Advanced Counting

Reading

- Malik Magdon-Ismail. Discrete Mathematics and Computing.
  - Chapter 14

Overview

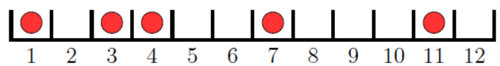
- Sequences with repetition
  - Anagrams
- Inclusion-exclusion: extending the sum-rule to overlapping sets
  - Derangements
- Pigeonhole principle
  - Social twins
  - Subset sums

Selecting k from n Distinguishable Objects

- Last time we saw the number of ways to select k from n objects in the following settings:
  1. k-sequence with repetition:
  $$n^k$$
  2. k-sequence without repetition (permutations):
  $$\frac{n!}{(n-k)!}$$
  3. k-subset with repetition (candy selection problem):
  $$\binom{n+k-1}{k-1}$$
  4. k-subset without repetition (combinations):
  $$\frac{n!}{(n-k)!\,k!}$$
- How about a sequences that contain a specific number per object type?
  - E.g., 5 red candies, 4 blue candies, 3 green candies
  - Known as $(k_1, k_2, \ldots, k_r)$-sequences

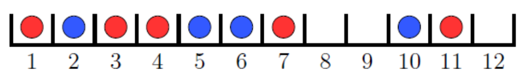
Selecting k from n Distinguishable Objects, cont'd

- How about sequences that contain a specific number per object type?
  - E.g., 5 red candies, 4 blue candies, 3 green candies
  - Known as $(k_1, k_2, \ldots, k_r)$-sequences
- How do we count this weird set?
  - Look at all possible positions for each candy type
  - First, count all possible ways to place red candies. How many is that?

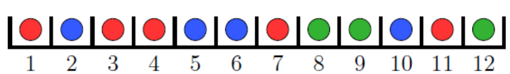


$$\binom{12}{5}$$

  - How many ways can we place the remaining blue candies?
    - We have 7 remaining slots and 4 candies, so $\binom{7}{4}$



  - Finally, we have 3 remaining slots and 3 green candies: $\binom{3}{3}$



Selecting k from n Distinguishable Objects, cont'd

- How about a sequences that contain a specific number per object type?
  - E.g., 5 red candies, 4 blue candies, 3 green candies
  - Known as $(k_1, k_2, \dots, k_r)$-sequences
- The final number of ways we can order the candies is:

$$\binom{12}{5,4,3} = \binom{12}{5} \times \binom{7}{4} \times \binom{3}{3}$$
$$= \frac{12!}{5!\,7!} \times \frac{7!}{3!\,4!} \times \frac{3!}{0!\,3!} = \frac{12!}{5!\,4!\,3!}$$

Anagrams: All “Words” Using the Letters AARDVARK

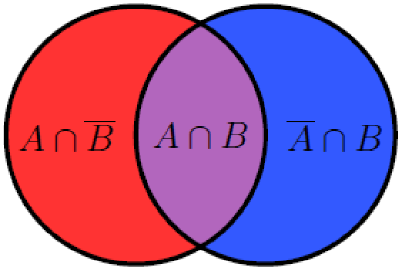
Source: wikipedia

- A sequence of 8 letters: 3 A’s, 2 R’s, 1 D, 1 V, 1 K
- How many sequences is that?
- Number of such sequences is

$$\binom{8}{3,2,1,1,1} = \frac{8!}{3!\,2!\,1!\,1!\,1!} = 3360$$

- **Exercise.** What is the coefficient of $x^2y^3z^4$ in the expansion of $(x+y+z)^9$?
  - *[Hint: Sequences of length 9 (why?) with 2 x’s, 3 y’s and 4 z’s.]*

Extending the Sum Rule to Overlapping Sets



- What is the size of $|A \cup B|$?

$$|A \cup B| = |A| + |B| - |A \cap B|$$

  – Breaks $A \cup B$ into smaller subsets

- **Example.** How many numbers in $1, \dots, 10$ are divisible by 2 or 5?

$A = \{$numbers divisible by 2$\}$. $|A| = 5$.

  – If the sequence contains n numbers, what is the general formula for $|A|$?

    - TINKER! Suppose n is even (as above):

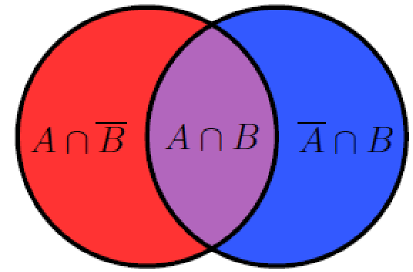
$$|A| = \frac{n}{2}$$

    - TINKER! Suppose n is odd:

$$|A| = \frac{n-1}{2}$$

    - We can write this using the short-hand notation $|A| = \left\lfloor \frac{10}{2} \right\rfloor$
    - The floor $\lfloor x \rfloor$ function returns the largest integer $n \leq x$

Extending the Sum Rule to Overlapping Sets



- What is the size of $|A \cup B|$?

$$|A \cup B| = |A| + |B| - |A \cap B|$$

  - Breaks $A \cup B$ into smaller subsets

- **Example.** How many numbers in $1, \ldots, 10$ are divisible by 2 or 5?

$A =$ {numbers divisible by 2}. $\quad |A| = 5. \quad \left(|A| = \left\lfloor \frac{10}{2} \right\rfloor\right)$

$B =$ {numbers divisible by 5}. $\quad |B| = 2.$

  - If the sequence contains n numbers, what is the general formula for $|B|$?
    - TINKER! Suppose n is divisible by 5 (as above):

$$|B| = \frac{n}{5}$$

    - TINKER! Suppose n is **not** divisible by 5:

$$|B| = \frac{n_{5^-}}{5}$$

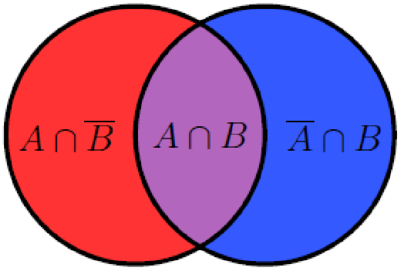
      - Inventing notation: n_{5^-} is the largest integer s.t. $5 | n_{5^-}$ AND $n_{5^-} < n$
    - Notice that once again $|B| = \left\lfloor \frac{10}{5} \right\rfloor$
      - when n not divisible by 5, $\frac{n_{5^-}}{5} < \frac{n}{5} < \frac{n_{5^+}}{5}$

Extending the Sum Rule to Overlapping Sets

- What is the size of $|A \cup B|$?

$$|A \cup B| = |A| + |B| - |A \cap B|$$

  - Breaks $A \cup B$ into smaller subsets



- **Example.** How many numbers in $1, \dots, 10$ are divisible by 2 or 5?

$A =$ {numbers divisible by 2}. $|A| = 5.$ $\left(|A| = \left\lfloor \frac{10}{2} \right\rfloor\right)$

$B =$ {numbers divisible by 5}. $|B| = 2.$ $\left(|B| = \left\lfloor \frac{10}{5} \right\rfloor\right)$

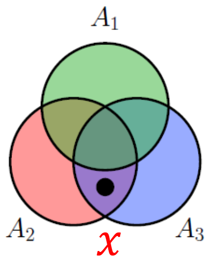
$A \cap B =$ {numbers divisible by 2 AND 5}. $|A \cap B| = 1.$ $\left(|A \cap B| = \left\lfloor \frac{10}{lcm(2,5)} \right\rfloor\right)$

- (verify that the lcm is indeed the number we want above!)

$A \cup B =$ {numbers divisible by 2 OR 5}

$$|A \cup B| = |A| + |B| - |A \cap B| = 5 + 2 - 1 = 6$$

Inclusion-Exclusion



- What about a union of three sets:

$$|A_1 \cup A_2 \cup A_3|$$

- Looking at the disjoint sets in the picture, I claim that the formula is:

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|$$

  - Why?
  - Avoid double-counting: start from largest set, then subtract overlap, then add back the overlap of the subtracted, etc.

- *Proof sketch*. Consider $x \in A_2 \cap A_3$. How many times is x counted?

$$\begin{array}{ccccccccccccc} |A_1| & + & |A_2| & + & |A_3| & - & |A_1 \cap A_2| & - & |A_1 \cap A_3| & - & |A_2 \cap A_3| & + & |A_1 \cap A_2 \cap A_3| \\ 0 & + & 1 & + & 1 & - & 0 & - & 0 & - & 1 & + & 0 \end{array}$$

  - Contribution of x to sum is +1. Repeat for each region.
  - Should be true for each region. Means there's no double-counting.

Inclusion-Exclusion, cont'd

- **Example.** Give 3 coats to 3 people so that no one gets their coat. How many ways?
  - How do we split the sets?

$$A_i = \{person\ i\ gets\ their\ coat\}, |A_i| = 2!$$

    - Why? (position i is fixed)

$$A_{ij} = \{people\ i\ and\ j\ get\ their\ coats\}, |A_{ij}| = 1!$$

    - Why? (positions i and j are fixed)

$$A_{123} = \{people\ 1, 2\ and\ 3\ get\ their\ coats\}, |A_{123}| = 1$$

    - All positions are fixed

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_{12}| - |A_{13}| - |A_{23}| + |A_{123}|$$
$$= 2 + 2 + 2 - 1 - 1 - 1 + 1 = 4$$

- The answer we seek is $3! - 4 = 2$
  - Why?
  - How big is the set of all possible coat assignments?

$$3 \times 2 \times 1 = 3!$$

  - Subtract from those the set A = {at least one person has their coat on}

$$A = A_1 \cup A_2 \cup A_3$$

- **Exercise.** How many numbers in $1, \ldots, 100$ are divisible by 2,3 or 5?

Inclusion-Exclusion, cont'd

- What about the general formula:

$$|A_1 + A_2 + \cdots + A_n|$$

- It seems that

$$\begin{aligned}|A_1 + A_2 + \cdots + A_n| &= \\ &= (|A_1| + \cdots + |A_n|) \\ &\quad -(|A_1 \cap A_2| + |A_1 \cap A_3| + \cdots + |A_{n-1} \cap A_n|) \\ &\quad +(|A_1 \cap A_2 \cap A_3| + |A_1 \cap A_3 \cap A_4| + \cdots + |A_{n-2} \cap A_{n-1} \cap A_n|) \\ &\quad - \cdots\end{aligned}$$

- Claim:

$$|A_1 + A_2 + \cdots + A_n| = \sum_{k=1}^{n} (-1)^{k+1} \times [\text{sum of all } k\text{-way intersection sizes}]$$

- *Proof sketch*. Suppose x lies in r sets.
  - How many 1-way intersections contain x?

$$\binom{r}{1}$$

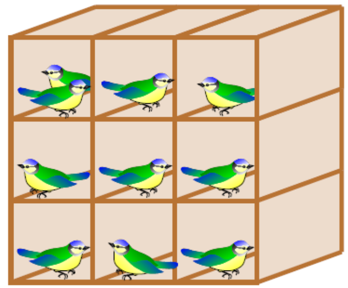
  - How many 2-way intersections contain x?

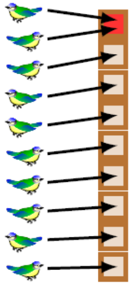
$$\binom{r}{2}$$

  - Verify that x contributes only 1 to the full sum.

Pigeonhole Principle

- If you have more guests than spare rooms, then some guests will have to share



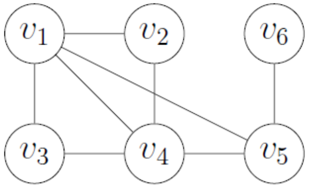


  - *More* pigeons than pigeonholes
- *Theorem*. A pigeonhole has two or more pigeons (if there are more pigeons than pigeonholes).
- *Proof.* (By contraposition). Suppose no pigeonhole has 2 or more pigeons.
  - Let x_i be the number of pigeons in hole i, $x_i \le 1$.

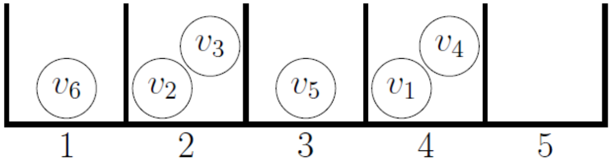
$$\text{number of pigeons} = \sum_i x_i \le \sum_i 1 = \text{number of pigeonholes}$$

Every Graph Has at Least One Pair of Social Twins

- Two nodes are *social twins* if they have the same degree.
- Consider a connected graph



- What are the nodes' degrees?



  - What if we had a graph with 0-degree nodes?
    - Exclude that node and only consider the connected sub-graph
- Degrees $1, 2, \ldots, (n-1)$, are the pigeonholes
- Vertices $v_1, v_2, \ldots, v_n$, are the pigeons
- There are n pigeons and $(n-1)$ pigeonholes, so at least two vertices are in the same degree-bin
- This proof is not very satisfactory (why?)
  - Who are those social twins? What are their degrees?
  - Known as a non-constructive proof

Non-Constructive Proof and the Eye-Spy Dilemma

- Non-constructive proofs are not always desirable
  – A non-constructive proof that P = NP is almost useless
  – Sure, we know that they are equal, but that still doesn’t tell us how to factor numbers
- Sometimes non-constructive proofs can be valuable
- Password checking is a type of non-constructive proof
  – You enter your password and you get a “yes/no” answer
  – A “no” answer doesn’t leave you any the wiser as to the true password

Non-Constructive Proof and the Eye-Spy Dilemma, cont'd

- Can you find the cat in this image?

Non-Constructive Proof and the Eye-Spy Dilemma, cont'd

- How do I convince you that the cat is in the image without pointing to the cat?
  - I want you to know the problem is fair without revealing the solution
- If only we had an infinite black cloth that has a cat-shaped hole
  - I could slide the image under the cloth until the cat shows up
- Suppose my cloth is not perfect and it reveals a bit more than necessary

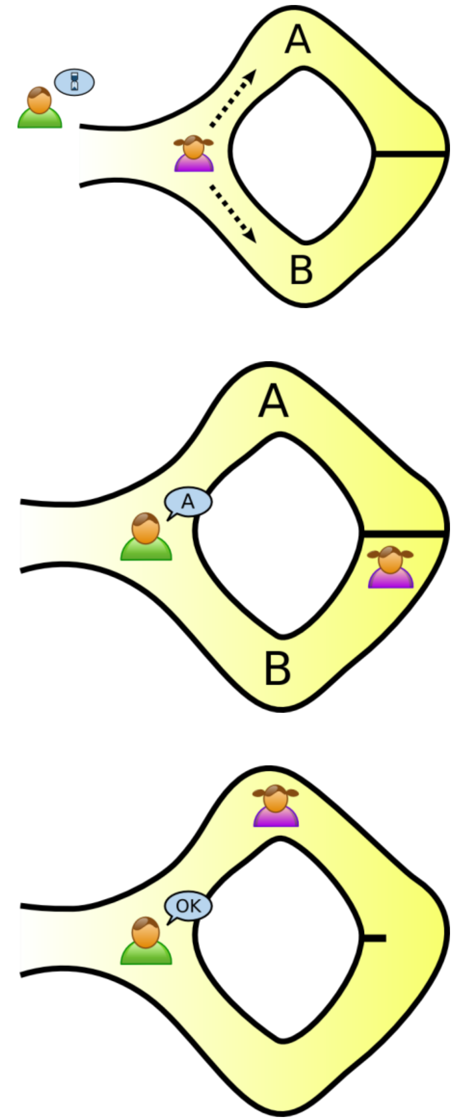
Non-Constructive Proof and the Eye-Spy Dilemma, cont’d

- Can you now find the cat in this image?

Zero-Knowledge Proof and the Ali Baba cave

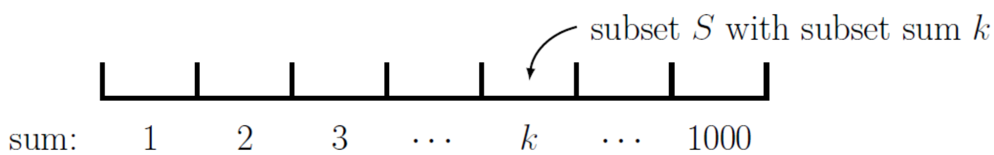
Rensselaer

- Suppose that Peggy found a secret word used to open a door in a cave
- Victor wants to know if Peggy really knows the secret word
  - (Peggy won't actually say the word because it's secret)
- So Victor designs an experiment
  - Peggy goes in the cave
  - Victor can't see which path she takes
  - Victor flips a coin
  - If coin comes up heads, Victors asks Peggy to come back using path A (o.w. using B)
  - If Peggy knows the word, she can use any path
  - If Peggy doesn't know the word, she has to go back the way she entered
    - She has a 50% chance of taking the right path
    - If they repeat this many times, her chance of guessing right goes down to 0



Subset Sums

- Suppose I pick 10 numbers between 1 and 100
  - Call my set S
    - e.g., $S = \{1,2,3,4,5,6,7,8,9,99\}$
  - I claim that at least two distinct subsets of S have the same subset-sum.
  - In my case, this is obvious: $\{1,2\}$ and $\{3\}$
    - This is a constructive proof, but let's look at a zero-knowledge one also
- A subset's sum is $x_1 + x_2 + \cdots + x_{10} \leq 10 \times 100 = 1000$



- Pigeonholes: bins corresponding to each possible subset-sum, $1, 2, \ldots, 1000$
- Pigeons: the non-empty subsets of a 10-element set:

$$2^{10} - 1 = 1023$$

- At least two subsets must be in the same subset-sum-bin.
- **Practice.** Exercise 14.6.
- **Practice.** Exercise 14.7.