Week 5 highlights

- Classify sets by cardinality into: finite sets, countable sets, uncountable sets.
- Product and sum rules
- Reason about the size of power sets
- Permutations and combinations
- Explain the central idea in Cantor's diagonalization argument.

Cantor-Schroder-Bernstein Theorem: For all nonempty sets,

$|A| = |B|$ if and only if $(|A| \leq |B|$ and $|B| \leq |A|)$ if and only if $(|A| \geq |B|$ and $|B| \geq |A|)$

To prove $|A| = |B|$, we can do any **one** of the following

- Prove there exists a bijection $f : A \to B$;
- Prove there exists a bijection $f : B \to A$;
- Prove there exists two functions $f_1 : A \to B$, $f_2 : B \to A$ where each of f_1, f_2 is one-to-one.
- Prove there exists two functions $f_1 : A \to B$, $f_2 : B \to A$ where each of f_1, f_2 is onto.

A set A is **finite** means it is empty or it is the same size as $\{1, \ldots, n\}$ for some unique $n \in \mathbb{N}$.
A set A is **countably infinite** means it is the same size as $\mathbb{N}$.

Key insight for proofs involving sizes of finite sets: Use the definition of size of a set S to mean the existence of a bijection from S to $\{1, \ldots, |S|\}$.

Theorem: If A and B are disjoint, finite sets, then $|A \cup B| = |A| + |B|$ sum rule

$\exists$ bijection $f: A \cup B \longrightarrow \{1, \ldots, |A|+|B|\}$

Order A, B

$\forall a \in A$ $f(a) = i$ where a is the i^{th} element in A

$\forall b \in B$ $f(b) = |A| + j$ where b is the j^{th} element in B

f is (i) well defined

(ii) one-one

(iii) onto

Theorem: If A and B are finite sets, then $|A \times B| = |A| \cdot |B|$ product rule

$\exists$ bijection $f: A \times B \longrightarrow \{1, 2, 3, \ldots, |A| \cdot |B|\}$

Corollary: If A is a finite set, then $|A^2| = |A|^2$

$A \times \cdots \times A$ (n times) $\rightarrow$ $|A^n| = |A|^n$ $\longrightarrow$ induction with this as base case

$|A \times A| = |A| \cdot |A|$

Applications of the sum and product rule

How many RNA strings of length 5 can be constructed from the basis set $B = \{\mathtt{A}, \mathtt{C}, \mathtt{U}, \mathtt{G}\}$?

4^5 or 5^4 Plug $

$A = B$ $|A| = 4$ $n = 5$ $\therefore |A|^n = 4^5$

1024

How many functions can be defined between two finite sets A and B ?

$|A|^{|B|}$ $|B| \cdot |B| \cdots |B|$ ($|A|$ times) $|B|^{|A|}$?

X ✓

for each $a \in A$ it can map to a $b \in B$

so $|B|$ options for each $a \in A$ $|A|$

$f: A \longrightarrow B$

#possible $f = |B|^{|A|}$

The CS department is looking for an instructor for CS40 who maybe selected among the faculty and grad students. If there are 35 faculty and 100 grad students, how many choices are there for the instructor?

A B

$100 + 35 = 135$

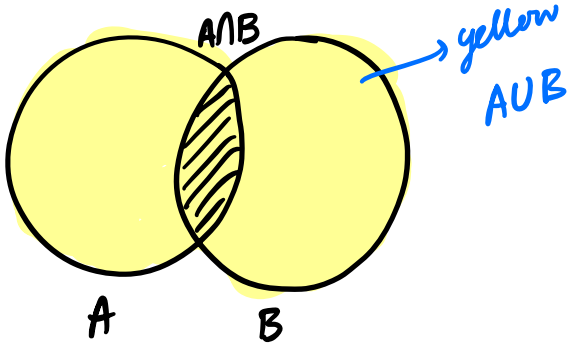
A & B are disjoint $A \cap B = \emptyset$

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

Theorem: If A and B are finite sets, not necessarily disjoint then $|A \cup B| = |A| + |B| - |A \cap B|$

How many bit strings of length 8 start with 1 or end with 00?

0 or 1 at each bit



bit strings of len $8 = 2^8$

bit strings of len 8 starting with $1 = 2^7$

bit strings of len 8 end with $00 = 2^6$

bit strings of len 8 that start with 1 or end with $00 = 2^7 + 2^6 - 2^5$

2^7: start with 1; 2^6: end with 00; 2^5: both

Definition: The **power set** of a set S is the set of all the subsets of S and is denoted by $\mathcal{P}(S)$

If $S = \{1, 2, 3\}$, *what is* $\mathcal{P}(S)$ *?*

$\mathcal{P}(S) = \{\phi, \{1\}, \{2\}, \{3\}, \{1,2\}, \{2,3\}, \{1,3\}, \{1,2,3\}\}$

Construct the power set of S *and reason about its size,* $|\mathcal{P}(S)|$

$|\mathcal{P}(S)| = 2^{|S|}$

Think of each element in $\mathcal{P}(S)$ (set) as a bit string of len $|S|$ where bit i says whether ith element of S $\in$ set or not.

ex:- $\{1,2\} = 110$

$\{1,2,3\} = 111$

$\{2\} = 010$

$S = \{1,2,3\}$

$\{1,2\} = 110$

$\mathcal{P}(S)$ ⟶ think as the set of all bit strings of len $|S|$.

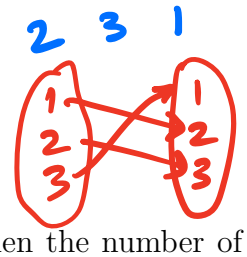
$\therefore |\mathcal{P}(S)| = 2^{|S|}$

A **permutation** is an ordered arrangement of the elements of a set.

$S = \{1, 2, 3\}$ ex:- permutation of S - 3, 2, 1

$\phi: S \to S$ such that ϕ is one-one & onto

perm



An **r-permutation** is an ordered arrangement of r elements of a set

$S = \{1, 2, 3\}$ 2, 3 → 2-permutation

Define $P(n, r)$ as the number of r-permutations of a set with n elements. $P(n, n)$ is then the number of permutations of a set with n elements

Example: List all the r-permutations of $S = \{1, 2, 3\}$.

use case perm: shuffling a deck

n-perm - black jack only ½ the deck is permuted

#permutations = n!

(i) n! ✓

Mapping

1st element n choices

2nd element n-1 ·

⋮

nth element 1 choices

Total = $n \cdot n-1 \cdots 1 = n!$

The traveling salesman problem (also TSP) asks the question: *Given a list of n cities, a city of origin, and the distances between each pair of cities, what is the shortest possible route that visits each city exactly once and returns to the origin city?*

Brute force: (i) go over all permutations of cities & compute the cost

There is no efficient solution to TSP. A solution by exhaustion will need to compute the length of all possible routes. How many routes are there? n!

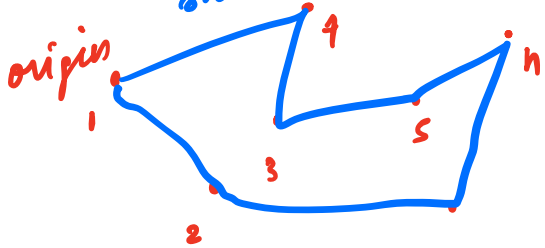
shortest hamiltonian cycle

(ii) return best one

Time: O(n!)

Qs: what is the shortest path that visits all cities & returns to origin

Think: mailman deliver letter



NP-complete

$$\#\,k\text{-permutations} = \frac{n!}{(n-k)!}$$

1st element: n choices
2nd element: $n-1$
⋮
k^{th} element: 1 choices

Total $= n \cdot n-1 \cdots 1 = n!$ — same as this but stop at $(n-k+1)$

$\therefore$ Total k-perm $= n(n-1)(n-2)\cdots(n-k+1)$

(element number: 1, 2, 3, …, k)

$$= \frac{n(n-1)(n-2)\cdots(n-k+1)\left[(n-k)\cdots(1)\right]}{\left[(n-k)\cdots(1)\right]}$$

$$= \frac{n!}{(n-k)!}$$

I am playing a card game (with 52 cards) and say there are b bad shuffling options, then what is the probability that we end up with a good shuffle:

$$P[\text{bad shuffle}] = \frac{\#\text{ bad options}}{\#\text{ total options}} = \frac{b}{52!}$$

$$P[\text{good shuffle}] = 1 - \frac{b}{52!}$$

→ we do not care about order!

Definition: An **r-combination** of a set with n elements is a subset of the set of size r and is denoted as

Fill in the table to list all the subsets of a given size of the set $S = \{1, 2, 3\}$

r	Subsets of S of size r
0	$\emptyset$
1	$\{1\}$ $\{2\}$ $\{3\}$
2	$\{1,2\}$ $\{2,3\}$ $\{1,3\}$
3	$\{1,2,3\}$

r-combinations = 1

$n C_n = 1$

r-combinations of n = $n C_r$ = $\binom{n}{r}$

↓

n choose r

also called binomial coefficients

In general, how many subsets of size r can be constructed from a set of size n?

$n C_r = \frac{n!}{(n-r)!\,r!}$ ← # r-perm

fix r-comb 1, 3, 2

how many perm = r!

each r-comb appears r! times in the set of all r-permutations

Two ways to write it

$S = \{1,2,3\}$

$n C_2$ Perm = 12 21, 23 32, 13 31

$\frac{n!}{(n-2)!} \cdot \frac{1}{2!}$

In general, how many subsets (of any size) are there for a set of size n?

Pascal's Δ le :

Fibonacci Δ le

n=0: 1

n=1: 1 1

n=2: 1 2 1

n=3: 1 3 3 1

n=4: 1 4 6 4 1

n=5: 1 5 10 10 5 1

r=0 r=1 r=2 r=3 r=4 r=5

How do we relate Pascal's Δ le to $n C_r$?

rows → n

cols → r

entry $n C_r$

Binomial Theorem: Let x and y be real numbers, and n a non-negative integer. Then,

$(x+y)^n =$

→ Properties of Binomial coefficients: ✱

(i) $n C_r = n C_{n-r}$

(ii) $n C_r = {}^{n-1}C_{r-1} + {}^{n-1}C_r$

Proof (i) $n C_r = \frac{n!}{r!\,(n-r)!}$

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

Binomial Theorem: Let x and y be real numbers, and n a non-negative integer. Then,

$(x+y)^n =$

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}$$

→ Can prove by induction (exercise)

$$(1+1)^n = \sum_{i=0}^{n} \binom{n}{i} (1)^i (1)^{n-i}$$

$$2^n = \sum_{i=0}^{n} \binom{n}{i}$$

$\binom{n}{i}$ - # subsets of size i of set of n elements

↑ # subsets of a set of size n

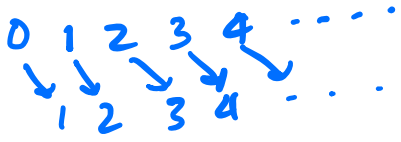
→ Alternate way to prove size of power set.

A set A is **finite** means it is empty or it is the same size as $\{1, \ldots, n\}$ for some $n \in \mathbb{N}$.
A set A is **countably infinite** means it is the same size as $\mathbb{N}$.
A set A is **countable** means it is either finite or countably infinite.

The set of positive integers ($\mathbb{Z}^+$) is countably infinite *List*: 1 2 3 4 5 6 7 8 9 10 11 . . .

bijection $f: \mathbb{N} \to \mathbb{Z}^+$ ↘ we need to show $|\mathbb{N}| = |\mathbb{Z}^+|$

$\forall x \in \mathbb{N}\ f(x) = x + 1$



The set of integers ($\mathbb{Z}$) is countably infinite *List*: 0 −1 1 −2 2 −3 3 −4 4 −5 5 . . .

$|\mathbb{N}| = |\mathbb{Z}|$

Consider the function $f:$ $\to$

$$f(x) = \begin{cases} 2x & \text{if } x \geq 0 \\ -2x - 1 & \text{if } x < 0 \end{cases}$$

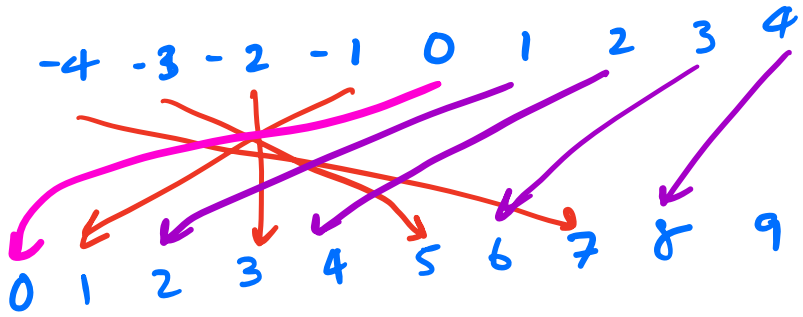
The function f is bijective between which possible domains and co-domains:

A. $f : \mathbb{Z}^+ \to \mathbb{N}$

B. $f : \mathbb{Z} \to \mathbb{N}$

C. $f : \mathbb{N} \to \mathbb{Z}$

C. $f : \mathbb{N} \to \mathbb{Z}^+$



show one-one & onto

Properties of cardinality

$$\forall A\ (\ |A| = |A|\ )$$
$$\forall A\ \forall B\ (\ |A| = |B|\ \to\ |B| = |A|\ )$$
$$\forall A\ \forall B\ \forall C\ (\ (|A| = |B|\ \wedge\ |B| = |C|)\ \to\ |A| = |C|\ )$$

More examples of countably infinite sets

Claim: $|\mathbb{Z}^+ \times \mathbb{Z}^+| = |\mathbb{Z}^+|$

Claim: L is countably infinite

One-to-one function from $\mathbb{N}$ to L

One-to-one function from L to $\mathbb{N}$

Countable sets

A set A is **finite** means it is empty or it is the same size as $\{1, \ldots, n\}$ for some $n \in \mathbb{N}$.

A set A is **countably infinite** means it is the same size as $\mathbb{N}$.

A set A is **countable** means it is either finite or countably infinite.

All countably infinite sets are the same size as one another!

Uncountable sets exist!

Implications: There are different sizes of infinity. Some infinities are smaller than other infinities!!

Extra example Prove or disprove: There is a set Y, $\neg(\ |Y| = |Y \times Y|\ )$

Extra example Prove or disprove: There is a set Y, $\neg(\ |Y| = |\mathcal{P}(Y)|\ )$

$\mathbb{N}$ and its power set

Example elements of $\mathbb{N}$

Example elements of $\mathcal{P}(\mathbb{N})$ *Recall*: For set A, its power set is $\mathcal{P}(A) = \{X \mid X \subseteq A\}$

Claim: $|\mathbb{N}| \leq |\mathcal{P}(\mathbb{N})|$

A set A is **uncountable** means it is not countable.

Claim: There is an uncountable set. Example: _____

Proof: By definition of countable, since _____ is not finite, **to show** is $|\mathbb{N}| \neq |\mathcal{P}(\mathbb{N})|$.

Rewriting using the definition of cardinality, **to show** is

Towards a proof by universal generalization, consider an arbitrary function $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$.

To show: f is not a bijection. It's enough to show that f is not onto.

Rewriting using the definition of onto, **to show**:

By logical equivalence, we can write this as an existential statement:

In search of a witness, define the following collection of nonnegative integers:

$$D_f = \{n \in \mathbb{N} \mid n \notin f(n)\}$$

By definition of power set, since all elements of D_f are in $\mathbb{N}$, $D_f \in \mathcal{P}(\mathbb{N})$. It's enough to prove the following Lemma:

Lemma: $\forall a \in \mathbb{N}$ ($f(a) \neq D_f$).

Proof of lemma:

By the Lemma, we have proved that f is not onto, and since f was arbitrary, there are no onto functions from $\mathbb{N}$ to $\mathcal{P}(\mathbb{N})$. QED

Where does D_f come from? The idea is to build a set that would "disagree" with each of the images of f about some element.

$n \in \mathbb{N}$	$f(n) = X_n$	Is $0 \in X_n$?	Is $1 \in X_n$?	Is $2 \in X_n$?	Is $3 \in X_n$?	Is $4 \in X_n$?	...	Is $n \in D_f$?
0	$f(0) = X_0$	**Y / N**	Y / N	Y / N	Y / N	Y / N	...	**N / Y**
1	$f(1) = X_1$	Y / N	**Y / N**	Y / N	Y / N	Y / N	...	**N / Y**
2	$f(2) = X_2$	Y / N	Y / N	**Y / N**	Y / N	Y / N	...	**N / Y**
3	$f(3) = X_3$	Y / N	Y / N	Y / N	**Y / N**	Y / N	...	**N / Y**
4	$f(4) = X_4$	Y / N	Y / N	Y / N	Y / N	**Y / N**	...	**N / Y**
$\vdots$								

$f_A : \mathbb{N} \to \mathcal{P}(\mathbb{N})$ where $f_A(x) = x^2$

$f_B : \mathbb{N} \to \mathcal{P}(\mathbb{N})$ where $f_B(x) = \{x^2\}$

$n \in \mathbb{N}$	$f_B(n) = X_n$	Is $0 \in X_n$?	Is $1 \in X_n$?	Is $2 \in X_n$?	Is $3 \in X_n$?	Is $4 \in X_n$?	...	Is $n \in D_{f_B}$?
0	$f_B(0) = \{0\} = X_0$	**Y**	N	N	N	N	...	No
1	$f_B(1) = \{1\} = X_1$	N	**Y**	N	N	N	...	No
2	$f_B(2) = \{4\} = X_2$	N	N	**N**	N	Y	...	Yes
3	$f_B(3) = \{9\} = X_3$	N	N	N	**N**	N	...	Yes
4	$f_B(4) = \{16\} = X_4$	N	N	N	N	**N**	...	Yes
$\vdots$								

Claim: $\{r \in \mathbb{R} \mid 0 \leq r \ \wedge \ r \leq 1\}$ is uncountable.

Proof: By definition of countable, since $\{r \in \mathbb{R} \mid 0 \leq r \ \wedge \ r \leq 1\}$ is not finite, **to show** is $|\mathbb{N}| \neq |\{r \in \mathbb{R} \mid 0 \leq r \ \wedge \ r \leq 1\}|$.

To show $\forall f : \mathbb{Z}^+ \to \{r \in \mathbb{R} \mid 0 \leq r \ \wedge \ r \leq 1\}$ (f is not a bijection) . Towards a proof by universal generalization, consider an arbitrary function $f : \mathbb{Z}^+ \to \{r \in \mathbb{R} \mid 0 \leq r \ \wedge \ r \leq 1\}$.

To show: f is not a bijection. It's enough to show that f is not onto. Rewriting using the definition of onto, **to show**:

$$\exists x \in \{r \in \mathbb{R} \mid 0 \leq r \ \wedge \ r \leq 1\} \ \forall a \in \mathbb{Z}^+ \ (\ f(a) \neq x \ )$$

List all the images of f for every $a \in \mathbb{Z}^+$

$f(1) = r1 = 0.b_{11}b_{12}b_{13}b_{14}...$

$f(2) = r2 = 0.b_{21}b_{22}b_{23}b_{24}...$

$f(3) = r3 = 0.b_{31}b_{32}b_{33}b_{34}...$

$f(4) = r4 = 0.b_{41}b_{42}b_{43}b_{44}...$
$\vdots$

In search of a witness, define the following real number by defining its binary expansion

$$d_f = 0.b_1b_2b_3\cdots$$

where $b_i = 1 - b_{ii}$ where b_{jk} is the coefficient of 2^{-k} in the binary expansion of $f(j)$. Since $d_f \neq f(a)$ for any positive integer a, f is not onto. ■

Examples of uncountable sets

- $\mathcal{P}(\mathbb{N})$, $\mathcal{P}(\mathbb{Z}^+)$, $\mathcal{P}(\mathbb{Z})$, power set of any countably infinite set.
- The closed interval $\{x \in \mathbb{R} \mid 0 \leq x \leq 1\}$, any other nonempty closed interval of real numbers whose endpoints are unequal, as well as the related intervals that exclude one or both of the endpoints.
- $\mathbb{R}$
- $\overline{\mathbb{Q}}$, the set of irrational numbers

Discrete Mathematics Material created by Mia Minnes and Joe Politz is licensed under a Creative Commons Attribution-Non Commercial 4.0 International License. Adapted for CMPSC40 by Diba Mirza.