Chapter 30

Solutions to Quizes & Exercises

Do the quizzes and exercises by yourself. When you get stuck, take a peak here.

Chapter 0

Numbers and Sets.

1. $252 = 2 \times 2 \times 3 \times 3 \times 7$.
2. minimum is 3.
3. union $= \{1, 3, 7, 8, 9, 10, 19\}$; intersection $= \{3, 10\}$.
4. Yes, there must be a minimum element and the minimum is at most 18.
5. 5 (integer, rational, real); $\frac{3}{4}$ (rational, real); π (real).
6. $3k$, $3k + 3$.
7. (i) In base 3, $3^3 + 2 \times 3^2 + 3^1 + 2 * 3^0 = 50$. (ii) In base 4, $4^3 + 2 \times 4^2 + 4^1 + 4 * 4^0 = 102$.

Logarithms and Exponentials.

1. $\ln(12) = \ln(2 \times 2 \times 3) = \ln(2) + \ln(2) + \ln(3) \approx 2.484$.
2. $2^{20} = (2^{10})^2 \approx 1000^2 = 10^6$.
3. $\ln(1 \times 2 \times 3 \times \cdots \times 10) = (\ln 1 + \ln 2 + \ln 3 + \cdots + \ln 10)$.
4. How are $2^a/2^b = 2^{a-b}$. $2^0 = 1$.
5. By definition of $\log_{10}$, $100 = 10^{\log_{10} 100}$. Taking $\log_2$ of both sides, $\log_2 100 = \log_2(10^{\log_{10} 100}) = \log_{10} 100 \times \log_2 10$. More generally, $x = \beta^{\log_\beta x}$; taking $\log_\alpha$ of both sides, $\log_\alpha x = \log_\beta x \times \log_\alpha \beta$.

Sums and Products.

1. (a) $1 + \cdots + 1000 = \frac{1}{2} \times 1000 \times 1001 = 500,500$. (b) $1 + \cdots + n = \frac{1}{2} n(n+1)$. (c) $1 + \frac{1}{7} + \frac{1}{7^2} + \frac{1}{7^3} + \cdots = \frac{1}{1 - \frac{1}{7}} = \frac{7}{6}$.
2. $5! = 20$; $n! = n \times (n-1) \times (n-2) \times \cdots \times 2 \times 1$; $0! = 1$.
3. $\sum_{i=1}^{1000} i = \sum_{k=1}^{1000} k = \frac{1}{2} \times 1000 \times 1001 = 500,500$. $\sum_{k=1}^{1000} i = 1000 \times i$. $\sum_{|i-1| \le 5} i = \sum_{i=-4}^{6} i = 11$.
4. $1 + 2 + 3 + \cdots + k = \sum_{i=1}^{k} i = \frac{1}{2} k(k+1)$. $\sum_{k=1}^{n} k = \frac{1}{2} n(n+1)$.
5. $\sum_{i=1}^{k} \ln(i) = \ln(k!)$; $\prod_{i=1}^{k} i = k!$.

Algebra.

1. $(1+2)^2 = 3^2 = 9$. Also, $(1+2)^2 = 1^2 + 2 \times 1 \times 2 + 2^2 = 9$.
2. $(a+b)^2 = a^2 + 2ab + b^2$; $(a+b)^3 = a^3 + 3a^2 b + 3ab^2 + b^3$; $(a+b)^4 \neq a^4 + 4a^3 b + 4a^2 b^2 + 4ab^3 + b^4$.
3. $x^2 - 5x - 6 = (x-6)(x+1) = 0$, therefore the roots are $x = 6$ and $x = -1$
4. To get solutions to $e^{2x} - 5e^x - 6 = 0$, set $y = e^x$; then $y^2 - 5y - 6 = 0$ and (from the previous problem) $y = e^x = 6$ or $y = e^x = -1$. So, $x = \ln 6$ or $x = i\pi$ where $i = \sqrt{-1}$. Other solutions are obtained by adding $2k\pi i, k \in \mathbb{Z}$.
5. $x + y = 2$ and $2x + 3y = 7$ implies $x = -1$ and $y = 3$.
6. $\frac{3x+11}{x^2-x-6} = \frac{4}{x-3} - \frac{1}{x+2}$ and $\frac{3x+11}{x^2+6x+9} = \frac{3}{x+3} + \frac{2}{(x+3)^2}$.

Calculus.

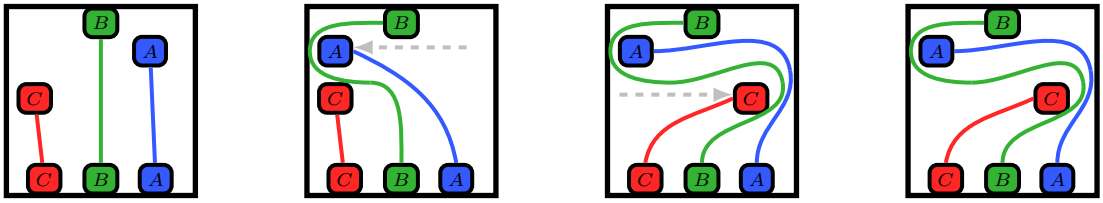
1.

$1 + 2 + 2^2 + 2^3 + 2^4 + \cdots$	diverges
$1 + \frac{1}{2} + (\frac{1}{2})^2 + (\frac{1}{2})^3 + (\frac{1}{2})^4 + \cdots$	converges to 2
$1 - 1 + 1 - 1 + 1 - 1 + 1 - 1 + \cdots$	diverges
$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots$	diverges
$1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \frac{1}{5} - \frac{1}{6} + \cdots$	converges to approx. 0.6931

2. Derivatives: $3x^2$; $2e^{2x}$; $2^x \ln 2$; $-1/x^2$; $-2/x^3$; $1/x$; $1/x \ln 2$; $1/x$.
3. Integrals: $x^4/4$; $e^{2x}/2$; $2^x/\ln 2$; $\ln|x|$; $-1/x$.
4. Limits as $x \to 0$: $\frac{e^x-1}{\sin(2x)} \xrightarrow{x\to 0} \frac{1}{2}$; $\frac{e^x-1}{1+x} \xrightarrow{x\to 0} 0$; $\frac{e^x-1}{\sin(x^2)} \xrightarrow{x\to 0} \infty$; $\frac{e^x-1}{x+x^2} \xrightarrow{x\to 0} 1$; $\frac{e^x-1}{e^{2x}-1} \xrightarrow{x\to 0} \frac{1}{2}$.
5. Limits as $x \to \infty$: $\frac{e^x-1}{e^{2x}-1} \xrightarrow{x\to\infty} 0$; $\frac{e^x-1}{x^3+2e^x} \xrightarrow{x\to\infty} \frac{1}{2}$; $\frac{e^x}{x^x} \xrightarrow{x\to\infty} 0$.
6. $f(x) = \frac{1}{2+\sin(x)} = \frac{1}{3} + \frac{1}{18}(x-\frac{\pi}{2})^2 + \frac{1}{216}(x-\frac{\pi}{2})^4 + \frac{1}{6480}(x-\frac{\pi}{2})^6 + \cdots$.
7. Using the substitution $u = \arctan(x)$, $du = dx/(1+x^2)$ and so $\int_0^T dx\ \frac{1}{1+x^2} = \arctan(T)$.
8. For $f(t) = \int_0^t dx\ \sin(1+x^2e^x)$, $\frac{d}{dt}f(t) = \sin(1+t^2e^t)$.

Pop Quiz 0.1. A powerful tactic when a problem looks hard is to make it easier. Suppose the letters lined up vertically. That's trivial. Now morph this simple problem into the one we want.

Easier problem | Modify: move A | Modify: move C | Solution.



Do not underestimate the power of simplification, the technique of making a problem easier: **tinker**. It helps to understand a problem, build confidence (by solving *something*) and can pinpoint the difficulty in the harder problem.

Chapter 1

Pop Quiz 1.1. The red square is safe. The final infection is on the right.

Exercise 1.2. Six infections won't infect the whole grid; seven is the minimum.

Exercise 1.3. (1995 Russian Mathematics Olympiad) The title serves as a hint. Tinker! No matter what heavy lifting you do when you end in the start configuration the total payment is 0. In such problems, it can help to find something that does not change, an *invariant*. Suppose a box has n stones. The revenue the box can generate by repeatedly removing coins is $(n-1)+(n-2)+\cdots+2+1$. Yes, there is a cost related to which box the coins will go, but for the moment we look only at the revenue. We won't need to compute this sum. We only need to observe that it is a function $R(n)$, which depends only on n. If a stone leaves a box with n stones, the potential revenue drops by $n-1$. Similarly, if a stone enters a box with n stones, its potential revenue increases by n. Let the boxes contain a, b and c. Let us compute the change in potential revenue if you move a stone from a to b.

$$R(a)+R(b)+R(c) \to R(a)-(a-1)+R(b)+b+R(c) = R(a)+R(b)+R(c)+b-a+1.$$

The payment for this move is $a-1-b$, which exactly offsets the change in the total revenue. We often use Δ to indicate change. Let R_1, R_2, R_3 be the revenue potential of the three boxes, and W your wealth. Then, in any move,

$$\Delta(R_1+R_2+R_3+W) = 0$$

The start and end configuration are the same, so $R_1+R_2+R_3$ is unchanged. Hence your wealth must stay 0.

Chapter 2

Pop Quiz 2.1. $O = \{n \mid n = 2k-1;\ k \in \mathbb{N}\}$

Exercise 2.2. True because {pigs that fly} is empty, hence it is a subset of {things which are green with purple spots}.

Pop Quiz 2.3. $M \cap V = \{a, i\}$; $M \cup V = \{m, a, e, i, k, l, o, u\}$. With $U = \{a, b, \ldots, z\}$, $\overline{M} = \{b, c, \ldots, h, j, n, o, \ldots, z\}$.

Exercise 2.4. (a) Drawings look different. (b) Friendships are the same, so it can be the same network.

Pop Quiz 2.5. A graph. The people on the grid are linked if they are neighbors. The EBOLA spreads along links.

Exercise 2.6.(a) $\{-1, -2, \ldots\} = \{n \mid n = -k;\ k \in \mathbb{N}\}$ (b) $\{1, \frac{1}{2}, \frac{1}{3}, \ldots\} = \{r \mid r = \frac{1}{n};\ n \in \mathbb{N}\}$

Chapter 3

Pop Quiz 3.1.

(a) Tough to verify. Ask A for a soul mate and check if $B, \ldots, F$ have that same soul mate. If not, ask A for another and repeat. Either A runs out of soul mates, or you verify the claim. (Assumes A has a finitely many soul mates.)

(b) Every American has their own dream, or there's one "American dream" for everyone (house, 2 cars, 3 kids,...).

Exercise 3.2. (a) F. (b) Don't know yet. (c) Who is Kilam? (d) T.

Exercise 3.3. $p \wedge r$: It is raining and it is cloudy (F; it can be cloudy without rain).
$p \to q$: If it is raining then Kilam has his umbrella (T; Kilam is a smart guy).
$p \to r$: If it is raining then it is cloudy (T; you need clouds for rain).
$q \to r$: If Kilam has his umbrella then it is cloudy (T; why does Kilam have an umbrella?).
$q \to p$: If Kilam has his umbrella then it is raining (F as it could just be cloudy).
$r \to p$: If it is cloudy then it is raining (F it can be cloudy without rain).

Exercise 3.4.
(a) T; (i) Yes, it is cloudy. (ii) No, it is clear.
(b) F; (i) We don't know if it is raining.
(c) T; (i) Yes. (ii) Don't know; you could just be smart. (iii) Don't know. (iv) No.
(d) T; (i) Yes. (ii) Don't know; you could just be wandering. (iii) Not hungry; not thirsty.

Pop Quiz 3.5. In C^{++}, || is OR, and && is AND. To show that both codes execute the instructions for the same x, y values, define the propositions $p:\ x > 0$, $q:\ y > 1$ and $r:\ x < y$.

The left code tests $p \vee (q \wedge r)$ before executing the instructions, and the right tests $p \vee q$. We show their truth-tables (right). The highlighted row 3 is a problem. The truth values are different. Let's examine closer: p is F, $x \leq 0$; q is T, $y > 1$; and, r is F, $x \geq y$. This row in the truth-table is *impossible*: $x \leq 0$ and $y > 1$ implies $x < y$, so r is T. To compare compound propositions, you only need to consider all the *possible* truth values of the basic propositions. If the basic propositions are independent all 8 possibilities are relevant: $p \vee (q \wedge r)$ is not equivalent to $p \vee q$ in general. In our case, p, q, r being F,T,F is *not possible*: our basic propositions are *not* independent because the truth value of r is constrained by the truth values of p and q.

	p	q	r	$p \vee (q \wedge r)$	$(p \vee q)$
1.	F	F	F	F	F
2.	F	F	T	F	F
3.	F	T	F	F	T
4.	F	T	T	T	T
5.	T	F	F	T	T
6.	T	F	T	T	T
7.	T	T	F	T	T
8.	T	T	T	T	T

For all *possible* truth values of p, q, r, the compound propositions match, so the two snipets perform identical computations. The right snipet is simpler, uses fewer operations and requires fewer gates (important in some applications).

Exercise 3.6. $\neg p \to q \overset{\text{eqv}}{\equiv} \neg q \to p \overset{\text{eqv}}{\equiv} p \vee q$ $\qquad$ $\neg(p \vee q) \overset{\text{eqv}}{\equiv} \neg p \wedge \neg q$

$(q \wedge \neg r) \to \neg p \overset{\text{eqv}}{\equiv} (\neg p \vee \neg q) \vee r \overset{\text{eqv}}{\equiv} (p \wedge q) \to r$ $\qquad$ $p \vee (q \vee r) \overset{\text{eqv}}{\equiv} \neg r \to (p \vee q)$

Pop Quiz 3.7. (a) $n \in \mathbb{N}$. (b) A predicate cannot be T or F. (c) "4 is a perfect square." (d) $P(4)$ and $P(9)$ are T.

Exercise 3.8.
(a) $P(x) =$ "x has grey hair". P(Kilam).
(b) $P(x) =$ "Map x can be colored with 4 colors with adjacent countries having different colors". $\forall x : P(x)$.
(c) $P(n) =$ "Integer n is a sum of two primes.". $\forall n \in E : P(n)$ (E is set of even natural numbers).
(d) $P(x) =$ "x has blue eyes and blond hair". $\neg\exists x : P(x)$. Another way to formulate the statement with predicates is: $P(x) =$ "x has blue eyes;" $Q(x) =$ "x has blonde hair." $\neg\exists x : P(x) \wedge Q(x)$.

Exercise 3.9.
$(\exists a : G(a)) \wedge (\exists a : H(a))$: someone has blue eyes and someone has blonde hair.
$(\exists b : G(b)) \wedge (\exists c : H(c))$: someone has blue eyes and someone has blonde hair. A quantified statement does not change when you change the name of a (variable) parameter.
$(\exists a : G(a)) \wedge H(c)$: "someone has blue eyes and c has blond hair." (A predicate, not a statement.) To make it a statement, specify a *value* for c.

Exercise 3.10.
(a) (i) $\forall a : (\forall b : P(a, b))$: Every person a has every person b as soul mate.
$\forall b : (\forall a : P(a, b))$: Every person b is soul mate to every person a. (Both are equivalent)
(ii) $\exists a : (\exists b : P(a, b))$: Some person has a soul mate.
$\exists b : (\exists a : P(a, b))$: Some person is soul mate to someone. (Both are equivalent)
(b) They are valid predicates. In English: $Q(a) = \exists b : P(a, b) =$ "Some person is soul mate to a"
$R(b) = \forall a : P(a, b) =$ "All people have b as soul mate"
Rewriting using Q and R, (3.2) is $\exists b : (\forall a : P(a, b)) = \exists b : R(b)$, and (3.3) is $\forall a : (\exists b : P(a, b)) = \forall a : Q(a)$

Exercise 3.10. Add a requirement that two people satisfying the soul mate condition must be equal,

$$\forall a : ((\exists b : P(a, b)) \wedge (\forall x, y : P(a, x) \wedge P(a, y) \to x = y))$$

Exercise 3.12. Easier to disprove (a): find a single n for which $2^{2^n} + 1$ is not prime. To disprove (b), show that for every choice of (a, b, c), $a^3 + b^3 \neq c^3$. *Disproving* a "there exists" is typically harder than disproving a "for all".

Similarly proving "for all" is harder than proving "there exists". This is because $\neg\exists x : P(x) \overset{\text{eqv}}{\equiv} \forall x : \neg P(x)$. So, showing "there exists" is false means showing a "for all" is true. Similarly $\neg\forall x : P(x) \overset{\text{eqv}}{\equiv} \exists x : \neg P(x)$.

Chapter 4

Pop Quiz 4.1.

(a) $p : n$ is greater than 2 and even — $q : n$ is the sum of two primes

(b) $p : x$ and y are rational — $q : x + y$ is rational

(c) $p : ax^2 + bx + c = 0$ and $a \neq 0$ — $q : x = (-b + \sqrt{b^2 - 4ac})/2a$ or $x = (-b - \sqrt{b^2 - 4ac})/2a$

Exercise 4.2.

(a) *Proof.* We use a direct proof.

1: Assume that a is divisible by b and b is divisible by c.
2: This means there are integers k, ℓ for which $a = kb$ and $b = \ell c$.
3: Then, $a = kb = k\ell c = mc$, where $m = k\ell$.
4: Since $m = k\ell$ is an integer, a is divisible by c, as was to be shown. ∎

(b) A proof does not have to be written in algorithmic steps.

Proof. Let x and y be arbitrary real numbers. First observe that $\pm x \leq |x|$ and $\pm y \leq |y|$. There are two cases: (i) $x + y \geq 0$, in which case $|x + y| = x + y \leq |x| + |y|$ (because $x \leq |x|$ and $y \leq |y|$). (ii) $x + y < 0$, in which case $|x + y| = -(x + y) = -x - y \leq |x| + |y|$ (because $-x \leq |x|$ and $-y \leq |y|$). In both cases $|x + y| \leq |x| + |y|$. ∎

(c) *Proof.* Consider any four consecutive integers $x, x + 1, x + 2, x + 3$. One of these four must be divisible by 4, and so equals $4k$. Among the remaining numbers, two are consecutive so one is divisible by 2 and so equals 2ℓ. Therefore the product of all four numbers is $4k \times 2\ell \times$ (integer), a multiple of 8. ∎

The proof is subtle. We ask the reader to prove by cases. Let r be the remainder when x is divided by 4, $x = 4k + r$ where $r \in \{0, 1, 2, 3\}$. Show that in each of the four cases for r, the product is divisible by 8. For example, if $x = 4k$ the product is $4k(4k + 1)(4k + 2)(4k + 3) = 8k(4k + 1)(2k + 1)(4k + 3)$.

Pop Quiz 4.3. You need to find one $n^* \in \mathcal{D}$ for which $Q(n^*)$ is F. Equivalent to disproving: IF $n \in \mathcal{D}$, THEN $Q(n)$.

Exercise 4.4.

(a) The two truth-tables are identical. The only way $p \to q$ is F is with p T and q F. The only case $\neg q \to \neg p$ is F is with $\neg q$ T and $\neg p$ F, i.e. with p T and q F.

(b) (i) IF the grass is not wet, THEN it did not rain last night.
(ii) IF you do not stay at home, THEN the mall is not crowded.

(c) (i) Contrapositive IF $x \leq 10$ and $y \leq 10$, THEN one of x, y is not positive or $xy \leq 100$.
Proof. (By contrposition) Suppose $x \leq 10$ and $y \leq 10$ (the consequent is false). There are two cases.
Case 1: One of x, y is not positive in which case the antecendent p is F.
Case 2: Both x, y are positive, so $0 < x, y \leq 10$. In this case $xy \leq 10 \times 10 = 100$ and the antecedent p is F. ∎

(ii) Contrapositive: IF $\sqrt{r}$ is rational THEN r is rational.
Proof. (By contraposition) Suppose $\sqrt{r}$ is rational (the consequent is false). Then $\sqrt{r} = a/b$ for integer a and natural number b. This means $r = a^2/b^2$ which is rational because a^2 is an integer and b^2 is a natural number. Hence the antecedent is false. ∎

Pop Quiz 4.5. The truth-tables are the same: $p \leftrightarrow q \overset{\text{eqv}}{\equiv} (p \to q) \wedge (q \to p)$ (logically equivalent).

Exercise 4.6.

(a) ⁄ ——— (Do not intersect, but not parallel according to the valid definition.)

(b) (a) Two line segments (in 3-dimensions) are parallel if and only if they both lie in the same plane and when both are extended to infinity in both directions, there is no point of intersection.
(b) A triangle is isosceles if and only if at least two sides have the same length.

Exercise 4.7.

(a) To get a contradiction, suppose there are $m, n \in \mathbb{Z}$ with $21m + 9n = 3(7m + 3n) = 1$. 3 divides the LHS, therefore 3 divides 1. **FISHY**! This contradiction proves the claim.

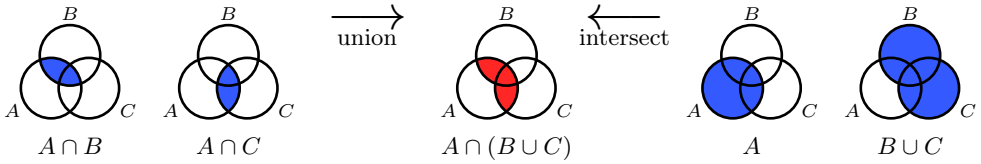
(b) Suppose $x, y > 0$ and $x + y < 2\sqrt{xy}$. Both sides of the inequality are positive. Squaring, $(x + y)^2 < 4xy$, or $x^2 + 2xy + y^2 < 4xy$, or $x^2 - 2y + y^2 < 0$ or $(x - y)^2 < 0$. This is **FISHY** because the square of a real numnber cannot be negative. This contradiction proves the claim. ∎

(c) Suppose that m and n are both odd, $m = 2k + 1$ and $n = 2\ell + 1$. $m^2 + n^2 = 4k^2 + 4k + 1 + 4\ell^2 + 4\ell + 1$. Since $m^2 + n^2$ is divisible by 4, $m^2 + n^2 = 4s$, therefore $4s = 4(k^2 + k + \ell^2 + \ell) + 2$, or $4(s - k^2 - k - \ell^2 - \ell) = 2$ or $2(s - k^2 - k - \ell^2 - \ell) = 1$. This means 1 is divisible by 2, **FISHY**. This contradiction proves the claim. ∎

Exercise 4.8.
(a) Direct proof because the result clearly follows from the assumption that x is real.
(b) Contraposition, for if n is even (not odd), then it is easy to show by algebra that n^2 is odd.
(c) Direct proof because by simple algebra if n is odd one can square and show n^2 is even.
(d) Show an example of a number that is not a square and prove it.
(e) Direct proof because, by simple algebra, a product of two ratios is a ratio.
(f) Direct proof. By simple algebra one can show that a product of two odd numbers is odd.
(g) Contradiction. This gives something to start with by assuming $\sqrt{6} = p/q$. Now find *any* contradiction.
(h) When the path is unclear try contradiction, because it gives you something to work with.
Proof. Let $x_1, \ldots, x_n$ be arbitrary numbers and let $\mu = (x_1 + \cdots + x_n)/n$ be the average, so that $x_1 + \cdots + x_n = n\mu$. Now assume that every $x_i < \mu$ (to obtain a contradiction). Then $x_1 + \cdots + x_n < \mu + \cdots + \mu = n\mu$. This is a contradiction. Therefore, not every $x_i < \mu$, so at least one number is as large (or larger) than the average μ. ∎
Commit this important fact to memory. Some number is as large as the average. What *larger* than the average?

Pop Quiz 4.9. We prove $x \in A \cap B \to x \in C$ by direct proof. Assume $x \in A \cap B$. Then $x \in A$ *and* $x \in B$, so x is even and $x = 9k$. If k is odd, then x is the product of two odd numbers which is odd. Therefore, k is even (to make x even). So, $k = 2n$, which means $x = 18n = 6 \cdot (3n)$, a multiple of 6. Therefore, $x \in C$, which concludes the proof.

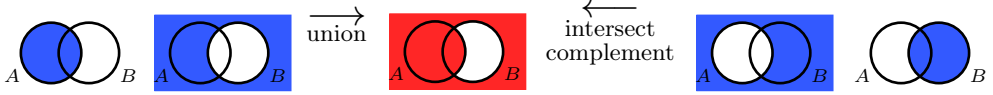
Exercise 4.10.
(a) $(A \cap B) \cup (A \cap C) = A \cap (B \cup C)$:



$A \cap B$ $\quad A \cap C$ $\quad A \cap (B \cup C)$ $\quad A$ $\quad B \cup C$
$(A \cap B) \cup (A \cap C)$

Suppose $x \in (A \cap B) \cup (A \cap C)$. Then either $x \in A$ and $x \in B$ or $x \in A$ and $x \in C$. In both cases, $x \in A$ and $x \in B \cup C$ so $x \in A \cap (B \cup C)$. Now suppose $x \in A \cap (B \cup C)$. Then $x \in A$ and either $x \in B$ or $x \in C$. If $x \in B$, then $x \in (A \cap B)$ and so $x \in (A \cap B) \cup (A \cap C)$. Similarly, if $x \in C$, then $x \in (A \cap C)$ and so $x \in (A \cap B) \cup (A \cap C)$.

(b) $A \cup \overline{B} = \overline{\overline{A} \cap B}$:



A $\quad \overline{B}$ $\quad A \cup \overline{B},\ \overline{\overline{A} \cap B}$ $\quad \overline{A}$ $\quad B$

Suppose $x \in A \cup \overline{B}$ This means $x \in A$ or $x \in \overline{B}$. $x \in A \to x \notin \overline{A} \to x \notin \overline{A} \cap B \to x \in \overline{\overline{A} \cap B}$; $x \in \overline{B} \to x \notin B \to x \notin \overline{A} \cap B \to x \in \overline{\overline{A} \cap B}$. In both cases, $x \in \overline{\overline{A} \cap B}$.

Now, suppose $x \in \overline{\overline{A} \cap B}$, that is $x \notin \overline{A} \cap B$. So either $x \notin \overline{A}$ or $x \notin B$. $x \notin \overline{A} \to x \in A \to x \in A \cup \overline{B}$; $x \notin B \to x \in \overline{B} \to x \in A \cup \overline{B}$. In both cases, $x \in A \cup \overline{B}$.

Exercise 4.11. We must prove a set equality, which is an if and only if.

First, suppose $x \in f^{-1}(C \cup D)$. Then, $f(x) = C \cup D$. If $f(x) \in C$, then $x \in f^{-1}(C)$; otherwise $f(x) \in D$ and $x \in f^{-1}(D)$. In either case, $x \in f^{-1}(C) \cup f^{-1}(D)$.

Second, suppose $x \in f^{-1}(C) \cup f^{-1}(D)$. If $x \in f^{-1}(C)$, then $f(x) \in C \to f(x) \in C \cup D$, which means $x \in f^{-1}(C \cup D)$. Otherwise $x \in f^{-1}(D)$ and $f(x) \in D \to f(x) \in C \cup D$ which means $x \in f^{-1}(C \cup D)$. In either case, $x \in f^{-1}(C \cup D)$.

We have proved $x \in f^{-1}(C \cup D) \leftrightarrow x \in f^{-1}(C) \cup f^{-1}(D)$, which proves the set equality. ∎

Chapter 5

Pop Quiz 5.1. Yes. When could a boy have entered the line? If the first boy is at position $k > 1$, then at $k - 1$ is a girl. But behind that girl must be a girl, not a boy.

Exercise 5.2.
(a) $S(n)$ is a sum of integers so it is an integer, call it k.
(b) By the high-school geometric sum formula: $1 + 4 + 4^2 + \cdots + 4^{n-1} = (4^n - 1)/(4 - 1) = (4^n - 1)/3$.
(c) Therefore $k = (4^n - 1)/3$, or $4^n - 1 = 3k$. That is, $4^n - 1$ is divisible by 3.

Exercise 5.3. (a) $n \geq 2$ (b) $n \geq 0$ (c) $n = 0, 1$ (d) $n \geq 1$ (e) $n \geq 1$

Exercise 5.4.
(a) Define the claim $P(n) : \sum_{i=1}^{n-1} a + id = na + \frac{1}{2}n(n-1)d$.

1: **[Base case]** $P(1)$ claims that $a = a$, which is clearly T.

2: **[Induction step]** We show $P(n) \to P(n+1)$ for all $n \geq 1$, using a direct proof.
Assume (induction hypothesis) $P(n)$ is T*:* $\sum_{i=1}^{n-1} a + id = na + \frac{1}{2}n(n-1)d$.
Show $P(n+1)$ is T*:* $\sum_{i=1}^{n} a + id = (n+1)a + \frac{1}{2}(n+1)(n)d$.
We compute the sum $\sum_{i=1}^{n} a + id$ as follows:

$$\begin{aligned}\sum_{i=1}^{n} a + id &= a + nd + \sum_{\boldsymbol{i=1}}^{\boldsymbol{n-1}} \boldsymbol{a + id} \\ &\overset{\text{IH}}{=} a + nd + \boldsymbol{na + \frac{1}{2}n(n-1)d} \\ &= (n+1)a + \tfrac{1}{2}(n(n-1) + 2n)d \;=\; (n+1)a + \tfrac{1}{2}(n+1)nd\end{aligned}$$

(IH stands for "by the induction hypothesis"). We have shown $P(n+1)$ is T, as needed.

3: By induction, $P(n)$ is T $\forall n \geq 1$. ∎

(b) Define the claim $P(n) : \sum_{i=1}^{n-1} ar^i = a(r^n - 1)/(r-1)$.

1: **[Base case]** $P(1)$ claims that $a = a$, which is clearly T.

2: **[Induction step]** We show $P(n) \to P(n+1)$ for all $n \geq 1$, using a direct proof.
Assume (induction hypothesis) $P(n)$ is T*:* $\sum_{i=1}^{n-1} ar^i = a(r^n - 1)/(r-1)$.
Show $P(n+1)$ is T*:* $\sum_{i=1}^{n} ar^i = a(r^{n+1} - 1)/(r-1)$.
We compute the sum $\sum_{i=1}^{n} ar^i$ as follows:

$$\sum_{i=1}^{n} ar^i = ar^n + nd + \sum_{\boldsymbol{i=1}}^{\boldsymbol{n-1}} \boldsymbol{ar^i} \overset{\text{IH}}{=} ar^n + \frac{\boldsymbol{a(r^n-1)}}{\boldsymbol{r-1}} \;=\; \frac{a(r^{n+1} - r^n + r^n - 1)}{r-1} \;=\; a(r^{n+1} - 1)/(r-1).$$

We have shown that $P(n+1)$ is T, as needed.

3: By induction, $P(n)$ is T $\forall n \geq 1$. ∎

(c) Define the claim $P(n) : n \leq 2^n$.

1: **[Base case]** $P(1)$ claims that $1 \leq 2^1$, which is clearly T.

2: **[Induction step]** We show $P(n) \to P(n+1)$ for all $n \geq 1$, using a direct proof.
Assume (induction hypothesis) $P(n)$ is T*:* $n \leq 2^n$.
Show $P(n+1)$ is T*:* $n + 1 \leq 2^{n+1}$.

$$n + 1 \overset{\text{IH}}{\leq} 2^n + 1 \;\leq\; 2^n + 2^n \;=\; 2^{n+1}.$$

We have shown that $P(n+1)$ is T, as needed.

3: By induction, $P(n)$ is T $\forall n \geq 1$. ∎

(d) Define the claim $P(n) : 5^n - 1$ is divisible by 4.

1: **[Base case]** $P(1)$ claims that $5 - 1$, is divisible by 4, which is clearly T.

2: **[Induction step]** We show $P(n) \to P(n+1)$ for all $n \geq 1$, using a direct proof.
Assume (induction hypothesis) $P(n)$ is T*:* $5^n - 1$ is divisible by 4, so $5^n - 1 = 4k$.
Show $P(n+1)$ is T*:* $5^{n+1} - 1$ is divisible by 4.

$$5^{n+1} - 1 = 5 \cdot 5^n - 1 \overset{\text{IH}}{=} 5 \cdot (4k+1) - 1 \;=\; 20k + 4 \;=\; 4(5k+1).$$

Therefore $5^{n+1} - 1$ is divisible by 4, and we have shown that $P(n+1)$ is T.

3: By induction, $P(n)$ is T $\forall n \geq 1$. ∎

(e) Define the claim $P(n) : \sum_{i=1}^{n} i \cdot i! = (n+1)! - 1$.

1: **[Base case]** $P(1)$ claims that $1 = 2! - 1$, which is clearly T.

2: **[Induction step]** We show $P(n) \to P(n+1)$ for all $n \geq 1$, using a direct proof.
Assume (induction hypothesis) $P(n)$ is T*:* $\sum_{i=1}^{n} i \cdot i! = (n+1)! - 1$.
Show $P(n+1)$ is T*:* $\sum_{i=1}^{n+1} i \cdot i! = (n+2)! - 1$. We compute $\sum_{i=1}^{n+1} i \cdot i!$ as follows:

$$\begin{aligned}\sum_{i=1}^{n+1} i \cdot i! &= (n+1)(n+1)! + \sum_{\boldsymbol{i=1}}^{\boldsymbol{n}} \boldsymbol{i \cdot i!} \\ &\overset{\text{IH}}{=} (n+1)(n+1)! + (n+1)! - 1 \\ &= (n+1)!(n+1+1) - 1 \;=\; (n+2)! - 1.\end{aligned}$$

We have shown that $P(n+1)$ is T, as needed.

3: By induction, $P(n)$ is T $\forall n \geq 1$. ∎

Pop Quiz 5.5. The claim is readily verified by substituting a_0, a_1, a_2, a_3 into the four equations.

Exercise 5.6.

(a) Tinker. Compute $S(n)$ for small n:

n	1	2	3	4	5	6	7	8	9	10	⋯
$S(n)$	1	4	9	16	25	36	49	64	81	100	⋯

A reasonable guess is $S(n) = n^2$. The proof by induction follows the standard template. For the base case, $S(1) = 1 = 1^2$. Suppose $S(n) = n^2$ and consider

$$S(n+1) = S(n) + 2n + 1 \overset{\text{IH}}{=} n^2 + 2n + 1 = (n+1)^2.$$

(IH stands for "by the induction hypothesis"). By induction, $S(n) = n^2$ for all $n \geq 1$. ∎

(b) As usual, first tinker with small n:

n	1	2	3	4	5	6	$\cdots$
$S(n)$	1	9	36	100	225	441	$\cdots$
$\sum_{i=1}^{n} i$	1	3	6	10	15	21	$\cdots$

A reasonable guess is $S(n) = (\sum_{i=1}^{n} i)^2$. The proof by induction follows the standard template. For the base case, $S(1) = 1 = 1^2$. Suppose $S(n) = (\sum_{i=1}^{n} i)^2$ and consider

$$S(n+1) = S(n) + (n+1)^3 \overset{\text{IH}}{=} \Big(\sum_{i=1}^{n} i\Big)^2 + (n+1)^3 = \tfrac{1}{4}n^2(n+1)^2 + (n+1)^3,$$

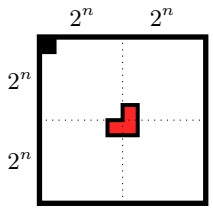
where the last step follows from the formula $\sum_{i=1}^{n} i = \frac{1}{2}n(n+1)$. Therefore,

$$S(n) = \tfrac{1}{4}(n+1)^2(n^2 + 4(n+1)) = \tfrac{1}{4}(n+1)^2(n+2)^2.$$

The last expression is $(\sum_{i=1}^{n+1} i)^2$. By induction, $S(n) = (\sum_{i=1}^{n} i)^2$ for all $n \geq 1$. ∎

Pop Quiz 5.7. (a) $n \geq 3$ (b) $n = 3, 4$ (c) $n \geq 1$

Exercise 5.8. The base cases $n = 1$ and $n = 2$ are demonstrated in the exercise. Assume the $2^n \times 2^n$ grid missing the top-left square can be L-tiled. We show a $2^{n+1} \times 2^{n+1}$ grid missing its top-left square. We divided the grid into four $2^n \times 2^n$ grids and placed an L-tile to cover three of the center-squares as shown in the figure. Each $2^n \times 2^n$ sub-grid is now missing a corner-square, which can be treated as the top-left square by rotating your view. By the induction hypothesis, each sub-grid can be L-tiled independently. So, the $2^{n+1} \times 2^{n+1}$ grid missing the top-left square can be L-tiled, proving the claim for $n+1$. By induction, the claim holds for all $n \geq 1$.



Exercise 5.9.

(i) Define $\mathcal{C} = \{x + z_0 \mid x \in \mathcal{B}\}$. Then $\mathcal{C}$ contains only natural numbers, and is non-empty because $\mathcal{B}$ is non-empty. By well-ordering $\mathcal{C}$ has a minimum element $c_* = b_* + z_0$ where $b_* \in \mathcal{B}$. Consider any $b \in \mathcal{B}$. Then $c = b + z_0 \in \mathcal{C}$ and therefore $c_* \leq c$, i.e. $b_* + z_0 \leq b + z_0$ or $b_* \leq b$. This proves that b_* is a minimum element of $\mathcal{B}$. ∎

(ii) (a) Let n_* be the smallest counter-example; $n_* \geq 2$ ($P(1)$ is T). Therefore $\sum_{i=0}^{n_*-1} a + id \neq n_*a + \frac{1}{2}n_*(n_*-1)d$; and, because n_* is the smallest counter-example, $\sum_{i=0}^{n_*-2} a + id = (n_*-1)a + \frac{1}{2}(n_*-1)(n_*-2)d$. But,

$$\begin{aligned}\sum_{i=0}^{n_*-1} a + id &= a + (n_*-1)d + \sum_{i=0}^{n_*-2} a + id \\ &= a + (n_*-1)d + (n_*-1)a + \tfrac{1}{2}(n_*-1)(n_*-2)d \\ &= n_*a + \tfrac{1}{2}n_*(n_*-1)d,\end{aligned}$$

which contradicts n_* being a counter-example. So, there is no counter-example. ∎

(b) Let n_* be the smallest counter-example; $n_* \geq 2$ ($P(1)$ is T). Therefore $\sum_{i=0}^{n_*-1} ar^i \neq a(r^{n_*}-1)/(r-1)$; and, $n_* - 1 \geq 1$ is not a counter-example, so $\sum_{i=0}^{n_*-2} ar^i = a(r^{n_*-1}-1)/(r-1)$. But,

$$\sum_{i=0}^{n_*-1} ar^i = ar^{n_*-1} + \sum_{i=0}^{n_*-2} ar^i = ar^{n_*-1} + \frac{a(r^{n_*-1}-1)}{r-1} = \frac{a(r^{n_*}-1)}{r-1},$$

which contradicts n_* being a counter-example. So, there is no counter-example. ∎

(c) Let n_* be the smallest counter-example: $n_* \geq 2$ ($P(1)$ is T) and $n_* > 2^{n_*}$. Also, $n_* - 1$ is not a counter-example (n_* is the smallest counter-example), so $n_* - 1 \leq 2^{n_*-1}$. But,

$$n_* = n_* - 1 + 1 \leq 2^{n_*-1} + 1 \leq 2^{n_*-1} + 2^{n_*-1} = 2^{n_*},$$

which contradicts n_* being a counter-example. So, there is no counter-example. ∎

(d) Let n_* be the smallest counter-example: $n_* \geq 2$ ($P(1)$ is T) and $5^{n_*} - 1$ is not divisible by 4. Also, $n_* - 1$ is not a counter-example (n_* is the smallest), so $5^{n_*-1} - 1 = 4k$. But,

$$5^{n_*} - 1 = 5 \cdot 5^{n_*-1} - 1 = 5(4k+1) - 1 = 4(5k+1),$$

so 4 divides $5^{n_*} - 1$ contradicting n_* being a counter-example. So, n_* does not exist. ∎

(e) Let n_* be the smallest counter-example; $n_* \geq 2$ ($P(1)$ is T). Therefore $\sum_{i=1}^{n_*} i.i! \neq (n_*+1)! - 1$. Since n_* is the smallest counter-example, $\sum_{i=1}^{n_*-1} i * i! = n_*! - 1$. But,

$$\sum_{i=1}^{n_*} i.i! = n_*n_*! + \sum_{i=1}^{n_*-1} i * i! = n_*n_*! + n_*! - 1 = (n_*+1)! - 1,$$

which contradicts n_* being a counter-example. So, there is no counter-example. ∎

Exercise 5.10. Suppose $P(1)$ is T; and, $P(n) \to P(n+1)$ is T for $n \geq 1$. We show $P(n)$ is T for all $n \geq 1$. Assume $P(n)$ is F for some n, and let n_* be the smallest counter-example; $n_* \geq 2$ because $P(1)$ is T. Therefore $n_* - 1$ is not a counter-example (n_* is the smallest), so $P(n_* - 1)$ is T. But, $P(n_* - 1) \to P(n_*)$, since $n_* - 1 \geq 1$ and since $P(n_* - 1)$ is T, it implies that $P(n_*)$ is T. This contradicts n_* being a counter example, so $P(n)$ is T for all $n \geq 1$. ∎

Chapter 6

Pop Quiz 6.1. Assume $2\sqrt{n} + \frac{1}{\sqrt{n+1}} > 2\sqrt{n+1}$. Multiply by $\sqrt{n+1}$ and rearrange to $2\sqrt{n(n+1)} > 2n+1$. Both sides are positive, so squaring gives $4n^2 + 4n > 4n^2 + 4n + 1$, or $0 > 1$, a contradiction. So, $2\sqrt{n} + \frac{1}{\sqrt{n+1}} \geq 2\sqrt{n+1}$. ∎

Exercise 6.2.

(a) Define the claim $P(n) : n^3 < 2^n$. Let us consider the induction step, so assume that $P(n)$ is T and consider $(n+1)^3 = n^3 + 3n^2 + 3n + 1 < 2^n + 3n^2 + 3n + 1$. $P(n+1)$ will follow if $3n^2 + 3n + 1 < 2^n$, so define $Q(n) : 3n^2 + 3n + 1 < 2^n$. Let us consider the induction step for Q: assume $Q(n)$, i.e. $3n^2 + 3n + 1 < 2^n$ and consider $Q(n+1)$. $3(n+1)^2 + 3(n+1) + 1 = 3n^2 + 3n + 1 + 6n + 6 < 2^n + 6n + 6$. $Q(n+1)$ will be T if $6n + 6 < 2^n$. Let us define the claim $R(n) : 6n + 6 < 2^n$. Let us prove the stronger claim $P(n) \wedge Q(n) \wedge R(n)$ for $n \geq 10$.

For the base case, the reader can verify that $P(10)$, $Q(10)$, $R(10)$ are all T. For the induction step, assume $P(n) \wedge Q(n) \wedge R(n)$ for $n \geq 10$, so $n^3 < 2^n \wedge 3n^2 + 3n + 1 < 2^n \wedge 6n + 6 < 2^n$. We prove $P(n+1) \wedge Q(n+1) \wedge R(n+1)$.

$$\begin{aligned} n+1^3 &= n^3 + 3n^2 + 3n + 1 \overset{\text{IH}}{<} 2^n + 2^n = 2^{n+1} \\ 3(n+1)^2 + 3(n+1) + 1 &= 3n^2 + 3n + 1 + 6n + 6 \overset{\text{IH}}{<} 2^n + 2^n = 2^{n+1} \\ 6(n+1) + 6 &= 6n + 6 + 1 \overset{\text{IH}}{<} 2^n + 6 < 2^n + 2^n = 2^{n+1}. \end{aligned}$$

The 1st equation uses $P(n)$ for n^3 and $Q(n)$ for $3n^2 + 3n + 1$. The 2nd equation uses $Q(n)$ for $3n^2 + 3n + 1$ and $R(n)$ for $6n + 6$. The 3rd equation uses $R(n)$ for $6n + 6$ and $6 < 2^n$ when $n \geq 10$. Therefore $P(n+1) \wedge Q(n+1) \wedge R(n+1)$ is T. By induction $P(n) \wedge Q(n) \wedge R(n)$ is T for $n \geq 10$. ∎

(b) Without strengthening the claim, in the induction step for $n^2 \leq 2^n$, we have

$$(n+1)^2 = n^2 + 2n + 1 \leq n^2 + 2n + n = n^2 + 3n \leq n^2 + n \cdot n = 2n^2.$$

The first inequality is because $1 \leq n$ and the second because $3 \leq n$. The rest of the induction step continues as before. The induction step works as long as $n \geq 3$. However, the base case only works for $n = 4$.

In the induction step for $n^3 \leq 2^n$, we have

$$(n+1)^3 = n^3 + 3n^2 + 3n + 1 \leq n^3 + 3n^2 + 4n \leq n^3 + 4n^2 \leq n^3 + n^3 = 2n^3.$$

The first inequality is because $1 \leq n$, hence $3n + 1 \leq 4n$; the second is because $4 \leq n$, hence $3n + 4n \leq 3n^2 + n^2 = 4n^2$; the third is because $4 \leq n$, hence $4n^2 \leq = n \cdot n^2 = n^3$. The rest of the induction step continues as before. The induction step works as long as $n \geq 4$. However, the base case only works for $n = 10$.

In the text, we strengthened the claim even though the original claim is provable with a little creativity for pedagogical reasons, to highlight this peculiarity with induction that proving stronger things can be easier. But we are not highilighting for highlighting's sake. In many cases (e.g. next problem) the original claim *cannot* be proved by induction and the only way to go is by strengthening the claim.

(c) The base case, $n = 1$, is easy to check. For the induction step, assume $1 + \frac{1}{2^2} + \cdots + \frac{1}{n^2} \leq 2$ and consider $n+1$:

$$1 + \tfrac{1}{2^2} + \cdots + \tfrac{1}{n^2} + \tfrac{1}{(n+1)^2} \leq 2 + \tfrac{1}{(n+1)^2}.$$

But now what? The RHS is *greater* than 2 and the induction step fails with no possibility of ressurection. Let us instead prove the stronger claim $1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} \leq 2 - \frac{1}{n}$. Again, the base case for $n = 1$ is easy to check. For the induction step, assume $1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{n^2} \leq 2 - \frac{1}{n}$ and consider $n+1$:

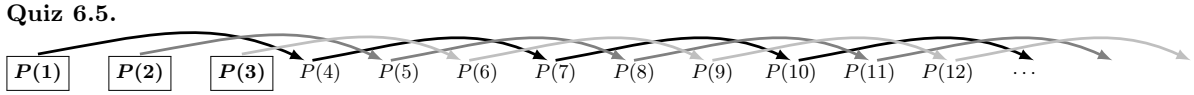
$$1 + \tfrac{1}{2^2} + \cdots + \tfrac{1}{n^2} + \tfrac{1}{(n+1)^2} \leq 2 - \tfrac{1}{n} + \tfrac{1}{(n+1)^2} = 2 - \tfrac{1}{n+1} + \tfrac{1}{n+1} - \tfrac{1}{n} + \tfrac{1}{(n+1)^2} = 2 - \tfrac{1}{n+1} - \tfrac{1}{n(n+1)^2}.$$

(Verify the last step using algebra.) The last expression is clearly less than $2 - \frac{1}{n+1}$, proving the induction step. ∎

Pop Quiz 6.3. No because each subgrid has 4^n squares, which is not a multiple of 3 (the number of squares in an L-tile). This is so because we know that $4^n - 1$ is divisible by 3, so 4^n can't be.

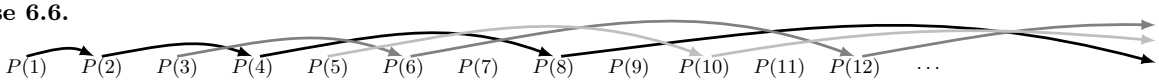
Exercise 6.4. We prove a stronger claim by induction, $P(n)$: the $2^n \times 2^n$ grid can be L-tiled for any missing square. The base case is the 2×2 square. For the induction step, assume $P(n)$, so the $2^n \times 2^n$ grid can be L-tiled for any missing square. For $P(n+1)$, consider the $2^{n+1} \times 2^{n+1}$ grid with any square missing. Divide the grid into its 4 sub-squares as in the text. Place an L-tile in the center overlapping with the 3 sub-grids that are empty. You now have four $2^n \times 2^n$ sub-grids, each with a square missing somewhere; three of them have a corner square missing and one has a square missing in some arbitrary position. By the induction hypothesis, each sub-grids can be independently L-tiled, which is an L-tiling of the whole $2^{n+1} \times 2^{n+1}$ grid, proving $P(n+1)$. By induction, $P(n)$ is true for $n \geq 1$. ∎

Pop Quiz 6.5.
(a)

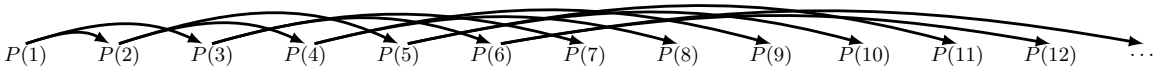


(b) There are three sets of arrows: black (starts at 1); gray (starts at 2); and, light gray (starts at 3). To touch every n with a chain of implications from a base case, we need the three boxed bases cases $P(1),\ P(2),\ P(3)$.

Exercise 6.6.
(a) (i)



A chain starts at every odd n (we have shown the chains starting at $1, 3, 5$).
(ii) There is no in-arrow into odd n, so you need infinitely many base cases $1, 3, 5, 7, 9, 11, \ldots$.
(b) (i)



Now, there is an incoming arrow to every n from $\lfloor n/2 \rfloor$.
(ii) Since there is an incoming arrow to every n, you only need the base case $P(1)$.

Exercise 6.7.
(a) $21 = 2^1 + 2^2 + 2^4$.
(b) Define $P(n)$: n is a sum of distinct powers of 2. The base case is $P(1)$ and $1 = 2^0$. We use strong induction. Assume $P(1), \ldots, P(n)$, and consider $P(n+1)$. There are two cases.

Case 1: Even n. Since $P(n)$ is T, $n = \sum_{i\geq 1} a_i 2^i$, where $a_i = 0, 1$. Hence, $n+1 = 2^0 + \sum_{i\geq 1} a_i 2^i$ proving $P(n+1)$.

Case 2: Odd n, so $n+1$ is even, and $1 \leq \frac{1}{2}(n+1) \leq n$. Since $P(\frac{1}{2}(n+1))$ is T, $\frac{1}{2}(n+1) = \sum_{i\geq 1} a_i 2^i$, where $a_i = 0, 1$. Therefore $n+1 = \sum_{i\geq 1} a_i 2^{i+1}$, proving $P(n+1)$.

In both cases, we proved $P(n+1)$, and so, by induction, $P(n)$ is T for $n \geq 1$. ∎

(c) Define $P(n)$: $n = \sum_{i=1}^{\infty} a_i i!$, where $a_i \in \{0, 1, \ldots, i\}$. The base case is $P(1)$ and $1 = 1!$. We use strong induction. Assume $P(1), \ldots, P(n)$, and consider $P(n+1)$.

Let $n = \sum_{i\geq 1} a_i i!$. Let k be the first index for which $a_k < k$, so $n = \sum_{i=1}^{k-1} ii! + a_k k! + \sum_{i\geq k+1} a_i i!$. We claim that $n+1 = (a_k+1)k! + \sum_{i\geq k+1} a_i i!$, which proves $P(n+1)$. To see this, there are two cases.

Case 1: $k = 1$, in which case the summation $\sum_{i=1}^{k-1} i$ is empty (i.e. zero) and $a_1 = 0$ (because $a_1 < 1$), therefore we are just adding 1 to n, which clearly gives $n+1$.

Case 2: $k \geq 2$. By Exercise 5.4(e), $n = k! - 1 + a_k k! + \sum_{i\geq k+1} a_i i! = (a_k+1)k! - 1 + \sum_{i\geq k+1} a_i i!$.

Adding 1 to both sides, $n+1 = (a_k+1)k! + \sum_{i\geq k+1} a_i i!$, proving $P(n+1)$. By induction $P(n)$ is T for $n \geq 1$. ∎

Exercise 6.8.
(a) Define $P(n)$: the greedy algorithm uses the fewest coins for n. The base case $P(1)$ is clearly T, since greedy uses one 1¢ coin, the best possible. We use strong induction, so assume $P(1), \ldots, P(n)$ and consider $P(n+1)$.

Let $n+1 \geq 25$. Suppose that the optimal way to obtain $n+1$ does not contain a quarter. It cannot contain 3 or more dimes, as you can replace 3 dimes with a quarter and a nickel and do better. We leave it to the reader to show in a similar way that it cannot contain 2 dimes, 1 dime or zero dimes, which is impossible. Therefore, optimal must contain a quarter; and then some number of coins for $n+1-25$. Greedy uses a quarter and by the induction hypothesis, the optimal number of coins for $n+1-25$, which means greedy is optimal for $n+1$.

Suppose $10 \leq n+1 < 25$. A similar reasoning shows there must be at least one dime, hence greedy is optimal. (If there is no dime, there aren't 2 nickels, or 1 nickel and at least 5 pennies, or no nickel and at least 10 pennies.)

Suppose $5 \leq n+1 < 10$. Using similar reasoning, there must be a nickel and greedy is therefore optimal. Lastly, Greedy is clearly optimal for $n+1 < 5$.

Thus greedy is optimal for $n+1$, and hence by induction, greedy is optimal for all $n \geq 1$. ∎

(b) Consider denominations {1¢,4¢,5¢}. To make 8¢, greedy uses {5¢,1¢,1¢,1¢}, but you only need two coins, {4¢,4¢}.

Pop Quiz 6.9. No. Only $P(1), P(5)$ are T. You need base cases $P(1), P(2), P(3), P(4)$. Then, $P(1) \to P(5)$; $P(1) \wedge P(2) \to P(6)$; $P(1) \wedge P(2) \wedge P(3) \to P(7)$; $P(1) \wedge P(2) \wedge P(3) \wedge P(4) \to P(8)$; $P(1) \wedge \cdots \wedge P(5) \to P(9)$; ...

Chapter 7

Pop Quiz 7.1. $f(3)$ cannot be computed. $f(3) = f(2) + 5 = f(1) + 3 + 5 = f(0) + 1 + 3 + 5 = \ldots$. Since we don't know any of $f(2), f(1), f(0), f(-1), \ldots$, we cannot compute $f(3)$.

Exercise 7.2. (a) $f(-1) = f(0) = 0; f(1) = f(0) + 1 = 1; f(2) = f(1) + 3 = 4; f(3) = f(2) + 5 = 9;$ (b) $f(n) = n^2$.

Exercise 7.3. (a) and (b) are well defined. In (c), the recursive part uses a larger value farther from a base case. In (d) you cannot compute $f(1)$.

Exercise 7.4. $P(0), P(1)$ are true since $f(0), f(1)$ are given. Assume $P(n)$, so $f(n)$ can be computed. Then $f(n+2) = f(n) + 2$, proving $P(n+2)$. Hence, $P(n) \to P(n+2)$. By leaping induction, $P(n)$ is T for $n \geq 0$. ∎

Exercise 7.5.

(a) $f(n) = 2n$. (Base case) $f(0) = 0$. (Induction step) Assume $f(n) = 2n$; then, $f(n+1) = 2 + f(n) = 2(n+1)$. ∎

(b) $f(n) = 0$. (Base case) $f(0) = 0$. (Induction step) Assume $f(n) = 0$; then, $f(n+1) = 2f(n) = 2 \times 0 = 0$. ∎

(c) $f(n) = 2^n$. (Base case) $f(0) = 1$. (Induction step) Assume $f(n) = 2^n$; then, $f(n+1) = 2f(n) = 2 \times 2^n = 2^{n+1}$. ∎

Exercise 7.6. First we unfold the recursions in (a), (b), (c); (d) is complicated.

(a)

$$\begin{aligned}
f(n) &= \cancel{f(n-1)} + \log_2 n \\
\cancel{f(n-1)} &= \cancel{f(n-2)} + \log_2(n-1) \\
\cancel{f(n-2)} &= \cancel{f(n-3)} + \log_2(n-2) \\
&\vdots \\
\cancel{f(3)} &= \cancel{f(2)} + \log_2 3 \\
\cancel{f(2)} &= \cancel{f(1)}^{\,0} + \log_2 2 \\
\hline
+\quad f(n) &= \log_2 2 + \cdots + \log_2 n \\
&= \log_2 n!
\end{aligned}$$

(b)

$$\begin{aligned}
f(n) &= 2\cancel{f(n-1)} \\
\cancel{f(n-1)} &= 2\cancel{f(n-2)} \\
\cancel{f(n-2)} &= 2\cancel{f(n-3)} \\
&\vdots \\
\cancel{f(3)} &= 2\cancel{f(2)} \\
\cancel{f(2)} &= 2\cancel{f(1)}^{\,1} \\
\hline
\times\quad f(n) &= 2 \times \cdots \times 2 \\
&= 2^{n-1}
\end{aligned}$$

(c)

$$\begin{aligned}
f(n) &= n\cancel{f(n-1)} \\
\cancel{f(n-1)} &= (n-1)\cancel{f(n-2)} \\
\cancel{f(n-2)} &= (n-2)\cancel{f(n-3)} \\
&\vdots \\
\cancel{f(2)} &= 2\cancel{f(1)} \\
\cancel{f(1)} &= 1\cancel{f(0)}^{\,1} \\
\hline
\times\quad f(n) &= 1 \times 2 \times \cdots \times n \\
&= n!
\end{aligned}$$

In (a), the cancelations occur when you equate the sum of the LHS terms to that of the RHS terms. In (b) and (c), the cancelations occur when you equate the products. Here are the proofs.

(a) $f(n) = \log_2 n!$. (Base case) $f(1) = 0 = \log_2 1!$. (Induction step) Assume $f(n) = \log_2 n!$; then, $f(n+1) = f(n) + \log_2(n+1) = \log_2 n! + \log_2(n+1) = \log_2(n+1)!$. ∎

(b) $f(n) = 2^{n-1}$. (Base case) $f(1) = 1 = 2^0 = 2^{1-1}$. (Induction step) Assume $f(n) = 2^{n-1}$; then, $f(n+1) = 2f(n) = 2 \times 2^{n-1} = 2^n = 2^{n+1-1}$. ∎

(c) $f(n) = n!$. (Base case) $f(0) = 1 = 0!$. (Induction step) Assume $f(n) = n!$; then, $f(n+1) = (n+1)f(n) = (n+1) \times n! = (n+1)!$. ∎

(d) It is possible to unfold the recursion, but one must be careful.

$$\begin{aligned}
f(n) &= \cancel{f(n-1)^2} \\
\cancel{f(n-1)^2} &= \cancel{(f(n-2)^2)^2} \\
\cancel{(f(n-2)^2)^2} &= \cancel{((f(n-3)^2)^2)^2} \\
&\vdots \\
\cancel{((f(2)^2)\cdots)^2} &= (((f(1)^2)^2)\cdots)^2 \\
\hline
+\quad f(n) &= (((f(1)^2)^2)\cdots)^2 \\
&= (((2^2)^2)\cdots)^2
\end{aligned}$$

The cancelations are after you sum on the LHS and RHS. So, $f(n)$ is 2 squared $n-1$ times. When you square, you multiply the exponent by 2, so

$$f(n) = 2^{1 \times 2 \times 2 \times \cdots \times 2} = 2^{2^{n-1}}.$$

Computing the formula was a little complicated, but the proof by induction *after* you have the formula is standard.

(Base case) $f(1) = 2 = 2^1 = 2^{2^0} = 2^{2^{1-1}}$.

(Induction step) Assume $f(n) = 2^{2^{n-1}}$. Then,

$$\begin{aligned}
f(n+1) &= f(n)^2 \\
&= 2^{2^{n-1}} \times 2^{2^{n-1}} \\
&= 2^{2 \times 2^{n-1}} \\
&= 2^{2^n} = 2^{2^{n+1-1}}.
\end{aligned}$$ ∎

There's an easier analysis of this recursion.

Transforming a recursion. We seize the chance to show a powerful trick for analyzing recursions: transform $f(n)$ to a function $g(n)$ that's easier to analyze. The recursion for $f(n)$ transforms to one for $g(n)$. We use the transformation

$$g(n) = \log_2 f(n).$$

Note: $g(1) = \log_2 f(1) = 1$. Taking logs of both sides of the recursion for $f(n)$ gives

$$\log_2 f(n) = \log_2 f(n-1)^2 = 2 \log_2 f(n-1).$$

We get a recursion for $g(n)$ by replacing $\log_2 f$ with g, $g(n) = 2g(n-1)$. We analyzed this recursion in part (b), $g(n) = 2^{n-1}$ and $f(n) = 2^{g(n)} = 2^{2^{n-1}}$.

Exercise 7.7. $T_1 = 1 = F(2)$ and $T_2 = 2 = F_3$, so the base cases are true. We use strong induction. Suppose $T_1 = F_2, \ldots, T_n = F_{n+1}$ for $n \geq 2$. By the recursion, $T_{n+1} = T_n + T_{n-1} = F_{n+1} + F_n$ (by the induction hypothesis). But by the Fibonacci recursion, $F_{n+1} + F_n = F_{n+2}$, hence $T_{n+1} = F_{n+2}$. By induction, $T_n = F_{n+1}$ for $n \geq 1$.

Exercise 7.8. Two base cases because F_{n+1} needs F_n and F_{n-1}. The induction starts at $n = 12$. To prove $F_n \leq 2^n$ with base cases $F_1 = 1 \leq 2^1$ and $F_2 = 2 \leq 2^2$, assume (induction hypothesis) $F_1 \leq 2^1, \ldots, F_n \leq 2^n$ for $n \geq 2$. Then, $F_{n+1} = F_n + F_{n-1} \leq 2^n + 2^{n-1} \leq 2^n + 2^n = 2^{n+1}$, so $F_{n+1} \leq 2^{n+1}$. By induction, $F_n \leq 2^n$ for $n \geq 1$.

Exercise 7.9. We use induction. The base case is `Big(0)=1` which is 2^0. Suppose `Big(n)` $= 2^n$. Since $n+1 > 0$, `Big(n+1)` $= 2 \cdot$ `Big(n)` $= 2 \cdot 2^n = 2^{n+1}$. By induction, `Big(n)` $= 2^n$ for $n \geq 1$.

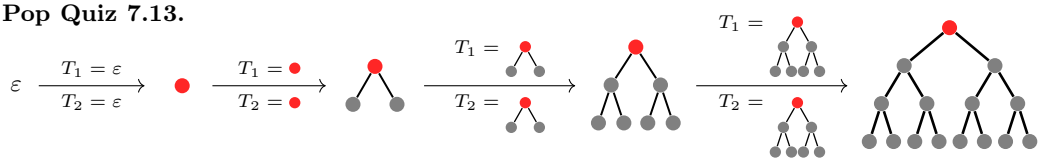
Exercise 7.10. Guess $T_n = 3n + 2$. Now for the proof by induction. The base case is $T_0 = 2 = 3 \times 0 + 2$. Suppose $T_n = 3n + 2$. Then, $T_{n+1} = T_n + 3 = 3n + 2 + 3 = 3(n + 1) + 2$. By induction, $T_n = 3n + 2$ for $n \geq 1$.

Pop Quiz 7.11. (a) Yes (b) Yes (c) No ($\frac{3}{2} \to \frac{5}{2}$) (d) Yes (e) No (1 is not in the set)

Exercise 7.12. Remember that in all cases, by default, nothing else is in the set.

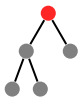
(a) (i) ① $1 \in \mathcal{S}$. ② $x \in \mathcal{S} \to 3x \in \mathcal{S}$. (ii) ① $1 \in \mathcal{S}$. ② $x \in \mathcal{S} \to x^2 \in \mathcal{S}$. (b) ① $\varepsilon, 0, 1 \in \mathcal{S}$. ② $x \in \mathcal{S} \to 0x0 \in \mathcal{S}$; $1x1 \in \mathcal{S}$. (c) ① $\varepsilon \in \mathcal{S}$. ② $x, y \in \mathcal{S} \to [x]y \in \mathcal{S}$.

Pop Quiz 7.13.



Exercise 7.14.

(a) Every RFBT is an RBT. This is because the basis case for the RFBT is an RBT; and, the constructor rules are the same. However, every RBT is not an RFBT.  is an RBT, but not an RFBT.

(b) There are no RFBTs with 6 vertices (only an odd # of vertices is possible). 5 node RFBT: 

Chapter 8

Pop Quiz 8.1. $\varepsilon \xrightarrow{x=\varepsilon,y=\varepsilon} [\,] \xrightarrow{x=\varepsilon,y=[\,]} [\,][\,] \xrightarrow{x=[\,][\,],y=[\,]} [[\,][\,]][\,]$

Exercise 8.2. The proof is by structural induction.

1: Clearly ε is matched (base case).

2: For the induction step, there is only one constructor rule. Suppose x and y are matched. Then xy is matched and so every prefix in $[xy$ has *at least one more* "[" than "]". Inserting "]" anywhere in $[xy$ can add *at most one* to "]"'s in *some* prefixes. Therefore, every prefix in $[x]y$ has *at least as many* "[" than "]" and so $[x]y$ is matched.

3: By structural induction, every string in $\mathcal{M}$ is matched. ∎

Since][is not matched, $][\notin \mathcal{M}$.

Exercise 8.3.

(a) Suppose s is balanced and matched. We use "CS-notation" for the bits of s, $s = s[0]s[1]s[2]\cdots$. $s[i]$ is the ith bit. For prefix $s[0]\cdots s[i]$, define the excess function $f(i)$ to be the number of "[" minus the number of "]". Since s is matched, $f(i) \geq 0$; s must begin with "[" so $f(0) = 1$ and s is balanced so $f(n) = 0$ (length$(s) = n+1$). Let i_* be the first prefix which is balanced, so $f(i_*) = 0$ and $i_* \leq n$ and $s[i_*] =$ "]". We have decomposed s as

$$s = [x]y,$$

where $x = s[1]\cdots s[i_*-1]$ and $y = s[i_*+1]\cdots s[n]$ (x or y could be empty). We show that x and y are balanced and matched. Since $s[0]\cdots s[i_*]$ is balanced ($f(i_*) = 0$), x is balanced. And since s and x are balanced, y is balanced. We now show that x and y are matched. Suppose y is not matched: some prefix α of y with more "]". Then $[x]\alpha$ is a prefix of s with more "]", because $[x]$ is balanced. This contradicts s being matched, hence y is matched. Suppose x is not matched. So, some prefix β of x has more "]"; $\beta \neq x$ because x is balanced. Consider $[\beta$ which is a prefix of s. $f([\beta) \geq 0$ because s is matched and β has more "]", so β has exactly one more "]" than "[", which means that $f([\beta) = 0$. But this contradicts $s[0]\cdots s[i_*]$ being the *first* prefix that is balanced. ∎

(b) Suppose s is a balanced and matched string that is not in $\mathcal{M}$.

(i) By well-ordering, choose s to be the balanced and matched string of *minimum* length that is not in $\mathcal{M}$.

(ii) By (a), $s = [x]y$ where x, y are both balanced and matched.

(iii) x and y are at least 2 characters shorter than s.

(iv) s has minimum length among balanced matched strings not in $\mathcal{M}$. x, y are both balanced and matched, but *shorter* than s. Thus $x, y \in \mathcal{M}$. By the constructor rule, $s = [x]y \in \mathcal{M}$, which contradicts $s \notin \mathcal{M}$. ∎

Exercise 8.4.

(a) $\mathbb{N}_s = \mathbb{N}$.

(b) Structural induction with $\mathbb{N}_s$ is exactly strong induction:

1. (Basis) Show property P holds for 1, i.e. $P(1)$ is T.
2. (Structural Induction) Assume $P(1), \ldots, P(n)$ and prove $P(n+1)$, i.e. show $P(1) \wedge P(2) \wedge \cdots \wedge P(n) \to P(n+1)$

Exercise 8.5.

(a) $x \bullet y = 0101110$; $y \bullet x = 1100101$. The order in which you do the two concatenations does not matter, $(x \bullet y) \bullet z = x \bullet (y \bullet z) = x \bullet y \bullet z = 010111010110$.

(b) $(x \bullet y)^{\mathrm{R}} = 0111010$; $(x \bullet y \bullet z)^{\mathrm{R}} = 011010111010$.

(c) Let $n = |y|$. We prove that $(x \bullet y)^{\mathrm{R}} = y^{\mathrm{R}} \bullet x^{\mathrm{R}}$ by strong induction on $n = |y|$. If $n = 0$ ($y = \varepsilon$), there is nothing to prove (base case). Suppose the claim holds up to $n \geq 0$, that is $(x \bullet y)^{\mathrm{R}} = y^{\mathrm{R}} \bullet x^{\mathrm{R}}$ whenever $|y| \leq n$. Now consider any y with $|y| = n + 1$ and write $y = y_{[n]}b$ where b is a single bit and $y_{[n]}$ is the prefix of length n. Then

$$(x \bullet y)^{\mathrm{R}} = ((x \bullet y_{[n]}) \bullet b)^{\mathrm{R}} \overset{\text{IH}}{=} b \bullet (x \bullet y_{[n]})^{\mathrm{R}} \overset{\text{IH}}{=} b \bullet y_{[n]}^{\mathrm{R}} \bullet x^{\mathrm{R}} \overset{\text{IH}}{=} (y_{[n]} \bullet b)^{\mathrm{R}} \bullet x^{\mathrm{R}} = y^{\mathrm{R}} \bullet x^{\mathrm{R}}.$$

First we apply IH to b, then to $y_{[n]}$ and then to b again (all of which have length at most n). ∎

(d) The base case, $n = 2$, is in (c). Assume the claim holds for $n \geq 2$ and consider $n + 1$:

$$\begin{aligned}(x_1 \bullet x_2 \bullet \cdots \bullet x_n \bullet x_{n+1})^{\mathrm{R}} &= ((x_1 \bullet x_2 \bullet \cdots \bullet x_n) \bullet x_{n+1})^{\mathrm{R}} \\ &\overset{\text{IH}}{=} x_{n+1}^{\mathrm{R}} \bullet (x_1 \bullet x_2 \bullet \cdots \bullet x_n)^{\mathrm{R}} \\ &\overset{\text{IH}}{=} x_{n+1}^{\mathrm{R}} \bullet x_n^{\mathrm{R}} \bullet x_{n-1}^{\mathrm{R}} \bullet \cdots \bullet x_1^{\mathrm{R}}.\end{aligned}$$

∎

Pop Quiz 8.6. $\varepsilon \to 11 \to 0110 \to 001100$. A length 6 palindrome is xx^{R} for with $|x| = 3$. There are 8 strings of length 3, hence 8 palindromes of length 6. In general, there are $2^{\lceil n/2 \rceil}$ palindromes of length n.

Exercise 8.7.

(a) We give the formal proof with numbered steps for easy reference.

1: The 3 base cases $\varepsilon, 0, 1$ are palindromes. (Strings of length at most 1 are palindromes.)
2: For the structural induction step, suppose we start with a palindrome $x = x^{\mathrm{R}}$. We must show that each constructor rule produces a new palindrome. Using Exercise 8.5, $(0 \bullet x \bullet 0)^{\mathrm{R}} = 0^{\mathrm{R}} \bullet x^{\mathrm{R}} \bullet 0^{\mathrm{R}} = 0 \bullet x \bullet 0$ and similarly, $(1 \bullet x \bullet 1)^{\mathrm{R}} = 1^{\mathrm{R}} \bullet x^{\mathrm{R}} \bullet 1^{\mathrm{R}} = 1 \bullet x \bullet 1$ (because $x = x^{\mathrm{R}}$). Therefore both constructor rules produce palindromes.
3: By structural induction, every member of $\mathcal{P}$ is a palindrome. ∎

(b) Consider s, the shortest palindrome not in $\mathcal{P}$. If s starts with 0, it ends in 0, so $s = 0 \bullet x \bullet 0$. Further, x must be a palindrome for s to be one. Now, x is shorter than s, so since s is the shortest palindrome not in $\mathcal{P}$, it must be that $x \in \mathcal{P}$. But then the constructor rule gives that $s = 0 \bullet x \bullet 0 \in \mathcal{P}$, a contradiction. A similar contradiction arises if $s = 1 \bullet x \bullet 1$. Therefore, there is no shortest palindrome not in $\mathcal{P}$, i.e. every palindrome is in $\mathcal{P}$. ∎

Exercise 8.8.

(a) We give the formal proof with numbered steps for easy reference.

1: The base case is 1 which clearly evaluates to 1 which is odd.
2: Structural induction: We consider each constructor rule separately. For rule 1, suppose $x \in \mathcal{A}_{\text{ODD}}$ and x is odd. The constructor rule produces $(x+1+1)$ and $\texttt{value}((x+1+1)) = \texttt{value}(x)+2$, which is odd because $\texttt{value}(x)$ is odd. For rule 2, suppose $x, y \in \mathcal{A}_{\text{ODD}}$ and x, y are odd. The constructor rule produces $(x \times y)$ whose value is $\texttt{value}(x) \times \texttt{value}(y)$, which is odd because the product of two odd numbers is odd.
3: By structural induction, the value of every member of $\mathcal{A}_{\text{ODD}}$ is odd. ∎

(b) $(1 + 1 + 1 + 1 + 1)$

Pop Quiz 8.9. The number of links is 15. The number of vertices is 15. For any RBT, the number of links must be one less than the number of vertices. So this tree cannot be an RBT.

Exercise 8.10.

(a) First size. By the recursion, size = 1 + size(left-subtree) + size(right-subtree) = $1 + 2 \cdot$ size(left-subtree). The last equality is because both child-subtrees are identical. Applying the same logic to the left-child,

$$\begin{aligned}\text{size} &= 1 + 2(1 + 2 \cdot \text{size(left-left-child)}) = 1 + 2 + 4 \cdot \text{size(left-left-child)} \\ &= 1 + 2 + 4 + 8 \cdot \text{size(left-left-left-child)} \\ &= 1 + 2 + 4 + 8 + 16 \cdot \text{size}(\underbrace{\text{left-left-left-left-child}}_{\varepsilon}) = 1 + 2 + 4 + 8 + 16 \cdot 0 = 15.\end{aligned}$$

Similarly, we can recursively obtain the height,

$$\text{height} = 1 + 1 + 1 + 1 + 1 \cdot \text{height}(\underbrace{\text{left-left-left-left-child}}_{\varepsilon}) = 1 + 1 + 1 + 1 - 1 = 3.$$

(b) size(T) is just the number of vertices in the tree.

(c) Define, for an RBT T, the property $P(T)$: $\text{size}(T) \leq 2^{\text{height}(T)+1} - 1$. $P(\varepsilon)$ is T because $0 = 2^{-1+1} - 1$. Now suppose that, for RBTs T_1 and T_2, $P(T_1)$ and $P(T_2)$ are T. That is,

$$\begin{aligned} \text{size}(T_1) &\leq 2^{\text{height}(T_1)+1} - 1 \\ \text{size}(T_2) &\leq 2^{\text{height}(T_2)+1} - 1 \end{aligned} \qquad \leftarrow \text{induction hypothesis}$$

By the recursive definitions of size and height,

$$\begin{aligned} \text{height}(T) &= 1 + \max(\text{height}(T_1), \text{height}(T_2)) \\ \text{size}(T) &= 1 + \text{size}(T_1) + \text{size}(T_2) \end{aligned}$$

By the induction hypothesis,

$$\begin{aligned} \text{size}(T) &\leq 1 + 2^{\text{height}(T_1)+1} - 1 + 2^{\text{height}(T_2)+1} - 1 \\ &= 2^{\text{height}(T_1)+1} + 2^{\text{height}(T_2)+1} - 1 \\ &\leq 2^{\max(\text{height}(T_1),\text{height}(T_2))+1} + 2^{\max(\text{height}(T_1),\text{height}(T_2))+1} - 1 \\ &= 2^{\max(\text{height}(T_1),\text{height}(T_2))+2} - 1 \\ &= 2^{\text{height}(T)+1} - 1. \end{aligned}$$

So, $P(T)$ is T and the constructor preserves property P. By structural iniduction, P is T for every RBT. ∎

Chapter 9

Pop Quiz 9.1. (a) 1+1+1=3. (b) 1+2+3=6. (c) $f(i) = 3$ gives $3 + 3 + 3 = 9$. (d) $f(1) = 1; f(2) = 2; f(3) = 3$ gives $1 + 2 + 3 = 6$.

Pop Quiz 9.2. $T_4(n) = 5 + \sum_{i=1}^{n} 10 = 5 + 10 \cdot \sum_{i=1}^{n} 1$. The last sum is n, so $T_4(n) = 5 + 10n$.

Exercise 9.3. We use several common sums together with the constant and addition rules:

$$\begin{aligned} S(n) = \sum_{i=1}^{n}(1 + 2i + 2^{i+2}) &= \sum_{i=1}^{n} 1 + \sum_{i=1}^{n} 2i + \sum_{i=1}^{n} 2^{i+2} && \text{(addition rule)} \\ &= \sum_{i=1}^{n} 1 + 2\sum_{i=1}^{n} i + 4\sum_{i=1}^{n} 2^i && \text{(constant rule)} \\ &= n + 2 \times \tfrac{1}{2}n(n+1) + 4 \times (2^{n+1} - 1 - 1) && \text{(common sums)} \\ &= 2^{n+3} + n^2 + n - 8 && \text{(simplify)} \end{aligned}$$

Exercise 9.4.

(a)
$$\begin{aligned} T_1(n) &= 2 + \sum_{i=1}^{n}\Big[2 + \sum_{j=i}^{n}\Big(5 + \sum_{k=i}^{j} 2\Big)\Big] \\ &= 2 + \sum_{i=1}^{n}\Big[2 + \sum_{j=i}^{n} 5 + \sum_{j=i}^{n}\sum_{k=i}^{j} 2\Big] && \text{(addition rule)} \\ &= 2 + \sum_{i=1}^{n} 2 + \sum_{i=1}^{n}\sum_{j=i}^{n} 5 + \sum_{i=1}^{n}\sum_{j=i}^{n}\sum_{k=i}^{j} 2 && \text{(addition rule)} \\ &= 2 + 2\sum_{i=1}^{n} 1 + 5\sum_{i=1}^{n}\sum_{j=i}^{n} 1 + 2\sum_{i=1}^{n}\sum_{j=i}^{n}\sum_{k=i}^{j} 1 && \text{(constant rule on all three nested sums)} \end{aligned}$$

(b) $\sum_{k=i}^{j} 1 = j + 1 - i$. This is a common sum.

(c) $\sum_{j=i}^{n}(j + 1 - i) = 1 + 2 + \cdots + (n + 1 - i) = \sum_{\ell=1}^{n+1-i} \ell = \frac{1}{2}(n + 1 - i)(n + 2 - i)$. (The last step is a common sum.)

(d) To compute $\sum_{i=1}^{n}(n + 1 - i)(n + 2 - i)$, we observe that as i goes from 1 up to n, $n + 1 - i$ goes from n down to 1. Letting $\ell = n + 1 - i$, our sum can equivalently be written

$$\sum_{\ell=1}^{n}(\ell)(\ell + 1) = \sum_{\ell=1}^{n} \ell^2 + \sum_{\ell=1}^{n} \ell. \qquad \text{(We used the addition rule to get the last expression.)}$$

(e) We use the nested sum rule to compute $\sum_{i=1}^{n}\sum_{j=i}^{n}\sum_{k=i}^{j} 1$,

$$\begin{aligned} \sum_{i=1}^{n}\sum_{j=i}^{n}\sum_{k=i}^{j} 1 &= \sum_{i=1}^{n}\sum_{j=i}^{n}(j + 1 - i) && \text{(nested sum rule and (b))} \\ &= \tfrac{1}{2}\sum_{i=1}^{n}(n + 1 - i)(n + 2 - i) && \text{(nested sum rule and (c))} \\ &= \tfrac{1}{2}\sum_{i=1}^{n} i^2 + \tfrac{1}{2}\sum_{i=1}^{n} i && \text{(using (d))} \\ &= \tfrac{1}{12}n(n+1)(2n+1) + \tfrac{1}{4}n(n+1) && \text{(common sums)} \end{aligned}$$

For complex sums like this, always tinker and see if your formula works for small n. You can program a function to compute the sum and test it against your formula. We did exactly that to verify our formula.

n	1	2	3	4	5	6	7
$\sum_{i=1}^{n}\sum_{j=i}^{n}\sum_{k=i}^{j} 1$	1	4	10	20	35	56	84
$\frac{1}{12}n(n+1)(2n+1)+\frac{1}{4}n(n+1)$	1	4	10	20	35	56	84

Pop Quiz 9.5. The formulas at the top of page 117 give $T_1 \in \Theta(n^3)$; $T_2 \in \Theta(n^2)$; $T_3 \in \Theta(n\log n)$; $T_4 \in \Theta(n)$. Thus,
(a) T_1 is in $\Omega(n\log n), \omega(n\log n), \Omega(n^2), \omega(n^2), O(n^3), \Theta(n^3), \Omega(n^3)$.
(b) T_2 is in $\Omega(n\log n), \omega(n\log n), O(n^2), \Theta(n^2), \Omega(n^2), O(n^3), o(n^3)$.
(c) T_3 is in $O(n\log n), \Theta(n\log n), \Omega(n\log n), O(n^2), o(n^2), O(n^3), o(n^3)$.
(d) T_4 is in $O(n\log n), o(n\log n), O(n^2), o(n^2), O(n^3), o(n^3)$.

Exercise 9.6.
(a) $f+f=2f\in\Theta(f)$ because 2 is a constant. Similarly $f+f+f=3f\in\Theta(f)$. With n terms, $f+f+\cdots+f = nf\in\Theta(nf)$ (you cannot ignore the n because it is *not a constant*).
(b) $\lim(c\cdot f)/f \to c =$ constant so $c\cdot f\in\Theta(f)$.
(c) (i) Follows from the calculus fact that for any $\epsilon, k>0$, $\lim_{n\to\infty}\log^k n/n^\epsilon = 0$.
(ii) Follows from $n^k/n^{\epsilon\log n} = n^{k-\epsilon\log n}\to 0$.
(iii) $n^k/2^{\epsilon n} = 2^{k\log_2 n-\epsilon n}\to 0$.
(iv) Follows from $\log n^k = k\log n$ so $\log n^k/\log n \to k =$ constant.
(d) (i) Follows from $(1+\sqrt{n})/n = 1/n + 1/\sqrt{n}\to 0$.
(ii) Follows from $(\frac{1}{n}+\frac{5}{n^2})/\frac{1}{n} = 1+5/n\to 1 =$ constant.
(iii) We must prove upper and lower bounds. The upper bound follows from:

$$\log n! = \log n + \log(n-1) + \cdots + \log 1 \le \log n + \log n + \cdots + \log n = n\log n.$$

For the lower bound, observe that $\log(2n)! = \log(2n)(2n-1)(2n-2)(2n-3)\cdots 2\cdot 1$, hence

$$\log(2n)! \le \log(2n)^2(2(n-1))^2\cdots 2^2 = 2\log n! + 2n\log 2.$$

(We get this bound by grouping in pairs, for example $2n(2n-1)\le(2n)^2$.) Also,

$$\begin{aligned}\log(2n)! &= \log(2n)+\log(2n-1)+\cdots+\log(n+1)+\log n!\\ &\ge \log(2n)+\log(2n-1)+\cdots+\log(n+1)\ge n\log n.\end{aligned}$$

Combining the two bounds, $2\log n! + 2n\log 2 \ge n\log n$, or,

$$\log n! \ge \tfrac{1}{2}n\log n - n\log 2 = \tfrac{1}{4}n\log n + \tfrac{1}{4}n(\log n - 4\log 2).$$

We conclude that $\log n!\ge\frac{1}{4}n\log n$ which is true from the inequality above for $n\ge 2^4$ because $\log n - 4\log 2\ge 0$ and it can be verified for $n=1,\ldots,15$ explicitly.
(e) $f = a_k n^k + g$ where g has only lower order terms, at most k such terms. Let the largest coefficient in g be A. Then $|g|\le k|A|n^{k-1}$. We have that $f/n^k = a_k + g/n^k$ and $|g/n^k|\le |A|kn^{k-1}/n^k = |A|k/n$. Since $|A|$ and k are constants, $|g/n^k|\to 0$ and we have that $f/n^k\to a_k =$ constant. This proves $f\in\Theta(n^k)$.
(f) Yes, f is polynomial. The highest power "appearing" is n which has order 1. From the previous problem you might think $f\in\Theta(n)$. Wrong. The notation is deceiving because there are many terms and the term of order n does not appear just once as in a traditional polynomial. For example $n/2$ appears somewhere in the middle, which is also of order 1. There are $n/2$ terms that are at least $n/2$, so $f\ge n^2/4$. In fact, we know that $f(n)=\frac{1}{2}n(n+1)\in\Theta(n^2)$.
To clarify (i), we emphasize that in a polynomial, each term of a particular order appears at most once.
(g) Suppose $n^2\in O(n)$, i.e. $n^2\le Cn$ for a constant C (by taking $\lceil C\rceil$, we may assume C is an integer). Let $n=2C$; then, $4C^2\le 2C^2$ or $4\le 2$, a contradiction. Therefore $n^2\notin O(n)$.
(h) Since $f\in\Theta(r)$ and $g\in\Theta(s)$, there are positive constants c, C and d, D for which

$$c\cdot r\le f\le C\cdot r \qquad\text{and}\qquad d\cdot s\le g\le D\cdot s.$$

(i) Adding the left hand sides and similarly the right hand sides gives $cr+ds\le f+g\le Cr+Ds$. Since $cr+ds\ge\min(c,d)(r+s)$ and $Cr+Ds\le\max(C,D)(r+s)$, we have that

$$\min(c,d)(r+s)\le f+g\le\max(C,D)(r+s) \qquad\to\qquad f+g\in\Theta(r+s).$$

(ii) Instead of adding, if we multiply, we get $cd\cdot(rs)\le fg\le CD\cdot(rs)$, or that $fg\in\Theta(rs)$.
(i) (i) No. Consider $f=2n$ and $g=n$, then $f\in\Theta(g)$. But $2^f/2^g - 2^{2n}/2^n = 2^n\to\infty$.

(ii) Yes. We have that $c \cdot g \le f \le C \cdot g$. Everything is positive and log is increasing so take log of both sides to get $\log g + \log c \le \log f \le \log g + \log C$. That is $\log f \in \Theta(\log g)$.

O-notation blurs small diffenences (constants). Exponentiation blows up those differences, so one must be careful. Logarithms further reduce differences and so are safe with O-notation.

(j) (a) $f \in \Theta(g) \to f \in O(g)$ is T because $\Theta(\cdot)$ requires upper and lower bounds but $O(\cdot)$ requires only the upper bound: $\Theta(g) \subset O(g)$. (b) The converse, $f \in O(g) \not\to f \in \Theta(g)$ is F. For a counter-example, consider $f = n$ and $g = n^2$. (c) Yes: $c \cdot g \le f \le C \cdot g$ implies $\frac{1}{C} \cdot f \le g \le \frac{1}{c} \cdot f$.

(k) Suppose $f \in O(n)$, then $f \le Cn \le Cn^2$. That is $f \in O(n^2)$, which means $O(n) \subset O(n^2)$. It is a proper subset because $n^2 \notin O(n)$ but $n^2 \in O(n^2)$. $\Theta(n) \not\subset \Theta(n^2)$ because $n \in \Theta(n)$ but $n \notin \Theta(n^2)$.

(l) We can use the definitions based on the limits or the more formal definitions based on bounds.

(i) $f/h = (f/g) \cdot (g/h)$; since both terms on the RHS converge to a constant because $f \in \Theta(g)$ and $g \in \Theta(h)$, $f/h \to$ constant, i.e. $f \in \Theta(h)$.

(ii) $f/h = (f/g) \cdot (g/h) \to 0$ (both terms on the RHS converge to 0), i.e. $f \in o(h)$.

(iii) $f \le C \cdot g$ and $g \le C' \cdot h$ implies $f \le C \cdot (C' \cdot h) = CC' \cdot h$, i.e. $f \in O(h)$.

(iv) $f/h = (f/g) \cdot (g/h) \to \infty$ (both terms on the RHS converge to ∞), i.e. $f \in \omega(h)$.

(v) $f \ge C \cdot g$ and $g \ge C' \cdot h$ implies $f \ge C \cdot (C' \cdot h) = CC' \cdot h$, i.e. $f \in \Omega(h)$.

(m) For positive numbers x, y, We use the identity: $\max(x, y) \le x + y \le 2\max(x, y)$. Suppose $r \in O(f + g)$. Then,

$$r \le C(f + g) \le 2C \max(f, g),$$

i.e., $r \in O(\max(f, g))$ and $O(f + g) \subseteq O(\max(f, g))$. Suppose $r \in O(\max(f, g))$. Then,

$$r \le C \max(f, g) \le C(f + g),$$

i.e., $r \in O(f + g)$ and $O(\max(f, g)) \subseteq O(f + g)$. $O(f + g) \subseteq O(\max(f, g))$ and $O(\max(f, g)) \subseteq O(f + g)$ implies $O(f + g) = O(\max(f, g))$.

Similarly, suppose $r \in \Theta(f + g)$. Then,

$$c \max(f, g) \le c(f + g) \le r \le C(f + g) \le 2C \max(f, g),$$

i.e., $r \in \Theta(\max(f, g))$ and $\Theta(f + g) \subseteq \Theta(\max(f, g))$. Suppose $r \in \Theta(\max(f, g))$. Then,

$$\tfrac{1}{2}c(f + g) \le c \max(f, g) \le r \le C \max(f, g) \le C(f + g),$$

i.e., $r \in \Theta(f + g)$ and $\Theta(\max(f, g)) \subseteq \Theta(f + g)$. $\Theta(f + g) \subseteq \Theta(\max(f, g))$ and $\Theta(\max(f, g)) \subseteq \Theta(f + g)$ implies $\Theta(f + g) = \Theta(\max(f, g))$.

(n) We have that $c \cdot g \le f \le C \cdot g$. Summing: $c \cdot \sum_i g(i) \le \sum_i f(i) \le C \cdot \sum_i g(i)$, which means $\sum_i f(i) \in \Theta(\sum_i g(i))$.

(o) We prefer T_1 because its running time is asymptotically faster.

(p) We don't know because T_2 could be n (we prefer T_2) or n^3 (we prefer T_1) – both cases are in $O(n^3)$. When possible, give runtimes using Θ-notation, $O(\cdot)$ is ambiguous. (If $T_1 = 10$ and $T_2 \le 20$, which is better?)

(q) Similar to (t). T_2 could be n or $n^{2.5}$. (If $T_1 = 10$ and $T_2 < 20$, which is better?)

(r) T_1 is asymptotically better than T_2 (T_1 is "equal to" n^2 versus T_2 is "greater than" n^2) so we definitely prefer T_1.

(s) T_1 is no worse than T_2 (T_1 "equals" n^2 versus T_2 is "at least" n^2). We prefer T_1, though T_2 could be as good.

(t) T_2 could be n or n^3, both are in $\Omega(n)$. Like $O(\cdot)$, $\Omega(\cdot)$ is ambiguous. Whenever possible, give a Θ-analysis.

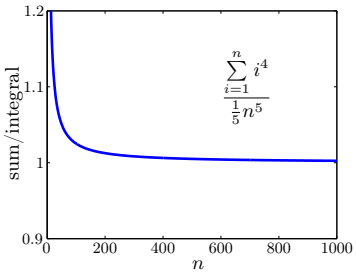
(u) T_2 is asymptotically better? Theoretically, T_2 is a better run time but see (z).

(v) Asymptotically T_2 is better: for $n \to \infty$, $T_2 < T_1$. But, T_2 does not win until $n > 10^{800}$. That is a large input, unlikely to occur in practice – most estimates for the number of atoms in the Universe are less than 10^{100}.

Pop Quiz 9.7. We have that $\sum_{i=1}^{n} i = n(n+1)/2$ and $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$. Therefore

(i) $\sum_{i=1}^{n^2} i = n^2(n^2+1)/2 \in \Theta(n^4)$. (ii) $\sum_{i=1}^{2^n} i = 2^n(2^n+1)/2 \in \Theta(2^{2n})$. (iii) $\sum_{i=0}^{2n} 2^i = 2^{2n+1} - 1 \in \Theta(2^{2n})$.

Exercise 9.8.



Exercise 9.9. In all cases, let $S(n)$ denote the sum.

(a) Since $(1+i)^2$ is increasing, $\int_0^n dx\ (1+x)^2 \le S(n) \le \int_1^{n+1} dx\ (1+x)^2$. Computing the integrals,

$$\tfrac{1}{3}(n+1)^3 \le S(n) \le \tfrac{1}{3}((n+2)^3 - 1).$$

Since the lower and upper bounds are in $\Theta(n^3)$, $S(n) \in \Theta(n^3)$.

(b) Since 2^i is increasing, $\int_0^n dx\ 2^x \le S(n) \le \int_1^{n+1} dx\ 2^x$. Computing the integrals,
$$\tfrac{1}{\ln 2}(2^n - 1) \le S(n) \le \tfrac{1}{\ln 2}(2^{n+1} - 2).$$
Since the lower and upper bounds are in $\Theta(2^n)$, $S(n) \in \Theta(2^n)$.

(c) Since $i2^i$ is increasing, $\int_0^n dx\ x2^x \le S(n) \le \int_1^{n+1} dx\ x2^x$. Computing the integrals,
$$\tfrac{1}{\ln 2}n2^n - \tfrac{1}{\ln^2 2}2^n + \tfrac{1}{\ln^2 2} \le S(n) \le \tfrac{1}{\ln 2}(n+1)2^{n+1} - \tfrac{1}{\ln^2 2}2^{n+1} - \tfrac{2}{\ln 2} + \tfrac{2}{\ln^2 2}.$$
Since the lower and upper bounds are in $\Theta(n2^n)$, $S(n) \in \Theta(n2^n)$.

(d) Since $(1+i^2)^{-1}$ is decreasing, $\int_1^{n+1} dx\ (1+x^2)^{-1} \le S(n) \le \int_0^n dx\ (1+x^2)^{-1}$. Computing the integrals,
$$\arctan(n+1) - \tfrac{\pi}{4} \le S(n) \le \arctan(n).$$
Since the lower and upper bounds are in $\Theta(1)$, $S(n) \in \Theta(1)$.

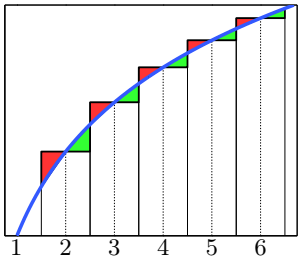
(e) Since $i/(1+i^2)$ is decreasing, $\int_1^{n+1} dx\ x/(1+x^2) \le S(n) \le \int_0^n dx\ x/(1+x^2)$. Computing the integrals,
$$\tfrac{1}{2}\ln\tfrac{1}{2}(1+(1+n)^2) \le S(n) \le \tfrac{1}{2}\ln(1+n^2).$$
Since the lower and upper bounds are in $\Theta(\log n)$, $S(n) \in \Theta(\log n)$.

(f) Since $i2^{i^2}$ is increasing, $\int_0^n dx\ x2^{x^2} \le S(n) \le \int_1^{n+1} dx\ x2^{x^2}$. Computing the integrals,
$$\tfrac{1}{2\ln 2}(2^{n^2} - 1) \le S(n) \le \tfrac{1}{2\ln 2}(2^{(n+1)^2} - 2).$$
The lower bound is in $\Theta(2^{n^2})$ and the upper bound is in $\Theta(2^{n^2+2n})$, which are asymptotically different, $2^{n^2} \in o(2^{n^2+2n})$. We cannot immediately get the Θ-behavior for $S(n)$. The integration bounds are too loose.

A simpler analysis gives tighter bounds. The largest term in the sum is $n2^{n^2}$ and there are n terms, so
$$n2^{n^2} \le S(n) \le n^2 2^{n^2}.$$
The lower bound is asymptotically tight because $S(n-1) \le (n-1)^2 2^{(n-1)^2}$, so $S(n) = S(n-1) + n2^{n^2}$, therefore
$$S(n) \le n2^{n^2} + (n-1)^2 2^{(n-1)^2} = n2^{n^2}\left(1 + 2\tfrac{(n-1)^2}{n}2^{-2n}\right) \le n2^{n^2}(1 + 2n2^{-2n}) \le \tfrac{3}{2}n2^{n^2},$$
(because $x2^{-x} \le \frac{1}{2}$ for $x \ge 0$). Therefore, $S(n) \in \Theta(n2^{n^2})$, because $n2^{n^2} \le S(n) \le \frac{3}{2}n2^{n^2}$.

Exercise 9.10.
(a) This is just the sum written out.
(b) Multiply the expression in (a) by 2 on both sides.
(c) Subtract (a) from (b): $2S(n) - S(n) = -2^1 - 2^2 - 2^3 - \cdots - 2^n + n2^{n+1} = n2^{n+1} - \sum_{i=1}^n 2^i$.
(d) Use (c) with $\sum_{i=1}^n 2^i = 2(2^n - 1)$, $S(n) = n2^{n+1} - 2(2^n - 1) = (n-1)2^{n+1} + 2$.

Exercise 9.11. The red areas are larger than the green because $(\ln x)'' = -1/x^2 < 0$ (the slope of $\ln x$ decreases). Computing the integral replaces each red region in the rectangle with the corresponding green region, therefore we get a lower bound:



$$\int_{3/2}^{n+1/2} dx\ \ln x \le \sum_{i=2}^{n} \ln i = \ln n!.$$
Evaluating the integral on the left, we get
$$\left(n+\tfrac{1}{2}\right)\ln\left(n+\tfrac{1}{2}\right) - \left(n+\tfrac{1}{2}\right) - \tfrac{3}{2}\ln\tfrac{3}{2} + \tfrac{3}{2} \le \ln n!.$$
Exponentiate both sides to get
$$n! \ge \left(n+\tfrac{1}{2}\right)^{\left(n+\frac{1}{2}\right)} e^{-n} e \left(\tfrac{2}{3}\right)^{3/2} = n^n e^{-n}\sqrt{n}e\left(\tfrac{2}{3}\right)^{3/2}\left(\tfrac{n+\frac{1}{2}}{n}\right)^{n+1/2}.$$
Lastly, using the approximation $(1+\frac{1}{x})^x \approx e$,
$$\left(\tfrac{n+\frac{1}{2}}{n}\right)^{n+\frac{1}{2}} = \left[\left(1+\tfrac{1}{2n}\right)^{2n}\right]^{(n+\frac{1}{2})/2n} \approx e^{\frac{1}{2}+\frac{1}{4n}} = \sqrt{e}\cdot e^{1/4n}.$$
And since $e^{1/4n} = 1 + \Theta(1/4n)$, we get the desired approximation $n! \approx n^n e^{-n}\sqrt{n}(2e/3)^{3/2}$.

Chapter 10

Pop Quiz 10.1. $27 = 3 \times 7 + 6$ ($r = 6$). By setting $q = 3, 2, 1, 0, -1, \ldots$ we get $r = 6, 13, 20, 27, \ldots$. The smallest positive remainder is 6. Generally, to get the smallest remainder, set $q = \lfloor n/d \rfloor$ and $r = n - qd = n - \lfloor n/d \rfloor \cdot d$.

Exercise 10.2. The proofs all use the fact that $d|n$ if and only if $n = dk$ for $k \in \mathbb{Z}$.
(a) $0 = 0 \cdot d$ ($q = 0$), so $d|0$.
(b) Suppose $d|m$ and $d'|n$, so $m = qd$ and $n = q'd'$. Then $mn = (qq')dd'$. That is $dd'|mn$ (quotient $= qq'$).
(c) Suppose $d|m$ and $m|n$, so $m = qd$ and $n = q'm$. Then, $n = q'qd$ so $d|n$ (quotient $= q'q$).
(d) Suppose $d|n$ and $d|m$, so $n = qd$ and $m = q'd$. Then $n + m = (q + q')d$. That is $d|n + m$ (quotient $= q + q'$).

(e) Suppose $d|n$, so $n = qd$. For $x \in \mathbb{N}$, $xn = qxd$, so $xd|xn$ (quotient $= q$).
(f) Suppose $d|m+n$ and $d|m$, so $m+n = qd$ and $m = q'd$. Then, $n = qd - n = qd - q'd = (q-q')d$. That is $d|n$ (quotient $= q - q'$).

Exercise 10.3.
(a) Let $P(n) = n$ is divisible by a prime. $P(2)$ is T because 2 is a prime. Suppose $P(2), \ldots, P(n)$ are all T. We show that $P(n+1)$ is T. If $n+1$ is prime, then $n+1$ is divisible by the prime $n+1$. Otherwise, $n+1$ is composite: $n+1 = k\ell$, where $2 \le \ell \le n$. By the induction hypothesis, ℓ is divisible by a prime, so $\ell = qp$ where p is prime. Therefore $n+1 = kqp$ which shows that $n+1$ is also divisible by the prime p. By induction, $P(n)$ is T for all $n \ge 2$.
(b) Suppose there are finitely many primes. Then, there is a largest prime p. Consider $p! + 1$, which has a remainder of 1 when divided by $2, 3, \ldots, p$. By part (a), $p! + 1$ must be divisible by a prime. This prime must therefore be larger than p contradicting p being the largest prime. Therefore there are infinitely many primes.

Pop Quiz 10.4. $\gcd(n, 0) = n$ because $n|0$ and $n|n$. $\gcd(0, 0)$ is not defined (not both integers can be zero). $\gcd(n, n) = n$ because $n|n$. $\gcd(n, 1) = 1$ because the largest divisor of 1 is 1.

$$\gcd(n,p) = \begin{cases} 1 & \text{if } p \text{ does not divide } n; \\ p & \text{if } p \text{ does divides } n. \end{cases} \qquad \text{(Because the only divisors of } p \text{ are 1 and } p.\text{)}$$

Exercise 10.5.

$$\begin{aligned}
&\gcd(34, 55) \\
=\ &\gcd(21, 34) && \mathbf{21} = \mathbf{55 - 34} \\
=\ &\gcd(13, 21) && \mathbf{13} = 34 - 21 = 34 - (55 - 34) = \mathbf{2 \cdot 34 - 55} \\
=\ &\gcd(8, 13) && \mathbf{8} = 21 - 13 = (55 - 34) - (2 \cdot 34 - 55) = \mathbf{2 \cdot 55 - 3 \cdot 34} \\
=\ &\gcd(5, 8) && \mathbf{5} = 13 - 8 = (2 \cdot 34 - 55) - (2 \cdot 55 - 3 \cdot 34) = \mathbf{5 \cdot 34 - 3 \cdot 55} \\
=\ &\gcd(3, 5) && \mathbf{3} = 8 - 5 = (2 \cdot 55 - 3 \cdot 34) - (5 \cdot 34 - 3 \cdot 55) = \mathbf{5 \cdot 55 - 8 \cdot 55} \\
=\ &\gcd(2, 3) && \mathbf{2} = 5 - 3 = (5 \cdot 34 - 3 \cdot 55) - (5 \cdot 55 - 8 \cdot 55) = \mathbf{13 \cdot 34 - 8 \cdot 55} \\
=\ &\gcd(1, 2) && \mathbf{1} = 3 - 2 = (5 \cdot 55 - 8 \cdot 55) - (13 \cdot 34 - 8 \cdot 55) = \mathbf{13 \cdot 55 - 21 \cdot 34} \\
=\ &\gcd(0, 1) \\
=\ &1
\end{aligned}$$

Each remainder is a linear combination of the original two numbers. Finally, $\gcd(34, 55) = 1 = \mathbf{55} \times 13 + \mathbf{34} \times (-21)$.

Exercise 10.6. $6x + 15y = 3 \cdot (2x + 5y)$. Setting $x = -2k, y = k$ gives $3k$, all the positive multiples of 3. $\gcd(6, 15) = 3$.

Exercise 10.7.
(a) Suppose $d|mn$. By Bezout, there are x, y for which $\gcd(m, d) = mx + dy$. Multiply both sides by n to get

$$\gcd(m, d) \cdot n = xmn + ynd.$$

d divides mn, so d divides both terms on the RHS. Therefore d must divide the LHS. ∎
(b) We are given that $\gcd(d, d') = 1 = dx + d'y$ (Bezout's identity). Multiply both sides by n to get

$$n = xdn + yd'n.$$

Since $d|n$, $n = \alpha d$; since $d'|n$, $n = \alpha' d'$. Rewriting the equation above,

$$n = x\alpha' dd' + y\alpha dd' = (x\alpha' + y\alpha)dd',$$

which means $dd'|n$ as was to be shown. ∎
(c) Let $D = \gcd(m, \ell)$ and $D' = \gcd(n, \ell)$. By Bezout's identity, $D = mx + \ell y$ and $D' = nx' + \ell y'$. Multiplying,

$$DD' = (mx + \ell y)(nx' + \ell y') = mn(xx') + \ell(ynx' + mxy' + \ell yy'). \qquad (*)$$

Since $DD' > 0$, the RHS is a positive linear combination of mn and ℓ. The smallest positive linear combination of mn and ℓ is $\gcd(mn, \ell)$, so $\gcd(mn, \ell) \le DD'$.

To show the reverse, that $DD' \le \gcd(mn, \ell)$, it suffices to show that DD' divides mn and ℓ because then it can't exceed the *greatest* common divisor. By Exercise 10.2(b), $DD'|mn$. We show that $DD'|\ell$ using part (a) of this exercise. For part (a) to apply, we must show that $\gcd(D, D') = 1$. Note that $\gcd(D, D')|m$ because $\gcd(D, D')|D$ and $D|m$; similarly, $\gcd(D, D')|n$. So, $\gcd(D, D')$ is a common divisor of m and n, hence

$$\gcd(D, D') \le \gcd(m, n) = 1.$$

Thus, $\gcd(D, D') = 1$. By part (a), since $D|\ell$ and $D'|\ell$ (why?), it follows that $DD'|\ell$. Thus DD' is a common divisor of mn and ℓ and hence $DD' \le \gcd(mn, \ell)$.

Since $\gcd(mn, \ell) \le DD'$ and $DD' \le \gcd(mn, \ell)$, it follows that $\gcd(mn, \ell) = DD'$. ∎

[Note: It is essential that $\gcd(m, n) = 1$ (consider $m = n = \ell = 5$).]
(d) Using the same notation in (b), we are to show that $\gcd(mn, \ell) = 1$ if and only if $D = 1$ and $D' = 1$.

First, suppose $D = 1$ and $D' = 1$. In (b), $(*)$ showed that $\gcd(mn, \ell) \le DD' = 1$, which proves $\gcd(mn, \ell) = 1$.

Now, suppose $\gcd(mn, \ell) = 1$. Any divisor of m and ℓ is also a divisor of mn and ℓ so $\gcd(m, \ell) \le \gcd(mn, \ell) = 1$. Similarly, $\gcd(n, \ell) \le \gcd(mn, \ell) = 1$. We conclude that $\gcd(m, \ell) = \gcd(n, \ell) = 1$. ∎

(e) Let $D = \gcd(\gcd(\ell, m), n)$ and $D' = \gcd(\ell, \gcd(m, n))$. Since $D|\gcd(\ell, m)$, $d|\ell$ and $d|m$; also $D|n$. Since $D|m$ and $D|n$, by GCD fact (ii) on page 132, $D|\gcd(m, n)$. Thus, D is a common divisor of ℓ and $\gcd(m, n)$, and $D \le D'$.

A similar argument proves reversed inequality $D' \le D$: D' divides ℓ, m and n; this means $D'|\gcd(\ell, m)$ and hence D' is a common divisor of $\gcd(\ell, m)$ and n. It follows that $D' \le D$. Therefore, $D = D'$. ∎

Exercise 10.8.

(a) By Bezout, we know $\gcd(m, n) = mx + ny = m(x + \alpha n) + n(y - \alpha m)$. By taking α as large as we wish, we can get Bezout coefficients so that the coefficient of m is positive. Now consider the smallest non-negative coefficient x, so $\gcd(m, n) = mx + ny$ and there is no smaller non-negative Bezout coefficient x. We claim $0 \le x < n$, because otherwise $x - n$ and $y + m$ are Bezout coefficients and $x - n$ is non-negative and smaller than x (a contradiction).

(b) Suppose $\gcd(m, n) = mx + ny = mx' + ny'$, where $0 \le x < x' < n$. Then $m(x' - x) = n(y - y')$ and n divides the RHS, so $n|m(x' - x)$. Since $\gcd(m, n) = 1$, it means $n|(x' - x)$ which is impossible because $0 < x' - x < n$. This contradiction proves that x' does not exist.

For the counter example, consider $m = 2, n = 4$. Then $\gcd(m, n) = 2 = 2 \cdot 1 + 4 \cdot 0 = 2 \cdot 3 - 4 \cdot 1$.

Exercise 10.9. We use induction on n. The base case is $n = 2$: if $p|q_1q_2$, then, by Euclid's Lemma, $p = q_1$ or $p = q_2$. For the induction, assume that for *any* n primes, if $p|q_1 \cdots q_2$ then p equals one of the q_i. Consider *any* $n+1$ such that $p|q_1 \cdots q_nq_{n+1}$. That is $p|(q_1 \cdots q_n)q_{n+1}$. By Euclid's Lemma, either $p|q_{n+1}$ or $p|q_1 \cdots q_n$. In the former case, because q_{n+1} is prime, $p = q_{n+1}$; in the latter case, by the induction hypothesis p equals one of the q_i. In either case p equals one of the $n + 1$ primes $q_1, \ldots, q_{n+1}$, proving the claim for $n + 1$. The claim follows by induction for $n \ge 2$. ∎

Pop Quiz 10.10. This is the Fundamental Theorem of Arithmetic in disguise. Every $n \ge 2$ is a product of primes, $n = p_1p_2 \cdots p_n$: a_1 is the number of times 2 appears; a_2 is the number of times 3 appears; and so on. The a_i must be unique because if not, then n is a product of primes in two different ways, which cannot be. ∎

Exercise 10.11. (a) False. 83 is prime, so if $83|38 \times 37 \times \cdots 1$, then 83 divides one of the terms in the product, which can't be as all the terms are smaller than 83. (b) True. $p^2 - 1 = (p - 1)(p + 1)$. Since p is prime, both $p - 1$ and $p + 1$ are even, and one is divisible by 4. So $p^2 - 1 = 8k$. Also, 3 divides $p^2 - 1$ because 3 divides one of the three consecutive numbers $p - 1, p, p + 1$, and it's not p because p is prime. Hence $3|8k$ and so $3|k$,that is $k = 3\ell$ and $p^2 - 1 = 24\ell$.

Exercise 10.12. We must show $\gcd(kM_1, kM_2) = k$. The only divisors of kM_1 are 1, k and M_1, since k and M_1 are different primes. Similarly, the only divisors of kM_2 are 1, k and M_2. The largest common divisor is k. ∎

Exercise 10.13. We have: $a \equiv b \pmod d$ and $r \equiv s \pmod d$. That is,

$$a - b = k_1 d \qquad \text{and} \qquad r - s = k_2 d.$$

(a) $ar - bs = (b + k_1d)(s + k_2d) - bs = (k_1s + k_2b + k_1k_2d)d$. So, $d|ar - bs$, i.e. $ar \equiv bs \pmod d$. ∎

(b) $(a + r) - (b + s) = b + k_1d + s + k_2d - b - s = (k_1 + k_2)d$. So, $d|(a + r) - (b + s)$, i.e. $a + r \equiv b + s \pmod d$. ∎

(c) We use (a) and induction. When $n = 1$, we are given that $a \equiv b \pmod d$. Suppose $a^n \equiv b^n \pmod d$. Applying (a) with $r = a^n$ and $s = b^n$, we get $a^{n+1} \equiv b^{n+1} \pmod d$. By induction, $a^n \equiv b^n \pmod d$ for $n \ge 1$. ∎

Pop Quiz 10.14.

(a) (mod 3): Oserve that $5^2 \equiv 1$. Therefore by Exercise 10.12(c), $5^{2n} \equiv 1^{2n}$. Note $1^{2n} = 1$. So, $5^{2014} \equiv 1$. Multiplying both sides by 5 (Exercise 10.12(a)), $5^{2015} \equiv 5 \equiv 2$. The remainder is 2.

(b) (mod 5): 5^{2015} is divisible by 5 so the remainder is 0.

(c) (mod 7): $5^3 \equiv -1$, so $5^{2013} = (5^3)^{671} \equiv (-1)^{671} \equiv -1$. Hence, $5^{2015} \equiv -25 \equiv 3$. The remainder is 3.

(d) (mod 9): $5^3 \equiv -1$, so $5^{2013} = \equiv -1$. Hence, $5^{2015} \equiv -25 \equiv 2$. The remainder is 2.

(e) (mod 11): $5^5 \equiv 1$, so $5^{2015} = (5^5)^{403} \equiv (1)^{403} \equiv 1$. The remainder is 1.

Exercise 10.15.

(a) $x = 15^{-1} \pmod 6$ which does not exist because $\gcd(15, 6) = 3 > 1$. Alternatively, $15x - 1 = 6k \to 15x - 6k = 1$, a contradiction (LHS is divisible by 3, not the RHS). Hence x does not exist.

(b) $x = 15^{-1} \pmod 7$, so $x = 1$. To get all solutions we can add any integer multiple of 7, so $x = 1 + 7k, k \in \mathbb{Z}$.

(c) $15x - 6 = 27k \leftrightarrow 5x - 2 = 9k$ so $5x \equiv 2 \pmod 9$. Note, $5^{-1} \equiv 2 \pmod 9$ because $2 \cdot 5 \equiv 1 \pmod 9$. We need $5x \equiv 2 \to 5^{-1} \cdot 5x \equiv 5^{-1} \cdot 2 \to x \equiv 4 \pmod 9$, because $5^{-1} \cdot 5 \equiv 1$. Adding multiples of 9 gives $x = 4 + 9k, k \in \mathbb{Z}$.

Exercise 10.16.

(a) (i) If $k = 0$ then $0^p = 0$ and $0 - 0 = 0$ is divisible by p. If $k = p$ then $p^p - p = p(p^{p-1} - 1)$ is divisible by p.

(ii) If $i \in \{1, \ldots, p - 1\}$, then $\gcd(p, i) = 1$. If $p|ik$ then by Exercise 10.7(a), $p|k$, that is k is a multiple of p, a contradiction. So, p does not divide ik and ik is not a multiple of p.

(iii) Immediate from Theorem 10.9 on page 135, because $\gcd(k, p) = 1$.

(iv) Since ik is not a multiple of p, by part (ii), $\alpha_i \ne 0$. Thus, $\alpha_i \in \{1, 2, \ldots, p - 1\}$.

Suppose $i, j \in \{1, \ldots, p - 1\}$. We show, by contradiction, that if $i \ne j$ then $\alpha_i \ne \alpha_j$. Suppose $\alpha_i \ne \alpha_j$. Then $ik = q_ip + \alpha_i$ and $jk = q_jp + \alpha_i$. Subtracting, $ik - jk = (q_i - q_j)p$. That is, $ik \equiv jk \pmod p$. By (iii), $i \equiv j$

(mod p). Since $i, j \in \{1, 2, \ldots, p-1\}$, this means $i = j$, a contradiction. Thus, $\alpha_i \neq \alpha_j$. Since no two α_i are equal, $\alpha_1, \alpha_2, \ldots, \alpha_{p-1}$ is a permutation of $1, 2, \ldots, p-1$, which means $\prod_{i=1}^{p-1} \alpha_i = (p-1)!$.

(v) Since $ik \equiv \alpha_i \pmod p$, by repeaded use of Exercise 10.12, $\prod_{i=1}^{p-1} ki \equiv \prod_{i=1}^{p-1} \alpha_i \pmod p$. $\prod_{i=1}^{p-1} ki = k^{p-1}(p-1)!$ and by (iv), $\prod_{i=1}^{p-1} \alpha_i = (p-1)!$, therefore

$$k^{p-1}(p-1)! \equiv (p-1)! \pmod p. \qquad (*)$$

If p divides $(p-1)!$, by Euclid's Lemma on page 133, p divides some term in the product. Since every term in the product is less than p, that is not possible, so p does not divide $(p-1)!$. The only other divisor of p is 1, so $\gcd(p, (p-1)!) = 1$. Use Theorem 10.9 on page 135, to cancel $(p-1)!$ from both sides of $(*)$ to get

$$k^{p-1} \equiv 1 \pmod p.$$

Multiplying both sides by k, since $k \equiv k \pmod p$, gives Fermat's Little Theorem.

(b) If p divides k, no multiplicative inverse exists as $\gcd(k, p) = p > 1$. If p doesn't divide k, $k^{p-1} \equiv 1 \pmod p$. Let $k^{-1} \equiv k^{p-2} \pmod p$. Then $k \cdot k^{-1} \equiv k^{p-1} \equiv 1 \pmod p$. That is, k^{p-2} is the multiplicative inverse of k.

(c) (i) We find x, y such that $8x + 19y = 1$ using the remainders in Euclid's GCD-algorithm:

$$\begin{aligned}
\gcd(8,19) &= \gcd(3,8) & \operatorname{rem}(19,8) = 3 &= -8 \cdot 2 + 19 \\
&= \gcd(2,3) & \operatorname{rem}(8,3) = 2 &= 8 - \mathbf{3} \cdot 2 \\
& & &= 8 - (-8 \cdot 2 + 19) \cdot 2 \\
& & &= 8 \cdot 5 - 19 \cdot 2. \\
&= \gcd(1,2) = 1 & \operatorname{rem}(3,2) = 1 &= \mathbf{3} - \mathbf{2} \\
& & &= -8 \cdot 2 + 19 - (8 \cdot 5 - 19 \cdot 2) \\
& & &= 8 \cdot (-7) + 19 \cdot 3.
\end{aligned}$$

Therefore $x = -7$ and $8^{-1} = \operatorname{rem}(-7, 19) = 12$. Indeed, $8 \times 12 \equiv 1 \pmod{19}$ because $8 \times 12 - 1 = 19 \times 5$.

(ii) $8^{-1} \equiv 8^{17} \pmod{19}$. We observe that $8^3 \equiv -1 \pmod{19}$. Therefore,

$$8^{15} \equiv (-1)^5 \equiv -1 \pmod{19}.$$

Finally, $8^{17} \equiv -64 \equiv 12 \pmod{19}$, so $8^{-1} = 12$ (for modulus 19).

Exercise 10.17. $M^{p-2}M_* \equiv M^{p-1}k \pmod p$. Assuming M is not a multiple of p, by Fermat's Little Theorem, $M^{p-1} \equiv 1 \pmod p$. Multiplying both sides by k gives $M^{p-1}k \equiv k \pmod p$, that is,

$$M^{p-2}M_* \equiv M^{p-1}k \equiv k \pmod p.$$

So Charlie obtains k by computing $\operatorname{rem}(M^{p-2}M_*, p)$.

Exercise 10.18. Alice encrypts to $M_* \equiv M^{225} \pmod{391}$ and Bob decrypts with $M_*^{97} \pmod{391}$. E.g., for $M = 2$,

$$2^7 \equiv 128 \to 2^{14} \equiv 128^2 \equiv 353 \to 2^{28} \equiv 353^2 \equiv 271 \to 2^{56} \equiv 271^2 \equiv 324 \to 2^{112} \equiv 324^2 \equiv 188,$$

and finally we have $2^{225} \equiv 2 \cdot 188^2 \equiv 308 \pmod{391}$. Bob decrypts as follows:

$$308^3 \equiv 246 \to 308^6 \equiv 246^2 \equiv 302 \to 308^{12} \equiv 302^2 \equiv 101 \to 308^{24} \equiv 101^2 \equiv 35 \to 308^{48} \equiv 35^2 \equiv 52,$$

and finally we have $308^{97} \equiv 308 \cdot 52^2 \equiv 2 \pmod{391}$. Here is the table of results for $M = 2, \ldots, 10$,

M	2	3	4	5	6	7	8	9	10	
M_*	308	105	242	158	278	109	246	77	180	(Bob always recovers M.)
Bob's decryption	2	3	4	5	6	7	8	9	10	

Exercise 10.19. Let $n = pq$; $M_* \equiv M^e \pmod n$. We decode using $M_*^d \equiv M^{ed} \pmod n$, and must show $M^{ed} \equiv M \pmod n$ (i.e. we recover the correct message for any M).

(a) Since $ed \equiv 1 \pmod{(p-1)(q-1)}$, $ed - 1$ is divisible by $(p-1)(q-1)$, or $ed - 1 = k(p-1)(q-1)$ for $k \in \mathbb{Z}$.

(b) (i) By (a) $ed - 1 = k(p-1)(q-1)$, so $M^{ed-1} = M^{k(p-1)(q-1)}$.

(ii) By Fermat's Little Theorem, $M^{p-1} \equiv 1 \pmod p$ (because p does not divide M). This means $M^{p-1} - 1 = \alpha p$ for an integer α, or that $M = 1 + \alpha p$. Therefore,

$$M^{ed-1} = M^{k(p-1)(q-1)} = (M^{p-1})^{k(q-1)} = (1 + \alpha p)^{k(q-1)}.$$

(iii) By the Binomial Theorem,

$$(1 + \alpha p)^{k(q-1)} = 1 + \sum_{i=1}^{k(q-1)} \binom{k(q-1)}{i} \alpha^i p^i = 1 + p \underbrace{\sum_{i=1}^{k(q-1)} \binom{k(q-1)}{i} \alpha^i p^{i-1}}_{\beta}.$$

We could also use $a^r - 1 = (a-b)(1 + a + a^2 + \cdots + a^{r-1})$ with $a = 1 + \alpha p$:

$$(1 + \alpha p)^{k(q-1)} - 1 = p \underbrace{(\alpha + \alpha(1 + \alpha p) + \alpha(1 + \alpha p)^2 + \cdots + \alpha(1 + \alpha p)^{k(q-1)-1})}_{\beta}.$$

Either way, β is a sum of integers, hence an integer. We have proved: $M^{ed-1} = (1 + \alpha p)^{k(q-1)} = 1 + \beta p$. ∎

(iv) From (iii), $M^{ed-1} - 1 = \beta p$, that is $p | M^{ed-1} - 1$.

(c) By (b), either p divides M or if not then it must divide $M^{ed-1} - 1$. That is p must divide their product $M^{ed} - M$. Everything is symmetric with respect to p and q and so using exactly the same reasoning, $q | M^{ed} - M$.

(d) Since $\gcd(p, q) = 1$ and both $p | M^{ed} - M$ and $q | M^{ed} - M$, Exercise 10.7(b) on page 132 gives $pq | M^{ed} - M$.

(e) From (d), by definition, $M^{ed} \equiv M \pmod{pq}$. Bob can decode by computing $\text{rem}(M_*^d, pq)$.

Chapter 11

Pop Quiz 11.1.

(a) $V = \{1, 2, 3, 4, 5, 6\}$; $E = \{(1, 2), (2, 3), (3, 4), (1, 4)\}$;

(b) $V = \{a, b, c, d, 1, 6\}$; $E = \{(a, b), (b, c), (c, 1), (a, 1)\}$;

(c) $V = \{i, j, k, \ell, m, n\}$; $E = \{(i, m), (j, \ell), (j, m), (j, n), (k, m), (k, n)\}$;

(d) $V = \{i, j, k, \ell, m, n\}$; $E = \{(i, \ell), (i, j), (j, m), (\ell, m), (j, k), (m, n)\}$;

Exercise 11.2. Isomorphic graphs: {I, II}

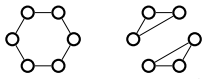
(a) Relabeling doesn't change the number of vertices. Similarly, the edge end points are relabelled, but their number is unchanged.

(b) In the relabeling, suppose vertex v is repabeled to $\ell(v)$. Then every edge in the graph (v, w) becomes $(\ell(v), \ell(w))$ and $\deg(v)$ becomes $\deg(\ell(v))$. Every vertex w which contributes to $\deg(v)$ is relabeled to a vertex $\ell(w)$ which contributes to the degree of $\ell(v)$. Therefore, the degree of each vertex does not change.

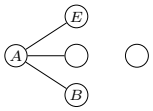
(c) Suppose $v_1 v_2 \cdots v_k$ is a path. Every edge (v_i, v_{i+1}) is in the graph since $v_1 v_2 \cdots v_k$ is a path. After relabeling, the edge $(\ell(v_i), \ell(v_{i+1}))$ is in the relabeled graph. Hence $\ell(v_1)\ell(v_2) \cdots \ell(v_k)$ is a path in the relabeled graph.

(d) Every path is preserved as a relabeled path. This includes shortest paths and shortest path lengths.

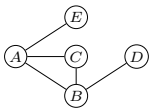
Exercise 11.3. There were some trick questions in this exercise.

(a)  An isomorphism preserves all paths (see Exercise 11.2). In the first graph, there is a path between every pair of vertices, but not so in the second, so the graphs cannot be isomorphic.

(b) Trick question. All graphs with the degree sequence [3,3,2,1,1] are isomorphic. To see this label the vertices A, B, C, D, E (highest to lowest degree). A has 3 neighbors. Either B is one of these neighbors or not. If not, then since B also has degree 3, A and B are neighbors of C, D, E. This is not possible since C, D, E have respective degrees $2, 1, 1$. Therefore B is a neighbor of A. The situation is illustrated on the right. (Since there are two degree 1 vertices, at least one (E) is a neighbor of A.)



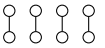
Since E cannot have any more neighbors, and B must have two more neighbors, it must be that B is connected to the other two vertices, completing the picture as shown on the right. There is no other way to construct a graph with this degree sequence. (Not all degree sequences can be realized by different, non-isomorphic, graphs. Another classic example is $[n-1, 1, 1, \ldots, 1]$.)



(c) Trick question. No graph has these degrees because the sum of the degrees is 13 (more later).

Pop Quiz 11.4. This graph cannot exist because there are an odd number of odd-degree vertices.

Exercise 11.5.

(a) If every degree is positive, $2m = \sum_i \delta_i \geq n$, so $m \geq n/2$. Example: 

(b) Equivalently, we compute the maximum number of edges a graph with a degree 0 vertex can have. Let v be the degree 0 vertex and n the number of vertices. Every vertex other than v can have an edge to every vertex other than v, so ever vertex other than v has degree $n - 1$. The number of edges is $\frac{1}{2}(n-1)(n-2)$ (half the sum of the degrees). This is the maximum number of edges for a graph with a degree 0 vertex. So, if a graph has $1 + \frac{1}{2}(n-1)(n-2)$ edges, it cannot have a degree 0 vertex.

(c) The sum of the degrees is $5 \times 3 = 15$. There are no such graphs, since the sum of the degrees must be even. You could also argue that such a graph would have 5 vertices of odd degree, which violates Corollary 11.3.

Exercise 11.6.

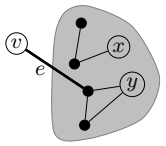
(a) The dotted edge creates a cycle, and a tree is connected with no cycles.

(b) Steps 1–5 are not connected. After step 6, any new edge would create a cycle.

(c) This is an important result so we give two different proofs.

Theorem 30.1. A graph with fewer than $n - 1$ edges is not connected.

Proof. We prove the claim by induction on n. The base case is $n = 2$ in which case the graph with 0 edges is clearly not connected. Consider any graph with $n + 1$ vertices and fewer than n edges. Every vertex cannot have degree at least 2 (the sum of the degrees would be at least $2(n + 1)$ implying at least $n + 1$ edges), so some vertex v has degree less than 2. If $\deg(v) = 0$ then the graph is disconnected as was to be shown.

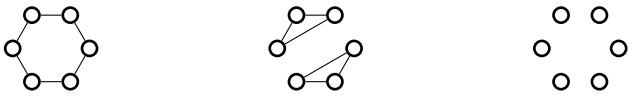


We show the situation with $\deg(v) = 1$ on the right. The shaded region is the rest of the graph, other than v, and there is an edge e from v to *one* node in the shaded region. Remove v and e from the graph. The shaded graph that remains has n vertices and fewer than $n-1$ edges (we removed one vertex and edge). By the induction hypothesis, this residual (shaded) graph is not connected: two vertices (illustrated by x and y) are not connected by any path. Adding back v and e cannot create a path between x and y, so x and y remain disconnected in the original graph. Thus, any graph with $n+1$ vertices and fewer than n edges is not connected, so the theorem follows by induction. ∎

We now give a proof of a more general result from which Theorem 30.1 follows. A component in a graph is a "maximal" set of vertices that is connected. The *component* of a vertex v is all the vertices connected to v,

$$\mathcal{C}(v) = \{u \mid u \text{ is connected to } v \text{ by a path}\}.$$

Any vertex in a component can be used to define that component, that is if $u \in \mathcal{C}(v)$ then $\mathcal{C}(u) = \mathcal{C}(v)$: any vertex in $\mathcal{C}(v)$ is connected to u by going first from u to v and then to the vertex, hence $\mathcal{C}(v) \subseteq \mathcal{C}(u)$; similarly any vertex in $\mathcal{C}(u)$ is connected to v by going first from v to u and then to the vertex, hence $\mathcal{C}(u) \subseteq \mathcal{C}(v)$.



1 component 2 components 6 components

A connected graph has one component. A graph with n isolated vertices (no edges) has n components. Adding an edge between two vertices in the same component, does not change the components. Adding an edge between two vertices in different components merges those two components, decreasing the number of components by 1.

Lemma 30.2. Adding an edge can decrease the number of components by at most 1.

We use this lemma to prove our general result:

Theorem 30.3. A graph with n vertices and e edges has at least $n-e$ components.

Proof. Start with the n isolated vertices, (n components) and add the edges one by one, each time decreasing the number of components by *at most* one. So the number of components decreases by at most e, leaving at least $n-e$ components. The formal proof is by induction on e, the number of edges. In the induction step start with $e+1$ edges and remove an edge. By the induction hypothesis there are at least $n+1-e$ components. Add back the edge and apply Lemma 30.2 to conclude there are at least $n-e$ components. ∎

Theorem 30.3 implies Theorem 30.1 because if $e < n-1$, then number of components $> n-(n-1) = 1$. This means the number of components is at least 2 and the graph is disconnected.

(d) Suppose the graph has $n+k$ edges, where $k \geq 0$. We first prove the case that the graph has a single component. This means that for any set of vertices there is at least one edge from a vertex in the set to a vertex not in the set (otherwise that set of vertices is disconnected from the rest of the graph).

Let us build a connected component by adding one vertex at a time. Start at any vertex v_1. There must be an edge from v_1 to a second vertex v_2. So we have build the set v_1, v_2. After we have built the set $v_1, v_2, \ldots, v_i$, there must be an edge from a vertex in our set to an $i+1$th vertex v_{i+1}. Continue this process until we have built the set containing all the nodes $v_1, \ldots, v_n$ using $n-1$ edges. By construction, this set of vertices is connected using only the $n-1$ edges – this set of $n-1$ edges is called a *spanning tree*.

There is at least one more edge in the graph, say (v_i, v_j), since the graph has at least n edges. Before adding the edge (v_i, v_j), there was a path from v_i to v_j in the spanning tree. The edge (v_i, v_j) plus this path is a cycle.

The formal proof is by strong induction. In the induction step, take any graph with n vertices and $n+k$ edges. Remove an edge e. If the graph stays connected, replacing e creates a cycle. If the graph gets disconnected then one of the components has as many edges as vertices and contains a cycle. Replacing e won't remove that cycle.

Now consider a graph with more than one component. Suppose the graph has ℓ components with $n_1, n_2, \ldots, n_\ell$ vertices in each component, and $e_1, e_2, \ldots, e_\ell$ edges in each component: $n_1+n_2+\cdots+n_\ell = n$ and $e_1+e_2+\cdots+e_\ell = e$. We claim that for some i^*, $e_{i^*} \geq n_{i^*}$ because if not, then $e_i < n_i$ for every i and

$$e = e_1 + e_2 + \cdots + e_\ell < n_1 + n_2 + \cdots + n_\ell = n,$$

which cannot be since $e \geq n$. There must therefore be a cycle in the i^*th component and hence in the graph.

(e) Since this is an "if and only if", there are two parts to the proof.

1. Suppose tree G is connected and has n vertices. By (d), if G has fewer than $n-1$ edges, it is not connected. If G has n or more edges, then by (e) it has a cycle and is not a tree. Hence G has $n-1$ vertices.

2. Suppose G is connected with n nodes and $n-1$ edges. We show G is a tree, i.e. there are no cycles. Suppose G has a cycle. Remove an edge on this cycle. Every vertex remains connected with every other vertex, hence the graph remains connected but has $n-2$ edges. This contradicts (d). Hence G has no cycles.

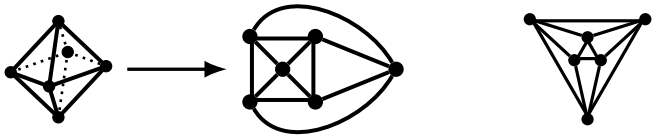
Exercise 11.7.

(a)

	Pyramid	Cube	Octahedron
V	4	8	6
E	6	12	12
F	4	6	8
$F+V-E$	2	2	2

(b) For the pyramid, project the apex onto the base. Similarly for the cube, after moving out the base vertices.

For the octahedron, project the upper apex down to the base plane and place the lower apex outside the base.



(To get the more symmetric looking graph (right) project an upper triangular face into the opposite lower triangular face.)

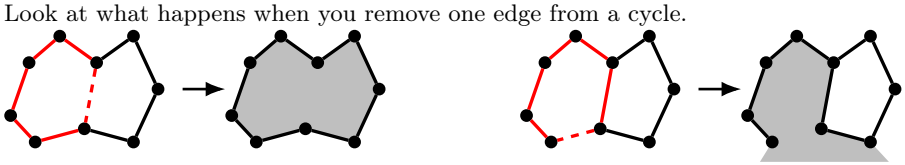
(c) The faces become regions (polygons). One of the faces becomes the external (unbounded) region.

(d) There is only one external face, so $F = 1$. For a tree, we know from Exercise 11.6 that $E = V - 1$. Therefore,

$$F + V - E = 1 + V - (V - 1) = 2.$$

(e) Consider a connected graph that is not a tree (i.e. has cycles).

(i) Look at what happens when you remove one edge from a cycle.



There are two cases: the edge is between two internal faces (left) and the internal faces merge into one internal face; the edge is between an internal face and the external face (right) and the external face merges with the internal face to make a larger external face. In either case, the number of faces F decreases by 1. We removed one edge but the number of vertices remained the same. So,

$$\Delta E = -1; \qquad \Delta F = -1; \qquad \text{and} \qquad \Delta V = 0.$$

Paths not using the removed edge are unaffected. Paths using the removed edge can go the other way around the cycle (instead of using the edge). Thus, if there was a path between two vertices, there still is.

Removing an edge from a cycle does not affect connectivity

(ii) Removing an edge from a cycle decreases E and F by the same amount, so the total change will be the same, $\Delta E = \Delta F$. The vertices are unchanged so $\Delta V = 0$.

(iii) When you remove the last edge, the graph is connected. Therefore it is a tree. In this process, $F \to F + \Delta F$, $E \to E + \Delta E$ and $V \to V + \Delta V$. For a tree, we proved in (d) that (faces) + (vertices) − (edges) = 2, therefore

$$F + \Delta F + V + \Delta V - (E + \Delta E) = 2,$$

where F, V and E are for the original graph with cycles. Since $\Delta V = 0$ and $\Delta F = \Delta E$, $F + V - E = 2$.

(f) When you traverse around every face, $\sum_f E(f)$ edges are traversed. Every edge is traversed twice: Edges on internal faces belongs to two faces and so are traversed once for each face; Edges on the external face that are not on an internal face are also traversed twice, back and forth. Since every edge is traversed twice, $\sum_f E(f) = 2E$.

(g) Internal faces are bounded by 3 or more edges, so $E(f) \geq 3$. If $V \geq 3$, the external face has at least 3 vertices and hence $E(\text{external face}) \geq 3$. Therefore $2E = \sum_f E(f) \geq 3F$. That is $F \leq \frac{2}{3}E$. Using Euler's Characteristic,

$$E \;=\; F + V - 2 \;\leq\; \tfrac{2}{3}E + V - 2 \quad\to\quad \tfrac{1}{3}E \leq V - 2 \quad\to\quad E \leq 3V - 6$$

In any planar graph with at least 3 vertices, $E \leq 3V - 6$.

In a planar graph, #edges $\propto$ #vertices. In K_5 $3V - 6 = 9$; yet, $E = 10$ which is greater, so K_5 cannot be planar.

(h) If there are no 3-cycles, then $E(f) \geq 4$ for every internal face f, because traversing around an internal face creates a cycle. The external face contains at least 3 vertices in which case going around the external face traverses at least 4 edges, so again $E(f) \geq 4$. Therefore, $2E = \sum_f E(f) \geq 4F$ and, using Euler's Characteristic,

$$E \;=\; F + V - 2 \;\leq\; \tfrac{1}{2}E + V - 2 \quad\to\quad \tfrac{1}{2}E \leq V - 2 \quad\to\quad E \leq 2V - 4$$

Any simple graph has no 2-cycles. In $K_{3,3}$ there are no 3-cycles because any path of odd length takes you from one side to the other. In $K_{3,3}$, $V = 6$, so $2V - 4 = 8$, but $E = 9$ which is larger, so $K_{3,3}$ cannot be planar.

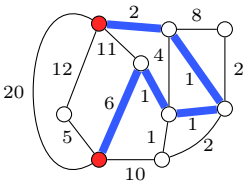
Exercise 11.8. Vertices in Euler's multi-graph are regions of Königsberg and edges are the bridges that connect two regions. Euler's problem is to start at a vertex, and follow a path of edges, ending at another vertex. The requirement is that every edge must be traversed exactly once. Other than the start and end vertex, every other vertex, if entered using some (untraversed) edge must be exited using a different (untraversed) edge, which means these vertices must have an even degree. Every vertex in Euler's graph has an odd degree, so Euler's problem is not solvable.

A path which uses every edge is called an *Euler tour*. If the path-endpoints are the same, it is an *Euler cycle*.

Theorem 30.4. A connected graph has an Euler cycle if and only if every vertex has even degree. A connected graph has an Euler tour from u to v if and only if the degrees of u and v are odd and every other vertex has even degree.

There are two parts to an if and only if proof. Try induction for the "hard part".

Exercise 11.9. We highlight the fastest path in blue, which takes 11ms. The fastest path is counterintuitive because it doesn't always move "toward" the destination. When you take a course in algorithms you will learn how to systematically compute shortest paths when the edge weights are non-negative. The idea is to compute the shortest paths to all vertices simultaneously, starting with the closest vertex, then the next closest and so on. The technique is called dynamic programming and the algorithm is Dijkstra's algorithm.



Pop Quiz 11.10.

(a) $V = \{v_1, v_2, v_3, v_4, v_5, v_6, v_7\}$ and $E = \left\{ \begin{matrix} (v_1 \to v_2), (v_3 \to v_1), (v_3 \to v_2), (v_2 \to v_4), \\ (v_2 \to v_5), (v_3 \to v_4), (v_5 \to v_4), (v_6 \to v_7), \\ (v_2 \to v_1), (v_4 \to v_2), (v_6 \to v_2) \end{matrix} \right\}$.

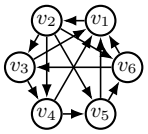
(b) The graph is not (strongly) connected (there is no path from v_7 to any other node).

Exercise 11.11.

(a) M, Z, D are top-dogs.

(b) Let t be a vertex with maximum out-degree (in case of ties, pick any one). We prove that t is a top-dog, i.e. t dominates every any other node u (either t beats u or t beats a vertex that beats u). Suppose, to the contrary, t does not dominate some vertex v. That is, v beats t and also beats everyone who t beats. Then out-deg(v) is at least $1 +$ out-deg(t), which contradicts t having maximum out-degree. Therefore such a v does not exist.

(c) Let $v_1 \to v_2$ but $v_i \to v_1$ for $i > 2$. So, v_1 wins one match. Let $v_2 \to v_i$ for $i > 2$. So, v_2 beats everyone but v_1. By construction, v_1 is a top-dog, having beaten just one vertex. Pick $v_2, \ldots, v_n$ to all have out-degree at least 2, e.g. $v_3 \to v_4 \to \cdots \to v_n \to v_3$ (all other match results can be arbitrary). This means v_1 won the fewest possible matches and yet is a top-dog.



Chapter 12

Exercise 12.1.

(a) Let $|E|$ be the total number of partners for men, which is the total number of partners for women have since every partnership is between a man and a woman. Let M be the number of men and F the number of women. Then,

$$\text{average partners per man} = \frac{|E|}{M} = \frac{|E|}{F}\frac{F}{M} = \text{average partners per woman} \times \frac{F}{M}.$$

Since $F/M = 50.8/49.2 \approx 1.0325$, average per man = average per woman $\times$ 1.0325. 3.25% more for men.

(b) Let $|E|$ be the number of heterosexual relationships, e_m be the number of same-sex relationships among males, and e_f the number of same-sex relationships among females. We have $e_m + e_f$ is 1% of all relationships,

$$\frac{e_m + e_f}{|E| + e_m + e_f} = 0.01 \qquad\to\qquad e_m + e_f = \frac{0.01}{0.99} \times |E|.$$

The total number of partners is $|E| + 2e_m$ for men and $|E| + 2e_f$ for women. So,

$$\text{average partners per male} = \frac{|E| + 2e_m}{M} \qquad \text{average partners per female} = \frac{|E| + 2e_f}{F}.$$

Taking the ratio,

$$\frac{\text{average partners per male}}{\text{average partners per female}} = \frac{|E| + 2e_m}{|E| + 2e_f} \times \frac{F}{M}.$$

The two extremes are when $e_m = 0$ and when $e_f = 0$. When $e_m = 0$, $e_f = |E| \times \frac{0.01}{0.99}$ and

$$\frac{\text{average partners per male}}{\text{average partners per female}} = \frac{\cancel{|E|}}{\cancel{|E|} + 2\cancel{|E|} \times \frac{0.01}{0.99}} \times \frac{F}{M} \approx 1.012.$$

When $e_f = 0$, $e_m = |E| \times \frac{0.01}{0.99}$ and

$$\frac{\text{average partners per male}}{\text{average partners per female}} = \frac{\cancel{|E|} + 2\cancel{|E|} \times \frac{0.01}{0.99}}{\cancel{|E|}} \times \frac{F}{M} \approx 1.0534.$$

On average, men have $1.2\% - 5.3\%$ more partners, depending on how the same sex relationships are distributed.

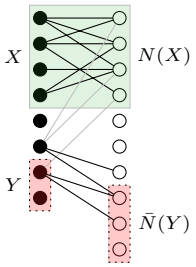
Pop Quiz 12.2. $(T_1, R_1), (T_2, R_3)(T_3, R_4), (T_4, R_5)$.

Exercise 12.3. For $|L| = 1$ (base case), pick any edge. Assume the theorem for $|L| \le n$. Consider $|L| = n + 1$.

(a) Case 1. Some proper left-subset X, with $1 \le |X| < n + 1$, has $|X| = |N(X)|$. The graph has two parts: X and its neighborhood $N(X)$, and the rest of the graph. $(X, N(X))$ satisfies Hall's condition so by the induction hypothesis X has a matching into $N(X)$. For any left-subset Y outside X, its neighborhood may overlap with $N(X)$ (gray edges). Let $\bar{N}(Y)$ be that part of $N(Y)$ not overlaping with $N(X)$. From the matching condition,

$$|N(X)| + |\bar{N}(Y)| = |N(X \cup Y)| \overset{*}{\ge} |X \cup Y| = |X| + |Y|.$$

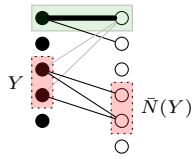
$*$ is because the full graph satisfies the matching condition. Since $|N(X)| = |X|$, we have $|\bar{N}(Y)| \ge |Y|$ satisfying the matching condition. By the induction hypothesis, the left-vertices outside X can be matched to the right-vertices outside $N(X)$. This gives a full left-matching.



(b) Case 2. Every proper left-subset X, has $|X| < |N(X)|$. Match the first left-vertex to any neighbor. In the remaining graph with n left-vertices, consider any left-subset Y and its neighborhood $\bar{N}(Y)$ in the remaining graph. Then the matching condition holds for Y,

$$|\bar{N}(Y)| \ge |N(Y)| - 1 \ge |Y|.$$

By the induction hypothesis, the remaining graph has left-matching, hence the full graph does.



In both cases, there is a left-matching which covers the $n+1$ left-vertices, which proves the Hall's theorem by induction.

Exercise 12.4. In the induction step, you might match and remove some left and right-vertices. Let us examine the residual graph. The degrees of some right-vertices decrease, but the maximum right-vertex degree *could stay the same*. If a removed a right-vertex was linked to remaining left-vertices, the degree of those left-vertices will decrease. This means that the minimum left-vertex degree *could decrease* and drop below the maximum right-vertex degree. Therefore, we may not be able to apply the induction hypothesis to the residual graph, and the proof by induction falters.

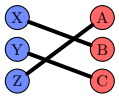
Hall's theorem implies Corollary 12.2 on page 164. Hall's theorem is stronger, yet easier to prove by induction because we assume more in $P(n)$ which offsets having to prove more in $P(n + 1)$.

Exercise 12.5. A matching is stable if there is no pair of matches that is volatile.

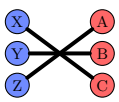
	X	Y	Z
1.	A	A	B
2.	B	C	A
3.	C	B	C

	A	B	C
1.	Z	Y	Z
2.	Y	X	X
3.	X	Z	Y

The match A–Z is "stable" because Z is A's top choice so A will not wish to break her current match. The only possible volatile pair is (X, Y) and (B, C). Since X prefers B to C, this is not a volatile pair. Since there are no volatile pairs of matches, the matching is stable.



We show a second matching. Again, Z is A's top choice, so the only possible volatile pair is (X, Y) and (B, C). Since B prefers Y to X, this is not a volatile pair. The matching is stable and A still gets her top choice. B prefers Y to X and C prefers X to Y so the girls prefer this second matching.



The boys prefer the first matching: Z is indifferent but X and Y are better off.

Exercise 12.6.

(a) If a woman w has more than one suitor, she chooses her favorite and the other suitors (at least one) cross w from their list. When there is at most one man under every woman's balcony, we have a stalemate. For every non-stalemate round (at least one woman has more than one suitor), a man crosses a woman from a list. There are a total of n^2 women on all the lists (each woman appears once on each list). Therefore there cannot be more than n^2 non-stalemate rounds of dating because there will be no more women left to cross out.

Conclusion: After at most n^2 rounds of dating, each woman has at most one suitor.

(b) If a woman w ever gets wooed, those suitors had w on the top of their current list. She picks her favorite who comes back (w remain on the top of that favorite's list). By induction, she will always have a suitor.

(c) According to the ritual, m woos as long as there are uncrossed women on his list. Since m is not married at the end, m has been rejected by every woman, which means that he has wooed every woman, including w.

If there is an unmarried man m at the end of the ritual, then there is an unmarried woman w who was wooed at sometime by m. By part (b), from that point on, w will always have a suitor and so must end up married, a contradiction. Therefore, every man is married at the end of the ritual (and therefore so too is every woman).

(d) Suppose w is at the ith position on m's list.

(a) If m never wooed w then m could not have been rejected by all the top $i-1$ candidates on m's list. Therefore m was ultimately accepted by one of these top $i-1$ candidates and ended up married to that better candidate: m prefers his current partner to w.

(b) If m did woo w, but is not married to w, then w rejected m for someone better, m'. From this point on, in the dating ritual, w will continue to accept only candidates who are at least as good as m' because m' will return to w unless someone *better* comes along and w rejects m'. Therefore, w will end up married to someone at least as good (in her view) as m', who she prefers to m: w prefers her current partner to m.

That the marriages are stable is now immediate from (i) and (ii). Consider *any* pair of married couples (m, w) and (m', w'). If m' had wooed w then w prefers m to m' and would not wish to switch to m'. If m' had not wooed w then m' prefers his current partner w' to w. Hence, the pair of married couples is not volatile.

Pop Quiz 12.7. The dating ends after two rounds.

Dating Round 1:

	A	B	C
1.	Z	Y	Z
2.	Y	X	X
3.	X	Z	Y

X	Y	Z
	B	A, ~~C~~

Dating Round 2:

	A	B	C
1.	Z	Y	~~Z~~
2.	Y	X	X
3.	X	Z	Y

X	Y	Z
C	B	A

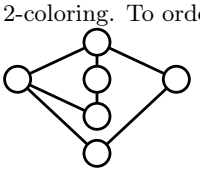
Pop Quiz 12.8.

(a) R_1, R_2, R_3 are a "clique": every pair has an edge. Therefore every vertex in this group must be colored a different color otherwise an edge will connect two vertices of the same color. Thus, we need at least 3 colors.

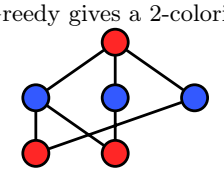
> If a graph contains a clique of size k then at least k colors are required.

(b) You need one color, and n suffice (color each vertex a different color). So $1 \leq \chi(G) \leq n$. The graph with n isoloted vertices needs can be colored with one color and K_n, the complete graph on n vertices, requires n colors.

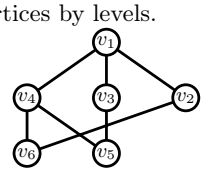
Exercise 12.9. The graph is an example of a leveled graph in which the nodes can be partitioned into levels $\ell = 1, 2, 3, 4, \ldots$ and edges only exist between vertices in adjacent levels. In this case you can alternate colors between levels and get a valid 2-coloring. We show how to represent the graph as a leveled graph which immediately gives a 2-coloring. To order the vertices so that Greedy gives a 2-coloring, simply order the vertices by levels.



Original graph G



Leveled view of G



Vertex ordering for Greedy

Exercise 12.10. Certainly if $V \leq 6$, then 6 colors are enough by coloring each vertex a different color. Therefore, we only need to consider $V > 6$ in which case $E \leq 3V - 6$.

(a) Suppose every node-degree is at least 6, then the sum of the node-degrees is at least $6V$, so

$$2E = \text{sum of node-degrees} \geq 6V.$$

We conclude that $E \geq 3V > 3V - 6$, which contradicts $E \leq 3V - 6$. So, at least 1 vertex has degree of 5 or less.

(b) Start with a planar drawing of a graph and remove a vertex and its edges. The remaining edges do not cross in the drawing that remains (since initially they did not cross). Therefore the remaining graph is planar.

(c) We use induction on V, the number of vertices in the graph. If $V \leq 6$ then the claim is trivially true. Suppose the claim is true for any planar graph of V vertices and consider *any* planar graph with $V + 1$ vertices. By (a), there

is a node with degree at most 5. Remove this vertex and its edges. By (b) the remaining graph is planar and has V vertices, so by the induction hypothesis this remaining graph is 6-colorable. Now add back the removed vertex, keeping the colors of the vertices obtained from the 6-coloring of the smaller graph. Among the 6 colors, there must be at least one free color for the node we added back because that vertex has at most 5 neighbors. Therefore, our graph with $V+1$ vertices is 6-colorable. By induction, every planar graph is 6-colorable.

(Every planar graph is 5-colorable. The same basic induction works, but you must be more careful in the induction step. The 4-color theorem says that every planar graph is 4-colorable, and that is hard to prove.)

Chapter 13

Exercise 13.1. We use induction on r. For $r=1$, there is nothing to prove. Suppose the product rule holds for sequences of length r and consider sequences of length $r+1$. Fix a prefix $X_1\cdots X_r$ to one of the possible choices of $x_1\cdots x_r$. By assumption, there are N_{r+1} choices for x_{r+1} *for this prefix*. So, there are N_{r+1} sequences that begin with $X_1\cdots X_r$, that is $|\{X_1\cdots X_r \bullet x_{r+1}\}| = N_{r+1}$. Define the type of a sequence by its prefix; there are $|\{x_1\cdots x_r\}|$ types. Every sequence $x_1\cdots x_r x_{r+1}$ is *one* of these types, depending on the prefix $x_1\cdots x_r$. So, by the sum rule,

$$|\{x_1\cdots x_r x_{r+1}\}| \;=\; \sum_{\substack{\text{prefixes}\\ X_1\cdots X_r}} |\{X_1\cdots X_r\bullet x_{r+1}\}| \;=\; \sum_{\substack{\text{prefixes}\\ X_1\cdots X_r}} N_{r+1}.$$

The last sum is just N_{r+1} times the number of possible prefixes,

$$|\{x_1\cdots x_r x_{r+1}\}| \;=\; |\{x_1\cdots x_r\}|\times N_{r+1} \;=\; (N_1\times N_2\times\cdots\times N_r)\times N_{r+1},$$

where the last equality follows by the induction hypothesis. This proves the induction step.

Pop Quiz 13.2. $10\times 9\times 8\times 7\times\cdots\times 2\times 1 = 10! = 3628800$.

Exercise 13.3. There are two types of outcome: HS_2 where S_2 is a sum of 2 dice; or TS_4 where S_4 is a sum of 4 dice. $S_2\in\{2,\ldots,12\}$ (11 choices) and $S_4\in\{4,\ldots,24\}$ (21 choices). The sum rule gives $11+21=32$ outcomes.

Exercise 13.4. Label the (distinguishible) "named" committees: 1, 2,..., 16.

(a) (i) An assignment can be specified by $s_1 s_2 s_3\cdots s_{100}$, where $s_i\in\{1,2,\ldots,16\}$ is the committee senator i gets assigned. By the product rule, there are 16^{100} such sequences, which equals the number of ways each senator can be assigned to exactly one of 16 "named" committees. (Ponder what happens if the committees are indistinguishable.)

(ii) A senator can be in 0 or 1 committee. The assignment can be specified by $s_1 s_2\cdots s_{100}$, where $s_i\in\{0,1,\ldots,16\}$: $s_i=0$ if senator i is assigned to no committee; otherwise, s_i is i's committee. By the product rule, there are 17^{100} such sequences, which is the number of ways each senator can be assigned to at most one of 16 "named" committees.

STOP: Skip the solution of (b) on first reading. It is hard.

(b) The complication arises because by requiring that each committee is not empty we introduce a dependency between the senators, where as previously the senators can be assigned independently. For example, if the first 99 senators all get assigned to the first 15 committees, now the only available choice for s_{100} is committee 16, otherwise that committee would be empty. Let us consider the case of 5 senators and 2 committees.

Exactly 1 committee per senator; no empty committee. When committees can be empty, there are 2^5 assignments. If all 5 senators are in either committee there is an empty committee, so these two assignments are not allowed. All others are allowed, so there are 2^5-2 ways.

Now consider n senators being distributed into k "named" committees (n distinguishable objects partitioned into k distinguishable non-empty sets). First suppose the committees are indistinguishable (not named). For example, with 5 senators and 3 committees, the following sequences $s_1 s_2 s_3 s_4 s_5$ are the same committees,

$$12333 \quad 21333 \quad 13222 \quad 31222 \quad 23111 \quad 32111.$$

What matters is who is in a committee with whom. Let $\left\{ {n \atop k} \right\}$ be the number of indistinguishable committees. Label the committees: pick one of the k labels for the first committee, one of the remaining $k-1$ labels for the second committee and so on resulting in $k\times(k-1)\times\cdots\times 1$ ways to label the committees (product rule). So,

$$\#\text{ ways to create } k \text{ non-empty "named" committees from } n \text{ senators} = k!\left\{ {n \atop k} \right\}.$$

The numbers $\left\{ {n \atop k} \right\}$ are known as *Stirling numbers of the second kind*,

$$\left\{ {n \atop k} \right\} = \#\text{ ways to partition } n \text{ labeled objects into } k \text{ non-empty unlabeled sets.}$$

Stirling numbers are well studied. Here are some facts for you to verify ($n\geq 1$, $k\geq 1$):

$$\left\{ {0 \atop 0} \right\} = 1 \qquad \left\{ {n \atop 0} \right\} = 0 \qquad \left\{ {0 \atop k} \right\} = 0 \qquad \left\{ {n \atop n-1} \right\} = \tfrac{1}{2}n(n-1) \qquad \left\{ {n \atop 2} \right\} = 2^{n-1}-1.$$

The Stirling numbers $\left\{ {n \atop k} \right\}$ satisfy a recurrence. To partition n objects into k sets: the first object can be in its own set and the other $n-1$ objects are partitioned into $k-1$ non-empty sets in $\left\{ {n-1 \atop k-1} \right\}$ ways; or, the first object

is in a set with some other objects, in which case the other $n-1$ objects are partitioned into k non-empty subsets in $\left\{ {n-1 \atop k} \right\}$ ways which we multiply by the k to account for the k possible sets for the first object. Therefore,

$$\left\{ {n \atop k} \right\} = k\left\{ {n-1 \atop k} \right\} + \left\{ {n-1 \atop k-1} \right\}.$$

The reader may use this recurrence and prove by induction that $\left\{ {n \atop k} \right\} = \sum_{i=0}^{k} (-1)^{k-i} \frac{i^n}{i!(k-i)!}$. To conclude,

$$\text{non-empty "named" } k\text{-committees from } n \text{ senators (one committee per senator)} = \sum_{i=0}^{k} (-1)^{k-i} \frac{k!}{i!(k-i)!} i^n.$$

At most 1 committee per senator; no empty committee. We consider the problem by "brute-force", first deciding the number of senators in no committees. There are 6 cases:

# senators not on a committee	0	1	2	3	4	5
# ways to pick the excluded senators	1	5	10	10	5	1

Verify the number of ways to exclude k senators in forming the committees: there is 1 way to exclude 0 senators (all senators are in committees) and 1 way to exclude 5 senators (no senators are in committees); there are 5 ways to exclude 1 senator (5 possible senators to exclude) and similarly 5 ways to exclude 4 senators (5 possible senators to include). There are 10 pairs of senators. So there are 10 ways to exclude 2 senators and 10 ways to exclude 3 senators (select a pair to include). If you exclude 4 or 5 senators, both committees cannot be nonempty.

Conclusion: there are 4 types of committees: those that exclude 0,1,2 or 3 senators.

Let's count the number of ways to form 2 non-empty committees if you exclude 2 senators. So you use 3 senators. There are 10 ways to pick which 2 senators to exclude, and then there are $2^3 - 2$ ways to form 2 non-empty committees using the remaining 3 senators. By the product rule, there are $10 \times (2^3 - 2)$ ways to form the two non-empty committees. Using this logic, we compute the entries in the following table for the number of committees that can be formed by excluding k senators, $k = 0, 1, 2, 3$.

# senators not on a committee	0	1	2	3
# committees	$1 \times (2^5 - 2)$	$5 \times (2^4 - 2)$	$10 \times (2^3 - 2)$	$10 \times (2^2 - 2)$

By the sum rule, the number of committees with at most 1 committee per senator and no empty committees is

$$1 \times (2^5 - 2) + 5 \times (2^4 - 2) + 10 \times (2^3 - 2) + 10 \times (2^2 - 2) = 170.$$

For n senators and k committees, we can leave out i senators and assign $n-i$ of them to k non-empty committees in $k!\left\{ {n-i \atop k} \right\}$, providing $n - i \geq k$. You will see later that there are $n!/i!(n-i)!$ ways in which to exclude i senators, so using the sum rule,

$$\begin{matrix}\#\text{ ways to create } k \text{ non-empty "named" committees} \\ \text{from } n \text{ senators (at most one committee per senator)}\end{matrix} = \sum_{i=0}^{n-k} \frac{n!k!}{i!(n-i)!} \left\{ {n-i \atop k} \right\}.$$

Pop Quiz 13.5.

(a) To list all the sequences of length 6, prepend 0 and 1 to the length-5 sequences:

000000	000001	000010	000011	000100	000101	000110	000111	100000	100001	100010	100011	100100	100101	100110	100111
001000	001001	001010	001011	001100	001101	001110	001111	101000	101001	101010	101011	101100	101101	101110	101111
010000	010001	010010	010011	010100	010101	010110	010111	110000	110001	110010	110011	110100	110101	110110	110111
011000	011001	011010	011011	011100	011101	011110	011111	111000	111001	111010	111011	111100	111101	111110	111111

Purple is 0 ones; green is 1 one; red is 2 ones; blue is 3 ones. Count the sequences of each color to verify the first 6 entries in the row for $n = 6$. The other entries follow by symmetry, e.g. flipping a sequence with 2 ones gives a sequence with 4 ones. Thus, the number of sequences with 4 ones equals the number of sequences with 2 ones.

(b) We want $\binom{10}{3}$, so we fill out our Pascal's-triangle table up to row $n = 10$.

We highlighted the number we seek: $\binom{10}{3} = 120$.

$\binom{n}{k}$	k = 0	1	2	3	4	5	6	7	8	9	10
0	1										
1	1	1									
2	1	2	1								
3	1	3	3	1							
4	1	4	6	4	1						
n 5	1	5	10	10	5	1					
6	1	6	15	20	15	6	1				
7	1	7	21	35	35	21	7	1			
8	1	8	28	56	70	56	28	8	1		
9	1	9	36	84	126	126	84	36	9	1	
10	1	10	45	120	210	252	210	120	45	10	1

Exercise 13.6.

(a) (i) Using (13.2) on page 13.2, $Q(n,k) = \sum_{j=0}^{n} Q(j, k-1) = Q(n, k-1) + \sum_{j=0}^{n-1} Q(j, k-1)$.
The sum on the RHS is $Q(n-1, k)$ by (13.2), so $Q(n,k) = Q(n,k-1) + Q(n-1,k)$.

(ii) If there are no candies of color-1 in the goody bag, the goody bag is made up of n candies using $k-1$ colors: there are $Q(n,k-1)$ such goody bags. Or, there is at least 1 candy of color-1. Place one candy of color-1 in the bag. The remaining $n-1$ candies make up a "goody bag" using k colors, so there are $Q(n-1,k)$ such goody bags. By the sum rule, the total number of goody bags is $Q(n,k-1)+Q(n-1,k)$.

(b) The dashed diagonal produces the same numbers as row 5 in Pascal's triangle. The next diagonal produces the numbers in Pascal's triangle for row 6. Along the diagonal, $n+k$ is constant. For the dashed diagonal, $n+k=6$.

dashed diagonal	$n+k=6 \leftrightarrow$ row 5 in Pascal's triangle;
next diagonal	$n+k=7 \leftrightarrow$ row 6 in Pascal's triangle.

A diagonal gives row $n+k-1$ in Pascal's triangle, so $Q(n,k)=\binom{n+k-1}{\ell}$, that is $m=n+k-1$. We can read off ℓ from the column k. Since $k=1$ gives $m=0$, $m=k-1$ and our guess is $Q(n,k)=\binom{n+k-1}{k-1}$.

Exercise 13.7. The sequences end in 0 with a prefix having $\le k$ 1s or end in 1 with a prefix having $\le k-1$ 1s. Thus, $\left|\begin{smallmatrix} n \\ k \end{smallmatrix}\right| = \left|\begin{smallmatrix} n-1 \\ k \end{smallmatrix}\right| + \left|\begin{smallmatrix} n-1 \\ k-1 \end{smallmatrix}\right|$. That is, $\left|\begin{smallmatrix} n \\ k \end{smallmatrix}\right|$ (Pascal's identity). The boundary conditions are $\left|\begin{smallmatrix} n \\ 0 \end{smallmatrix}\right| = 1$ and $\left|\begin{smallmatrix} n \\ k \end{smallmatrix}\right| = 2^n$ for $k \ge n$. The reader may build Pascal's triangle and get $\left|\begin{smallmatrix} 6 \\ 3 \end{smallmatrix}\right| = 42$. Note, $\left|\begin{smallmatrix} 6 \\ 3 \end{smallmatrix}\right| = \binom{6}{0}+\binom{6}{1}+\binom{6}{2}+\binom{6}{3}$.

Exercise 13.8.

(a) The first thing to do with build-up is identify the object you are counting with a name and tinker. Let $F(n)$ be the number of subsets of $[n]=\{1,2,\ldots,n\}$ that do not contain consecutive numbers. Now tinker with small n.

n	subsets	$F(n)$
1	$\varnothing, \{1\}$	$F(1)=2$
2	$\varnothing, \{1\}, \{2\}$	$F(2)=3$
3	$\varnothing, \{1\}, \{2\}, \{3\}, \{1,3\}$	$F(3)=5$

If S contains n, it can't contain $n-1$. The remaining elements in S are a subset of $1,\ldots,n-2$ not containing two consecutive numbers, and there are $F(n-2)$ such subsets. If S doesn't contain n, then S is a subset of $1,\ldots,n-1$ and there are $F(n-1)$ such subsets. Those are the only options. By the sum rule,

$$F(n)=F(n-1)+F(n-2).$$

We can now compute $F(20)$,

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$F(n)$	2	3	5	8	13	21	34	55	89	144	233	377	610	987	1597	2584	4181	6765	10946	17711

There are 17,711 subsets of {1,2,...,20} that do not contain consecutive numbers.

(b) Let $G(n)$ be the number of subsets of $[n]$ with at most 1 of any 3 consecutive numbers. Tinker with small n.

n	subsets	$G(n)$
1	$\varnothing, \{1\}$	$G(1)=2$
2	$\varnothing, \{1\}, \{2\}$	$G(2)=3$
3	$\varnothing, \{1\}, \{2\}, \{3\}$	$G(3)=4$
4	$\varnothing, \{1\}, \{2\}, \{3\}, \{4\}, \{1,4\}$	$G(4)=6$

Now, let us build such a subset S. If S contains n, it cannot contain $n-1$ or $n-2$. So the remaining elements in S are a subset of $1,2,\ldots,n-3$ containing at most one of any three consecutive numbers, and there are $G(n-3)$ different such subsets (by definition of $G(n)$). If S does not contain n, then the elements in S are a subset of $1,2,\ldots,n-1$ and there are $G(n-1)$ different such subsets. Those are the only options for S. By the sum rule,

$$G(n)=G(n-1)+G(n-3).$$

We can now compute $G(20)$,

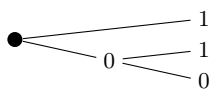
n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$G(n)$	2	3	4	6	9	13	19	28	41	60	88	129	189	277	406	595	872	1278	1873	2745

There are 2,745 subsets of {1,...,20} containing at most one of any three consecutive numbers.

(c) Same method, different problem. Let $B(n)$ be the number of length-n sequences not containing 001. Tinker.

n	length n sequences	$B(n)$
1	$0, 1$	$B(1)=2$
2	$00, 01, 10, 11$	$B(2)=4$
3	$000, 010, 011, 100, 101, 110, 111$	$B(3)=7$

Let us now try to build a sequence s of length n. It either starts with 1 or 0.



$B(n-1)$ sequences
$B(n-2)$ sequences
1 sequence

If s starts with 1, what follows is any sequence of length $n-1$ that does not conatin 001, and there are $B(n-1)$ of these. If s starts with 0, there are two cases: the second bit is 1 in which case what follows is any sequence of length $n-2$ that does not conatin 001, and there are $B(n-2)$ of these; the second bit is 0 in which case all remaining bits are 0, because otherwise the sequence contains 001. Therefore,

$$B(n) = B(n-1) + B(n-2) + 1;$$

We can now compute $B(20)$,

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$B(n)$	2	4	7	12	20	33	54	88	143	232	376	609	986	1596	2853	4180	6764	10945	17710	28656

Do you see a similarity between $B(n)$ and $F(n)$ above. There are 28,656 sequences of length 20 not containing 001.

(d) Start small. For 2 players, there is one way to configure the first round. Let $P(n)$ be the number of ways to configure the first round with $2n$ players. $P(1) = 1$. With $2n$ players, the first player can pair with any of $2n-1$ players leaving $2(n-1)$ players to be paired in $P(n-1)$ ways. Therefore, $P(n) = (2n-1)P(n-1)$, and we have

n	1	2	3	4	5	6	7	8
$P(n)$	1	3	15	105	945	10395	135135	2027025

There are 2,027,025 different configurations for the first round matches.

Exercise 13.9.

(a) The claim is that $Q(n,k) = \binom{n+k-1}{k-1}$. We prove this by a "double induction". We prove by induction on k, and within the induction on k, we use induction on n. We prove, by induction, $P(k)$ for $k \geq 1$, for the claim:

$$P(k) : Q(n,k) = \tbinom{n+k-1}{k-1} \text{ for all } n \geq 0.$$

The base case is $k = 1$ which claims $Q(n,1) = \binom{n}{n} = 1$, T. For the induction, assume $P(k)$. We show

$$P(k+1) : Q(n,k+1) = \tbinom{n+k}{k} \text{ for all } n \geq 0.$$

When $n = 0$, $Q(0,k+1) = 1\binom{k}{k}$. Let n_* be the smallest n for which $Q(n,k+1) \neq \binom{n+k}{k}$ (well-ordering principle). Thus, $n_* > 0$. By the innduction hypothesis, $Q(n_*,k) = \binom{n_*+k-1}{k-1}$. Since n_* is the smallest n which fails, $Q(n_*-1,k+1) = \binom{n_*+k-1}{k}$. By Exercise 13.6, $Q(n,k) = Q(n,k-1) + Q(n-1,k)$, therefore

$$Q(n_*,k+1) = Q(n_*,k) + Q(n_*-1,k+1) = \tbinom{n_*+k-1}{k-1} + \tbinom{n_*+k-1}{k} = \tbinom{n_*+k}{k}.$$

In the last step we used the recursion $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$. The last expression shows that n_* is not a counterexample, a contradiction. So, there is no smallest counterexample, and $P(k+1)$ is true. ∎

(b) The expression for $Q(n,k)$ follows by using (a) with $n+k-1$ instead of n, and $k-1$ instead of k. We prove that $\binom{n}{k} = n!/k!(n-k)!$. Define our claim,

$$P(n) : \tbinom{n}{k} = \tfrac{n!}{k!(n-k)!} \text{ for } 0 \leq k \leq n.$$

We prove by induction that $P(n)$ is true for all $n \geq 1$. First, we verify the base case $n = 1$, $\binom{1}{0} = 1 = 1!/0!1!$ and similarly $\binom{1}{1} = 1 = 1!/1!0!$. For the induction, assume $P(n)$ is true.

$$\begin{aligned}
\tbinom{n+1}{k} &= \tbinom{n}{k} + \tbinom{n}{k-1} && \text{(recursion in (13.1))} \\
&= \tfrac{n!}{k!(n-k)!} + \tfrac{n!}{(k-1)!(n-k+1)!} && \text{(induction hypothesis)} \\
&= \tfrac{n!}{(k-1)!(n-k)!}\left(\tfrac{1}{k} + \tfrac{1}{n-k+1}\right) && \text{(algebra)} \\
&= \tfrac{n!}{(k-1)!(n-k)!} \cdot \tfrac{n+1}{k(n-k+1)} && \text{(algebra)} \\
&= \tfrac{(n+1)!}{k!(n+1-k)!} && \text{(algebra)}
\end{aligned}$$

Therefore $P(n+1)$ is true, and, by induction, $P(n)$ is true for all $n \geq 1$.

(c) We denoted these numbers by $F(n)$ in the solution to Exercise 13.9(a), where we showed that $F(1) = 2, F(2) = 3$ and $F(n) = F(n-1) + F(n-2)$ (the Fibonacci recursion). We prove that $F(n) = F_{n+2}$ by strong induction. The base cases $n = 1, 2$ are true because $F_3 = 2$ and $F_4 = 3$. For the induction step, we have that

$$F(n+1) = F(n) + F(n-1) = F_{n+2} + F_{n+1} = F_{n+3}.$$

(The first step is the recursion for $F(n)$; the second is by the strong induction hypothesis; and, the third uses the Fibonacci recursion.) By induction, $F(n) = F_{n+2}$ for $n \geq 1$.

(d) We denoted these numbers by $B(n)$ in the solution to Exercise 13.9(c) (we showed that $B(1) = 2, B(2) = 4$). For these two base cases, $B(n) = F_{n+3} - 1$. For the strong induction step,

$$B(n+1) = B(n) + B(n-1) + 1 = F_{n+3} - 1 + F_{n+2} - 1 + 1 = F_{n+3} + F_{n+2} - 1 = F_{n+4} - 1.$$

(The first step is the recursion for $B(n)$; the second is by the strong induction hypothesis; and, the last step uses the Fibonacci recursion.) By induction, $B(n) = F_{n+3} - 1$ for $n \geq 1$.

Pop Quiz 13.10.
(a) Everything in A maps to one element of B, $f(1) = f(2) = f(3) = f(4) = 2$.
(b) Trick question. 1-to-1 but not onto can only be done if $|A| < |B|$.
(c) Trick question. Not 1-to-1 but onto can only be done if $|A| > |B|$.
(d) $F(1) = 2$; $F(2) = 3$; $F(3) = 4$; $F(4) = 5$;

Pop Quiz 13.11.
(a) $\{3\text{●}, 4\text{●}, 2\text{●}\}$
(b) 000101000000
(c) Let $0^{\bullet i}\bullet 1\bullet 0^{\bullet j}\bullet 1\bullet 0^{\bullet k}$ be a binary sequence of length $n+2$ with 2 ones. So, $i, j, k \geq 0$ and $i + j + k = n$. The sequence corresponds to the bag $\{i\text{●}, j\text{●}, k\text{●}\}$ containing i red candies, j blue candies and k green candies.

Clearly the correspondence is 1-to-1, different sequences will have different triples (i, j, k) which map to different candy bags. For any candy bag, we can construct the sequence, so the mapping is onto, hence a bijection.

Exercise 13.12.
(a) x_i is the number of candies of color i and since there are 10 candies, $\sum_i x_i = 10$. Any goody bag with the 10 candies gives non-negative x_i's which sum to 10. Any non-negative integer solution to $x_1 + \cdots + x_4 = 10$ gives a candy bag with x_i of candy i. We have a bijection between the candy bags and the non-negative solutions, that is

$$Q(10, 4) = \binom{10+4-1}{4-1} = \binom{10}{3} = \text{number of non-negative solutions to } x_1 + \cdots + x_4 = 10.$$

(b) Let $y_i = x_i - 1$. Then y_i are non-negative and $y_1 + \cdots + y_4 = x_1 + \cdots + x_4 - 4 = 6$. A non-negative solution to $y_1 + \cdots + y_4 = 6$ gives a positive solution to $x_1 + \cdots + x_4 = 10$ and *vice versa*. So, we want $Q(6, 4) = \binom{6+4-1}{4-1} = \binom{9}{3}$.
(c) Introduce a dummy variable $x_5 = 10 - (x_1 + \cdots + x_4)$, $x_5 \geq 0$ and $x_1 + \cdots + x_5 = 10$. Every non-negative solution to $x_1 + \cdots + x_5 = 10$ gives a non-negative solution to $x_1 + \cdots + x_4 \leq 10$, so the answer is $Q(10, 5) = \binom{10+5-1}{5-1} = \binom{14}{4}$.
(d) A roll is one of 6 "colors": $1, \ldots, 6$. For identical dice, we care only about the number of rolls of each color. With 4 rolls, we have $\binom{4+6-1}{6-1} = \binom{9}{5}$.
(e) For the binary sequence $b_1 \cdots b_{10}$ let the subset A contain all elements where $b_i = 1$, $A = \{x_i \mid b_i = 1\}$. Every binary sequence with three 1s gives a unique subset of A with 3 elements and every 3-subset identifies a binary sequence with three 1s, so we have a bijection. Thus, the number of such subsets equals the number of binary sequences with 3 ones, which is $\binom{10}{3}$. In general, the number of k-subsets of an n-element set is $\binom{n}{k}$.
(f) A 3-subset corresponds uniquely to its complement (a 7-subset) and *vice versa*. Since we have a bijection from 3-subsets to 7-subsets, $\binom{10}{3} = \binom{10}{7}$. In general $\binom{n}{k} = \binom{n}{n-k}$.
(g) Same bijection in (d), but to n-bit binary sequences with k ones. The ones identify the elements in the subset.
(h) Use the bijection in (e) from a k-subset to its complement, an $(n-k)$-subset.
(i) On page 180, we used the product rule to show that there are 2^n binary sequences of length n. The 1s in a sequence identify the elements in the subset, so there are 2^n subsets of a set (see also Example 13.1 about Senate committees on page 181). We can also count the subsets using the sum rule:

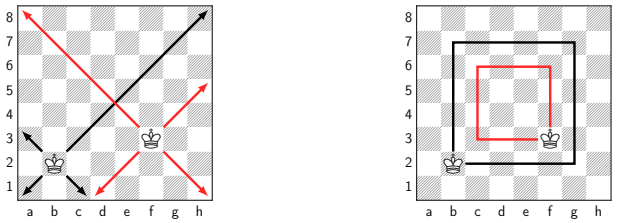
$$|\{\text{subsets}\}| = |\{\text{subsets of size 0}\}| + |\{\text{subsets of size 1}\}| + \cdots + |\{\text{subsets of size n}\}|.$$

From parts (d) and (f), the number of subsets of size k is $\binom{n}{k}$, therefore

$$2^n = |\{\text{subsets}\}| = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n}.$$

(A fundamental technique for establishing that two combinatorial expressions are equal: count a set in two different ways. The answers must be equal. Here, one way of counting gave 2^n, and the other gave $\sum_{k=0}^{n} \binom{n}{k}$.)

Pop Quiz 13.13. This problem is deceptively complicated. The king has 64 positions. Each removes 15 possible row-column squares for the queen. How many diagonal squares are removed? *It depends on where the king is.*



On the left we show two king positions. The king on $b2$ covers 9 squares (excluding its own square), but the king on $f3$ covers 11 squares. Verify using the figure on the right that positions on the black box all cover 9 squares and those on the red box all cover 11 squares. We can use the sum rule with four types of positions for the king: the outer-most ring of size 28 (covering 7 squares) to inner-most ring of size 4 (covering 13 squares)

ring size	28	20	12	4
diagonal squares covered	7	9	11	13

The number of positions available to the queen, given the position of the king is

$$64 - 15 \text{ row-column squares} - \text{number of diagonal squares covered.}$$

Denoting the rings by 0,1,2,3 (ring-0 is outermost). Here are our observations:

type of king position	ring-0	ring-1	ring-2	ring-3
number of possible king positions	28	20	12	4
diagonal squares covered	8	10	12	14
number of possible queen positions	42	40	38	36

Using the product rule within the types of king positions and the sum rule to add up the positions of each type to get the total number of possible positioins,

$$\text{number of possible positions } = 28 \times 42 + 20 \times 40 + 12 \times 38 + 4 \times 36 = 2576$$

For practice, consider a general $n \times n$ board. First, if the queen cannot be on the same row and column as the king, the number of ways to specify the sequence $c_K r_K c_Q r_Q$ is

$$n \times n \times (n-1) \times (n-1) = n^2(n-1)^2.$$

If the queen cannot be on the same diagonal, the number of row-columns squares covered by the king is $2n-1$. In the outermost ring with $4n-4$ squares, the number of diagonals covered is $n-1$, so the number of possible queen positions is $n^2 - (2n-1) - (n-1)$. Each time you move in by one ring, the number of possible king positions decreases by 8 and the number of diagonals covered increases by 2, so the number of possible queen positions decreases by 2. Thus, in ring-i, the number of possible king positions is $4n-4-8i$ and queen positions is $n^2-3n+2-2i = (n-1)(n-2)-2i$. The number of rings is $n/2$ when n is even. When n is odd, the number of rings is $(n-1)/2$ plus the single center square. Using the product and sum rule for the rings,

$$\text{number of possible positions} = \sum_{i=0}^{k} (4n-4-8i)((n-1)(n-2)-2i).$$

where $k = n/2-1$ if n is even and $k = (n-1)/2-1$ when n is odd (when n is odd, there is also the center square to consider). We use techniques from Chapter 9 to compute the sum.

$$\begin{aligned}
\text{number of possible positions } &= 4\sum_{i=0}^{k} (n-1-2i)((n-1)(n-2)-2i) \\
&= 4\left[\sum_{i=0}^{k}(n-1)^2(n-2) - 2\sum_{i=0}^{k}(n-1)^2 i + 4\sum_{i=0}^{k} i^2\right] \\
&= 4\left[(k+1)(n-1)^2(n-2) - k(k+1)(n-1)^2 + \tfrac{4}{6}k(k+1)(2k+1)\right]
\end{aligned}$$

When n is even, we plug in $k = n/2-1$ to get

$$\text{number of possible positions} = \tfrac{1}{3}n(n-1)(n-2)(3n-1).$$

When n is odd, we plug in $k = (n-1)/2-1$ and add the n^2-4n+3 positions with the king on the center square. The resulting formula is the same.

Pop Quiz 13.14. To specify the positions of the 8 castles, specify the column and row of each castle, the sequence

$$(c_1r_1)(c_2r_2)(c_3r_3)(c_4r_4)(c_5r_5)(c_6r_6)(c_7r_7)(c_8r_8)$$

For the columns, there are $8 \times 7 \times \cdots \times 1 = 8!$ ways. For the rows, there are $8 \times 7 \times \cdots \times 1 = 8!$ ways. For the rows and columns, by the product rule, there are $(8!)^2$ ways. Consider one such sequence, $(a1)(b2)(c3)(d4)(e5)(f6)(g7)(h8)$. If we reorder some positions, for example to $(b2)(a1)(c3)(d4)(e5)(f6)(g7)(h8)$, we get a *different* sequence but the *same* position. There are $8 \times 7 \times \cdots \times 1 = 8!$ possible reorderings of this position sequence, so this means that every position corresponds to 8! different sequences, a 1-to-8! mapping. By the multiplicity rule, there are 8! times as many sequences as there are positions. So the number of positions is $(8!)^2/8! = 8! = 40320$.

Alternatively, we may assume the rows increasing, so a position is a sequence $(c_1 1)(c_2 2)(c_3 3)(c_4 4)(c_5 5)(c_6 6)(c_7 7)(c_8 8)$ (we only get to choose the columns). There are 8! ways to choose the columns.

Exercise 13.15.

(a) The number of poker hands is the number of subsets of 5 cards from 52, or $\binom{52}{5} = 52!/(5! \times 47!) = 2598960$.

(b) The idea for such problems is to give a sequence of instructions to uniquely construct the object. The instructions must be unambiguous. Effectively, you construct a bijection between sequences of instructions and the objects. Now count the sequences. Here is a "recipe" to construct a 4-of-a-kind poker hand:

1: Choose a value v and pick all four cards of value v: ♠v ♥v ♢v ♣v.

2: Choose one of the other cards of a different value c.

The sequence vc completely specifies the 4-of-a-kind. Change any part of the sequence and you get a different 4-of-a-kind hand. We have a bijection between sequences vc and 4-of-a-kind hands. Counting the sequences is

"easy". There are 13 possible choices for v and for each choice of v there are 48 choices for c. By the product rule,

$$|\{\text{4-of-a-kind hands}\}| = |\{\text{sequences } vc\}| = 13 \times 48 = 624.$$

(c) To construct a flush, here is a recipe:
1: Pick the suit s, either ♠♥♢or ♣.
2: Choose a set of 5 values $\mathcal{V} = \{v_1, v_2, v_3, v_4, v_5\}$ from the 13 values in suit s.
The sequence $s\mathcal{V}$ completely specifies the flush. There are 4 choices for s. Given s, $\mathcal{V}$ is a 5-*subset* of the 13 values, so there are $\binom{13}{5}$ choices for this subset. By the product rule,

$$|\{\text{flushes}\}| = |\{\text{sequences } s\mathcal{V}\}| = 4 \times \binom{13}{5} = 5148.$$

(d) To construct a full-house, here is a recipe:
1: Choose a value v_1.
2: Choose $\mathcal{T}_1 = \{s_1, s_2, s_3\}$, a set of 3 suits having value v_1.
3: Choose a second value $v_2 \neq v_1$.
4: Choose $\mathcal{T}_2 = \{s_1, s_2\}$, a set of 2 suits having value v_2.
The sequence $v_1\mathcal{T}_1v_2\mathcal{T}_2$ completely specifies the full-house. There are 13 choices for v_1; given v_1, $\mathcal{T}_1$ is a 3-subset of the 4 suits, which can be picked in $\binom{4}{3}$ ways; given $v_1\mathcal{T}_1$, v_2 has 12 choices (since $v_2 \neq v_1$); given $v_1\mathcal{T}_1v_2$, $\mathcal{T}_2$ is a 2-subset of the 4 suits, which can be picked in $\binom{4}{2}$ ways. By the product rule,

$$|\{\text{full-houses}\}| = |\{\text{sequences } v_1\mathcal{T}_1v_2\mathcal{T}_2\}| = 13 \times \binom{4}{3} \times 12 \times \binom{4}{2} = 3744.$$

(e) To construct a 3-of-a-kind, here is a recipe:
1: Choose a value v
2: Choose $\mathcal{T} = \{s_1, s_2, s_3\}$, a set of 3 suits having value v.
3: Choose c_1, a card of value $v_1 \neq v$.
4: Choose c_2, a card of value $v_2 \neq v$ or v_1.
Let's count sequences $v\mathcal{T}c_1c_2$. There are 13 choices for v. Given v, pick $\mathcal{T}$, a 3-subset of the 4 suits, in $\binom{4}{3}$ ways. Then pick c_1 in 48 ways ($v_1 \neq v$), and c_2 in 44 ways ($v_2 \neq v$ or v_1). By the product rule,

$$|\{\text{3-of-a-kinds}\}| = |\{\text{sequences } v\mathcal{T}c_1c_2\}| = 13 \times \binom{4}{3} \times 48 \times 44 = 109842.$$

WRONG! The mistake is similar to the issue with counting positions of two indistinguishible castles versus a king and a queen (distinguishable pieces). These two 3-of-a-kind hands (♠A,♥A,♣A,♥7,♣2) and (♠A,♥A,♣A,♣2,♥7) are the same. However, the two sequences $v\mathcal{T}c_1c_2$ are different. So two different sequences map to the same hand: we do not have a 1-to-1 mapping. There are many ways to resolve this problem. Every hand maps to two sequences, so by the multiplicity rule, there are twice as many sequences as hands: the number of hands is $109842/2 = 54912$. Alternatively, we view the remaining 48 cards in some order and pick c_1c_2 with $c_1 < c_2$ (as with the castle positions). The number of ways to pick $c_1 < c_2$ is half the number of ways to pick c_1c_2 (the other half have $c_1 > c_2$). The systematic route is to give a recipe to uniquely construct a 3-of-a-kind hand:
1: Choose a value v
2: Choose $\mathcal{T} = \{s_1, s_2, s_3\}$, a set of 3 suits having value v.
3: Choose a pair of values $\mathcal{V} = \{v_1, v_2\}$ from the remaining 12 values.
4: Choose x_1, a suit from value v_1.
5: Choose x_2, a suit from value v_2.
Now, the sequence $v\mathcal{T}\mathcal{V}x_1x_2$ uniquely constructs a 3-of-a-kind hand and we can count the sequences. There are 13 choices for v; given v, $\mathcal{T}$ is a 3-subset of the 4 suits, which can be picked in $\binom{4}{3}$ ways; $\mathcal{V}$ is a 2-subset of the remaining 12 values, with $\binom{12}{2}$ choices; given $\mathcal{V}$, x_1 and x_2 each have 4 choices. By the product rule,

$$|\{\text{3-of-a-kinds}\}| = |\{\text{sequences } v\mathcal{T}\mathcal{V}x_1x_2\}| = 13 \times \binom{4}{3} \times \binom{12}{2} \times 4 \times 4 = 54912.$$

(f) To construct a two-pair, here is a recipe:
1: Choose $\mathcal{V} = \{v_1, v_2\}$ the values for each pair.
2: Choose $\mathcal{S}_1 = \{s_1, s_2\}$, a set of 2 suits having value v_1.
3: Choose $\mathcal{S}_2 = \{s_1, s_2\}$, a set of 2 suits having value v_2.
4: Choose a the 5th card c from the 44 not of value v_1, v_2.
Let's count sequences $\mathcal{V}\mathcal{S}_1\mathcal{S}_2c$: $\binom{13}{2}$ choices for the 2-subset of values from 13; $\mathcal{S}_1$ and $\mathcal{S}_2$ are 2-subsets of the 4 suits, which can be picked in $\binom{4}{2}$ ways each; lastly, there are 44 choices for c. By the product rule,

$$|\{\text{two-pairs}\}| = |\{\text{sequences } \mathcal{V}\mathcal{S}_1\mathcal{S}_2c\}| = \binom{13}{2} \times \binom{4}{2} \times \binom{4}{2} \times 44 = 123552.$$

Exercise 13.16. The top vertex must be used. The other two vertices must be on the same "level". Choose a level in 4 ways and then a pair of points within the level in $\binom{6}{2}$ ways, for a total of $4 \times \binom{6}{2} = 60$ triangles.

Exercise 13.17.
1. From the binomial expansion, the terms in $(2x^2+1/x^3)^{10}$ are $\binom{10}{i}(2x^2)^i(1/x^3)^{10-i} = \binom{10}{i}2^ix^{5i-30}$. The constant term has $5i - 30 = 0$, or $i = 6$ and the coefficient is $2^6\binom{10}{6} = 64 * \frac{10!}{6!\times 4!} = 13440$.

2. From the binomial expansion, the terms in $(1+3x)^{20}$ are $\binom{20}{i}(3x)^i = \binom{20}{i}3^i x^i$. So, the ith coefficient is $a_i = \binom{20}{i}3^i$. Let us consider a_{i+1}/a_i,
$$\frac{a_{i+1}}{a_i} = \frac{\binom{20}{i+1}3^{i+1}}{\binom{20}{i}3^i} = 3\cdot\frac{\frac{20!}{(i+1)!(19-i)!}}{\frac{20!}{i!(20-i)!}} = 3\cdot\frac{i!(20-i)!}{(i+1)!(19-i)!} = \frac{60-3i}{i+1}.$$
Observe that $\frac{60-3i}{i+1} \le 1 \leftrightarrow 59 \le 4i \leftrightarrow i \ge 14\frac{3}{4}$. Since i is an integer, this means that $a_{i+1} \le a_i \leftrightarrow i \ge 15$. Therefore, the maximum occurs at $i = 15$ and that coefficient is $a_{15} = \binom{20}{15}3^{15}$.

Chapter 14

Exercise 14.1.
(a) The number of length 8 sequences with 3 a, 2 r, 1 d, 1 k and 1 d is $\binom{8}{3,2,1,1,1} = \frac{8!}{3!\times2!\times1!\times1!\times1!} = 3360$.
(b) A bouquet (goody-bag) has 36 objects of 4 colors. The number of bouquets is $Q(36,4) = \binom{36+4-1}{4-1} = \binom{39}{3} = 9139$.
(c) Let the students be $s_1 s_2 \cdots s_{25}$ (think of them all standing in a line).
   (i) There are 5 types of students: those assigned to cook, clean, laundry, entertainment, groceries. There are 5 of each type, so we need a sequence of length 25 with 5 of each type. This can be done in $\binom{25}{5,5,5,5,5}$ ways.
$$\binom{25}{5,5,5,5,5} = \frac{25!}{(5!)^5} \approx \frac{25^{25}e^{-25}\sqrt{50\pi}}{5^{25}e^{-25}(10\pi)^{5/2}} = 5^{25}\cdot\frac{\sqrt{50\pi}}{(10\pi)^{5/2}} \approx 6.75\times10^{14}.$$
   (We used Stirling's formula, $n! \approx n^n e^{-n}\sqrt{2\pi n}$. The exact answer is about 6.234×10^{14}.)
   (ii) For each task we pick a subset of 5 students to perform the task, which can be done in $\binom{25}{5}$ ways. By the product rule, the number of ways to perform the tasks is $\binom{25}{5}^5$ and $\binom{25}{5}^5 = 53130^5 \approx 4.2\times10^{23}$.

Exercise 14.2.
(a) For this problem we use the binomial and multinomial theorem:
   (i) We want the coefficient of 1^4x^5 which is $\binom{9}{4} = 126$.
   (ii) The coefficient of $(2x)^4(3y)^3$ is $\binom{7}{4} = 35$ which gives $35(2x)^4(3y)^3 = 35\cdot2^4\cdot3^3x^4y^3$, so the coefficient of x^4y^3 is $35\times2^4\times3^3 = 15120$.
   (iii) x^4y^8 is the coefficient of $x^1(x^2)^2(y^2)^4$ which is $\binom{7}{1,2,5} = 105$.
(b) Monomials in $(x+y)^n$ are x^iy^j. There are $n+1$ possible i $(0,1,\ldots,n)$, and given i, $j = n-i$. So, the number of different monomials is $n+1$.
For $(x+y+z)^n$, the monomials are specified by (i,j,k), the powers of x, y and z respectively: i ranges from 0 to n; j ranges from 0 to $n-i$ which is $(n-i+1)$ choices for j; and k is $n-i-j$. So the number of monomials is
$$\sum_{i=0}^{n}(n-i+1) = (n+1)+n+\cdots+1 = \tfrac{1}{2}(n+1)(n+2).$$
(c) There are k^n terms (n-sequences of $a_1,\ldots,a_k$ with repetition), and $\binom{n}{i_1,i_2,\ldots,i_k}$ have i_1 a_1's, i_2 a_2's, …, i_k a_k's. Each such term is $a_1^{i_1}a_2^{i_2}\cdots a_k^{i_k}$. With $i_1 \ge 0,\ldots,i_k \ge 0$ and $i_1+\cdots+i_k = n$, we get the multinomial theorem:
$$(a_1+a_2+\cdots+a_k)^n = \sum_{\substack{i_1\ge0,\ i_2\ge0,\ldots i_k\ge0\\ i_1+i_2+\cdots+i_k=n}}\binom{n}{i_1,i_2,\ldots,i_k}a_1^{i_1}a_2^{i_2}\cdots a_k^{i_k}.$$
(d) The result is immediate from setting $a_1 = a_2 = \cdots = a_k = 1$ in part (c).
(e) Let's first tinker a little to make sure we understand. $(a_1+a_2)^n = \binom{n}{0}a_1^na_2^0+\binom{n}{1}a_1^{n-1}a_2^1+\binom{n}{2}a_1^{n-2}a_2^2+\cdots+\binom{n}{n}a_1^0a_2^n$, which is $(n+1)$ different monomials. From part (b) we see that $(a_1+a_2+a_3)^n$ has $\frac{1}{2}(n+1)(n+2)$ different monomials. For the general case, $(a_1+a_2+\cdots+a_k)^n$, we want the number of different terms in the sum of part (c). That is, we need the number of different non-negative solutions to $i_1+i_2+\cdots+i_k = n$. Think of a_1 to a_k as k colors. We want a goody bag of size n with these k colors, where $i_1,i_2,\ldots,i_k$ represent the number of color-1, color-2, …, color-k in the goody bag. So the number of non-negative solutions to $i_1+i_2+\cdots+i_k = n$ is exactly the number of goody bags you can make, which is $Q(n,k) = \binom{n+k-1}{k-1}$. Let us check with $k = 2,3$.
$$(a_1+a_2)^n \text{ has } Q(n,2) = \tbinom{n+1}{1} = n+1 \text{ different monomials;}\checkmark$$
$$(a_1+a_2+a_3)^n \text{ has } Q(n,3) = \tbinom{n+2}{2} = \tfrac{1}{2}(n+1)(n+2) \text{ different monomials.}\checkmark$$

Pop Quiz 14.3. For convenience we repeat the derivation here.
$$\begin{aligned}
|A_1\cup A_2\cup A_3| &\overset{(a)}{=} |A_1\cup A_2| + |A_3| - |(A_1\cup A_2)\cap A_3|\\
&\overset{(b)}{=} |A_1|+|A_2|+|A_3| - |A_1\cap A_2| - |(A_1\cap A_3)\cup(A_2\cap A_3)|\\
&\overset{(c)}{=} |A_1|+|A_2|+|A_3| - |A_1\cap A_2| - (|A_1\cap A_3|+|A_2\cap A_3| - |A_1\cap A_3\cap A_2\cap A_3|)\\
&\overset{(d)}{=} |A_1|+|A_2|+|A_3| - |A_1\cap A_2| - |A_1\cap A_3| - |A_2\cap A_3| + |A_1\cap A_2\cap A_3|.
\end{aligned}$$

(a) Let $B = A_1 \cup A_2$. Using inclusion-exclusion for two sets, $|B \cup A_3| = |B| + |A_3| - |B \cap A_3|$.
(b) Apply two set inclusion-exclusion to $|A_1 \cup A_2|$ and use the distributive property of intersection, $(A_1 \cup A_2) \cap A_3 = (A_1 \cap A_3) \cup (A_2 \cap A_3)$ (see Figure 2.1 on page 17).
(c) Let $A = A_1 \cap A_3$ and $B = A_2 \cap A_3$ and apply two set inclusion-exclusion to $|A \cup B|$.
(d) $|A_1 \cap A_3 \cap A_2 \cap A_3| = |A_1 \cap A_2 \cap A_3|$.

Exercise 14.4.

(a) $$\begin{aligned}|A_1 \cup A_2 \cup A_3 \cup A_4| = &+(|A_1| + |A_2| + |A_3| + |A_4|)\\ &-(|A_1 \cap A_2| + |A_1 \cap A_3| + |A_1 \cap A_4| + |A_2 \cap A_3| + |A_2 \cap A_4| + |A_3 \cap A_4|)\\ &+(|A_1 \cap A_2 \cap A_3| + |A_1 \cap A_2 \cap A_4| + |A_1 \cap A_3 \cap A_4| + |A_2 \cap A_3 \cap A_4|)\\ &-(|A_1 \cap A_2 \cap A_3 \cap A_4|)\end{aligned}$$

We give a proof that will generalize to the induction step for the general case.

$$\begin{aligned}|A_1 \cup A_2 \cup A_3 \cup A_4| &= |A_1 \cup A_2 \cup A_3| + |A_4| - |(A_1 \cup A_2 \cup A_3) \cap A_3|\\ &= |A_1 \cup A_2 \cup A_3| + |A_4| - |(A_1 \cap A_4) \cup (A_2 \cap A_4) \cup (A_3 \cap A_4)|\end{aligned}$$

We can apply 3-set inclusion-exclusion to the first and third terms:

$$|A_1 \cup A_2 \cup A_3| = \sum_{k=1}^{3} (-1)^{k+1} \cdot \sum |\{k\text{-intersection of } A_1, A_2, A_3\}|$$

$$|(A_1 \cap A_4) \cup (A_2 \cap A_4) \cup (A_3 \cap A_4)| = \sum_{k=1}^{3} (-1)^{k+1} \cdot \sum |\{k\text{-intersection of } A_1 \cap A_4, A_2 \cap A_4, A_3 \cap A_4\}|$$

A k-way intersection of $A_1 \cap A_4, A_2 \cap A_4, A_3 \cap A_4$ is the intersection of A_4 with that k-way intersection of A_1, A_2, A_3. For example $(A_1 \cap A_4) \cap (A_2 \cap A_4) = A_1 \cap A_2 \cap A_4$. Hence, $|A_1 \cup A_2 \cup A_3 \cup A_4|$ equals

$$\sum_{k=1}^{3} (-1)^{k+1} \cdot \sum |\{k\text{-intersection of } A_1, A_2, A_3\}| + |A_4| + \sum_{k=1}^{3} (-1)^{k+2} \cdot \sum |\{A_4 \cap k\text{-intersection of } A_1, A_2, A_3\}|$$

The summands in the last term are the $k+1$-way intersections involving A_4. The summands in the first term are the k-way intersections that *do not include* A_4. So, $|A_1 \cup A_2 \cup A_3 \cup A_4|$ equals

$$\sum_{k=1}^{3} (-1)^{k+1} \cdot \sum |\{k\text{-intersection without } A_4\}| + |A_4| + \sum_{k=1}^{3} (-1)^{k+2} \cdot \sum |\{(k+1)\text{-intersection with } A_4\}|$$

The last two terms are all k-way intersections involving A_4 with $k = 1, \ldots, 4$. So, $|A_1 \cup A_2 \cup A_3 \cup A_4|$ is

$$\sum_{k=1}^{3} (-1)^{k+1} \cdot \sum |\{k\text{-intersection without } A_4\}| + |A_4| + \sum_{k=1}^{4} (-1)^{k+2} \cdot \sum |\{k\text{-intersection with } A_4\}|$$

Summing over k-way intersections with and without A_4 amounts to summing over all k-way intersections,

$$|A_1 \cup A_2 \cup A_3 \cup A_4| = \sum_{k=1}^{4} (-1)^{k+1} \cdot \sum |\{k\text{-intersection}\}|$$

(b) Let A_2, A_3, A_5, A_7 be the sets of numbers from 1 to 2015 that *are divisible* by 2,3,5,7 respectively. We want $2015 - |A_2 \cup A_3 \cup A_5 \cup A_7|$. Here are two facts:

Lemma 30.5. There are $\lfloor n/k \rfloor$ numbers from 1 to n that are divisible by k.

Lemma 30.6. x is divisible by $d_1, d_2, \ldots, d_k$ if and only if x is divisible by least common multiple$(d_1, d_2, \ldots, d_k)$.

To get $|A_2 \cup A_3 \cup A_5 \cup A_7|$, we need all k-way intersections. For example, $|A_2| = \lfloor 2015/2 \rfloor$ and $|A_2 \cap A_3| = \lfloor 2015/6 \rfloor$ because numbers in $A_2 \cap A_3$ are divisible by 2 and 3, and $\operatorname{lcm}(2,3) = 6$. Define $A_{ij} = A_i \cap A_j$ and similarly A_{ijk} and A_{ijkl}. We have:

$$\begin{aligned}&|A_2| = 1007;\ |A_3| = 671;\ |A_5| = 403;\ |A_7| = 287.\\ &|A_{23}| = 335;\ |A_{25}| = 201;\ |A_{27}| = 143;\ |A_{35}| = 134;\ |A_{37}| = 95;\ |A_{57}| = 57.\\ &|A_{235}| = 67;\ |A_{237}| = 49;\ |A_{257}| = 28;\ |A_{357}| = 19.\\ &|A_{2357}| = 9.\end{aligned}$$

Therefore, for $|A_2 \cup A_3 \cup A_5 \cup A_7|$ we get:

$$1007 + 671 + 403 + 287 - 335 - 201 - 143 - 134 - 95 - 57 + 67 + 49 + 28 + 19 - 9 = 1557.$$

We conclude that $2015 - 1557 = 458$ numbers are not divisible by any of $\{2, 3, 5, 7\}$.

(c) We count the ways to distribute the hats so that some girl gets the right hat and subtract from 4!, the number of ways to distribute the hats. Let A_1 be the orderings in which girl 1 gets her correct hat; similarly define A_2, A_3, A_4. The number of ways in which some girl gets the right hat is $|A_1 \cup A_2 \cup A_3 \cup A_4|$. For inclusion-exclusion, we need the intersections. Let $A_{12} = A_1 \cap A_2$ be the number of ways girls 1 and 2 get the correct hats; similarly define

$A_{13}, A_{14}, A_{23}, A_{24}, A_{34}$ and so on. Now, $|A_i| = 3!$ (3! ways to distribute the other 3 hats after giving girl i his hat). Similarly, $|A_{ij} = 2!$ because there are 2! ways to distribute the other 2 hats after giving girls i and j their hats; $|A_{ijk}| = 1!$; and, $A_{ijkl}| = 0!$. We have

$$|A_1| = |A_2| = |A_3| = |A_4| = 6.$$
$$|A_{12}| = |A_{13}| = |A_{14}| = |A_{23}| = |A_{24}| = |A_{34}| = 2.$$
$$|A_{123}| = |A_{124}| = |A_{134}| = |A_{234}| = 1.$$
$$|A_{1234}| = 1.$$

Applying the inclusion-exclusion formula, $|A_1 \cup A_2 \cup A_3 \cup A_4| = 4 \times 6 - 6 \times 2 + 4 \times 1 - 1 = 15$.
The answer is $4! - 15 = 9$. Distributing n objects so that no object goes into its correct spot is a derangement. Example 14.5 on page 201 discusses how to count derangements of n objects.

(d) The proof for general n by induction mimics the proof for $n = 4$. The base case is $n = 2$, which we have already established. For the induction step, consider any $n + 1$ sets.

$$\begin{aligned}|A_1 \cup A_2 \cup \cdots \cup A_n \cup A_{n+1}| &= |A_1 \cup A_2 \cup \cdots \cup A_n| + |A_{n+1}| - |(A_1 \cup A_2 \cup \cdots \cup A_n) \cap A_{n+1}| \\ &= |A_1 \cup A_2 \cup \cdots \cup A_n| + |A_{n+1}| - |(A_1 \cap A_{n+1}) \cup (A_2 \cap A_{n+1}) \cup \cdots \cup (A_n \cap A_{n+1})|\end{aligned}$$

The first term, by the induction hypothesis, sums over the k-way intersections not involving A_{n+1}. The last two terms sum over the k-way intersections involving A_{n+1}. So, $|A_1 \cup A_2 \cup A_3 \cup \cdots \cup A_n \cup A_{n+1}|$ equals

$$\begin{aligned}&\sum_{k=1}^{n} (-1)^{k+1} \cdot \sum |\{k\text{-intersection not involving } A_{n+1}\}| + \sum_{k=1}^{n+1} (-1)^{k+1} \cdot \sum |\{k\text{-intersection involving } A_{n+1}\}| \\ = &\sum_{k=1}^{n+1} (-1)^{k+1} \cdot \sum |\{(k\text{-intersection})\}|.\end{aligned}$$

That is, the formula holds for a union of $n + 1$ sets, and by induction for all $n \geq 2$.

Exercise 14.5.

(a) Let A be all the passwords, A_U be all passwords *not* containing an uppercase letter and A_S be all passwords *not* containing a special character. We want $|A| - |A_U \cup A_S|$. We have that $|A_U \cup A_S| = |A_U| + |A_S| - |A_U \cap A_S|$. Passwords in A_U have $72 - 26 = 46$ choices per character, so $|A_U| = 46^8$. Passwords in A_S have $72 - 10 = 62$ choices per character, so $|A_S| = 62^8$. Passwords in $A_U \cap A_S$ use $72 - 26 - 10 = 36$ choices per character, so $|A_U \cap A_S| = 36^8$. Since $|A| = 72^8$, our answer is $72^8 - 46^8 - 62^8 + 36^8 \approx 4.866 \times 10^{14}$.

(b) Let A_{12} be the permutations containing 12 and A_{24} the permutations containing 24. There are 10! pins. The invalid pins are in $A_{12} \cup A_{24}$, so the number of valid pins is $10! - |A_{12} \cup A_{24}|$. By inclusion-exclusion,

$$|A_{12} \cup A_{24}| = |A_{12}| + |A_{24}| - |A_{12} \cap A_{24}|.$$

To count pins containing 12, treat 12 as a single token. We want a permutation of $0\boxed{12}3456789$. There are 9! permutations, i.e. 9! such pins. Similarly, there are 9! pins contatining 24. Therefore $|A_{12}| = |A_{24}| = 9!$. The pins containing 12 and 24 must contain 124. Treating 124 as a single token, we need the permutations of $0\boxed{124}356789$, of which there are 8!. Thus, $|A_{12} \cap A_{24}| = 8!$. The number of valid pins is

$$10! - 2 \times 9! + 8! = 2943360.$$

(c) Each element in A can map to m elements in B, so the total number of functions is m^n. Let $B = \{b_1, b_2, \ldots, b_m\}$. Let F_1 be the functions which do not have b_1 in the range (so no element of A maps to b_1); similarly define $F_2, \ldots, F_m$. A function is *not onto* if one of the b_i's is not in the range. That is, the functions which are not onto are in $F_1 \cup F_2 \cup \cdots \cup F_m$. Let us compute the size of a k-way intersection $|F_{i_1} \cap F_{i_2} \cap \cdots \cap F_{i_k}|$ – the functions which do not use $b_{i_1}, b_{i_2}, \ldots, b_{i_k}$. The function can map each element of A to $m - k$ of the b_i's, so there are $(m - k)^n$ such functions. Since there are $\binom{n}{k}$ such k-way intersections, by inclusion-exclusion,

$$|F_1 \cup F_2 \cup \cdots \cup F_m| = \sum_{k=1}^{m} (-1)^{k+1} \tbinom{m}{k} (m - k)^n.$$

The number of onto functions is $m^n - |F_1 \cup F_2 \cup \cdots \cup F_m|$,

$$\text{number of onto functions from } [n] \text{ to } [m] = m^n - \sum_{k=1}^{m} (-1)^{k+1} \tbinom{m}{k} (m - k)^n = \sum_{k=0}^{m} (-1)^k \tbinom{m}{k} (m - k)^n.$$

Recall that in the solution to Exercise 13.4(c) we introduced $\left\{ {n \atop m} \right\}$ (Stiring numbers of the second kind): the number of ways to distribute n named objects (the elements of A) into m unnamed (indistinguishable) bins (the elements of B) so that no bin is empty. Here, the bins are distinguishable, so multiplying by $m!$, the number of ways to label the bins with the labels $b_1, \ldots, b_m$, we have that $m!\left\{ {n \atop m} \right\}$ is the number of ways to distribute the n objects (A) into m bins (B), each such way being an onto function from A to B, so

$$\text{number of onto functions from } [n] \text{ to } [m] \;=\; m!\left\{ {n \atop m} \right\} \;=\; \sum_{k=0}^{m} (-1)^k \tbinom{m}{k} (m - k)^n.$$

This gives us another formula for the Stirling number, $\left\{ {n \atop m} \right\} = \frac{1}{m!} \sum_{k=0}^{m} (-1)^k \binom{m}{k} (m - k)^n$.

(d) If there were no upper bound constraints, we know how to compute the number of solutions:

$$\text{number of solutions to } x_1+x_2+x_3=30 \text{ with } x_1,x_2,x_3\geq 0 \text{ is } Q(30,3)=\tbinom{32}{2}=496.$$

(We used $Q(n,k)=\binom{n+k-1}{k-1}$.) Let S_1 be the solutions which *violate* the upper bound on x_1. So S_1 contains solutions to $x_1+x_2+x_3=30$ with $x_1\geq 11$ and $x_2,x_3\geq 0$. Similarly, define S_2, the solutions to $x_1+x_2+x_3=30$ with $x_2\geq 16$ and $x_1,x_3\geq 0$ and S_3, the solutions to $x_1+x_2+x_3=30$ with $x_3\geq 21$ and $x_1,x_2\geq 0$. The number of solutions which *satisfy* the upper bounds is $Q(30,3)-|S_1\cup S_2\cup S_3|$. By inclusion-exclusion,

$$|S_1\cup S_2\cup S_3|=|S_1|+|S_2|+|S_3|-|S_1\cap S_2|-|S_1\cap S_3|-|S_2\cap S_3|+|S_1\cap S_2\cap S_3|.$$

To get $|S_1|$, observe that solutions to $x_1+x_2+x_3=30$ with $x_1\geq 11$ and $x_2,x_3\geq 0$ are solutions to $x_1+x_2+x_3=19$ with $x_1,x_2,x_3\geq 0$ after subtracting 11 from x_1 (and *vice versa*). So, $|S_1|=Q(19,3)$. Similarly, $|S_2|=Q(14,3)$ and $|S_3|=Q(9,3)$. $S_1\cap S_2$ contains solutions to $x_1+x_2+x_3=30$ with $x_1\geq 11, x_2\geq 16, x_3\geq 0$. These solutions give solutions to $x_1+x_2+x_3=3$ with $x_1,x_2,x_3\geq 0$ after subtracting 11 from x_1 and 16 from x_2, so $|S_1\cap S_2|=Q(3,3)$. Similarly, $|S_1\cap S_3|=Q(-2,3)=0$ and $|S_2\cap S_3|=Q(-7,3)=0$. Finally, $S_1\cap S_2\cap S_3$ contains solutions to $x_1+x_2+x_3=30$ with $x_1\geq 11, x_2\geq 16, x_3\geq 21$ which are solutions to $x_1+x_2+x_3=-18$ with $x_1,x_2,x_3\geq 0$ after subtracting 11 from x_1, 16 from x_2 and 21 from x_3. So, $|S_1\cap S_2\cap S_3|=Q(-18,3)=0$. Putting all this together,

$$|S_1\cup S_2\cup S_3| = Q(19,3)+Q(14,3)+Q(9,3)-Q(3,3)-0-0+0=\tbinom{21}{2}+\tbinom{16}{2}+\tbinom{11}{2}-\tbinom{5}{2}=375.$$

Our answer is $496-375=121$ solutions.

(e) The numbers in $[n]$ not relatively prime to n are divisible by p_1 or p_2 or $\ldots$ or p_m. Let A_i be the numbers in $[n]$ that are divisible by p_i. Then the numbers in $[n]$ which are not relatively prime to n are in $A_1\cup\cdots\cup A_m$, and so

$$\varphi(n)=n-|A_1\cup\cdots\cup A_m|.$$

The k-way intersection $A_{i_1}\cap\cdots\cap A_{i_k}$ has the numbers divisible by p_{i_1} and p_{i_2} and $\ldots$ and p_{i_k}, hence

$$|A_{i_1}\cap\cdots\cap A_{i_k}|=\left\lfloor \tfrac{n}{p_{i_1}p_{i_2}\cdots p_{i_k}}\right\rfloor=\tfrac{n}{p_{i_1}p_{i_2}\cdots p_{i_k}},$$

where the last equality follows because n is divisible by $p_{i_1}p_{i_2}\cdots p_{i_k}$. By inclusion-exclusion,

$$|A_1\cup\cdots\cup A_m|=\sum_{k=1}^{m}(-1)^{k+1}\cdot(\text{sum over all } k\text{-way products of } n/p_{i_1}p_{i_2}\cdots p_{i_k}).$$

Therefore, Euler's totient function is

$$\begin{aligned}\varphi(n) &= n-\sum_{k=1}^{m}(-1)^{k+1}\cdot(\text{sum over all } k\text{-way products of } n/p_{i_1}p_{i_2}\cdots p_{i_k})\\ &= n\sum_{k=0}^{m}(-1)^{k}\cdot(\text{sum over all } k\text{-way products of } 1/p_{i_1}p_{i_2}\cdots p_{i_k}).\end{aligned}$$

Let's compare with the formula $\varphi(n)=n\prod_{i=1}^{m}\left(1-\frac{1}{p_i}\right)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_m}\right)$.
Multiplying out the RHS gives 2^m terms. Each term is a product of k reciprocal primes, $1/p_{i_1}p_{i_2}\cdots p_{i_k}$ with sign $(-1)^k$. Each term matches one term in our inclusion-exclusion sum, and so the two expressions are equal.

Pop Quiz 14.6. There are 7 days of the week (pigeonholes). Place 8 friends (pigeons) in pigeonholes by the day of the week on which they were born, there will be at least two guests in the same pigeonhole.

Even with infinitely many friends, all could be born on Tuesday. This is important. Pigeonhole guarantees two are born on the *same* day with 8 friends, but you don't know *which* day (it could be any).

Exercise 14.7. The proof is similar to the example in the text with 10 numbers between 1 and 100. We have 100 numbers between 1 and 10^{28}. The maximum possible subset sum is $100\times 10^{28}=10^{30}$. So there are 10^{30} bins. The number of possible subsets is 2^{100}. Since $2^{100}\geq 1.26\times 10^{30}$, the number of subsets is larger than the number of bins. By pigeonhole principle, some bin has more than one subset. Those two subsets in the same bin have the same sum.

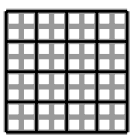
Exercise 14.8.

(a) This is the same result as social twins, except with social enemies.

(b) You need to research two facts to solve this problem:
Population of New York City: larger than 8 million people.
Human head-hairs: the estimate is at most 200,000. So lets be safe and say 1 million.

Number pigeonholes $0,1,\ldots,10^6$. Place a person (pigeon) into the pigeonhole labeled with their number of head-hairs. Two or more people are in the same pigeonhole and have the same number of head-hairs.

(c) We partitioned the 8×8 grid into 16 disjoint 2×2 buckets (right). 16 kings can be placed, one in the top-left of each bucket. The buckets are pigeonholes and the kings are pigeons. Each king is in one bucket. If there are more than 16 kings, two or more kings are in the same bucket and attack each other. So there are at most 16 non-attacking kings. The argument generalizes to a $2n\times 2n$ board, for which n^2 is the maximum number of non-attacking kings.



(d) With $k+1$ numbers, some difference is divisible by k. Define pigeonholes $0, 1, \ldots, k-1$. There are k pigeonholes. The $k+1$ numbers are the pigeons. Place a number x in pigeonhole i if the remainder when x is divided by k is i. That is, pigeonhole$(x) = \text{rem}(x, k)$. There are more numbers than pigeonholes, so two or more numbers x_1 and x_2 are in the same pigeonhole. That is, $\text{rem}(x_1, k) = \text{rem}(x_2, k)$, or $x_1 \equiv x_2 \pmod{k}$ and $k | x_1 - x_2$.

(e) Pick any $n+1$ distinct numbers from $1, 2, \ldots, 2n$. Consider the n bins $\{1, 2n\}, \{2, 2n-1\}, \ldots, \{n, n+1\}$. Place each number picked into its bin. Since there are $n+1$ numbers, some bin has two numbers and those two numbers sum to $2n+1$.

(f) The 4 suits are pigeonholes and cards are pigeons. Place a card into the pigeonhole for its suit. By part (e) sub-part (i), there are at least $\lceil 17/4 \rceil = 5$ cards in one pigeonhole (suit). That is, there must be a 5-card flush.

(g) If no the unit squares overlap, they cover an area of. The circle's area is $A = 4\pi \approx 12.57 < 13$. So, if the squares do not overlap, they cover an area larger than the circle, a contradiction. Thus, the squares must overlap.

Exercise 14.9. Let there be z_i pigeons in pigeonhole i, for $i = 1, \ldots, k$. Then $n = \sum_{i=1}^{k} z_i$. If no pigeonhole has at least $\lceil n/k \rceil$ pigeons, $z_i < \lceil n/k \rceil$. Since $\lceil n/k \rceil$ is an integer, it means that $z_i \leq \lceil n/k \rceil - 1$. One can verify $\lceil n/k \rceil - 1 < n/k$ by separately considering the cases n/k is an integer or not. Therefore,

$$n = \sum_{i=1}^{k} z_i \leq \sum_{i=1}^{k} (\lceil n/k \rceil - 1) < \sum_{i=1}^{k} n/k = n.$$

This contradiction proves that $z_i \geq \lceil n/k \rceil$ for at least one i.

(a) 350 students are pigeons and each month is a pigeonhole. At least $\lceil 350/12 \rceil = 30$ pigeons are born in some month.

(b) The 25 pigeonholes are $0, 1, \ldots, 24$ corresponding to the number of apples. The 51 baskets are pigeons. Some pigeonhole has at least $\lceil 51/25 \rceil = 3$ baskets. Those baskets have the same number of apples.

(c) The 10 grades are the bins. (i) Let s be the number of students. To gguarantee at least 10 with the same grade, we need $\lceil s/10 \rceil = 10$ or $s/10 > 9$. The smallest such s is 91. (ii) No matter how many students you have, they could all get `A-`, so you can't guarantee this.

Exercise 14.10.

(a) (i) Certainly the longest non-increasing subsequence ending at x_i contains x_i, so $1 \leq \ell_i$. By assumption, $\ell_i \leq n$. So, there are n possibilities for ℓ_i: $1, 2, \ldots, n$. Define the pigeonholes $1, 2, \ldots, n$. The numbers $x_1, \ldots, x_{n^2+1}$ are the pigeons. Place the number x_i into the pigeonhole corresponding to ℓ_i. Since there are n^2+1 pigeons and n pigeonholes, there is at least one pigeonhole with at least $\lceil (n^2+1)/n \rceil$ pigeons. $\lceil (n^2+1)/n \rceil = \lceil n + 1/n \rceil = n+1$. That is, there are at least $n+1$ of the ℓ_i that are equal.

(ii) Suppose $\ell_i = \ell_j$. Then we show that $x_j < x_i$. Suppose, to the contrary, that $x_j \geq x_i$. The longest non-decreasing sequence ending at x_i has length ℓ_i. Take this sequence and add x_j to the end: since $x_j \geq x_i$, this is a non-decreasing sequence that ends at x_j, so the *longest* non-decreasing sequence ending at x_j has length at least $\ell_i + 1$ which contradicts the fact that $\ell_j = \ell_i$ So $x_j < x_i$.

Thus, if $\ell_{i_1} = \ell_{i_2} = \cdots \ell_{i_k}$, then $x_{i_k} < x_{i_{k-1}} < \cdots < x_{i_2} < x_{i_1}$. That is, $x_{i_1}, \ldots, x_{i_k}$ are non-increasing.

By (ii), there are $n+1$ of the ℓ_i that are equal. That is, $\ell_{i_1} = \cdots \ell_{i_{n+1}}$, which means $x_{i_1}, \ldots, x_{i_{n+1}}$ are a non-increasing subsequence of length $n+1$, concluding the proof. ∎

This result is tight in that there are n^2 numbers for which there are non-increasing and non-decreasing sequences of length n but neither of length $n+1$. For example

$$2, 4, 1, 3 \ (n = 2) \qquad\qquad 3, 6, 9, 2, 5, 8, 1, 4, 7 \ (n = 3)$$

(b) More generally let $a_1, a_2, \ldots, a_n$ be a string of n integers and define $S_i = a_1 + a_2 + \cdots + a_i$,

$$\begin{aligned} S_1 &= a_1 \\ S_2 &= a_1 + a_2 \\ &\vdots \\ S_n &= a_1 + a_2 + \cdots + a_n. \end{aligned}$$

If $S_i \equiv= 0 \pmod{n}$ for any i then that substring solves our problem. Otherwise $S_i \equiv= k \pmod{n}$ for $1 \leq k \leq n-1$. Define $n-1$ pigeonholes for the possible values of k and place each S_i into its corresponding bin. So at least two sums are in the same bin, that is for $i < j$, $S_j \equiv S_i \pmod{n}$. This means $n | S_j - S_i$, or the substring sum $a_{i+1} + a_{i+2} + \cdots + a_j$ is divisible by n.

(c) We colored the squares in the 4×4 grid so that each color is in each column and each row (a latin square). This construction generalizes to an $n \times n$ latin square. Two castles on the same colored square are non-attacking. Since there are 4 colors (the pigeonholes), placing 9 castles will require at least $\lceil 9/4 \rceil = 3$ castles to occupy one color. Those castles don't attack each other.

Chapter 15

Pop Quiz 15.1.

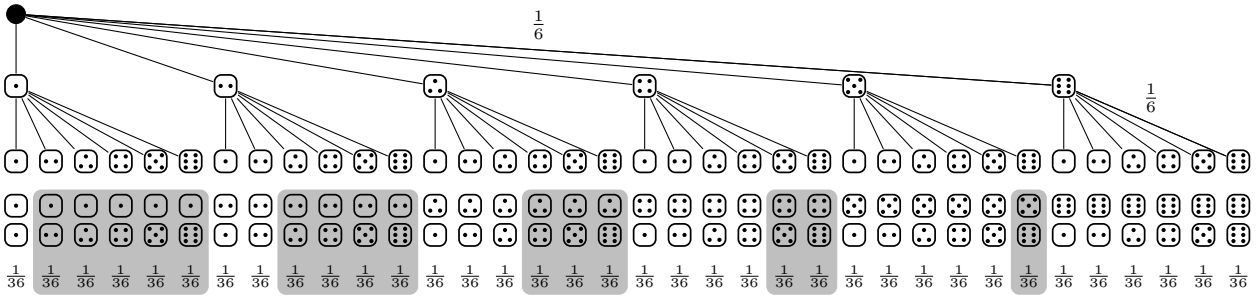
(a) The statement involves John Smith and liver disease. The crucial aspect about a probabilistic statement is to determine exactly what is the "source of the randomness". Is it that 30% of the John Smiths will survive till seventy? Is it that 30% of the *John Smiths* who are diagnosed with liver disease will survive till seventy? Is it that 30% of people diagnosed with liver disease will survive till seventy (and this persons name being John Smith is incidental)? Based on our intuitive understanding of the context, most would agree that the name is incidental, and the probabilistic statement is being made about people diagnosed with liver disease.

My interpretation: from all people diagnosed with liver disease, about 30% of them will survive till seventy.

(b) Approximately 0.01% of internet packets are "dropped" and about 99.99% of them reach their destination.

(c) Between now and your wedding, several "random things will occur". In some cases I make the wedding (e.g. I finish my thesis); and, in some cases, I won't (e.g. my experiments fails and I must redo it). In half the cases I make it. This is similar to "The chance of rain tomorrow is 40%". If we "re-live" the time between now and your wedding 100 times, in approximately 50 of those reincarnations I will be at your wedding.

Pop Quiz 15.2. Here is the outcome-tree with edge probabilities and outcome-probabilitities.

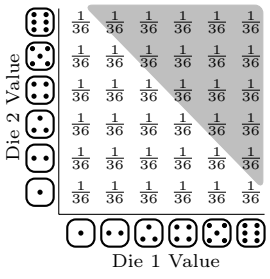


The edge probabilities are all $\frac{1}{6}$ because at each vertex the die-rolls is random. You win in the shaded outcomes when the second roll is larger than the first (event of interest). Adding outcome probabilities for the shaded event,

$$\mathbb{P}[\text{"Win"}] = \tfrac{1}{36} \times (5+4+3+2+1) = \tfrac{5}{12}.$$

The probability to win the dice game is less, by $\frac{1}{12}$ than the probability to win the coin game. Over many games, you win 8.33% more coin games. You prefer the coin game.

We mention a more convenient representation for the outcomes of a pair of dice. Instead of using a cumbersome tree, we can use a two dimensional grid illustrated on the right. On the x-axis are rolls for die 1 and on the y-axis are rolls for die 2. The outcomes are pairs, one from the x-axis and one from the y-axis, and every pair has the same outcome probability $\frac{1}{36}$. This representation of the outcomes is much more compact than the tree. The event of interest is the same, and we have shaded the outcomes where you win. As above, there are 15 outcomes in the event of interest, so again, $\mathbb{P}[\text{"Win"}] = \frac{15}{36} = \frac{5}{12}$.



The outcome-tree is the way to obtain the outcomes and outcome-probabilities. Once you have the outcomes and outcome probabilities, you have no further need for the outcome tree. What matters are the outcomes, when defining the event of interest, and the outcome-probabilities when computing the probability of the event. Thus, it is often more convenient to represent the outcomes and their probabilities in a more compact way as we did here with a grid.

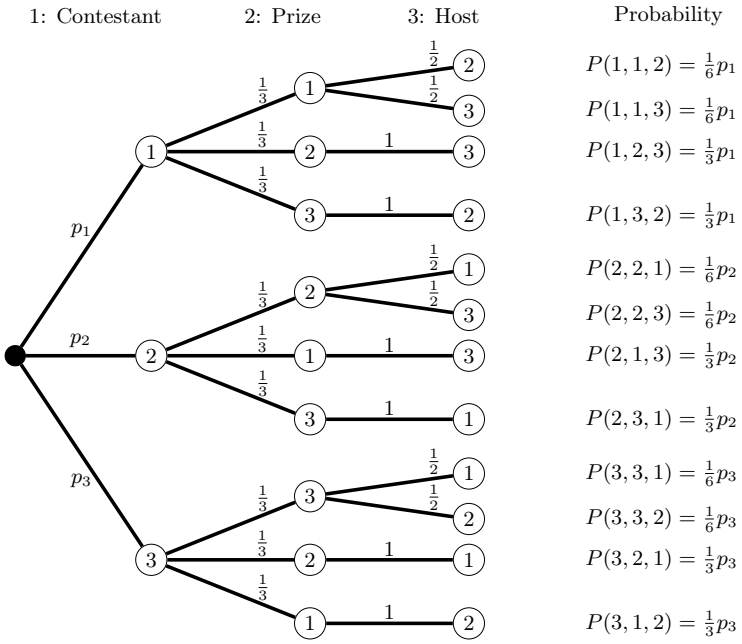
Pop Quiz 15.3. From partial outcome (1,2), the host has only one option, to open empty door 3. From partial outcome (1,1), the host has a choice because both doors are empty. The two edges correspond to the two choices.

Pop Quiz 15.4.

(a) We use the 6-step method with the outcome-tree.

(i) Instead of the contestant choosing door 1, the contestant chooses any door he wishes. Since we are not told the probabilities with which the contestant chooses each door, we denoted these (possibly different) probabilities by p_1, p_2, p_3, where $p_1 + p_2 + p_3 = 1$. By switching, the contestent wins for the event

$$\mathcal{E} = \{(1,2,3),(1,3,2),(2,1,3),(2,3,1),(3,2,1),(3,1,2)\}.$$



The probability of winning by switching is

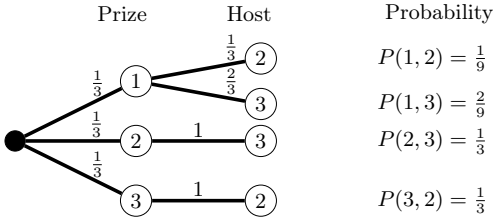
$$\mathbb{P}[\mathcal{E}] \;=\; \tfrac{1}{3}p_1 + \tfrac{1}{3}p_1 + \tfrac{1}{3}p_2 + \tfrac{1}{3}p_2 + \tfrac{1}{3}p_3 + \tfrac{1}{3}p_3 \;=\; \tfrac{2}{3}(p_1+p_2+p_3) \;=\; \tfrac{2}{3}.$$

The probability to win by switching has not changed, as expected. All we are doing is relabeling the doors: "contestant door" is door 1. The other two doors are arbitrarily labeled 2 and 3.

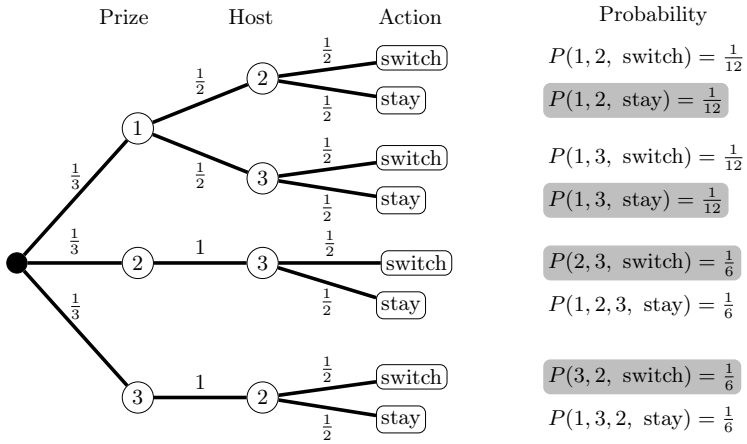
(ii) The outcome-tree is the same; the edge-probabilities change.

The outcome-probabilities for the winning outcomes are the same.

The probility to win by switching is still $\frac{2}{3}$.



(b) We add a level in the outcome-tree for what the contestant does after the host opens a door.



The probability of the outcomes where the contestant wins are highlighted with gray shading. Adding these outcome-probabilities gives $\mathbb{P}[\text{"ContestantWins"}] = \frac{1}{12} + \frac{1}{12} + \frac{1}{6} + \frac{1}{6} = \frac{1}{2}$.

(c) You should do the outcome tree for practice. We reason as follows. You win by staying with probability $\frac{1}{4}$, when the prize is at door 1. $\frac{3}{4}$-th of the time, the prize is at one of the doors 2,3,4. The host opens one door, so that leaves 2 doors, which means half the time that the prize is behind one of the doors 2,3,4, you get it right by switching. That is you win with probability $\frac{3}{4} \times \frac{1}{2}$ if you switch.

$$\mathbb{P}[\text{"WinBySwitching"}] = = \tfrac{3}{8} \qquad\qquad \mathbb{P}[\text{"WinByStaying"}] \;=\; \tfrac{1}{4}.$$

Note, now the sum of these two probabilities is no longer 1. Why?

You may also wonder whether the answer depends on which door you switch to. For, example, what if you switch to the lowest number door available, or you switch to a door randomly. It does not matter. The reason is the prize is equally likely to be behind any door you switch to, so it does not matter which door you switch to.

Exercise 15.5.

(a) If you implement the algorithm and repeatedly run with $n = 120$, you might get different answers each time. So there is no "right" answer. We ran it once and got

outcome	(3,2)	(2,3)	(1,2)	(1,3)
number of times	42	34	22	22

Prize Door	1	2	3
number of times	44	34	42

Each prize door occurs roughly $\frac{1}{3}$rd of the time. The prize has no "preference" for any door.

Half of the time when the prize door is 1, the host opens door 2, and the other half the time, he opens door 3. When the prize door is 1, the host has no "preference" for a door.

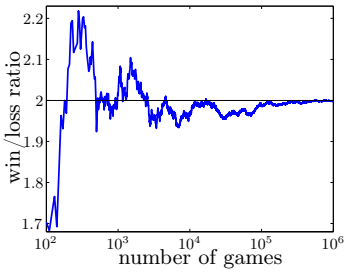
(b) If you switch, you win for the outcomes (3,2) and (2,3), which is 76 times.

(c) Switching is better: you win 76 times versus 44 times if you stay.

(d)

n	120	1,200	12,000
$\frac{\text{win}}{\text{loss}}$ ratio for switch	1.73	2.03	1.99

On the right we plot the win/loss ratio as you play more and more games. As the number of games played becomes larger, by switching, your win/loss ratio appears to "converge" to 2. You win about twice as often if you switch.



Exercise 15.6.

(a) In the table, we show the result of 10,000 games using the boxed Monte Carlo algorithm.

Die Battle	A versus B	B versus C	A versus C
Result	A wins 5527 games	B wins 5531 games	C wins 5538 games

```
1: dieA=[2,2,6,6,7,7]; dieB=[1,1,5,5,9,9];          % Die faces
2: NumGames = 1000;                                  % Number of games
3: Awins = 0;
4: for games = 1 to NumGames do
5:     a ← random value from dieA;
6:     b ← random value from dieB;
7:     if a > b then
8:         Awins ← Awins + 1;                        % Die A wins
9: return Awins
```

(b) Since we are on a roll with Monte-Carlo, lets see what simulation gives sum of two rolls:

A versus B	B versus C	A versus C
B wins 5171 games	C wins 5172 games	A wins 5371 games
A wins 4616 games	B wins 4584 games	C wins 4143 games
tie 213 games	tie 244 games	tie 486 games

```
1: dieA=[2,2,6,6,7,7]; dieB=[1,1,5,5,9,9];          % Die faces
2: NumGames = 1000;                                  % Number of games
3: Awins = 0; Bwins = 0;
4: for games = 1 to NumGames do
5:     a ← sum of two random values from dieA;
6:     b ← sum of two random values from dieB;
7:     if a > b then
8:         Awins ← Awins + 1;                        % Die A wins
9:     if b > a then
10:        Bwins ← Bwins + 1;                        % Die B wins
11: return Awins, Bwins
```

The winners of each battle are different. Though A dominates B in one roll, B dominates when you take the sum of two rolls. Very strange. Let's now do the outcome-tree analysis.

An outcome specifies the value of 4 rolls. For example, in the battle of A versus B, the outcome (2,2)(1,1) stands for die A rolling 2 then 2, and die B rolling 1 then 1.

Here are the die A outcomes:

outcome	(2,2)	(2,6)	(6,2)	(2,7)	(7,2)	(6,6)	(6,7)	(7,6)	(7,7)
sum	4	8	8	9	9	12	13	13	14

Here are the die B outcomes:

outcome	(1,1)	(1,5)	(5,1)	(1,9)	(9,1)	(5,5)	(5,9)	(9,5)	(9,9)
sum	2	6	6	10	10	10	14	14	18

Here are the die C outcomes:

outcome	(3,3)	(3,4)	(4,3)	(4,4)	(3,8)	(8,3)	(4,8)	(8,4)	(8,8)
sum	6	7	7	8	11	11	12	12	16

There are 9 outcomes for each die (2 rolls) and so in a battle, there are 81 possible outcomes (product rule). All the outcomes have the same probability $\frac{1}{3}\times\frac{1}{3}\times\frac{1}{3}\times\frac{1}{3}=\frac{1}{81}$.

<u>A versus B.</u> Let us count the outcomes where B beats A. If A is (2,2), 8 of B's outcomes beat the sum 4. In this way, for each outcome of A we count the outcomes of B which beat A, and then add them up (sum rule) to get the number of outcomes where B beats A:

$$\text{Number of outcomes where } B \text{ beats } A = 8+6+6+6+6+3+3+3+1 = 42.$$

Similarly, the number of outcomes where A beats B and A ties B are:

$$\text{Number of outcomes where } A \text{ beats } B = 9+8+8+4+4+4+0+0+0 = 37;$$
$$\text{Number of outcomes where } A \text{ ties } B = 0+0+0+0+0+0+0+0+2 = 2.$$

Therefore, B wins over A because

$$\mathbb{P}[\text{“}A \text{ beats } B\text{”}] = \frac{37}{81}; \qquad \mathbb{P}[\text{“}B \text{ beats } A\text{”}] = \frac{42}{81}; \qquad \mathbb{P}[\text{“}A \text{ ties } B\text{”}] = \frac{2}{81}.$$

<u>B versus C.</u> We perform the same analysis:

$$\text{Number of outcomes where } C \text{ beats } B = 9+8+8+5+5+5+1+1+0 = 42;$$
$$\text{Number of outcomes where } B \text{ beats } C = 6+6+6+6+3+3+3+3+1 = 37;$$
$$\text{Number of outcomes where } B \text{ ties } C = 0+1+1+0+0+0+0+0+0 = 2.$$

Therefore, C wins over B because

$$\mathbb{P}[\text{“}B \text{ beats } C\text{”}] = \frac{37}{81}; \qquad \mathbb{P}[\text{“}C \text{ beats } B\text{”}] = \frac{42}{81}; \qquad \mathbb{P}[\text{“}B \text{ ties } C\text{”}] = \frac{2}{81}.$$

<u>A versus C.</u> We perform the same analysis:

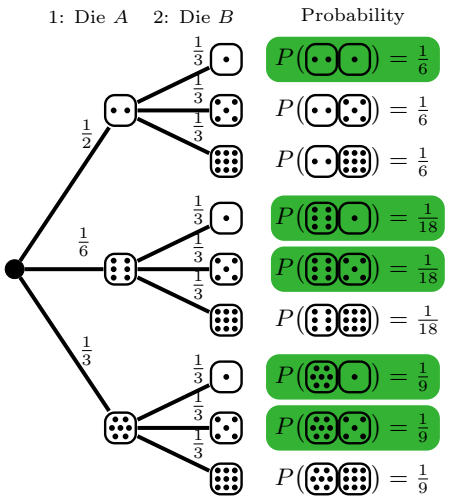
$$\text{Number of outcomes where } C \text{ beats } A = 9+5+5+5+5+1+1+1+1 = 33;$$
$$\text{Number of outcomes where } A \text{ beats } C = 8+8+8+6+4+4+3+3+0 = 44;$$
$$\text{Number of outcomes where } A \text{ ties } C = 0+1+1+0+0+2+0+0+0 = 4.$$

Therefore, A wins over C because

$$\mathbb{P}[\text{“}A \text{ beats } C\text{”}] = \frac{44}{81}; \qquad \mathbb{P}[\text{“}C \text{ beats } A\text{”}] = \frac{33}{81}; \qquad \mathbb{P}[\text{“}A \text{ ties } C\text{”}] = \frac{4}{81}.$$

(c) Now, for die A, $P(\square\square) = \frac{1}{2}$, $P(\square\square) = \frac{1}{6}$ and $P(\square\square) = \frac{1}{3}$. Only battles involving A change.

(i) The outcome-tree for A versus B is shown below. The probabilities for die A change, and this changes the outcome probabilities. The event of interest, outcomes where A beats B are unchanged (shaded).



Adding up the outcome-probabilities,

$$\mathbb{P}[\text{“Die}A\text{Beats}B\text{”}] = \tfrac{1}{6}+\tfrac{1}{18}+\tfrac{1}{18}+\tfrac{1}{9}+\tfrac{1}{9} = \tfrac{1}{2}.$$

It is now a tie between die A and B. We can repeat the analysis for dies A and C. The outcomes where C beats A are unchanged,

$$\{\square\square, \square\square, \square\square, \square\square, \square\square\}$$

The outcomes involving $\square$ for die A have probability $\frac{1}{6}$; those involving $\square$ have probability $\frac{1}{18}$; and, those involving $\square$ have probability $\frac{1}{9}$. So,

$$\mathbb{P}[\text{“Die}C\text{Beats}A\text{”}] = \tfrac{1}{6}+\tfrac{1}{6}+\tfrac{1}{6}+\tfrac{1}{18}+\tfrac{1}{9} = \tfrac{2}{3}.$$

A vs. B	B vs. C	A vs. C
$\mathbb{P}[A \text{ wins}] = \frac{1}{2}$	$\mathbb{P}[B \text{ wins}] = \frac{5}{9}$	$\mathbb{P}[C \text{ wins}] = \frac{2}{3}$

In a Monte-Carlo simulation with 10,000 rolls:

A vs. B	B vs. C	A vs. C
A wins 4967	B wins 5579	C wins 6658

(ii) Ayfos should choose die B (which beats C and is no worse than A). Now the best you can do is choose die A and its a dead tie. Ayfos wins about 500 of the 1000 games.

Pop Quiz 15.7. See the outcome-tree and outcome-probabilities in Exercise 15.6(c).

Pop Quiz 15.8.

(a) Valid because all probabilities are positive and sum to 1.

(b) Not valid because $P(\text{HT}) < 0$, and probabilities must be positive.

(c) Not valid. Even though all probabilities are positive, they do not sum to 1. Rescaling each probability by multiplying by $1/(\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5})$ would make them valid.

Exercise 15.9. Remember always that an event is a set of outcomes. We assume that students have only one color hair (hair cannot be both black and blonde).

(a) The outcomes are each student. Each student is equally likely.

(b) The event has all students with black or blonde hair (80% of the students): $\mathbb{P}[\text{“either black or blonde hair”}] = 0.8$.

(c) The event has the 20% of students in the complement of the previous event: $\mathbb{P}[\text{“neither black nor blonde hair”}] = 0.2$

(d) Trick question. We can only bound the probability. We want to know $|\{\text{Black hair}\} \cup \{\text{Brown eyes}\}|$. This size is at least 60% of the students (the brown eyed ones) and at most all the students, so

$$0.6 \leq \mathbb{P}[\text{“either black hair or brown eyes”}] \leq 1.$$

Assuming proportionality, $0.6 \times 50\% = 30\%$ of black haired students have brown eyes. By inclusion-exclusion,

$$|\{\text{Black hair}\} \cup \{\text{Brown eyes}\}| = 50\% + 60\% - 30\% = 80\%,$$

and therefore, assuming proportionality, $\mathbb{P}[\text{“either black hair or brown eyes”}] = 0.8$.

(e) Trick question. We can only give bounds. If all black-haired students have brown eyes, the intersection can be as large as 50%. If all the other 50% of students have brown eyes, then the intersection is as small as 10%. Therefore, $0.1 \leq \mathbb{P}[\text{“black hair and brown eyes”}] \leq 0.5$. Assuming proportionality, $\mathbb{P}[\text{“black hair and brown eyes”}] = 0.3$.

Exercise 15.10.

(a) We are told $\mathcal{E}_1 \cap \mathcal{E}_2 = \varnothing$.

$$\mathbb{P}[\mathcal{E}_1 \cup \mathcal{E}_2] = \sum_{\omega \in \mathcal{E}_1 \cup \mathcal{E}_2} P(\omega) \overset{(*)}{=} \sum_{\omega \in \mathcal{E}_1} P(\omega) + \sum_{\omega \in \mathcal{E}_2} P(\omega) = \mathbb{P}[\mathcal{E}_1] + \mathbb{P}[\mathcal{E}_2].$$

$(*)$ is because the outcomes in $\mathcal{E}_1 \cup \mathcal{E}_2$ can be partitioned into those in $\mathcal{E}_1$ and those in $\mathcal{E}_2$ because $\mathcal{E}_1 \cap \mathcal{E}_2 = \varnothing$. The sum rule generalizes to an arbitrary numebr of disjoint events.

$$\mathbb{P}[\cup_{i=1}^n \mathcal{E}_i] = \sum_{i=1}^n \mathbb{P}[\mathcal{E}_i].$$

(b) $\mathcal{E}$ and $\overline{\mathcal{E}}$ are disjoint, so $\mathbb{P}[\mathcal{E} \cap \overline{\mathcal{E}}] = \mathbb{P}[\mathcal{E}] + \mathbb{P}[\overline{\mathcal{E}}]$. Since $\mathcal{E} \cap \overline{\mathcal{E}} = \Omega$ and $\mathbb{P}[\Omega] = 1$, we have that

$$1 = \mathbb{P}[\Omega] = \mathbb{P}[\mathcal{E} \cap \overline{\mathcal{E}}] = \mathbb{P}[\mathcal{E}] + \mathbb{P}[\overline{\mathcal{E}}].$$

(c) Consider $\mathbb{P}[\mathcal{E}_1] + \mathbb{P}[\mathcal{E}_2] = \sum_{\omega \in \mathcal{E}_1} P(\omega) + \sum_{\omega \in \mathcal{E}_2} P(\omega)$. Every ω that is only in $\mathcal{E}_1$ contributes $P(\omega)$ to this sum once. Similarly, every ω that is only in $\mathcal{E}_2$ contributes $P(\omega)$ to the sum once. However, every $\omega \in \mathcal{E}_1 \cap \mathcal{E}_2$ contributes $P(\omega)$ twice to the sum, once in the sum over $\omega \in \mathcal{E}_1$ and once in the sum over $\omega \in \mathcal{E}_2$. By subtracting $P(\omega)$ from the total for every $\omega \in \mathcal{E}_1 \cap \mathcal{E}_2$, we ensure such $\omega \in \mathcal{E}_1 \cap \mathcal{E}_2$ contributes $P(\omega)$ exactly once. That is,

$$\mathbb{P}[\mathcal{E}_1 \cup \mathcal{E}_2] = \sum_{\omega \in \mathcal{E}_1 \cup \mathcal{E}_2} P(\omega) = \sum_{\omega \in \mathcal{E}_1} P(\omega) + \sum_{\omega \in \mathcal{E}_2} P(\omega) - \sum_{\omega \in \mathcal{E}_1 \cap \mathcal{E}_2} P(\omega) = \mathbb{P}[\mathcal{E}_1] + \mathbb{P}[\mathcal{E}_2] - \mathbb{P}[\mathcal{E}_1 \cap \mathcal{E}_2].$$

This formula mimics the inclusion-exclusion formula for counting the size of a union.

(d) By (c), $\mathbb{P}[\mathcal{E}_1 \cup \mathcal{E}_2] = \mathbb{P}[\mathcal{E}_1] + \mathbb{P}[\mathcal{E}_2] - \mathbb{P}[\mathcal{E}_1 \cap \mathcal{E}_2] \leq \mathbb{P}[\mathcal{E}_1] + \mathbb{P}[\mathcal{E}_2]$ because $\mathbb{P}[\mathcal{E}_1 \cap \mathcal{E}_2] \geq 0$.

(e) Let $\mathcal{E}_p$ be the outcomes where p is T. Let $\mathcal{E}_q$ be the outcomes where q is T. $p \to q$ means that whenever p is T, q is T. That is $\omega \in \mathcal{E}_p \to \omega \in \mathcal{E}_q$, or $\mathcal{E}_p \subseteq \mathcal{E}_q$. Since $P(\cdot)$ is non-negative, the sum over outcomes in $\mathcal{E}_q$ includes the sum over outcomes in $\mathcal{E}_p$ plus possibly other outcome-probabilities. That is, $\mathbb{P}[\mathcal{E}_p] \leq \mathbb{P}[\mathcal{E}_q]$, which means

$$\mathbb{P}[\text{“}p \text{ being true”}] \leq \mathbb{P}[\text{“}q \text{ being true”}].$$

(f) This follows from (e) because $p \to p \wedge q$. Alternatively, observe that $\mathcal{E}_1 \cap \mathcal{E}_2 \subseteq \mathcal{E}_1$.

Exercise 15.11.

(a) There are 36 outcomes in this uniform probability space (see Pop Quiz 15.2). The outcomes where the sum is 9 are $\{$  ,  ,  ,  $\}$. Therefore, $\mathbb{P}[\text{“Sum is 9”}] = \frac{1}{|\Omega|} \cdot (\#\text{ outcomes with sum 9}) = \frac{4}{36} = \frac{1}{9}$.

(b) You are not going to be able to draw the outcome tree here. To get to ann outcome, e.g. TTTTTTTTTT (ten tails in a row), you multiply 10 edge probabilities which are all $\frac{1}{2}$. This is the same for every outcome, so we have a uniform probability space with $|\Omega| = 2^{10}$ and $P = 2^{-10}$. The number of sequences with 4 heads is $\binom{10}{4}$. Therefore,

$$\mathbb{P}[\text{“4 heads”}] = \frac{\#\text{ outcomes with 4 heads}}{|\Omega|} = \frac{\binom{10}{4}}{2^{10}} \approx 0.2051.$$

(c) Each roll has 3 choices: {⚁, ⚂, ⚃}. The edge probabilities are $\frac{1}{3}$, a uniform probability space with 3^{10} outcomes.

(i) Choose 4 sevens in $\binom{10}{4}$ ways; the remaining 6 rolls can be chosen in 2 ways each for 2^6 ways (product rule). So, there are $\binom{10}{4} \times 2^6$ outcomes (product rule again). Therefore,

$$\mathbb{P}[\text{“4 sevens”}] = \frac{\#\text{ outcomes with 4 sevens}}{|\Omega|} = \frac{\binom{10}{4} \times 2^6}{3^{10}} \approx 0.2276.$$

(ii) Choose the 4 sevens in $\binom{10}{4}$ ways; of the remaining six rolls, choose 3 sixes in $\binom{6}{3}$ ways. By the product rule, there are $\binom{10}{4} \times \binom{6}{3} = 10!/4!3!3!$ outcomes. Therefore,

$$\mathbb{P}[\text{“4 sevens and 3 sixes”}] = \frac{\#\text{ outcomes with 4 sevens and 3 sixes}}{|\Omega|} = \frac{\binom{10}{4}\binom{6}{3}}{3^{10}} \approx 0.0711.$$

(iii) There are $\binom{10}{4} \times 2^6$ outcomes with 4 sevens; there are $\binom{10}{3} \times 2^7$ outcomes with 3 sixes; there are $\binom{10}{4} \times \binom{6}{3}$ outcomes with 4 sevens and 3 sixes. By inclusion-exclusion, there are $\binom{10}{4}\times 2^6 + \binom{10}{3}\times 2^7 - \binom{10}{4}\times\binom{6}{3} = 24,600$ outcomes with 4 sevens *or* 3 sixes. So,

$$\mathbb{P}[\text{“4 sevens or 3 sixes”}] = \frac{\#\text{ outcomes with 4 sevens or 3 sixes}}{|\Omega|} = \frac{24600}{3^{10}} \approx 0.4166.$$

(d) From Exercise 13.15, the number of Two-pair hands is 123,552 and the number of Three-of-a-kinds is (54,912). So,

$$\mathbb{P}[\text{“Two-pair”}] = \frac{123,552}{\binom{52}{5}} \approx 0.0475 \qquad \mathbb{P}[\text{“Three-of-a kind”}] = \frac{54,912}{\binom{52}{5}} \approx 0.0211.$$

Three-of-a-kind should win because it is rarer.

(e) We have a uniform probability space in which each of the $\binom{52}{13}$ possible 13-card hands is equally likely. A hand has no Ace means the 13 cards are selected from 48 cards. This can be done in $\binom{48}{13}$ ways. So the probability to not have any Aces is $\binom{48}{13}/\binom{52}{13}$. The complementary event is that the hand has an Ace, therefore

$$\mathbb{P}[\text{“Ace”}] = 1 - \frac{\binom{48}{13}}{\binom{52}{13}} = 1 - \frac{39 \times 38 \times 37 \times 36}{52 \times 51 \times 50 \times 49} \approx 0.6962.$$

Exercise 15.12. Tough problem. Rather than construct the infinite outcome-tree, we work directly with the probability space. The outcomes in the sample space are sequences of tosses of the form $\mathrm{T}^{\bullet i}\mathrm{HT}^{\bullet j}\mathrm{H}$, where $i, j \geq 0$,

$$\Omega = \{\mathrm{T}^{\bullet i}\mathrm{HT}^{\bullet j}\mathrm{H} \mid i, j \geq 0\}.$$

The probability of an outcome is $P(\mathrm{T}^{\bullet i}\mathrm{HT}^{\bullet j}\mathrm{H}) = 2^{i+j+2}$. For practice, let us verify these probabilities sum to 1,

$$\sum_{\omega} P(\omega) = \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} (\tfrac{1}{2})^{i+j+2} = \tfrac{1}{4}\sum_{i=0}^{\infty}(\tfrac{1}{2})^i \sum_{j=0}^{\infty}(\tfrac{1}{2})^j = \tfrac{1}{4}\times 2 \times 2 = 1.$$

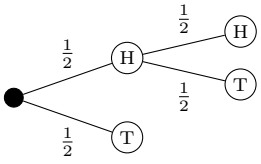
The outcomes where Ayfos wins are when $i+j$ is odd, so the event of interest is $\mathcal{E} = \{\mathrm{T}^{\bullet i}\mathrm{HT}^{\bullet j}\mathrm{H} \mid i, j \geq 0, i+j \text{ is odd}\}$. There are two cases, either i is odd and j is even, or i is even and j is odd. Therefore,

$$\mathbb{P}[\mathcal{E}] = \tfrac{1}{4}\sum_{k=0}^{\infty}(\tfrac{1}{2})^{2k+1}\sum_{\ell=0}^{\infty}(\tfrac{1}{2})^{2\ell} + \tfrac{1}{4}\sum_{k=0}^{\infty}(\tfrac{1}{2})^{2k}\sum_{\ell=0}^{\infty}(\tfrac{1}{2})^{2\ell+1} = \tfrac{1}{2}\sum_{k=0}^{\infty}(\tfrac{1}{2})^{2k+1}\sum_{\ell=0}^{\infty}(\tfrac{1}{2})^{2\ell} = \tfrac{1}{4}\sum_{k=0}^{\infty}(\tfrac{1}{2})^{2k}\sum_{\ell=0}^{\infty}(\tfrac{1}{2})^{2\ell} = \tfrac{1}{4}\times\tfrac{4}{3}\times\tfrac{4}{3} = \tfrac{4}{9}$$

So Ayfos, who goes first has the disadvantage. Ayfos wins with probability $\frac{4}{9}$. Liamsi wins with probability $1 - \frac{4}{9} = \frac{5}{9}$.

Exercise 15.13.

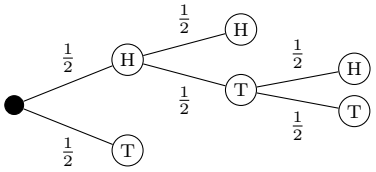
(a) The possible outcomes are sequences of heads and tails which end in either HHT or THH and there is no earlier occurrence of HHT or THH. So, HHT (you win), HHHT (you win), THH (friend wins), TTHTHH (friend wins) are possible outcomes, but TTHHT is not a possible outcome because though the sequence ends in HHT, there is an earlier occurrence of THH. The outcome space is infinite. It is quite a complicated outcome space. We cannot list out the possible outcomes with their probabilities. We show the how the game plays out as an outcome-tree.



Outcome	Probability	Winner
HH	$\frac{1}{4}$	You
HT	$\frac{1}{4}$	Friend
T	$\frac{1}{2}$	Friend

This outcome-tree is not showing outcomes of the game, but outcomes of coin tosses. Based on these outcomes of the coin tosses, we reason about the game. If a tail appears, and the game is not over, then we know your friend wins. This is because for you to win, there must occur HH; at the first occurrence of HH, a THH has appeared and your friend has won. If HH appears, then you win, because for your friend to win, a T must appear and at the first appearence of T, you have won. You win only if the coin tosses start out HH, that is $\mathbb{P}[\text{“you win”}] = \frac{1}{4}$.

(b) We use a similar reasoning here using outcomes of the coin tosses.



Outcome	Probability	Winner
HH	$\frac{1}{4}$	You
HTH	$\frac{1}{8}$	Friend
HTT	$\frac{1}{8}$	Restart
T	$\frac{1}{2}$	Restart

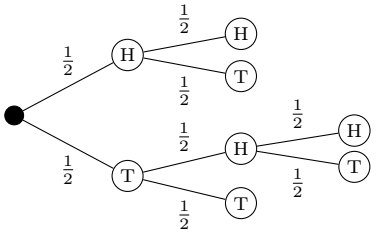
Let us explain the outcomes of the coin toss. As in (a), if the coin starts with HH, then you win, because for your friend to win, a tail must be tossed, but at the first toss of a tail, you win. If the coin tosses HTH, then your friend wins and the game ends. A winning sequence for either you or your friend must start with H. So, ff the coin starts with HTT or T, both of you are waiting for an H to start a possible winning sequence. This is the same situation as at the beginning of the game where you are both waiting for H. So the game effectively restarts.

You win (Y) with probability $\frac{1}{4}$; your friend wins (F) with probability $\frac{1}{8}$; the game "restarts" (R) with probability $\frac{5}{8}$. So the outcomes of the game are of the form $\mathrm{R}^{\bullet i}\mathrm{Y}$ (i restarts followed by you winning), or $\mathrm{R}^{\bullet i}\mathrm{F}$ (i restarts followed by your friend winning), where $i \geq 0$.

outcome	$\mathrm{R}^{\bullet i}\mathrm{Y}$	$\mathrm{R}^{\bullet i}\mathrm{F}$
probability	$\frac{1}{4} \times (\frac{5}{8})^i$	$\frac{1}{8} \times (\frac{5}{8})^i$

The outcomes where you win are $\mathrm{R}^{\bullet i}\mathrm{Y}$, so the probability is $\mathbb{P}[\text{"you win"}] = \frac{1}{4}\left[1 + \left(\frac{5}{8}\right) + \left(\frac{5}{8}\right)^2 + \cdots\right] = \frac{1}{4} \times \frac{1}{1-\frac{5}{8}} = \frac{2}{3}$.

(c) We use a similar reasoning here using outcomes of the coin tosses.



Outcome	Probability	Winner
HH	$\frac{1}{4}$	You
HT	$\frac{1}{4}$	?
THH	$\frac{1}{8}$	You
THT	$\frac{1}{8}$	Friend
TT	$\frac{1}{4}$	?

As above, for HH, you win at the first toss of tails. A similar reasoning applies to THH and THT is the winning sequence for your friend. The interesting cases are the questions marks when a tail is tossed, T or HT. Now, any number of tails can follow. At the first H, you win if the next toss is H and your friend wins if the next toss is T. We show the outcomes in the table below, where $i \geq 1$:

outcome	HH	$\mathrm{HT}^{\bullet i}\mathrm{HH}$	$\mathrm{HT}^{\bullet i}\mathrm{HT}$	$\mathrm{T}^{\bullet i}\mathrm{HH}$	$\mathrm{T}^{\bullet i}\mathrm{HT}$
probability	$\frac{1}{4}$	$\frac{1}{8} \times (\frac{1}{2})^i$	$\frac{1}{8} \times (\frac{1}{2})^i$	$\frac{1}{4} \times (\frac{1}{2})^i$	$\frac{1}{4} \times (\frac{1}{2})^i$
winner	you	you	friend	you	friend

The probability you win is the sum of the probabilities for the outcomes HH, $\mathrm{HT}^{\bullet i}\mathrm{HH}$ and $\mathrm{T}^{\bullet i}\mathrm{HH}$, for $i \geq 1$:

$$\mathbb{P}[\text{"you win"}] = \frac{1}{4} + \frac{1}{8}\sum_{i=1}^{\infty}\left(\frac{1}{2}\right)^i + \frac{1}{4}\sum_{i=1}^{\infty}\left(\frac{1}{2}\right)^i = \frac{1}{4} + \frac{1}{8} + \frac{1}{4} = \frac{5}{8}.$$

(d) Monte Carlo is useful for checking a probability analysis. In Figure 30.1 is a simulation to compute the probability that you win given your string and your friend's string. Let us justify the update in step 13.

Let W be the number of wins up to that point; *games* is the number of games played (including the current game) and *win* is the outcome of the current game. The previous value of *Pwin* is $W/(games-1)$ (0 if $games = 1$), that is $W = Pwin(games-1)$. The updated value of *Pwin* should be $(W + win)/games$

$$Pwin \leftarrow \frac{W + win}{games} = \frac{Pwin(games-1) + win}{games} = Pwin + \frac{win - Pwin}{games}.$$

The results of the simulation for 10^4, 10^5 and 10^6 games are shown in the next table.

Number of games	10,000	100,000	1,000,000
Probability you win (a)	0.2477	0.25	0.25
Probability you win (b)	0.6626	0.666	0.667
Probability you win (c)	0.6294	0.6235	0.6255

```
you = [1,1,0]; friend = [0,1,1];                          % H=1, T=0
NumGames = 10000;                                         % Number of games
Pwin = 0;                                                 % Probability you win
for games = 1 to NumGames do
   x ← random binary vector of length 3;
   while TRUE do
      if isequal(x, you) then
         win = 1; break out of while;                     % You win
      else if isequal(x, friend) then
         win = 0; break out of while;                     % Your friend wins
      else
         x[1] = x[2]; x[2] = x[3]; x[3] = random bit;     % Next toss
   Pwin ← Pwin + (win − Pwin)/games;                      % Update the probability
return Pwin
```

Figure 30.1: Monte Carlo algorithm to simulate tossing game.

The frequency (probability from the simulation) gets closer to the true probability as you play more.

(e) Behold the power of simulation. By symmetry, we may assume your friend's sequence starts with H. For each of the 4 possibilities, we can evaluate your 8 possible sequences and pick the best. Here are the simulation results.

	friend	your best choice	ℙ["your best wins"]	ℙ["your 2nd-best wins"]
(i)	HHH	THH	0.8747	0.7005
(ii)	HHT	THH	0.7500	0.5000
(iii)	HTH	HHT	0.6668	0.6253
(iv)	HTT	HHT	0.6658	0.5004

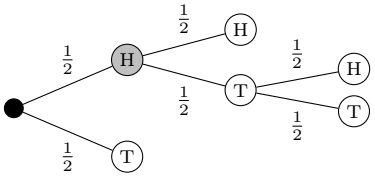
Let us analyze each of the 4 cases for your friends choice of string.

(i) If a T is tossed, you win at the first arrival of HH. So your friend can only win if the game specifically starts HHH, which has probability $\frac{1}{8}$. ℙ["THH beats HHH"] = $\frac{7}{8}$. You cannot do better with any other sequence (you must lose if the game starts HHH).

(ii) If the game starts HH (probability $\frac{1}{4}$), your friend wins at the first arrival of T. If the game starts any other way, you win at the first arrival of HH. So, ℙ["THH beats HHT"] = $\frac{3}{4}$.

(iii) We analyzed this in part (b). ℙ["HHT beats HTH"] = $\frac{2}{3}$.

(iv) Here are relevant outcomes of the coin tosses.



Outcome	Probability	Winner
HH	$\frac{1}{4}$	You
HTH	$\frac{1}{8}$	?
HTT	$\frac{1}{8}$	Friend
T	$\frac{1}{2}$	Restart

The outcome with the question mark is equivalent to restarting from the shaded H vertex. We conclude that the outcomes where you win start with any number of T's followed by any number of HT's followed by HH. That is, the outcomes where you win are $\mathrm{T}^{\bullet i}(\mathrm{HT})^{\bullet j}\mathrm{HH}$, having probability $(\frac{1}{2})^i \times (\frac{1}{4})^j \times \frac{1}{4}$. Therefore,

$$\mathbb{P}[\text{"HHT beats HTT"}] = \tfrac{1}{4}\sum_{i=0}^{\infty}\sum_{j=0}^{\infty}(\tfrac{1}{2})^i(\tfrac{1}{4})^j = \tfrac{1}{4}\times 2\times\frac{1}{1-\frac{1}{4}} = \tfrac{2}{3}.$$

Chapter 16

Pop Quiz 16.1.

(a) Barring catastrophes, ℙ[There is a living Human tomorrow] ≈ 1 and ℙ[Sun does not rise tomorrow] ≈ 1.

(b) *Given* the Sun does not rise tomorrow, some catastrophe indeed occurred. Humans are likely wiped out,

$$\mathbb{P}[\text{There is a living Human tomorrow} \mid \text{Sun does not rise tomorrow}] \approx 0.$$

The new information *significantly* changes the probability of Humans being around tomorrow.

Exercise 16.2.

(a) $\mathbb{P}[\text{CS} \mid \text{MATH}] = \dfrac{\mathbb{P}[\text{CS} \cap \text{MATH}]}{\mathbb{P}[\text{MATH}]} = \dfrac{0.016}{0.02} = 0.8$; (In general, $\mathbb{P}[A \mid B] \neq \mathbb{P}[B \mid A]$.)

$\mathbb{P}[\text{MATH} \mid \text{CS}] = \dfrac{\mathbb{P}[\text{CS} \cap \text{MATH}]}{\mathbb{P}[\text{CS}]} = \dfrac{0.016}{0.2} = 0.08.$

(b) (i) $\mathbb{P}[A|A] = \mathbb{P}[A \cap A]/\mathbb{P}[A] = 1$.
(ii) $\mathbb{P}[A|A \cap B] = \mathbb{P}[A \cap (A \cap B)]/\mathbb{P}[A \cap B] = \mathbb{P}[A \cap B]/\mathbb{P}[A \cap B] = 1$.
(iii) $\mathbb{P}[A \cap B|B] = \mathbb{P}[(A \cap B) \cap B]/\mathbb{P}[B] = \mathbb{P}[A \cap B]/\mathbb{P}[B] = \mathbb{P}[A \mid B]$.
(iv) $\mathbb{P}[A \cup B|B] = \mathbb{P}[(A \cup B) \cap B]/\mathbb{P}[B] = \mathbb{P}[B]/\mathbb{P}[B] = 1$.
(v) $\mathbb{P}[A|A \cup B] = \mathbb{P}[A \cap (A \cup B)]/\mathbb{P}[A \cup B] = \mathbb{P}[A]/\mathbb{P}[A \cup B]$.

(c) (i) $P_B(\omega) = \mathbb{P}[\{w\} \cap B]/\mathbb{P}[B]$. If $w \notin B$, $\mathbb{P}[\{w\} \cap B] = P[\varnothing] = 0$; otherwise, $\mathbb{P}[\{w\} \cap B] = \mathbb{P}[\{w\}] = P(w)$.
(ii) Recall $\mathbb{P}[B] = \sum_{w \in B} P(w)$.

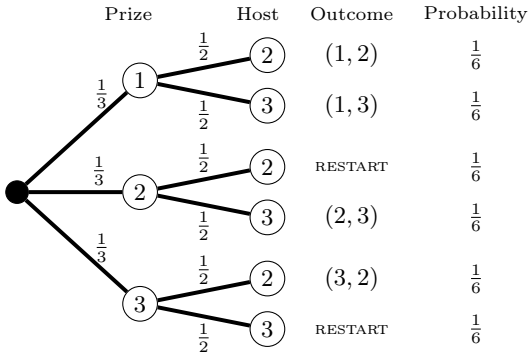
$$\sum_{w \in \Omega} P_B(\omega) = \sum_{w \in B} P_B(\omega) + \sum_{w \notin B} P_B(\omega) = \sum_{w \in B} \frac{P(\omega)}{\mathbb{P}[B]} + \sum_{w \notin B} 0 = \frac{1}{\mathbb{P}[B]} \sum_{w \in B} P(\omega) = \frac{\mathbb{P}[B]}{\mathbb{P}[B]} = 1$$

Pop Quiz 16.3.

(a) The outcomes are (i, j), where i is the first roll and j is the second roll. So, $1 \leq i, j \leq 6$. This is a uniform probability space so $P(i, j) = 1/(\text{number of outcomes}) = \frac{1}{36}$.
(b) The number of outcomes in the event is 3 so $\mathbb{P}[\text{Sum is 10}] = \frac{3}{36} = \frac{1}{12}$.
(c) The number of outcomes in the event is 9 so $\mathbb{P}[\text{Both are Odd}] = \frac{9}{36} = \frac{1}{4}$.
(d) Only 1 outcome has both dice odd and a sum 10, so $\mathbb{P}[(\text{Sum is 10}) \text{ AND } (\text{Both are Odd})] = \frac{1}{36}$.
(e) $\mathbb{P}[\text{Sum is 10} \mid \text{Both are Odd}] = \dfrac{\mathbb{P}[(\text{Sum is 10}) \text{ AND } (\text{Both are Odd})]}{\mathbb{P}[\text{Both are Odd}]} = \dfrac{\frac{1}{36}}{\frac{1}{4}} = \dfrac{1}{9}$.
(f) $\mathbb{P}[\text{Both are Odd} \mid \text{Sum is 10}] = \dfrac{\mathbb{P}[(\text{Sum is 10}) \text{ AND } (\text{Both are Odd})]}{\mathbb{P}[\text{Sum is 10}]} = \dfrac{\frac{1}{36}}{\frac{1}{12}} = \dfrac{1}{3}$.

Exercise 16.4.

(a) Similar to the example before Exercise 16.4 on page 228, with $P(1, 2) = 0$ and $P(1, 3) = 1$. The intuition is that Monty must open door 3 if it's available. If he doesn't, door 3 is not available and you must win by switching.
(b) The outcome tree is shown on the left. We want $\mathbb{P}[\text{WinBySwitching} \mid \text{Door2Opened}]$.

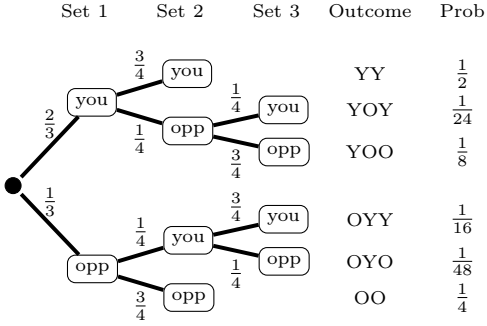


Door 2 is opened in outcomes $(1, 2)$ and $(3, 2)$. You win by switching in outcome $(3, 2)$, so the conditional probability that we need is

$$\frac{\mathbb{P}[\{(3,2)\}]}{\mathbb{P}[\{(1,2),(3,2)\}]} = \frac{\frac{1}{6}}{\frac{1}{6} + \frac{1}{6}} = \frac{1}{2}.$$

Now, it is even odds whether to switch or not. The intuition is that when the prize is behind door 3, Monty is no longer *forced* to open door 2. He may restart by opening door 3 half the time.

Exercise 16.5. On the left is the outcome-tree from which we can obtain the probabilities.



(a) Your wins are {YY,YOY,OYY}, with probability $\frac{1}{2} + \frac{1}{24} + \frac{1}{16} = \frac{29}{48}$
(b) (i) You win the set 1: {YY,YOY,YOO}. You win set 1 and match: {YY,YOY}.

$$\mathbb{P}[\text{Win set 1}] = \tfrac{1}{2} + \tfrac{1}{24} + \tfrac{1}{8} = \tfrac{2}{3};$$
$$\mathbb{P}[\text{Win set 1 \& match}] = \tfrac{1}{2} + \tfrac{1}{24} = \tfrac{13}{24};$$
$$\mathbb{P}[\text{Win match} \mid \text{set 1}] = \tfrac{13}{24}/\tfrac{2}{3} = \tfrac{13}{16};$$

(ii) From (a), $\mathbb{P}[\text{Win}] = \frac{29}{48}$. From (b), $\mathbb{P}[\text{Win set 1 \& match}] = \frac{13}{24}$. Therefore,

$$\mathbb{P}[\text{Win set 1} \mid \text{match}] = \tfrac{13}{24}/\tfrac{29}{48} = \tfrac{26}{26}.$$

Exercise 16.6.

(a) Yes. You estimate $\mathbb{P}[\text{student likes the course} \mid \text{student rated course}]$. Students who rate the course is not a random sampling of students. In general, surveys suffer from sampling bias. This type of sampling bias is sometimes called *non-response* bias. Those who do not respond tend to be a particular type of person, not random.

(b) Wald first surmised that the hits taken on planes should be somewhat random (shot accuracy is not high enough in an aerial battle to target specific parts of a plane). So there should be just as many hits on the tail and nose as main body. So the returing war-planes are not indicative of where the planes are getting hit; there are indicative of which planes *survive* given they are hit. He concluded that

$$\mathbb{P}[\text{survive} \mid \text{hit on mid-body}] \gg \mathbb{P}[\text{survive} \mid \text{hit on nose or tail}].$$

Therefore, the nose and tail are the regions that needed fortification.

Pop Quiz 16.7. You are not old enough to have any profession but student.

Pop Quiz 16.8. We require $\mathbb{P}[A \cap B]/\mathbb{P}[B] = \mathbb{P}[A \cap B]/\mathbb{P}[A]$ (assuming $\mathbb{P}[A], \mathbb{P}[B] > 0$), or $\mathbb{P}[A \cap B](\mathbb{P}[A] - \mathbb{P}[B]) = 0$. Either A and B must be disjoint so that $\mathbb{P}[A \cap B] = 0$, or $\mathbb{P}[A] = \mathbb{P}[B]$.

Exercise 16.9.

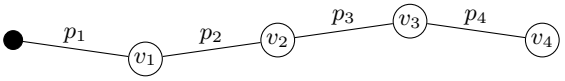
(a) By (16.1) on page 231, $\mathbb{P}[A_1 \cap (A_2 \cap A_3)] = \mathbb{P}[A_1 \mid A_2 \cap A_3] \times \mathbb{P}[A_2 \cap A_3]$. Applying (16.1) again,

$$\mathbb{P}[A_1 \cap A_2 \cap A_3] = \mathbb{P}[A_1 \mid A_2 \cap A_3] \times \mathbb{P}[A_2 \mid A_3] \times \mathbb{P}[A_3].$$

The general formula, which we encourage you to prove by induction, is

$$\mathbb{P}[A_1 \cap A_2 \cap \cdots \cap A_n] = \mathbb{P}[A_1 \mid A_2 \cap \cdots \cap A_n] \times \mathbb{P}[A_2 \mid A_3 \cap \cdots \cap A_n] \times \cdots \times \mathbb{P}[A_{n-1} \mid A_n] \times \mathbb{P}[A_n].$$

(b) Let us consider an example path on the outcome-tree to a leaf. The outcome is $v_1v_2v_3v_4$:



p_1 is the probability that v_1 occurs at the start, $p_1 = \mathbb{P}[v_1]$. *After* v_1 occurs, p_2 is the probability that v_2 occurs, given v_1 has occurred, $p_2 = \mathbb{P}[v_2 \mid v_1]$. Similarly, p_3 is the probability that v_3 occurs, given v_1, v_2 have occurred, $p_3 = \mathbb{P}[v_3 \mid v_1 \text{ AND } v_2]$; $p_4 = \mathbb{P}[v_4 \mid v_1 \text{ AND } v_2 \text{ AND } v_3]$. By part (a),

$$\mathbb{P}[v_4 \wedge v_3 \wedge v_2 \wedge v_1] = \mathbb{P}[v_4 \mid v_1 \wedge v_2 \wedge v_3] \times \mathbb{P}[v_3 \mid v_1 \wedge v_2] \times \mathbb{P}[v_2 \mid v_1] \times \mathbb{P}[v_1] = p_4p_3p_2p_1.$$

That is, the probability of the leaf outcome is exactly the product of the edge probabilities leading to that leaf.

Exercise 16.10.

(a) We don't care about rolls that are not x or 7, so we want the conditional probability

$$\mathbb{P}[x \mid x \text{ OR } 7] = \frac{\mathbb{P}[x \cap \{x \text{ OR } 7\}]}{\mathbb{P}[x \text{ OR } 7]} = \frac{\mathbb{P}[x]}{\mathbb{P}[x] + \mathbb{P}[7]},$$

where the last step is because getting x or 7 are disjoint events.

x	2	3	4	5	6	7	8	9	10	11	12
$\mathbb{P}[x]$	$\frac{1}{36}$	$\frac{2}{36}$	$\frac{3}{36}$	$\frac{4}{36}$	$\frac{5}{36}$	$\frac{6}{36}$	$\frac{5}{36}$	$\frac{4}{36}$	$\frac{3}{36}$	$\frac{2}{36}$	$\frac{1}{36}$
$\mathbb{P}[x \text{ before } 7]$	$\frac{1}{7}$	$\frac{2}{8}$	$\frac{3}{9}$	$\frac{4}{10}$	$\frac{5}{11}$	–	$\frac{5}{11}$	$\frac{4}{10}$	$\frac{3}{9}$	$\frac{2}{8}$	$\frac{1}{7}$

If you don't see the conditional probability, use total probability with three cases for the first roll: x, 7, not x or 7.

$$\begin{aligned}\mathbb{P}[x \text{ before } 7] &= \mathbb{P}[x \text{ before } 7 \mid x] \cdot \mathbb{P}[x] + \mathbb{P}[x \text{ before } 7 \mid 7] \cdot \mathbb{P}[7] + \mathbb{P}[x \text{ before } 7 \mid \text{not } x \text{ or } 7] \cdot \mathbb{P}[\text{not } x \text{ or } 7] \\ &= 1 \cdot \mathbb{P}[x] + 0 \cdot \mathbb{P}[7] + \mathbb{P}[x \text{ before } 7](1 - \mathbb{P}[x] - \mathbb{P}[7]).\end{aligned}$$

Solving for $\mathbb{P}[x \text{ before } 7]$ gives $\mathbb{P}[x \text{ before } 7] = \mathbb{P}[x]/(\mathbb{P}[x] + \mathbb{P}[7])$ as before.

(b) $\mathbb{P}[\text{win} \mid x]$ is 1 if $x \in \{7, 11\}$, 0 if $x \in \{2, 3, 12\}$ and $\mathbb{P}[x \text{ before } 7]$ if $x \in \{4, 5, 6, 8, 9, 10\}$. Using total probability,

$$\begin{aligned}\mathbb{P}[\text{win}] &= \sum_{x=2}^{12} \mathbb{P}[\text{win} \mid x]\mathbb{P}[x] \\ &= \mathbb{P}[7] + \mathbb{P}[11] + \sum_{x \in \{4,5,6,8,9,10\}} \mathbb{P}[x \text{ before } 7]\mathbb{P}[x] \\ &= \tfrac{6}{36} + \tfrac{2}{36} + \tfrac{3}{9} \cdot \tfrac{3}{36} + \tfrac{4}{10} \cdot \tfrac{4}{36} + \tfrac{5}{11} \cdot \tfrac{5}{36} + \tfrac{5}{11} \cdot \tfrac{5}{36} + \tfrac{4}{10} \cdot \tfrac{4}{36} + \tfrac{3}{9} \cdot \tfrac{3}{36} = \tfrac{976}{1908} \approx 0.4929.\end{aligned}$$

This is a dangerously close to a fair game, so whoever designed it was sure to know about probability.

Exercise 16.11. The conditional probability, $\mathbb{P}[A \mid B] = \mathbb{P}[A \cap B]/\mathbb{P}[B]$. Also, $\mathbb{P}[A \cap B] = \mathbb{P}[B \mid A]\mathbb{P}[A]$. Therefore,

$$\mathbb{P}[A \mid B] = \frac{\mathbb{P}[B \mid A]\mathbb{P}[A]}{\mathbb{P}[B]} = \frac{\mathbb{P}[B \mid A]\mathbb{P}[A]}{\mathbb{P}[B \mid A]\mathbb{P}[A] + \mathbb{P}[B \mid \overline{A}]\mathbb{P}[\overline{A}]}.$$

(The second equality is by the law of total probability, $\mathbb{P}[B] = \mathbb{P}[B \mid A]\mathbb{P}[A] + \mathbb{P}[B \mid \overline{A}]\mathbb{P}[\overline{A}]$.)

(a) Using R for Republican and D for democrat,

$$\mathbb{P}[\text{oppose taxes}] = \mathbb{P}[\text{oppose taxes} \mid \text{R}]\mathbb{P}[\text{R}] + \mathbb{P}[\text{oppose taxes} \mid \text{D}]\mathbb{P}[\text{D}] = 0.7 \times 0.4 + 0.5 \times 0.6 = 0.58.$$

(b) Using Bayes' Theorem, $\mathbb{P}[\text{R} \mid \text{oppose taxes}] = \dfrac{\mathbb{P}[\text{oppose taxes} \mid \text{R}]\mathbb{P}[\text{R}]}{\mathbb{P}[\text{oppose taxes}]} = \dfrac{0.7 \times 0.4}{0.58} \approx 0.483.$

Exercise 16.12. You win if two consecutive heads arrive before two consecutive tails.

(a) The outcomes where you win begin with $(\text{HT})^{\bullet i}$ or $\text{T}(\text{HT})^{\bullet i}$, and end with HH.

Winning outcomes	$(\text{HT})^{\bullet i}\text{HH}$	$\text{T}(\text{HT})^{\bullet i}\text{HH}$
Probability	$(p(1-p))^i \times p^2$	$(1-p) \times (p(1-p))^i \times p^2$

To get the probability of winning, we add these probabilities,

$$\mathbb{P}[\text{win}] = p^2 \sum_{i=0}^{\infty} (p(1-p))^i + p^2(1-p) \sum_{i=0}^{\infty} (p(1-p))^i = \frac{p^2(2-p)}{1-p(1-p)}.$$

(b) By the law of total probability,

$$\mathbb{P}[\text{win}] = \mathbb{P}[\text{win}|\text{H}]\mathbb{P}[\text{H}] + \mathbb{P}[\text{win}|\text{T}]\mathbb{P}[\text{T}] = p\mathbb{P}[\text{win}|\text{H}] + (1-p)\mathbb{P}[\text{win}|\text{T}].$$

Let us compute $\mathbb{P}[\text{win}|\text{H}]$ and $\mathbb{P}[\text{win}|\text{T}]$ using total probability.

$$\mathbb{P}[\text{win}|\text{H}] = (1-p)\mathbb{P}[\text{win}|\text{T}] + p.$$

(If you get H you won, and if you get T, it is as if you started with T.) Similarly,

$$\mathbb{P}[\text{win}|\text{T}] = p\mathbb{P}[\text{win}|\text{H}].$$

(If you get T you lost, and if you get H, it is as if you started with H.) Using this expression for $\mathbb{P}[\text{win}|\text{T}]$, we have: $\mathbb{P}[\text{win}|\text{H}] = p(1-p)\mathbb{P}[\text{win}|\text{H}] + p$. Solving for $\mathbb{P}[\text{win}|\text{H}]$:

$$\mathbb{P}[\text{win}|\text{H}] = \frac{p}{1-p(1-p)} \qquad \text{and} \qquad \mathbb{P}[\text{win}|\text{T}] = \frac{p^2}{1-p(1-p)}.$$

Substituting back, we get $\mathbb{P}[\text{win}] = \dfrac{p^2}{1-p(1-p)} + \dfrac{p^2(1-p)}{1-p(1-p)} = \dfrac{p^2(2-p)}{1-p(1-p)}.$

Chapter 17

Pop Quiz 17.1. This is a tricky question. The second toss is H with probability p, and that *is* independent of whether the first toss came up H or T. You can view this independence as "full-knowledge" independence, or the "universe"-view.

Suppose *you* must *predict* the second toss. Does knowing the first toss help you? Yes. From *your point of view*, the two tosses are *not* independent. The first toss tells you about p, which helps to predict the second toss. If the first toss is H, then you would guess that $p > \frac{1}{2}$ and predict the second toss as H. Imagine if the first 10 tosses are H. Now you most certainly would suspect that $p \approx 1$ (biased coin) and predict the 11th toss as H. Compare: The sun has risen every day in recorded history. Does that help you predict whether or not the sun will rise tomorrow?

If you fix $p = \frac{1}{3}$, now you don't care what the first toss was; p is what governs the second toss, so the two tosses are independent. Your view becomes the full-knowledge (or universe) view.

Exercise 17.2.

(a) False. Consider two disjoint events, each having positive probability.

(b) False. Consider the rain and clouds example, or $A = B$ with $\mathbb{P}[A] < 1$.

(c) True. $A \cap B \subseteq A$, therefore $\mathbb{P}[A \cap B] \leq \mathbb{P}[A]$; similarly $\mathbb{P}[A \cap B] \leq \mathbb{P}[B]$.

Exercise 17.3. We proved this formula in Exercise 16.11. Define the event

$$A = \{\text{Person is using a cellphone during a particular (fixed) weekday minute.}\}$$

Randomly pick a US-person. We want $\mathbb{P}[A]$. To use Fermi's method, break down A into smaller events.

$$A_1 = \text{"Has cellphone"}; \qquad A_2 = \text{"Uses cellphone in the particular minute"}.$$

A occurs if A_1 and A_2 occur.

$$\mathbb{P}[A] = \mathbb{P}[A_1 \cap A_2] = \mathbb{P}[A_1] \times P[A_2 \mid A_1]$$

Typical surveys say that 9 in 10 adults (15-70 years old) have a cellphone and adults are about 50% of the population. The typical cellphone plan is 1000 weekday minutes per month, which suggests that people who have a cellphone use about 1000 weekday minutes. Assume that phone usage is evenly spaced during the month and a weekday has 12 hours (8am-8pm) which is 720 minutes, so 20 weekdays in a month equals 14400 weekday minutes. 1000 minutes are spread evenly over these 14400 minutes. There are $\binom{14400}{1000}$ ways to pick 1000 of the 14400 minutes. If you do not use a particular minute, there are only $\binom{14399}{1000}$ ways. The probability to *not use* a particular weekday minute is $\binom{14399}{1000}/\binom{14400}{1000}$. Since $\binom{n-1}{k} = \frac{n-k}{n}\binom{n}{k}$, $\binom{14399}{1000}/\binom{14400}{1000} = \frac{14400-1000}{14400}$.

$\mathbb{P}[\text{Has cellphone}] \approx \frac{9}{10} \times \frac{1}{2} = \frac{9}{20}$.

$\mathbb{P}[\text{Uses cellphone on the minute} \mid \text{Has cellphone}] \approx \frac{1000}{14400} \approx \frac{1}{15}$.

Multiplying, $\mathbb{P}[A] \approx \frac{9}{20} \times \frac{1}{15} = \frac{3}{100}$. There are 320 million people in the USA, so about 10 million are in A.

Pop Quiz 17.4.

(a) Coins are independent, so any pair matches with probability $\frac{1}{2}$. This is also verified by "brute force" because, for example, $A_1 = \{\text{HHH, HHT, TTH, TTT}\}$ contains 4 outcomes and each has probability $\frac{1}{8}$ so $\mathbb{P}[A_1] = 4 \times \frac{1}{8} = \frac{1}{2}$.

(b) $A_2 = \{\text{HHH, THH, HTT, TTT}\}$, so $A_1 \cap A_2 = \{\text{HHH,TTT}\}$, and so $\mathbb{P}[A_1 \cap A_2] = 2 \times \frac{1}{8} = \frac{1}{4}\mathbb{P}[A_1] \times \mathbb{P}[A_2]$. A_1 and A_2 are independent. The other 2 cases are analogous.

(c) $A_1 \cap A_2 \cap A_3 = \{\text{HHH,TTT}\}$ (events A_1, A_2, A_3 simultaneously hold). So, $\mathbb{P}[A_1 \cap A_2 \cap A_3] = \frac{1}{4}$. If coins 1 and 2 match and 2 and 3 match, then 1 and 3 must match, so any two pairs matching means the third matches as well.

Pop Quiz 17.5.

(a) A_1 (blue) contains 18 outcomes, as does A_2, so $\mathbb{P}[A_1] = \mathbb{P}[A_2] = \frac{18}{36} = \frac{1}{2}$. A_3 contains 4 outcomes so $\mathbb{P}[A_3] = \frac{4}{36} = \frac{1}{9}$. The intersection of the three shaded regions contains just the one outcome (3,6), and so $\mathbb{P}[A_1 \cap A_2 \cap A_3] = \frac{1}{36}$, which is the product of the three probabilities. That is, we have 3-way independence.

(b) $A_1 \cap A_3$ contains the one outcome (3,6), so $\mathbb{P}[A_1 \cap A_3] = \frac{1}{36}$ and $\mathbb{P}[A_1] \cdot \mathbb{P}[A_3] = \frac{1}{18}$.

(c) $A_2 \cap A_3$ contains the three outcomes {(3,6), (4,5), (5,4)} so $\mathbb{P}[A_2 \cap A_3] = \frac{3}{36} = \frac{1}{12}$ and $\mathbb{P}[A_2] \cdot \mathbb{P}[A_3] = \frac{1}{18}$.

(d) The events are not 2-way independent.

Exercise 17.6.

(a) We use the definition of conditional probability.

$$\mathbb{P}[A_3 \mid A_1 \cap A_2] = \frac{\mathbb{P}[A_1 \cap A_2 \cap A_3]}{\mathbb{P}[A_1 \cap A_2]} = \frac{\mathbb{P}[A_1]\mathbb{P}[A_2]\mathbb{P}[A_3]}{\mathbb{P}[A_1]\mathbb{P}[A_2]} = \mathbb{P}[A_3].$$

The penultimate step is by independence.

(b) If $X = A_1, Y = A_2, Z = A_3$ the probability of the intersection equals the product by indemendence. Suppose that exactly one of sets is the complement, for example $Z = \overline{A_3}$. Then, by the law of total probability,

$$\mathbb{P}[A_1 \cap A_2 \cap \overline{A_3}] + \mathbb{P}[A_1 \cap A_2 \cap A_3] = \mathbb{P}[A_1 \cap A_2] \to \mathbb{P}[A_1 \cap A_2 \cap \overline{A_3}] = \mathbb{P}[A_1 \cap A_2] - \mathbb{P}[A_1 \cap A_2 \cap A_3].$$

Now we can use independence to obtain

$$\mathbb{P}[A_1 \cap A_2 \cap \overline{A_3}] = \mathbb{P}[A_1]\mathbb{P}[A_2] - \mathbb{P}[A_1]\mathbb{P}[A_2]\mathbb{P}[A_3] = \mathbb{P}[A_1]\mathbb{P}[A_2](1 - \mathbb{P}[A_3]) = \mathbb{P}[A_1]\mathbb{P}[A_2]\mathbb{P}[\overline{A_3}].$$

Let us give the general case and prove it by induction. Suppose $A_1, A_2, \ldots, A_n$ are independent. Let $X_i = A_i$ or $\overline{A_i}$. Then we want to show that

$$\mathbb{P}[X_1 \cap \cdots \cap X_n] = \mathbb{P}[X_1] \times \cdots \times \mathbb{P}[X_n].$$

We prove a stronger claim by induction: the probability of any k-way intersection of the X's equals the product of the k probabilities. The base case, $k = 1$, trivially holds. Suppose the claim holds for any k-way intersection and consider a $(k+1)$-way intersection. We must prove:

$$\mathbb{P}[X_{i_1} \cap \cdots \cap X_{i_{k+1}}] = \mathbb{P}[X_{i_1}] \times \cdots \times \mathbb{P}[X_{i_{k+1}}].$$

We use a second induction on the number of complements among these $k+1$ sets. When there are no complements, the claim follows by independence of the X_i. Suppose this claim holds when there are ℓ complements and consider the case where there are $\ell+1$ complements. Without loss of generality, we may assume that $X_{i_{k+1}} = \overline{A_{i_{k+1}}}$. Then,

$$\begin{aligned}
\mathbb{P}[X_{i_1} \cap \cdots \cap X_{i_k} \cap \overline{A_{i_{k+1}}}] &= \mathbb{P}[X_{i_1} \cap \cdots \cap X_{i_k}] - \mathbb{P}[X_{i_1} \cap \cdots \cap X_{i_k} \cap A_{i_{k+1}}] \\
&= \mathbb{P}[X_{i_1}] \times \cdots \times \mathbb{P}[X_{i_k}] - \mathbb{P}[X_{i_1} \cap \cdots \cap X_{i_k} \cap A_{i_{k+1}}] \\
&= \mathbb{P}[X_{i_1}] \times \cdots \times \mathbb{P}[X_{i_k}] - \mathbb{P}[X_{i_1}] \times \cdots \times \mathbb{P}[X_{i_k}] \times \mathbb{P}[A_{i_{k+1}}]. \\
&= \mathbb{P}[X_{i_1}] \times \cdots \times \mathbb{P}[X_{i_k}] \times (1 - \mathbb{P}[A_{i_{k+1}}]). \\
&= \mathbb{P}[X_{i_1}] \times \cdots \times \mathbb{P}[X_{i_k}] \times \mathbb{P}[X_{i_{k+1}}].
\end{aligned}$$

(The first step follows because the claim holds for all k-way intersections. The second because the second term has ℓ complements and the claim holds for ℓ complements.)

(c) Suppose $(*)$ in Exercise 17.6 holds for all 2^3 choices of (X, Y, Z). We must show 1,2 and 3-way independence. 3-way follows directly from $(*)$. Suppose we have proved k-way independence, and consider $(k-1)$-way independence.

$$\begin{aligned}
\mathbb{P}[A_{i_1} \cap \cdots \cap A_{i_{k-1}}] &= \mathbb{P}[A_{i_1} \cap \cdots \cap A_{i_{k-1}} \cap A_{i_k}] + \mathbb{P}[A_{i_1} \cap \cdots \cap A_{i_{k-1}} \cap \overline{A_{i_k}}] \\
&= \mathbb{P}[A_{i_1}] \cdots \mathbb{P}[A_{i_{k-1}}]\mathbb{P}[A_{i_k}] + \mathbb{P}[A_{i_1}] \cdots \mathbb{P}[A_{i_{k-1}}](1 - \mathbb{P}[A_{i_k}]) \\
&= \mathbb{P}[A_{i_1}] \cdots \mathbb{P}[A_{i_{k-1}}]
\end{aligned}$$

If $(*)$ in Exercise 17.6 holds, then k-way independence implies $(k-1)$-way independence. Since we have 3 way independence, we have 2 and then 1. Our argument holds for general $n > 3$.

Pop Quiz 17.7. Given $E_1, E_2, \ldots, E_{k-1}$, none of $s_k, \ldots, s_N$ are born on day 1 to day mathk-1. Suppose s_k is born on day k, then $s_{k+1}, \ldots, s_N$ ($N - k$ students) are all born on days $k+1$ to B ($B - k$ of the $B - k + 1$ days, given $E_1, E_2, \ldots, E_{k-1}$). By independence,

$$\mathbb{P}[E_k \mid E_1 \cap E_2 \cap \cdots \cap E_{k-1}] = \left(\tfrac{B-k}{B-k+1}\right)^{N-k}.$$

Exercise 17.8.

(a) We want $P = \prod_{k=1}^{N} \left(\frac{B-k}{B-k+1}\right)^{N-k}$, or equivalently, $\ln P = \sum_{k=1}^{N} (N-k) \ln \frac{B-k}{B-k+1}$. The sum can be evaluated, but the product is numerically unstable. Using $(1+\frac{1}{x})^x \approx e$ for large x, observe that

$$\left(\frac{B-k+1}{B-k}\right)^{N-k} = \left(1+\frac{1}{B-k}\right)^{N-k} = \left(1+\frac{1}{B-k}\right)^{B-k(N-k)/(B-k)} \approx e^{(N-k)/(B-k)},$$

Using this approximation in P, $P \approx \prod_{k=1}^{N} \exp(-\frac{N-k}{B-k}) = \exp\left(-\sum_{k=1}^{N} \frac{N-k}{B-k}\right)$. We evaluate the sum in the exponent,

$$\sum_{k=1}^{N} \frac{N-k}{B-k} = \sum_{k=1}^{N} \frac{N-B+B-k}{B-k} = \sum_{k=1}^{N} \frac{N-B}{B-k} + 1 = N + \sum_{k=1}^{N} \frac{N-B}{B-k}$$

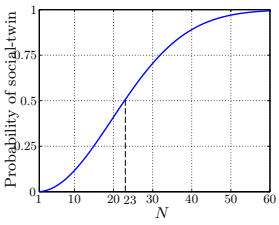
Using the integration method, $\sum_{k=1}^{N} \frac{N-B}{B-k} \approx (N-B) \int_1^N dx\ \frac{1}{B-x} = (N-B) \ln \frac{B-1}{B-N}$. Therefore,

$$P \approx e^{(B-N)\ln \frac{B-1}{B-N} - N}.$$

When $B = 366$ and $N = 200$, $P \approx e^{-69.2}$. Using the exact sum for $\ln P$, $P = e^{-68.4}$.

(b) Trick question. With 367 people and only 366 birthdays, by pigeonhole, two people must share the same birthday.

(c) We compute $\ln P = \sum_{k=1}^{N} (N-k) \ln \frac{B-k}{B-k+1}$, from which we obtaiin P The probability of no social twin is $1-P$. We show a plot $1-P$ versus N in th figure to the right. The probability of a social-twin rapidly increases and first goes over 0.5 for $N = 23$. So in a party of just 23, the odds favor there being a social-twin. By $N = 60$, it is essentially guaranteed that you have a social-twin.



(d) (i) Repetition is allowed. Each student has B choices giving B^N sequences.

(ii) Each sequence is equally likely so each has probability $1/B^N$.

(iii) The first k birthdays are chosen in $B(B-1)\cdots(B-k+1) = B!/(B-k)!$ ways. The remaining $N-k$ students choose (with repetition) from the remaining $B-k$ birthdays in $(B-k)^{N-k}$ ways. By the product rule, the number of sequences with no repetitions of the first k birthdays is

$$\frac{B!}{(B-k)!} \times (B-k)^{N-k}.$$

(iv) Multiply the number of allowed sequences in (iii) by their probability in (ii) to get

$$\mathbb{P}[\text{no repetition of first } k \text{ birthdays}] = \frac{1}{B^N} \times \frac{B!}{(B-k)!} \times (B-k)^{N-k}.$$

(v) We can cancel many terms in Equation (17.6) as follows:

$$\left(\tfrac{B-1}{B}\right)^{N-1} \left(\tfrac{B-2}{B-1}\right)^{N-2} \left(\tfrac{B-3}{B-2}\right)^{N-3} \cdots \left(\tfrac{B-k+1}{B-k+2}\right)^{N-k+1} \left(\tfrac{B-k}{B-k+1}\right)^{N-k}$$
$$= \frac{(B-1)^{N-1}}{B^{N-1}} \cdot \frac{(B-2)^{N-2}}{(B-1)^{N-2}} \cdot \frac{(B-3)^{N-3}}{(B-2)^{N-3}} \cdots \frac{(B-k+1)^{N-k+1}}{(B-k+2)^{N-k+1}} \cdot \frac{(B-k)^{N-k}}{(B-k+1)^{N-k}}$$

Terms in the same color simplify: the red terms simplify to $(B-1)$; the green to $(B-2)$; and so on. We get:

$$\frac{1}{B^{N-1}} \times \underbrace{(B-1)(B-2)\cdots(B-k+1)}_{\frac{1}{B} \times \frac{B!}{(B-k)!}} \times (B-k)^{N-k} = \frac{1}{B^N} \times \frac{B!}{(B-k)!} \times (B-k)^{N-k}.$$

(vi) When $k = N$, the result follows from

$$\frac{B(B-1)(B-2)\cdots(B-(N-1))}{B^N} = \frac{B}{B} \cdot \frac{(B-1)}{B} \cdot \frac{(B-2)}{B} \cdots \frac{(B-(N-1))}{B},$$

To derive this formula directly, observe that

$$\begin{aligned}
\mathbb{P}[s_2 \text{ does not match } s_1] &= 1 - \tfrac{1}{B}; \\
\mathbb{P}[s_3 \text{ does not match any of } s_1, s_2 \mid \text{no match in } s_1, s_2] &= 1 - \tfrac{2}{B} \\
\mathbb{P}[s_4 \text{ does not match any of } s_1, s_2, s_3 \mid \text{no match in } s_1, s_2, s_3] &= 1 - \tfrac{3}{B} \\
&\vdots \\
\mathbb{P}[s_N \text{ does not match any of } s_1, \ldots, s_{N-1} \mid \text{no match in } s_1, \ldots, s_{N-1}] &= 1 - \tfrac{N-1}{B}.
\end{aligned}$$

Multiplying these conditional probabilities,

$$\mathbb{P}[\text{no match in } s_1, s_2, \ldots, s_N] = (1-\tfrac{1}{B}) \times (1-\tfrac{2}{B}) \times (1-\tfrac{3}{B}) \times \cdots \times (1-\tfrac{N-1}{B}).$$

Exercise 17.9.

(a) $B = 300$ and $N = 100$, so we can use $e^{-N(N-1)/B} \le \mathbb{P}[\text{no collisions}] \le e^{-N(N-1)/2B}$:

$$e^{-33} \le \mathbb{P}[\text{no collisions}] \le e^{-16.5} \qquad \text{(essentially 0)}.$$

(i) There are no collisions if and only if every bin has at most one object, so:
$$e^{-33} \le \mathbb{P}[\text{every bin has at most one object}] \le e^{-16.5}.$$
(ii) A bin has more than one object if and only if there's a collision which has probability $1-\mathbb{P}[\text{no collisions}]$. So,
$$1-e^{-16.5} \le \mathbb{P}[\text{some bin has more than one object}] \le 1-e^{-33}.$$

(b) We want $\mathbb{P}[\text{no collisions}] \ge 0.9$, so we set $e^{-N(N-1)/B} \ge 0.9$ which gives $B \ge \lceil N(N-1)/\ln(1/0.9) \rceil$, or $B = 93,964$. That is a pretty big table size for just 100 words.

(c) $\mathbb{P}[\text{no collisions}] \ge e^{-N(N-1)/B}$. When $B = N^{2+\epsilon}$, $N(N-1)/B = N^{-\epsilon} - 1/N^{1+\epsilon} \to 0$. Therefore $e^{-N(N-1)/B} \to 1$. Probabilities are at most 1, so $\mathbb{P}[\text{no collisions}] \to 1$.

(d) $\mathbb{P}[\text{no collisions}] \le e^{-N(N-1)/2B}$. When $B = N^{2-\epsilon}$, $N(N-1)/2B = \frac{1}{2}N^{\epsilon} - \frac{1}{2}N^{\epsilon-1} \to \infty$ for $1 > \epsilon > 0$. Therefore $e^{-N(N-1)/2B} \to 0$. Probabilities are at least 0, so $\mathbb{P}[\text{no collisions}] \to 0$.

Pop Quiz 17.10. By interchanging home and the lockup, $\mathbb{P}[\text{home}] = \frac{1}{3}$. Alternatively, the successful step-sequences are L(RL)$^{\bullet i}$L, having probability $\frac{1}{2} \times (\frac{1}{4})^i \times \frac{1}{2}$. Summing these probabilities,
$$\mathbb{P}[\text{home}] = \tfrac{1}{4}\sum_{i=0}^{\infty}\left(\tfrac{1}{4}\right)^i = \tfrac{1}{4} \times \tfrac{1}{1-\frac{1}{4}} = \tfrac{1}{3}.$$
Alternatively, by the law of total probability,
$$\mathbb{P}[\text{home}] = \underbrace{\mathbb{P}[\text{home} \mid \text{LR}]\mathbb{P}[\text{LR}]}_{P[\text{home}] \times \frac{1}{4}} + \underbrace{\mathbb{P}[\text{home} \mid \text{LL}]\mathbb{P}[\text{LL}]}_{1 \times \frac{1}{4}} + \underbrace{\mathbb{P}[\text{home} \mid \text{R}]\mathbb{P}[\text{R}]}_{0 \times \frac{1}{2}}.$$
That is, $\mathbb{P}[\text{home}] = \frac{1}{4} \cdot \mathbb{P}[\text{home}] + \frac{1}{4}$. Solving, $\mathbb{P}[\text{home}] = \frac{1}{4}/(1-\frac{1}{4}) = \frac{1}{3}$.

Exercise 17.11.

(a) As in example 17.5, we want $P(200, 200, \frac{18}{38}) = (\beta^{400} - \beta^{200})/(\beta^{400} - 1)$, where $\beta = 0.9$. The probability to double up is about $7 \times 10^{-10} \approx 0$. If the bet size is \$5, she is 40 steps from the goal and ruin, so the chances increase to 0.015. The best bet-size is \$200, betting all or nothing with a double up probability of $\frac{18}{38} \approx 0.474$.

(b) Let x be the amount of money you start with. Then for $p = 18/38$, $\beta = 18/20 = 9/10$ and
$$\mathbb{P}[\text{win}] = \frac{\beta^{100} - \beta^{100+x}}{1 - \beta^{100+x}} = \beta^{100}\frac{1-\beta^x}{1-\beta^{100+x}} \le \beta^{100}.$$
The win-probability is at most $\beta^{100} \approx 0.0027\%$, no matter how much money you start with!. A more accurate estimate, ignoring the minute denominator is $\mathbb{P}[\text{win}] \approx \beta^{100}(1-\beta^x)$.

Exercise 17.11. This interesting problem has a counter-intuitive answer. One expects the person farthest from you is most likely to get bread last, but this is not true. Everyone but yourself is *equally likely* to be the last. This includes the person next to you as well as the person diametrically opposite. Everyone has a probability $\frac{1}{14}$ to be the last.

Consider person x. One of x's two neighbors gets the bread before the other. In this situation, the bread needs to travel $n-2$ steps to the other neighbor before reaching x if x is the last to get the bread (n is the number of people). That is, we have a random walk with $k = 1$ (one step to reach x) $n-2$ steps in the other direction to reach the other neighbor *before* x. So, $k = 1, L = n-1$ and $\beta = 1$. The probability to reach x first is $(L-1)/L = (n-2)/(n-1)$. This is the probability that x is not last. The probability x is last is $1/(n-1)$, as claimed.

Important: If you do not believe it, use Monte Carlo to play out bread passing with 5 people and check.

Chapter 18

Pop Quiz 18.1.

(a) (i) $\mathbf{X} = 2$ and $\mathbf{Y} = 1$ are disjoint so $\mathbb{P}[\mathbf{X} = 2 \cap \mathbf{Y} = 1] = 0$. $\mathbb{P}[\mathbf{X} = 2] \times \mathbb{P}[\mathbf{Y} = 1] = \frac{3}{8} \times \frac{1}{4} = \frac{3}{32}$. The two do not match. The events are not independent.

(ii) $\{\mathbf{X} = 2\} \cap \{\mathbf{Y} = 1\} = \{\text{HHH}\}$, hence $\mathbb{P}[\mathbf{X} = 2 \cap \mathbf{Y} = 1] = \frac{1}{8}$. $\mathbb{P}[\mathbf{X} \ge 2] \times \mathbb{P}[\mathbf{Y} = 1] = \frac{1}{2} \times \frac{1}{4} = \frac{1}{8}$. The two match. The events are independent.

(b) (i) $\mathbb{P}[\mathbf{X} = 2 \mid \mathbf{Y} = 0] = \dfrac{\mathbb{P}[\mathbf{X} = 2 \cap \mathbf{Y} = 0]}{\mathbb{P}[\mathbf{Y} = 0]} = \frac{3}{8}/\frac{6}{8} = \frac{1}{2}$. (ii) $\mathbb{P}[\mathbf{X} \ge 2 \mid \mathbf{Y} = 0] = \dfrac{\mathbb{P}[\mathbf{X} \ge 2 \cap \mathbf{Y} = 0]}{\mathbb{P}[\mathbf{Y} = 0]} = \frac{3}{8}/\frac{6}{8} = \frac{1}{2}$.

Exercise 18.2. Let us first construct the (non-uniform) probability space and the random variables.

outcome	HHHH	HHHT	HHTH	HHTT	HTHH	HTHT	HTTH	HTTT	THHH	THHT	THTH	THTT	TTHH	TTHT	TTTH	TTTT
probability	$\frac{16}{81}$	$\frac{8}{81}$	$\frac{8}{81}$	$\frac{4}{81}$	$\frac{8}{81}$	$\frac{4}{81}$	$\frac{4}{81}$	$\frac{2}{81}$	$\frac{8}{81}$	$\frac{4}{81}$	$\frac{4}{81}$	$\frac{2}{81}$	$\frac{4}{81}$	$\frac{2}{81}$	$\frac{2}{81}$	$\frac{1}{81}$
$\mathbf{X}_{12}$	2	2	2	2	1	1	1	1	1	1	1	1	0	0	0	0
$\mathbf{X}_{23}$	2	2	1	1	1	1	0	0	2	2	1	1	1	1	0	0
$\mathbf{X}_{34}$	2	1	1	0	2	1	1	0	2	1	1	0	2	1	1	0
$\mathbf{X}_{12} + \mathbf{X}_{23}$	4	4	3	3	2	2	1	1	3	3	2	2	1	1	0	0
$\mathbf{X}_{12} + \mathbf{X}_{34}$	4	3	3	2	3	2	2	1	3	2	2	1	2	1	1	0

Using this table, we can compute the probabilities of interest.
(a) (i) $\mathbb{P}[\mathbf{X}_{12} \geq 2] = \frac{36}{81} = \frac{4}{9}$. (ii) $\mathbb{P}[\mathbf{X}_{12} + \mathbf{X}_{23} \geq 2] = \frac{66}{81} = \frac{22}{27}$. (iii) $\mathbb{P}[\mathbf{X}_{12} + \mathbf{X}_{34} \geq 2] = \frac{72}{81} = \frac{8}{9}$.
(b) (i) $\mathbb{P}[\mathbf{X}_{12} \geq 2] = \frac{4}{9}$; $\mathbb{P}[\mathbf{X}_{23} \geq 2] = \frac{4}{9}$; $\mathbb{P}[\mathbf{X}_{12} \geq 2 \cap \mathbf{X}_{23} \geq 2] = \frac{24}{81} \neq \frac{4}{9} \times \frac{4}{9}$. Not independent.
(ii) $\mathbb{P}[\mathbf{X}_{12} \geq 2] = \frac{4}{9}$; $\mathbb{P}[\mathbf{X}_{34} \geq 2] = \frac{4}{9}$; $\mathbb{P}[\mathbf{X}_{12} \geq 2 \cap \mathbf{X}_{34} \geq 2] = \frac{16}{81} = \frac{4}{9} \times \frac{4}{9}$. Independent.

Pop Quiz 18.3. The shaded upper-left to lower-right diagonals as shown in the probability space for $\mathbf{X} = 9$ contain all the outcomes with a particular value of $\mathbf{X}$. The probability is the number of outcomes in the diagonal divided by 36 (table below). Simplifying the fractions gives the answer.

x	2	3	4	5	6	7	8	9	10	11	12
$P_{\mathbf{X}}(x)$	$\frac{1}{36}$	$\frac{2}{36}$	$\frac{3}{36}$	$\frac{4}{36}$	$\frac{5}{36}$	$\frac{6}{36}$	$\frac{5}{36}$	$\frac{4}{36}$	$\frac{3}{36}$	$\frac{2}{36}$	$\frac{1}{36}$

Exercise 18.4. A is a normalizing constant for the PDF, which ensures that the PDF sums to 1.
(a) The PDF must sum to 1, $\sum_x P_{\mathbf{X}}(x) = 1$. Here, $\sum_{x=1}^{10} Ax = 1 \to 55A = 1$ or $A = 1/55$.
(b) $\mathbb{P}[\mathbf{X} \geq 5] = \frac{1}{55}\sum_{x=5}^{10} x = 45/55 = 9/11$.

Pop Quiz 18.5. The outcome-probabilities in the underlying probability space sum to 1. Every outcome is represented once in the joint probabilities, so the sum of the joint probabilities is 1.

Summing column sums just sums all the joint probabilities. So the column sums add to 1. Similarly for the row sums.

Pop Quiz 18.6. Yes. The first 5 coin tosses are one experiment; the second 5 tosses are another; and, the 2 dice rolls are a third. $\mathbf{X}$ depends only on the first experiment, $\mathbf{Y}$ only on the 2nd and 3rd experiments (unrelated to the 1st).

Exercise 18.7.
(a) Start with the probability space and construct the random variables, as shown on the right.

	Sample Space Ω							
ω	HHH	HHT	HTH	HTT	THH	THT	TTH	TTT
$P(\omega)$	1/27	2/27	2/27	4/27	2/27	4/27	4/27	8/27
$\mathbf{X}(\omega)$	3	2	2	1	2	1	1	0
$\mathbf{Y}(\omega)$	1	1	0	0	1	0	0	0
$\mathbf{X}(\omega) + \mathbf{Y}(\omega)$	4	3	2	1	3	1	1	0

We use the probability space to derive the joint PDF and the marginals shown on the right. We shaded the event $\mathbf{X}+\mathbf{Y} \geq 2$, from which $\mathbb{P}[\mathbf{X}+\mathbf{Y} \geq 2] = \frac{7}{27}$. The event $\mathbf{X} \leq 2 \cap \mathbf{X} + \mathbf{Y} \geq 2$ has its probabilities in red. The conditional probability is the ratio (red sum)/(shaded sum) $= \frac{6}{7}$.

$P_{\mathbf{XY}}(x,y)$		$\mathbf{X}$				$P_{\mathbf{Y}}$
		0	1	2	3	
$\mathbf{Y}$	0	8/27	12/27	2/27	0	**22/27**
	1	0	0	4/27	1/27	**5/27**
$P_{\mathbf{X}}$		**8/27**	**12/27**	**6/27**	**1/27**	

(b) In each case, we give the joint PDF and the joint PDF obtained from the product of the marginals. If the two match, the random variables are independent. Otherwise they are not.

(i)

$P_{\mathbf{X}_{12}\mathbf{X}_{23}}$

$\mathbf{X}_{23}$ \ $\mathbf{X}_{12}$	0	1	2	
0	$\frac{3}{81}$	$\frac{6}{81}$	0	$\frac{1}{9}$
1	$\frac{6}{81}$	$\frac{18}{81}$	$\frac{12}{81}$	$\frac{4}{9}$
2	0	$\frac{12}{81}$	$\frac{24}{81}$	$\frac{4}{9}$
	$\frac{1}{9}$	$\frac{4}{9}$	$\frac{4}{9}$	

$P_{\mathbf{X}_{12}}P_{\mathbf{X}_{23}}$

$\mathbf{X}_{23}$ \ $\mathbf{X}_{12}$	0	1	2	
0	$\frac{1}{81}$	$\frac{4}{81}$	$\frac{4}{81}$	$\frac{1}{9}$
1	$\frac{4}{81}$	$\frac{16}{81}$	$\frac{16}{81}$	$\frac{4}{9}$
2	$\frac{4}{81}$	$\frac{16}{81}$	$\frac{16}{81}$	$\frac{4}{9}$
	$\frac{1}{9}$	$\frac{4}{9}$	$\frac{4}{9}$	

$P_{\mathbf{X}_{12}\mathbf{X}_{23}} \neq P_{\mathbf{X}_{12}}P_{\mathbf{X}_{23}}$, so $\mathbf{X}_{12}$ and $\mathbf{X}_{23}$ are not independent.

(ii)

$P_{\mathbf{X}_{12}\mathbf{X}_{34}}$

$\mathbf{X}_{34}$ \ $\mathbf{X}_{12}$	0	1	2	
0	$\frac{1}{81}$	$\frac{4}{81}$	$\frac{4}{81}$	$\frac{1}{9}$
1	$\frac{4}{81}$	$\frac{16}{81}$	$\frac{16}{81}$	$\frac{4}{9}$
2	$\frac{4}{81}$	$\frac{16}{81}$	$\frac{16}{81}$	$\frac{4}{9}$
	$\frac{1}{9}$	$\frac{4}{9}$	$\frac{4}{9}$	

$P_{\mathbf{X}_{12}}P_{\mathbf{X}_{34}}$

$\mathbf{X}_{34}$ \ $\mathbf{X}_{12}$	0	1	2	
0	$\frac{1}{81}$	$\frac{4}{81}$	$\frac{4}{81}$	$\frac{1}{9}$
1	$\frac{4}{81}$	$\frac{16}{81}$	$\frac{16}{81}$	$\frac{4}{9}$
2	$\frac{4}{81}$	$\frac{16}{81}$	$\frac{16}{81}$	$\frac{4}{9}$
	$\frac{1}{9}$	$\frac{4}{9}$	$\frac{4}{9}$	

In all entries, $P_{\mathbf{X}_{12}\mathbf{X}_{34}} = P_{\mathbf{X}_{12}}P_{\mathbf{X}_{34}}$, so $\mathbf{X}_{12}$ and $\mathbf{X}_{34}$ are independent. No surprise because the first 2 coin tosses and the last 2 coin tosses are unrelated experiments.

(iii)

$P_{\mathbf{X}_{12}^2\mathbf{X}_{34}^2}$

$\mathbf{X}_{34}^2$ \ $\mathbf{X}_{12}^2$	0	1	4	
0	$\frac{1}{81}$	$\frac{4}{81}$	$\frac{4}{81}$	$\frac{1}{9}$
1	$\frac{4}{81}$	$\frac{16}{81}$	$\frac{16}{81}$	$\frac{4}{9}$
4	$\frac{4}{81}$	$\frac{16}{81}$	$\frac{16}{81}$	$\frac{4}{9}$
	$\frac{1}{9}$	$\frac{4}{9}$	$\frac{4}{9}$	

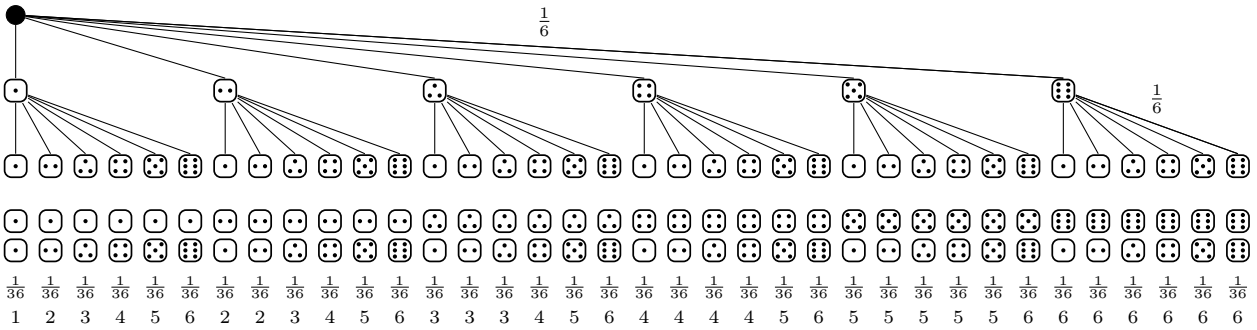
$P_{\mathbf{X}_{12}^2}P_{\mathbf{X}_{34}^2}$

$\mathbf{X}_{34}^2$ \ $\mathbf{X}_{12}^2$	0	1	4	
0	$\frac{1}{81}$	$\frac{4}{81}$	$\frac{4}{81}$	$\frac{1}{9}$
1	$\frac{4}{81}$	$\frac{16}{81}$	$\frac{16}{81}$	$\frac{4}{9}$
4	$\frac{4}{81}$	$\frac{16}{81}$	$\frac{16}{81}$	$\frac{4}{9}$
	$\frac{1}{9}$	$\frac{4}{9}$	$\frac{4}{9}$	

No surprise. If two random variables have nothing to do with each other (are independent) then functions of the random variables will also be unrelated.

(c) $\sum_x \sum_y P_{\mathbf{X}}(x)P_{\mathbf{Y}}(y) = \sum_x P_{\mathbf{X}}(x) \sum_y P_{\mathbf{Y}}(y)$. Each individual sum is 1, so the product is 1.

Exercise 18.8. We reproduce the outcome tree from Exercise 15.2. Below each outcome in the outcome-tree, is its probability and the value the maximum (the random variable).



(a)

x	1	2	3	4	5	6
$P_{\mathbf{X}}(x)$	$\frac{1}{36}$	$\frac{3}{36}$	$\frac{5}{36}$	$\frac{7}{36}$	$\frac{9}{36}$	$\frac{11}{36}$

(b) We only give the CDF at the values with positive PDF. The PDF can be computed from jumps in the CDF.

x	1	2	3	4	5	6
$F_{\mathbf{X}}(x)$	$\frac{1}{36}$	$\frac{4}{36}$	$\frac{9}{36}$	$\frac{16}{36}$	$\frac{25}{36}$	$\frac{36}{36}$

(c) Consider n dice values $\mathbf{X}_1, \ldots, \mathbf{X}_n$. In the problem, n is 10. Note:

$$\max(\mathbf{X}_1, \ldots, \mathbf{X}_n) \le x \quad \leftrightarrow \quad \mathbf{X}_1 \le x \text{ AND } \mathbf{X}_2 \le x \text{ AND } \cdots \text{ AND } \mathbf{X}_n \le x$$

The outcomes in the first event are the same as the outcomes in the second. That means,

$$\mathbb{P}[\max(\mathbf{X}_1, \ldots, \mathbf{X}_n) \le x] = \mathbb{P}[\mathbf{X}_1 \le x \text{ AND } \mathbf{X}_2 \le x \text{ AND } \cdots \text{ AND } \mathbf{X}_n \le x].$$

Since $\mathbf{X}_1, \ldots, \mathbf{X}_n$ are independent, the RHS is a product of probabilities. Using $\mathbb{P}[\mathbf{X}_i \le x] = x/6$ for $x \in \{1, \ldots, 6\}$,

$$\mathbb{P}[\max(\mathbf{X}_1, \ldots, \mathbf{X}_n) \le x] = F_{\mathbf{X}}(x) = (x/6)^n .$$

The jumps in $F_{\mathbf{X}}$ give us the PDF $P_{\mathbf{X}}$,

$$P_{\mathbf{X}}(x) = F_{\mathbf{X}}(x) - F_{\mathbf{X}}(x-1) = (x^n - (x-1)^n)/6^n.$$

Pop Quiz 18.9.

(a) Since I show you the smaller number half the time, you will be wrong half the time.

(b) Using the law of total probability for the two cases you say smaller or larger,

$$\mathbb{P}[\text{you win}] \;=\; \mathbb{P}[\text{you win} \mid \text{smaller}]\mathbb{P}[\text{smaller}] + \mathbb{P}[\text{you win} \mid \text{larger}]\mathbb{P}[\text{larger}] \;=\; \tfrac{1}{2} \times \tfrac{1}{2} + \tfrac{1}{2} \times \tfrac{1}{2} \;=\; \tfrac{1}{2}.$$

(c) I choose (3,4). You always say smaller and win half the time.

(d) Yes! See the discussion following the pop quiz in the text and Exercise 18.10.

Exercise 18.10.

(a)
$$\begin{aligned} \mathbb{P}[\text{you win}] &= \mathbb{P}[\mathcal{E}] \cdot \mathbb{P}[\text{you win} \mid \mathcal{E}] + \mathbb{P}[\,\overline{\mathcal{E}}\,] \cdot \mathbb{P}[\text{you win} \mid \overline{\mathcal{E}}\,] && \text{(total probability)} \\ &= \mathbb{P}[\mathcal{E}] \cdot 1 + (1 - \mathbb{P}[\mathcal{E}]) \cdot \tfrac{1}{2} && \text{(if } \mathcal{E} \text{ occurs you win; if not you win half the time)} \\ &= \tfrac{1}{2} + \tfrac{1}{2}\mathbb{P}[\mathcal{E}] \;\ge\; \tfrac{2}{3} && \text{(algebra and } P(\mathcal{E}) = (H-L)/3 \ge 1/3) \end{aligned}$$

For last step, $\mathcal{E}$ contains $H - L$ values of $\mathbf{X}$ in the interval (L, H) each with probability 1/3.

(b) Let the PDF of $\mathbf{X}$ be p_1, p_2, p_3 with minimum $p_i < \frac{1}{3}$. I now choose $L = i$ and $H = i + 1$. Then $\mathbb{P}[\mathcal{E}] = p_i$. And so, $\mathbb{P}[\text{you win}] = \frac{1}{2} + \frac{1}{2}\mathbb{P}[\mathcal{E}] = \frac{1}{2} + \frac{1}{2}p_i < \frac{1}{2} + \frac{1}{2} \times \frac{1}{3} = \frac{2}{3}$.

Pop Quiz 18.11.

(a) Binomial. A kid is a "trial". A "success" is a boy. Children are independent and the chances of a boy are the same for each kid, approximately 1/2. We have 10 independent trials with success probability 1/2.

(b) Not Binomial. Again a trial is a child, but the number of trials is not some fixed number.

(c) Not Binomial. This is tricky. The 10 trials are each kid in the team. A success is a boy. The success probability on the first trial is 10/30. If the first trial succeeds, the second trial success probability is 9/29 (sampling without replacement). Trials are not independent and the success probabilities change depending on the outcomes.

Exercise 18.12.

(a) $\mathbf{X}_i = 1$ if you get question i correct; $\mathbb{P}[\mathbf{X}_i = 1] = \frac{1}{5}$. The number of correct answers is $\mathbf{X} = \mathbf{X}_1 + \cdots + \mathbf{X}_{20}$, a Binomial with $n = 20$ and $p = \frac{1}{5}$. We want $\mathbb{P}[\mathbf{X} \geq 10] = \mathbb{P}[\mathbf{X} \geq 10] = \sum_{k=10}^{20} \binom{20}{k} \left(\frac{1}{5}\right)^k \left(\frac{4}{5}\right)^{20-k} \approx 0.0026$.

(b) The outcomes $AAAA$ (A wins four in a row) or $BBBB$ each have probability $(\frac{1}{2})^4 = \frac{1}{16}$. So $\mathbb{P}[4 \text{ games}] = \frac{1}{8}$.

If the series ends in 5 games, there are two cases: A wins or B wins. Each has the same probability. If A wins, the series looks like $xxxxA$, and A must win 3 games in the first 4. We have a Binomial with $n = 4$ and $p = \frac{1}{2}$. $\mathbb{P}[k = 3] = \binom{4}{3}(\frac{1}{2})^3(\frac{1}{2})^1 = \frac{4}{16}$. Therefore $\mathbb{P}[\text{A wins in 5}] = \frac{4}{16} \times \frac{1}{2}$ (the last $\frac{1}{2}$ is because A wins the last game). So,

$$\mathbb{P}[5 \text{ games}] = \mathbb{P}[\text{A wins in 5}] + \mathbb{P}[\text{B wins in 5}] = \frac{4}{16}.$$

Similarly, A wins in 6 games with probability $\binom{5}{3}(\frac{1}{2})^3(\frac{1}{2})^2 \times \frac{1}{2}$, and

$$\mathbb{P}[6 \text{ games}] = \mathbb{P}[\text{A wins in 6}] + \mathbb{P}[\text{B wins in 6}] = \frac{10}{32} = \frac{5}{16}.$$

Lastly, A wins in 7 games with probability $\binom{6}{3}(\frac{1}{2})^3(\frac{1}{2})^3 \times \frac{1}{2}$, and

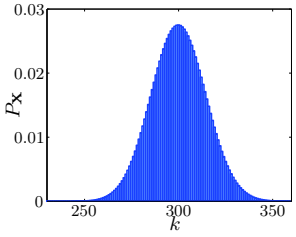
$$\mathbb{P}[7 \text{ games}] = \mathbb{P}[\text{A wins in 7}] + \mathbb{P}[\text{B wins in 7}] = \frac{20}{64} = \frac{5}{16}.$$

(c) There are $\binom{100}{20} \times \binom{80}{30} \times 4^{50}$ sequences with 20 ones and 30 fours ($\binom{100}{20}$ ways to choose the 1s; of the remaining 80 positions there are $\binom{80}{30}$ ways to choose the 4s; each of the remaining 50 slots can be picked in 4 ways for 4^{50}). The probability of each sequence is $(\frac{1}{6})^{100}$, so

$$\mathbb{P}[20 \text{ ones and } 30 \text{ fours}] = \binom{100}{20} \times \binom{80}{30} \times 4^{50} \times \left(\frac{1}{6}\right)^{100} \approx 9.226 \times 10^{-6}.$$

Here is another derivation of the multinomial distribution. The number of sequences with k_1 objects of type 1, k_2 of type 2 and k_3 of type 3 is $\binom{k_1+k_2+k_3}{k_1,k_2,k_3}$. There are $\binom{100}{20,30,50}$ sequences with 20-ones, 30-fours, and 50-other-values (three types). Each 1 and 4 have probability 1/6 and each non-1-or-4 has probability 4/6. The probability of each such sequence is $(\frac{1}{6})^{20} \cdot (\frac{1}{6})^{30} \cdot (\frac{4}{6})^{50}$ and we recover the same result from:

$$\mathbb{P}[20 \text{ ones and } 30 \text{ fours}] = \binom{100}{20,30,50}(\tfrac{1}{6})^{20} \cdot (\tfrac{1}{6})^{30} \cdot (\tfrac{4}{6})^{50}$$



(d) The challenge is to evaluate small numbers, like $(1-p)^n$. It is numerically more stable to compute the $\log P_{\mathbf{X}}$. So, $\log P_{\mathbf{X}}(0) = n \log(1-p)$. Having computed $\log P_{\mathbf{X}}(k-1)$, you can use the following update to get $\log P_{\mathbf{X}}(k)$,

$$\log P_{\mathbf{X}}(k) \leftarrow \log P_{\mathbf{X}}(k-1) + \log\left(\frac{p(n-k+1)}{(1-p)k}\right).$$

Exercise 18.13.

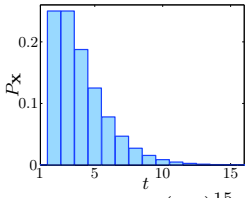
(a) A boy is "success" and the probability of success is 1/2. Let $\mathbf{X}$ be the number of trials till success. We want $\mathbb{P}[\mathbf{X} \geq 5]$ where $P_{\mathbf{X}}(t) = \beta(1-p)^t$ with $p = 1/2$ and $\beta = p/(1-p) = 1$

$$\mathbb{P}[\mathbf{X} \geq 5] = \sum_{t=5}^{\infty} \left(\frac{1}{2}\right)^t = \left(\frac{1}{2}\right)^5 \times \frac{1}{1-1/2} = \frac{1}{16}.$$

Alternatively, observe that $\mathbf{X} \geq 5$ if and only if the first 4 children are girls, which happens with probability $(\frac{1}{2})^4$.

(b) Your wait for two successes is t when the tth trial is a success and there is one success in trials $1, \ldots, t-1$. There are $t-1$ sequences with one success in the first $t-1$. The probability of each such sequence is $p^2(1-p)^{t-2}$ (two successes and $t-2$ failures), where the success probability $p = 1/2$. Therefore,

$$\mathbb{P}[\mathbf{X} = t] = P_{\mathbf{X}}(t) = (t-1)p^2(1-p)^{t-2} = \beta^2(t-1)(1-p)^t.$$



(c) (i) You fail to send any packet with probability $(0.1)^{15}$, so the probability of at least 1 success is $1 - (0.1)^{15}$.

(ii) If you need at least 15 transmissions, then in the first 14 transmissions at most 11 are successful. Let $\mathbf{X}$ be the number of successful transmissions in the first 14 trials, $\mathbf{X} \sim B(14, 0.9)$. We want $\mathbb{P}[\mathbf{X} \leq 11]$,

$$\mathbb{P}[\mathbf{X} \leq 11] = \sum_{k=0}^{11} \binom{14}{k} (0.9)^k (0.1)^{14-k} \approx 0.16$$

.

Chapter 19

Exercise 19.1. The discussion after the exercise suggests the values you should observe for the Monte Carlo averages. (a) Average dice roll is about 3.5. (b) 10 coin tosses yields on average 5 heads. (c) 7.5mm of rain per day on average. (d) The gamblers lose on average $52.63.

Pop Quiz 19.2. For the two coin tosses: $\sum_{\omega\in\Omega} \mathbf{X}(\omega)\cdot P(\omega) = 2\cdot\frac{1}{4}+1\cdot\frac{1}{4}+1\cdot\frac{1}{4}+0\cdot\frac{1}{4}=1$. More generally, consider all outcomes ω with $\mathbf{X}(\omega)=x$. The contribution of these outcomes is

$$x\cdot(\text{sum of probabilites for the outcomes whose value is } x) = xP_{\mathbf{X}}(x),$$

which is one of the terms in $\sum_{x\in\mathbf{X}(\Omega)} xP_{\mathbf{X}}(x)$, which means the two sums are equal. Here is a formal mathematical proof. Let $\mathbf{X}(\Omega)=\{x_1,x_2,\ldots,x_M\}$ be the possible values for x. Since we have entered a proof, we know you are on high alert and take this as an opportunity to introduce a useful notation, the *Boolean indicator function* $[\![A]\!]$ which is 1 when A is TRUE and 0 when FALSE. We are going to use $[\![\cdot]\!]$ to express $P_{\mathbf{X}}(x)$ as a convenient summation

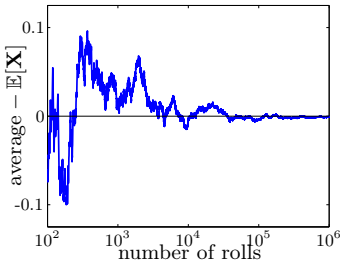
$$P_{\mathbf{X}}(x) \;=\; \mathbb{P}[\mathbf{X}=x] \;=\; \sum_{\omega:\mathbf{X}(\omega)=x} P(\omega) \;=\; \sum_{\omega\in\Omega} P(\omega)\,[\![\mathbf{X}(\omega)=x]\!]\,.$$

The first sum is from the definition of $\mathbb{P}[\mathbf{X}=x]$: add the probabilities of all outcomes for which $\mathbf{X}(\omega)=x$. The second sum is over *all* ω; the Boolean indicator ensures that the summand is 0 when $\mathbf{X}(\omega)\neq x$. So, the second sum also adds the probabilities only when $\mathbf{X}(\omega)=x$. Thus,

$$\begin{aligned}
\sum_{x\in\mathbf{X}(\Omega)} x\cdot P_{\mathbf{X}}(x) \;&=\; \sum_{x\in\mathbf{X}(\Omega)} x \sum_{\omega\in\Omega} P(\omega)\,[\![\mathbf{X}(\omega)=x]\!] \\
&\overset{(a)}{=} \sum_{x\in\mathbf{X}(\Omega)}\sum_{\omega\in\Omega} P(\omega)x\,[\![\mathbf{X}(\omega)=x]\!] && \text{pull } x \text{ inside } \textstyle\sum_{\omega} \\
&\overset{(b)}{=} \sum_{x\in\mathbf{X}(\Omega)}\sum_{\omega\in\Omega} P(\omega)\mathbf{X}(\omega)\,[\![\mathbf{X}(\omega)=x]\!] && \text{replace } x \text{ with } \mathbf{X}(\omega) \\
&\overset{(*)}{=} \sum_{\omega\in\Omega}\sum_{x\in\mathbf{X}(\Omega)} P(\omega)\mathbf{X}(\omega)\,[\![\mathbf{X}(\omega)=x]\!] && \text{reverse order of sums} \\
&\overset{(c)}{=} \sum_{\omega\in\Omega} P(\omega)\mathbf{X}(\omega) \sum_{x\in\mathbf{X}(\Omega)} [\![\mathbf{X}(\omega)=x]\!] && \text{pull } P(\omega)\mathbf{X}(\omega) \text{ outside } \textstyle\sum_{x} \\
&\overset{(d)}{=} \sum_{\omega\in\Omega} P(\omega)\mathbf{X}(\omega). && \textstyle\sum_{x} [\![\mathbf{X}(\omega)=x]\!] = 1
\end{aligned}$$

(a) is because x is a constant w.r.t. ω; (b) is because when the summand is non-zero, $x=\mathbf{X}(\omega)$; $(*)$ is a technical. You can always reverse the order of summation for finite sums;[1] (c) is because $\mathbf{X}(\omega)$ is a constant w.r.t. x as summation index; (d) is because only one term contributes to the sum, the unique x which equals $\mathbf{X}(\omega)$.

Pop Quiz 19.3.



Pop Quiz 19.4. We show the probability space with the random variables below.

[1] In general you can't reverse order of summation in infinite sums unless the sums are absolutely convergent. The expected value is defined only when $\sum_{\omega\in\Omega} P(\omega)|\mathbf{X}(\omega)| < \infty$ (absolute convergence) and then you can add the terms in any order.

Probability Space

Die 2 Value \ Die 1 Value	⚀	⚁	⚂	⚃	⚄	⚅
⚀	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$
⚁	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$
⚂	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$
⚃	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$
⚄	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$
⚅	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$

$\mathbf{X} = \mathbf{D}_1 - \mathbf{D}_2$

Die 2 Value \ Die 1 Value	⚀	⚁	⚂	⚃	⚄	⚅
⚀	−5	−4	−3	−2	−1	0
⚁	−4	−3	−2	−1	0	1
⚂	−3	−2	−1	0	1	2
⚃	−2	−1	0	1	2	3
⚄	−1	0	1	2	3	4
⚅	0	1	2	3	4	5

$\mathbf{X} = |\mathbf{D}_1 - \mathbf{D}_2|$

Die 2 Value \ Die 1 Value	⚀	⚁	⚂	⚃	⚄	⚅
⚀	5	4	3	2	1	0
⚁	4	3	2	1	0	1
⚂	3	2	1	0	1	2
⚃	2	1	0	1	2	3
⚄	1	0	1	2	3	4
⚅	0	1	2	3	4	5

To compute expectation, weight each random-variable value by its probability and add. For $\mathbf{D}_1 - \mathbf{D}_2$, every positive value cancels a corresponding negative value, so $\mathbb{E}[\mathbf{D}_1 - \mathbf{D}_2] = 0$. The cancelation does not occur for $\mathbb{E}[|\mathbf{D}_1 - \mathbf{D}_2|]$,

$$\mathbb{E}[|\mathbf{D}_1 - \mathbf{D}_2|] = \tfrac{1}{36} \times 2 \times (5 \times 1 + 4 \times 2 + 3 \times 3 + 2 \times 4 + 1 \times 5) = \tfrac{70}{36} = 1\tfrac{17}{18}.$$

We argued from the sample space. You can get these same results by first computing the PDF.

Exercise 19.5.

(a) Directly computing the expected value from the sample space, (Pop Quiz 19.2),

$$\mathbb{E}[\mathbf{X}] = \sum_{\omega\in\Omega} \mathbf{X}(\omega)P(\omega) = \sum_{\omega\in\Omega} \mathbf{X}(\omega)\frac{1}{|\Omega|} = \frac{1}{|\Omega|}\sum_{\omega\in\Omega} \mathbf{X}(\omega).$$

For two dice, the probability space is uniform, so the expected sum is:

$$\mathbb{E}[\mathbf{X}] = \tfrac{\text{sum}(2,\ldots,7)+\text{sum}(3,\ldots,8)+\text{sum}(4,\ldots,9)+\cdots+\text{sum}(7,\ldots,12)}{36} = \tfrac{252}{36} = 7.$$

(b) This is easiest to prove directly from the sample space (Pop Quiz 19.2):

$$\mathbb{E}[\mathbf{Y}] = \sum_{\omega\in\Omega} P(\omega)\mathbf{Y}(\omega) = \sum_{\omega\in\Omega} P(\omega)(a\mathbf{X}(\omega)+b) = a\sum_{\omega\in\Omega} P(\omega)\mathbf{X}(\omega) + b\sum_{\omega\in\Omega} P(\omega) = a\mathbb{E}[\mathbf{X}] + b.$$

(c) Again, it's easiest to prove directly from the sample space, with $\mathbf{Y}(\omega) = \mathbf{X}_1(\omega) + \mathbf{X}_2(\omega)$.

$$\mathbb{E}[\mathbf{Y}] = \sum_{\omega\in\Omega} P(\omega)\mathbf{Y}(\omega) = \sum_{\omega\in\Omega} P(\omega)(\mathbf{X}_1(\omega)+\mathbf{X}_2(\omega)) = \sum_{\omega\in\Omega} P(\omega)\mathbf{X}_1(\omega) + \sum_{\omega\in\Omega} P(\omega)\mathbf{X}_2(\omega) = \mathbb{E}[\mathbf{X}_1] + \mathbb{E}[\mathbf{X}_2].$$

Exercise 19.6.

(a) $n = 20$ and $p = \frac{1}{2}$, so $\mathbb{E}[\mathbf{X}] = np = 10$. The expected number of heads is 10.

(b) $n = 20$ and $p = \frac{1}{5}$, so $\mathbb{E}[\mathbf{X}] = np = 4$. The expected number of correct answers is 4.

(c) $n = 5$. If you hit a region with probability proportional to its area, then $p = 1/100$ (area is proportional to radius squared). So, $\mathbb{E}[\mathbf{X}] = np = 5 \times 1/100 = 1/20$.

(d) $\mathbb{E}[\mathbf{X}(\mathbf{X}-1)] = \sum_{k=0}^{n} k(k-1)\binom{n}{k}p^k(1-p)^{n-k} = \sum_{k=2}^{n} k(k-1)\binom{n}{k}p^k(1-p)^{n-k}$. Observe that

$$k(k-1)\tbinom{n}{k} = \tfrac{k(k-1)n!}{k!(n-k)!} = \tfrac{n!}{(k-2)!(n-k)!} = \tfrac{n(n-1)(n-2)!}{(k-2)!(n-k)!} = n(n-1)\tbinom{n-2}{k-2}.$$

Using this identity in the expression for $\mathbb{E}[\mathbf{X}(\mathbf{X}-1)]$,

$$\begin{aligned}
\mathbb{E}[\mathbf{X}(\mathbf{X}-1)] &= \sum_{k=2}^{n} n(n-1)\tbinom{n-2}{k-2}p^k(1-p)^{n-k} \\
&= n(n-1)p^2\sum_{k=2}^{n}\tbinom{n-2}{k-2}p^{k-2}(1-p)^{n-k} && (n(n-1)p^2 \text{ is a constant}) \\
&= n(n-1)p^2\sum_{\ell=0}^{n-2}\tbinom{n-2}{\ell}p^{\ell}(1-p)^{n-2-\ell} && (\text{change index to } \ell = k-2) \\
&= n(n-1)p^2(p+1-p)^{n-2} && (\text{Binomial theorem}) \\
&= n(n-1)p^2 && (p+1-p=1)
\end{aligned}$$

Exercise 19.7.

(a) Hitting the bulls-eye is success. The bulls-eye area is $\frac{1}{100}$th the area of the board, so $p = \frac{1}{100}$. Therefore, the expected number of darts you throw is $\frac{1}{p} = 100$.

(b) A 5-pack contains no EX with probability $0.99^5 \approx 0.95$. So a 5-pack contains an EX (success) with probability $p \approx 0.05$. You expect to buy $\frac{1}{p} \approx 20$ 5-packs to get an EX.

(c) If you pay x, with probability 10^{-7} you win 10^6 and with probability $1 - 10^{-7}$ you lose x, so your expected profit is $10^{-7} \times 10^6 - x(1 - 10^{-7})$. You play if you make a profit so $x < \frac{1}{10}/(1 - 10^{-7}) \approx 10¢$.

(d) (i) We may assume the first child is a boy (the argument is identical if the first is a girl). You are now waiting for a girl with success probability $p = \frac{1}{2}$. Therefore you expect 2 trials to get a girl, for a total of 3.

(ii) You expect to wait 2 trials for the first boy and 2 more for the second for a total of 4 kids. Let's compute this from the PDF for waiting time to 2 successes in Exercise 18.13. Since $p = \frac{1}{2}$, $P_{\mathbf{X}}(t) = (t-1)(\frac{1}{2})^t$,

$$\mathbb{E}[\mathbf{X}] = \sum_{t=1}^{\infty} t(t-1)(\tfrac{1}{2})^t. \qquad (*)$$

We need to compute this infinite sum. Note that the first term in the sum is zero and

$$\tfrac{1}{2}\mathbb{E}[\mathbf{X}] = \sum_{t=1}^{\infty} t(t-1)(\tfrac{1}{2})^{t+1} = \sum_{t=2}^{\infty}(t-1)(t-2)(\tfrac{1}{2})^t. \qquad (**)$$

Subtracting $(**)$ from $(*)$, the LHS is $\mathbb{E}[\mathbf{X}] - \frac{1}{2}\mathbb{E}[\mathbf{X}] = \frac{1}{2}\mathbb{E}[\mathbf{X}]$ and we have:

$$\tfrac{1}{2}\mathbb{E}[\mathbf{X}] = \sum_{t=2}^{\infty}(t(t-1) - (t-1)(t-2))(\tfrac{1}{2})^t = \sum_{t=2}^{\infty} 2(t-1)(\tfrac{1}{2})^t = \sum_{t=2}^{\infty}(t-1)(\tfrac{1}{2})^{t-1}.$$

The last sum is $\sum_{t=1}^{\infty} t(\frac{1}{2})^t$ which equals 2 by Lemma 19.6 on page 281, so we get $\mathbb{E}[\mathbf{X}] = 4$.

Exercise 19.8.

(a) Conditioned on $D_1 + D_2 \geq 4$, there are now 33 outcomes, each having probability $\frac{1}{33}$. So,

$$\mathbb{E}[D_1 + D_2 \mid D_1 + D_2 \geq 4] = \frac{3\times 4 + 4\times 5 + 5\times 6 + 6\times 7 + 5\times 8 + 4\times 9 + 3\times 10 + 2\times 11 + 1\times 12}{33} = \frac{244}{33} \approx 7.4.$$

(b) (i) The relevant outcomes are $\{0, 2, 4, \ldots, 20\}$.

$$\mathbb{P}[\mathbf{X} = 2i \mid \text{even}] = \frac{\mathbb{P}[\mathbf{X} = 2i \cap \text{even}]}{\mathbb{P}[\text{even}]} = \frac{1}{\mathbb{P}[\text{even}]}\tbinom{20}{2i} \cdot (\tfrac{1}{2})^{2i} \cdot (\tfrac{1}{2})^{20-2i} = \frac{1}{2^{20}\mathbb{P}[\text{even}]}\tbinom{20}{2i}.$$

We can compute $\mathbb{P}[\text{even}]$ as a sum over Binomial coefficients:

$$\mathbb{P}[\text{even}] = (\tfrac{1}{2})^{20} \sum_{\text{even } i} \tbinom{20}{i} = (\tfrac{1}{2})^{20} \times 2^{19} = \tfrac{1}{2},$$

where we used $\sum_{\text{even } i} \binom{n}{i} = 2^{n-1}$ (also equals $\sum_{\text{odd } i} \binom{n}{i}$). To see this, the Binomial Theorem gives:

$$\left.\begin{aligned} 2^n &= (1+1)^n &&= \sum_{i=0}^{n}\tbinom{n}{i} = \sum_{\text{even } i}\tbinom{n}{i} + \sum_{\text{odd } i}\tbinom{n}{i} \\ 0 &= (-1+1)^n &&= \sum_{i=0}^{n}\tbinom{n}{i}(-1)^i = \sum_{\text{even } i}\tbinom{n}{i} - \sum_{\text{odd } i}\tbinom{n}{i} \end{aligned}\right\} \text{solve} \to \sum_{\text{even } i}\tbinom{n}{i} = \sum_{\text{odd } i}\tbinom{n}{i} = 2^{n-1}.$$

Now for the conditional expectation:

$$\begin{aligned} \mathbb{E}[\mathbf{X} \mid \text{even}] = \sum_{\text{even } i} i \cdot \mathbb{P}[\mathbf{X} = i \mid \text{even}] &= \sum_{\text{even } i} \frac{i}{2^{20}\mathbb{P}[\text{even}]}\binom{20}{i} \\ &= \frac{1}{2^{19}} \sum_{\text{even } i>0} \frac{20!}{(i-1)!(20-i)!} \\ &= \frac{20}{2^{19}} \sum_{\text{even } i>0} \frac{19!}{(i-1)!(19-(i-1))!} \\ &= \frac{20}{2^{19}} \sum_{\text{even } i>0} \binom{19}{i-1} \\ &= \frac{20}{2^{19}} \sum_{\text{odd } i} \binom{19}{i}. \end{aligned}$$

The last sum is 2^{18} and so $\mathbb{E}[\mathbf{X} \mid \text{even}] = 10$.

(ii) We need to do a similar analysis: $\mathbb{E}[\mathbf{X} \mid \text{at least 8}] = \sum_{i\geq 8} i \cdot \mathbb{P}[\mathbf{X} = i \mid \text{at least 8}]$, where

$$\mathbb{P}[\mathbf{X} = i \mid \text{at least 8}] = \frac{1}{2^{20}\mathbb{P}[\text{at least 8}]}\binom{20}{i},$$

and $\mathbb{P}[\text{at least 8}] = 2^{-20}\sum_{i\geq 8}\binom{20}{i} \approx 0.86841$. Therefore,

$$\mathbb{E}[\mathbf{X} \mid \text{at least 8}] = \frac{1}{2^{20}\mathbb{P}[\text{at least 8}]} \sum_{i\geq 8} i \cdot \binom{20}{i} \approx 10.553.$$

(c) The relevant outcomes are $\{5, 7, 11, 13\}$ each with conditional probability 1/4. So

$$\mathbb{E}[\mathbf{X}^2 \mid \text{prime}] = \tfrac{1}{4}(5^2 + 7^2 + 11^2 + 13^2) = 91.$$

(d) We want $\mathbb{E}[\mathbf{X} \mid \mathbf{X} \geq k+1]$. We need the conditional probability

$$\mathbb{P}[\mathbf{X} = t \mid \mathbf{X} \geq k+1] = \frac{\mathbb{P}[\mathbf{X} = t \cap \mathbf{X} \geq k+1]}{\mathbb{P}[\mathbf{X} \geq k+1]} = \frac{\beta(1-p)^t}{(1-p)^k},$$

Because $\mathbb{P}[\mathbf{X} \geq k+1]$ is the probability to fail on the first k trials which is $(1-p)^k$. Therefore,

$$\mathbb{E}[\mathbf{X} \mid \mathbf{X} \geq k+1] = \frac{\beta}{(1-p)^k} \sum_{t=k+1}^{\infty} t(1-p)^t = \frac{\beta}{(1-p)^k} \sum_{t=1}^{\infty} (t+k)(1-p)^{t+k} = \frac{1}{p} + k.$$

Exercise 19.9. $\mathbb{E}[\mathbf{X} \mid \mathbf{X} \geq 25] = \sum_{x \geq 25} x P_{\mathbf{X}}(x) / \mathbb{P}[\mathbf{X} \geq 25]$ and $\mathbb{E}[\mathbf{X} \mid \mathbf{X} \geq 17] = \sum_{x \geq 17} x P_{\mathbf{X}}(x) / \mathbb{P}[\mathbf{X} \geq 17]$. So,

$$\mathbb{E}[\mathbf{X} \mid \mathbf{X} \geq 25] - \mathbb{E}[\mathbf{X} \mid \mathbf{X} \geq 17] = \frac{\left(\mathbb{P}[\mathbf{X} \geq 17] \sum_{x \geq 25} x P_{\mathbf{X}}(x) - \mathbb{P}[\mathbf{X} \geq 25] \sum_{x \geq 17} x P_{\mathbf{X}}(x)\right)}{\mathbb{P}[\mathbf{X} \geq 25]\mathbb{P}[\mathbf{X} \geq 17]}.$$

We show that the numerator is positive: Let $P_1 = \mathbb{P}[17 \leq \mathbf{X} < 25]$; $P_1 = \mathbb{P}[\mathbf{X} \geq 25]$; $S_1 = \sum_{x=17}^{24} x P_{\mathbf{X}}(x)$; and, $S_2 = \sum_{x \geq 25} x P_{\mathbf{X}}(x)$. Note: $S_2 > 25P_2$ and $S_1 < 24P_1$. We have,

$$\begin{aligned} & \mathbb{P}[\mathbf{X} \geq 17] \sum_{x \geq 25} x P_{\mathbf{X}}(x) - \mathbb{P}[\mathbf{X} \geq 25] \sum_{x \geq 17} x P_{\mathbf{X}}(x) \\ = \; & (P_1 + P_2) S_2 - P_2 (S_1 + S_2) \\ = \; & P_1 S_2 - P_2 S_1 > 25 P_1 P_2 - 24 P_2 P_1 > 0. \end{aligned}$$

Pop Quiz 19.10.
(a) Definition of expected value.
(b) By the law of total probability, $\mathbb{P}[\mathbf{X} = x] = \mathbb{P}[A]\mathbb{P}[\mathbf{X} = x \mid A] + \mathbb{P}[\overline{A}]\mathbb{P}[\mathbf{X} = x \mid \overline{A}]$.
(c) $\mathbb{P}[A]$ and $\mathbb{P}[\overline{A}]$ are independent of x and can be pulled out of the sum (constant rule).
(d) Definition of the conditional expectation.

Exercise 19.11.
(a) $\mathbb{E}[\mathbf{X}] = \mathbb{E}[\mathbf{X} \mid \text{fair}]\mathbb{P}[\text{fair}] + \mathbb{E}[\mathbf{X} \mid \text{biased}]\mathbb{P}[\text{biased}]$, where $\mathbb{P}[\text{fair}] = \frac{m}{m+k}$ and $\mathbb{P}[\text{biased}] = \frac{k}{m+k}$.
  (i) $\mathbb{E}[\mathbf{X}] = \frac{1}{2} n \times m/(m+k) + n \times k/(m+k) = n(\frac{1}{2}m + k)/(m+k)$.
  (ii) $\mathbb{E}[\mathbf{X}] = 2 \times m/(m+k) + 1 \times k/(m+k) = (2m+k)/(m+k)$.

(b) $\mathbb{E}[\mathbf{X}] = \mathbb{E}[\mathbf{X} \mid \text{B}]\mathbb{P}[\text{B}] + \mathbb{E}[\mathbf{X} \mid \text{G}]\mathbb{P}[\text{G}]$ (the two cases are the first child is B and the first child is G). Let p be the probability of a boy. If the first child is B, you are waiting for a G, so the expected wait is 1 (for the boy you already have) plus the expected wait to the girl which is $1/(1-p)$, $\mathbb{E}[\mathbf{X} \mid \text{B}] = 1 + 1/(1-p)$. If the first child is G, you are waiting for a B, so the expected wait is 1 (for the girl you already have) plus the expected wait to the boy which is $1/p$, $\mathbb{E}[\mathbf{X} \mid \text{G}] = 1 + 1/p$. So,

$$\mathbb{E}[\mathbf{X}] = \left(1 + \tfrac{1}{1-p}\right) p + \left(1 + \tfrac{1}{p}\right)(1-p) = \tfrac{1}{p(1-p)} - 1.$$

When $p = \frac{1}{2}$, you expect to 3 kids till you get a boy and a girl.

(c) Since girls are twice as likely as boys, $p = \frac{1}{3}$ and the expected number of children is $3\frac{1}{2}$.

(d) As with 3 dice. Let $\mathbf{X}_1$ be the first die, and $\mathbf{X}_3$ the sum of the remaining 3 dice. The dice are independent, so $\mathbb{P}[\mathbf{X}_3 = x_3 \mid \mathbf{X}_1 = x_1] = P_{\mathbf{X}_3}(x_3)$. By the law of total probability,

$$\mathbb{E}[\mathbf{X}] = \sum_{i=1}^{6} \mathbb{E}[\mathbf{X}_3 \mid \mathbf{X}_1 = i]\mathbb{P}[\mathbf{X}_1 = i].$$

Since $\mathbb{E}[\mathbf{X} \mid \mathbf{X}_1 = i] = \sum_{x_3} (i + x_3) P_{\mathbf{X}_3}(x_3) = i + \mathbb{E}[\mathbf{X}_3] = i + 10.5$, we have

$$\tfrac{1}{6}\mathbb{E}[\mathbf{X}] = \sum_{i=1}^{6} (i + 10.5) = \tfrac{1}{6}\mathbb{E}[\mathbf{X}] = \sum_{i=1}^{6} gi + \tfrac{1}{6}\mathbb{E}[\mathbf{X}] = \sum_{i=1}^{6} 10.5 = 3.5 + 10.5 = 14.$$

The expected sum of 4 dice is 4 times the expexted value of one die.

(e) $\mathbb{E}[\mathbf{X}] = \mathbb{E}[\mathbf{X} \mid \text{H}]\mathbb{P}[\text{H}] + \mathbb{E}[\mathbf{X} \mid \text{T}]\mathbb{P}[\text{T}] = 7p + 10.5(1-p) = 10.5 - 3.5p$, where $p = \mathbb{P}[\text{H}]$.

(f) Let $\mathbf{Y}$ be the waiting time. $\mathbf{X} = \mathbf{Y}^2$. $\mathbb{E}[\mathbf{Y}^2] = \mathbb{E}[\mathbf{Y}^2 \mid \text{success}]\mathbb{P}[\text{success}] + \mathbb{E}[\mathbf{Y}^2 \mid \text{fail}]\mathbb{P}[\text{fail}]$. In case of success, $\mathbf{Y}^2 = 1$. In case of failure, the process restarts and $\mathbf{Y}^2 = (1 + \mathbf{Z})^2$, where $\mathbf{Z}$ is the waiting time to success. So,

$$\mathbb{E}[\mathbf{Y}^2] = p + (1-p)\mathbb{E}[(1+\mathbf{Z})^2] = p + (1-p) + 2(1-p)\mathbb{E}[\mathbf{Z}] + (1-p)\mathbb{E}[\mathbf{Z}^2].$$

Since $\mathbb{E}[\mathbf{Y}^2] = \mathbb{E}[\mathbf{Z}^2]$, we can solve for $\mathbb{E}[\mathbf{Y}^2]$ to get $\mathbb{E}[\mathbf{Y}^2] = (2-p)/p^2$. This problem is trickier than it appeared.

Exercise 19.12.
(a) For $n > 1$, let A_i be the event the pivot is ith smallest, $i = 1, \ldots, n$. $\mathbb{P}[A_i] = \frac{1}{n}$. By total probability,

$$T_n = \mathbb{E}[\text{runtime}(n)] = \sum_{i=1}^{n} \mathbb{E}[\text{runtime} \mid A_i]\mathbb{P}[A_i] = \tfrac{1}{n} \sum_{i=1}^{n} \mathbb{E}[\text{runtime} \mid A_i].$$

Given A_i, the runtime is $n+1$ plus the time on the left list of size $i-1$ plus the time on the right list of size $n-i$.

$$\text{runtime given } A_i = n + 1 + \text{runtime}(i-1) + \text{runtime}(n-i).$$

Taking the expection, $\mathbb{E}[\text{runtime} \mid A_i] = (n+1) + T_{i-1} + T_{n-i}$. Therefore,

$$T_n = \tfrac{1}{n}\sum_{i=1}^{n}[(n+1) + T_{i-1} + T_{n-i}] = n+1+\tfrac{1}{n}(T_0 + T_{n-1} + T_1 + T_{n-2} + \cdots + T_{n-2} + T_1 + T_{n-1} + T_0).$$

The sum contains two copies of each T_i. Since T_0=0, we have $T_n = n+1+\frac{2}{n}\sum_{i=1}^{n-1} T_i$.

(b) Using (a), $T_2 = 3 + \frac{2}{2}T_1 = 4$. Rewriting the recursion in (a), $nT_n = n(n+1) + 2\sum_{i=1}^{n-1} T_i$.

Similarly, for $n > 2$, we have $(n-1)T_{n-1} = (n-1)n + 2\sum_{i=1}^{n-2} T_i$.

Subtracting the latter equation from the former equation gives,

$$nT_n - (n-1)T_{n-1} = n(n+1) - (n-1)n + 2\sum_{i=1}^{n-1} T_i - 2\sum_{i=1}^{n-2} T_i = 2n + 2T_{n-1}.$$

Rearranging gives $nT_n = (n+1)T_{n-1} + 2n$. Dividing both sides by n gives the desired result.

(c) Deriving the upper bound is interesting. Given the bound, proving it by induction is good practice. We need two facts: $1 + x \le e^x$; $e^{H_n} \ge n+1$ (which we proved using the integration method on page 120.) One can verify the bound for T_1 and T_2. Suppose the bound holds for T_n and apply this induction hypothesis to T_{n+1}:

$$T_{n+1} = (1+\tfrac{1}{n+1})T_n + 2 \le 2(1+\tfrac{1}{n+1})H_n e^{H_n} + 2 \le 2e^{1/(n+1)}H_n e^{H_n} + 2 = 2H_n e^{H_{n+1}} + 2.$$

Writing $H_n = H_{n+1} - \frac{1}{n+1}$, we get that

$$T_{n+1} \le 2(H_{n+1} - \tfrac{1}{n+1})e^{H_{n+1}} + 2 = 2H_{n+1}e^{H_{n+1}} + 1 - \tfrac{1}{n+1}e^{H_{n+1}}.$$

$e^{H_{n+1}} > n+2$ implies $\frac{1}{n+1}e^{H_{n+1}} \ge \frac{n+2}{n+1} > 1$, or $1 - \frac{1}{n+1}e^{H_{n+1}} < 0$. Therefore,

$$T_{n+1} \le 2H_{n+1}e^{H_{n+1}} + 1 - \tfrac{1}{n+1}e^{H_{n+1}} \le 2H_{n+1}e^{H_{n+1}}.$$

How did we derive the upper bound? We unfolded the recursion:

$$\begin{aligned}
T_n &= (1+\tfrac{1}{n})T_{n-1} + 2 \\
(1+\tfrac{1}{n})T_{n-1} &= (1+\tfrac{1}{n})(1+\tfrac{1}{n-1})T_{n-2} + 2(1+\tfrac{1}{n}) \\
(1+\tfrac{1}{n})(1+\tfrac{1}{n-1})T_{n-2} &= (1+\tfrac{1}{n})(1+\tfrac{1}{n-1})(1+\tfrac{1}{n-2})T_{n-3} + 2(1+\tfrac{1}{n})(1+\tfrac{1}{n-1}) \\
&\vdots \\
(1+\tfrac{1}{n})\cdots(1+\tfrac{1}{4})T_3 &= (1+\tfrac{1}{n})(1+\tfrac{1}{n-1})\cdots(1+\tfrac{1}{3})T_2 + 2(1+\tfrac{1}{n})\cdots(1+\tfrac{1}{4}).
\end{aligned}$$

Now equate the sum of the left hand sides to the sum of the right hand sides,

$$T_n = (1+\tfrac{1}{n})\cdots(1+\tfrac{1}{3})T_2 + 2\left(1 + (1+\tfrac{1}{n}) + (1+\tfrac{1}{n})(1+\tfrac{1}{n-1}) + \cdots + (1+\tfrac{1}{n})\cdots(1+\tfrac{1}{4})\right).$$

The first term is bounded by $e^{1/n}e^{1/(n-1)}\cdots e^{1/3} = e^{H_n - H_2}$. The second term is a sum of terms of the form a_k, where $a_k = (1+\frac{1}{n})\cdots(1+\frac{1}{k})$. Using $\ln(1+x) \le x$ (because $1 + x \le e^x$),

$$\log a_k \le \sum_{i=k}^{n} \tfrac{1}{i} = H_n - H_{k-1},$$

$$\text{which implies} \qquad T_n \le T_2 e^{H_n - H_2} + 2\sum_{k=3}^{n} e^{H_n - H_k} = T_2 e^{H_n - H_2} + 2e^{H_n}\sum_{k=3}^{n} e^{-H_k}.$$

Since $H_k \ge \ln k$, $e^{-H_k} \le \frac{1}{k}$ and so $\sum_{k=3}^{n} e^{-H_k} \le \sum_{k=3}^{n} \frac{1}{k} = H_n - H_2$. We conclude that

$$T_n \le T_2 e^{H_n - H_2} + 2e^{H_n}(H_n - H_2) = 2H_n e^{H_n} + e^{H_n}(T_2 e^{-H_2} - 2H_2).$$

Since $T_2 = 4$, you may verify that $T_2 e^{-H_2} - 2H_2 < 0$ which gives the bound.

Chapter 20

Exercise 20.1.

(a) $\mathbf{X}$ is the sum of the dice, $\mathbf{X} = \mathbf{X}_1 + \cdots + \mathbf{X}_n$. $\mathbf{X}_i$ is an r_i-sided dice, so $\mathbb{E}[\mathbf{X}_i] = \frac{1}{r_i}(1 + \cdots + r_i) = \frac{1}{r_i} \times \frac{1}{2}r_i(r_i+1) = \frac{1}{2}(r_i+1)$. By linearity of expectation, $\mathbb{E}[\mathbf{X}] = \sum_{i=1}^{n}\mathbb{E}[\mathbf{X}_i] = \frac{1}{2}\sum_{i=1}^{n}(1+r_i) = \frac{n}{2} + \frac{1}{2}\sum_{i=1}^{n} r_i$.

(b) Let $\mathbf{X}_i$ indicate (0 or 1) whether trial i is a success. $\mathbf{X}_i$ is a Bernoulli with success probability p_i and $\mathbb{E}[\mathbf{X}_i] = p_i$. The number of successes $\mathbf{X} = \mathbf{X}_1 + \cdots + \mathbf{X}_n$. By linearity of expectation, $\mathbb{E}[\mathbf{X}] = \sum_{i=1}^{n}\mathbb{E}[\mathbf{X}_i] = \sum_{i=1}^{n} p_i$.

(c) $\mathbf{X}_i$ is the number of trials from the $(i-1)$th success to the ith and $\mathbf{X} = \mathbf{X}_1 + \cdots + \mathbf{X}_n$. $\mathbb{E}[X_i] = 1/p_i$. By linearity of expectation, $\mathbb{E}[\mathbf{X}] = \sum_{i=1}^{n} 1/p_i$.

(d) Computing the PDF is *very* challenging, let alone computing the expectation from the PDF.

Pop Quiz 20.2. Let's count possible outcomes. If die 1 is i, there are i further rolls, so there are 6^i possible outcomes given i. Thus, the number of possible outcomes is $6^1 + \cdots + 6^6 = 55986$.

The probability space is not uniform. Outcome $(1,1)$ has probability $1/6^2$, but outcome $(2,1,1)$ has probability $1/6^3$.

You could creat a uniform outcome space by tossing 7 dice. You would then define the equivalent random variable $\mathbf{X}_1$ as the first roll and $\mathbf{X}_2$ as the sum of the next $\mathbf{X}_1$ rolls.

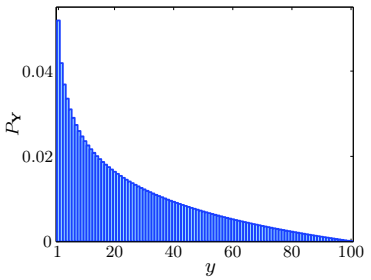
Exercise 20.3.

(a) For cases $\mathbf{X} = 1, 2, \ldots, 100$, total probability gives

$$P_{\mathbf{Y}}(y) = \sum_{x=1}^{100} P_{\mathbf{Y}}(y \mid x) P_{\mathbf{X}}(x) = \tfrac{1}{100} \sum_{x=y}^{100} 1/x$$

because: $P_{\mathbf{X}}(x) = 1/100$ ($\mathbf{X} \sim \mathbf{U}[100]$); $P_{\mathbf{Y}}(y \mid x) = 0$ for $x < y$; $P_{\mathbf{Y}}(y \mid x) = 1/x$ for $x \geq y$. ($\mathbf{Y} \sim \mathbf{U}[x]$). The sum is H_{100} for $y = 1$ and $H_{100} - H_{y-1}$ for $y > 1$, where H_n is the nth harmonic number. So,

$$P_{\mathbf{Y}}(y) = \begin{cases} H_{100}/100 & y = 1; \\ (H_{100} - H_{y-1})/100 & y \in \{2, \ldots, 100\} \end{cases}$$



To verify that the probabilities sum to 1, use the Harmonic sum $\sum_{i=1}^{n} H_n = (n+1)H_n - n$ (prove it by induction). Computing the expected value from this PDF is torture by summation. Since we are young, let's do it, especially since Harmonic sums are frequent. We do the computation for general n (in our case $n = 100$).

$$\mathbb{E}[\mathbf{Y}] = \sum_{i=1}^{n} i P_{\mathbf{Y}}(i) = \frac{1}{n}\left(H_n + \sum_{i=2}^{n} i(H_n - H_{i-1})\right) = \frac{1}{n}\left(H_n \sum_{i=1}^{n} i - \sum_{i=2}^{n} i H_{i-1}\right).$$

The first sum is $\frac{1}{2}n(n+1)$. The second sum is an example of a Harmonic sum.

$$\begin{aligned}
\sum_{i=2}^{n} i H_{i-1} = \quad & 2 \times H_1 && = \tfrac{2}{1} \\
& + 3 \times H_2 && = \tfrac{3}{1} + \tfrac{3}{2} \\
& + 4 \times H_3 && = \tfrac{4}{1} + \tfrac{4}{2} + \tfrac{4}{3} \\
& + 5 \times H_4 && = \tfrac{5}{1} + \tfrac{5}{2} + \tfrac{5}{3} + \tfrac{5}{4} \\
& \vdots && \vdots \\
& + n \times H_{n-1} && = \tfrac{n}{1} + \tfrac{n}{2} + \tfrac{n}{3} + \tfrac{n}{4} + \cdots + \tfrac{n}{n-1}
\end{aligned}$$

Let's sum columns (shaded) instead of rows. The 1st column is $(2 + \cdots + n) = \frac{1}{2}(n(n+1) - 1(1+1))/1$; the 2nd is $(3 + \cdots + n)/2 = \frac{1}{2}(n(n+1) - 2(2+1))/2$; the ith column is $((i+1) + \cdots + n)/i = \frac{1}{2}(n(n+1) - i(i+1))/i$. So,

$$\begin{aligned}
\sum_{i=2}^{n} i H_{i-1} &= \tfrac{1}{2} \sum_{i=1}^{n-1} \tfrac{n(n+1) - i(i+1)}{i} \\
&= \tfrac{1}{2} n(n+1) H_{n-1} - \tfrac{1}{2} \sum_{i=1}^{n-1} (i+1) \\
&= \tfrac{1}{2} n(n+1) H_{n-1} - \tfrac{1}{2} \sum_{i=1}^{n-1} (i+1) \;=\; \tfrac{1}{2} n(n+1) H_{n-1} - \tfrac{1}{2}(\tfrac{1}{2} n(n+1) - 1).
\end{aligned}$$

(You may use this technique to compute the Harmonic sum $\sum_{i=1}^{n} H_n$.) For $\mathbb{E}[\mathbf{Y}]$ we get

$$\mathbb{E}[\mathbf{Y}] = \frac{1}{n}\left(\tfrac{1}{2}n(n+1)H_n - \tfrac{1}{2}n(n+1)H_{n-1} + \tfrac{1}{4}n(n+1) - \tfrac{1}{2}\right) = \frac{1}{n}\Big(\tfrac{1}{2}n(n+1)\underbrace{(H_n - H_{n-1})}_{1/n} + \tfrac{1}{4}n(n+1) - \tfrac{1}{2}\Big) = \frac{n+3}{4}.$$

In our case, $n = 100$, so $\mathbb{E}[\mathbf{Y}] = 25\frac{3}{4}$.

(b) $\mathbf{Y} \sim \mathbf{U}[\mathbf{X}]$. By Theorem 19.3 on page 279, $\mathbb{E}[\mathbf{Y} \mid \mathbf{X}] = \frac{1}{2}(\mathbf{X} + 1)$. By iterated expectation,

$$\mathbb{E}[\mathbf{Y}] = \mathbb{E}_{\mathbf{X}}[\mathbb{E}[\mathbf{Y} \mid \mathbf{X}]] = \mathbb{E}[\tfrac{1}{2}(\mathbf{X}+1)] = \tfrac{1}{2} + \tfrac{1}{2}\mathbb{E}[\mathbf{X}] = 25\tfrac{3}{4},$$

where the last step follows because $\mathbf{X} \sim \mathbf{U}[100]$, so $\mathbb{E}[\mathbf{X}] = \frac{1}{2}(100+1)$. How much easier!

Exercise 20.4.

(a) $\mathbf{Y}$ depends on $\mathbf{Z}$. If $\mathbf{Z} = 0$, $\mathbf{Y} = 0$, so $\mathbb{E}[\mathbf{Y} \mid \mathbf{Z} = 0] = 0$. If $\mathbf{Z} = 1$, $\mathbf{Y}$ has the same PDF as $\mathbf{X}$, so $\mathbb{E}[\mathbf{Y} \mid \mathbf{Z} = 1] = \mathbb{E}[\mathbf{X}]$ and $\mathbb{E}[\mathbf{Y}^2 \mid \mathbf{Z} = 1] = \mathbb{E}[\mathbf{X}^2]$. We can summarize both cases as

$$\mathbb{E}[\mathbf{Y} \mid \mathbf{Z}] = \mathbb{E}[\mathbf{X}] \cdot \mathbf{Z}, \qquad \mathbb{E}[\mathbf{Y}^2 \mid \mathbf{Z}] = \mathbb{E}[\mathbf{X}^2] \cdot \mathbf{Z}.$$

(b) $\mathbb{E}[\mathbf{Y}] = \mathbb{E}_{\mathbf{Z}}\big[\mathbb{E}[\mathbf{Y} \mid \mathbf{Z}]\big] = \mathbb{E}_{\mathbf{Z}}\big[\mathbb{E}[\mathbf{X}] \cdot \mathbf{Z}\big] = \mathbb{E}[\mathbf{X}] \cdot \mathbb{E}_{\mathbf{Z}}[\mathbf{Z}] = (1-p)\mathbb{E}[\mathbf{X}]$

$\mathbb{E}[\mathbf{Y}^2] = \mathbb{E}_{\mathbf{Z}}\big[\mathbb{E}[\mathbf{Y}^2 \mid \mathbf{Z}]\big] = \mathbb{E}_{\mathbf{Z}}\big[\mathbb{E}[\mathbf{X}^2] \cdot \mathbf{Z}\big] = \mathbb{E}[\mathbf{X}^2] \cdot \mathbb{E}_{\mathbf{Z}}[\mathbf{Z}] = (1-p)\mathbb{E}[\mathbf{X}^2]$

(Remember that $\mathbb{E}[\mathbf{X}]$ is just a number, so it can be pulled outside the expectation w.r.t. $\mathbf{Z}$.)

(c) $\mathbb{E}[\mathbf{X}] = 1 + \mathbb{E}[\mathbf{Y}] = 1 + (1-p)\mathbb{E}[\mathbf{X}] \quad \to \quad \mathbb{E}[\mathbf{X}] = 1/p.$
$\mathbb{E}[\mathbf{X}^2] = 1 + 2\mathbb{E}[\mathbf{Y}] + \mathbb{E}[\mathbf{Y}^2] = 2/p - 1 + (1-p)\mathbb{E}[\mathbf{X}^2] \quad \to \quad \mathbb{E}[\mathbf{X}^2] = (2-p)/p^2.$

Why derive something we already derived using total expectation? First, to showcase iterated expectation, which is often useful in more complicated situations. Second, it always helps to revisit old results using new tools.

Pop Quiz 20.5.
(a) $\mathbf{X}$ is fixed with respect to the inner expectation that is w.r.t. $\mathbf{Y}$.
(b) $\mathbf{Y}$ is independent of $\mathbf{X}$, so its PDF is unchanged, given $\mathbf{X}$. The conditional and unconditional expectations match.
(c) $\mathbb{E}[\mathbf{Y}]$ is a number independent of $\mathbf{X}$ that can be pulled outside the expectation.

Exercise 20.6.
(a) Knowing $\mathbf{X}_1 + \mathbf{X}_2 = 9$ makes $\mathbf{X}_1$ and $\mathbf{X}_2$ dependent. The possible outcomes are $(3,6),(4,5),(5,4),(6,3)$, each with conditional probability $\frac{1}{4}$. The conditional expectation of the product is $\frac{1}{4}(18+20+20+18) = 19$. The conditional expectation of each roll is $\frac{1}{4}(3+4+5+6) = 4.5$ and $4.5^2 = 20.25$, so the conditional expectation of the product is not the product of condtional expectations, even though the random variables started out independent.
(b) (i) $\mathbb{E}[\frac{1}{\mathbf{X}_1}] = \frac{1}{6}(\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6}) \approx 0.41$, where as $1/\mathbb{E}[\mathbf{X}_1] = 1/3.5 \approx 0.29$. Not equal.
(ii) By total expectation, $\mathbb{E}[\mathbf{X}_1/\mathbf{X}_2] = \sum_{i=1}^{6} \mathbb{E}[\mathbf{X}_1/\mathbf{X}_2 \mid \mathbf{X}_1 = i]\mathbb{P}[\mathbf{X}_1 = i]$. Since $\mathbb{E}[\mathbf{X}_1/\mathbf{X}_2 \mid \mathbf{X}_1 = i] = i\mathbb{E}[1/\mathbf{X}_2]$,

$$\mathbb{E}[\mathbf{X}_1/\mathbf{X}_2] = \tfrac{1}{6}\mathbb{E}[1/\mathbf{X}_2] \sum_{i=1}^{6} i = \mathbb{E}[\mathbf{X}_1]\mathbb{E}[1/\mathbf{X}_2] \approx 1.43.$$

$\mathbb{E}[\mathbf{X}_1]/\mathbb{E}[\mathbf{X}_2] = 1$. Not equal.
(iii) In (ii) we showed that $\mathbb{E}[\mathbf{X}_1/\mathbf{X}_2] = \mathbb{E}[\mathbf{X}_1]\mathbb{E}[1/\mathbf{X}_2]$.

Exercise 20.7. The insight to solving problems like this is to "reparameterize" a sum, just like changing variables in a double integral. That is, change the order in which the terms are added. Here, we let $n = k + i$. The possible values of n are $0, 1, \ldots, r$. Given n, the possible values of k are $0, 1, \ldots, n$; and given n, k fixes $i = n - k$. Therefore,

$$\sum_{k=0}^{r} \sum_{i=0}^{r-k} f(k,i) = \sum_{n=0}^{r} \sum_{k=0}^{n} f(k, n-k).$$

The identity holds for any $f(k,i)$; every term on the left is accounted for on the right and *vice-versa*. Using this identity,

$$\sum_{k=0}^{r} \sum_{i=0}^{r-k} \tfrac{(-1)^i}{k!i!} = \sum_{n=0}^{r} \sum_{k=0}^{n} \tfrac{(-1)^{n-k}}{k!(n-k)!} = \sum_{n=0}^{r} \tfrac{(-1)^n}{n!} \sum_{k=0}^{n} \tfrac{n!}{k!(n-k)!}(-1)^k = \sum_{n=0}^{r} \tfrac{(-1)^n}{n!} \sum_{k=0}^{n} \binom{n}{k}(-1)^k.$$

By the Binomial theorem, $\sum_{k=0}^{n} \binom{n}{k}(-1)^k = (-1+1)^n = 0$, unless $n = 0$, which contributes $(-1)^0/0! = 1$.

Exercise 20.8.
(a) Year 1 is always a record-breaker (there is no record to break), so $\mathbb{P}[\mathbf{X}_1 = 1] = 1$.
For $t \geq 2$, we use total probability with n cases $(y_1, y_2, \ldots, y_n)$ for the temperature in year t, and $\mathbb{P}[\mathbf{Y} = y_i] = \frac{1}{n}$:

$$\mathbb{P}[\mathbf{X}_t = 1] \;=\; \sum_{i=1}^{n} \mathbb{P}[\mathbf{X}_t = 1 | \mathbf{Y} = y_i] \cdot \mathbb{P}[\mathbf{Y} = y_i] \;=\; \tfrac{1}{n} \sum_{i=2}^{n} \mathbb{P}[\mathbf{X}_t = 1 | \mathbf{Y} = y_i], \tag{30.1}$$

(b) The temperature y_i is a record-breaker $y_1, \ldots, y_{i-1}$ are lower. This occurs with probability $(i-1)/n$. $\mathbb{P}[\mathbf{X}_t = 1 \mid \mathbf{Y}_t = y_i]$ is the probability that every prior year has a temperature lower than y_i, which by independence is

$$\mathbb{P}[\text{year } 1 < y_i \text{ AND } \cdots \text{ AND year } t-1 < y_i] = \mathbb{P}[\text{year } 1 < y_i] \times \cdots \times \mathbb{P}[\text{year } t-1 < y_i] = \left(\tfrac{i-1}{n}\right)^{t-1}.$$

(c) We can now compute $\mathbb{P}[\mathbf{X}_t = 1]$ from (30.1),

$$\mathbb{P}[\mathbf{X}_t = 1] \;=\; \tfrac{1}{n} \sum_{i=2}^{n} \left(\tfrac{i-1}{n}\right)^{t-1} \;=\; \tfrac{1}{n} \sum_{i=1}^{n-1} \left(\tfrac{i}{n}\right)^{t-1} \tag{30.2}$$

In the last expression, we just changed the summation index i to go from 1 to $n-1$.
(d) The number of records is $\mathbf{X} = \mathbf{X}_1 + \mathbf{X}_2 + \cdots + \mathbf{X}_T = 1 + \sum_{t=2}^{T} \mathbf{X}_t$. We used $\mathbf{X}_1 = 1$. By linearity of expectation,

$$\mathbb{E}[\mathbf{X}] \;=\; 1 + \sum_{t=2}^{T} \mathbb{E}[\mathbf{X}_t] \overset{(a)}{=} 1 + \tfrac{1}{n} \sum_{t=2}^{T} \sum_{i=1}^{n-1} \left(\tfrac{i}{n}\right)^{t-1} \overset{(b)}{=} 1 + \tfrac{1}{n} \sum_{i=1}^{n-1} \sum_{t=2}^{T} \left(\tfrac{i}{n}\right)^{t-1}.$$

In (a) we used (30.2) and $\mathbb{E}[\mathbf{X}_t] = \mathbb{P}[\mathbf{X}_t = 1]$ because $\mathbf{X}_t$ is Bernoulli; in (b) we reversed summations, which you can always do for finite sums (you can add terms in any order). The sum with respect to t is a geometric series,

$$\sum_{t=2}^{T} \left(\tfrac{i}{n}\right)^{t-1} \;=\; \tfrac{i}{n} \sum_{t=0}^{T-2} \left(\tfrac{i}{n}\right)^{t} \;=\; \tfrac{i}{n} \cdot \left(\tfrac{1-(i/n)^{T-1}}{1-i/n}\right) \;=\; \tfrac{i}{n-i} \cdot \left[1 - \left(\tfrac{i}{n}\right)^{T-1}\right].$$

We now have our expression for $\mathbb{E}[\mathbf{X}]$, $\mathbb{E}[\mathbf{X}] \;=\; 1 + \frac{1}{n} \sum_{i=1}^{n-1} \frac{i}{n-i} \left[1 - \left(\frac{i}{n}\right)^{T-1}\right]$.

(e) When $T \to \infty$, $i/n \to 0$ because $i < n$. So, $\mathbb{E}[\mathbf{X}] \to 1 + \frac{1}{n}\sum_{i=1}^{n-1} \frac{i}{n-i}$ and

$$1 + \tfrac{1}{n}\sum_{i=1}^{n-1} \tfrac{i}{n-i} = 1 + \tfrac{1}{n}\sum_{i=1}^{n-1}\Big(\tfrac{n}{n-i} - 1\Big) = 1 - \tfrac{n-1}{n} + \sum_{i=1}^{n-1} \tfrac{1}{n-i} = \tfrac{1}{n} + \tfrac{1}{n-1} + \cdots + \tfrac{1}{1} = H_n.$$

(f) When $n \approx 200$, we expect about $H_{200} \approx 5.88$ records over history.

(g) The model in Example 20.9 assumes arbitrarily precise temperatures, so the highs are all distinct and the number of records grows as $\ln T$. With finite precision, there are only a finite number n of possible highs, depending on the level of precision. There cannot be more than n records, and on average one observes $O(\ln n)$ records.

Exercise 20.9.

(a) Let $\mathbf{X}_i$ indicate if i is picked. $\mathbb{P}[\mathbf{X}_i = 0] = (1 - 1/n)^m$ (by independence, because i is *not* picked with probability $1 - 1/n$), so $\mathbb{E}[\mathbf{X}_i] = 1 - (1 - 1/n)^m$. The number of distinct elements is $\mathbf{X} = \mathbf{X}_1 + \cdots + \mathbf{X}_n$. By linearity,

$$\mathbb{E}[\mathbf{X}] = \sum_{i=1}^{n} \mathbb{E}[\mathbf{X}_i] = n\left(1 - (1 - 1/n)^m\right) = n - n\left(1 - 1/n\right)^m.$$

(b) Let $\mathbf{X}_i$ indicate that white ball i is picked, $i = 1, \ldots, a$. There are $\binom{a+b}{k}$ ways to choose k balls (no replacement), each equally likely. If ball i is not picked, there are $\binom{a+b-1}{k}$ ways. So, $\mathbb{P}[\mathbf{X}_i = 0] = \binom{a+b-1}{k}/\binom{a+b}{k} = 1 - k/(a+b)$ and $\mathbb{E}[\mathbf{X}_i] = k/(a+b)$. The number of white balls picked is $\mathbf{X} = \mathbf{X}_1 + \cdots + \mathbf{X}_a$. By linearity of expectation,

$$\mathbb{E}[\mathbf{X}] = \sum_{i=1}^{a} \mathbb{E}[\mathbf{X}_i] = ak/(a+b).$$

(c) Getting expectations from the PDF is hard. We need the PDF, which requires counting. Then, we compute the expectation, a heavy duty summation. Why go through the effort? Because the PDF contains more information. What if you wanted to know how large m should be to see at least half the objects in part (a)?

(a) We need $P(k) =$ probability that k distinct elements are sampled. There are n^m m-sequences of the n objects. How many of these contain *exactly* k distinct objects?

First choose the k elements to sample in $\binom{n}{k}$ ways. Now from these elements, construct your m-sequence, with the condition that each of the k elements are used at least once. The number of m-sequences of the k objects is k^m. Let A_i be the sequences that do not use element i. The number of sequences using all k elements is $k^m - |A_1 \cup A_2 \cup \cdots \cup A_k|$. Since $|\ell\text{-way intersection of } A_i| = (k-\ell)^m$, by inclusion-exclusion,

$$|A_1 \cup A_2 \cup \cdots \cup A_k| = \sum_{\ell=1}^{k} (-1)^{\ell+1}\tbinom{k}{\ell}(k-\ell)^m.$$

$k^m - \sum_{\ell=1}^{k}(-1)^{\ell+1}\binom{k}{\ell}(k-\ell)^m = \sum_{\ell=0}^{k}(-1)^{\ell}\binom{k}{\ell}(k-\ell)^m$ sequences use all k objects. Dividing by n^m gives

$$P(k) = \tbinom{n}{k}\sum_{\ell=0}^{k}(-1)^{\ell}\tbinom{k}{\ell}\left(\tfrac{k-\ell}{n}\right)^m = \tbinom{n}{k}\sum_{\ell=0}^{k}(-1)^{k-\ell}\tbinom{k}{\ell}\left(\tfrac{\ell}{n}\right)^m,$$

where $k = 1, 2, \ldots, n$. The second expression changes summation index to $k - \ell$ and uses $\binom{k}{k-l} = \binom{k}{l}$. Note that if $k > m$, then $P(k)$ should be 0 and this is indeed the case.

Lemma 30.7. If $k > m$, then $\sum_{\ell=0}^{k}(-1)^{\ell}\binom{k}{\ell}\ell^m = 0$.

Proof. Strong induction on m. When $m = 0$, $\sum_{\ell=0}^{k}(-1)^{\ell}\binom{k}{\ell} = (1-1)^k = 0$. For $m \geq 0$ assume $\sum_{\ell=0}^{k}(-1)^{\ell}\binom{k}{\ell}\ell^x = 0$ for all $x \leq m$ and $k > x$. Consider $\sum_{\ell=0}^{k}(-1)^{\ell}\binom{k}{\ell}\ell^{m+1}$ with $k > m+1$. Since $m \geq 0$, the first term is 0, so we have

$$\sum_{\ell=1}^{k}(-1)^{\ell}\tbinom{k}{\ell}\ell^{m+1} = \sum_{\ell=1}^{k}(-1)^{\ell}\ell\tbinom{k}{\ell}\ell^m = \sum_{\ell=1}^{k}(-1)^{\ell}k\tbinom{k-1}{\ell-1}\ell^m.$$

(We used $\ell\binom{k}{\ell} = k\binom{k-1}{\ell-1}$.) Summing from 0 to $k-1$ instead of 1 to k, we get

$$-k\sum_{\ell=0}^{k-1}(-1)^{\ell}\tbinom{k-1}{\ell}(\ell+1)^m = -k\sum_{\ell=0}^{k-1}(-1)^{\ell}\tbinom{k-1}{\ell}\sum_{i=0}^{m}\tbinom{m}{i}\ell^i = -k\sum_{i=0}^{m}\tbinom{m}{i}\sum_{\ell=0}^{k-1}(-1)^{\ell}\tbinom{k-1}{\ell}\ell^i.$$

We used the Binomial theorem for $(\ell+1)^m$. In the last step, we change the order of summing. Since $k > m+1$, $k - 1 > m$ and the right sum is zero for $i \in \{0, \ldots, m\}$ by the induction hypothesis, concluding the proof. ∎

Using this lemma, we compute $\mathbb{E}[\mathbf{X}]$ as $\sum_{k=1}^{n} kP(k)$ without regard to m because if $k > m$ then $P(k) = 0$.

Exercise: We know that $\sum_{k=1}^{n} P(k) = 1$ since it is a PDF (prove it). This task is advanced. We want

$$\begin{aligned}
\sum_{k=1}^{n} kP(k) &= \sum_{k=1}^{n} (k-n+n)P(k) \\
&= n - \sum_{k=1}^{n} (n-k)P(k) && \text{use: } \sum_{k=1}^{n} P(k) = 1 \\
&= n - \sum_{k=1}^{n} \sum_{\ell=1}^{k} (-1)^{k-\ell}(n-k)\tbinom{n}{k}\tbinom{k}{\ell}(\tfrac{\ell}{n})^m \\
&= n - \sum_{k=1}^{n} \sum_{\ell=1}^{k} (-1)^{k-\ell}(n-k)\tbinom{n}{\ell}\tbinom{n-\ell}{n-k}(\tfrac{\ell}{n})^m && \text{use: } \tbinom{n}{k}\tbinom{k}{\ell} = \tbinom{n}{\ell}\tbinom{n-\ell}{n-k} \\
&= n - \sum_{\ell=1}^{n} \sum_{k=\ell}^{n} (-1)^{k-\ell}(n-k)\tbinom{n}{\ell}\tbinom{n-\ell}{n-k}(\tfrac{\ell}{n})^m && \text{use: } \sum_{k=1}^{n}\sum_{\ell=1}^{k} = \sum_{\ell=1}^{n}\sum_{k=\ell}^{n} \\
&= n - \sum_{\ell=1}^{n} \sum_{k=\ell}^{n-1} (-1)^{k-\ell}(n-\ell)\tbinom{n}{\ell}\tbinom{n-\ell-1}{n-k-1}(\tfrac{\ell}{n})^m
\end{aligned}$$

In the last step we used $(n-k)\binom{n-\ell}{n-k} = (n-\ell)\binom{n-\ell-1}{n-k-1}$ and dropped the term with $k = n$ because it is zero. Now move all terms involving only ℓ outside the inner sum,

$$\begin{aligned}
\sum_{k=1}^{n} kP(k) &= n - \sum_{\ell=1}^{n} (-1)^{-\ell}(n-\ell)\tbinom{n}{\ell}(\tfrac{\ell}{n})^m \sum_{k=\ell}^{n-1} (-1)^k \tbinom{n-\ell-1}{n-k-1} \\
&= n - \sum_{\ell=1}^{n} (-1)^{-\ell}(n-\ell)\tbinom{n}{\ell}(\tfrac{\ell}{n})^m \sum_{i=0}^{n-1-\ell} (-1)^{n-1-i} \tbinom{n-\ell-1}{i} \\
&= n - \sum_{\ell=1}^{n} (-1)^{n-1-\ell}(n-\ell)\tbinom{n}{\ell}(\tfrac{\ell}{n})^m \sum_{i=0}^{n-1-\ell} (-1)^{i} \tbinom{n-\ell-1}{i}
\end{aligned}$$

The inner alternating sum of Binomial coefficients is 0, unless $n-1-\ell = 0$ in which case the inner sum is 1. Therefore, the entire sum for the expectation collapses to one term, the one with $\ell = n-1$:

$$\sum_{k=1}^{n} kP(k) = n - (-1)^{n-1-(n-1)}(n-(n-1))\tbinom{n}{n-1}\left(\tfrac{n-1}{n}\right)^m = n - n\left(1-\tfrac{1}{n}\right)^m.$$

That's the same answer we got by using indicators, but what a computation. Wow!

(b) There are $\binom{a+b}{k}$ ways to choose k balls. If i are white, there are $\binom{a}{i}$ ways to choose the i white balls and $\binom{b}{k-i}$ ways to choose the remaining balls as black. So, $P(i) = \binom{a}{i}\binom{b}{k-i}/\binom{a+b}{k}$.

Exercise: We know that $\sum_{k=1}^{n} P(k) = 1$ since it is a PDF. Prove it. To prove that $\sum_k P(k) = 1$ you need a famous identity known as Vandermonde convolution, which is an application of the Binomial theorem:

$$\begin{aligned}
\sum_{k=0}^{a+b} \tbinom{a+b}{k} x^k \;=\; (1+x)^{a+b} &= (1+x)^a(1+x)^b \\
&= \sum_{i=0}^{a} \tbinom{a}{i} x^i \sum_{j=0}^{b} \tbinom{b}{j} x^j \\
&= \sum_{i=0}^{a}\sum_{j=0}^{b} \tbinom{a}{i}\tbinom{b}{j} x^{i+j} && \text{let } k = i+j, \\
&= \sum_{k=0}^{a+b} \alpha_k x^k, && \text{where } \alpha_k = \sum_{i=0}^{a} \tbinom{a}{i}\tbinom{b}{k-i}
\end{aligned}$$

On the left is a polynomial in x. On the right is also a polynomial in x. Two polynomials are equal if and only if their coefficients match. That is, $\alpha_k = \binom{a+b}{k}$.

Lemma 30.8 (Vandermonde convolution)**.** $\sum_{i=0}^{a} \binom{a}{i}\binom{b}{k-i} = \binom{a+b}{k}$.

Now for the expectation. We need $\sum_{i=0}^{a} iP(i) = \sum_i i\binom{a}{i}\binom{b}{k-i}/\binom{a+b}{k}$:

$$\begin{aligned}
\sum_{i=0}^{a} i\tbinom{a}{i}\tbinom{b}{k-i} &= \sum_{i=1}^{a} i\tbinom{a}{i}\tbinom{b}{k-i} && (i=0 \text{ term is zero}) \\
&= \sum_{i=1}^{a} a\tbinom{a-1}{i-1}\tbinom{b}{k-i} && \text{use: } i\tbinom{a}{i} = a\tbinom{a-1}{i-1} \\
&= a\sum_{i=0}^{a-1} \tbinom{a-1}{i}\tbinom{b}{k-1-i)} && (\text{sum over } i = 0,\ldots,a-1) \\
&= a\tbinom{a+b-1}{k-1}. && (\text{Vandermonde convolution})
\end{aligned}$$

Finally, $\mathbb{E}[\mathbf{X}] = a\binom{a+b-1}{k-1}/\binom{a+b}{k} = \frac{ak}{a+b}$, as we got before with indicators.

Exercise 20.10. A permutation σ of the vertices is a potential ranking. Let $\mathbf{X}_\sigma$ indicate if it is a ranking. Then, $\mathbb{P}[\mathbf{X}_\sigma = 1] = 1/2^9$ because there are 9 edges in the path and each edge will be oriented correctly with probability 1/2.

So $\mathbb{E}[\mathbf{X}_\sigma] = 1/2^9$. The number of rankings is $\sum_\sigma \mathbf{X}_\sigma$ and so the expected number of rankings is

$$\mathbb{E}[\text{number of rankings}] = \sum_\sigma \mathbb{E}[\mathbf{X}_\sigma] = \frac{1}{2^9}\sum_\sigma 1 = \frac{10!}{2^9} = 7087.5.$$

This formula can be generalized to $n!/2^{n-1}$ for a random tournament with n vertices.
An interesting corollary is that some tournament on 10 vertices has at least 7088 rankings. Do you see why?

Chapter 21

Pop Quiz 21.1. $\mathbb{E}[\mathbf{\Delta}] = \frac{-5}{36} + \frac{-4}{18} + \frac{-3}{12} + \frac{-2}{9} + \frac{-1\times5}{36} + \frac{0}{6} + \frac{1\times5}{36} + \frac{2}{9} + \frac{3}{12} + \frac{4}{18} + \frac{5}{36} = 0$. In general,

$$\mathbb{E}[\mathbf{\Delta}] = \mathbb{E}[\mathbf{X} - \mu] = \mathbb{E}[\mathbf{X}] - \mathbb{E}[\mu] = \mu - \mu = 0.$$

Exercise 21.2.
(a) (i) To get the table on the right, we use $\mathbb{E}[\mathbf{X}] = 3\frac{1}{2}$.

$$\sigma^2 = \mathbb{E}[\mathbf{\Delta}^2] = \tfrac{1}{24}(25+9+1+1+9+25) = 35/12$$
$$\text{std. deviation} = \sigma = \sqrt{35/12}.$$

$\mathbf{X}$	1	2	3	4	5	6	
$\mathbf{\Delta}^2$	$\frac{25}{4}$	$\frac{9}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{9}{4}$	$\frac{25}{4}$	$\leftarrow (\mathbf{X} - 3\frac{1}{2})^2$
$P_{\mathbf{X}}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	

(ii) We show the possible outcomes for the *average* of two dice, with the PDF. We know that $\mathbb{E}[\text{average}] = 3\frac{1}{2}$.

$\mathbf{X}$	1	$1\frac{1}{2}$	2	$2\frac{1}{2}$	3	$3\frac{1}{2}$	4	$4\frac{1}{2}$	5	$5\frac{1}{2}$	6	
$\mathbf{\Delta}^2$	$\frac{25}{4}$	$\frac{16}{4}$	$\frac{9}{4}$	$\frac{4}{4}$	$\frac{1}{4}$	$\frac{0}{4}$	$\frac{1}{4}$	$\frac{4}{4}$	$\frac{9}{4}$	$\frac{16}{4}$	$\frac{25}{4}$	$\leftarrow (\mathbf{X} - \frac{7}{2})^2$
$P_{\mathbf{X}}$	$\frac{1}{36}$	$\frac{1}{18}$	$\frac{1}{12}$	$\frac{1}{9}$	$\frac{5}{36}$	$\frac{1}{6}$	$\frac{5}{36}$	$\frac{1}{9}$	$\frac{1}{12}$	$\frac{1}{18}$	$\frac{1}{36}$	

Note that the probabilities do not change. It is just the random variable that changed.
$\sigma^2 = \mathbb{E}[\mathbf{\Delta}^2] = \frac{1}{4\times36}(25+32+27+16+5+0+5+14+27+32+25) = \frac{35}{24}$ ⟶ std. deviation $= \sqrt{35/24}$.

(b) The mean is p, so the deviations are

$$\mathbf{\Delta} = \begin{cases} -p & \text{prob} = 1-p; \\ 1-p & \text{prob} = p. \end{cases} \qquad \rightarrow \qquad \sigma^2 = (1-p)p^2 + p(1-p)^2 = p(1-p).$$

The standard deviation is $\sigma = \sqrt{p(1-p)}$.
(c) $\mu = 7$ and $\sigma = 2.52$ so the event of interest is $5 \le \mathbf{X} \le 9$. So, $\mathbb{P}[\mu - \sigma \le \mathbf{X} \le \mu + \sigma] = \frac{1}{9} + \frac{5}{36} + \frac{1}{6} + \frac{5}{36} + \frac{1}{9} = \frac{2}{3}$.

Exercise 21.3.
(a) (i) $\mathbb{E}[\mathbf{X}^2] = \frac{1}{6}(1^2 + \cdots + 6^2) = 15\frac{1}{6}$; $\mathbb{E}[\mathbf{X}^2] - \mathbb{E}[\mathbf{X}]^2 = 15\frac{1}{6} - (3\frac{1}{2})^2 = \frac{35}{12}$ ✓
(ii) $\mathbb{E}[\mathbf{X}^2] = \frac{2^2\cdot1+3^2\cdot2+\cdots+7^2\cdot6+8^2\cdot5+\cdots+12^2\cdot1}{4\times36} = \frac{329}{24}$; $\mathbb{E}[\mathbf{X}^2] - \mathbb{E}[\mathbf{X}]^2 = \frac{329}{24} - \frac{49}{4} = \frac{35}{24}$ ✓
(b) $\mathbb{E}[\mathbf{X}^2] = (1-p)\times0^2 + p\times1^2 = p$; $\mathbb{E}[\mathbf{X}^2] - \mathbb{E}[\mathbf{X}]^2 = p - p^2 = p(1-p)$ ✓

Exercise 21.4. By linearity, $\mathbb{E}[\mathbf{Y}] = \mathbb{E}[a + b\mathbf{X}] = a + b\mathbb{E}[\mathbf{X}]$. The deviations in $\mathbf{Y}$ are

$$\mathbf{\Delta}_\mathbf{Y} = \mathbf{Y} - \mathbb{E}[\mathbf{Y}] = a + b\mathbf{X} - a + b\mathbb{E}[\mathbf{X}] = b(\mathbf{X} - \mathbb{E}[\mathbf{X}]) = b\mathbf{\Delta}_\mathbf{X}.$$

So, $\sigma^2(\mathbf{Y}) = \mathbb{E}[\mathbf{\Delta}_\mathbf{Y}^2] = \mathbb{E}[b^2\mathbf{\Delta}_\mathbf{X}^2] = b^2\mathbb{E}[\mathbf{\Delta}_\mathbf{X}^2] = b^2\sigma^2(\mathbf{X})$.
Let $\mathbf{X}$ be a Bernoulli. The drunk's step is $\mathbf{Y} = 2\mathbf{X} - 1$. By Theorem 21.3, $\sigma^2(\mathbf{Y}) = 2^2\sigma^2(\mathbf{X}) = 4p(1-p)$.

Exercise 21.5. This exercise requires careful manipulation of sums that are squared.

$$\begin{aligned}
\sigma^2\Big(\sum_{i=1}^n a_i\mathbf{X}_i Big) &= \mathbb{E}\Big[\Big(\sum_{i=1}^n a_i\mathbf{X}_i\Big)^2\Big] - \mathbb{E}\Big[\sum_{i=1}^n a_i\mathbf{X}_i\Big]^2 && \text{(definition)} \\
&= \mathbb{E}\Big[\sum_{i=1}^n a_i\mathbf{X}_i \sum_{j=1}^n a_j\mathbf{X}_j\Big] - \Big(\sum_{i=1}^n a_i\mathbb{E}[\mathbf{X}_i]\Big)^2 && \text{(linearity)} \\
&= \sum_{i=1}^n\sum_{j=1}^n a_ia_j\mathbb{E}\left[\mathbf{X}_i\mathbf{X}_j\right] - \sum_{i=1}^n\sum_{j=1}^n a_ia_j\mathbb{E}[\mathbf{X}_i]\mathbb{E}[\mathbf{X}_j] && \text{(linearity)} \\
&= \sum_{i=1}^n a_i^2(\mathbb{E}\left[\mathbf{X}_i^2\right] - \mathbb{E}[\mathbf{X}_i]^2) - \sum_{i=1}^n\sum_{j\neq1}^n a_ia_j\underbrace{(\mathbb{E}\left[\mathbf{X}_i\mathbf{X}_j\right] - \mathbb{E}[\mathbf{X}_i]\mathbb{E}[\mathbf{X}_j])}_{\text{0 for independent random variables}} \\
&= \sum_{i=1}^n a_i^2\sigma^2(\mathbf{X}_i)
\end{aligned}$$

The key step is to break the double sum into $i = j$ ($\mathbf{X}_i\mathbf{X}_j = \mathbf{X}_i^2$) and $i \neq j$ ($\mathbf{X}_i$ and $\mathbf{X}_j$ are independent).

Exercise 21.6. $\mathbf{X} = \mathbf{X}_1+\mathbf{X}_2+\mathbf{X}_3+\mathbf{X}_4+\mathbf{X}_5$, where $\mathbf{X}_i$ are independent waiting times each with variance $(1-p)/p^2 = 6$. So $\sigma^2(\mathbf{X}) = 5 \times 6 = 30$.

A Monte Carlo with 100,000 experiments gave average wait time of 14.98 with variance 29.99, matching the theory.

Pop Quiz 21.7. $\mathbf{X}_1 = 1 \wedge \mathbf{X}_2 = 0 \to \mathbf{X}_3 = 0$; $\quad \mathbf{X}_1 = 0 \wedge \mathbf{X}_2 = 0 \to \mathbf{X}_3 = 0$ or 1.

Exercise 21.8. $\mathbf{X} = \sum_{i=1}^n \mathbf{X}_i$ and $\mathbb{E}[\mathbf{X}^2] = \mathbb{E}\Big[\sum_{i=1}^n \sum_{j=1}^n \mathbf{X}_i\mathbf{X}_j\Big] = \sum_{i=1}^n \sum_{j=1}^n \mathbb{E}[\mathbf{X}_i\mathbf{X}_j] = \sum_{i=1}^n \mathbb{E}[\mathbf{X}_i^2] + \sum_{i=1}^n \sum_{j\neq 1}^n \mathbb{E}[\mathbf{X}_i\mathbf{X}_j]$.

(The second step uses linearity of expectation.) $\mathbf{X}_i$ is a Bernoulli with probability $p = \frac{1}{n}$ so $\mathbb{E}[\mathbf{X}_i^2] = p$. Since $\mathbf{X}_i\mathbf{X}_j$ is a Bernoulli with probability $p = \mathbb{P}[\mathbf{X}_i = 1 \wedge \mathbf{X}_j = 1] = (n-2)!/n! = 1/n(n-1)$, we have $\mathbb{E}[\mathbf{X}_i\mathbf{X}_j] = 1/n(n-1)$ and

$$\mathbb{E}[\mathbf{X}^2] = \sum_{i=1}^n \tfrac{1}{n} + \sum_{i=1}^n \sum_{j\neq 1}^n \tfrac{1}{n(n-1)} = \tfrac{1}{n} \times n + \tfrac{1}{n(n-1)} \times n(n-1) = 2.$$

Since $\mathbb{E}[\mathbf{X}] = 1$, we have $\sigma^2(\mathbf{X}) = \mathbb{E}[\mathbf{X}^2] - \mathbb{E}[\mathbf{X}]^2 = 2 - 1 = 1$.

Exercise 21.9.

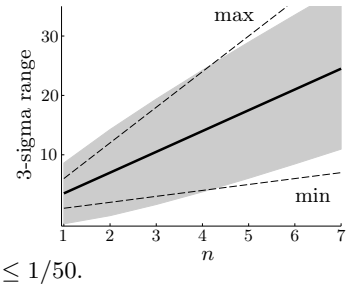
(a) A fair dice roll is a $\mathbf{U}[6]$, so $\sigma^2 = \frac{1}{12}(6^2-1) = 35/12$. Since the n dice are independent, the variance of the sum is the sum of the variances and so σ^2(sum of n dice) $= 35n/12$.

(b) The expected sum is $\mu(n) = 7n/2$.

(c) Using (a) and (b),

$$\mu \pm 3\sigma = 7n/2 \pm 3\sqrt{35n/12}.$$

In the figure, the 3σ-envelope is gray. The max ($6n$) and min (n) are dotted lines, and the mean μ is the solid line.



(d) The bound is not trivial when $7n/2 + 3\sqrt{35n/12} \leq 6n$. Since n is an integer, this means $n \geq 5$.

Pop Quiz 21.10. Since $\mathbf{X}$ is a positive random variable, and $\mathbb{E}[\mathbf{X}] = 1$, $\mathbb{P}[\mathbf{X} \geq 50] \leq 1/50$.

Pop Quiz 21.11. Since $\mu = 1$ and $\sigma = 1$,

$$\mathbb{P}[\mathbf{X} \geq 50] = \mathbb{P}[\mathbf{X} - 1 \geq 49] \leq \mathbb{P}[|\mathbf{X} - 1| \geq 49] = \mathbb{P}[|\mathbf{X} - \mu| \geq 49\sigma] \leq 1/49^2 \approx 0.00042.$$

The first inequality is because $\mathbf{X} - 1 \geq 49 \to |\mathbf{X} - 1| \geq 49$; the second uses Chebyshev's Inequality. The probability that at least 50 men get the correct hat is the sum of $P(k)$ for $k = 50$ to 100.

$$\mathbb{P}[\mathbf{X} \geq 50] = \sum_{k=50}^{100} \frac{1}{k!} \sum_{i=0}^{100-k} \frac{(-1)^i}{i!} \leq \frac{51}{50!} \approx 0,$$

because, for $k \in [50, 100]$, $\sum_{i=0}^{100-k} \frac{(-1)^i}{i!} \leq 1$ and $1/k! \leq 1/50!$. (Much smaller than the Chebyshev or Markov bounds.)

Exercise 21.12. $\mathbf{X} = \mathbf{X}_1 + \cdots + \mathbf{X}_n$, where $\mathbf{X}_i$ is Bernoulli with probability $p = 1/2$.

(a) By linearity, $\mathbb{E}[\mathbf{X}] = np = 100 \times \frac{1}{2} = 50$. For the variance, $\sigma^2(\mathbf{X}_i) = p(1-p)$. By independence and linearity, $\sigma^2(\mathbf{X}) = np(1-p) = n \times \frac{1}{4} = 25$ and $\sigma = 5$.

(b) Since $\mathbf{X}$ has a Binomial PDF, $\mathbb{P}[40 \leq \mathbf{X} \leq 60] = \sum_{k=40}^{60} \binom{100}{k} (\frac{1}{2})^k (\frac{1}{2})^{100-k} = \frac{1}{2^{100}} \sum_{k=40}^{60} \binom{100}{k} \approx 0.9648$.

(c) $\mathbb{P}[40 \leq \mathbf{X} \leq 60] = \mathbb{P}[|\mathbf{X} - \mu| < 10] = \mathbb{P}[|\mathbf{X} - \mu| < 2\sigma] \geq 1 - \frac{1}{2^2} = 0.75$.

Exercise 21.13.

(a) $\mathbb{P}[|\mathbf{X} - \mu| \geq t\sigma] = \mathbb{P}[\mathbf{X} - \mu \geq t\sigma] + \mathbb{P}[\mathbf{X} - \mu \leq -t\sigma]$. Using (21.7),

$$\mathbb{P}[\mathbf{X} - \mu \leq -t\sigma] = \mathbb{P}[\mathbf{X} \leq \mu - t\sigma] = F_{\mathbf{X}}(\mu - t\sigma) \approx \phi\left(\tfrac{\sqrt{n}(\mu - t\sigma)}{\sigma}\right) = \phi(-t\sqrt{n}) = 1 - \phi(t\sqrt{n}).$$

$$\mathbb{P}[\mathbf{X} - \mu \geq t\sigma] = 1 - \mathbb{P}[\mathbf{X} - \mu \leq t\sigma] = 1 - F_{\mathbf{X}}(\mu + t\sigma) \approx 1 - \phi(t\sqrt{n}).$$

Adding, these two equations gives the desired result: $\mathbb{P}[|\mathbf{X} - \mu| \geq t\sigma] \approx 2(1 - \phi(t\sqrt{n}))$.

(b) When $t\sqrt{n}$ is large, $\phi(t\sqrt{n}) \approx 1 - e^{-\frac{1}{2}nt^2}/\sqrt{2\pi nt^2}$. Therefore, $\mathbb{P}[|\mathbf{X} - \mu| \geq t\sigma] \approx 2e^{-\frac{1}{2}nt^2}/\sqrt{2\pi nt^2}$.

Chapter 22

Pop Quiz 22.1.

(a) (i) An injection maps A to a three-ordering of B. There are $4 \times 3 \times 2 = 24$ 3-orderings. (ii) Since $|A| < |B|$, there are no surjections. (iii) Similarly, there are no bijections.

(b) (i) $|A| \leq |B|$ (ii) It is not the case that $|A| \leq |B|$, which means $|A| > |B|$.

(c) (i) $|A| \geq |B|$ (ii) It is not the case that $|A| \geq |B|$, which means$|A| < |B|$.

(d) The injection means $|A| \leq |B|$. No bijection means $|A| \neq |B|$. Together this means $|A| < |B|$.

Exercise 22.2.
(a) $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 4$ is a bijection from A to B so $|A| = |B|$.

(b) Suppose $n \le k$, then $a_i \mapsto b_i$ is an injection from A to B, so $|A| \le |B|$.
Suppose $|A| \le |B|$: there is an injection $f : A \mapsto B$. We prove by induction on n that $n \le k$. If $n = 1$, then B contains $f(a_1)$, so $k \ge 1$. Suppose the claim holds for n. Consider any set A with $n+1$ elements. Let $f(a_{n+1}) = b_\ell$. Relabel the elements of B so that $b_\ell \to b_k$ and $b_k \to b_\ell$ (swap b_ℓ and b_k). Now, f maps $a_{n+1} \mapsto b_k$. If there was an element a_r which mapped to b_k under f, a_r now maps to b_ℓ. Now remove b_k from B and a_{n+1} from A. The new f is an injection from $a_1, \ldots, a_n$ to $b_1, \ldots, b_{k-1}$. By the induction hypothesis, $n \le k-1$ or $n+1 \le k$. ∎

(c) If $|A| \le |B|$ and $|B| \le |A|$, by (b), $\left.\begin{array}{l} |A| \le |B| \to n \le k \\ |B| \le |A| \to k \le n \end{array}\right\} \to n = k$. So, $a_i \mapsto b_i$ is a bijection and $|A| = |B|$.

(d) If $A \subseteq B$, then for $a \in A$, $f(a) = a$ is an injection from A to B. Therefore, $|A| \le |B|$.

(e) No: in (a), $A \not\subseteq B$ and $B \not\subseteq A$. When any two sets are comparable, the relationship is a *total order*. The subset relationship does not give a total order. You can always compare two sets using the injection relationship. Either $A \overset{\text{INJ}}{\mapsto} B$ or $B \overset{\text{INJ}}{\mapsto} A$, so either $|A| \le |B|$ or $|B| \le |A|$, which means size comparison using injection gives a total order.

Pop Quiz 22.3. Surely, there are twice as many natural numbers as even numbers or odd numbers, and far more than squares? Nope. The cardinalities of all four sets are the same. Here is a bijection from E to $\mathbb{N}$, $f(x) = x/2$:

E:	2	4	6	8	10	12	14	16	18	20	$\cdots$
	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	
$\mathbb{N}$:	1	2	3	4	5	6	7	8	9	10	$\cdots$

Simularly, $f(x) = (x+1)/2$ and $f(x) = \sqrt{x}$ are bijections from respectively O and S to $\mathbb{N}$. Note that, in this case, E, O, S are all subsets of $\mathbb{N}$, hence $|E| \le |\mathbb{N}|$, $|O| \le |\mathbb{N}|$, $|S| \le |\mathbb{N}|$. It suffices to find injections from $\mathbb{N}$. Injections from $\mathbb{N}$ to E, O, S are respectively $f(k) = 2k$, $f(k) = 2k-1$ and $f(k) = k^2$ (these happen to be bijections too).

Exercise 22.4. First we show f is 1-to-1. Suppose not. Let $n_1 \ne n_2$ and $f(n_1) = f(n_2)$. So,

$$\tfrac{1}{4}(1 + (-1)^{n_1}(2n_1 - 1)) = \tfrac{1}{4}(1 + (-1)^{n_2}(2n_2 - 1)) \;\to\; (-1)^{n_1}(2n_1 - 1) = (-1)^{n_2}(2n_2 - 1).$$

The sign of both sides must be the same, so $(-1)^{n_1} = (-1)^{n_2}$ and we conclude $2n_1 - 1 = 2n_2 - 1$. That is, $n_1 = n_2$, a contradiction. So, f is an injection. Now we show that f is onto. Given $z \in \mathbb{Z}$, we must find n for which $f(n) = z$.

$$\begin{aligned} z > 0 :\; & n = 2z && \to\; f(n) = \tfrac{1}{4}(1 + (-1)^{2z}(4z - 1)) = z; \\ z \le 0 :\; & n = 2|z| + 1 && \to\; f(n) = \tfrac{1}{4}(1 + (-1)^{2|z|+1}(4|z| + 1)) = -|z| = z. \end{aligned}$$

Therefore, f is onto, and hence a bijection from $\mathbb{N}$ to $\mathbb{Z}$.

Pop Quiz 22.5. f is an injection, so two elements of A cannot map to the same element of $\mathbb{N}$.

Pop Quiz 22.6. Yes (every integer has a unique list position). Mathematically, one can show $z_1 \ne z_2 \to f(z_1) \ne f(z_2)$. The positions of $\{0, +3, -3, +6, -6\}$ are $\{1, 6, 7, 12, 13\}$.

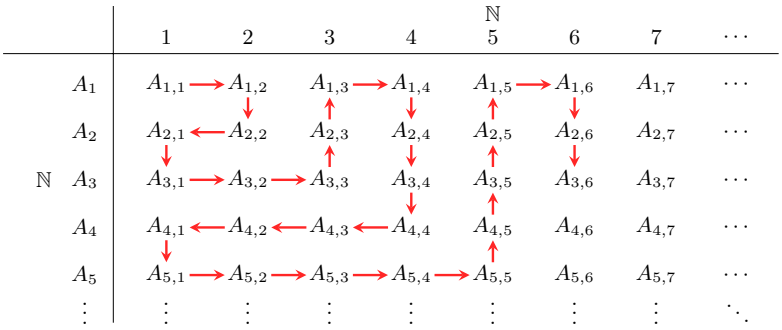
Exercise 22.7.
(a) The zig-zag path moves out one square at a time. Given $z/n \in \mathbb{Q}$, the column in which z appears is $c = 2z$ if $z > 0$ and $c = 2|z| + 1$ if $z \le 0$. We want to know when the path hits the cth column and nth row. This entry will be hit when traversing the column and row for the square of size $\max(n, c)$. If $z > 0$ (c even), you come down the RHS of the square; if $z \le 0$ (c odd), you go up the RHS of the square. So, there are four cases:

$$\begin{aligned} & n \ge c;\ n \text{ even} && i \;=\; (n-1)^2 + 2n - c \;=\; n^2 - c + 1 \\ & n \ge c;\ n \text{ odd} && i \;=\; (n-1)^2 + c \\ & c > n;\ c \text{ even} && i \;=\; (c-1)^2 + n \\ & c > n;\ c \text{ odd} && i \;=\; (c-1)^2 + 2c - n \;=\; c^2 - n + 1 \end{aligned}$$

(b) What is the list position of $\frac{0}{2}$? All positions are used by rationals with denominator 1.

(c) The sets are countable, so can be listed $\{A_1, A_2, A_3, \ldots, \}$. Each set is countable, so too can be listed, for example:

$A_1 = \{A_{1,1}, A_{1,2}, A_{1,3}, \ldots\}$. So, all the elements in $A_1 \cup A_2 \cup A_3 \cup \cdots$ can be put in a grid as follows (similar to $\mathbb{Q}$):



The path of arrows starting at $A_{1,1}$ lists the elements in the union. So, the union is countable.

(d) We have not shown $\mathbb{R}$ is countable (it's not), so we don't know if we can list the columns.

Exercise 22.8.

(a) No: $\bar{b}$, the complement of the diagonal, is infinite, and is not required to be in the list.

(b) Countable means you must produce a fixed list (injection to $\mathbb{N}$). Cantor diagonalization shows that there is no injection from $\mathcal{B}_\infty$ to $\mathbb{N}$. Adding $\bar{b}$ won't help because the complement of the new diagonal won't be in the list.

(c) Every infinite binary string is a subset of $\mathbb{N}$. The ones in the string identify the elements of $\mathbb{N}$. This is a bijection between the subsets and infinite binary strings, so $|\text{subsets of } \mathbb{N}| = |\mathcal{B}_\infty|$.

(d) Given a *finite* subset, construct a finite binary string for the subset by taking its infinite binary string and truncating it at the last 1. For example $\{1, 3, 7\} \mapsto 1010001$. Two different subsets will have 1's in different positions and so the truncated finite binary strings will be different. We have an injection from finite binary strings to $\mathcal{B}$ which proves that $|\{\text{finite binary strings}\}| \leq |\mathcal{B}| \leq |\,\mathbb{N}\,|$. So, the finite binary strings are countable.

Exercise 22.9.

(a) For any string that is eventually zero, construct a finite binary string by truncating it at the last 1. Two different strings which are eventually zero have 1s in different positions, and so will truncate to different finite strings. Hence, we have an injection from the strings which are eventually zero and finite binary strings. So,

$$|\{\text{strings which are eventually zero}\}| \leq |\{\text{finite binary strings}\}| \leq |\,\mathbb{N}\,|.$$

(b) An infinite string is either eventually zero or it is not, so (by definition) $\mathcal{B}_\infty = \mathcal{B}^0_\infty \cup \mathcal{B}^*_\infty$.

(c) Suppose $\mathcal{B}^*_\infty$ is countable. In (a) we showed that $\mathcal{B}^0_\infty$ is countable, so $\mathcal{B}_\infty = \mathcal{B}^0_\infty \cup \mathcal{B}^*_\infty$ is a union of countable sets and, by Theorem 22.3, is countable. That contradicts Theorem 22.6, hence $\mathcal{B}^*_\infty$ is uncountable.

(d) Let $a_1a_2a_3\cdots$ and $b_1b_2b_3\cdots$ be two different infinite strings in $\mathcal{B}^*_\infty$. We prove that they map to different values in $[0, 1]$ which proves the mapping is an injection and therefore $|\mathcal{B}^*_\infty| \leq |[0, 1]|$.

Let $x_a = \sum_{i=1}^{\infty} a_i 2^{-i}$ and $x_b = \sum_{i=1}^{\infty} b_i 2^{-i}$. Since $a_i \neq b_i$ for all i, by well-ordering, there is some minimum k for which $a_k \neq b_k$. Suppose $a_k = 1$ and $b_k = 0$. We have:

$$x_a - x_b = 2^{-k} + \sum_{i=k+1}^{\infty} a_i 2^{-i} - \sum_{i=k+1}^{\infty} b_i 2^{-i}.$$

Since a is not eventually zero, the a_i for $i \geq k+1$ cannot all be zero, so $\sum_{i=k+1}^{\infty} a_i 2^{-i} > 0$. Setting $b_i = 1$ for all $i \geq k+1$ gives $\sum_{i=k+1}^{\infty} b_i 2^- i \leq \sum_{i=k+1}^{\infty} 2^- i = 2^{-k}$. Therefore, $x_a - x_b > 2^{-k} + 0 - 2^{-k} = 0$ and $x_a \neq x_b$ as was to be shown. The same argument works if $a_k = 0$ and $b_k = 1$.

Chapter 23

Pop Quiz 23.1.

(a) $\mathcal{L}_{\text{push}}$ contains odd numbers, or strings that end in 1.

(b) Start the string with a the state of the light (1 on, 0 for off). The rest of the string is the binary string encoding the number of pushes. $\mathcal{L}_{\text{push}}$ contains strings whose first and last bit are different, $\mathcal{L}_{\text{push}} = \{01, 10, 001, 110, \ldots\}$.

Pop Quiz 23.2. Strings with more 1's than 0's in which every prefix has at least as many 1's as 0's.

(a) Open. (b) Closed. (c) Closed (not a valid sequence of walk-on/walk off). (d) Open. (e) Open. (f) Closed. (g) Closed (not a valid sequence).

Pop Quiz 23.3. The graph represented by the string is shown on the right. The distance between vertices 1 and 5 is three, so the answer is (NO).

Exercise 23.4.
(a) Starting from 1, you get your answer after D decision problems, for lengths $1, 2, \ldots, D$. To handle the case when there is no path, you answer ∞ after n decision problems, the number of vertices in the network.
(b) Use distances $1, 2, 4, \ldots$, doubling each time. Suppose the first (YES) is at 2^k using $k+1$ questions. Then, $2^{k-1} < D \leq 2^k$. Perform a binary search in the interval $[2^{k-1}, 2^k]$. Binary search needs $O(\log_2(\text{length of interval}))$ questions. The length of the interval is $2^k - 2^{k-1} = 2^{k-1}$. So the total number of questions is at most $k + 1 + O(\log_2(2^{k-1})) \in O(k)$. Since $2^{k-1} < D$, it follows that $k < 1 + \log_2 D \in O(\log_2 D)$ and you need only $O(\log_2 D)$ questions.

Pop Quiz 23.5. The (YES)-set $\subseteq$ {finite binary strings}, so it's countable and hence can be listed.

Exercise 23.6.
(a) $\mathcal{L}_{\text{balanced}} = \{\varepsilon, 01, 10, 0011, 0101, 0110, 1001, 1010, 1100, \ldots\}$
(b) $\overline{\mathcal{L}_1}, \mathcal{L}_1 \cup \mathcal{L}_2, \mathcal{L}_1 \cap \mathcal{L}_2$ are all collections of finite binary strings, so they are computing problems.
(c) Finite binary strings can be listed, $\Sigma^* = \{w_1, w_2, \ldots, \}$. A computing problem $\mathcal{L}$ (subset of Σ^*) can be identified by an infinite binary sequence, where the 1's in the sequence identify the strings in $\mathcal{L}$. This injection from infinite binary sequences (which are uncountable) to computing problems means computing problems are uncountable,

$$\text{uncountable} = |\{\text{infinite binary sequences}\}| \leq |\{\text{computing problems}\}|.$$

Pop Quiz 23.7.
(a) (i) $\{01, 011, 01111\}$. (ii) $\{\varepsilon, 00, 0000\}$. (iii) $\{00, 000, 001, 100, 0000, 0001, 0010, 0011, 1000, 1001, 0100, 1000, 1100\}$.
(b) $\{0,1\}^*1$ or $*1$.
(c) $\overline{*1*1*1*}$ describes strings with at most two 1s. Here are two regular expressions without using complement.

$$\{0\}^* \bullet \{\varepsilon, 1\} \bullet \{0\}^* \bullet \{\varepsilon, 1\} \bullet \{0\}^* \quad \text{and} \quad (\{0\}^*) \cup (\{0\}^* \bullet 1 \bullet \{0\}^*) \cup (\{0\}^* \bullet 1 \bullet \{0\}^* \bullet 1 \bullet \{0\}^*)$$

Pop Quiz 23.8.
$\varepsilon \to 00, 11 \to 0000, 1001, 0110, 1111$
$0 \to 000, 101 \to 00000, 10001, 01010, 11011$
$1 \to 010, 111 \to 00100, 10101, 01110, 11111$

Exercise 23.9.
(a) $\mathcal{L}_{0^n1^k} = 0^*1^*$. If you find a regular expression for $\mathcal{L}_{0^n1^n}$, let us know. The challenge is enforcing equality.
(b) There is no regular expression for $\mathcal{L}_{0^n1^n}$, yet it's easy to describe recursively. (Minimality is there by default.)

$\mathcal{L}_{0^n1^k}$: (1) $\varepsilon \in \mathcal{L}_{0^n1^k}$.
(2) $w \in \mathcal{L}_{0^n1^k} \to 0 \bullet w \in \mathcal{L}_{0^n1^k}$,
$w \in \mathcal{L}_{0^n1^k} \to w \bullet 1 \in \mathcal{L}_{0^n1^k}$.

$\mathcal{L}_{0^n1^n}$: (1) $\varepsilon \in \mathcal{L}_{0^n1^n}$.
(2) $w \in \mathcal{L}_{0^n1^n} \to 0 \bullet w \bullet 1 \in \mathcal{L}_{0^n1^n}$.

Pop Quiz 23.10.
(a) All these strings are in $\mathcal{L}_{\text{push}}$. The states traversed, ending in the resting state are:
(i) $q_0q_1q_1q_1\boldsymbol{q_1}$ (ii) $q_0q_0q_1q_0\boldsymbol{q_1}$ (iii) $q_0q_1q_0q_0\boldsymbol{q_1}$ (iv) $q_0q_1q_1q_1q_0q_0q_0\boldsymbol{q_1}$ (v) $q_0q_1q_0q_0q_0q_0q_0q_0q_1\boldsymbol{q_1}$
(b) None of these strings are in $\mathcal{L}_{\text{push}}$. The states traversed, ending in the resting state are:
(i) $q_0q_1\boldsymbol{q_0}$ (ii) $q_0q_0q_0q_1\boldsymbol{q_0}$ (iii) $q_0q_1q_0q_1\boldsymbol{q_0}$ (iv) $q_0q_1q_1q_1q_1q_1\boldsymbol{q_0}$ (v) $q_0q_0q_0q_0q_0q_0q_1q_1\boldsymbol{q_0}$

Chapter 24

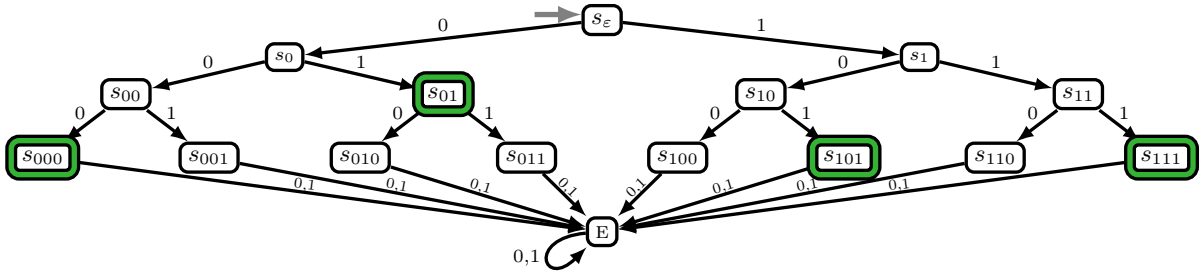
Pop Quiz 24.1.
(a) (i) $q_0|\triangleright 0000 \overset{M}{\mapsto} q_1|0\triangleright 000 \overset{M}{\mapsto} q_1|00\triangleright 00 \overset{M}{\mapsto} q_1|000\triangleright 0 \overset{M}{\mapsto} q_1|0000\triangleright$
(ii) $q_0|\triangleright 1000 \overset{M}{\mapsto} q_2|1\triangleright 000 \overset{M}{\mapsto} q_2|10\triangleright 00 \overset{M}{\mapsto} q_2|100\triangleright 0 \overset{M}{\mapsto} q_2|1000\triangleright$
(iii) $q_0|\triangleright 0001 \overset{M}{\mapsto} q_1|0\triangleright 001 \overset{M}{\mapsto} q_1|00\triangleright 01 \overset{M}{\mapsto} q_1|000\triangleright 1 \overset{M}{\mapsto} q_2|0001\triangleright$
(iv) $q_0|\triangleright 0100 \overset{M}{\mapsto} q_1|0\triangleright 100 \overset{M}{\mapsto} q_2|01\triangleright 00 \overset{M}{\mapsto} q_2|010\triangleright 0 \overset{M}{\mapsto} q_2|0100\triangleright$
(v) $q_0|\triangleright 0^{\bullet k}1^{\bullet \ell} \overset{M}{\mapsto} q_1|0\triangleright 0^{\bullet k-1}1^{\bullet \ell} \overset{M}{\mapsto} q_1|0^{\bullet 2}\triangleright 0^{\bullet k-2}1^{\bullet \ell}$
$\vdots$
$\overset{M}{\mapsto} q_1|0^{\bullet k}\triangleright 1^{\bullet \ell} \overset{M}{\mapsto} q_2|0^{\bullet k}1\triangleright 1^{\bullet \ell-1} \overset{M}{\mapsto} q_2|0^{\bullet k}1^{\bullet 2}\triangleright 1^{\bullet \ell-2}$
$\vdots$
$\overset{M}{\mapsto} q_2|0^{\bullet k}1^{\bullet \ell}\triangleright$
(b) Non-empty string containing only 0's.
(c) (i) (YES)(goes to q_1 and stays). (ii) (YES)(stays in q_1). (iii) (NO)(cannot escape q_2).

Exercise 24.2.
(a) When M processes a 1, it enters q_2 and stays leaves, so $M(w) =$ (NO) if w contains a 1. If $w = \varepsilon$, then M stops in q_0 and rejects. If $w = 0^{\bullet n}$ for $n > 0$, then M enters q_1 and never leaves, accepting. Therefore, $\mathcal{L}(M) = \{0^{\bullet n} \mid n > 0\}$

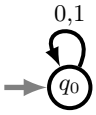
(b) (i) Strings with no 1's: $\mathcal{L}(M) = \{0\}^*$. (ii) Strings which are not only 0's: $\mathcal{L}(M) = \overline{\{0^{\bullet n} \mid n > 0\}}$.
(iii) Strings with an even number of zeros (incuding no 0's and ε). (iv) Strings with an odd number of zeros.
(v) $\mathcal{L}(M) = \{\varepsilon, 0\}$ (a finite language with just 2 (YES)-strings). (vi) Every string except ε and 0: $\mathcal{L}(M) = \overline{\{\varepsilon, 0\}}$.

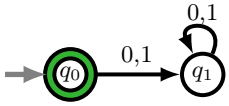
Exercise 24.3.

(a) We give a construction that generalizes to any finite language. Let ℓ be the length of the longest string in $\mathcal{L}$. Construct the binary tree to depth ℓ corresponding to every binary string of length at most ℓ, as shown in the DFA below. Every string of length at most ℓ leads the DFA to its unique state, which is a (YES)-state or not depending on whether the string is in $\mathcal{L}$. In the automaton below, the (YES)-states are $s_{00}, s_{000}, s_{101}, s_{111}$.

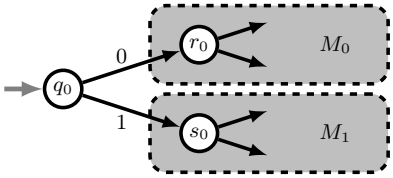


(b) One can generalize (a). Instead, we use induction on ℓ, the length of the longest string in $\mathcal{L}$.

Base Cases: $\mathcal{L} = \varnothing$: 

$\mathcal{L} = \{\varepsilon\}$: 

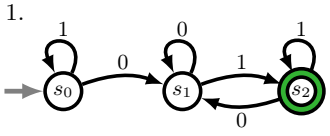
Suppose a finite language with maximum string length at most ℓ can be solved by a DFA. Consider any language $\mathcal{L}$ with maximum string length $\ell + 1$. $\mathcal{L}$ has two types of strings: those starting with 0 and those starting with 1. So $\mathcal{L} = (0 \bullet \mathcal{L}_0) \cup (1 \bullet \mathcal{L}_1)$ where $\mathcal{L}_0$ contains the suffixes of strings in $\mathcal{L}$ that start with 0 and L_1 the suffixes of the strings in $\mathcal{L}$ that start with 1. $\mathcal{L}_0$ and $\mathcal{L}_1$ are finite languages with maximum string length at most ℓ. By the induction hypothesis, there are DFAs M_0 and M_1 that solve $\mathcal{L}_0$ and $\mathcal{L}_1$. We construct a DFA M for $\mathcal{L}$ as follows.

M : 

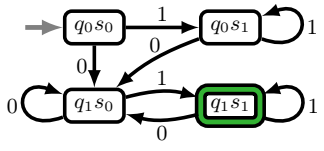
If a string starts with 0, the DFA transitions to r_0, the start state of M_0, runs M_0 and accepts if and only the suffix is in $\mathcal{L}_0$, i.e. if and only if the string is in $\mathcal{L}$. The logic is similar for a string that starts with 1. So, M accepts a *nonempty* string if and only if the string is in $\mathcal{L}$. Lastly, if the empty string $\varepsilon \in \mathcal{L}$, make q_0 a (YES)-state.

Exercise 24.4.

(a) Strings in $\mathcal{L}_1 \cap \mathcal{L}_2$ contain a zero and end in 1 so they are strings of the form: $*0*1$.
From the start state, you wait for 0, transition to s_1 and wait for 1. If you get 1, you must ensure it is the last bit. The DFA which implements this logic is on the right.



(b) Using product states, the DFA structure is exactly the same as for the union $\mathcal{L}_1 \cup \mathcal{L}_2$. However, the DFA should accept only the states $q_i s_j$ where both q_i is a (YES)-state of M_1 *and* s_j is a (YES)-state of M_2. The resulting DFA is on the right



Pop Quiz 24.5.

(a) $\mathcal{L}$ contains a string with a zero concatenated with a string ending in 1, which gives any string with a zero that ends with 1. That is, $*0*1$. So we can use the same DFA in Exercise 24.4(b).
(b) From Exercise 24.4(a), $\mathcal{L} = \mathcal{L}_1 \cap \mathcal{L}_2$. We can use the same DFA from Exercise 24.4(c).
(c) False. Consider any two $\mathcal{L}_1, \mathcal{L}_2$ with $\mathcal{L}_1 \cap \mathcal{L}_2 = \varnothing$. For example, $\mathcal{L}_1 = \{0\}$ and $\mathcal{L}_2 = \{1\}$.

Pop Quiz 24.6. In M_1', every zero toggles between q_0 and q_1. An odd number of 0's leaves you in q_1 which accepts. Similarly, in M_2' the DFA toggles between q_0 and q_1 for every bit.

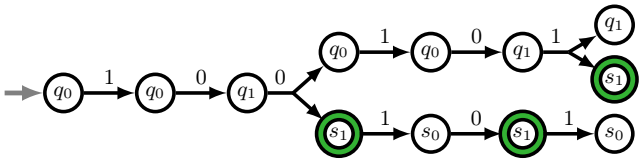
Exercise 24.7.

(a) After processing 100, the automaton state is q_0 or s_1, and 101 remains to be processed.

(b) $\{q_0\}|\triangleright 100101 \overset{M''}{\mapsto} \{q_0\}|1\triangleright 00101$
$\overset{M''}{\mapsto} \{q_1\}|10\triangleright 0101$
$\overset{M''}{\mapsto} \{q_0, s_1\}|100\triangleright 101$
$\overset{M''}{\mapsto} \{q_0, s_0\}|1001\triangleright 01$
$\overset{M''}{\mapsto} \{q_1, s_1\}|10010\triangleright 1$
$\overset{M''}{\mapsto} \{q_0, s_0, s_1\}|100101\triangleright$

At the end of the computation the non-deterministic automaton could be in either of the states q_0, s_0 or s_1.

We show the "computation-tree" on input 100101. The automaton starts in q_0 and processes the bits 10, transitioning to state q_0 then q_1. At the next 0, there are two possible actions so the computation branches. This happens each time the automaton is in q_1.



At the end, there are three possible computation paths the automaton could have taken (3 final states).

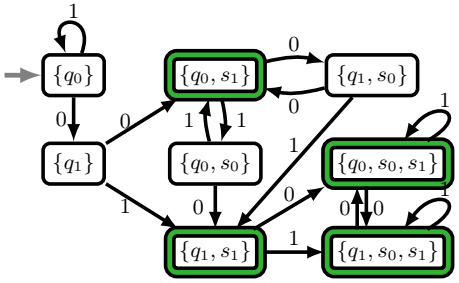
(c) If s_1 is one of the possible ending states, then there is a computation path that must have gone through q_1 (prefix in $\mathcal{L}_1$) and ended in s_1 without re-entering q_0 (suffix in $\mathcal{L}_2$), so M'' should accept. In this case the decision is (YES).

(d) Construct a state for every non-empty subset of states in M''. We use the subset as state-label. The states are

$\{q_0\}, \{q_1\}, \{s_0\}, \{s_1\}$
$\{q_0, q_1\}, \{q_0, s_0\}, \{q_0, s_1\}, \{q_1, s_0\}, \{q_1, s_1\}, \{s_0, s_1\}$
$\{q_0, q_1, s_0\}, \{q_0, q_1, s_1\}, \{q_0, s_0, s_1\}, \{q_1, s_0, s_1\}$
$\{q_0, q_1, s_0, s_1\}$

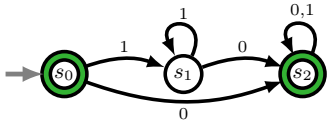
For each "subset"-state, the DFA transitions to a subset of states for each bit by considering all the possible ending states starting from any of the possible starting states of the transition. Consider, for example, state $\{q_1, s_1\}$ and input bit 1. $q_1 \overset{1}{\to} \{q_1, s_1\}$ and $s_1 \overset{1}{\to} s_0$, so $\{q_1, s_1\} \overset{1}{\to} \{q_1, s_0, s_1\}$. The DFA accepts whenever s_1 is in the set of possible states. The full automaton is on the right. Though there are 15 subset states, only 8 are reachable from the start state.

Our "principled" approach may not give the most efficient DFA. For example, states $\{q_1, s_1\}, \{q_0, s_0, s_1\}, \{q_1, s_0, s_1\}$ state $\{q_1 s_0\}$ can be connected directly to are all accepting and only transition amongst themselves, so they can all be merged into a single accepting state.

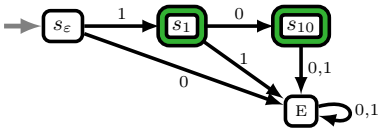


Exercise 24.8.

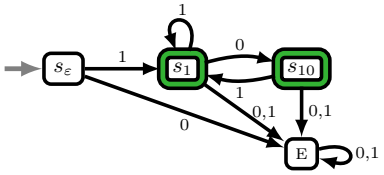
(a) $\mathcal{L}_1^* = \mathcal{L}_1^{\bullet 0} \cup \mathcal{L}_1^{\bullet 1} \cup \mathcal{L}_1^{\bullet 2} \cup \cdots$ where $\mathcal{L}_1^{\bullet 0} = \{\varepsilon\}$. Since $\mathcal{L}_1$ contains all strings with a 0, any string in $\mathcal{L}_1^{\bullet k}$ for $k \geq 1$ must contain a 0. That means $\mathcal{L}_1^{\bullet k} \subseteq \mathcal{L}_1$, hence $\mathcal{L}_1^* = \{\varepsilon\} \cup \mathcal{L}_1$. The DFA for $\mathcal{L}_1^*$ is on the right,



(b) Start with a DFA for $\mathcal{L}$ and convert it to a DFA for $\mathcal{L}^*$. Using the method in Exercise 24.3 gives a DFA for $\mathcal{L} = \{1, 10\}$, shown on the right. To implment $\mathcal{L}^*$, from an accept state of $\mathcal{L}$, we must restart the DFA as well as continue with the current path. That is, for input 0, add an arrow to the state s_ϵ would transition to for 0. Similarly, for input 1, add an arrow to where s_ϵ would transition. For example, add a 0-arrow from s_1 to E and a 1-arrow from s_1 to s_1. We get a non-deterministic automaton for $\mathcal{L}^+$.



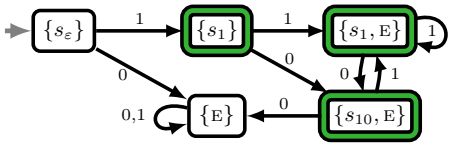
non-deterministic automaton for $\mathcal{L}^+$



Let us emphasize that a non-deterministic automaton is an interesting machine in its own right. However, for our purposes, it merely serves as an intermediate tool for getting at the DFA we need. One more small detail: since

$\varepsilon \in \mathcal{L}^*$, the non-deterministic automaton above only captures the non-empty strings in $\mathcal{L}^*$ (often denoted $\mathcal{L}^+$). At the end, we must augment the automaton to accept ε. We now use the subset-state method to get the DFA for $\mathcal{L}^+$. We only show the subset-states that are used in the DFA, not all 15 subset-states.

DFA for $\mathcal{L}^+$

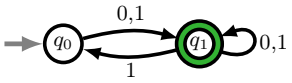


Lastly, to get the DFA for $\mathcal{L}^*$, simply make the start state $\{s_\varepsilon\}$ accepting.

(c) (i) $\{0, 1, 00, 10, 000, 100, 0000, 1000, 110, 111, 010, 011, 1010, 1100, 1011, 1110, 0010, 0100, 0011, 0110\}$

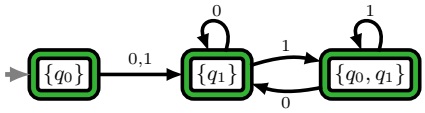
(ii) We use the same approach as in (b). From any accept state, we must allow the automaton to continue its current path or "restart" from state q_0 for the next bit. The only accept state is q_1, so q_1 should also transition to wherever q_0 transitions for bits 0,1. This gives the non-deterministic automaton for $\mathcal{L}(M)^+$.

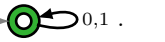
non-deterministic automaton for $\mathcal{L}(M)^+$



We use subset-states to get a DFA for $\mathcal{L}(M)^*$. To accept ε, the start state accepting. The result is:

DFA for $\mathcal{L}(M)^*$

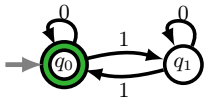


You will notice that this DFA accepts every string including ε: $\mathcal{L}(M)^* = \Sigma^*$. This is no surprise because the Kleene star of any language that contains 0 and 1 is Σ^*. So, a much simpler solution for $\mathcal{L}(M)^*$ is 

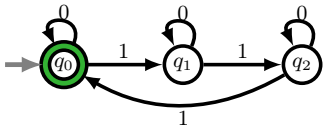
. We are not after the simplest solution. We are after a systematic solution.

Exercise 24.9. Let $\mathcal{L}_1$ contain strings with an even number of 1's and $\mathcal{L}_2$ strings whose number of 1's is divisible by 3. We first argue that $\mathcal{L}_1$ and $\mathcal{L}_2$ are regular, which means there are DFAs M_1 and M_2 to solve $\mathcal{L}_1$ and $\mathcal{L}_2$:

M_1:

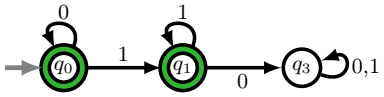


M_2:



We build $\mathcal{L} = \overline{\mathcal{L}_1 \cup \mathcal{L}_2}$ using set operations on $\mathcal{L}_1$ and $\mathcal{L}_2$. By Theorem 24.2, $\mathcal{L}_1 \cup \mathcal{L}_2$ is regular because $\mathcal{L}_1$ and $\mathcal{L}_2$ are (closure under union). Again, by Theorem 24.2, $\overline{\mathcal{L}_1 \cup \mathcal{L}_2}$ is regular (closed under complement). Therefore $\mathcal{L}$ is regular.

Pop Quiz 24.10.



Pop Quiz 24.11. The same proof used for Theorem 24.3 works. If the DFA has k states then for some $0 \le i < j \le k$, the DFA gives the same answer for $0^{\bullet i}1^{\bullet i}$ and $0^{\bullet i}1^{\bullet j}$, but the first is balanced and the second is not, a contradiction.

Exercise 24.12.

(a) The start state is q_0. It is an accept state if the input string is empty.

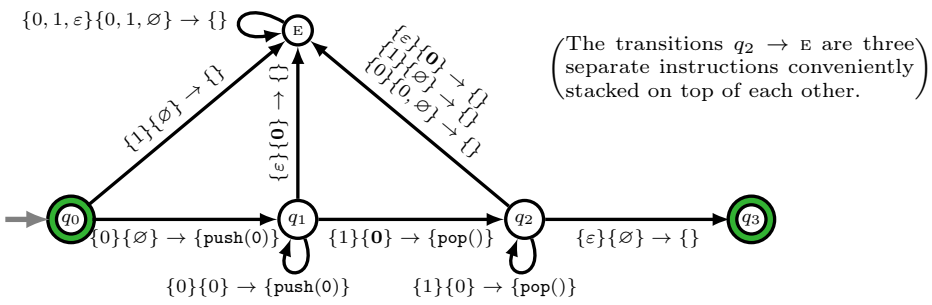
$q_0 \to$ E: If the first bit is 1, transition to error, doing nothing to the stack.

$q_0 \to q_1$: If the first bit is 0, push it onto the stack and transition to q_1. (Step I.)

E $\to$ E: remain in the error state for any input $(0, 1, \varepsilon)$ and stack symbol $(0, 1, \varnothing)$, doing nothing to the stack. symbol. If the input is ε, the automaton stops and rejects.

$q_1 \to q_1$: if input is 0 and stack is 0, push 0 onto the stack and remain in q_1. (Step II.)

(b)



(c) Left of the head is the substring processed and to the right is the substring remaining. The stack is to the left of the state (the top of the stack is rightmost in black). Denote our PDA by M. The traces for the four strings are:

$\varnothing \,|\, q_0 \,|\, \triangleright 010\varepsilon$
$\overset{M}{\mapsto} \varnothing 0 \,|\, q_1 \,|\, 0\triangleright 10\varepsilon$
$\overset{M}{\mapsto} \varnothing \,|\, q_2 \,|\, 01\triangleright 0\varepsilon$
$\overset{M}{\mapsto} \varnothing \,|\, \text{E} \,|\, 010\triangleright\varepsilon$
$\overset{M}{\mapsto} \varnothing \,|\, \text{E} \,|\, 010\varepsilon\triangleright$
STOP, REJECT

$\varnothing \,|\, q_0 \,|\, \triangleright 00011\varepsilon$
$\overset{M}{\mapsto} \varnothing 0 \,|\, q_1 \,|\, 0\triangleright 0011\varepsilon$
$\overset{M}{\mapsto} \varnothing 00 \,|\, q_1 \,|\, 00\triangleright 011\varepsilon$
$\overset{M}{\mapsto} \varnothing 000 \,|\, q_1 \,|\, 000\triangleright 11\varepsilon$
$\overset{M}{\mapsto} \varnothing 00 \,|\, q_2 \,|\, 0001\triangleright 1\varepsilon$
$\overset{M}{\mapsto} \varnothing 0 \,|\, q_2 \,|\, 00011\triangleright\varepsilon$
$\overset{M}{\mapsto} \varnothing 0 \,|\, \text{E} \,|\, 00011\varepsilon\triangleright$
STOP, REJECT

$\varnothing \,|\, q_0 \,|\, \triangleright 0011\varepsilon$
$\overset{M}{\mapsto} \varnothing 0 \,|\, q_1 \,|\, 0\triangleright 011\varepsilon$
$\overset{M}{\mapsto} \varnothing 00 \,|\, q_1 \,|\, 00\triangleright 11\varepsilon$
$\overset{M}{\mapsto} \varnothing 0 \,|\, q_1 \,|\, 001\triangleright 1\varepsilon$
$\overset{M}{\mapsto} \varnothing \,|\, q_2 \,|\, 0011\triangleright\varepsilon$
$\overset{M}{\mapsto} \varnothing \,|\, q_3 \,|\, 0011\varepsilon\triangleright$
STOP, ACCEPT

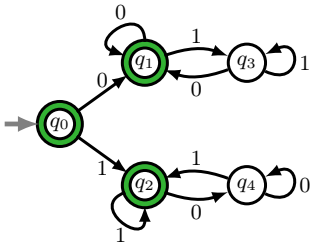
$\varnothing \,|\, q_0 \,|\, \triangleright 00111\varepsilon$
$\overset{M}{\mapsto} \varnothing 0 \,|\, q_1 \,|\, 0\triangleright 0111\varepsilon$
$\overset{M}{\mapsto} \varnothing 00 \,|\, q_1 \,|\, 00\triangleright 111\varepsilon$
$\overset{M}{\mapsto} \varnothing 0 \,|\, q_1 \,|\, 001\triangleright 11\varepsilon$
$\overset{M}{\mapsto} \varnothing \,|\, q_2 \,|\, 0011\triangleright 1\varepsilon$
$\overset{M}{\mapsto} \varnothing \,|\, \text{E} \,|\, 00111\triangleright\varepsilon$
$\overset{M}{\mapsto} \varnothing \,|\, \text{E} \,|\, 00111\varepsilon\triangleright$
STOP, REJECT

(d) The PDA is mechanically plausible. The only concern is the infinite stack to process inputs like $0^{\bullet n}1^{\bullet n}$ for arbitrarily large n. In practice, ofcourse, we can only implement a PDA with a finite stack memory.

Exercise 24.13.

(a) No DFA exists for $(01)^{\bullet n}(10)^{\bullet n}$. This is similar to $0^{\bullet n}1^{\bullet n}$. Suppose the language is solved by a DFA with k states, and consider its state after processing $(01)^{\bullet 0}$, $(01)^{\bullet 1}$, …, $(01)^{\bullet k}$. By pigeonhole, at least two of these states for $(01)^{\bullet i}$ and $(01)^{\bullet j}$ with $i < j$ must be the same, say q. The strings $(01)^{\bullet i}(10)^{\bullet i}$ and $(01)^{\bullet j}(10)^{\bullet i}$ pose a problem for this DFA. The final states must be the same. However, the DFA must accept one string and reject the other. This contradiction implies that such a DFA does not exist.

(b) $\mathcal{L}_2$ is actually quite simple though it looks superficially similar to $\mathcal{L}_1$. If the string starts with 0, we are okay unless a 1 appears in which case a 01 substring has appeared. To balance this 01, another 0 must appear to generate a 10 substring, at which point we are back to begining situation where the string started with a 0. This means if the string starts with 0, it must end with 0. Similarly, if it starts with 1, it must end with 1. We leave it to the reader to prove by induction that a string is in $\mathcal{L}_2$ iff it starts and ends in the same bit. Checking if the start and end bit are the same is actually quite easy to do with a DFA.



Chapter 25

Pop Quiz 25.1. This CFL is $\{0^{\bullet n}1^{\bullet n} \mid n \geq 0\}$. (a) $S \overset{1:}{\Rightarrow} T_0A \overset{3:}{\Rightarrow} T_0XT_1 \overset{2:}{\Rightarrow} T_0T_0T_1T_1 \overset{4:}{\Rightarrow} T_00T_1T_1 \overset{4:}{\Rightarrow} 00T_1T_1 \overset{5:}{\Rightarrow} 001T_1 \overset{5:}{\Rightarrow} 0011$ (b) impossible (c) impossible (d) impossible. Starting from X: $\{0^{\bullet n}1^{\bullet n} \mid n > 0\}$. Starting from A: $\{0^{\bullet n}1^{\bullet n+1} \mid n > 0\}$.

Pop Quiz 25.2. $S \overset{1:}{\Rightarrow}$ `<phrase><verb>` $\overset{5:}{\Rightarrow}$ `<phrase>`runs.␣S $\overset{2:}{\Rightarrow}$ `<article><noun>`runs.␣S
$\overset{3:}{\Rightarrow}$ A␣`<noun>`runs.␣S $\overset{4:}{\Rightarrow}$ A␣cat␣runs.␣S $\overset{1:}{\Rightarrow}$ A␣cat␣runs.␣`<phrase><verb>`
$\overset{5:}{\Rightarrow}$ A␣cat␣runs.␣`<phrase>`walks. $\overset{2:}{\Rightarrow}$ A␣cat␣runs.␣`<article><noun>`walks.
$\overset{3:}{\Rightarrow}$ A␣cat␣runs.␣The␣`<noun>`walks. $\overset{4:}{\Rightarrow}$ A␣cat␣runs.␣The␣dog␣walks.

Exercise 25.3.

(a) (i) $S \overset{1:}{\Rightarrow}$ `<stmt>;`S $\overset{2:}{\Rightarrow}$ `<declare>;`S $\overset{3:}{\Rightarrow}$ `int␣<variable>;`S $\overset{7:}{\Rightarrow}$ `int␣x;`S
$\overset{1:}{\Rightarrow}$ `int␣x;<stmt>;`S $\overset{2:}{\Rightarrow}$ `int␣x;<declare>;`S $\overset{3:}{\Rightarrow}$ `int␣x;int␣<variable>;`S
$\overset{7:}{\Rightarrow}$ `int␣x;int␣x<variable>;`S $\overset{7:}{\Rightarrow}$ `int␣x;int␣xx;`S
$\overset{1:}{\Rightarrow}$ `int␣x;int␣xx;<stmt>;`S $\overset{2:}{\Rightarrow}$ `int␣x;int␣xx;<assign>;`S
$\overset{4:}{\Rightarrow}$ `int␣x;int␣xx;<variable>=<integer>;`S $\overset{7:}{\Rightarrow}$ `int␣x;int␣xx;x=<integer>;`S
$\overset{5:}{\Rightarrow}$ `int␣x;int␣xx;x=<integer><digit>;`S $\overset{6:}{\Rightarrow}$ `int␣x;int␣xx;x=<integer>2;`S
$\overset{5:}{\Rightarrow}$ `int␣x;int␣xx;x=<digit>2;`S $\overset{6:}{\Rightarrow}$ `int␣x;int␣xx;x=22;`S
$\overset{1:}{\Rightarrow}$ `int␣x;int␣xx;x=22;<stmt>;` $\overset{2:}{\Rightarrow}$ `int␣x;int␣xx;x=22;<assign>;`
$\overset{4:}{\Rightarrow}$ `int␣x;int␣xx;x=22;<variable>=<integer>;`
$\overset{7:}{\Rightarrow}$ `int␣x;int␣xx;x=22;x<variable>=<integer>;`
$\overset{7:}{\Rightarrow}$ `int␣x;int␣xx;x=22;xx=<integer>;`
$\overset{5:}{\Rightarrow}$ `int␣x;int␣xx;x=22;xx=<digit>;` $\overset{6:}{\Rightarrow}$ `int␣x;int␣xx;x=22;xx=8;`

Long and tedious, but that's what it takes to derive non-trivial strings in non-trivial grammars.

(ii) $S \overset{1:}{\Rightarrow}$ `<stmt>;`S $\overset{2:}{\Rightarrow}$ `<assign>;`S $\overset{4:}{\Rightarrow}$ `<variable>=<integer>;`S $\overset{7:}{\Rightarrow}$ `x=<integer>;`S
$\overset{5:}{\Rightarrow}$ `x=<digit>;`S $\overset{6:}{\Rightarrow}$ `x=8;`S
$\overset{1:}{\Rightarrow}$ `x=8;<stmt>;` $\overset{2:}{\Rightarrow}$ `x=8;<declare>;` $\overset{3:}{\Rightarrow}$ `x=8;int␣<variable>;` $\overset{7:}{\Rightarrow}$ `x=8;int␣x;`

(iii) $S \overset{1:}{\Rightarrow}$ `<stmt>;`$S \overset{2:}{\Rightarrow}$ `<declare>;`$S \overset{3:}{\Rightarrow}$ `int␣<variable>;`$S \overset{7:}{\Rightarrow}$ `int␣x;`S
$\overset{1:}{\Rightarrow}$ `int␣x;<stmt>;` $\overset{2:}{\Rightarrow}$ `int␣x;<assign>;` $\overset{4:}{\Rightarrow}$ `int␣x;<variable>=<integer>;`
$\overset{7:}{\Rightarrow}$ `int␣x;x<variable>=<integer>;` $\overset{7:}{\Rightarrow}$ `int␣x;xx=<integer>;`
$\overset{5:}{\Rightarrow}$ `int␣x;xx=<digit>;` $\overset{6:}{\Rightarrow}$ `int␣x;xx=8;`

(b) (i) semantically correct. (ii) variable used before declared. (iii) variable used is not declared.

(c) Add the white space variable in the rule for S and a new rule to create the white space:

```
1:           S → <stmt>;WS | <stmt>;
2:     <stmt> → <assign> | <declare>
3:  <declare> → int␣<variable>
4:   <assign> → <variable>=<integer>
5:  <integer> → <integer><digit> | <digit>
6:    <digit> → 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9
7: <variable> → x | x<variable>
8:          W → WW | ε | ␣ | \n
```

Pop Quiz 25.4. Let w be a non-empty string in $\mathcal{L}_{\text{equal}}$. Either w starts with 0 or with 1. Consider the case 0, $w = 0v$. Since w has an equal number of 0's and 1's, v has more 1's than 0's. Therefore some prefix of v (for example v itself) has more 1's than 0's. By the well-ordering principle, there is a shortest prefix of v that has more 1's than 0's. Call this prefix v_1, $v = v_1 w_2$ and v_1 must end in 1 otherwise some shorter prefix has more 1's than 0's. Therefore, $v_1 = w_1 1$ and w_1 cannot have more 1's than 0's, since v_1 is the shortest prefix with this property. Therefore, w_1 must have an equal number of 1's than 0's, because otherwise v_1 would not have *more* 1's. We have proved:

$$w = 0v = 0v_1 w_2 = 0w_1 1 w_2,$$

where w_1 has an equal number of 1's and 0's. Since w has an equal number of 1's and 0's, this means that w_2 must also have an equal number of 1's and 0's. The case where w starts with 1 uses analogous reasoning.

Exercise 25.5.

(a) (i) 1: $S \to \varepsilon \mid 1S$ (Every non-empty string in $\mathcal{L}$ is of the form $1w$ where $w \in \mathcal{L}$.)
(ii) By induction on the length of the derivation. The base cases are $S \Rightarrow \varepsilon$ and $S \Rightarrow 1$. All other derivations start $S \Rightarrow 1S$ followed by a shorter derivation for the S on the RHS. For this shorter derivation, by the induction hypothesis the string derived is $1^{\bullet n}$ for $n \geq 0$ and so the full derivation fives $1^{\bullet n+1}$.
(iii) By induction on n: Suppose $S \overset{*}{\Rightarrow} 1^{\bullet n}$. Then, $S \Rightarrow 1S \overset{*}{\Rightarrow} 1 \bullet 1^{\bullet n}$ is a derivation of $1^{\bullet n+1}$.

(b) (i) 1: $S \to A1$
2: $A \to \varepsilon \mid 0 \mid 1 \mid AA$
(ii) All derivations start $S \Rightarrow A1$ followed any derivation from A. The result is a string in A followed by 1.
(iii) By induction on string-length, any string v can be derived from A. The base cases are $v = \varepsilon, 0, 1$. If $v = 0x$, then x is shorter and $A \overset{*}{\Rightarrow} x$ (induction hypothesis), so $A \Rightarrow AA \Rightarrow 0A \overset{*}{\Rightarrow} 0x$. Similarly if $v = 1x$. Therefore, any string of the form $v1$ can be derived as follows: $S \Rightarrow A1 \overset{*}{\Rightarrow} v1$ (derivation of v from A).

(c) (i) 1: $S \to A00A$
2: $A \to \varepsilon \mid 0 \mid 1 \mid AA$
(ii) All derivations start $S \Rightarrow A00A$ followed by a derivations from each A, therefore the final string contains 00 because it is $v00w$ where $A \overset{*}{\Rightarrow} v$ and $A \overset{*}{\Rightarrow} w$.
(iii) In (b) we showed that any string can be derived from A so any string of the form $v00w$ can be derived from S by $S \Rightarrow A00A \overset{*}{\Rightarrow} v00w$ (derivations of v and w from the A's).

(d) (i) 1: $S \to \varepsilon \mid 1S0$
(ii) Induction on the length of the derivation. Every derivation starts $S \Rightarrow 1S0$ followed by a shorter derivation on the RHS S, which by the induction hypothesis gives $1^{\bullet k}0^{\bullet k}$. Therefore the full derivation gives $1^{\bullet k+1}0^{\bullet k+1}$
(iii) Induction on string-length. Suppose $S \overset{*}{\Rightarrow} 1^{\bullet n}0^{\bullet n}$ then $S \Rightarrow 1S0 \overset{*}{\Rightarrow} 1 \bullet 1^{\bullet n}0^{\bullet n} \bullet 0$ is a derivation of $1^{\bullet n+1}0^{\bullet n+1}$.

(e) (i) 1: $S \to AB$ (S is composed of two types of strings, A and B)
2: $A \to \varepsilon \mid 1A0$ (A generates $1^{\bullet k}0^{\bullet k}$ as in part (e))
3: $B \to \varepsilon \mid 1B$ (B generates $1^{\bullet \ell}$ as in part (a))
(ii) S is a string derived from A followed by one derived from B. In (e,ii) we showed that all derivations from A yield $1^{\bullet k}0^{\bullet k}$. In (a,ii) we showed that all derivations from B yield $1^{\bullet \ell}$. So, all derivations from S yield $1^{\bullet k}0^{\bullet k}1^{\bullet \ell}$.
(iii) In (e,iii) we showed that every string of the form $1^{\bullet k}0^{\bullet k}$ can be derived from A. In (a,iii) we showed that every string of the form $1^{\bullet \ell}$ can be derived from B. Therefore every string of the form $1^{\bullet k}0^{\bullet k}1^{\bullet \ell}$ can be derived from S.

(f) (i) The basic palindromes are $\varepsilon, 0, 1$. All other palindromes either start and end in 0 (with a palindrome in between) or they start and end in 1 (with a palindrome in between). This observation suggests the grammar

1: $S \to \varepsilon \mid 0 \mid 1 \mid 0S0 \mid 1S1$

(ii) Induction on the length of the derivation. For the derivation, which starts $0S0$ (the same logic applies if it starts $1S1$), suppose ultimately that the middle S yields x (via a shorter derivation). By the induction hypothesis, x is palindrome, and so the final string $0x0$ is a palindrome because $(0x0)^{\mathrm{R}} = 0x^{\mathrm{R}}0 = 0x0$.
(iii) Induction on length. If w is a (non-basic) palindrome, $w = 0x0$ or $w = 1x1$ where x is shorter. Therefore $S \stackrel{*}{\Rightarrow} x$ by the induction hypothesis and $S \Rightarrow 0S0 \stackrel{*}{\Rightarrow} 0x0$ (or $S \Rightarrow 1S1 \stackrel{*}{\Rightarrow} 1x1$) is a derivation of w.

Exercise 25.6.

(a) $*0*$: 1: $S_0 \to A0A$
2: $A \to \varepsilon \mid 0 \mid 1 \mid AA$

$*1*$: 1: $S_1 \to B1B$
2: $B \to \varepsilon \mid 0 \mid 1 \mid BB$

Union ($*0*$ or $*1*$): 1: $S \to S_0 \mid S_1$
2: $S_0 \to A0A$
3: $A \to \varepsilon \mid 0 \mid 1 \mid AA$
4: $S_1 \to B1B$
5: $B \to \varepsilon \mid 0 \mid 1 \mid BB$

(b) $0^{\bullet k}1^{\bullet k+\ell}0^{\bullet \ell} = 0^{\bullet k}1^{\bullet k} \bullet 1^{\bullet \ell}0^{\bullet \ell}$, so $\mathcal{L}$ is the concatenation of $0^{\bullet k}1^{\bullet k}$ with $1^{\bullet \ell}0^{\bullet \ell}$.

$0^{\bullet k}1^{\bullet k}$: 1: $A \to \varepsilon \mid 0A1$

$1^{\bullet \ell}0^{\bullet \ell}$: 1: $B \to \varepsilon \mid 1B0$

Concatenation $0^{\bullet k}1^{\bullet k+\ell}0^{\bullet \ell}$: 1: $S \to AB$
2: $A \to \varepsilon \mid 0A1$
3: $B \to \varepsilon \mid 1B0$

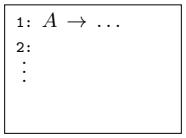
(c) A CFG for $\mathcal{L}$ on the right with start variable A, we wish to construct a grammar for $\mathcal{L}^*$. The idea is to first construct $A^{\bullet i}$ for $i \geq 0$ and use the grammar for $\mathcal{L}$ to independently derive each A into a string from $\mathcal{L}$. A CFG for $A^{\bullet i}$ is

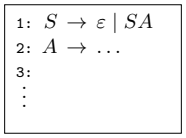
$$1\text{: } S \to \varepsilon \mid SA.$$

In the grammar on the right (bottom), the first rule generates a concatenation of A's and the remaining rules from $\mathcal{L}$ independently derive each A into a string from $\mathcal{L}$. In our case the grammar for $\mathcal{L}$ is 1: $A \to \varepsilon \mid 0A1$, therefore the grammar for $\mathcal{L}^*$ is

$$\begin{array}{l} 1\text{: } S \to \varepsilon \mid SA \ , \\ 2\text{: } A \to \varepsilon \mid 0A1 \end{array}$$

You should derive some strings within this grammar and verify they are all in $\mathcal{L}^*$.





(d) We observe that strings not containing 00 are any concatenation of the strings in $\{1, 01\}$ terminated by 0 or ε. That is, $\mathcal{L} = \{1, 01\}^* \bullet \{\varepsilon, 0\}$. The set $\{1, 01\}$ is generated by 1: $A \to 1 \mid 01$ and the set $\{\varepsilon, 0\}$ is generated by 1: $B \to \varepsilon \mid 0$. Therefore,

$\{1, 01\}^*$: 1: $X \to \varepsilon \mid XA$
2: $A \to 1 \mid 01$

$\{1, 01\}^* \bullet \{\varepsilon, 0\}$: 1: $S \to XB$
2: $X \to \varepsilon \mid XA$
3: $A \to 1 \mid 01$
4: $B \to \varepsilon \mid 0$

We can also use the recursive approach to derive the CFG. Let S represent a string in $\mathcal{L}$. Either S is empty or begins with 1 or 0. If S begins with 1, then it can be followed by any string in $\mathcal{L}$, generically represented by S. If S starts with 0, then it either ends or follows with a 1 and then any string in S. Therefore a grammar for $\mathcal{L}$ is

$$1\text{: } S \to \varepsilon \mid 0 \mid 1S \mid 01S$$

For yet another approach to constructing a CFG for $\mathcal{L}$, see Problem 25.12

Exercise 25.7.

(a) Let us walk through a systematic procedure for converting a CFG into Chomsky Normal Form. Our grammar is 1: $S \to \varepsilon \mid 0S1S \mid 1S0S$. First, we make sure that the start variable does not appear on the RHS of any rule. To do this, we change the start variable and add a new rule from the new start variable to the old one:

$$\begin{array}{l} 1\text{: } S \to X \\ 2\text{: } X \to \varepsilon \mid 0X1X \mid 1X0X \end{array}$$

This trivial change does not alter the derivable strings. All derivations start $S \to X$ and proceed as before. Now remove all rules which take a variable to ε: if a variable A may transition to ε, remove that transition and replace every occurrence of the variable on the RHS of a rule with a new instance of the rule that replaces A with ε. Note that *every* instance of A must be replaced "independently". For example $X \to 0X1X$ gets replaced by $X \to 0X1X \mid 01X \mid 0X1 \mid 01$, which captures all possible ways of replacing the X's with ε. Our grammar becomes:

$$\begin{array}{l} 1\text{: } S \to \varepsilon \mid X \\ 2\text{: } X \to 0X1X \mid 01X \mid 0X1 \mid 01 \mid 1X0X \mid 10X \mid 1X0 \mid 10 \end{array}$$

Now replace each terminal with a corresponding terminal variable (for example T_0 for 0 and T_1 for 1) and add a rule from each terminal variable to its corresponding terminal:

$$\begin{array}{ll}
1\text{:} & S \to \varepsilon \mid X \\
2\text{:} & X \to T_0XT_1X \mid T_0T_1X \mid T_0XT_1 \mid T_0T_1 \mid T_1XT_0X \mid T_1T_0X \mid T_1XT_0 \mid T_1T_0 \\
3\text{:} & T_0 \to 0 \\
4\text{:} & T_1 \to 1
\end{array}$$

Every rule (except for the rules to terminals) now has the form

$$\texttt{<variable>} \to \text{string of } \texttt{<variables>}.$$

Now reduce rules with more than two variables on the RHS. The rule $A_1 \to A_2A_3 \cdots A_k$ becomes

$$A_1 \to A_2B_1; \qquad B_1 \to A_3B_2; \qquad B_2 \to A_4B_3; \qquad \cdots \qquad B_{k-2} \to A_{k-1}A_k$$

When you combine all the rules above, it becomes the single rule $A_1 \to A_2A_3 \cdots A_k$. In general, you can pick any consecutive variables on the RHS and reduce it to a new variable, while providing a new rule from the new variable to the pair. For our grammar let us use $A_0 \to T_0X$ and $A_1 \to T_1X$, then the rule for X becomes

$$X \to T_0T_1 \mid T_1T_0 \mid A_0A_1 \mid T_0A_1 \mid A_0T_1 \mid A_1A_0 \mid T_1A_0 \mid A_1T_0$$

Our grammar becomes

$$\begin{array}{ll}
1\text{:} & S \to \varepsilon \mid X \\
2\text{:} & X \to T_0T_1 \mid T_1T_0 \mid A_0A_1 \mid T_0A_1 \mid A_0T_1 \mid A_1A_0 \mid T_1A_0 \mid A_1T_0 \\
3\text{:} & A_0 \to T_0X \\
4\text{:} & A_1 \to T_1X \\
5\text{:} & T_0 \to 0 \\
6\text{:} & T_1 \to 1
\end{array}$$

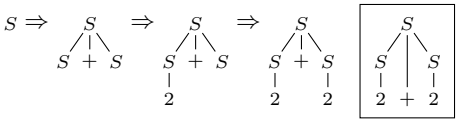
Finally, for rules that take a variable to a single variable (e.g. $S \to X$), replace the variable on the RHS by the entire rule for that variable. Our grammar in Chomsky Normal Form is

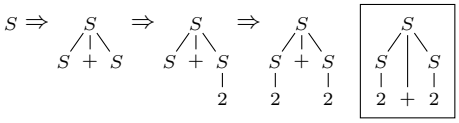
$$\begin{array}{ll}
1\text{:} & S \to \varepsilon \mid T_0T_1 \mid T_1T_0 \mid A_0A_1 \mid T_0A_1 \mid A_0T_1 \mid A_1A_0 \mid T_1A_0 \mid A_1T_0 \\
2\text{:} & X \to T_0T_1 \mid T_1T_0 \mid A_0A_1 \mid T_0A_1 \mid A_0T_1 \mid A_1A_0 \mid T_1A_0 \mid A_1T_0 \\
3\text{:} & A_0 \to T_0X \\
4\text{:} & A_1 \to T_1X \\
5\text{:} & T_0 \to 0 \\
6\text{:} & T_1 \to 1
\end{array}$$

(b) Every application of a production rule increases the length of the hybrid string by 1 (starting from S of length 1). Every application of a terminal rule keeps the length of the hybrid string fixed. Since the final string has length n, this means there must be $n-1$ steps which increase the length by 1 and n steps which convert variables to terminal for a total of $2n-1$ steps. This argument works because no rule decreases the length of the hybrid string.

(c) For a grammar in Chomsky Normal Form and an input string w of length n, try all derivations of length $2n-1$. If w resulted from one of these (possibly exponentially many) derivations, then $w \in \mathcal{L}$, otherwise $w \notin \mathcal{L}$. Note that this is a relatively inefficient procedure to test for membership in a CFL, but a finite one.

Pop Quiz 25.8. Though the derivations are different, the final parse trees (boxed beside each derivation) are identical.

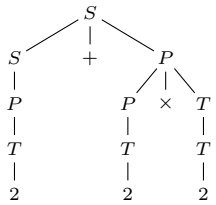




Exercise 25.9.

(a) Change the order of some of the transitions to get a different derivation.

$$\begin{aligned}
S &\Rightarrow S + P \\
&\Rightarrow P + P \\
&\Rightarrow T + P \\
&\Rightarrow T + P \times T \\
&\Rightarrow T + T \times T \\
&\overset{*}{\Rightarrow} 2 + 2 \times 2
\end{aligned}$$



We get a different derivation but the same parse tree.

(b) Grammar in (25.5)

$$\begin{aligned} S &\Rightarrow P \Rightarrow P \times T \Rightarrow T \times T \Rightarrow (S) \times T \Rightarrow (S) \times (S) \Rightarrow (S + P) \times (S) \Rightarrow (P + P) \times (S) \Rightarrow (T + P) \times (S) \\ &\Rightarrow (T + T) \times (S) \Rightarrow (T + T) \times (S + P) \Rightarrow (T + T) \times (S + P \times T) \Rightarrow (T + T) \times (P + P \times T) \\ &\Rightarrow (T + T) \times (T + P \times T) \Rightarrow (T + T) \times (T + T \times T) \\ &\overset{*}{\Rightarrow} (2 + 2) \times (2 + 2 \times 2) \end{aligned}$$

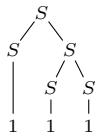
Grammar in (25.3)

$$\begin{aligned} S &\Rightarrow S \times S \Rightarrow (S) \times S \Rightarrow (S) \times (S) \Rightarrow (S + S) \times (S) \Rightarrow (S + S) \times (S + S) \Rightarrow (S + S) \times (S + S \times S) \\ &\overset{*}{\Rightarrow} (2 + 2) \times (2 + 2 \times 2) \end{aligned}$$

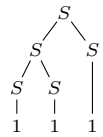
At the end of both derivations, every variable transitions to 2. The derivation for the unambiguous grammar in (25.5) is much longer, the price of unambiguous parse trees (additional information is embedded in the rules).

(c) (i) For emphasis we give 3 different derivations with different parse trees.

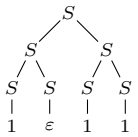
$S \Rightarrow \boldsymbol{S}S \Rightarrow S\boldsymbol{S} \overset{*}{\Rightarrow} 111$



$S \Rightarrow \boldsymbol{S}S \Rightarrow SSS \overset{*}{\Rightarrow} 111$



$S \Rightarrow S\boldsymbol{S} \Rightarrow \boldsymbol{S}SS \Rightarrow SSSS \overset{*}{\Rightarrow} 1\varepsilon 11$



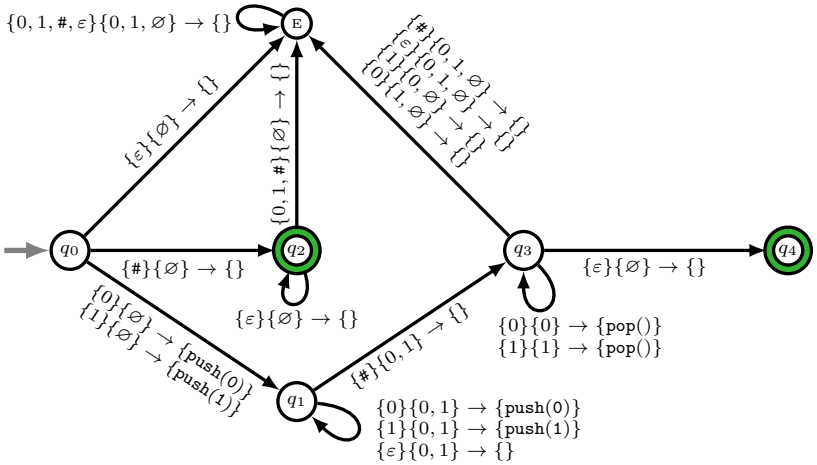
At the end of each derivation, every variable transitions to a terminal in some order. In case of ambiguity we identify in bold the variable that is transitioning.

(ii) To remove the ambiguity, we give just one way to add a 1 to the string, $S \to \varepsilon \mid 1S$.

Pop Quiz 25.10. $S \Rightarrow 0S0 \Rightarrow 01S10 \Rightarrow 011S110 \Rightarrow 011\#110$

Exercise 25.11.

(a)



(b) Left of the head is the substring processed and to the right the substring remaining. The stack is to the left of the state (the top of the stack is rightmost in black). Denote our PDA by M. The traces for the strings are:

$$\begin{aligned} &\varnothing \mid q_0 \mid \triangleright 0110\varepsilon \\ \overset{M}{\mapsto}\ &\varnothing 0 \mid q_1 \mid 0\triangleright 110\varepsilon \\ \overset{M}{\mapsto}\ &\varnothing 01 \mid q_1 \mid 01\triangleright 10\varepsilon \\ \overset{M}{\mapsto}\ &\varnothing 011 \mid q_1 \mid 011\triangleright 0\varepsilon \\ \overset{M}{\mapsto}\ &\varnothing 0110 \mid q_1 \mid 0110\triangleright\varepsilon \\ \overset{M}{\mapsto}\ &\varnothing 0110 \mid q_1 \mid 0110\varepsilon\triangleright \end{aligned}$$

STOP, REJECT

$$\begin{aligned} &\varnothing \mid q_0 \mid \triangleright 01\#01\varepsilon \\ \overset{M}{\mapsto}\ &\varnothing 0 \mid q_1 \mid 0\triangleright 1\#01\varepsilon \\ \overset{M}{\mapsto}\ &\varnothing 01 \mid q_1 \mid 01\triangleright \#01\varepsilon \\ \overset{M}{\mapsto}\ &\varnothing 01 \mid q_3 \mid 01\#\triangleright 01\varepsilon \\ \overset{M}{\mapsto}\ &\varnothing 01 \mid \mathrm{E} \mid 01\#0\triangleright 1\varepsilon \\ \overset{M}{\mapsto}\ &\varnothing 01 \mid \mathrm{E} \mid 01\#01\triangleright\varepsilon \\ \overset{M}{\mapsto}\ &\varnothing 01 \mid \mathrm{E} \mid 01\#01\varepsilon\triangleright \end{aligned}$$

STOP, REJECT

$$\begin{aligned} &\varnothing \mid q_0 \mid \triangleright 01\#10\varepsilon \\ \overset{M}{\mapsto}\ &\varnothing 0 \mid q_1 \mid 0\triangleright 1\#10\varepsilon \\ \overset{M}{\mapsto}\ &\varnothing 01 \mid q_1 \mid 01\triangleright \#10\varepsilon \\ \overset{M}{\mapsto}\ &\varnothing 01 \mid q_3 \mid 01\#\triangleright 10\varepsilon \\ \overset{M}{\mapsto}\ &\varnothing 0 \mid q_3 \mid 01\#1\triangleright 0\varepsilon \\ \overset{M}{\mapsto}\ &\varnothing \mid q_3 \mid 01\#10\triangleright\varepsilon \\ \overset{M}{\mapsto}\ &\varnothing \mid q_4 \mid 01\#10\varepsilon\triangleright \end{aligned}$$

STOP, ACCEPT

Exercise 25.12.

(a) $\mathcal{L}_1$ is the concatenation of $0^{\bullet n}1^{\bullet n}$ (context free, $S \to \epsilon \mid 0S1$) with $0^{\bullet m}$ (context free, $S \to \epsilon \mid 0S$). Since CFLs are closed under concatenation, $\mathcal{L}_1$ is a CFL. Similarly, $\mathcal{L}_2$ is the concatenation of $0^{\bullet m}$ with $0^{\bullet n}1^{\bullet n}$ and also a CFL.

(b) $\mathcal{L}_1 \cap \mathcal{L}_2 = \{0^{\bullet n}1^{\bullet n}0^{\bullet n} \mid n \geq 0\} = \mathcal{L}$. If CFLs are closed under intersection, then, since $\mathcal{L}_1$ and $\mathcal{L}_2$ are CFLs, $\mathcal{L} = \mathcal{L}_1 \cap \mathcal{L}_2$ is a CFL. This contradicts $\mathcal{L}$ not being a CFL. Therefore, CFLs are *not* closed under intersection.

(c) Assume CFLs are closed under complement. So, $\overline{\mathcal{L}_1}$ and $\overline{\mathcal{L}_2}$ are CFLs. CFLs are closed under union, so $\overline{\mathcal{L}_1} \cup \overline{\mathcal{L}_2}$ is a CFL. This means $\overline{\overline{\mathcal{L}_1} \cup \overline{\mathcal{L}_2}}$ is a CFL (closure under complement). But

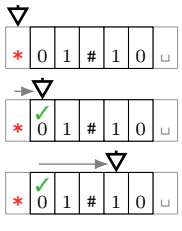
$$\overline{\overline{\mathcal{L}_1} \cup \overline{\mathcal{L}_2}} = \overline{\overline{\mathcal{L}_1}} \cap \overline{\overline{\mathcal{L}_2}} = \mathcal{L}_1 \cap \mathcal{L}_2 \ (= \mathcal{L}).$$

(The first step uses $\overline{A \cup B} = \overline{A} \cap \overline{B}$.) Since $\mathcal{L}$ is not a CFL, CFLs are *not* closed under complement. (Note, we have proved, more generally, that closure under union and complement implies closure under intersection.)

Chapter 26

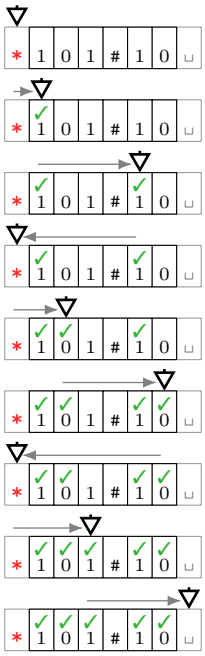
Pop Quiz 26.1. On 0110, the TM halts with (NO) at step 1 because there is no # in the input.

01#10



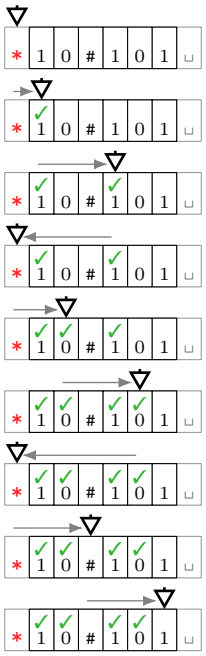
HALT, (NO)

101#10



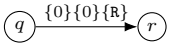
HALT, (NO)

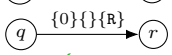
10#101

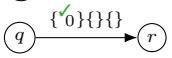


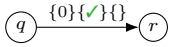
HALT, (NO)

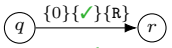
Pop Quiz 26.2.

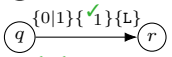
(a)  From q if you read 0, transition to r, write 0 and move right.

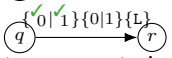
(b)  From q if you read 0, transition to r, and move right.

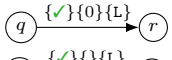
(c)  From q if you read marked 0, transition to r.

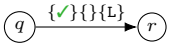
(d)  From q if you read 0, mark it and transition to r.

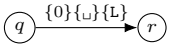
(e)  From q if you read 0, mark it, transition to r and move right.

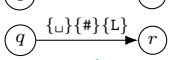
(f)  From q if you read 0 or 1, write marked 1, transition to r and move left.

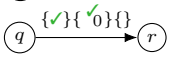
(g)  From q unmark a marked bit, transition to r and move left. We are being lazy. There are really two separate instructions, which we combined into a single instruction.

(h)  From q if marked, write 0 (unmarked), transition to r and move left.

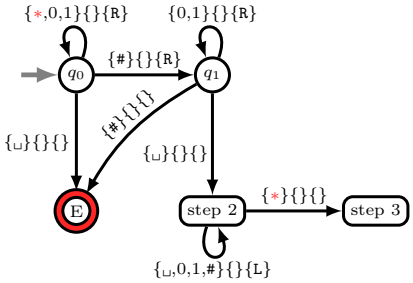
(i)  From q if marked, transition to r and move left.

(j)  From q if 0, erase, transition to r and move left.

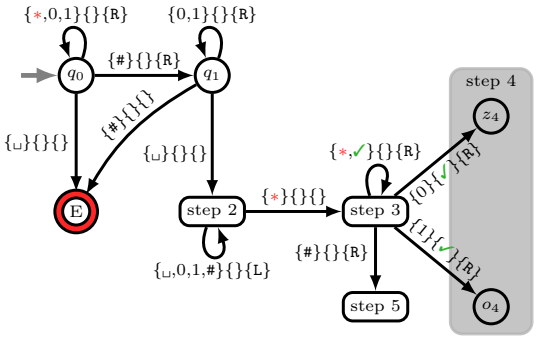
(k)  From q if blank, write #, transition to r and move left.

(l)  From q if marked, write marked 0 and transition to r.

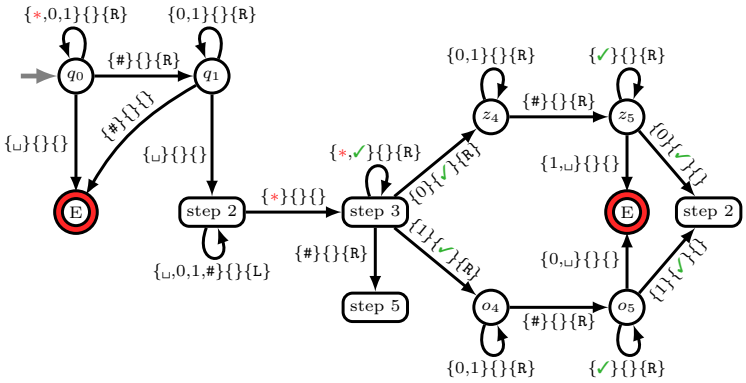
Pop Quiz 26.3. The error state is a halting state, so there are no more transitions. To combine the automata, simply identify the step 2 states in the automata for Step 1 and Step 2, and "snap" the automata together by merging the step 2 states. The result is shown on the right.



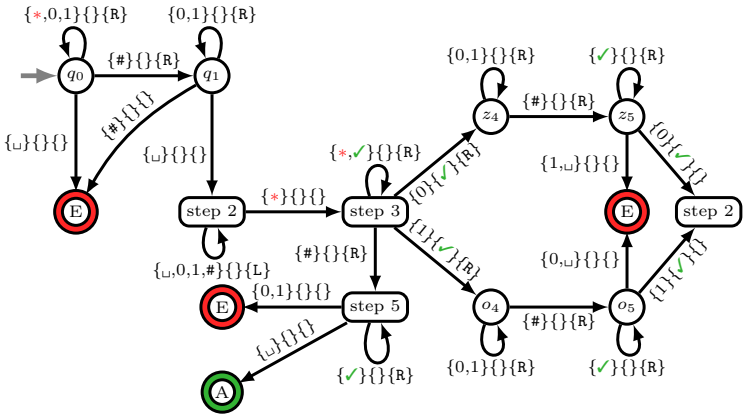
Pop Quiz 26.4. At the end of each step the machine transitions to a success state which is the starting point for the next step. Merging the automaton from the previous pop quiz with the automaton for step 3 at the state step 3 gives



Merging the states z_4 and o_4 with the step-4 machine gives



Filling in step 5 gives the final Turing machine.



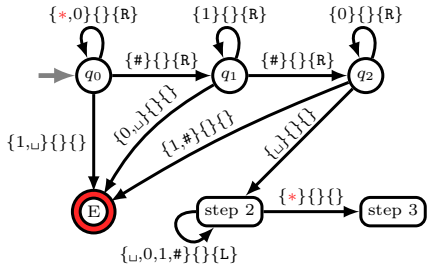
(a) $\to q_0 \to q_0 \to q_0 \to q_0 \to q_1 \to q_1 \to q_1$
$\to$ step 2 $\to$ step 2 $\to$ step 2 $\to$ step 2 $\to$ step 2 $\to$ step 2 $\to$ step 2
$\to$ step 3 $\to$ step 3 $\to z_4 \to z_4 \to z_5 \to$ step 2 $\to$ step 2 $\to$ step 2 $\to$ step 2 $\to$ step 2
$\to$ step 3 $\to$ step 3 $\to$ step 3 $\to o_4 \to o_5 \to o_5$
$\to$ step 2 $\to$ step 2 $\to$ step 2 $\to$ step 2 $\to$ step 2 $\to$ step 2
$\to$ step 3 $\to$ step 3 $\to$ step 3 $\to$ step 3 $\to$ step 5 $\to$ step 5 $\to$ step 5 $\to$ A

(b) $\to q_0 \to q_0 \to q_0 \to q_0 \to q_1 \to q_1 \to q_1$
$\to$ step 2 $\to$ step 2 $\to$ step 2 $\to$ step 2 $\to$ step 2 $\to$ step 2 $\to$ step 2
$\to$ step 3 $\to$ step 3 $\to z_4 \to z_4 \to z_5 \to$ E

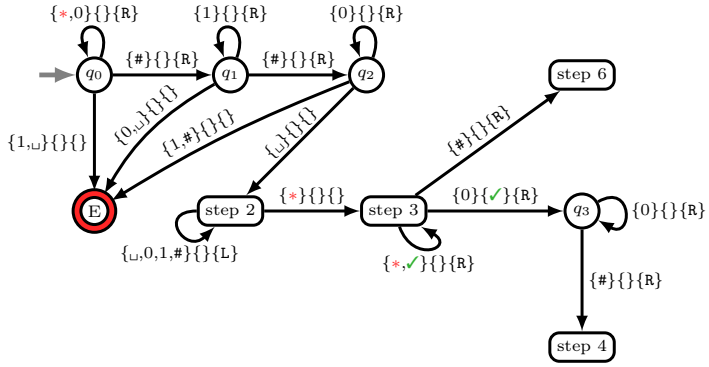
(c) $\to q_0 \to q_0 \to q_0 \to q_1 \to q_1 \to q_1$
$\to$ step 2 $\to$ step 2 $\to$ step 2 $\to$ step 2 $\to$ step 2 $\to$ step 2 $\to$ step 3 $\to$ step 3 $\to z_4 \to z_5$
$\to$ step 2 $\to$ step 2 $\to$ step 2 $\to$ step 2 $\to$ step 3 $\to$ step 3 $\to$ step 5 $\to$ step 5 $\to$ E

(d) $\to q_0 \to q_0 \to q_0 \to q_0 \to q_1 \to q_1$
$\to$ step 2 $\to$ step 2 $\to$ step 2 $\to$ step 2 $\to$ step 2 $\to$ step 2 $\to$ step 3 $\to$ step 3
$\to z_4 \to z_4 \to z_5 \to$ step 2 $\to$ step 2 $\to$ step 2 $\to$ step 2 $\to$ step 2
$\to$ step 3 $\to$ step 3 $\to$ step 3 $\to o_4 \to o_5 \to o_5 \to$ E

Exercise 26.5. Step 1 and 2 are very similar to our Turing machine which solved $w\#w$. Instead, we are now looking for two #'s and a specific format of 0's and 1's. A DFA solves this problem, ending in step 3 if it succeeds.

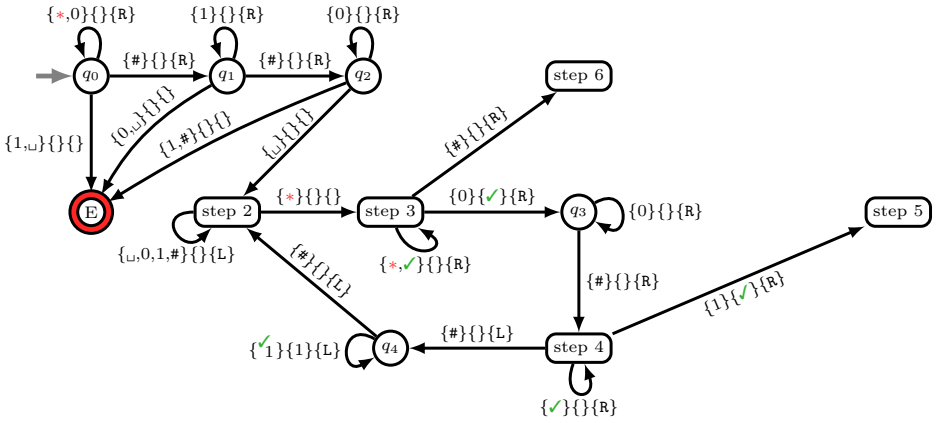


In Step 3 you are looking for the first unmarked 0; if you find it, mark it and move to #:

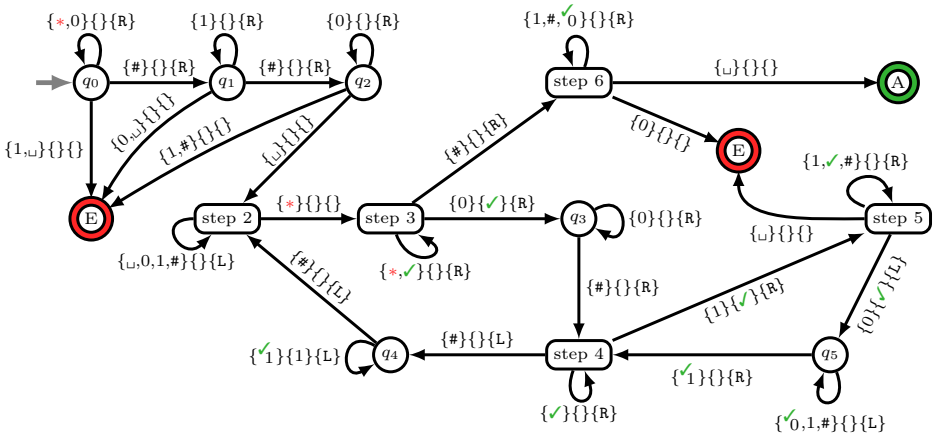


Note, in state step 3 we did not show what to do if the input is 1; and in state q_3 we did not show what to do for 1

and ␣. This is because the TM already verified the input format so a 1 or ␣ is not possible. Now for step 4.

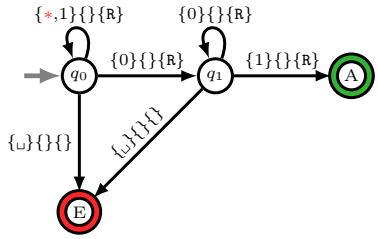


(State q_4 is responsible for moving right while unmarking the 1's.) In step 6 you are just checking for no unmarked right 0. In step 5 you are moving right to mark a 0. We implement both steps together. The final TM is:



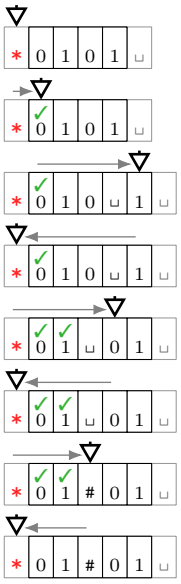
Exercise 26.6.

(a) Using a Turing machine for a regular language is using a sledgehammer on a thumb-tack. Our TM is a glorified DFA:



(b) A simple solution inserts # between the two w's and uses the Turing machine for $w\#w$.

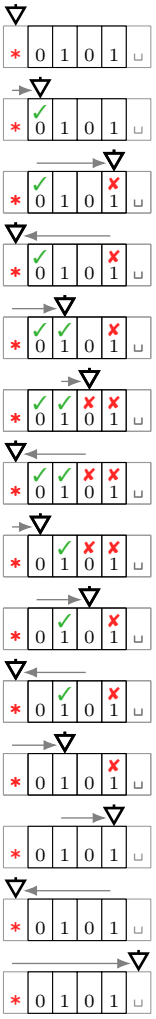
1: If the first symbol is ␣, ACCEPT (empty input).
2: Return to $*$.
3: Move right to the first unmarked bit and mark it.
    If you come to ␣ (equal number of unmarked bits right of ␣):
        mark it with #, return to $*$, unmarking any marked bits, and GOTO Step 5.
4: Move right to the first unmarked bit before ␣.
    If none exists (odd-length string) REJECT.
    Erase and copy the bit to the blank on its right; GOTO Step 2.
5: Use the Turing machine that solves $w\#w$.
    ACCEPT or REJECT using the output of this Turing machine.



On the right is the Turing machine in action up to the point where it invokes the Turing machine that solves $w\#w$. The entire purpose of this Turing machine is to insert the punctuation character at the midpoint of the input, and can be viewed as a preprocessing machine which reconfigures the input into a format that be used by some other Turing machine. This concept should be familiar to computer scientists: using someone else's program to solve a task, but reconfiguring your input so that their program will accept the input. This approach is modular by leads to program (Turing machine) bloat.

Our second approach directly solves ww which gives a more compact Turing machine.

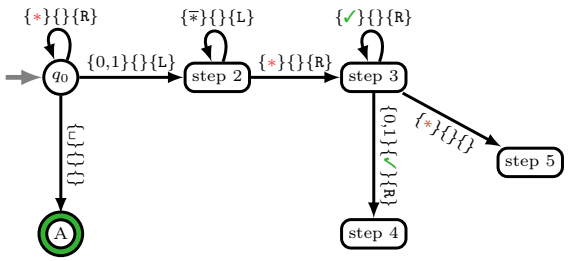
1: If the first symbol is ␣, ACCEPT (empty input).
2: Return to $*$.
`// Mark the first half with ✓ and the second with ✘`
3: Move right to the *first* unmarked bit and mark it ✓.
    If none exists (you come to ✘), GOTO Step 5.
4: Move right to the *last* unmarked bit and mark it ✘.
    If none exists (the first right symbol is ␣ or ✘) REJECT.
        (the input has an odd number of bits)
    Otherwise, after marking, GOTO Step 2.



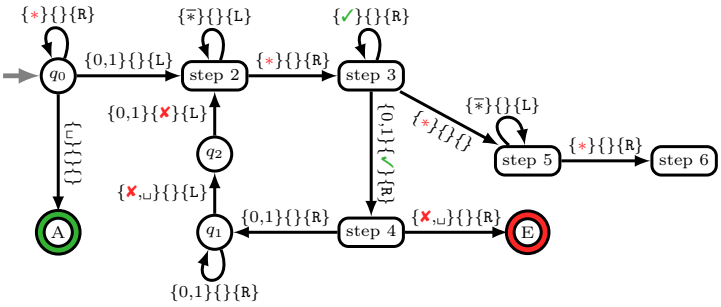
After the loop involving steps 3 and 4, the input string is partitioned into two halves: the first is marked with ✓ and the second with ✘. We now compare ✓ bits with ✘ bits.

5: Return to $*$
`// Match each ✓-bit with a corresponding ✘-bit`
6: Move right to the first bit marked ✓.
    If none exists (you come to ␣) ACCEPT
    Otherwise remember the bit and unmark it.
7: Move right to the first bit marked ✘.
    If the bit does not match the bit remembered, REJECT.
    If it is a match, unmark the bit and GOTO Step 5.

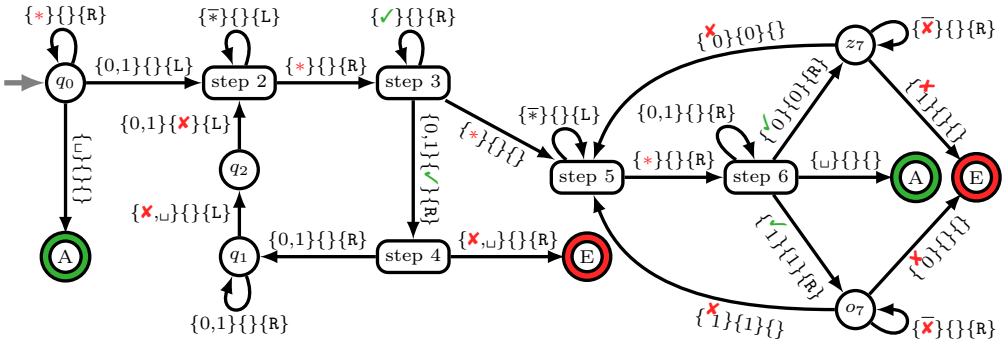
It is now just a matter of constructing the machine-level instructions for each step and snapping them together. Let's do it for our second approach which directly solves ww. First, we do steps 1–3. The notation $\overline{*}$ means any symbol that is not $*$. Step 3 transitions to either step 4 or 5.



Now for steps 4 and 5.

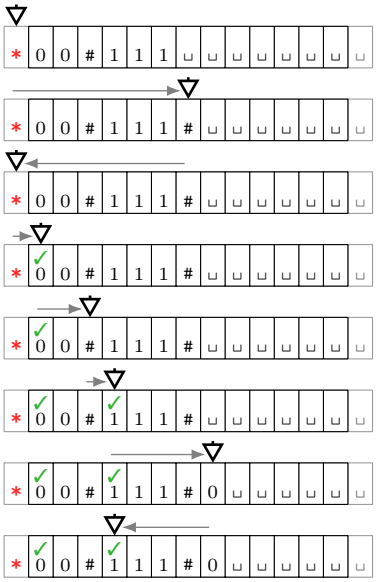


Lastly, we must implement step 6 and 7 to match bits marked ✓ with bits marked ✘.



Practice. Construct the TM which preprocesses the string into $w\#w$ and cascade it with our TM for $w\#w$.

Pop Quiz 26.7.



Exercise 26.8.

(a) (i) The Turing machine copies the bits over one by one.

1: Move right to the first ␣ and write #.
2: Return to ∗.
3: Move right to first non-marked before #.
Remember and mark the bit.
If, instead, you reach #, return to ∗ unmarking all the ✓ and halt.
4: Move right to first ␣, write the remembered bit and GOTO step 2.

(ii) $\mathcal{L} = \{w\#w \mid w \in \Sigma^*\}$.

(b) (i) We use a ✘ to simulate the punctuation #.

1: Move right to the first ␣ and mark with ✘.

2: Return to $*$.
3: Move right to first non-marked before ✘.
Remember and mark the bit with ✓.
If you reach ✘, unmark the bit, return to $*$ unmarking all the ✓ and halt.
4: Move right to first $\sqcup$, write the remembered bit and GOTO step 2.

(ii) $\mathcal{L} = \{ww \mid w \in \Sigma^*\}$.

(c) (i) Write a 1 for every zero and repeat for every zero.
1: Move right to the first $\sqcup$ and mark with #.
2: Return to $*$.
3: Move right to first non ✘-marked 0 and mark with ✘.
If you reach #, return to $*$ unmarking all 0's and halt.
4: Return to $*$.
5: Move right to first non ✓-marked 0 and mark with ✓
If you reach #, return to $*$ unmarking ✓s (leaving the ✘s) and GOTO step 3.
6: Move right to first $\sqcup$ and write 0.
7: Move left to first ✓ and GOTO step 5.

(ii) $\mathcal{L} = \{0^{\bullet^n}\#1^{\bullet^{n^2}} \mid n \geq 0\}$.

(d) (i) Mark and replace the first with the last bit and *vice versa* and continue.
1: Move right to the first non-marked bit. Mark it and remember it.
If you reach $\sqcup$, return to $*$, erasing all marks and halt.
2: Move right to the last non-marked bit.
If there is none, return to $*$, erasing all marks and halt.
Otherwise, remember it, replace it with the bit from step 1 and mark it.
3: Move left to the first marked bit.
Replace the bit with the bit remembered in step 2 and GOTO step 1.

(ii) $\mathcal{L} = \{w\#w^{\mathrm{R}} \mid w \in \Sigma^*\}$.

Pop Quiz 26.9. (a) $\to q_0 \to$ E (b) $\to q_0 \to q_1 \to$ A (c) $\to q_0 \to q_0 \to q_1 \to q_0 \to q_1 \to \cdots$ (infinite loop).

Pop Quiz 26.10. Yes. Every decider trivially recognizes its language so every decidable language is also recognizable.

Exercise 26.11. Let M be a decider for $\mathcal{L}$. Assume states, symbols and instructions are suitably punctuated.
1: Process each state. Check for a valid instruction telling the machine what to do if in that state for *every* symbol.
2: **for** each state, marking it when you process it **do**
3: **for** each symbol, marking it when you process it **do**
4: Find the instruction begining with the state and symbol and verify that it is a valid instruction.

Our TM verifies if the input is a valid TM. Compare with a compiler which verifies that an input program is valid.

Chapter 27

Pop Quiz 27.1.

(a) To correctly grade, the TA must check if the program prints "Hello World!". If yes, Goldbach's conjecture is false. If no, Goldbach's conjecture is true. Either way, the TA resolves an open conjecture and gains fame.

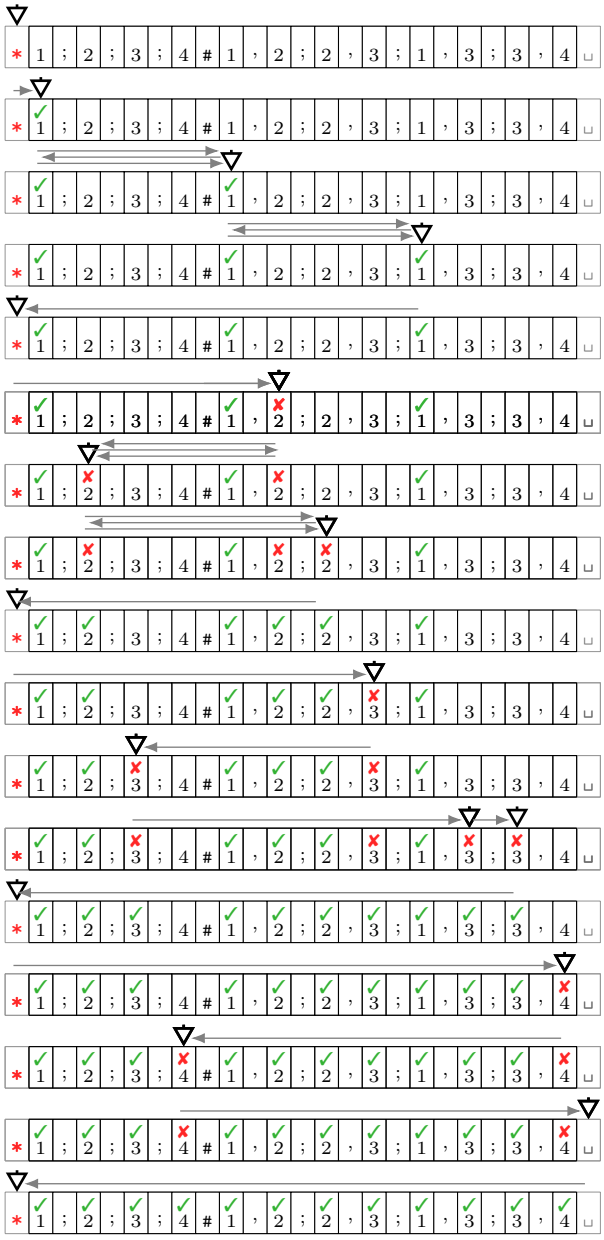
(b) Run the ultimate debugger on the student's submission. If the debugger says the program halts, then Goldbach's conjecture is false. If the debugger says the program does not halt (runs forever), Goldbach's conjecture is true.

(c) Before entering the mess, you may ask: can a program (CONFUSED) run another program (AUTO-GRADE) on *itself*. The answer is yes, a nontrivial result called the Recursion Theorem. We won't get into that. Lets see what happens.

CONFUSED first runs AUTO-GRADE on the program CONFUSED (this must halt with (YES) or (NO)).
If AUTO-GRADE says (NO), it means CONFUSED *does not* print "Hello World!"; but in this case, by definition CONFUSED replaces the output file with "Hello World!" and halts. That is CONFUSED *does* print "Hello World!": a contradiction.
If AUTO-GRADE says (YES), it means CONFUSED *does* print "Hello World"; but then CONFUSED erases the output file which means it does not print "Hello World". Again, a contradiction.

CONFUSED is a paradoxical program which must halt by construction, since AUTO-GRADE is a decider. But if CONFUSED halts, then it must either print "Hello World" or not, and both lead to contradiction, so the program CONFUSED cannot exist. But CONFUSED exists if AUTO-GRADE exists, therefore AUTO-GRADE cannot exist. Something is **FISHY** here. If AUTO-GRADE does not exist, then what are the TA's using to grade the CS1 assignments?

Exercise 27.2. When we mark a vertex, we also mark the edges containing this vertex. This requires a lot of zig-zagging (we supress the details). Note: the encoding $\langle G \rangle$ contains all the punctuation.



Marking node "1" in the edges requires zig-zagging. The TM cannot just "remember" the label "1" and mark in in the edges, because the TM cannot "remember" labels. The TM has a finite number of states with which to "remember" things. The vertex labels are arbitrary, and there can be arbitrarily many of them since the graph can have any finite size. Vertex label "1" is really "00000001" (ASCII code). What happens is that the TM marks the *position* of the vertex label and remembers the *first bit* in the label (marking it). Then the TM moves right to the edges looking for a vertex with that first bit. If it finds one, it marks the bit and then zig-zags to match and mark all bits.

Continuing, if all bits match, the vertex is marked as matched. If some bit does not match, the vertex is marked as non-matched and it need not be checked again. After processing the vertex, all edge vertices that were marked as non-matched are unmarked. In our figure, we skipped the steps when no match is found. At the end of this phase, the TM is ready to scan the edges for an unmarked vertex.

The head moves right to mark with ✘ the first unmarked vertex in the edges, also finding and marking this vertex in the node-list. Now, the TM marks all locations in the edges where the newly marked vertex occurs. Lastly, the head returns to $*$ changing every ✘ to ✓. Again, the TM is ready to scan the edges for another unmarked vertex. For the remaining steps we suppress the zig-zagging and only show the high-level of what happens.

Next, the TM marks an unmarked vertex among the edges (in this case vertex "3"), and repeats the dance of marking the vertex, and then all edges in which the vertex appears. Finally, the TM gets to vertex "4", and when all is said and done, the TM returns to $*$ to perform one last scan of the vertices. In the last scan, the TM looks for an unmarked vertex, in which case the graph is disconnected. Here, all vertices are marked, and the graph is connected.

We went through the details in some of their gore to show you that a TM can indeed solve problems which we are accustomed to writing programs to solve. The TM can indeed solve all the nice problems we are used to seeing solved by a computer. The TM is a good model of a computer.

Exercise 27.3. No, because if $w \notin \mathcal{L}_1$ but $w \in \mathcal{L}_2$, we need a TM M that will halt with accept. However, because M_1 is a recognizer for $\mathcal{L}_1$, in step 1 it may not halt which means the construction for M will not halt.

Recognizable languages are closed under union, but we need a more sophisticated construction for M. Essentially M must interleave M_1 and M_2, so M runs one step of M_1 and then one step of M_2 and so on. You can fill in the details.

Pop Quiz 27.4. (See also Exercise 27.2.) The TM can only remember finitely many things using its states. Since M on the other hand can an arbitrary number of states, the TM cannot "remember" the state. It marks the state, and must zig-zag to match bit-by-bit to the transition instruction (depending on the tape symbol at $\triangledown$).

Pop Quiz 27.5. A TM M can take as input any binary string w. In particular, w can be the binary encoding of M itself. So, $M(\langle M \rangle)$ is valid and the language $\mathcal{L}_{\text{DIAG}}$ is a well defined computing problem. Either $D \in \mathcal{L}_{\text{DIAG}}$ or $D \notin \mathcal{L}_{\text{DIAG}}$. If $\langle D \rangle \in \mathcal{L}_{\text{DIAG}}$, $D(\langle D \rangle) = \boxed{\text{NO}}$. But, since D is a decider for $\mathcal{L}_{\text{DIAG}}$, $D(\langle D \rangle) = \boxed{\text{YES}}$. This contradiction means $\langle D \rangle \notin \mathcal{L}_{\text{DIAG}}$. If $\langle D \rangle \notin \mathcal{L}_{\text{DIAG}}$, $D(\langle D \rangle) = \boxed{\text{YES}}$. But, since D is a decider for $\mathcal{L}_{\text{DIAG}}$, it means $D(\langle D \rangle) = \boxed{\text{NO}}$. This contradiction means $\langle D \rangle \in \mathcal{L}_{\text{DIAG}}$. So D is not in $\mathcal{L}_{\text{DIAG}}$ and its not outside $\mathcal{L}_{\text{DIAG}}$. It can't exist.

Exercise 27.6. Recall that $\mathcal{L}(U) = \{w \mid U(w) = \text{halt and accept}\}$. U is not a decider for $\mathcal{L}(U)$ because U may infinitely loop on (NO)-strings. This Demonic fixed TM is U_{TM}: $\mathcal{L}(U_{\text{TM}}) = \mathcal{L}_{\text{TM}}$, which we know is undecidable.

Exercise 27.7. Let A_{TM} be a decider for $\mathcal{L}_{\text{TM}}$.
We sketch a TM for the diabolical program in Pop Quiz 27.1 (right). Run A_{TM} on D with empty input to resolve Goldbach's conjecture. The conjecture is false if and only if A_{TM} accepts.
A_{TM} is general and doesn't exist. D is special and exists. Either D halts or it doesn't. We can prove or disprove Goldbach's conjecture by analyzing D.

D = Diabolical student's Turing Machine
INPUT: empty tape.
1: Write 4 (in binary) on the tape.
2: Test if the number on the tape is a sum of two primes.
If not, ACCEPT;
otherwise add 2 to the number on tape and repeat step 2.

Pop Quiz 27.8. In our reduction terminology, (building a bike) $\leq_{\text{R}}$ (building a car).
(a) (i) Cars are harder so we must be able to build bikes. (ii) We don't know. Cars could be much harder.
(b) (i) We don't know. Maybe we can't build anything. (ii) No way. Forget hard things if you can't do simple things.

Exercise 27.9.
(a) $\mathcal{L}_{\text{empty}} = \{\langle M\rangle \mid M \text{ is a TM and } \mathcal{L}(M) = \varnothing\}$.
Suppose E_{TM} decides $\mathcal{L}_{\text{empty}}$. We sketch a decider H_{TM} for $\mathcal{L}_{\text{HALT}}$ that uses E_{TM}. Since $\mathcal{L}_{\text{HALT}}$ is undecidable, this is a contradiction, which proves that E_{TM} does not exist.
There are several interesting points in H_{TM}.
(i) The inputs $\langle M\rangle$ and w, are "hard-coded" into M'.
(ii) You can define a TM, in this case M', inside a TM.
(iii) M' accepts every input providing M halts on w.
(iv) H_{TM} never actually runs M' or M on w; it only *encodes* M' into its description $\langle M'\rangle$.

H_{TM} = Decider for $\mathcal{L}_{\text{HALT}}$ that uses E_{TM}
INPUT: $\langle M\rangle\#w$, where M is a TM and w its input.
1: Modify M to M'
M' = Modified version of M
INPUT: w'
1: Run M on w.
2: ACCEPT
2: Obtain $\langle M'\rangle$, the encoding of M'.
3: Run $E_{\text{TM}}(\langle M'\rangle)$ and ACCEPT iff E_{TM} REJECTS.

First H_{TM} always halts, so it is a decider, because E_{TM} is a decider and always halts. Second, $\mathcal{L}(M') = \varnothing$ if and only if M does not halt on w, therefore H_{TM} is a decider for $\mathcal{L}_{\text{HALT}}$, which is the contradiction we desire.
(b) $\mathcal{L}_{\text{EQ}} = \{\langle M_1\rangle\#\langle M_2\rangle \mid M_1 \text{ and } M_2 \text{ are TM's and } \mathcal{L}(M_1) = \mathcal{L}(M_2)\}$.
Suppose EQ_{TM} is decider for $\mathcal{L}_{\text{EQ}}$. We construct a decider E_{TM} for $\mathcal{L}_{\text{empty}}$. Let M^* be a TM that immediately halts and rejects on every input. So $\mathcal{L}(M^*) = \varnothing$. Now let $E_{\text{TM}}(\langle M\rangle) = EQ_{\text{TM}}(\langle M\rangle\#\langle M^*\rangle)$. E_{TM} accepts if and only if $\mathcal{L}(M) = \mathcal{L}(M^*) = \varnothing$. Therefore E_{TM} decides $\mathcal{L}_{\text{HALT}}$, a contradiction, and so EQ_{TM} does not exist.

Exercise 27.10. The start domino must have the same first bit on top and bottom. The only possibility is d_1,

$$d_1 = \begin{array}{|c|}\hline 10 \\ \hline 101 \\ \hline \end{array}$$

The next domino's top first bit must be 1 and the remaining bits on top and bottom must match. That only leaves d_3,

$$d_1 d_3 = \begin{array}{|c|}\hline 10 \\ \hline 101 \\ \hline \end{array}\begin{array}{|c|}\hline 101 \\ \hline 011 \\ \hline \end{array} = \begin{array}{|c|}\hline 10101 \\ \hline 101011 \\ \hline \end{array}$$

We have an extra 1 on the bottom so again, the next domino is d_3. The argument repeats – you never get rid of the extra 1 on the bottom. The only solution is $d_1 d_3 d_3 d_3 \cdots$, which is infinite. This instance of PCP has no solution.

Exercise 27.11. A domino is a pair n, m, n 1's on top and m on the bottom. For input $n_1, n_2, \ldots, n_\ell\#m_1, m_2, \ldots, m_\ell$. We give an *algorithm* to decide the problem. We encourage the reader to sketch the TM.
1: If $n_i > m_i$ for all i or $n_i < m_i$ for all i then REJECT.
2: ACCEPT

The algorithm tests if the top values are either all less than or all greater than the bottom values. It must halt.
We prove the decision is always correct. First suppose $n_i > m_i$ (resp. $n_i < m_i$) for all i. Then the top string will always be longer (resp. shorter) than the bottom string, and so it is not possible to have a match and REJECT is correct.
Now suppose $n_i \leq m_i$ for some i AND $n_j \geq m_j$ for some j. The decision is ACCEPT. We show this is correct by finding a domino sequence with matching top and bottom strings. If $n_k = m_k$ for any k then d_k is a solution. So, w.l.o.g., assume $n_1 < m_2$ and $n_2 > m_1$. Consider $d_1^{\bullet(n_2-m_2)} d_2^{\bullet(m_1-n_1)}$. The number of top-1s is $n_1(n_2-m_2)+n_2(m_1-n_1) = m_1n_2-n_1m_2$. The number of bottom-1s is $m_1(n_2-m_2)+m_2(m_1-n_1) = m_1n_2-n_1m_2$. These match.

Exercise 27.12.
(a) Use a second tape as the counter. Every time the TM M executes a transition instruction, it first moves right *on the counter tape* and writes 1, then it performs its instruction. So, for every instruction, the counter tape will have a 1. If a single tape TM is desired, merge the second tape with the first using the trick in Example 27.1.

(b) Each step touches at most one new tape-slot, so at most n tape-slots are touched.

(c) First, come back to $*$. For every 1 on the counter move L one step. Now, for every 1 on the counter tape, move R twice, each time erasing the tape (if you come to $*$, move R). All slots within n of $*$ are now erased.

Exercise 27.13. The homework should require programs to halt in a given number of steps (CPU-cycles or time). Determining if a TM prints "Hello World!" and halts within a given number of steps is decidable. Simply simulate the machine for that number of steps. If it halts, examine the tape for "Hello World!". If it does not halt, REJECT.

Exercise 27.14.

(a) Let M and $\overline{M}$ recognize $\mathcal{L}$ and $\overline{\mathcal{L}}$ respectively. We sketch a decider for $\mathcal{L}$. First, we show a failed attempt. One of M, $\overline{M}$ accept because either $w \in \mathcal{L}$ or $w \in \overline{\mathcal{L}}$. However, in step 1, M may infinite-loop (M is only a recognizer). In this case D also infinite-loops and so is not a decider.

D = Flawed Decider for $\mathcal{L}$ that uses M and $\overline{M}$
INPUT: w (the input to M or $\overline{M}$)
1: Run M on w; if M ACCEPTS, then ACCEPT.
2: Run $\overline{M}$ on w; if $\overline{M}$ ACCEPTS, then REJECT.

The solution is to interleave the running of M with $\overline{M}$, and if either accepts at any point in the interleaved execution, then perform the appropriate action. To implement the interleaving, use a second tape. Each time you switch machines, you switch tapes. Now, since one of M, $\overline{M}$ must halt, D also halts. If $w \in \mathcal{L}$, then M halts and accepts, so D also accepts; If $w \notin \mathcal{L}$, then $\overline{M}$ halts and accepts, so D rejects. That is, D is a decider for $\mathcal{L}$ and $\mathcal{L}$ is decidable.

D = Decider for $\mathcal{L}$ that uses M and $\overline{M}$
INPUT: w (the input to M or $\overline{M}$)
1: Run M *for one step* on w;
if M ACCEPTS, then ACCEPT.
2: Run $\overline{M}$ *for one step* on w;
if $\overline{M}$ ACCEPTS, then REJECT.
3: GOTO step 1.

(b) In (a) we proved: IF $\mathcal{L}$ and $\overline{L}$ are recognizable THEN $\mathcal{L}$ is decidable. The contrapositive (which is equivalent) is:

IF $\mathcal{L}$ is undecidable THEN it is not the case that $\mathcal{L}$ and $\overline{L}$ are recognizable.

This is exactly what was to be proved.

(c) $\mathcal{L}_{\text{TM}}$ recognized by U_{TM}. $\mathcal{L}_{\text{TM}}$ is undecidable, therefore by (b) $\overline{\mathcal{L}_{\text{TM}}}$ is unrecognizable.
$\mathcal{L}_{\text{HALT}}$ is recognizable (simulate and accept if the machine halts), but undecidable. So, by (b), $\overline{\mathcal{L}_{\text{HALT}}}$ is unrecognizable.
Fact: Every undecidable problem $\mathcal{L}$ provides at least one unrecognizable problem ($\mathcal{L}$ or $\overline{\mathcal{L}}$).

Chapter 28

Exercise 28.1. At any stage, M_{HALF} ignores marked bits and proceeds as if the only bits present are the unmarked bits.

(a) First, let $k = \ell$. In the first scan. an equal number of 0's and 1's are marked, leaving fewer unmarked 0's and the same number of unmarked 1's. By strong induction on the number of unmarked 0's, all unmarked bits get marked.
Suppose $k \neq \ell$. We use strong induction on the number of unmarked bits. If the number of unmarked bits is odd, there is nothing to prove, hence base case with one unmarked bit is trivial. Suppose the number of unmarked bits at the first scan is even. The number of unmarked 0's and 1's are both even or both odd. Consider each case.
(i) Both even: Suppose there are $2k$ unmarked 0's and 2ℓ unmarked 1's, with $\ell \neq k$. After one scan, marking every other 0 and 1, there will be k unmarked 0's and ℓ unmarked 1's, with $k \neq \ell$. Since there are fewer unmarked bits, by the induction hypothesis, an odd number of unmarked bits will occur and the algorithm will reject.
(ii) Both odd: Suppose there are $2k+1$ unmarked 0's and $2\ell+1$ unmarked 1's, with $\ell \neq k$. After one scan, marking every other 0 and 1, there will be k unmarked 0's and ℓ unmarked 1's, with $k \neq \ell$. Again, by the induction hypothesis, at some point there will be an odd number of unmarked bits and the algorithm will reject.
In both cases, an odd number of unmarked bits occur proving the claim for $n+1$. So, the claim holds for all $n \geq 1$.

(b) We give the sketch and analyze the runtime. Fixing the size of the input, the worst case runtime is for $0^{\bullet n}\#1^{\bullet n}$, because otherwise the algorithm exits early with a reject. For $0^{\bullet n}\#1^{\bullet n}$, steps 1,2 and 3 can all be accomplished in a single scan of the input, that is $\Theta(n)$ steps. Abusing notation a little, the runtime is given by

number of executions of steps 2 and 3 $\times\ \Theta(n)$.

M = Efficient Turing Machine that solves $\{0^{\bullet n}\#1^{\bullet n}\}$
INPUT: Binary string w.
1: Check the input has the correct format and return to $*$.
2: Check the number of *unmarked* bits is even.
If not, REJECT.
If there are no unmarked bits, ACCEPT.
3: Mark every other *unmarked* 0 and every other *unmarked* 1.
GOTO step 2.

If the number of unmarked zeros is $2k$ or $2k+1$ before step 3 is executed, then the number of unmarked zeros after step 3 is $2k$ (see part (b)). That is, each time step 3 is executed, the number of unmarked 0's drops by a factor

of at least 2. If step 3 is executed m times, then the number of unmarked 0's is at most $n/2^m$, which will be less than one if $2^m > n$. If the number of unmarked 0's is less than one, the machine exits. This means the machine exits after $\lfloor 1 + \log_2 n \rfloor$ steps and the worst case runtime is

$$\lfloor 1 + \log_2 n \rfloor \times \Theta(n) \in \Theta(n \log n).$$

Pop Quiz 28.2. $\log n$, $\sqrt{n}$, n, $n^2 \log n$ are all fast, upper bounded by n^3 which is fast with $\lambda = 8$, because $(2n)^3 \leq 8n^3$. $(\log_2 n)^{\log_2 n}$, $n^{\log_2 n}$, $2^{\sqrt{n}}$, 2^n are all not-fast because for $n \geq 2^{20}$, they are all at least $(\log_2 n)^{\log_2 n}$, and we show, by contradiction, that $(\log_2 n)^{\log_2 n}$ is not fast. Suppose $(\log_2 n)^{\log_2 n}$ is fast. So there is a function $f(n)$ for which

$$(\log_2 n)^{\log_2 n} \leq f(n) \qquad \text{and} \qquad f(2n) \leq \lambda f(n).$$

Because f is fast, $f(2^k) \leq \lambda f(2^{k-1}) \leq \lambda^2 f(2^{k-2}) \leq \cdots \leq \lambda^{k-1} f(2)$. Since f is an upper bound, $f(2^k) \geq k^k$. Choose any $k > \max(\lambda, f(2))$. Then

$$f(2^k) \geq k^k > k^{k-1} \cdot k > \lambda^{k-1} f(2),$$

which contradicts $f(2^k) \leq \lambda^{k-1} f(2)$. Therefore, $(\log_2 n)^{\log_2 n}$ is not fast.

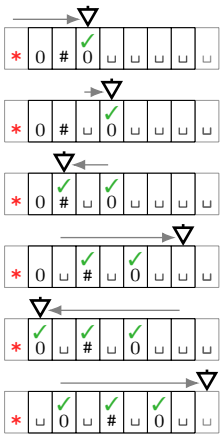
fast	$\log n$	$\sqrt{n}$	n	$n^2 \log n$
not fast	$(\log_2 n)^{\log_2 n}$	$n^{\log_2 n}$	$2^{\sqrt{n}}$	2^n

Exercise 28.3. Let $n = 2^k$, so $k = \log_2 n$.

$$\begin{aligned} f(2^k) &= 2^k f(2^{k-1}) \\ &= 2^k 2^{k-1} f(2^{k-2}) \\ &= \cdots \\ &= 2^k 2^{k-1} \cdots 2^1 f(2^0) \\ &= 2^{k+(k-1)+\cdots+1} f(1) \\ &= 2^{k(k+1)/2} f(1) \\ &= (2^k)^{(k+1)/2} f(1) \\ &= \sqrt{n^{\log_2 n + 1}} f(1). \end{aligned}$$

Pop Quiz 28.4. Our algorithm assumes the input does not contain ␣ symbols.

1: Move to the end of the input and mark the last symbol.
2: Shift all marked symbols 1 step right
    repeat, moving right, until you come to two blank symbols.
3: Move left to the first unmarked symbol.
    Mark the symbol and got to step 2.
    If you come to ∗, unmark all symbols.



We illustrate with input 0#0 on the right. For an input of size n, step 1 takes $\Theta(n)$ steps. In steps 2 and 3, for k marked symbols, the work done is approximately $2k$ steps to shift the marks and $2k$ steps to come back to an unmarked symbol, for a total of about $4k$. The number of marked symbols goes from 1 to n, and so the runtime is of this loop is

$$\sum_{k=1}^{n} 4k = 2n(n+1) \in \Theta(n^2).$$

The total run time is in $\Theta(n + n^2)$ which is in $\Theta(n^2)$.

Pop Quiz 28.5. If M_{two} has implemented t steps, the heads are at most $2t$ slots right of their beacon (∗ or ‡). So, move `L` until you find the beacon (at most $2t$ moves) and then move `R` until you find the head (another at most $2t$ moves). The total number of steps is at most $4t \in O(t)$.

We assumed that the head is always right of the beacon (start point). Alternatively, in M_{one}, we can implement left and right boundary markers, `LB` and `RB`, which mark the left most and right most points touched. You only need to update `LB` if you move `L` from `LB` and similarly update `RB` if you move `R` from `RB`. Now, to find the head, move to one of the boundary markers and then in the other direction until you reach the head. Again, this would be in $O(t)$ steps.

Exercise 28.6.

(a) By Pop Quiz 28.4, step 1 takes $O(n^2)$ steps. All operations in M_{one} are constant time except for SWITCH, which runs in $O(n)$ steps because M_{two} runs in $\Theta(n)$ steps (see Pop Quiz 28.5).
So, step 4 is $O(n)$ steps and it's done n times for $O(n^2)$ steps. Similarly for step 5. The total is $O(n^2)$ steps.

(b) The proof is analogous to (a). Reconfiguring the tape into odd and even slots requires $O(n^2)$ steps. Now, M_{one} simulates each step of M_{two}, with the added complication of SWITCH. In the worst case M_{one} must SWITCH at every step of M_{two}, which is at most $t(n)$ SWITCH's. Each SWITCH requires $O(t(n))$ steps (Pop Quiz 28.5), so the number of steps spent switching is $t(n) \times O(t(n)) \in O(t(n)^2)$ (abuse of O-notation). Once the SWITCH is done, M_{one} simply implements M_{two}'s instruction in $O(1)$ steps, so it takes $O(t(n))$ steps to implement all M_{two}'s instructions.

The total runtime is in $O(n^2 + t(n) + t(n)^2)$. Notice that if M_{two} is trivial and immediately rejects, then the overhead to reconfigure the tape, n^2, dominates. Assuming M_{two} is non-trivial and at least examines its input, then $t(n) \geq n$ in which case $t(n)^2$ dominates and $n^2 + t(n) + t(n)^2 \in O(t(n)^2)$, completing the proof.

If you had a k-tape machine, the only difference in the analysis is that

(i) The overhead to reconfigure the tape into k interleaved tapes is kn^2.
(ii) The SWITCH takes $O(kt(n))$ steps.
(iii) An instruction of M_k on M_{one} takes $O(k)$ steps (e.g. move R becomes move k steps R).

The runtime is $O(kn^2 + kt(n) + kt(n)^2) \in O(kt(n)^2) \in O(t(n)^2)$ (since k is a constant).

Exercise 28.7. To prove a problem is decidable, we must sketch a Turing Machine for it.

(a) The idea is to try all permutations of the vertices, sketched to the right. The algorithm has non-trivial steps, e.g. listing every permutation of the vertices. If there is one vertex it is easy. If there are n, you can solve the problem "recursively": for each vertex v, list the permutations of the other $n-1$ vertices and prepend v to each.

M = Decider for HAMILTONIAN-PATH
INPUT: Encoding of a graph, $\langle G \rangle$.
1: Check that the input has the correct graph-format and return to $*$.
2: List *every* permutation of the vertices to the right of the graph input (with a punctuation character # to separate each permutation).
3: Process each permutation $v_{i_1} v_{i_2} \cdots v_{i_n}$
Check that consecutive vertices $(v_{i_k}, v_{i_{k+1}})$ are an edge.
If every edge exists ACCEPT; otherwise try the next permutation.
4: If you didn't accept for any permutation, REJECT

(b) The idea in the sketch is to try all subsets of the vertices of size $\lceil n/2 \rceil$. Again, you may wonder how to list out every $\lceil \frac{n}{2} \rceil$-subset. This would be equivalent to listing out all binary strings of n bits with exactly $\lceil \frac{n}{2} \rceil$ 1's. Again it can be done recursively, listing the binary strings with $n-1$ bits and $\lceil \frac{n}{2} \rceil$ 1's and then prepending 0, plus the binary strings with $n-1$ bits and $\lceil \frac{n}{2} \rceil - 1$ 1's and then prepending 1.

M = Decider for CLIQUE
INPUT: Encoding of a graph, $\langle G \rangle$.
1: Check the input is a graph and return to $*$.
2: List *every* $\lceil \frac{n}{2} \rceil$-subset of the vertices to the right of the graph input (with a punctuation character # to separate each subset).
3: Process each subset of the nodes: $v_{i_1} v_{i_2} \cdots v_{i_{\lceil n/2 \rceil}}$
Check every pair of vertices (u, v) in the subset is an edge.
If every edge exists ACCEPT; otherwise try the next subset.
4: If you didn't accept for any subset, REJECT

We did not get into some of the algorithmic details of our deciders, and it is clear that we have taken a very lazy approach to solving the problem. Essentially, try all possibilities, and if one works ACCEPT. If none work REJECT. These deciders take a *very* long time, but they always halt. For HAMILTONIAN-PATH, the number of permutations is $n!$ which is super-exponential. For CLIQUE, the number of subsets is $\binom{n}{n/2}$. For n even,

$$\binom{n}{\frac{n}{2}} = \frac{n(n-1)(n-2)\cdots(n+1-\frac{n}{2})}{\frac{n}{2}(\frac{n}{2}-1)(\frac{n}{2}-2)\cdots(\frac{n}{2}-(\frac{n}{2}-1))} = 2 \times 2\frac{n-1}{n-2} \times 2\frac{n-2}{n-4} \cdots \times 2\frac{n-(\frac{n}{2}-1)}{n-(n-2)} \geq 2^{n/2}.$$

So, the number of subsets is super-polynomial. Neither of our TMs have polynomial runtime.

Exercise 28.8.

(a) Try every factor p from 2 to $n-1$. If none work, REJECT. Otherwise output the factor. The ✘ marks p. Each time p fails, it increments by 1 in step 4. Step 5 tests if p divides n. We analyze the runtime of M_{unary}.

1: One scan, in $\Theta(n)$.
2: n zig-zags of $\Theta(2n)$ steps for $\Theta(n^2)$.
3: As we are already at #, this is $O(1)$ steps.
4: $O(n)$ to find the ✘; this step is repeated at most n times, for $O(n^2)$ in total.
5: p zig-zags repeated about n/p times for $p \times 2(n+p) \times n/p \in \Theta(n^2)$ steps.

Step 5 is run at most n times, once for each p, which is $O(n^3)$ steps.

M_{unary}=Transducer to compute a factor of n.
INPUT: $1^{\bullet n}$. Assume $n \geq 2$.
1: Check the input format and place a # at the end.
2: Copy the input $1^{\bullet n}$ to the right of the #.
3: Mark the first 1 after the # ($p = 1$) with an ✘.
4: Move the ✘ one step R ($p \leftarrow p + 1$).
If ␣ is to the right of ✘, you came to $p = n$. REJECT.
5: Mark an unmarked left 1 for each right 1 from # *up to* ✘.
if you run out of left 1's (p does not divide n),
erase all left marks and GOTO step 4.
if there are no left 1's which remain unmarked (p divides n),
erase all 1's after the ✘ and ACCEPT.
if left 1's remain unmarked (continue "dividing" by p),
repeat step 5.

Step 5 dominates, so the worst case runtime is in $O(n^3)$, polynomial in n. One can make this algorithm more efficient, for example only test factors up to $\sqrt{n}$. Making algorithms more efficient is the dominant goal of an algorithms course. Our concern was to get a polynomial runtime, *any* polynomial.

(b) We use a particularly lazy approach. First compute the unary representation of w_n and then run the algorithm from part (a) on this unary representation.

Step 1 is non-trivial, converting binary to unary. Let $w_n = b_{k-1}b_{k-2}\cdots b_1b_0$ be the k bits of w_n, where $b_{k-1} = 1$. Going from $i = 0$ to $k-1$, if b_i=1, you add 2^{i-1} 1's to the unary representation.

M_{binary}=Transducer to compute a factor of n.
INPUT: w_n, n in binary. Assume $n \geq 2$.
1: Compute w_n in unary and write $1^{\bullet n}$ to the left of $*$.
2: Run the TM M_{unary} on the left of $*$ (replacing L $\leftrightarrow$ R).
3: If M_{unary} rejects, REJECT.
4: If M_{unary} accepts,
Compute the binary w_p for the unary p from M_{unary}.
Copy w_p to the right of w_n. Erase the tape left of $*$.

We encourage the reader to construct a TM for binary-to-unary conversion. The details are not essential here. Since $w_n = b_{k-1}b_{k-2}\cdots b_1b_0$ and $b_{k-1} = 1$, $n \geq 2^{k-1} = 2^{|w_n|-1}$. We know that M_{unary} uses at least $n \geq 2^{|w_n|-1}$ steps, which is a lower bound on the runtime of M_{binary}. The additional steps like the binary to unary conversion can only add more to the runtime. Hence, the runtime of M_{binary} is *at least* exponential, which is non-polynomial.

We emphasize the difference between the natural parameter in the problem, n, and the *length of the input to the TM*. Runtimes refer to the length of the input. In (a), the natural parameter and the length of the input are comparable, equal to n and so a polynomial TM will have runtime which is polynomial in n (the length of the input).

In (b), the input is w_n, which is the binary representation of n. This input has length $\log_2 n$, and so a polynomial TM for the problem with the input formatted in binary must have a runtime that is polynomial in $\log_2 n$ (for example $\log_2^{13} n$ would work). Our runtime in (b) is at least $2^{\log_2 n - 1}$ which is not polynomial in $\log_2 n$.

You may also be astounded by the stupidity of our algorithm in (b). Yes, it is stupid, but not far off from reality. Nobody has found a factoring-algorithm that is a polynomial in $\log_2 n$. So our simple algorithm is not that far off from the best we know. Be the first to find an algorithm which is polynomial in $\log_2 n$ and fame will come.

Chapter 29

Pop Quiz 29.1.

(a) YES: For $A = \{5, 11\}$, $\text{sum}(A) = 16 \geq 15 = \frac{1}{2}\text{sum}(S)$

(b) NO: It is not obvious how to prove a no-answer. The simplest "proof" is to list out all the possible subset-sums. We used the simple program on the right to create this list of possible subset-sums. The idea is to start with 0, and add each value in S to the current possible subset-sums (removing duplicates). The possible subset-sums are:

$0, 2, 3, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 27, 28, 30.$

Observe that 15 is not one of the possible subset-sums.

(c) YES: $\text{sum}(S) = 30$ and $3 + 6 + 6 = 15$ (also $2 + 11 + 2 = 15$).

X=SubsetSum(S)
// $S = \{s_1, \ldots, s_n\}$
1: $X = \{0\}$;
2: for $i = 1$ to $|S|$ do
3: $X_S \leftarrow \{\}$;
4: for $j = 1$ to $|X|$ do
5: add $s_i + x_j$ to X_S;
6: $X \leftarrow X \cup X_S$;
7: return X;

Exercise 29.2.

(a) 001101.

(b) The evidence would be an encoding of all subsets. The certifier would check each subset's sum to verify that it does not work. Since there are exponentially many subsets, the evidence is exponential and the runtime is exponential.

(c) Let n be the number of elements in the input S. Assume that the runtime of the certifier (given the input) is a polynomial $p(n)$. To solve a problem with input S, run the certifier with every possible setting for the certificate (n-bit string). If any certificate verifies to YES then ACCEPT. If no certificate verifies to YES then REJECT.

There are 2^n possible certificates, so the runtime is $2^n p(n)$, not polynomial. (The input-length is related to n.)

Exercise 29.3.

(a) Easier to prove YES. The evidence is the subset; the proof checks that the subset-sum is k.

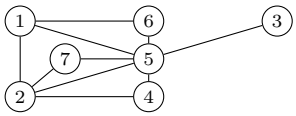
(b) Easier to prove YES. The evidence is the clique; the proof checks that there are at least k clique-vertices and there is an edge between every pair of vertices in the clique.

(c) Easier to prove YES. The evidence is an assignment of colors to every vertex; the proof checks that there are at most k different colors and that every edge has two vertices of different colors.

(d) Easier to prove NO. The evidence is integers p, q; the proof checks $p, q > 1$ and $pq = n$.

The YES-answer can also be proved quickly because the AKS-test (proved in 2002) shows that IsPrime $\in$ P. If you can *solve* a problem in polynomial time, you can prove either answer in polynomial time. Still, NO is much easier.

(e) Easier to prove YES. The evidence is an isomorphism f from G_1 to G_2; the proof checks that the number of vertices and edges match and for each edge $(u, v) \in G_1$, $(f(u), f(v)) \in G_2$.

Pop Quiz 29.4. The valid inputs have length $\frac{1}{2}n(n-1) = 0, 1, 3, 6, 10, 15, 21, 28, 36, \ldots$.
(a) 12 is not a valid input length.
(b) 

Pop Quiz 29.5. We may use multi-tape TMs because a polynomial multi-tape TM can be simulated by a polynomial single-tape TM. The first phase checks that e has at least k 1's.

1: Initialize a second tape with one 1.
2: Mark the rightmost unmarked bit of k as the current bit. If there are no bits of k to mark this first phase is a success.
3: If the marked bit is 0, GOTO step 2.
If the marked bit is 1, Mark as many unmarked 1's in e as there are 1's on the second tape.
If you run out of 1's in e, REJECT.
4: Double the number of 1's on the second tape and GOTO step 2.

In the algorithm above the number of 1's on the second tape is 2^{i-1} when bit i of k is processed. The head on the main tape just moves right along the evidence E, marking 1's, making at most n steps in total. The expensive step is doubling the number of 1's on the second tape. If there are 2^{i-1} 1's then adding another 2^{i-1} 1's takes $\Theta((2^{i-1})^2)$ steps. Let ℓ be the number of bits in k, then the work in doubling is in $\Theta(\sum_{i=1}^{\ell} 2^{2i-2}) = \Theta(\frac{1}{3}(4^{\ell}))$. Since $k \leq n$, it means $2^{\ell} \leq n$ and so the total time spent in step 4 is in $\Theta(n^2)$.

Assume phase 1 succeeds. In phase 2 the algorithm ensures that an edge is present between every pair of vertices in the clique. Equivalently, for every edge not present, we ensure that pair of vertices are not both present in E. Our algorithm needs to mark each edge while simultaneously keeping track of which pair vertices in E that edge connects.

On the right, we illustrate the algorithm keeping track of the node-pairs as it walks through the edgdes on

1: Mark the first edge e_1 and the first two vertices in E.
2: If the last edge marked is 0, REJECT if both marked vertices are 1.
3: Mark the next edge. If there are no more, ACCEPT
4: Update the vertex marks and GOTO step 2.
To update the vertex marks, move the ✘ one right.
If the ✘ cannot move right,
move the ✓ one right and the ✘ to the right of the ✓.

Walking through the edges one step at a time is $\frac{1}{2}n(n-1)$ steps. For each edge, you move right to the ✘ and update it. Finding the ✘ is $O(|\langle G \rangle|)$ since $|\langle G \rangle|$ dominates the size of the input, and updating is $O(n)$. So, there are $\frac{1}{2}n(n-1)$ steps each taking $O(n^2)$ time, for a total of $O(n^4)$ time, which dominates the runtime of the entire algorithm. The runtime is in $O(n^4)$. The input size is in $\Theta(n^2)$, so it's a quadratic algorithm.

✓ ✘✘
1010110101#11#11010
✓✓ ✘ ✘
1010110101#11#11010
✓✓✓ ✘ ✘
1010110101#11#11010
✓✓✓✓ ✘ ✘
1010110101#11#11010
✓✓✓✓✓ ✘✘
1010110101#11#11010
✓✓✓✓✓✓ ✘ ✘
1010110101#11#11010
✓✓✓✓✓✓✓ ✘ ✘
1010110101#11#11010
✓✓✓✓✓✓✓✓ ✘✘
1010110101#11#11010
✓✓✓✓✓✓✓✓✓ ✘ ✘
1010110101#11#11010
✓✓✓✓✓✓✓✓✓✓ ✘✘
1010110101#11#11010

Exercise 29.6.

(a) COLORING: The evidence E is a set of colors, $1, 2, \ldots, \ell$ and a color assignment to each vertex. Since $\ell \leq n$, we need $\log_2 n$ bits to encode each color and $\ell \log_2 n \leq n \log_2 n$ bits to encode all the colors. The color assignments to each vertex also requires at most $n \log_2 n$ bits. So the $|\text{E}|$ is polynomial. The certifier checks that the number of colors ℓ is at most k. Then the certifier processes each edge (u, v) and verifies that the colors assigned to u and v are different. The certifier is polynomial because it does polynomially many things, each taking polynomial time.

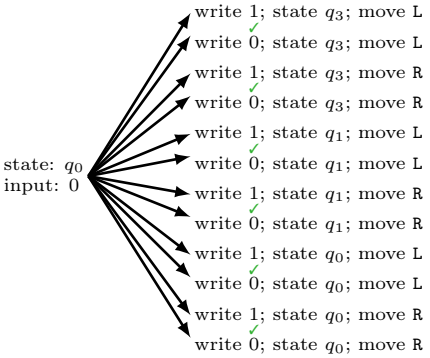
(b) Any problem in P has a polynomial decider. The certifier is just this polynomial decider with no evidence $\text{E} = \varepsilon$. Any polynomial time decider is a polynomial time verifier of (YES).

Pop Quiz 29.7. The second automaton is the first one with (YES) and (NO) states switched. Yet, strings accepted by the first automaton are not necessarily rejected by the second and *vice versa*.

first automaton							second automaton						
ε	0	1	00	01	10	11	ε	0	1	00	01	10	11
(NO)	(YES)	(YES)	(YES)	(YES)	(NO)	(YES)	(YES)	(YES)	(NO)	(YES)	(YES)	(YES)	(YES)

For the complement, you can't just swap accept and reject states. For example, if (say) 2 of 4 computation paths accept, when you exchange (YES) and (NO) states, 2 of 4 computation paths still accept, so you accept. There is asymmetry between accept and reject. To accept, *one* path must accept. To reject, *all* paths must reject. To solve the complement language, you first get an equivalent DFA using subset states (Exercise 24.7), and then flip (YES) and (NO) states.

Pop Quiz 29.8. The deterministic instruction is:
"If in q_1 and bit 0 is read, transition to q_3, write '1' and move R."
The non-deterministic instruction is:
"If in q_1 and bit 0 is read, transition to one of the states q_0, q_1, q_3 (which?), write 0 or 1 (which?), and move R or L (which?)."
The non-deterministic machine gets to try all of these choices, so there are $2 \times 2 \times 3 = 12$ possible choices. The computation splits into 12 possible branches as shown on the right.
In keeping with the tradition for non-deterministic automata, the non-deterministic TM will accept if any one of these branches accepts.



Pop Quiz 29.9. (a) $y = (1 \wedge 0) \wedge (1 \wedge 1) = 0 \wedge 1 = 0$. (b) Yes. $x_1 x_2 = 01$.

Exercise 29.10.

(a) Given input w and evidence E of length $p(n)$, the certifier M runtime is $t(n)$, a polynomial in n. By Theorem 29.4 in time $\text{poly}(t(n))$, we construct a circuit of size $\text{poly}(t(n))$ which is fed into the black-box. The runtime of the black-box is polynomial in the size of *its* input, therefore, the runtime of the black-box is $\text{poly}(\text{poly}(t(n)))$. So,

$$\text{total runtime} = \text{time to create circuit} + \text{time to run the black-box} = \text{poly}(t(n)) + \text{poly}(\text{poly}(t(n))),$$

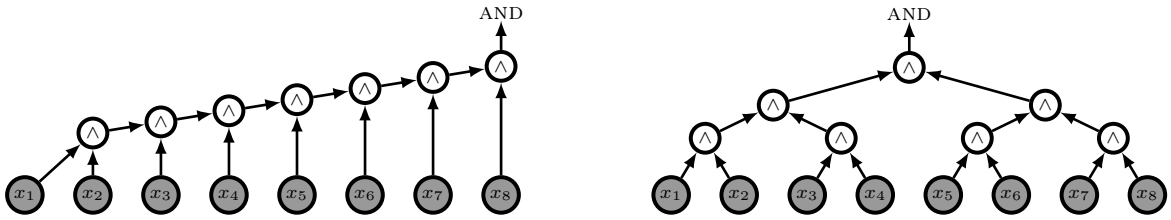
which is polynomial because a polynomial evaluated on a polynomial is a polynomial.

(b) We must construct different certifier circuits for each evidence length from $0, 1, \ldots, p(n)$. So, we need to run the black-box $p(n)$ times, for each of the $p(n)$ circuits, which essentially multiplies the polynomial running time by $p(n)$. Since the product of polynomials is a polynomial, the runtime remains polynomial.

Note that if you wish to only use the black-box just once, you can take each of the $p(n)$ circuits and send them through a massive $p(n)$-way OR. Feed this gigantic circuit (which is only about $p(n)$ times bigger than the one in (a)) into the black-box. If the black-box says the circuit is satisfiable, then one of the smaller circuits is satisfiable. If the black-box says the circuit is not satisfiable, then none of the smaller circuits is satisfiable.

Exercise 29.11.

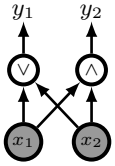
(a) We give two different types of AND circuits, illustrating the constructions for $\ell = 8$.



In both circuits, the number of AND-gates used is $\ell - 1$. The number of gates used is called the *size* of the circuit, so the sizes of our circuits are $\ell - 1$. A circuit is a directed graph. The *depth* of a circuit is the length of the longest path. The main difference between our two circuits is the depth. On the left, the depth is $\ell - 1$, linear in ℓ. You should convince yourself that the circuit on the right has depth $\lceil \log_2 \ell \rceil$, logarithmic in ℓ.

Processor-chips are implemented using gates, starting with building blocks like multi-input-AND, adders, multipliers, sorters, etc. Designing circuits to accomplish tasks while minimizing size and depth are important considerations for efficienct chip-design. Circuit complexity theorists study the minimum size and depth requirements for certain basic operations which are primitives of more complex operations. We know quite impressive designs for many basic operations, but surprisingly little about the best one can do, even for basic operations.

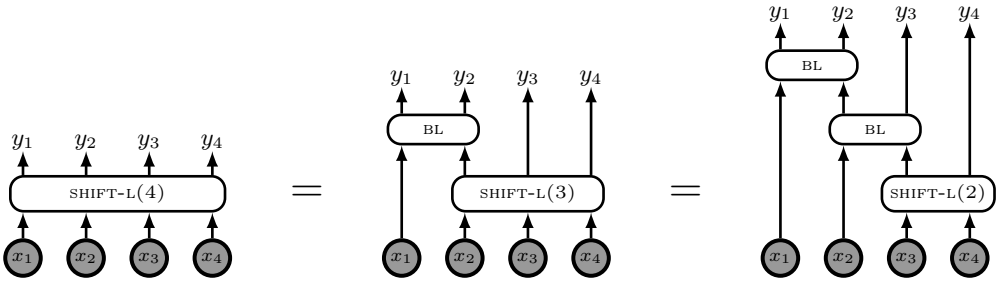
(b) We begin with the primitive task of moving a 1 all the way to the left. To simplify, consider $n = 2$ (two input bits). On the left is a circuit for 2 input bits. Verify the input-output table on the right to confirm that this circuit shifts the 1 to the left. This circuit also sorts two input-bits. Let us denote this circuit as the bubble-left (BL) "gate". The 1 in the input bubbles "up" to the left. We now combine BL-gates to build a circuit that shifts a 1 (if there is a 1) all the way to the left of an n-bit string. This is a SHIFT-L circuit.



input		output	
x_1	x_2	y_1	y_2
0	0	0	0
0	1	1	0
1	0	1	0
1	1	1	1

Suppose we have a SHIFT-L circuit for $n-1$ bits. For the n bits $x_1, \ldots, x_n$, apply the SHIFT-L circuit to $x_2, \ldots, x_n$. Now, if there is a 1 in $x_2, \ldots, x_n$, it will be on the left, at position x_2. Applying the BL-gate to x_1 and the output

at the x_2 position will move the 1 at the x_2-position to the left. Here is an illustration for a 4-bit input.



In the second step, we recursively applied the construction to SHIFT-L(3). Observe that SHIFT-L(2) is just a BL-gate, and so SHIFT-L(4) is just a cascade from right to left of 3 BL-gates. In general, SHIFT-L(n) is a cascade from right to left of $n-1$ BL-gates. Since a BL-gate consists of two $\wedge/\vee$ gates, SHIFT-L(n) uses $2n-2$ gates. The proof is by induction. The base case is SHIFT-L(2) which is just a BL-gate that uses 2 $\wedge/\vee$ gates. For the induction, assume SHIFT-L(n) uses $2n-2$ gates; by our construction, SHIFT-L($n+1$) adds one BL-gate to SHIFT-L(n), adding 2 $\wedge/\vee$ gates, resulting in a total of $2n$ gates. The two important properties of SHIFT-L(n) that we need are:

Lemma 30.9. Let $(y_1, \ldots, y_n) = \text{SHIFT-L}(n)(x_1, \ldots, x_n)$. Then,

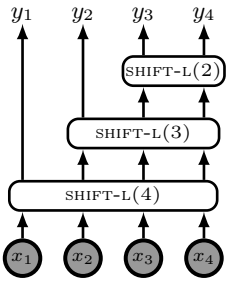
(i) $(y_1, \ldots, y_n)$ and $(x_1, \ldots, x_n)$ have the same number of 1's;
(ii) if $(x_1, \ldots, x_n)$ contains a 1, then $y_1 = 1$.

In words, SHIFT-L(n) outputs a permutation of its input with at least one 1 having "bubbled-up" all the way to the left. Tinker and confirm that SHIFT-L(4) on 0111 gives 1011. The proof of the lemma is by induction.

Proof. The base case is SHIFT-L(2) for which the claim is true by inspecting the input-output table for the BL-gate. Suppose the claim holds for SHIFT-L(n) and consider SHIFT-L($n+1$) applied to $(x_1, x_2, \ldots, x_{n+1})$ in two steps. First apply SHIFT-L(n) to $(x_2, \ldots, x_{n+1})$ to get $(y_2', y_3, \ldots, y_{n+1})$. Now apply the BL-gate to (x_1, y_2') to get (y_1, y_2). By the induction hypothesis, both operations preserve the bits, so the result is a permutation. We prove the contrapositive of (ii). If $y_1 = 0$, then, from the input-output table of the BL-gate, the only possibility is $x_1 = y_1' = 0$. If $y_1' = 0$, then by the induction hypothesis there were no 1's in $(x_2, \ldots, x_{n+1})$, for if there were 1's, the application of SHIFT-L(n) would make $y_1' = 1$. Thus, if $y_1 = 0$, then $x_1 = x_2 = \cdots = x_{n+1} = 0$, that is there are no 1's in the input (the contrapositive of property (ii)). Therefore, properties (i) and (ii) hold for SHIFT-L($n+1$), and the lemma follows by induction. ∎

We now use SHIFT-L(n) to construct the sorter. The idea is simple. Repeatedly shift a 1 to the left. Eventually, all the 1's will be on the left. This idea is illustrated on the right for 4 inputs. For an n-bit input, the number of gates in the sorter is

$$2 + 4 + \cdots + 2(n-1) = 2\sum_{i=1}^{n-1} i = n(n-1) \in \Theta(n^2).$$



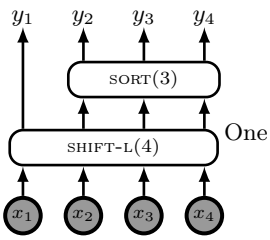
It is helpful to see how the sorter works on input 0111.

$$0111 \xrightarrow{\text{SHIFT-L}(4)} 1011 \xrightarrow{\text{SHIFT-L}(3)} 1101 \xrightarrow{\text{SHIFT-L}(2)} 1110$$

We need all the layers of SHIFT-L, because intermediate outputs may not be sorted. Observe that in each application of SHIFT-L, a 1 "bubbles-up" to the left. You may have seen bubble-sort in earlier programming courses. Here is circuit version of bubble-sort. We now prove the sorter works.

Theorem 30.10. Our construction produces a sorter using $\Theta(n^2)$ $\wedge/\vee$ gates.

Proof. The proof is by induction, based on the observation that our SORT(n) circuit is composed of a SHIFT-L(n) circuit followed by a SORT($n-1$) circuit applied to the last $n-1$ outputs of the SHIFT-L(n) circuit, as illustrated for $n = 4$ on the right. The SHIFT-L(n) circuit moves a 1 to the left, which becomes the output y_1. By the induction hypothesis, we assume that SORT($n-1$) works, which means that its output is 1's followed by 0's, which become the outputs $y_2, \ldots, y_n$. Therefore the full output $y_1, \ldots, y_n$ is 1's followed by zeros, which is sorted as required. ∎



One of the undesirable features of our sorter is that its depth is in $\Theta(n)$. You may now try to find a sorting circuit with smaller depth.

Pop Quiz 29.12.

(a) The first three bits after sorting are 1, so the AND after the sorter outputs 1. It suffices to show that every input to the AND in the clique-verifier is 1: $C_{1,2} = C_{1,3} = C_{1,4} = C_{1,5} = 1$ because $x_1 = 0$; $C_{2,3} = 1$ because $e_{2,3} = 1$;

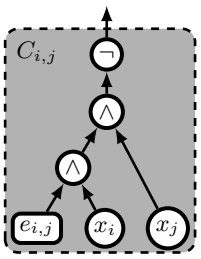
$C_{2,4} = 1$ because $e_{2,4} = 1$; $C_{2,5} = 1$ because $x_5 = 0$; $C_{3,4} = 1$ because $e_{3,4} = 1$; $C_{3,5} = C_{4,5} = 1$ because $x_5 = 0$. The output being 1 means that 01110 is a clique of size at least 3 in the graph 1010110101.

(b) Each circuit $C_{i,j}$ uses 2 gates, and there are $\frac{1}{2}n(n-1)$ of those for a total of $n(n-1)$ gates, where n is the number of vertices. (we usually exclude NOT-gates from the size of a circuit. If you counted NOT-gates, it is not a big deal.) The AND in the clique-verifier therefore needs $\frac{1}{2}n(n-1)-1$ gates, so the size of our clique verifier is $\frac{3}{2}n(n-1)-1$. The sorter uses $n(n-1)$ gates and the AND after the sorter uses $k-1$ gates. So the total number of gates used is

$$\tfrac{5}{2}n(n-1) + k - 2 \in \Theta(n^2).$$

The input size is in $\Omega(n^2)$, so the verifier size is linear in the input size. For $n = 5$ and $k = 3$, our formula evaluates to 51 gates. (If you counted NOT-gates, your should get 71 gates.)

Exercise 29.13. We mimic the Clique-verifier. The only difference is the primitive circuit $C_{i,j}$ which ensured the "clique-condition". Here, we must ensure the "independent set-condition". For the clique-condition, the circuit $C_{i,j}$ verified that if vertices i, j are in the clique, then edge $e_{i,j}$ is in the graph. For the independent set-condition, it is the opposite: if vertices i, j are in the independent set, then edge $e_{i,j}$ is *not* in the graph. That is, for the IndSet problem, $C_{i,j}$ computes $\overline{e_{i,j}} \vee \overline{x_i} \vee \overline{x_j}$ (as opposed to $e_{i,j} \vee \overline{x_i} \vee \overline{x_j}$ for the Clique problem). Equivalently, we want $C_{i,j}$ to compute $\overline{e_{i,j} \wedge x_i \wedge x_j}$. We give a circuit which implements this independent set-condition on the right. The rest of the circuit, including the size-verifier, is identical to that for Clique.



Pop Quiz 29.14. We use direct proof to prove, for every $\mathcal{L} \in \mathsf{NP}$,

IF $\mathcal{L}^*$ is polynomialy solvable, THEN $\mathcal{L}$ is polynomialy solvable.

Suppose $\mathcal{L}^*$ is polynomialy solvable and consider any $\mathcal{L} \in \mathsf{NP}$. Since (29.3) is T, it means CircuitSat is polynomialy solvable. Since CircuitSat is NP-complete (claim in (29.2)), it means $\mathcal{L}$ is polynomialy solvable.

Pop Quiz 29.15.

(a) There is nothing to prove because 1 means T and 0 means F.

(b) Suppose $u = v$, so $u = v = 0$ or $u = v = 1$. In both cases, $(u \vee \overline{v})$ and $(\overline{u} \vee v)$ are T, $u = v \to (u \vee \overline{v}) \wedge (\overline{u} \vee v)$.
Now suppose $(u \vee \overline{v}) \wedge (\overline{u} \vee v)$ is T. If $u = 1$, then for $(\overline{u} \vee v)$ to be T, $v = 1$ so $u = v$. If $u = 0$, then for $(u \vee \overline{v})$ to be T, $v = 0$ so $u = v$. In both cases $v = u$, therefore $(u \vee \overline{v}) \wedge (\overline{u} \vee v) \to u = v$.
You may wonder how we got this equivalent logical expression to $u = v$. So, we take this opportunity to introduce two fundamental representations of Boolean functions in computer science: the disjunctive normal form (DNF) which is an OR of ANDs and the conjunctive normal form (CNF) which is an AND of ORs. Both representations are based on the truth-table for $u = v$ shown on the right.

u	v	$u = v$?
0	0	T
0	1	F
1	0	F
1	1	T

For $u = v$ to be T, either $u = 0$ and $v = 0$ or $u = 1$ and $v = 1$. That is,

$$u = v \text{ is equivalent to } (\overline{u} \wedge \overline{v}) \vee (u \wedge v) \qquad \text{(DNF)}$$

For $u = v$ to be F, either $u = 0$ and $v = 1$ or $u = 1$ and $v = 0$. That is,

$$\overline{u = v} \text{ is equivalent to } (\overline{u} \wedge v) \vee (u \wedge \overline{v})$$

This means $u = v$ is equivalent to $\overline{(\overline{u} \wedge v) \vee (u \wedge \overline{v})}$. We now use De Morgan's laws for negation, namely $\overline{A \vee B} \overset{\text{eqv}}{\equiv} \overline{A} \wedge \overline{B}$ and $\overline{A \wedge B} \overset{\text{eqv}}{\equiv} \overline{A} \vee \overline{B}$ to get

$$u = v \text{ is equivalent to } (u \vee \overline{v}) \wedge (\overline{u} \vee v) \qquad \text{(CNF)}$$

(c) Suppose $u = v \vee w$. There are four cases corresponding to (v, w) being $(0,0), (0,1), (1,0), (1,1)$. In each case $(u \vee \overline{v}) \wedge (u \vee \overline{w}) \wedge (\overline{u} \vee v \vee w)$ is T.
Now suppose $(u \vee \overline{v}) \wedge (u \vee \overline{w}) \wedge (\overline{u} \vee v \vee w)$ is T. If $u = 1$, then for $(\overline{u} \vee v \vee w)$ to be T, $(v \vee w)$ must be T, that is $u = v \vee w$. If $u = 0$, then for $(u \vee \overline{v})$ to be T, $v = 0$ and for $(u \vee \overline{w})$, $w = 0$. So $v \vee w = 0$, i.e. $u = v \vee w$.
It is a useful exercise to recover this logical expression for $u = v \vee w$ from its truth-table using the CNF construction.

(d) This follows from (c) because $u = v \wedge w$ if and only if $\overline{u} = \overline{v \wedge w} \overset{\text{eqv}}{\equiv} \overline{v} \vee \overline{w}$. So, we get the expression in (c) with u, v, w replaced by $\overline{u}, \overline{v}, \overline{w}$.

Pop Quiz 29.16.

clause 1	clause 2	clause 3	clause 4		
y	$\overline{x}$	$\overline{x}$	$\overline{z}$	$\to$	$(x, y, z) = (\text{F}, \text{T}, \text{F})$;
y	$\overline{x}$	$\overline{z}$	$\overline{z}$	$\to$	$(x, y, z) = (\text{F}, \text{T}, \text{F})$;
z	$\overline{x}$	$\overline{x}$	$\overline{y}$	$\to$	$(x, y, z) = (\text{F}, \text{F}, \text{T})$;
z	z	$\overline{x}$	$\overline{y}$	$\to$	$(x, y, z) = (\text{F}, \text{F}, \text{T})$;

Exercise 29.17. Only problems in NP can be NP-complete. So when trying to show that a problem is NP-complete, you should always verify first that the problem is in NP.

(a) We know Clique $\in$ NP. For the NP-complete problem $\mathcal{L}^*$, we choose IndSet. We show that IndSet is polynomialy reducible to Clique. Recall the complement graph $\overline{G}$ to a graph G. The complement graph is obtained from the

original graph by removing all existing edges and adding all other edges:

$$(u, v) \text{ is an edge in } \overline{G} \leftrightarrow (u, v) \textit{ is not } \text{an edge in } G.$$

An independent set in the graph is a clique in the complement graph and *vice versa*. Therefore, G has an independent set of size k if and only if the complement graph has a clique of size k. If we have a black-box which polynomialy solves Clique, we can solve IndSet by using the black-box on the complement graph. Therefore,

Theorem 30.11 (Clique is NP-complete)**.** *If* Clique $\in$ P, *then* IndSet $\in$ P.

(b) First, VertexCover is in NP: check each edge to verify in polynomial time whether a set is a vertex cover – every edge should have at least one end in the vertex cover; all that remains is to check the size of the vertex cover. So, a (YES)-instance of VertexCover can be polynomialy verified given the evidence, which is the vertex cover.

We polynomially reduce from the NP-complete problem $\mathcal{L}^* =$ IndSet to VertexCover. Assume a graph has n vertices $V = \{v_1, \ldots, v_n\}$, and let $S \subseteq V$ be a subset of the vertices. The complement of S is $\overline{S} = V - S$.

Lemma 30.12. *S is an independent set of size k if and only if $\overline{S}$ is a vertex cover of size $n - k$.*

Proof. Suppose S is an independent set of size k. Consider any edge e. If both endpoints of e are in S then S is not an independent set (there cannot be an edge between any two vertices in S). Therefore at least one endpoint of e is in $\overline{S}$. Since e is arbitrary, every edge has at least one endpoint in $\overline{S}$, and so $\overline{S}$ is a vertex cover of size $n - k$.

Suppose $\overline{S}$ is a vertex cover of size $n - k$. Now consider any pair of vertices in S. If there is an edge between these two vertices, then that edge does not have an endpoint in $\overline{S}$, contradicting $\overline{S}$ being a vertex cover. Therefore no pair of vertices in S is adjacent and so S is an independent set of size k. ∎

Given a black-box to solve VertexCover, we solve IndSet with size k by running the black-box on the same graph with size $n - k$ (seeking a vertex cover of size at most $n - k$). Lemma 30.12 assures us that this works.

Theorem 30.13 (VertexCover is NP-complete)**.** *If* VertexCover $\in$ P, *then* IndSet $\in$ P.

Exercise 29.18.

(a) This is an NP-completeness reduction from a general problem (Clique) to a restriction of the problem to special cases (in BigClique, k must be large). We need to show that if we have a polynomial black-box that solves BigClique we can polynomialy solve Clique.

Consider any instance G, k of Clique and suppose G has n vertices $v_1, \ldots, v_n$. We cannot use our black-box to solve this problem because k may be too small. Our solution is to convert this clique problem to another equivalent one with a large k. Construct a new graph G' by adding n new vertices $w_1, \ldots, w_n$ to G. Also add edges from every w-vertex to every other vertex in G'. Clearly, it takes polynomial time to construct G' from G.

Given a k-clique in G, its vertices plus all the w-vertices are a $(k+n)$-clique in G'. Further, every $(k+n)$-clique in G' contains at least k v-vertices which are all connected to each other and so contain a k-clique in G. Therefore,

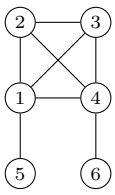
Lemma 30.14. *G contains a k-clique if and only if G' contains a $(k+n)$-clique.*

Here is an algorithm for Clique. First construct G'. Now run the black-box on G' with $k' = k+n$ (which is larger than half the vertices in G'). Output the answer (YES)/(NO) from the black-box. The Lemma ensures correctness.

(b) We use a polynomial black-box for FreqItems to polynomialy solve Clique.[2] Hence, FreqItems is NP-complete. Given inputs $G = (V, E)$ and k to Clique, construct an input to FreqItems (binary matrix A, popularity n and basket-size ℓ). Run the black-box on this input to FreqItems. The answer tells if G has a k-clique.

Customers are vertices in G and items are edges in G. Each vertex (customer) buys an edge (item) if the customer is *not* an end point of the edge. Here is an example. The input to Clique is on the left; A is on the right.

$G; k = 4$



A; $n = 2, \ell = 6$

customers (nodes)	items (edges) (1,2)	(1,3)	(1,4)	(1,5)	(2,3)	(2,4)	(3,4)	(4,6)
1	0	0	0	0	1	1	1	1
2	0	1	1	1	0	0	1	1
3	1	0	1	1	0	1	0	1
4	1	1	0	1	1	0	0	0
5	1	1	1	0	1	1	1	1
6	1	1	1	1	1	1	1	0

We highlighted a solution to FreqItems with a basket of size $\ell = 6$ bought by $n = 2$ customers. The other 4 customers (nodes) must form a 4-clique in G because the 6 edges in our basket (bought by two customers) have

[2] FreqItems is more general than BalancedBipartiteClique which is the NP-complete problem GT24 in the Garey & Johnson book *Computers and Intractability*. A more general problem cannot be easier.

endpoints among the 4 customers who did *not* buy the edges. The maximum number of edges in a group of 4 vertices is 6, which can only be so if every edge is present. That is, those 4 vertices are a 4-clique.

For a general instance of Clique, we construct an instance A of FreqItems as we described. Now run our black-box on A with $n = |V| - k$ and $\ell = \frac{1}{2}k(k-1)$ to get the answer to the instance of Clique. The next lemma proves the answer is correct. Further, since the black-box is polynomial, the entire solution to Clique is polynomial.

Lemma 30.15. There is a k-clique in $G = (V, E)$ if and only if the instance A of FreqItems that we constructed has a basket of size $\frac{1}{2}k(k-1)$ which is bought by $|V| - k$ customers.

Proof. Suppose there is a k-clique in $G = (V, E)$. In A, the $\frac{1}{2}k(k-1)$ edges in the k-clique is a basket of edges which is bought by each of the $|V| - k$ vertices (customers) not in the clique.

Suppose A has a basket of size $\frac{1}{2}k(k-1)$ which is bought by $|V| - k$ customers. Those $\frac{1}{2}k(k-1)$ edges in the basket only connect to the k customers who did not by the basket. Therefore, those k customers are a subgraph with $\frac{1}{2}k(k-1)$ edges, which can only be the case if every edge is present, and they form a k-clique in G. ∎

Let us summarize the general methodology for proving a problem is NP-complete.

To show $\mathcal{L}$ is NP-complete using the NP-complete problem $\mathcal{L}^*$

1: Start with a *general* instance I^* of $\mathcal{L}^*$.
2: Construct an instance I of $\mathcal{L}$ from I^*, in polynomial time.
3: Show that $I^* \in \mathcal{L}^*$ *if and only if* $I \in \mathcal{L}$.