Unit 8
Counting

Computer Science 1002

Introduction to Logic for Computer Scientists

1

Puzzle: chocolate squares

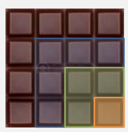
- Suppose you have a piece of chocolate like this:

- How many squares are in it?
  – of all sizes, from single to the whole thing

2

Puzzle: chocolate squares

Suppose you have a piece of chocolate like this. How many squares are in it?
- – One square 4x4
- – Four squares 3x3
  - Can start (e.g, top-left corner) at (1,1), (1,2), (2,1), (2,2)
  - 2 choices for a row, 2 choices for a column.
- – Nine squares 2x2
  - Can start at any (x,y) with $x \in \{1,2,3\}$, $y \in \{1,2,3\}$
  - So 3*3 = 9 choices.
- – 16 squares 1x1.



- Total: 1+4+9+16=30 squares

3

Puzzle: chocolate squares

Suppose you have a piece of chocolate like this. How many squares are in it?
- – One square 13x13
- – …
- – 13*13=169 squares 1x1
  - 12*12 2x2
  - 11*11 3x3
  - ….

- General formula: starting with an n x n piece of chocolate, get
- $\sum_{i=1}^{n} i^2 = n(n+1)(2n+1)/6$ squares.

4

Combinatorics

- Counting various ways to arrange things.
  – Leading to probability theory.
- How long would a program that does brute-force search over possibilities will run?
  – Depends on the number of potential answers.
    - How many ways a sorting algorithm can rearrange its n-element input?
- How many possibilities need to be checked to break 4-digit PIN? A 8-letter password (with digits and special symbols)? A 80-letter passphrase (with just letters)? Which one is more secure?
  - 10 digits + 23 special symbols + 26 lowercase + 26 uppercase letters.

5

Combinatorics

- What if some of the possibilities are identical? How can we count then?
  – How many different trees are there, if two trees are considered the same if one can be transformed into another by moving/renaming vertices, keeping edges attached.
    - Flip and move bottom vertex.

6

Rules of sum and product

- **Rule of sum**:
  - If there are n choices for A, and m choices for B, then there are n+m choices for "A or B"
    - Provided A and B do not overlap.
    - If there are 16 squares of size 1, and 9 squares of size 2, then there are 25 squares of size either 1 or 2.
- **Rule of product**:
  - If there are n choices for A, and m choices for B, then there are n*m choices for "A and B".
    - 3 choices for a row times 3 choices for a column: 9 of 2x2 squares.
      - Can also count rectangles rather than squares…

7

Cartesian products

- When a sequence is Cartesian product of n copies of the same set:
  - How many possible PINs consisting of 4 digits are there?

    - Use the rule of product. Each of the digits has 10 possibilities (0…9), and picking a digit for one position does not affect others. 10*10*10*10=$10^4 = 10{,}000$.
      - So by the Pigeon Hole Principle, there are (lots of) people at MUN that have the same PINs.
  - How many rows does a truth table on n variables have?
    - Each variable has 2 possibilities. So 2^n.
- In general, if there are n independent places in the sequence, and m possibilities for each place, get m^n possible sequences.

8

Cartesian products

- Cartesian product of n different sets:
  - Multiply together sizes of these sets.
    - Holds for same sizes too, of course.
- How many different dishes can you make from:
  - 3 types of protein (meat, chicken, falafel)
  - 2 types of starch (noodles, rice)
  - 4 types of sauces

3*2*4.

9

Assigning offices example

- Our department has 20 faculty offices in the Engineering building, and 4 more in the Earth Sciences building, and needs to assign them to 24 faculty members.

  - How many ways are there to select 4 out of 24 faculty to go to Earth Sciences?
  - How many ways are there to assign offices ER-6030 to ER-6033 to specific 4 people?
    - To Oscar, Antonina, Yuanzhu and Dave?
  - How many ways, overall, to choose 4 people to go to Earth Sciences and assign them to four offices in Earth Sciences?

10

11

Assigning offices example

- Our department has 20 faculty offices in the Engineering building, and 4 more in the Earth Sciences building, and needs to assign them to 24 faculty members.

  - How many ways are there to select 4 out of 24 faculty to go to Earth Sciences?
  - How many ways are there to assign offices ER-6030 to ER-6033 to specific 4 people?
    - To Oscar, Antonina, Yuanzhu and Dave?
  - How many ways, overall, to choose 4 people to go to Earth Sciences and assign them to four offices in Earth Sciences?

12

Permutations

- **Permutations**: number of sequences of objects.
  - Without repetition: each object appears once.
- How many ways to assign offices ER-6030 to ER-6033 to Antonina, Dave, Oscar and Yuanzhu?
  - 4 choices to pick who gets ER-6030. This leaves 3 choices to pick who gets ER-6031. Now 2 remain for ER-6032, and the last is stuck with ER-6033.
    - By the product rule, get 4*3*2*1 = 4!=24 (that is, 4 factorial)
- In general, number of permutations of n elements is 1*2*…*n=n!
  - "Permutations": the difference between choices is only the order of elements.

13

r-Permutations.

- An **r-permutation** P(n,r) is a number of ways to take r out of n objects, and arrange these r objects in a sequence.
  - Before, we talked about permutations of all objects in the set.
  - Choose 4 faculty members to go to Earth Sciences building, and assign offices to just these 4.

14

r-Permutations.

- How many ways to assign ER offices to 4 out of 24 faculty?
  - Pick one out of 24 to be in ER-6030. One out of remaining 23 to be in ER-6031, one out of 22 for ER-6032, one out of 21 for ER-6033.
  - By the product rule, get P(24,4) = 24*23*22*21.
- Alternative calculation:
  - There are 24! ways to assign offices to everybody.
  - Out of them, 20! ways to assign non-ER offices.
    - We are not interested in what everybody else got – so once the way to assign ER offices is fixed, all sequences with this assignment to ER offices are the same for us.
  - $\mathrm{P}(24{,}4) = \frac{24!}{20!}$ =24*23*22*21 ways to get 4 people specific offices in ER.

15

r-Permutations.

- **r-permutations**: P(n,k) is number of ways to choose k objects out of n, where only the order of selected objects matters.
- General formula: the number of r-permutations out of n objects is

$$P(n,r) = \frac{n!}{(n-r)!}$$

- Example: how many ways to choose 1st, 2nd, and 3rd place winners in a contest with n participants?
  - n choices for 1st place, (n-1) for 2nd place, (n-2) for 3rd place.
  - $P(n,3) = \frac{n!}{(n-3)!} = n*(n-1)*(n-2)$

16

Combinations.

- In general, how many ways to pick k out of n objects?
  - The number of k-permutations divided by the number of different permutations of the k objects themselves.
- How many ways to choose 4 out of 24 faculty members to get an office in Earth Science?
  - 24! ways to assign offices altogether.
  - 4! ways to assign the first 4 offices (ones in Earth Sciences).
  - 20! ways to assign offices not in Earth Sciences.
  - Overall, $\frac{24!}{4!\ 20!}$ ways to pick who gets an Earth Sciences office,
    - Considering only who goes to which building, ignoring which specific office they get.

17

Combinations.

- **Combinations**: C(n,k) is number of ways to choose k objects out of n.
  - "n choose k": $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ = C(n,k)
  - How many ways to choose 4 out of 24 faculty members to get an office in Earth Science?
    - C(24,4)=$\frac{24!}{4!\ 20!}$ ways to pick who gets an Earth Science office.
  - How many ways to select a crew of 6 astronauts out of a team of 30 to go to Mars?
    - C(30,6) = $\binom{30}{6} = \frac{30!}{6!(24!)}$ = 593,775

18

Coffee ordering puzzle

- Suppose that 10 of you came to the office hour, and we decided to go to Jumping Bean to get some coffee.
- Jumping Bean sells 6 types of coffee drinks: drip coffee, cappucino, espresso, latte, mocca and americano.
- How many different combinations of drinks can we get, if each of 11 of us gets one coffee drink?
  – Here, all of us getting drip coffee is one combination, 6 espresso and 5 americano is another, etc.

19

20

Coffee ordering puzzle

- Suppose that 10 of you came to the office hour, and we decided to go to Jumping Bean to get some coffee.
- Jumping Bean sells 6 types of coffee drinks: drip coffee, cappucino, espresso, latte, mocca and americano.
- How many different combinations of drinks can we get, if each of 11 of us gets one coffee drink?
  – Here, all of us getting drip coffee is one combination, 6 espresso and 5 americano is another, etc.

21

Coffee ordering: smaller puzzle

- Suppose that 2 students decided to get coffee at Treats.
  – Treats sells 4 kinds of coffee: Medium, House, Decaf and Flavoured.
- How many different combinations of drinks can they get, if each gets one drink?
  – If we take into account who gets what, then the answer would be 4x4 by the Cartesian product rule. But here we consider "decaf and Medium" to be the same as "Medium and decaf".
  – Let's list the possibilities. To save space, let's denote each possible drink by the first letter ("m" for Medium, etc), and a combination by a string of letters in alphabetical order.
    - So if they get one decaf and one flavoured, we'll write "df"
  – dd,df,dh,dm,ff,fh,fm,hh,hm,mm: 10 combinations of drinks.

22

Coffee ordering: smaller puzzle

Suppose that 2 students decided to get coffee at Treats. Treats sells 4 kinds of coffee: Medium, Houseblend, Decaf and Flavoured. How many different combinations of drinks can they get, if each gets one drink?
- dd,df,dh,dm,ff,fh,fm,hh,hm,mm: 10 combinations of drinks.
- We could write $4 + (4 * 4 - 4)/2$ to count sets with 2 of the same drinks separately, but that does not quite generalize to 11 people getting drinks…

– Instead, let's encode combination of drinks differently. Rather than using letters (d,f,h,m), we'll encode which drink is which by "dividers".
- Let's now use "c" for "coffee", and "|" for a divider. So for 2 people it is 2 c's.
- We will need one less divider than the number of drink types (k bins, k-1 dividers)
- Then "c||c|" encodes one coffee of the first type (decaf), no coffees of the second type (no flavoured), one coffee of the third type (house), and no mediums.
- |cc|| encodes two flavoured coffees.

23

Coffee ordering: smaller puzzle

Suppose that 2 students decided to get coffee at Treats. Treats sells 4 kinds of coffee: Medium, Houseblend, Decaf and Flavoured. How many different combinations of drinks can they get, if each gets one drink?
- dd,df,dh,dm,ff,fh,fm,hh,hm,mm: 10 combinations of drinks.

– Now, the problem reduces to counting how many different strings we can make out of 2 "c" (for 2 coffees) and 3 dividers (for 4-1 coffee types).

– The number of ways to choose 2 places in a string of length 2+3 to be "c"
- Equivalently, choosing 3 out of 5 places to be "|"

– Choosing k out of n is $C(n, k) = \binom{n}{k} = \frac{n!}{k!(n-k)!}$
- $\binom{5}{2} = \frac{5!}{2!3!} = 10$

24

Combinations with repetition

- Now we can do 11 people and 6 types drinks (any number of people and types of drinks)
  - 6 types of drinks give us 6-1= 5 dividers
  - Number of people + number of dividers: 11+6-1=16 positions in a string.
  - So $\binom{16}{11} = \binom{16}{5}$ = 4368 possible combinations of drinks.
- In general, number of ways to select r objects out of n categories with repetition is

$$\binom{r+n-1}{r}$$

25

Summary

Selecting k out of n objects	Order matters (permutations)	Order ignored (combinations)
With repetitions	n^k 	$\binom{k+n-1}{k}$ 
Without repetitions	$P(n,k) = \frac{n!}{(n-k)!}$ 	$\binom{n}{k}$ 

26

Puzzle: misspelling OSOYOOS

- In the game of Scrabble, players make words out of the letters they have on a rack.
  - Suppose that someone puts the word “OSOYOOS” on the board, using up all her 7 pieces.
  - How many ways could she have had the letters arranged on the rack in front of her?
    - The order of multiple copies of a letter does not matter: switching two S around results in the same sequence, but switching O and S does not.
    - The letters on the rack do not have to form a word.

27

28

Puzzle: misspelling OSOYOOS

- In the game of Scrabble, players make words out of the letters they have on a rack.
  - Suppose that someone puts the word “OSOYOOS” on the board, using up all her 7 pieces.
  - How many ways could she have had the letters arranged on the rack in front of her?
    - The order of multiple copies of a letter does not matter: switching two S around results in the same sequence, but switching O and S does not.
    - The letters on the rack do not have to form a word.

29

Puzzle: misspelling OSOYOOS

- Suppose that someone puts the word “OSOYOOS” on the board, using up all her 7 pieces. How many ways could she have had the letters arranged on the rack in front of her?
  - There are 7 letters in the word OSOYOOS. If they were all distinct, that would be 7! = 5040 ways.
  - But there are 4 Os, and 2 Ss, order of which does not matter.
  - There are 4! ways to order Os, and 2! ways to order Ss.
  - Therefore, the total number of ways to order the letters ignoring the order of Os and Ss is $^{7!}/_{4!2!}$ = 105

30

Puzzle: misspelling OSOYOOS

- Suppose that someone puts the word “OSOYOOS” on the board, using up all her 7 pieces. How many ways could she have had the letters arranged on the rack in front of them, *such that Ss are not next to each other*?
  - First, let’s consider all possible orderings of remaining letters: 5!/4! of them
    - Since order of Os does not matter, there are 5 choices where to put Y.
  - Now, consider places where S can go, without two S being next to each other: _o_o_y_o_o_ (here, ooyoo are in arbitrary order). There are 6 such places.
    - So there are $\binom{6}{2} = {}^{6!}/_{2!4!}$ ways to place Ss.
  - Therefore, the total number of ways to order the letters ignoring the order of Os and Ss and with Ss not next to each other is ${}^{5!6!}/_{4!4!2!} = 75$
  - Alternatively, consider all orderings with Ss next to each other: there are $\frac{6!}{4!} = 30$ of them (treating the “SS” as a single letter).
    - Now, the total is 105-30 = 75.

31

32

Binomial coefficients

- Binomial expansion: open parentheses in $(x+y)^n$
  - Open the parentheses in $(x+y)^2$: $(x+y)^2 = x^2 + 2xy + y^2$
  - Open parentheses in $(x+y)^3$
    - $x^3 + xxy + xyx + yxx + xyy + yxy + yyx + y^3 = x^3 + 3x^2y + 3xy^2 + y^3$
- That is, a coefficient in front of x^2y is the number of ways to pick one y (or 2 x) out of 3 positions.
  - The coefficient in front of $x^k y^{n-k}$ in the expansion of $(x+y)^n$ is $C(n,k) = \binom{n}{k}$
  - Call these coefficients **binomial coefficients**.

Binomial theorem: $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$

33

Pascal’s identity and triangle

- How to compute binomial coefficients?
  - Only need to compute them for $0 \le k \le \lceil \frac{n}{2} \rceil$, since $\binom{n}{k} = \binom{n}{n-k} = \frac{n!}{k!(n-k)!}$
- **Pascal’s identity**: $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$
  - Recurrence for $\binom{n}{k}$, with $\binom{n}{n} = \binom{n}{0} = 1$ as basis
  - In practice, use Stirling approximation n! ~ $\sqrt{2\pi n}\,(n/e)^n$
  - So $\frac{n^k}{k^k} \le \binom{n}{k} < \frac{(en)^k}{k^k}$,
  - And $\ln n! \sim n \ln n - n$

1
1 1
1 2 1
1 3 3 1
1 4 6 4 1
1 5 10 10 5 1
1 6 15 20 15 6 1

Pascal’s triangle

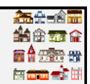
34

Binomial theorem

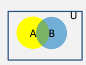
- **Binomial theorem:** $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$
- **Corollary 1**: $\sum_{k=0}^{n} \binom{n}{k} = 2^n$
  - **Proof**: Apply the binomial theorem with $x = y = 1$.
    2=1+1, so $2^n = (1+1)^n = \sum_{k=0}^{n} \binom{n}{k} 1^k 1^{n-k} = \sum_{k=0}^{n} \binom{n}{k}$
- **Corollary 2**: $\sum_{k=0}^{n} \binom{n}{k} (-1)^k = 0$
  - **Proof**: Apply the binomial theorem with $x = -1,\ y = 1$.
    0=(-1)+1, so $0 = 0^n = ((-1)+1)^n = \sum_{k=0}^{n} \binom{n}{k} (-1)^k 1^{n-k} = \sum_{k=0}^{n} \binom{n}{k} (-1)^k$

35

Enrollment puzzle



- There are 160 students in COMP 1000 this semester
- There are 105 students in COMP 1002
- The total number of students in either of these two courses is 200
- How many students are in both COMP 1000 and COMP 1002?

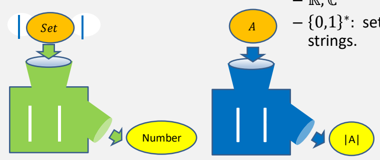


36

37

Size (cardinality)

- If a set A has n elements, for a natural number n, then A is a **finite** set. Its **cardinality** is |A|=n.
  - $|\{1,2,3\}| = 3$. $|\emptyset| = 0$

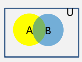


- Sets that are not finite are **infinite**.
  - More on cardinality of infinite sets later…
  - $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$
  - $\mathbb{R}, \mathbb{C}$
  - $\{0,1\}^*$: set of all finite-length binary strings.

38

Enrollment puzzle

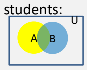
- There are 160 students in COMP 1000 this semester
- There are 105 students in COMP 1002
- The total number of students in either of these two courses is 200
- How many students are in both COMP 1000 and COMP 1002?



39

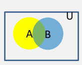
Enrollment puzzle

- There are 160 students in COMP 1000 this semester, and 105 students in COMP 1002. The total number of students in either of these two courses is 200. How many students are in both COMP 1000 and COMP 1002?
- Let A be the set of students in COMP 1000, and let B the set of students in COMP 1002.
  - |A| = 160 and |B| = 105.
  - The number of students in either course is $|A \cup B| = 200$.
  - We want to know $|A \cap B|$.
- If we take |A|+|B|, we would count students in both courses twice.
  - So the number of students in both is the number of double-counted students:
- $|A \cap B| = |A| + |B| - |A \cup B|$= 160+105-200=65.

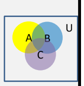


40

Rule of inclusion-exclusion

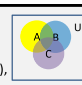


- Let A and B be two sets. Then
  $$|A \cup B| = |A| + |B| - |A \cap B|$$
  - Why? Elements in $|A \cap B|$ are counted twice in |A|+|B|, so need to subtract one copy.
  - If A and B are disjoint, then $|A \cup B| = |A| + |B|$
  - If there are 160 students in COMP 1000, 105 in COMP 1002, and 65 of them are in both, then the total number of students in 1000 or 1002 is 160+105-65=200.
- What if we have three sets?



41

Rule of inclusion-exclusion



- How many students in total if
  - 160 students in COMP1000 (A), 105 in COMP1002 (B), and 120 in COMP 1001 (C),
  - where 45 are in both COMP 1000 and COMP 1002: $|A \cap B| = 45$
  - 30 are in both COMP 1000 and COMP 1001: $|A \cap C| = 30$
  - 50 are in both COMP 1001 and COMP 1002: $|B \cap C| = 50$.
  - 20 students are in all three: $|A \cap B \cap C| = 20$

  - $|A| + |B| + |C|$ counts students in all three 3 times, students in two courses twice.
  - $|A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C|$ counts students in two courses once, but subtracts out students in all three courses! Need to add them back in.

$$\begin{aligned}|A \cup B \cup C| = {} & |A| + |B| + |C| \\ & -|A \cap B| - |A \cap C| - |B \cap C| \\ & +|A \cap B \cap C|\end{aligned}$$

So total number of students in COMP 1000,1001, 1002 is:
$$|A \cup B \cup C| = 160 + 105 + 120 - 45 - 30 - 50 + 20 = 280$$

42

Rule of inclusion-exclusion

- What happens if there are n sets?
  - Suppose an element is in k sets out of n.
  - It will appear $k = C(k,1)$ times when counting individual sets
    - $C(k,2)$ times when counting intersections of 2 sets…
    - $C(k,i)$ times when counting intersections of i sets…
    - $C(k,k)$ times when counting intersections of k sets.
  - Suppose $x \in A,\ and\ x \in B\ and\ x \notin C$.
    - Then x is counted twice ($C(2,1) = 2$) in $|A| + |B| + |C|$,
    - and once ($C(2,2) = 1$) in $|A \cap B| + |A \cap C| + |B \cap C|$.
    - It is not in $|A \cap B \cap C|$, so counted 0 times there.

43

Rule of inclusion-exclusion

- What happens if there are n sets?
  - Suppose an element is in k sets out of n.
  - It will appear $k = C(k,1)$ times when counting individual sets
    - $C(k,2)$ times when counting intersections of 2 sets…
    - $C(k,i)$ times when counting intersections of i sets…
    - $C(k,k)$ times when counting intersections of k sets.
  - Suppose x is in all three sets A, B, C.
    - It is counted 3=$C(3,1)$ times in $|A| + |B| + |C|$,
    - $3 = C(3,2)$ times in in $|A \cap B| + |A \cap C| + |B \cap C|$
    - and once, C(3,3) times, in $|A \cap B \cap C|$.

44

Rule of inclusion-exclusion

- What happens if there are n sets?
  - Suppose an element is in k sets out of n.
  - It will appear $k = C(k,1)$ times when counting individual sets
    - $C(k,2)$ times when counting intersections of 2 sets…
    - $C(k,i)$ times when counting intersections of i sets…
    - $C(k,k)$ times when counting intersections of k sets.
- Remember the binomial theorem (or, rather, its corollary): $\sum_{k=0}^{n}\binom{n}{k}(-1)^k = C(k,0) - C(k,1) + C(k,2) - \cdots + (-1)^k C(k,k) = 0$
  - Now, $1 = C(k,0) = C(k,1) - C(k,2) - \cdots - (-1)^k C(k,k)$
  - Writing $-(-1)^k$ as $(-1)^{k+1}$, get $1 = C(k,1) - C(k,2) + \cdots + (-1)^{k+1} C(k,k)$

45

Rule of inclusion-exclusion

- We just derived: $1 = C(k,1) - C(k,2) + \cdots + (-1)^{k+1} C(k,k)$
- So if we add sizes of intersections of odd number of sets (including individual sets) and subtract sizes of intersections of even number of sets, then every element is counted once!

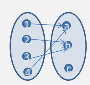
$$|A_1 \cup \cdots \cup A_n| = |A_1| + \cdots + |A_n|$$
$$-\Sigma_{1 \le i_1 < i_2 \le n} |A_{i_1} \cap A_{i_2}|$$
$$+\Sigma_{1 \le i_1 < i_2 < i_3 \le n} |A_{i_1} \cap A_{i_2} \cap A_{i_3}|$$
$$- \cdots + (-1)^{n+1} |A_1 \cap A_2 \cap \cdots \cap A_n|$$

46

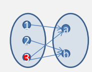
47

Functions

- **A function** $f: X \to Y$ is a relation on X $\times$ Y such that for every $x \in$ X there is at most one $y \in Y$ for which (x, y) is in the relation.
- Usual notation: $f(x) = y$, where
  - y is an **image** of x under f.
  - X is the **domain** of f
  - Y is the **codomain** of f
  - **Range** of f (**image** of X under f):
    - $\{y \in Y \mid \exists x \in X, f(x) = y\}$
  - **Preimage** of a y in range of f:
    - $\{x \in X \mid f(x) = y\}$
      - Preimage of b is {2,3}.



This R is a function with domain {1,2,3,4}, codomain {a,b,c} and range {a,b}

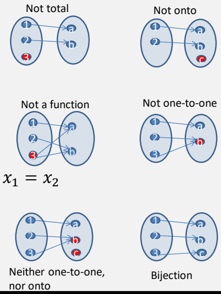


This R is not a function

48

Functions

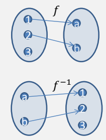
- **A function** $f: X \to Y$ is
  - **Total**: $\forall x \in X\ \exists y \in Y\ f(x) = y$
    - f: $\mathbb{Z} \to \mathbb{Z}$
    - $f(x) = x + 1$ is total. $f(x) = \frac{100}{x}$ is not total.
    - A function that is not necessarily total is **partial**
  - **Onto**: $\forall y \in Y\ \exists x \in X\ f(x) = y$
    - $f(x) = x + 1$ is onto over $\mathbb{Z}$, but not over $\mathbb{N}$
    - $f(x) = 5x$ is not onto (over $\mathbb{Z}$)
  - **One-to-one:** $\forall x_1, x_2 \in X\ f(x_1) = f(x_2) \to x_1 = x_2$
    - $f(x) = x + 1$ is one-to-one.
    - $f(x) = x^2$ is not one-to-one
  - **Bijection**: total, one-to-one and onto.
    - $f(x) = x + 1$ is a bijection over $\mathbb{Z}$.



49

Functions

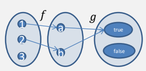
- An **inverse** of f is a function $f^{-1}: Y \to X$, such that $f^{-1}(y) = x$ iff $f(x) = y$
  - $f(x) = x + 1, f^{-1}(y) = y - 1$
  - Only one-to-one functions have an inverse



50

Functions

- **Composition** of functions $f: X \to Y$ and $g: Y \to Z$ is a function $g \circ f: X \to Z$ such that $(g \circ f)(x) = g(f(x))$
  - $f(x) = \frac{x}{5}$, $g(x) = \lceil x \rceil$, over $\mathbb{R}$
    - $\lceil x \rceil$ is ceiling: x rounded up to nearest integer.
  - $(g \circ f)(x) = g(f(x)) = \left\lceil \frac{x}{5} \right\rceil$
  - $(f \circ g)(x) = f(g(x)) = \frac{\lceil x \rceil}{5}$
  - $(g \circ f)$(12.5)=$\lceil 2.5 \rceil$ = 3. $(f \circ g)$(12.5)=13/5= 2.6
    - Order matters!



51

Barbers club puzzle

- In a certain barbers club,
  - Every member has shaved at least one other member
  - No member shaved himself
  - No member has been shaved by more than one member
  - There is a member who has never been shaved.
- *Question: how many barbers are in this club?*

52

53

Barbers club puzzle

- In a certain barbers club,
  - Every member has shaved at least one other member
  - No member shaved himself
  - No member has been shaved by more than one member
  - There is a member who has never been shaved.

- *Question: how many barbers are in this club?*

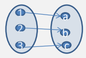
…

Infinitely many!
Barber 0 grows a beard.
For all n∈ $\mathbb{N}$, barber n shaves barber n+1

54

Cardinalities of infinite sets

- Two finite sets A and B have the same *cardinality* (size) if they have the same number of elements
  - That is, for each element of A there is exactly one matching element of B.



- For infinite A and B, define |A|=|B| iff there exists a bijection between A and B.
  - If it is possible to map every element of A to one element of B, covering all elements of B.
  - So that every element of A and every element of B is paired up with exactly one element from the other set.

55

Countable sets

- An infinite set A is *countable* iff |A| = |ℕ|.
- That is, there is a bijection between elements of A and natural numbers.
  - So it is possible to assign a natural number to each element of A, that is, "count" elements of A.
  - Name the first element of A, the second element of A, and so on, covering all elements of A.
    - Starting with either 0 or 1 is ok.
    - Either $f: A \rightarrow \mathbb{N}$ or $f: \mathbb{N} \rightarrow A$ is OK.

56

Set of all integers is countable

- The set of integers $\mathbb{Z}$ is countable:
  - Let $f: \mathbb{Z} \rightarrow \mathbb{N}$ where $f(x) = 2x$ if $x \geq 0$, else $f(x) = -(1 + 2x)$
    - Here, for simplicity, let's allow $0 \in \mathbb{N}$
- This f is a bijection, that is, a one-to-one and onto function.
  - Onto: for each $y \in \mathbb{N}$, there is an $x \in \mathbb{Z}$ such that $f(x) = y$
    - If y is even, then $x = y/2$, which is an integer when y is even.
    - If y is odd, then $x = (1 - y)/2$, which is an integer when y is odd.
  - One-to-one: for each $x \in \mathbb{Z}$, there is a different $f(x) \in \mathbb{N}$
    - Why? Let $f(x_1) = f(x_2) = y$.
    - If y is even, $x_1 = x_2 = \frac{y}{2}$, and if y is odd, then $x_1 = x_2 = (1 - y)/2$.

$\mathbb{Z}$		$\mathbb{N}$
0		0
-1		1
1		2
-2	f	3
2		4
-3		5
3		6
⋮		⋮

57

Cardinality and subsets

- So $|\mathbb{N}| = |\mathbb{Z}|$, even though not only all of $\mathbb{N}$ is in $\mathbb{Z}$, but $\mathbb{Z}$ also contains all the negative numbers!

Surprise! Strange things happen in the infinite world.
Two sets A and B, where $A \subset B$, can have the same size (cardinality)!

- In general, an infinite subset of a countable set is countable.
  - Set of all primes is countable, because it is an infinite subset of $\mathbb{N}$
  - Set of all even integers is countable, because it is an infinite subset of $\mathbb{Z}$

58

59

Counting finite strings

- Let us first show that the set of finite strings over {a,b}, denoted $\{a,b\}^*$, is countable.
- We will count strings in order of their increasing lengths, counting shorter strings before longer strings.
  - First, count all strings of length 0. There is one such string: λ
    - Map it to number 1: let's start with 1 this time.
  - Then count strings of length 1: there are two, "a" and "b".
    - Map them to numbers 2 and 3, respectively
  - Four strings of length 2: aa, ab, ba, bb: map those to 4,5,6,7…

$\{a,b\}^*$	$\mathbb{N}$
λ	1
a	2
b	3
aa	4
ab	5
ba	6
bb	7
aaa	8
⋮	⋮

60

Set $\{a, b\}^*$ is countable

- Without going into details: how to turn it into a bijection
  - There are finitely many strings of any given length.
    - So there are finitely many strings shorter than any given length.
  - Within the set of strings of the same length, we can assign a separate number (index) to each string.
    - A number between 1 and the number of strings of that length.
  - Now, the bijection $f: \{a, b\}^* \to \mathbb{N}$ assigns to each string a number which is a sum of the number of shorter strings plus the index of this string among strings of the same length.
    - For example, there are 3 strings of length less than 2: λ, a, b
    - Let's enumerate strings of length 2 as follows: aa is 1, ab 2, ba 3, bb 4
    - Then $f(ab) = 3 + 2 = 5$
- Because we have presented (omitting many details) a bijection f from $\{a, b\}^*$ to $\mathbb{N}$, $\{a, b\}^*$ is countable.

$\{a,b\}^*$	$\mathbb{N}$
λ	1
a	2
b	3
aa $\xrightarrow{f}$	4
ab	5
ba	6
bb	7
aaa	8
⋮	⋮

61

Order of strings

- Couldn't we just count strings in dictionary order?
  - $\lambda, a, aa, aaa, aaaa$ …
    - But that would go forever, and we would never get to "b".
    - We must count shorter strings before longer strings to avoid this.
  - But when we are counting strings of the same length, then we might as well do it in the dictionary order.
    - Length 3 strings: aaa, aab, aba, abb, baa, bab, bba, bbb.
- So what is the actual formula for f?
  - There are 2^n strings of length n,
  - And $2^n - 1$ strings of length less than n (we will show it later).
  - So $f(x) = 2^{|x|} - 1 + index(x)$, where $index(x)$ is its index in dictionary order among strings of length $|x|$, 1 to $2^{|x|}$.
  - You can check that $f(x)$ is a bijection.

$\{a,b\}^*$	$\mathbb{N}$
λ	1
a	2
b	3
aa $\xrightarrow{f}$	4
ab	5
ba	6
bb	7
aaa	8
⋮	⋮

62

Set of all finite binary strings is countable

- Now, let's show that the set of all binary strings, that is, finite strings over {0,1}, denoted $\{0,1\}^*$, is countable.
- Use a composition of two functions to map $\{0,1\}^*$ to $\mathbb{N}$
  - $g: \{0,1\}^* \to \{a, b\}^*$ and $f: \{a, b\}^* \to \mathbb{N}$ from the previous proof. The resulting bijection will be $f(g(x))$.
  - To compute $g(x)$, change every 0 in x to a, and every 1 to b.
    - For example, $g(0010) = aaba$. $g(\lambda) = \lambda$.
  - A composition of two bijections is a bijection. So $f(g(x))$ is a bijection from $\{0,1\}^* \to \mathbb{N}$, proving that $\{0,1\}^*$is countable.

$\{0,1\}^*$	$\{a,b\}^*$	$\mathbb{N}$
λ	λ	0
0	a	1
1	b	2
00	aa	3
01 $\xrightarrow{g}$	ab $\xrightarrow{f}$	4
10	ba	5
11	bb	6
000	aaa	7
⋮	⋮	⋮

63

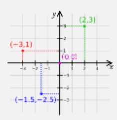
64

Useful properties of countable sets

- An infinite subset of a countable set is itself a countable set.
- A union, intersection or difference of countable sets is a countable set.
- A Cartesian product of countable sets is a countable set.

65

Cartesian product of sets



Theorem: the Cartesian product of countable sets is countable.
Proof:

- Let's first show that $\mathbb{N} \times \mathbb{N}$ is countable
  - $\mathbb{N} \times \mathbb{N}$: (0,0), (0,1), (1,0), (2,0), (1,1), (0,2), (3,0), (2,1), (1,2),…
  - Count pairs with elements summing up to 0 first, then summing up to 1, etc
  - There are $n + 1$ pairs summing up to n for each n
  - Now build a bijection $g: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ in a similar way to the $\{a, b\}^*$ example.
- Let A, B be countable sets
  - That is, there are bijections $f_1: A \to \mathbb{N}$ and $f_2: B \to \mathbb{N}$
  - To show that $A \times B$ is countable, define a bijection $f: A \times B \to \mathbb{N}$ as follows:
  - For every $a \in A, b \in B$, let $f(a, b) = g(f_1(a), f_2(b))$, where $g: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is the bijection we just defined above.

□ (Done).

66

Set of all rational numbers is countable

Corollary: The set of rational numbers $\mathbb{Q}$ is countable

- Every rational number r is representable by an irreducible pair of integers (n, m): $r = n/m$
  - To make it a bijection, assume that $m > 0$, in addition to irreducibility.
- So $\mathbb{Q} \subset \mathbb{Z} \times \mathbb{Z}$, and we just showed that $\mathbb{Z} \times \mathbb{Z}$ is countable.
  - Since $\mathbb{Z} \times \mathbb{Z}$ is a Cartesian product of countable sets.
- Therefore, $\mathbb{Q}$ is an infinite subset of a countable set, and so $\mathbb{Q}$ is countable.
  - An easy way to see that $\mathbb{Q}$ is infinite is to note that $\mathbb{N} \subset \mathbb{Q}$.

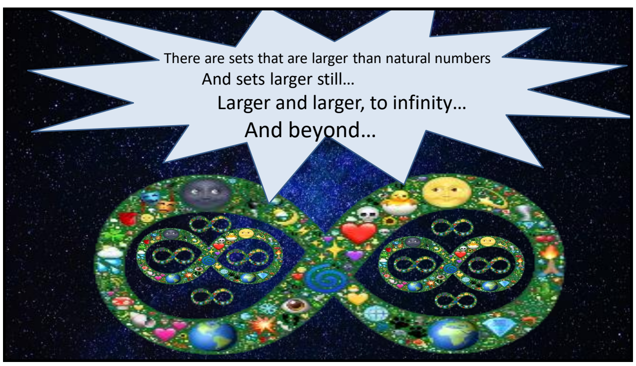
□ (Done).

67

68

69

70



71

Uncountable sets

- Infinite sets that are not countable (that is, which have cardinality larger than $|\mathbb{N}|$) are called *uncountable.*
- We will introduce a technique called "diagonalization" due to Georg Cantor, and use it to show that
  - the set of all real numbers, $\mathbb{R}$, is uncountable.
  - a power set of a set is always larger than the original set
    - Thus a power set of a countable set is uncountable
- And finish with a surprising computer science consequence:
  - There are well-defined computational problems that are unsolvable!
  - Including bug-checking in software…

72

Diagonalization

- Let A={a,b,c}. $\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}$
- Let's show that |A| < $|\mathcal{P}(A)|$
  - Imagine that someone is trying to convince you that |A| = $|\mathcal{P}(A)|$. Then they should give you a bijection $f: A \to \mathcal{P}(A)$
    - That is, give you $S_1, S_2, S_3 \in \mathcal{P}(A)$ such that $f(a) = S_1, f(b) = S_2, f(c) = S_3$ and there is nothing in $\mathcal{P}(A)$ except S_1, S_2, S_3.
      - Say they gave you $S_1 = \{a\}$, $S_2 = \{b,c\}$ and $S_3 = \emptyset$. Here is how you can construct a set in $\mathcal{P}(A)$ which is not in the list S_1, S_2, S_3.
        - Make a table with rows marked by elements of A
        - To represent a set $S \in \mathcal{P}(A)$, use its characteristic string: say for every element of the universe of S, A, if it is in S or not.

	a	b	c
$f(a) = S_1$	1	0	0
$f(b) = S_2$	0	1	1
$f(c) = S_3$	0	0	0

73

Diagonalization

- Let A={a,b,c}. $\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}$
- Let's show that |A| < $|\mathcal{P}(A)|$
  - Imagine that someone is trying to convince you that |A| = $|\mathcal{P}(A)|$. Then they should give you a bijection $f: A \to \mathcal{P}(A)$
    - That is, give you $S_1, S_2, S_3 \in \mathcal{P}(A)$ such that $f(a) = S_1, f(b) = S_2, f(c) = S_3$ and there is nothing in $\mathcal{P}(A)$ except S_1, S_2, S_3.
      - Say they gave you $S_1 = \{a\}$, $S_2 = \{b,c\}$ and $S_3 = \emptyset$. Here is how you can construct a set in $\mathcal{P}(A)$ which is not in the list S_1, S_2, S_3.
        - Make a table with rows marked by elements of A
        - To represent a set $S \in \mathcal{P}(A)$, use its characteristic string: say for every element of the universe of S, A, if it is in S or not.
      - Now, the diagonal set is D={c} is in $\mathcal{P}(A)$, but it is not one of S_1, S_2, S_3.
      - Therefore, f cannot be a bijection! And this works for any S_1, S_2, S_3.

	a	b	c
$f(a) = S_1$	1	0	0
$f(b) = S_2$	0	1	1
$f(c) = S_3$	0	0	0
D	0	0	1

74

Diagonalization: ℝ

- ℝ is uncountable. Even [0,1) interval of the real line is uncountable!
  - Reals may have infinite strings of digits after the decimal point.
  - Imagine if there were a numbered list of all reals in [0,1)
    - $a_1, a_2, a_3, \ldots$
  - For example:
    - a_1 = 0.23145…
    - a_2 = 0.30000…
    - …
- Let $d[i] = (a_i[i] + 1)\ mod\ 10$
  - Here, $[i]$ is i^{th} digit.
  - This d is a valid real number!
- But if number d were in the list, e.g. k^{th}, a contradiction
  - It would have to differ from itself in k^{th} place.

0.	r[1]	r[2]	r[3]	r[4]	r[5]	…	r[k]	
a_1	2	3	1	4	5	…		
a_2	3	0	0	0	0	…		
a_3	9	9	9	9	9	…		
…								
a_k	3	1	0	4	3	…	5	…
…								
d	3	1	0	…	…	…	6	…

75

Diagonalization: set of all languages

- Recall that a language is a set of finite strings over a finite alphabet:
  - $\{a,b\}^*$, English, PYTHON… Each is countable.
- *Theorem*: Set of all languages is uncountable.
  - Here, we'll prove it for languages over $\{0,1\}^*$
- Encode a language L by its "characteristic string"
  - Put "yes" if string $s \in L$, "no" if $s \notin L$
- Let language D be: $s_i \in$ D iff $s_i \notin L_i$
- If D were in the list, e.g. L_k, contradiction:
  - It would have to differ from itself in k^{th} place.

	λ	0	1	00	01	…	s_k		
L_1	yes	yes	no	yes	yes	…			
L_2	yes	no	yes	no	yes	…			
L_3	no	no	no	no	no	…			
…									
L_k	no	yes	yes	no	yes	…	yes	..	
…									
D	no	yes	yes	…	…	…	no	..	

- So there is a language for which there is no Python program which would correctly print "yes" on strings in the language, and "no" otherwise.
- In general, for any set A, finite or infinite, its powerset $P(A)$ is larger than A: that is, |A| < $P(A)$

76

The Halting problem

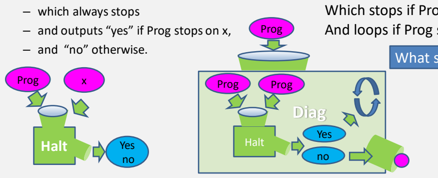
A specific example of unsolvable language: the **Halting problem,** due to Alan Turing

$L_{HALT} = \{(Prog, x)\ |$ program $Prog$ stops when ran with input $x\}$

- $Prog$ is a piece of code, e.g. in Python, and x can be any string.

- Suppose there is a program Halt(Prog,x)
  - which always stops
  - and outputs "yes" if Prog stops on x,
  - and "no" otherwise.

Then there is a program Diag(Prog)
Which stops if Prog loops on x="Prog"
And loops if Prog stops on x="Prog"



What should Diag(Diag) do?

Contradiction!

Such program Diag cannot exist.

So a program Halt cannot exist

- There is no program that always stops and gives the right answer to the Halting problem.

77

Puzzle: playing poker

- There are 52 cards in a standard deck; 4 suits of 13 ranks each.
- In poker, some 5-card combinations ("hands") are special:
  - For example, a "three of a kind" consists of three cards with the same rank, together with two arbitrary cards.
- What are the chances to get
  - a three of a kind hand?
  - A two pairs hand (5 cards with 2 same-rank pairs)?
  - Other hands?...

78