M halts with $0^{\bullet n^2}$ on the tape.
(d) Exponentiate: The input is $0^{\bullet n}$ and M halts with $0^{\bullet 2^n}$ on the tape.
(e) Copying: The input is w and M halts with ww on the tape.
(f) Reversal: The input is w and M halts with w^{R} on the tape.
(g) Switching: The input is $w\#v$ and M halts with $v\#w$ on the tape.
(h) Delete first: The input is xw where $x \in \Sigma$ and $w \in \Sigma^*$, and M halts with w on the tape.
(i) Prefixing: The input is $w \in \Sigma^*$ and M halts with $0w$ on the tape.
(j) Binary to unary: The input w is the binary representation of n and M halts with $0^{\bullet n}$ on the tape.
(k) Unary to binary: The input is $0^{\bullet n}$ and M halts with binary representation of n on the tape. .
(l) Binary addition: The input is $w_1\#w_2$, two binary strings and M halts with $w_1 + w_2$ (binary addition) on the tape.
(m) Division: The input is $0^{\bullet n}$. M rejects if n is odd. If n is even, M accepts with $0^{\bullet n/2}$ on the tape.

Problem 26.10. LR-Turing Machines move left or right. LRS-Turing Machines may also stay put. Prove that LR and LRS-Turing Machines solve the same problems (LRS-decidable languages are LR-decidable). *[Hint: S = LR.]*

Problem 26.11. True or false? (a) $\mathcal{L}$ is decidable $\rightarrow \overline{\mathcal{L}}$ be decidable.   (b) $\mathcal{L}$ is recognizable $\rightarrow \overline{\mathcal{L}}$ is recognizable.

Problem 26.12. If the input of a Turing Machine is write-protected, prove that it can't decide $\{0^{\bullet n}1^{\bullet n} \mid n \geq 0\}$. (Such TMs solve only regular languages. The proof relies on the Myhill-Nerode Theorem, Problem 24.55.)

27.5 Problems

Problem 27.1. Answer YES or NO and explain your reasoning. "Is the correct answer to Problem 27.1 'NO'?"

Problem 27.2. A collection of sets $\mathcal{C}$ is closed under union and complement. Prove that $\mathcal{C}$ is closed under intersection. If $\mathcal{C}$ were closed under union and intersection, is it necessarily closed under complement?

Problem 27.3. Given an ultimate-debugger which takes $\langle M \rangle \# w$ and decides if TM M halts on input w, show that every recognizer of a language $\mathcal{L}$ can be converted into a decider for the language.

Problem 27.4. Given an untimate-debugger that determines if a program halts, show how to resolve each conjecture.
  (a) Goldbach's conjecture that every even number greater than 2 is a sum of two primes.
  (b) The twin primes conjecture that n and $n+2$ are prime for infinitely many n.
  (c) The Collatz $(3n+1)$ conjecture in Problem 1.45 on page 14.
[Hint: If necessary, you can use the ultimate-debugger on a program which itself uses the ultimate-debugger.]

Problem 27.5. Identify which of DFA, CFG or Turing Machine can solve each problem.
  (a) $\mathcal{L} = \{\text{programs that HALT}\}$ (b) $\mathcal{L} = \{\text{strings with an even number of 1s}\}$ (c) $\mathcal{L} = \{0^{\bullet n} \# 0^{\bullet n^2}, n \geq 0\}$.

Problem 27.6. For $p \geq 0$, define the language $\mathcal{L}_p = \{w \mid \text{length}(w) < p\}$. For what p is $\mathcal{L}_p$ decidable?

Problem 27.7. Define a strange language, $\mathcal{L} = \{w \mid \text{length}(w) < \text{mass of Universe in lbs}\}$. Is $\mathcal{L}$ decidable?

Problem 27.8 (Hilbert's 10th Problem). A polynomial $p(x; \mathbf{a}) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n$, where $a_i \in \mathbb{Q}$. One must decide if $p(x; \mathbf{a})$ has an integral root, that is $p(x_*; \mathbf{a}) = 0$ for an integer $x_* \in \mathbb{Z}$. Define the language

$$\mathcal{L}_{\text{root}} = \{\langle \mathbf{a} \rangle \mid n \geq 1, \ p(x; \mathbf{a}) \text{ has an integral root}\}.$$

Prove that $\mathcal{L}_{\text{root}}$ is decidable. *[Hint: Show that any root satisfies $|x_*| < (n+1) \max_i |a_i|$. Matiyasevich's Theorem implies no such bound is possible for the multivariate version of Hilbert's 10th problem, which is only recognizable.]*

Problem 27.9. Prove that any regular language is TM-decidable. *[Hint: Encode a DFA in a sketch of a TM.]*

Problem 27.10. Prove that any CFL is TM-decidable. *[Hint: Encode a CFG in a sketch of a TM and use Exercise 25.7]*

(Problems 27.9 and 27.10 prove the set inclusions on page 395 that DFA $\subset$ CFG $\subset$ TM.)

Problem 27.11. Show that one can encode a TM in unary, using only 0's. Specifically, sketch a TM that takes a "regular" encoding of a TM as in Section 26.3 and produces the unary encoding. *[Hint: TMs are countable.]*

Problem 27.12. Sketch a universal TM to simulate a TM M on input w from a unary encoding of M (Problem 27.11).

Problem 27.13 (Program Translation). Given a TM M in some encoding $\langle M \rangle_1$, the task is to "translate" it into another encoding $\langle M \rangle_2$. Do you think this problem is solvable by an algorithm?

Problem 27.14 (Enumerators). Generating the strings of a language is useful. A language $\mathcal{L}$ is *enumerable* if some Turing Machine M_{E} sequetially generates all the strings of $\mathcal{L}$, with possible repetition. Envision M_{E} being hooked up to a printer (a second tape). Every now and again, M_{E} prints out a string. Every printed string must be in $\mathcal{L}$ and eventually, every string in L must be printed. So, M_{E} outputs strings $s_1, s_2, \ldots$ where $s_i \in \mathcal{L}$. Further, if $w \in \mathcal{L}$, then for some i, $s_i = w$. You can stop M_{E} after it has printed i strings and perform operations on the strings $s_1, \ldots, s_i$.
  (a) Sketch a recognizer M_{R} for $\mathcal{L}$ given an enumerator M_{E}.
  (b) Sketch an enumerator M_{E} for $\mathcal{L}$ given a recognizer M_{R}. Be careful. *[Hint: Let $\Sigma^* = \{w_1, w_2, \ldots\}$. Simulate M_{R} on each of $w_1, \ldots, w_i$ for i steps.]*
  (c) Prove that a language is enumerable if and only if it is recognizable.
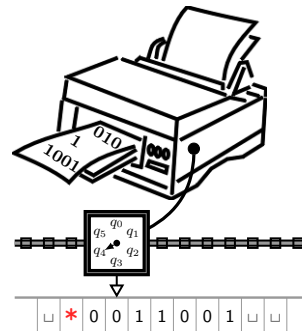
Problem 27.15. The binary strings in lexicographic order are $\Sigma^* = \{\varepsilon, 0, 1, 00, 01, 10, 11, 000, \ldots\}$. Shorter strings appear first and strings of the same length appear in order of increasing value. Prove that a language $\mathcal{L}$ is decidable if and only if there is an enumerator for $\mathcal{L}$ which prints the strings in lexicographic order.

Problem 27.16. Prove: an infinite recognizable language has an infinite decidable subset. *[Hint: 27.14 & 27.15.]*

Problem 27.17. $\mathcal{L}_{\text{TM}}$ is undecidable. You suspect $\mathcal{L}$ is unsolvable by an algorithm. Explain how to prove it.

Problem 27.18. Do you think $\mathcal{L}_{\text{HALT}} \leq_{\text{R}} \mathcal{L}_{\text{TM}}$? Explain your intuition and then give a proof.

Problem 27.19. Intuitively explain the difficulty in constructing a recognizer for the language $\mathcal{L}_{\text{TM-reject}}$, where

$$\mathcal{L}_{\text{TM-reject}} = \{\langle M\rangle\#w \mid M \text{ is a Turing Machine that does not accept } w\}.$$

Prove that $\mathcal{L}_{\text{TM-reject}}$ is non-recognizable. *[Hint: How is $\mathcal{L}_{\text{TM-reject}}$ related to $\overline{\mathcal{L}_{\text{TM}}}$.]*

Problem 27.20. In each case you are given some information and asked to answer a question.
 (a) A is reducible to B and A is undecidable. What can you say about B?
 (b) A is reducible to B and A is decidable. What can you say about B?
 (c) A is reducible to B and B is undecidable. What can you say about A?
 (d) A is reducible to B and B is decidable. What can you say about A?
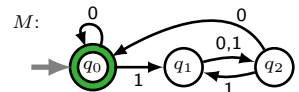
Problem 27.21. Which of the following do you think is decidable? Give your intuition.
 (a) Input: $\langle M\rangle$. Does Turing Machine M accept at least one string?
 (b) Input: $\langle M\rangle$. Does Turing Machine M accept all strings?
 (c) Input: $\langle M\rangle$. Does Turing Machine M accept 011?
 (d) Input: $\langle M_1\rangle\#\langle M_2\rangle$. Does Turing Machine M_1 accept a subset of the strings that Turing Machine M_2 accepts?
 (e) Input: $\langle M\rangle\#w$. Does Turing Machine M run for more than 10^6 steps on input w

> **Definition 27.6.** The languages defined below are based on properties of computing machines.
> (a) $\mathcal{L}_{\text{DFA}} = \{\langle M\rangle\#w \mid M \text{ is a DFA and } M \text{ accepts } w.\}$
> (b) $\mathcal{L}_{\text{CFG}} = \{\langle C\rangle\#w \mid C \text{ is a CFG and } C \text{ generates } w.\}$
> (c) $\mathcal{L}_{\text{TM}} = \{\langle M\rangle\#w \mid M \text{ is a TM and } M \text{ accepts } w.\}$
> (d) $\mathcal{L}_{\text{DFA-00}} = \{\langle M\rangle \mid M \text{ is a DFA and } M \text{ accepts the string 00.}\}$
> (e) $\mathcal{L}_{\text{CFG-00}} = \{\langle C\rangle \mid C \text{ is a CFG and } C \text{ generates the string 00.}\}$
> (f) $\mathcal{L}_{\text{TM-00}} = \{\langle M\rangle \mid M \text{ is a TM and } M \text{ accepts the string 00.}\}$
> (g) $\mathcal{L}_{\text{EMPTY-DFA}} = \{\langle M\rangle \mid M \text{ is a DFA and } M \text{ accepts no strings, } \mathcal{L}(M) = \varnothing.\}$
> (h) $\mathcal{L}_{\text{EMPTY-CFG}} = \{\langle C\rangle \mid C \text{ is a CFG and } C \text{ generates no strings, } \mathcal{L}(C) = \varnothing.\}$
> (i) $\mathcal{L}_{\text{EMPTY-TM}} = \{\langle M\rangle \mid M \text{ is a TM and } M \text{ accepts no strings, } \mathcal{L}(M) = \varnothing.\}$
> (j) $\mathcal{L}_{\text{EQ-DFA}} = \{\langle M_1\rangle\#\langle M_1\rangle \mid M_1, M_2 \text{ are DFAs that accept the same strings, } \mathcal{L}(M_1) = \mathcal{L}(M_2).\}$
> (k) $\mathcal{L}_{\text{EQ-CFG}} = \{\langle C_1\rangle\#\langle C_2\rangle \mid C_1, C_2 \text{ are CFGs that generate the same strings, } \mathcal{L}(C_1) = \mathcal{L}(C_2).\}$
> (l) $\mathcal{L}_{\text{EQ-TM}} = \{\langle M_1\rangle\#\langle M_2\rangle \mid M_1, M_2 \text{ are TMs that accept the same strings, } \mathcal{L}(M_1) = \mathcal{L}(M_2).\}$
> (m) $\mathcal{L}_{\text{ALL-DFA}} = \{\langle M\rangle \mid M \text{ is a DFA that accepts all strings, } \mathcal{L}(M) = \Sigma^*.\}$
> (n) $\mathcal{L}_{\text{ALL-CFG}} = \{\langle C\rangle \mid C \text{ is a CFG that generates all strings, } \mathcal{L}(C) = \Sigma^*.\}$
> (o) $\mathcal{L}_{\text{ALL-TM}} = \{\langle M\rangle \mid M \text{ is a TM that accepts all strings, } \mathcal{L}(M) = \Sigma^*.\}$
> (p) $\mathcal{L}_{\text{FINITE-DFA}} = \{\langle M\rangle \mid M \text{ is a DFA that accepts a finite language, } \mathcal{L}(M) \text{ is finite.}\}$
> (q) $\mathcal{L}_{\text{FINITE-CFG}} = \{\langle C\rangle \mid C \text{ is a CFG that generates a finite language, } \mathcal{L}(C) \text{ is finite.}\}$
> (r) $\mathcal{L}_{\text{FINITE-TM}} = \{\langle M\rangle \mid M \text{ is a TM that accepts a finite language, } \mathcal{L}(M) \text{ is finite.}\}$

Problem 27.22. Answer these questions for the DFA M on the right.
 (a) Explain how to get an encoding for the DFA, $\langle M\rangle$.
 (b) Is $\langle M\rangle\#011 \in \mathcal{L}_{\text{DFA}}$? Does it depend on your encoding $\langle M\rangle$?
 (c) Are $\langle M\rangle$ and/or $\langle M\rangle\#\langle M\rangle$ in these languages? Does it depend on your encoding $\langle M\rangle$?
        (i) $\mathcal{L}_{\text{DFA}}$ (ii) $\mathcal{L}_{\text{DFA-00}}$ (iii) $\mathcal{L}_{\text{EMPTY-DFA}}$ (iv) $\mathcal{L}_{\text{EQ-DFA}}$ (v) $\mathcal{L}_{\text{ALL-DFA}}$ (vi) $\mathcal{L}_{\text{FINITE-DFA}}$ (vii) $\mathcal{L}_{\text{TM-00}}$

Problem 27.23. Guess if each problem in Definition 27.6 is decidable, recognizable or neither. Give your intuition.

Problem 27.24. Prove that $\mathcal{L}_{\text{DFA}}$ is decidable by giving a sketch of a TM-decider. Is $\mathcal{L}_{\text{DFA-00}}$ decidable?

Problem 27.25. Sketch a TM which can decide if a (YES) state is reachable from the start state of a DFA. Hence, prove that $\mathcal{L}_{\text{EMPTY-DFA}}$ is decidable? *[Hint: Traverse the state diagram of a DFA, which is a directed multigraph.]*

Problem 27.26. Use a decider for $\mathcal{L}_{\text{EMPTY-DFA}}$ to sketch a TM that decides if the language of one DFA is a subset of the language of another DFA. *[Hints: $\mathcal{L}_1 \subseteq \mathcal{L}_2$ iff $\overline{\mathcal{L}_1} \cap L_2 = \varnothing$. Regular languages are closed under set operations.]*

Problem 27.27. Use Problems 27.25 and 27.26 to prove that $\mathcal{L}_{\text{EQ-DFA}}$ is decidable by sketching a TM for $\mathcal{L}_{\text{EQ-DFA}}$.

Problem 27.28. Use Problem 27.25 to prove that $\mathcal{L}_{\text{ALL-DFA}}$ is decidable by sketching a TM for $\mathcal{L}_{\text{ALL-DFA}}$.

Problem 27.29. Prove that $\mathcal{L}_{\text{FINITE-DFA}}$ is decidable by sketching a TM for $\mathcal{L}_{\text{FINITE-DFA}}$. *[Hint: Problem 24.37.]*

Problem 27.30. Prove that $\mathcal{L}_{\text{CFG}}$ is decidable. Is $\mathcal{L}_{\text{CFG-00}}$ decidable? *[Hint: Chomsky Normal Form, Exercise 25.7.]*

Problem 27.31. Prove that $\mathcal{L}_{\text{EMPTY-CFG}}$ is decidable. *[Hint: Work "backwards". Mark all terminals. Repeat: Mark a variable on the left of a production rule if the string produced on the right of the rule has only marked variables.]*

Problem 27.32. By Problem 27.31, one can decide if a CFG generates no strings. Build a decider for $\mathcal{L}_{\text{ALL-CFG}}$ as follows. Given a CFG C for $\mathcal{L}$, construct a CFG $\overline{C}$ for $\overline{L}$ and decide if $\overline{C}$ generates no strings using Problem 27.31. What is wrong with this proof that $\mathcal{L}_{\text{ALL-CFG}}$ is decidable? (Unlike $\mathcal{L}_{\text{ALL-DFA}}$ & $\mathcal{L}_{\text{EQ-DFA}}$, $\mathcal{L}_{\text{ALL-CFG}}$ & $\mathcal{L}_{\text{EQ-CFG}}$ are undecidable.)

Problem 27.33. Sketch a recognizer for $\overline{\mathcal{L}_{\text{EQ-CFG}}}$. What is the difficulty with recognizing $\mathcal{L}_{\text{EQ-CFG}}$?

Problem 27.34. Prove that $\mathcal{L}_{\text{FINITE-CFG}}$ is decidable. *[Hint: Problems 25.29 and 27.30.]*

Problem 27.35. Show that each problem is solvable. *[Hint: Closure for regular languages. Problems 27.25-27.31.]*
  (a) Determine if a DFA accepts no string with an odd number of 1's.
  (b) Determine if a DFA accepts all strings with an odd number of 1's.
  (c) Determine if a DFA accepts w^{R}, the reversal of w, whenever it accepts w.
  (d) Determine if a DFA, for some string w, accepts both w as well as the reversal w^{R}.

Problem 27.36. Show that each problem is solvable. You may find Problem 25.26 useful.
  (a) Determine if a DFA accepts some string of the form $0^{\bullet n}1^{\bullet n}$.
  (b) Determine if a DFA accepts some balanced string with an equal number of 1's and 0's.
  (c) Determine if a DFA accepts some string with more 1's than 0's.

Problem 27.37. Show that each problem is solvable. You may assume a generalization of Problem 25.26, that the intersection of a CFL with a regular language is context free. Problem 27.31 may be useful.
  (a) Determine if a DFA accepts some string which is a palindrome.
  (b) Determine if a CFG generates some string whose length is not a multiple of 3.
  (c) Determine if a CFG generates some string in $\{1\}^*$.
  (d) Determine if a CFG generates all strings in $\{1\}^*$. *[Hint: Problem 25.32.]*

Problem 27.38. Suppose that $A_{\text{TM-00}}$ is a decider for $\mathcal{L}_{\text{TM-00}}$. On the right, we sketch another TM which uses $A_{\text{TM-00}}$.
  (a) Does A ever run M on w?
  (b) Prove that A is a decider.
  (c) Prove that A accepts $\langle M \rangle \# w$ if and only if M accepts w.
  (d) What language from Definition 27.6 does A decide?
  (e) Prove that $\mathcal{L}_{\text{TM-00}}$ is undecidable.
Don't confuse running M' with running $A_{\text{TM-00}}$ on $\langle M' \rangle$.

> $A = $ TM that uses $A_{\text{TM-00}}$.
> **INPUT:** $\langle M \rangle \# w$
> 1: Create a new TM M' with encoding $\langle M' \rangle$.
>> $M' = $ New TM taking INPUT x
>> 1: If $x = 00$, run M on w.
>>   Accept if M accepts.
>> 2: Otherwise, reject.
>
> 2: Output the decision of $A_{\text{TM-00}}$ on $\langle M' \rangle$.

Problem 27.39. Suppose that E is a decider for $\mathcal{L}_{\text{EMPTY-TM}}$. On the right, we sketch another TM which uses E.
  (a) Does A ever run M on w?
  (b) Prove that A is a decider.
  (c) Prove that A accepts $\langle M \rangle \# w$ if and only if M accepts w.
  (d) What language from Definition 27.6 does A decide?
  (e) Prove that $\mathcal{L}_{\text{EMPTY-TM}}$ is undecidable.
Don't confuse running M' with running E on $\langle M' \rangle$.

> $A = $ TM that uses E.
> **INPUT:** $\langle M \rangle \# w$
> 1: Create a new TM M' with encoding $\langle M' \rangle$.
>> $M' = $ New TM taking INPUT x
>> 1: If $x = w$, run M on w.
>>   Accept if M accepts.
>> 2: Otherwise, reject.
>
> 2: Output the opposite decision of E on $\langle M' \rangle$.

Problem 27.40. Problem 27.39 proved that $\mathcal{L}_{\text{EMPTY-TM}}$ is undecidable. Sketch a decider for $\mathcal{L}_{\text{EMPTY-TM}}$ given a decider for $\mathcal{L}_{\text{EQ-TM}}$, and hence prove that $\mathcal{L}_{\text{EQ-TM}}$ is undecidable. *[Hint: Use a vacuous TM whose language is empty.]*

Problem 27.41. Given a TM $\langle M \rangle$, the task is to determine if its language is regular and could be decided by a DFA.

(a) Formulate a language which corresponds to the task. Call this language $\mathcal{L}_{\text{REG-TM}}$ and let R be a decider for $\mathcal{L}_{\text{REG-TM}}$.

(b) On the right, we sketch another TM which uses R.
   (i) Does A ever run M on w?
   (ii) What language does M' accept if M accepts w?
   (iii) What language does M' accept if M does not accept w?
   (iv) Prove that A is a decider which accepts $\langle M \rangle \# w$ if and only if M accepts w.
   (v) Prove that $\mathcal{L}_{\text{REG-TM}}$ is undecidable.

(c) Use the same technique as in (b) to show that no algorithm can decide if a TM accepts a language which is a CFL.

> $A =$ TM that uses R.
> **INPUT:** $\langle M \rangle \# w$
> 1: Create a new TM M' with encoding $\langle M' \rangle$.
>> $M' =$ New TM taking INPUT x
>> 1: If $x \in \{0^{\bullet n} 1^{\bullet n}\}$, accept.
>> 2: If $x \notin \{0^{\bullet n} 1^{\bullet n}\}$, run M on w.
>>   Accept if M accepts.
> 2: Output the decision of R on $\langle M' \rangle$.

Problem 27.42. Use methods similar to Problems 27.38-27.41 to show that $\mathcal{L}_{\text{ALL-TM}}$ and $\mathcal{L}_{\text{FINITE-TM}}$ are undecidable.

Problem 27.43 (Rice's Theorem). Problems 27.38-27.42 show that testing a TM for a property is undecidable. Indeed this is true for any non-trivial property. Let $\mathcal{L}_{\text{P-TM}}$ be the language of all TMs with property P,

$$\mathcal{L}_{\text{P-TM}} = \{\langle M \rangle \mid M \text{ is a TM that has property } P\}.$$

Property P depends only on the language of the TM, so if $\mathcal{L}(M_1) = \mathcal{L}(M_2)$, then $\langle M_1 \rangle \in \mathcal{L}_{\text{P-TM}}$ iff $\langle M_2 \rangle \in \mathcal{L}_{\text{P-TM}}$. Property P is non-trivial, which means both $\mathcal{L}_{\text{P-TM}}$ and $\overline{\mathcal{L}_{\text{P-TM}}}$ are nonempty (some TM has property P and some TM does not). Let T_P be a TM with property P, so $\langle T_P \rangle \in \mathcal{L}_{\text{P-TM}}$. Let $T_\varnothing$ be the trivial TM that rejects all strings, so $\mathcal{L}(T_\varnothing) = \varnothing$. Without loss of generality, you may assume that $\langle T_\varnothing \rangle \notin \mathcal{L}_{\text{P-TM}}$. Suppose that $A_{\text{P-TM}}$ decides $\mathcal{L}_{\text{P-TM}}$.

(a) Why may we assume $\langle T_\varnothing \rangle \notin \mathcal{L}_{\text{P-TM}}$, w.l.o.g?

(b) We sketch a TM which uses $A_{\text{P-TM}}$, T_P and $T_\varnothing$.
   (i) Does A ever run M on w? Is A a decider?
   (ii) What is $\mathcal{L}(M')$ if M accepts w?
   (iii) What is $\mathcal{L}(M')$ if M does not accept w?
   (iv) Prove that A accepts $\langle M \rangle \# w$ if and only if M accepts w. (A uses $A_{\text{P-TM}}$'s ability to distinguish $\langle T_\varnothing \rangle$ from $\langle T_P \rangle$.)

(c) Prove Rice's Theorem: $\mathcal{L}_{\text{P-TM}}$ is undecidable for non-trivial P.

(d) Use (c) to prove undecidability of these languages.
   (i) $\mathcal{L}_{\text{TM-00}}$. (ii) $\mathcal{L}_{\text{EMPTY-TM}}$. (iii) $\mathcal{L}_{\text{ALL-TM}}$. (iv) $\mathcal{L}_{\text{FINITE-TM}}$.

(e) Does Rice's Theorem imply that $\mathcal{L}_{\text{EQ-TM}}$ is undecidable?

> $A =$ TM that uses $\mathcal{L}_{\text{P-TM}}$, T_P and $T_\varnothing$.
> **INPUT:** $\langle M \rangle \# w$
> 1: Create a new TM M' with encoding $\langle M' \rangle$.
>> $M' =$ New TM taking INPUT x
>> 1: Run M on w.
>> 2: If M accepts w, run T_P on x.
>>   Accept if T_P accepts.
>> 3: Otherwise reject.
> 2: Output the decision of $A_{\text{P-TM}}$ on $\langle M' \rangle$.

Problem 27.44. Show that determining if a TM accepts w^{R} (reversal) whenever it accepts w is undecidable.

Problem 27.45. Find a solution to these instances of PCP: (a) $\begin{array}{|c|}\hline 0 \\ \hline 00000 \\ \hline \end{array} d_1 \quad \begin{array}{|c|}\hline 00000 \\ \hline 00 \\ \hline \end{array} d_2$ (b) $\begin{array}{|c|}\hline 01 \\ \hline 0101 \\ \hline \end{array} d_1 \quad \begin{array}{|c|}\hline 00 \\ \hline 0 \\ \hline \end{array} d_2 \quad \begin{array}{|c|}\hline 010 \\ \hline 1 \\ \hline \end{array} d_3 \quad \begin{array}{|c|}\hline 1 \\ \hline 0 \\ \hline \end{array} d_4$

Problem 27.46. Sketch a decider for a variant of PCP where the two strings in every domino are the same length.

Problem 27.47. We claimed that PCP is undecidable. Is PCP recognizable?

Problem 27.48. Prove that there exists an undecidable language which is a subset of $\{1\}^*$.

Problem 27.49. Prove directly by contradiction, not using a reduction from the undecidable problems in this Chapter, that "Hello-World" is undecidable. Obtain a paradox as in Pop Quiz 27.1.

Problem 27.50. Prove the undecidability of an *easier* version of the "Hello-World" autograding task, to determine if a Turing Machine halts with the first bit after the $*$ being 0. (The rest of the tape need not be empty.)

$$\mathcal{L} = \{\langle M \rangle \# w \mid M \text{ is a TM that halts on } w \text{ with 0 as the first bit on the tape after } * \}.$$

Problem 27.51. In your favorite language (e.g. python), write a program that prints an exact copy of itself to a file or stdout. Such a program is called a self-replicating program or *quine*. If you don't think it is possible, explain why.

Problem 27.52 (Viruses). Define a virus as a program that writes an exact copy of itself to a file and exits.

(a) Prove that virus detection is an undecidable problem.

(b) For a more general type of virus, is virus detection easier or harder?

(c) The antivirus package shows a 100% GUARANTEE*. The asterisk points to fine print 😟. Are you paying around \$50 for a program that solves an unsolvable problem? How do you think such anti-virus software actually works? What guarantees can be made (what is the fine print)?
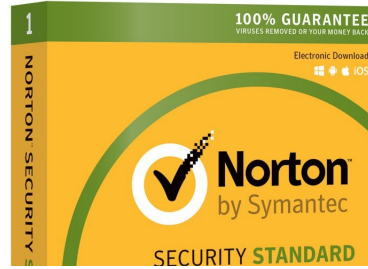
Problem 27.53. Suppose M_1 and M_2 are recognizers for $\mathcal{L}_1$ and $\mathcal{L}_2$. Sketch a recognizer M for $\mathcal{L}_1 \cup \mathcal{L}_2$.

(a) Does this attempt at M work? On input w, run $M_1(w)$ and then $M_2(w)$. If M_1 or M_2 accept, M says (YES).

(b) Give a high-level Turing Machine M which computes $M_1(w)$ and $M_2(w)$ *in parallel* for input w (implement a step of M_1, then a step of M_2, then M_1, and so on). That is, M interleaves the steps of $M_1(w)$ with those of $M_2(w)$.

(c) Use (b) to sketch M and show it recognizes $\mathcal{L}_1 \cup \mathcal{L}_2$. Thus, *recognizable* languages are closed under union.

(Note the resemblence to the proof that countable languages are closed under union in Theorem 22.3.)

Problem 27.54. If $\mathcal{L}$ and $\overline{\mathcal{L}}$ are recognizable, show that $\mathcal{L}$ is decidable by sketching a decider for $\mathcal{L}$. Be careful. You must show how to construct a *decider* for $\mathcal{L}$ given *recognizers* for $\mathcal{L}$ and $\overline{\mathcal{L}}$.

Problem 27.55. Prove that the decidable languages are closed under:

(a) Union.   (b) Intersection.   (c) Complement.   (d) Concatenation.   (e) Kleene star.   (f) Reversal

Problem 27.56. Prove that the recognizable languages are closed under:

(a) Union.   (b) Intersection.   (c) Concatenation.   (d) Kleene star.   (e) Reversal

Problem 27.57. Explain why recognizable languages are not closed under complement.

Problem 27.58. Consider the task to test if two TMs are equivalent, $\mathcal{L}_{\text{EQ-TM}}$ from Definition 27.6.

(a) Show that $\mathcal{L}_{\text{EQ-TM}}$ is non-recognizable. *[Hint: Use a recognizer for $\mathcal{L}_{\text{EQ-TM}}$ to sketch a recognizer for $\overline{\mathcal{L}_{\text{HALT}}}$.]*

(b) Show that $\overline{\mathcal{L}_{\text{EQ-TM}}}$ is non-recognizable. (Both a language and its complement can be non-recognizable.)

Problem 27.59. Consider the task to test if a TM accepts no strings (not even ε), $\mathcal{L}_{\text{EMPTY-TM}}$ from Definition 27.6.

(a) Show that $\overline{\mathcal{L}_{\text{EMPTY-TM}}}$ (the complement of $\mathcal{L}_{\text{EMPTY-TM}}$) is recognizable. Be careful.

(b) What difficulty do you face in trying to construct a recognizer for $\mathcal{L}_{\text{EMPTY-TM}}$? Prove $\mathcal{L}_{\text{EMPTY-TM}}$ is non-recognizable.

Problem 27.60 (Mapping Reduction). $\mathcal{L}$ is undecidable if a TM for $\mathcal{L}$ can be used to solve a known undecidable problem $\mathcal{L}_*$. To show this formally, one must mapping reduce $\mathcal{L}_*$ to $\mathcal{L}$. That is, find a computable function $f : \Sigma^* \mapsto \Sigma^*$, such that

$$w \in \mathcal{L}_* \leftrightarrow f(w) \in \mathcal{L} \qquad \forall w \in \Sigma^*.$$
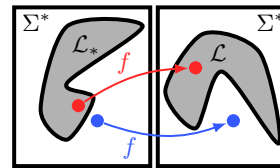
We say $\mathcal{L}_*$ is reducible to $\mathcal{L}$, written $\mathcal{L}_* \leq_{\text{R}} \mathcal{L}$ ($\mathcal{L}_*$ is easier than $\mathcal{L}$). A function f is computable if some transducer-TM halts on any input w, leaving $f(w)$ on the tape.

(a) If $\mathcal{L}_*$ is reducible to $\mathcal{L}$, does it necessarily mean that $\mathcal{L}$ is reducible to $\mathcal{L}_*$?

(b) If $\mathcal{L}_*$ is reducible to $\mathcal{L}$, does it necessarily mean that $\mathcal{L}$ is reducible to $\overline{\mathcal{L}_*}$?

(c) If $\mathcal{L}_*$ is reducible to $\mathcal{L}$, does it necessarily mean that $\overline{\mathcal{L}}$ is reducible to $\overline{\mathcal{L}_*}$?

(d) If $\mathcal{L}$ is decidable and $\mathcal{L}_*$ is reducible to $\mathcal{L}$, then prove that $\mathcal{L}_*$ is decidable.

(e) If $\mathcal{L}$ is decidable and $\mathcal{L}_*$ is reducible to $\overline{\mathcal{L}}$, then prove that $\mathcal{L}_*$ is decidable.

(f) If $\mathcal{L}$ is recognizable and $\mathcal{L}_*$ is reducible to $\mathcal{L}$, then prove that $\mathcal{L}_*$ is recognizable.

(g) If $\mathcal{L}$ is regular and $\mathcal{L}_*$ is reducible to $\mathcal{L}$, does that mean $\mathcal{L}_*$ is regular. Why or why not?

(h) If $\mathcal{L}_*$ is undecidable and $\mathcal{L}_*$ is reducible to $\mathcal{L}$, then prove that $\mathcal{L}$ is undecidable.

(i) If $\mathcal{L}_*$ is undecidable and $\mathcal{L}_*$ is reducible to $\overline{\mathcal{L}}$, then prove that $\mathcal{L}$ is undecidable.

(j) If $\mathcal{L}_*$ is non-recognizable and $\mathcal{L}_*$ is reducible to $\mathcal{L}$, then prove that $\mathcal{L}$ is non-recognizable.

(k) If $\mathcal{L}$ is recognizable and $\mathcal{L} \leq_{\text{R}} \overline{\mathcal{L}}$, then prove that $\mathcal{L}$ is decidable.

Problem 27.61. Show that any recognizable language is reducible to $\mathcal{L}_{\text{TM}}$. *[Hint: Use a recognizer for the language.]*

Problem 27.62. Recall that $\mathcal{L}_{\text{TM}}$ is recognizable, but not decidable.

(a) Suppose $\mathcal{L}_{\text{TM}}$ is reducible to $\mathcal{L}$, so $\mathcal{L}_{\text{TM}} \leq_{\text{R}} \mathcal{L}$. Prove that $\mathcal{L}$ is undecidable.

(b) Suppose $\overline{\mathcal{L}_{\text{TM}}}$ is reducible to $\mathcal{L}$, so $\overline{\mathcal{L}_{\text{TM}}} \leq_{\text{R}} \mathcal{L}$. Prove that $\mathcal{L}$ is non-recognizable.

(c) Suppose $\mathcal{L}_{\text{TM}}$ is reducible to $\overline{\mathcal{L}}$, so $\mathcal{L}_{\text{TM}} \leq_{\text{R}} \overline{\mathcal{L}}$. Prove that $\mathcal{L}$ is non-recognizable.

Problem 27.63. Problem 27.62 will be useful to answer these questions.

(a) Give a mapping reduction from $\mathcal{L}_{\text{TM}}$ to $\overline{\mathcal{L}_{\text{EMPTY-TM}}}$. What does it prove? *[Hint: Problem 27.39.]*

(b) Sketch a recognizer for $\overline{\mathcal{L}_{\text{EMPTY-TM}}}$.

(c) Prove there is no mapping reduction from $\mathcal{L}_{\text{TM}}$ to $\mathcal{L}_{\text{EMPTY-TM}}$. *[Hint: $\mathcal{L}_{\text{TM}} \leq_{\text{R}} \mathcal{L}_{\text{EMPTY-TM}}$ implies $\overline{\mathcal{L}_{\text{TM}}} \leq_{\text{R}} \overline{\mathcal{L}_{\text{EMPTY-TM}}}$.]*

Problem 27.64. Use mapping reduction to prove that both $\mathcal{L}_{\text{EQ-TM}}$ and $\overline{\mathcal{L}_{\text{EQ-TM}}}$ are non-recognizable.

(a) Give a mapping reduction from $\mathcal{L}_{\text{TM}}$ to $\overline{\mathcal{L}_{\text{EQ-TM}}}$. What does it prove? *[Hint: Sketch a transducer taking $\langle M \rangle$#w to $\langle M_1 \rangle$#$\langle M_2 \rangle$ where $\mathcal{L}(M_1) = \varnothing$ and $\mathcal{L}(M_2) = \Sigma^*$ if M accepts w, otherwise $\mathcal{L}(M_2) = \varnothing$.]*

(b) Give a mapping reduction from $\mathcal{L}_{\text{TM}}$ to $\mathcal{L}_{\text{EQ-TM}}$. What does it prove? *[Hint: Sketch a transducer taking $\langle M \rangle$#w to $\langle M_1 \rangle$#$\langle M_2 \rangle$ where $\mathcal{L}(M_1) = \Sigma^*$ and $\mathcal{L}(M_2) = \Sigma^*$ if M accepts w, otherwise $\mathcal{L}(M_2) = \varnothing$.]*

Problem 27.65. A linearly bounded Turing Machine is a machine with restricted memory. It cannot move off the slots occupied by the input. You can imagine a second beacon symbol ⁑ placed on the right of the input beyond which the machine cannot move. The TM can mark the tape in different ways, so the symbols that can appear on the tape are $\sqcup, 0, 1, \check{0}, \check{1}$, etc. Let g be the number of symbols that can appear on the tape. Suppose the input w has length n.

(a) Show that the number of possible strings that can be on the part of the tape occupied by the input is g^n. (The amount of tape memory available for the machine is $n \log_2 g$ bits, linear in the input size.)

(b) As a computation proceeds, we can describe the configuration of the system (TM and tape) by the position of the TM head, the state of the TM and the string on the available n slots of tape. Show that the number of possible system-configurations for a TM with q states is qng^n.

(c) If the computation takes more than qng^n steps, prove that the TM loops for ever on input w.

(d) Sketch a decider H_{LB} that decides if a linearly bounded TM M halts or loops forever on input w. Note, the input to H_{LB} is $\langle M \rangle$#w where M is linearly bounded, but H_{LB} can be a regular TM not necessarily linearly bounded.

(e) Sketch a decider A_{LB} for the language $\mathcal{L}_{\text{TM-LB}} = \{\langle M \rangle$#$w \mid M$ is a linearly bounded TM which accepts $w\}$.

Problem 27.66. Let $\mathcal{L}_{\text{TM-DECIDER}} = \{\langle M \rangle \mid M$ is a decider$\}$ be the language containing descriptions of all TMs that are deciders. Prove that $\mathcal{L}_{\text{TM-DECIDER}}$ is not decidable. That is, no algorithm can tell if some other program halts on all inputs. This should not surprise you because it looks very similar to the halting problem.

Use a proof by contradiction. Assume $A_{\text{TM-DECIDER}}$ is a decider for $\mathcal{L}_{\text{TM-DECIDER}}$. We sketched another TM on the right that uses $A_{\text{TM-DECIDER}}$. Is this TM a decider? What language does it decide?

A = TM that uses $A_{\text{TM-DECIDER}}$.

INPUT: $\langle M \rangle$#w
1: Create TM M' with encoding $\langle M' \rangle$.

M' = New TM taking INPUT x
 1: Ignore x and run M on w.
 2: Accept.

2: Output the decision of $A_{\text{TM-DECIDER}}$ on $\langle M' \rangle$.

Problem 27.67. Prove that the language of all deciders $\mathcal{L}_{\text{TM-DECIDER}}$ from Problem 27.66 is not recognizible. Use a proof by contradiction. Assume $\mathcal{L}_{\text{TM-DECIDER}}$ is recognizable. Sketch a Turing Machine E which prints the TMs in $\mathcal{L}_{\text{TM-DECIDER}}$ in some order, $M_1, M_2, \ldots$ (see Problem 27.14). Similarly, sketch a Turing Machine S which prints the strings of Σ^* in some order $s_1, s_2, \ldots$ (for example lexicographic order). Consider the decisions Turing Machine M_i makes on strings s_j. We show what these decisions might look like in the table, in which we highlighted the diagonal.

	s_1	s_2	s_3	s_4	$\cdots$
$\langle M_1 \rangle$	YES	YES	NO	YES	$\cdots$
$\langle M_2 \rangle$	NO	NO	NO	YES	$\cdots$
$\langle M_3 \rangle$	YES	YES	NO	NO	$\cdots$
$\langle M_4 \rangle$	YES	NO	NO	NO	$\cdots$
$\vdots$		$\vdots$			$\ddots$

(a) Use the diagonal to construct a language $\mathcal{L}$ which is not decided by any of the M_i.

(b) Sketch a decider for $\mathcal{L}$ from part (a). Prove you have a decider. *[Hint: On input w, first run S until it prints w. Suppose $s_i = w$. Now run M_i on s_i. How will you get M_i? Must M_i halt? What is the final output?]*

(c) Prove that $\mathcal{L}_{\text{TM-DECIDER}}$ is not recognizable.

You have proved that any recognizable language containing only encodings of deciders can't be complete.

Problem 27.68. A real number in binary is $x = 0.b_1b_2\cdots = \sum_i b_i 2^{-i}$. The number x is computable if there is a Turing Machine M which, for any input $i \in \mathbb{N}$, halts and accepts if $b_i=1$ or halts and rejects if $b_i = 0$.

(a) Show that each of these numbers is computable (also give the first 10 binary digits): (i) $1/3$ (ii) $1/\sqrt{2}$ (iii) $1/\pi$.

(b) Prove there are uncountably many non-computable numbers.

(c) Prove that each of the numbers defined below is not computable. Let $\{M_1, M_2, \ldots\}$ be a list of all TMs.
  (i) b_i is 1 if and only if M_i accepts 00.   (ii) b_i is 1 if and only if M_i accepts $\langle M_i \rangle$.

Problem 27.69 (Busy Beaver). In 1962, Tibor Radó found a non-computable function $B : \mathbb{N} \mapsto \mathbb{N}$. Given n, consider all possible n-state TMs which halt on the empty input ε. The Busy Beaver function $B(n)$ is the largest number of steps made by any of these halting n-state TMs. Busy Beaver captures the maximum activity you can get from a fixed complexity machine, where complexity is measured by number of states.

(a) Prove that $B(n)$ is a non-computable function. To do so, assume that some transducer-TM M_{BB} always halts on input n with $B(n)$ remaining on the tape. Sketch a TM which decides $\mathcal{L}_{\text{TM}}$. *[Hint: Embed $\langle M \rangle$#w into a TM which runs M on w and use M_{BB} to determine how long to run to decide if M halts on w.]*

(b) Let $f(n)$ be any computable function. Prove that $B(n) > f(n)$ for infinitely many n. That is, in a sense, $B(n)$ is larger than *any* computable function. *[Hint: Modify the proof in (a) to use $f(n)$ instead of $B(n)$.]*

Problem 27.70 (Kolmogorov Complexity, Information and Randomness). For a string x, $\langle M \rangle$#w is a *description* of x if TM M when run with input w halts with x left on the tape. The Kolmogorov complexity $\mathcal{K}(x)$ is the length of the shortest description of x (also called the descriptive complexity),

$$\mathcal{K}(x) = \min_{\langle M \rangle \text{\#} w \text{ is a description of } x} |\langle M \rangle \text{\#} w|.$$

(a) Which of these two strings do you think is more "complex" or "contains" more information? Give your intuition.

$$x_1 = 0011001100110011001100110011001100110011001100110011001100110011$$
$$x_2 = 1000110100010110111010111000000001001010111010101110100010101111101$$

(b) Show that there is a universal constant c for which $\mathcal{K}(x) \le |x| + c$ for all x. (Descriptive complexity can't be much worse than using the string itself, but it can be much smaller.) *[Hint: Use a trivial TM in the description.]*

(c) String x is compressible if $\mathcal{K}(x) < x$. For all $n \in \mathbb{N}$, prove: some length-n string is incompressible. *[Hint: Count.]*
(Incompressible strings have many properties of a "typical" random string, e.g. about the same number of 0s and 1s.)

Problem 27.71. The Kolmogorov complexity $\mathcal{K}(x)$ in Problem 27.70 is a function from Σ^* to $\mathbb{N}$. Prove that $\mathcal{K}(x)$ is a non-computable function by following these steps. Assume a TM Q on any input x halts with $\mathcal{K}(x)$ on the tape.

(a) Let $\{s_1, s_2, \ldots\}$ be a lexicographic ordering of strings in Σ^*. We use Q to sketch another TM A on the right. Prove that A halts on any input n and outputs x_n.
One may use A to produce a sequence of strings $x_1, x_2, \ldots$, where x_n is produced by running A on n. By construction of A, what is a lower bound for $\mathcal{K}(x_n)$, for $n = 1, 2, \ldots$?

> A = TM that uses Q.
> ___
> **INPUT:** $n \in \mathbb{N}$.
> 1: **for** $x = s_1, s_2, \ldots$ **do**
> 2:   Run Q on x to get $\mathcal{K}(x)$.
> 3:   If $\mathcal{K}(x) \ge n$, print x and HALT.

(b) Prove that $|\langle A \rangle|$ is some universal constant c. The main complication is the statement "for $x = s_1, s_2, \ldots$". You may wish to give a more detailed sketch of A.

(c) Show that $\langle A \rangle$#$\langle n \rangle$ is the description of x_n. Use $|\langle A \rangle$#$\langle n \rangle|$ to get an upper bound $\mathcal{K}(x_n)$ which is in $O(\log_2(n))$.

(d) Use your upper bound from (c) and lower bound from (a) to get a contradiction, and hence prove Q doesn't exist.

28.5   Problems

Problem 28.1. Which worst-case runtimes are fast and which are slow. Justify your answers mathematically. Plot all the functions versus n on a log-log plot. Explain why your plot visually justifies the separation between fast and slow.

$$(\log_2 n)^{\log_2 n} \qquad \sqrt{n} \qquad n \log \log n \qquad 2^{\log n} \qquad 2^{\log^2 n} \qquad 2^{\sqrt{n}} \qquad 2^n \qquad n^3 \qquad n^{100}$$

Problem 28.2. Show that each problem is in P by sketching a decider and analyzing the worst-case runtime. A transducer is polynomial if its worst-case runtime is polynomial in the sum of the input and output sizes.
  (a) Regular language: $\mathcal{L}_1 = \{*01*\}$ and $\mathcal{L}_2 = \{*01\}$.
  (b) Not CFL: $\mathcal{L} = \{0^{\bullet n}\#1^{\bullet n}\#0^{\bullet n}\}$ (# is a 'punctuation' symbol).
  (c) Squaring: $\mathcal{L} = \{0^{\bullet n}\#1^{\bullet n^2}, n \geq 0\}$ (# is a 'punctuation' symbol).
  (d) Exponentiating: $\mathcal{L} = \{0^{\bullet n}\#1^{\bullet 2^n}, n \geq 0\}$ (# is a 'punctuation' symbol).
  (e) Repetition: $\mathcal{L} = \{ww|w \in \{0,1\}^*\}$.
  (f) Palindromes: $\mathcal{L} = \{w|w \in \{0,1\}^*, w = w^{\mathrm{R}}\}$.
  (g) Addition of 2: $\mathcal{L} = \{0^{\bullet n}1^{\bullet n+2}\}$.
  (h) Addition of 2: The input is $0^{\bullet n}$. Halt with $0^{\bullet n+2}$ on the tape.
  (i) Multiplication by 2: The input is $0^{\bullet n}$. Halt with $0^{\bullet 2n}$ on the tape.
  (j) Squaring: The input is $0^{\bullet n}$. Halt with $0^{\bullet n^2}$ on the tape.
  (k) Exponentiate: The input is $0^{\bullet n}$. Halt with $0^{\bullet 2^n}$ on the tape.
  (l) Exponentiate: The input w is the binary representation of n. Halt with 2^n in binary on the tape.
  (m) Copying: The input is a string w. Halt with ww on the tape.
  (n) Reversal: The input is w. Halt with w^{R} on the tape.
  (o) Switching: The input is $w\#v$. Halt with $v\#w$ on the tape.
  (p) Deleting first: The input is $xw \in \Sigma^*$. Halt with w on the tape.
  (q) Prefixing: The input is $w \in \Sigma^*$. Halt with $0w$ on the tape.
  (r) Binary to unary: The input w is the binary representation of n. Halt with $0^{\bullet n}$.
  (s) Unary to binary: The input is $0^{\bullet n}$. Halt with the binary representation of n on the tape.
  (t) Binary addition: The input is two binary strings $w_1\#w_2$. Halt with $w_1 + w_2$ (binary addition) on the tape.
  (u) Division: For input $0^{\bullet n}$, reject if n is odd. If n is even, accept with $0^{\bullet n/2}$ on the tape.
  (v) Division: The input w is binary for n. Reject if n is odd. If n is even, accept with $n/2$ in binary on the tape.

Problem 28.3. Prove that P is closed under union, intersection, concatenation, and complement.

Problem 28.4. Formulate each task as a language and show that it is in P. If appropriate, use a transducer-TM.
  (a) MAKE-CHANGE: Make change for n using the fewest coins in a given coin-system (e.g. 1¢, 3¢, 6¢, 10¢).
  (b) NUM-CHANGE: Find the number of ways to make change for n in a given coin-system (e.g. 1¢, 3¢, 6¢, 10¢).
  (c) RELPRIME: Given two integers x, y in binary, determine if they are relatively prime.
  (d) PATH: Given a graph and two vertices, determine if there are path connecting the two vertices.
  (e) COMPOSITE-VERIFY: Given n and a factor $1 < p < n$, verify that p divides n.
  (f) COLOR-VERIFY: Given a graph and a coloring of the vertices, verify that the coloring is valid.
  (g) HAMILTONIAN-VERIFY: Given a graph and a Hamiltonian path, verify that the path is Hamiltonian.
  (h) CLIQUE-VERIFY: Given a graph and a K-clique, verify that it is a K-clique.

Problem 28.5. Prove that every regular language is in P.

Problem 28.6. The decider for a CFL in Problem 27.10 uses the Chomsky Normal Form. Given input w of length n, the TM checks every derivation of length $2n - 1$. Is this TM polynomial? Does this mean CFL's are not in P?

Problem 28.7. Prove that every context free language is in P. Use a build-up method. Let the CFG be in Chomsky Normal Form and consider input string w. Let $w_{i,j}$ be the substring of w from position i to j, where $i \leq j$.
  (a) Let $S_{i,j}$ be the subset of variables that can generate $w_{i,j}$. How do you determine $S_{i,i}$?
  (b) Given $S_{i,j}$ for all $w_{i,j}$ up to length k (strong induction), show how to determine $S_{i,j}$ for $w_{i,j}$ of length $k + 1$.
  (c) Suppose you have computed $S_{1,n}$. How do you determine if the CFG can generate w.
  (d) Sketch a TM for the CFL and prove that it's polynomial. *[Hint: How many choices are there for $w_{i,j}$?]*

Problem 28.8. Prove that there is no decider for $\mathcal{L}_{\mathrm{EXP}}$ with worst case runtime in $o(2^n)$, where $n = |\langle M \rangle \# w|$. The argument follows the same general line we used to prove there is no polynomial decider for $\mathcal{L}_{\mathrm{EXP}}$.

29.4   Problems

Problem 29.1. The average earth-to-moon distance is 238,855 miles. Express this distance using Roman numerals. How is your answer relevant to the way we define if a problem is hard? *[Hint: Unary vs. radix in a base larger than 1.]*

> **Definition 29.10.** Here is a list of useful problems, some of which we proved are NP-complete.
> (a) PATH-DIR(G, s, t): Is there a path from vertices s to t in the directed graph G?
> (b) k-SAT$(C_1, \ldots, C_m)$: Each clause C_i is an OR of at most k terms. Is there a truth assignment to the variables satisfying every clause?
> (c) IND-SET(G, k): Is there an independent set with k or more vertices in the undirected graph G?
> (d) CLIQUE(G, k): Is there an clique with k or more vertices in the undirected graph G?
> (e) k-COLORING(G): Is there a valid coloring of undirected graph G using at most k colors?
> (f) VERTEX-COVER(G, k): Is there a vertex cover with k or fewer vertices in the undirected graph G?
> (g) DOM-SET(G, k): Is there a dominating set with k or fewer vertices in the undirected graph G?
> (h) SUBSET-SUM(S, t): Is there a subset of the multiset S whose elements sum to the target t?
> (i) FACTOR(n, k): Is the kth bit of the smallest prime divisor of n a 1?

Problem 29.2. For each problem in Definition 29.10, is it easier to give evidence for a (YES) or (NO) answer?

Problem 29.3. Prove each problem in Definition 29.10 is in NP. Give the evidence and a polynomial certifier. (For part (i), assume testing primality is in P.)

Problem 29.4. Why is every problem in P also in NP? What is the evidence E and polynomial certifier C?

Problem 29.5. Prove that PATH-DIR is in P.

Problem 29.6. If PATH-DIR is NP-complete, prove that P = NP. Do you think PATH-DIR is NP-complete?

Problem 29.7. Prove that for any fixed k, e.g. $k = 10$, determining if a graph G has a clique of size k is in P. Why then do we say that CLIQUE is NP-complete and that we do not know of a polynomial algorithm for CLIQUE.

Problem 29.8. A problem's (YES)-answer is polynomialy verifiable. Does it mean its (NO)-answer is also polynomialy verifiable? Show that the answer is affirmative for all problems in P.

Problem 29.9. A sorter outputs all the bits in the n-bit input, but with all the 1's on the left. For the problem IS-SORTER defined below, which is easier to verify given the right evidence: (YES) or (NO)?

   IS-SORTER: Given a circuit that takes n inputs, determine if the circuit is a valid sorter.

Problem 29.10 (coNP). The set coNP contains all problems whose (NO)-answer can be verified in polynomial time. Prove that FACTOR $\in$ NP $\cap$ coNP. (**Burning question:** Is NP = coNP?)

Problem 29.11. We introduced two notions for comparing problems $\mathcal{L}_1$ and $\mathcal{L}_2$: $\mathcal{L}_1 \leq_R \mathcal{L}_2$ in Chapter 27 and $\mathcal{L}_1 \leq_P \mathcal{L}_2$ in this chapter. Carefully explain both notions and the difference between them.

Problem 29.12. The problem $\mathcal{L}_*$ is NP-complete. What can you conclude about the problem $\mathcal{L} \in$ NP?
   (a) An instance w of $\mathcal{L}$ can be converted to an instance w_* of $\mathcal{L}_*$ and $w \in \mathcal{L} \leftrightarrow w_* \in \mathcal{L}_*$.
   (b) An instance w of $\mathcal{L}$ can be quickly converted, in polynomial time, to an instance w_* of $\mathcal{L}_*$ and $w \in \mathcal{L} \leftrightarrow w_* \in \mathcal{L}_*$.
   (c) An instance w_* of $\mathcal{L}_*$ can be converted to an instance w of $\mathcal{L}$ and $w \in \mathcal{L} \leftrightarrow w_* \in \mathcal{L}_*$.
   (d) An instance w_* of $\mathcal{L}_*$ can be quickly converted, in polynomial time, to an instance w of $\mathcal{L}$ and $w \in \mathcal{L} \leftrightarrow w_* \in \mathcal{L}_*$.

Problem 29.13. PATH is the same problem as PATH-DIR, but for undirected graphs. Prove that PATH $\leq_P$ PATH-DIR.

Problem 29.14. Sketch a fast Turing Machine that implements the solution of LARGE-SUM in Section 29.1 on page 414 and argue that the runtime of your Turing Machine is polynomial.

Problem 29.15. The certifier for a problem in NP takes the input w, a polynomial certificate c and has polynomial worst-case runtime. How do you *solve* the problem using the certifier? Is your worst-case runtime polynomial?

Problem 29.16. DIRECTED-HAM-PATH is the task of determining if a directed graph G, has a Hamiltonian path.
   (a) Similar to Example 29.2, what would be a simplified encoding for a directed graph G?
   (b) Show that DIRECTED-HAM-PATH $\in$ NP.

Problem 29.17. Prove that NP is closed under the Kleene star operation. That is, if $\mathcal{L} \in$ NP then $\mathcal{L}^* \in$ NP.

Problem 29.18. Prove that P is closed under the Kleene star operation. That is, if $\mathcal{L} \in$ P then $\mathcal{L}^* \in$ P. *[Hint: Use a build-up method (dynamic programming). For string $w = b_1 b_2 \cdots b_n$, define $Q(i) = 1$ if $b_1 \cdots b_i \in \mathcal{L}^*$ for $i = 1, \ldots, n$.]*

Problem 29.19. A circuit is a directed *acyclic* graph of gates. We show a cyclic circuit on the right. What is the output y? Explain your reasoning.
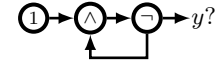
Problem 29.20. In each case, is the instance of 3-SAT satisfiable? Give a proof of your answer.
(a) $(x \vee y \vee z)(x \vee \overline{y} \vee z)(x \vee \overline{y} \vee \overline{z})(\overline{x} \vee y \vee z)(\overline{x} \vee y \vee \overline{z})(\overline{x} \vee \overline{y} \vee \overline{z})$.
(b) $(x \vee y \vee z)(x \vee y \vee \overline{z})(x \vee \overline{y} \vee z)(x \vee \overline{y} \vee \overline{z})(\overline{x} \vee y \vee z)(\overline{x} \vee y \vee \overline{z})(\overline{x} \vee \overline{y} \vee z)(\overline{x} \vee \overline{y} \vee \overline{z})$.

Problem 29.21. Build a "naive" circuit to determine if the input-string $x_1 \cdots x_n$ has at least k 1's.
(a) Let $S_{i_1, i_2, \ldots, i_k}$ be a circuit that takes the AND of bits $x_{i_1}, \ldots, x_{i_k}$. How many different circuits $S_{i_1, i_2, \ldots, i_k}$ are there, and how many gates are in each of them?
(b) Show that the OR of the outputs of all the $S_{i_1, i_2, \ldots, i_k}$ is 1 if and only if the input-string has at least k ones.
(c) How many gates do you need to implement the gigantic OR?
(d) How many gates does the entire circuit need? For $k = n/2$, show that the number of gates is exponential in n.

Problem 29.22. Is $\mathcal{L} = \{0^{\bullet n} 1^{\bullet n} \mid n \geq 1\}$ in NP?
(a) Give a Boolean circuit which takes four inputs $x_1 x_2 x_3 x_4$ with output 1 if and only if $x_1 x_2 x_3 x_4 \in \mathcal{L}$.
(b) Transform the Boolean circuit to an instance of 3-SAT such that the Boolean circuit is satisfied if and only if the instance of 3-SAT is satisfied. How many variables and clauses do you need?
(c) Transform the instance of 3-SAT to an instance of IND-SET. Find an independent set of the appropriate size and use that to find a satisfying assignment to the variables for the instance of 3-SAT.

Problem 29.23. A problem is in the set EXP if it can be solved by a Turing Machine M with at most exponential runtime, which means for a polynomial $p(\cdot)$, the worst-case runtime of M on input w is at most $p(2^{|w|})$. Show:
(a) P $\subseteq$ NP $\subseteq$ EXP   (b) P $\subset$ EXP   (c) Either P $\subset$ NP or NP $\subset$ EXP

Problem 29.24. Show that if a problem is decided by a polynomial non-deterministic Turing Machine, the problem has a polynomial certifier. *[Hint: Use the choices made in an accepting branch of the non-deterministic computation as the evidence. To prove ⓎⒺⓈ, run the Turing Machine, with the choices given by the evidence.]*

Problem 29.25. A Turing machine has 2 states q_0, q_1, and takes at most 3 steps on an input of size 2. Let bits $s_0 s_1$ represent the state; so 10 is state q_0 and 01 is state q_1. Let $w_0 w_1 w_2 w_3$ be the bits at tape-slots 0,1,2,3 ($*$ is at slot 0) – the Turing Machine will not read or write to other slots. Let $p_0 p_1 p_2 p_3$ be the head's position, so 0100 means the head is at tape-slot 1. The *configuration* of the Turing Machine is represented by $s_0 s_1 \# w_0 w_1 w_2 w_3 \# p_0 p_1 p_2 p_3$.
(a) What is the configuration at the begining for input $w = 01$.
(b) The configuration is $01\#*11_\sqcup\#0100$. What does this mean? Build a circuit to implement the instruction:

"In state q_1 with the head at slot 1 reading '1': write '0'; move L; transition to q_0."

(The circuit takes an input configuration and outputs the next configuration.) Apply your circuit to $01\#*11_\sqcup\#0100$.

Problem 29.26 (Turing Machines and Circuits). A Turing Machine M has worst-case runtime $t(|w|)$ on input w. Show that the function computed by M on inputs of size n can be computed by a circuit with $O(t(n)^2)$ gates.

Problem 29.27. Prove that HAM-CYCLE $\leq_P$ HAM-PATH, where

HAM-CYCLE: Given a graph G, is there a Hamiltonian cycle using every vertex once?
HAM-PATH: Given a graph G, is there a Hamiltonian path using every vertex once?

(a) Consider any edge $e = (u, v)$ in G. Construct G' from G by adding vertices u', v' and edges (u', u) and (v', v). Show that there is a Hamiltonian cycle in G if and only if there is a Hamiltonian path in G'.
(b) Show that IF HAM-PATH $\in$ P THEN HAM-CYCLE $\in$ P.
(c) How many times does your solver for HAM-CYCLE use the blackbox-solver for HAM-PATH?
(d) Can you find a reduction which uses the blackbox-solver for HAM-PATH just once?

Problem 29.28. Show that the problem BOUNDED-k defined below is NP-complete by reducing every problem in NP to BOUNDED-k, just as we reduced every problem in NP to CIRCUIT-SAT.

BOUNDED-k: Given a Turing Machine M and k, is there some input w for which M halts after at most k steps?

Problem 29.29. The problem BIPARTITE is to determine if an input graph is bipartite. Show that BIPARTITE ∈ NP. Show also that BIPARTITE is polynomialy solvable and hence that 2-COLORING is in P. Does this mean P = NP?

Problem 29.30 (BALANCED-BIPARTITE-CLIQUE). Show that FREQITEMS remains NP-complete even when the popularity and basket sizes are equal. *[Hint: Exercise 29.18(b); add spurious customers who buy every item.]*
(A problem can be easier when restricted (not the case here). With this restriction, FREQITEMS is equivalent to BALANCED-BIPARTITE-CLIQUE, NP-complete problem GT24 in *Computers and Intractability* by Garey & Johnson.)

Problem 29.31. Why is PARTITION a special case of SUBSET-SUM? Nevertheless, prove that PARTITION is not easier than SUBSET-SUM, that is SUBSET-SUM $\leq_P$ PARTITION. *[Hint: To solve SUBSET-SUM(S,t) add $\sum_{x_i \in S} x_i - 2t$ to S.]*

Problem 29.32. Consider the instance of 3-SAT: $\varphi = (x_1 \vee x_2 \vee x_3)(\overline{x_1} \vee x_3)(\overline{x_1} \vee \overline{x_3})(x_1 \vee \overline{x_2} \vee \overline{x_3})$.

(a) Is φ satisfiable? Let ℓ be the number of variables, and k the number of clauses in φ. What are ℓ and k?

(b) Corresponding to φ, construct $2(\ell+k)$ numbers, each with $\ell+k$ digits. Corresponding to each variable x_i for $i = 1, \ldots, \ell$ are two numbers $a_i, \overline{a_i}$ (2ℓ numbers), and corresponding to each clause C_j for $j = 1, \ldots, k$ are two buffer numbers $b_j, \overline{b_j}$. The least significant k digits correspond to clauses and the most significant ℓ digits correspond to the variables. The digits of a_i indicate the variable and the clauses containing that variable. The digits of $\overline{a_i}$ indicate the variable and the clauses containing the negation of that variable. The digits of b_i and $\overline{b_i}$ simply indicate the clause. For φ, we partially filled a table with one row for each number.

	variables			clauses			
	x_1	x_2	x_3	c_1	c_2	c_3	c_4
a_1	1	0	0	1	0	0	1
$\overline{a_1}$	1	0	0	0	1	1	0
a_2	0	1	0	1	0	0	0
$\overline{a_2}$							
a_3							
$\overline{a_3}$							
b_1	0	0	0	1	0	0	0
$\overline{b_1}$	0	0	0	1	0	0	0
b_2	0	0	0	0	1	0	0
$\overline{b_2}$							
b_3							
$\overline{b_3}$							
b_4							
$\overline{b_4}$							
t	1	1	1	3	3	3	3

  (i) Complete the table by filling in the digits for all the numbers.
  (ii) At the bottom of the table is a target number t whose digits are ℓ 1's followed by k 3's. Find a subset of the numbers which sums to t.
  (iii) In your subset of numbers, explain why exactly one of a_i or $\overline{a_i}$ must be picked.
  (iv) Use your subset to assign $x_i = \text{T}$ if and only if a_i is in the subset.
  (v) What is the truth value of φ for the assignment you obtained.
  (vi) Prove the φ is satisfiable if and only if some subset-sum equals t.
  (vii) Generalize the construction to an arbitrary instance of 3-SAT with ℓ variables and k clauses. Hence, prove that SUBSET-SUM is NP-complete.

(c) Prove that PARTITION is NP-complete.

Problem 29.33. Consider SUBSET-SUM with set $S = \{3, 5, 3, 11, 6, 2\}$ and target $t = 9$. Build a table in which the columns are labeled by the possible subset-sums up to t, $0, 1, \ldots, t$, and the rows are labeled by the possible prefixes of S, that is $S_0 = \varnothing, S_1 = \{3\}, S_2 = \{3, 5\}, \ldots$. The entry in cell (S_i, j) is 1 if the prefix-subset S_i has a subset with sum j and 0 otherwise. We filled the first 3 rows.

	0	1	2	3	4	5	6	7	8	9
S_6										
S_5										
S_4										
S_3										
S_2	1	0	0	1	0	1	0	0	1	0
S_1	1	0	0	1	0	0	0	0	0	0
S_0	1	0	0	0	0	0	0	0	0	0

(a) Explain row S_0, and how to get row S_1 from S_0 and row S_2 from row S_1.

(b) Complete the table. How do you tell this is a (YES)-instance of SUBSET-SUM.

(c) Sketch an algorithm to solve SUBSET-SUM for a general set with n elements and target t. Show that your algorithm's runtime is polynomial in n and t.

(d) Since SUBSET-SUM is NP-complete, have you proved that P = NP?

Problem 29.34. Determine whether these two instances of 2-SAT are satisfiable,
$$\varphi_1 = (x_1 \vee x_2)(x_1 \vee \overline{x_2})(\overline{x_1} \vee x_3)(\overline{x_1} \vee \overline{x_3}) \quad \text{and} \quad \varphi_2 = (x_1 \vee x_2)(x_1 \vee \overline{x_2})(\overline{x_1} \vee x_3).$$
Construct a graph for an expression as follows. For each variable x_i, add two vertices x_i and $\overline{x_i}$. Consider satisfying a clause $(a \vee b)$. If $a = \text{F}$ then $b = \text{T}$ and if $b = \text{F}$ then $a = \text{T}$. Hence, add two directed edges $\overline{a} \to b$ and $\overline{b} \to a$.

(a) Construct the graphs G_1 and G_2 for φ_1 and φ_2 respectively.

(b) If there is a directed path from a vertex a to a vertex b and $a = \text{T}$, what can you conclude about b? Explain.

(c) In G_1, find a pair of vertices $x_i, \overline{x_i}$ that are on the same directed cycle. Hence prove that ϕ_1 is unsatisfiable.

(d) In G_2, is there a pair of vertices $x_i, \overline{x_i}$ that are on the same directed cycle?

  Use G_2 to assign truth values to the variables in φ_2 as follows. For any unassigned variable x_i, either there is no path from x_i to $\overline{x_i}$, in which case let $x_i = \text{T}$ or there is no path from $\overline{x_i}$ to x_i, in which case let $\overline{x_i} = \text{T}$. Now give T to all vertices reachable from that assigned vertex and F to their negations. Continue until all variables have been assigned. What is the assignment you get? Show that for your assignment, φ_2 is satisfied. *[Hint: To prove correctness, observe that if there is a path from a to b then there is also a path from $\overline{b}$ to $\overline{a}$.]*

(e) Prove that 2-SAT is in P. (You may assume PATH-DIR is in P.)

Problem 29.35 (Interval Graphs). Give efficient (linear time) algorithms for solving these NP-complete problems when restricted to an interval graph (see Problem 12.66). Assume that the graph is specified by a set of intervals.
  (a) IND-SET.   (b) CLIQUE.   (c) COLORING.

Problem 29.36. Give a polynomial algorithm for 2-COLORING. That is, show that 2-COLORING is in P.

Problem 29.37. Reduce the instance $\varphi = (x_1 \vee x_2 \vee x_3)(\overline{x_1} \vee x_3)$ of 3-SAT to 3-COLORING.
  (a) Start with a triangle and vertices corresponding to T, F and base B colored green, red and blue respectively. For each variable x_i, add vertices x_i and $\overline{x_i}$ and form a triangle with B. We illustrate with x_1. Give the graph after adding all variable vertices. Prove that in any valid 3-coloring of the graph, one of a variable's vertices will be green and one red.
  (b) We show an OR-gadget which corresponds to the clause $(a \vee b)$. Prove that in any valid 3-coloring of this OR-gadget, at least one of a or b must be colored green which corresponds to T and hence implies that the clause $(a \vee b)$ is T. Construct a similar OR-gadget for $(a \vee b \vee c)$ and prove it. *[Hint: $(a \vee b \vee c) = (a \vee (b \vee c))$.]*
  (c) Combine the gadgets in (a) and (b) to get a graph which is 3-colorable if and only if φ is satisfiable. Prove it.
  (d) Generalize the argument to arbitrary instances of 3-SAT and prove that 3-COLORING is NP-complete.
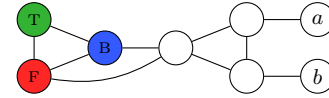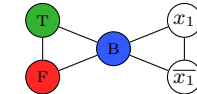
Problem 29.38. For $k > 3$, prove k-COLORING is NP-complete. *[Hint: To solve 3-COLORING add $k - 3$ vertices.]*

Problem 29.39. Use a reduction from VERTEX-COVER to show that DOM-SET is NP-complete. *[Hints: Why can you remove isolated vertices? For each edge $e = (v_i, v_j)$ add a new vertex v_{ij} and edges $(v_i, v_{ij}), (v_j, v_{ij})$.]*

Problem 29.40 (Bin Packing). Disks have capacity M and you have n files of (positive) sizes $S = \{x_1, \ldots, x_n\}$. The task is to determine if k disks will suffice to hold all the files (a file cannot be split between disks).

    BIN-PACKING(S, M, k): Can the values in S be partitioned into k bins with the sum of values in each bin at most M.

  (a) S_1 and S_2 are two instances of partition. Can the values in each set be packed into two bins of capacity 15:
    (i) $S_1 = \{3, 5, 3, 11, 6, 2\}$ (ii) $S_2 = \{3, 6, 2, 11, 6, 2\}$.
  (b) Prove that a set can be partitioned into two equal sets if and only if the values can be placed into two bins of an appropriate capacity (what is that capacity). Hence, prove that BIN-PACKING is NP-complete (even fixing $k = 2$).

Problem 29.41. Here is a greedy algorithm, first fit, to pack $x_1, \ldots, x_n$ into as few bins of capacity M as possible (see Problem 29.40). Label the bins $B_1, B_2, \ldots$. Process the values one by one, placing each value into the first available bin with enough space. Let k be the number of bins used and k_* the minimum number of bins needed.
  (a) Prove that at least $k - 1$ bins are more than half full. Hence, prove that $\sum_i x_i > M(k-1)/2$.
  (b) Prove that first fit uses at most twice the optimal number of bins, $k \leq 2k_*$.
  (c) Prove that if P $\neq$ NP, no polynomial algorithm guarantees $k < 3k_*/2$. *[Hint: Solve PARTITION.]*
  (d) FIRST FIT DECREASING processes values in decreasing order $x_1 \geq x_2 \cdots \geq x_n$. Prove that FIRST FIT DECREASING uses at most $3k_*/2$ bins. *[Hint: Suppose ℓ of the x_i exceed $M/2$. Consider the two cases $\ell \geq 2k/3$ and $\ell < 2k/3$.]*

Problem 29.42 (Knapsack). A truck has capacity c, and n packages of sizes $S = \{s_1, \ldots, s_n\}$ have corresponding values $V = \{v_1, \ldots, v_n\}$. The task is fill the truck with as much value as possible without exceeding it's capacity. As a decision problem, is there a subset of the packages having total size at most c with total value at least v?

    KNAPSACK(S, V, c, v): Is there a subset $I \subseteq [n]$ for which $\sum_{i \in I} s_i \leq c$ and $\sum_{i \in I} v_i \geq v$?

  (a) Let X be an instance of PARTITION with total sum M. Form an instance of KNAPSACK with sizes $S = X$, values $V = X$, capacity $c = M/2$ and target value $v = M/2$. Prove that the answer to PARTITION(S) is (YES) if and only if the answer to KNAPSACK$(S, S, M/2, M/2)$ is (YES). Hence, prove that KNAPSACK is NP-complete.
  (b) Use build up (dynamic programming) to sketch an algorithm for KNAPSACK with worst-case runtime poly(n, c, v).

Problem 29.43. The maximization version of KNAPSACK (Problem 29.42) asks for the maximum value of items given the capacity c. An item's efficiency is $e_i = v_i/s_i$. Order items by decreasing efficiency, $e_1 \geq e_2 \geq \cdots \geq e_n$.
  (a) In the fractional version of KNAPSACK (see Problem 29.42), one can place a fractional part of an item in the truck. Greedy picks items in order of decreasing efficiency, and the last item picked may be fractional. Prove that Greedy is polynomial and maximizes the value that can be fit into capacity c. Let the values of items picked by Greedy be $v_1, \ldots, v_k$. Prove that for non-fractional KNAPSACK, Greedy would pick $v_1, \ldots, v_{k-1}$ and possibly v_k.
  (b) Let v_* be the optimal value that can be packed into capacity c and v the value packed by Greedy. Give an example to show that v_*/v can be arbitrarily large.
  (c) Prove that $v_* \leq v_1 + v_2 + \cdots + v_k$. Hence, modify Greedy to obtain a value at least half of optimal.

Problem 29.44 (Scheduling). Each student in $S = \{s_1, \ldots, s_n\}$ is taking a subset of courses in $C = \{c_1, \ldots, c_m\}$. Each course must be assigned to one of k final exam slots such that two courses in the same final exam slot cannot have a student in common. Formulate this problem as a language and show that it is NP-complete. *[Hint: Reduce from* coloring. *Let each edge in the input graph to* coloring *be a student and each vertex a course.]*

Problem 29.45 (Integer Programming is NP-complete). An instance of 3-sat has variables $x_1, \ldots, x_\ell$. For each x_i, define a $z_i \in \{0, 1\}$. For each clause form an inequality constraint. For example $(\overline{x_1} \vee x_3)$ becomes $(1 - z_1) + z_3 \geq 1$, where if x_i is in the clause, z_i is in the constraint and if $\overline{x_i}$ is in the clause, $(1 - z_i)$ is in the constraint.
  (a) Give all the constraints for $\varphi = (x_1 \vee x_2 \vee x_3)(\overline{x_1} \vee x_3)(\overline{x_1} \vee \overline{x_3})(x_1 \vee \overline{x_2} \vee \overline{x_3})$.
  (b) Find $z_i \in \{0, 1\}$ so that all constraints are obeyed. Use the values for z_i to get a satisfying assignment for φ.
  (c) Prove that φ is satisfiable if and only if every constraint in (a) is satisfied for some $z_i \in \{0, 1\}$.
  (d) Generalize to an arbitrary instance of 3-sat and prove that determining if a set of linear inequality constraints over Boolean variables can all be simultaneously satisfied is NP-complete. (Formally define a problem int-program.)

Problem 29.46 (Solitaire). Many versions of solitaire are NP-complete. Here is a simple version. Each square on an $n \times n$ board has either a red or blue stone, or no stone. The player removes stones one-by-one, but must keep at least one stone in each row. The goal is to make each column monochromatic, having stones of only one color. The task is to determine if the game is winnable. Prove that this version of solitaire is NP-complete. *[Hint: Reduce from* 3-sat. *For an instance of* 3-sat *with variables* $x_1, \ldots, x_n$ *and clauses* $c_1, \ldots, c_m$, *if* $x_i \in c_j$ *place a blue stone in square* (c_j, x_i), *and if* $\overline{x_i} \in c_j$ *place a red stone in square* (c_j, x_i). *What do you do if* $m \neq n$?]
(Most non-trivial 2-player games (e.g. checkers/draughts, chess, go) are much harder, *requiring* exponential time to solve.)

Problem 29.47. Assume 3-sat is in P, i.e., in polynomial time one can decide if an instance of 3-sat is satisfiable. Sketch a polynomial algorithm to find a satisfying assignment for the variables. *[Hint: Try* $x_1 = $ t *or* f, *checking which gives a new* 3-sat *instance that is satisfiable. Fix* x_1 *and continue with* x_2, *and so on. Is the algorithm polynomial?]*

Problem 29.48. Assume factor is in P. Sketch a polynomial algorithm to factor an integer into its prime divisors.

Problem 29.49. Assume subset-sum is in P. Sketch a polynomial algorithm to *find* a subset with sum t.

Problem 29.50. Assume ind-set is in P. Sketch a polynomial algorithm to find a *maximum* independent set. *[Hints: First find the size of the maximum independent set; Problem 23.37.]*

Problem 29.51. Assume clique is in P. Sketch a polynomial algorithm to find a *maximum* clique.

Problem 29.52. Exact-3-sat or x3-sat is the special case of 3-sat where all clauses have exactly 3 variables.
  (a) Show that for $(\overline{z_1} \vee z_2 \vee z_3)(\overline{z_1} \vee \overline{z_2} \vee z_3)(\overline{z_1} \vee z_2 \vee \overline{z_3})(\overline{z_1} \vee \overline{z_2} \vee \overline{z_3})$ to be satisfied, z_1 must be f.
  (b) Show, by a reduction from 3-sat that x3-sat is NP-complete.

Problem 29.53. Prove that any instance of x3-sat (see Problem 29.52) with fewer than 8 clauses is satisfiable.

Problem 29.54. Consider an instance φ of 3-sat with n variables $\mathbf{x} = x_1, \ldots, x_n$ and m clauses.
  (a) Sketch a deterministic brute force algorithm with $O(m2^n)$ steps by trying all possible assignments to the variables.
  (b) Suppose that φ is satisfiable and let $\boldsymbol{\alpha} = \alpha_1 \alpha_2 \cdots \alpha_n$ be a satisfying assignment. Pick a random assignment $\mathbf{x}$
    (i) Let A_k be the event that $\mathbf{x}$ has k disagreements with $\boldsymbol{\alpha}$. Show that $\mathbb{P}[A_k] = \binom{n}{k}2^{-n}$.
    (ii) Repeat up to n times if the current assignment does not satisfy φ: pick any unsatisfied clause and flip the bit of a random variable in the clause. Show that with probability at least $1/3$, the number of disagreements between $\boldsymbol{\alpha}$ and $\mathbf{x}$ decreases by 1.
    (iii) Given A_k, show that if the first k flips in (ii) are successful, increasing the agreement with $\boldsymbol{\alpha}$ by 1 each time, then you succesfully find a satisfying assignment. Use total probability and the binomial theorem to prove:
    $$\mathbb{P}[\text{success}] \geq 2^{-n} \sum_{k=0}^{n} \binom{n}{k} 3^{-k} = (2/3)^n.$$
    (iv) Try t times to get success. Give a t so that $\mathbb{P}[\text{no successes}] \leq 1/n^{100}$.
  (c) Give a randomized decider M for 3-sat with the following properties on an instance φ.
    (i) If φ is unsatisfiable, M says $\overline{\text{NO}}$. If φ is satisfiable, M says $\overline{\text{YES}}$ with probability at least $1 - 1/n^{100}$.
    (ii) The worst-case runtime of M is $\text{polynomial}(n) \times (3/2)^n$. What is your $\text{polynomial}(n)$?
(Repeat up to $3n$ times in (b)(ii) and consider at least $2k$ improvements to $\mathbf{x}$ in the first $3k$ flips. This gives a $\text{polynomial}(n) \times (4/3)^n$ runtime. The best known is $\text{polynomial}(n) \times 1.31^n$ runtime.)

Problem 29.55. Let φ be an instance of 3-SAT with n variables $x_1, \ldots, x_n$ and m clauses. Even if φ is unsatisfiable, one often wants to maximize the number of satisfied clauses (e.g. to maximize the number of constraints satisfied).

(a) Show that one of the assignments all $x_i = $ T or all $x_i = $ F satisfies at least half the clauses. *[Hint: Pigeonhole.]*

(b) One can do better. For simplicity, let φ be an instance of X3-SAT (every clause has 3 terms). Assign each variable randomly to T or F. Find the expected number of satisfied clauses and show that some assignment satisfies at least $(7/8)$-th of the clauses.

(c) Sketch an algorithm to satisfy at least $(7/8)$-th of the clauses in any instance of X3-SAT. *[See also Problem 20.68.]*

Problem 29.56 (Boolean Games). A Boolean game is based on a Boolean formula $Q(x_1, x_2, \ldots, x_n)$ with n variables $x_1, x_2, \ldots, x_n$. Alice sets T/F for x_1, then Bob sets T/F for x_2, then Alice sets T/F for x_3, and so the game continues until all variables are set. Alice wins if at the end the Boolean formula is T. Assume players are optimal.

(a) Show that Alice wins for $Q(x_1, x_2, x_3) = (x_1 \vee x_2) \wedge (x_2 \vee x_3) \wedge (\overline{x_2} \vee \overline{x_3})$. True or false: $\exists x_1 \forall x_2 \exists x_3 : Q(x_1, x_2, x_3)$.

(b) Show that Bob wins for $Q(x_1, x_2, x_3) = (x_1 \vee x_2) \wedge (x_2 \vee x_3) \wedge (x_2 \vee \overline{x_3})$. True or false: $\exists x_1 \forall x_2 \exists x_3 : Q(x_1, x_2, x_3)$.

(c) For a general Q, show that Alice wins if and only if $\exists x_1 \forall x_2 \exists x_3 \forall x_4 \cdots : Q(x_1, x_2, \ldots, x_n)$ is true.

(More generally a quantified Boolean formula (QBF) is in prenex normal form if all quantifiers are listed first. Alice sets existentially quantified variables and Bob sets universaly quantified variables. The order of play is the order in which the variables appear. Determining if Alice wins amounts to determining if the QBF is true, known as the TQBF problem. It is not known whether TQBF is in NP.)

Problem 29.57 (Zero Knowledge Proof (ZKP)). The ATM-setting in Problem 17.42 requires a test which you can pass with the password but which you pass or fail randomly without the password. The important requirement is that when you pass the test with the password, you should give the ATM no knowledge about your password. That is the hard part. Analyze the following approach to such a test that uses an NP-hard problem (we choose CLIQUE).

Your "account number" is a large graph $G = (V, E)$ with n vertices, e.g. $n = 1000$ in which there is a clique C of size $n/2$. Your password is the clique C. Both you and the ATM know the graph G. Only you know the password C. When you arrive at the ATM, here is the test you will face.

1: You construct a random isomorphism which randomly permutes the vertices and correspondingly relabels the edges of G. The isomorphism is a function $f : V \mapsto V$.

2: You apply f to G, constructing the adjacency matrix of the transformed graph. You *commit* to this adjacency matrix, i.e. it cannot be changed. The clique in the transformed graph is $f(C)$.

3: The ATM randomly tests you by asking you to do one of two things:

    (i) Reveal all entries of the transformed adjacency matrix and the isomorphism f. The ATM has the original graph G, and so can verify if f is an isomorphism, in which case you pass the test.

    (ii) Reveal the edges in the transformed adjacency matrix involving all vertices in the clique $f(C)$. The user *does not* reveal f. If all revealed edges are 1, you pass the test.

(a) Even though the ATM knows the graph G, explain why your passward is "safe".

(b) Why don't you reveal any information about the password, when you answer either of the two tests correctly?

(c) One way for an imposter with your ATM-card (i.e. the graph G) to try to get access to your money is to commit to the adjacency matrix which is all 1. What is the probability the imposter wins?

(d) Alternatively, the imposter commits to a random isomorphism, and if asked to reveal the clique, he randomly picks vertices. Which test might the imposter fail. Give an upper bound on the probability the imposter wins.

(Some critical issues with regard to implementing the scheme above are: (i) How does the user generate their account graph G with an embedded clique C of size $n/2$ which they know through the process of generating the G, but which is hard to find given only the graph G. (ii) In the test the user must *commit* to the transformed adjacency matrix. A separate cryptographic protocol exists to ensure that the user cannot change the edges after commitment (otherwise an imposter can easily pass the test). (iii) One must also ensure that after the user reveals clique edges, the ATM cannot access anything that the user did not reveal (the isomorphism or unrevealed edges in the transformed adjacency matrix), otherwise information about the password gets leaked. Again, standard cryptographic protocols can be used here.)