Week 6 Part A 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,

$$|A| = |B| \quad \text{if and only if} \quad (|A| \leq |B| \text{ and } |B| \leq |A|) \quad \text{if and only if} \quad (|A| \geq |B| \text{ and } |B| \geq |A|)$$

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

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

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

Applications of the sum and product rule

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

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

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?

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?

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* $\mathcal{P}(S)$ *?*

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

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

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

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

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?*

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?

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	
1	
2	
3	

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

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

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

$(x + y)^n =$

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 ...

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

Consider the function $f : \quad \to$

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

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

Properties of cardinality

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

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

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

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

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**:

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

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

$$d_f = 0.b_1 b_2 b_3 \cdots$$

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