Definitions

Relations

For the following definitions, consider a relation R on a set S.

1. *Transitivity*: R is transitive $\Leftrightarrow (a, b) \in S, (b, c) \in S \Rightarrow (a, c) \in S$.
2. *Reflexivity*: R is reflexive $\Leftrightarrow \forall a \in S, (a, a) \in R$.
   Irreflexivity: R is irreflexive $\Leftrightarrow \forall a \in S, (a, a) \notin R$.
3. *Symmetry*: R is symmetric $\Leftrightarrow (a, b) \in R \Rightarrow (b, a) \in R$.
   Antisymmetry: R is antisymmetric $\Leftrightarrow (a, b) \wedge (b, a) \in R \Rightarrow a = b$.

- *Binary Relation*: A relation from a set to itself.
- *Equivalence Relation*: A relation that is reflexive, symmetric, and transitive.

Partitions: For a set A to be a partition of B, the following must be true of A:

1. The sets contained in A must be mutually disjoint.
2. The union of the sets contained in A must be B.
3. Every set in A must $\neq \varnothing$

- *Equivalence Class*: $[x]$ denotes the set of all elements related to x.

Ordering

- *Partial Ordering*: A relation R on S is a partial order if it is reflexive, antisymmetric, and transitive.
  - Relations with partial orders may be drawn using a Hasse diagram.
- *Total Ordering*: A relation R on S is a total order if it is a partial order and $\forall a, b \in S, (a, b) \in R$.
- *Strict Ordering*: Partial and Total orderings are strict if they are irreflexive.

Function

A *Function* is a relation F on a set X to a set Y where every element in X maps to exactly one element of set Y.

- *Injectivity*: $\forall (a, b) \in X, f(a) = f(b) \Leftrightarrow a = b$
- *Surjectivity*: $\forall a \in Y, \exists b \in X \text{ s.t. } f(b) = a$
- *Bijectivity*: Injective and Surjective

Useful Facts:

- Composing two injective functions gives an injective function.
- 2-regular functions: $f : A \to B$ is 2-regular $\Leftrightarrow \forall b \in B, \exists$ exactly two distinct $a_1, a_2 \in A$ s.t. $f(a_1) = f(a_2) = b$.
- Within the context of this class, invertible means bijective.
  - Invertible isn't really a formally defined term, so it can vary. In other contexts, it tends to simply mean injective.

Images: Given some $f : X \to Y$, The image of an input value x is the set of outputs it may produce. The preimage of an output y is the set of input values that produce y.

Cantor-Bernstein Theorem: Given infinite sets $A \to B$, iff $\exists$ some injective function from $A \to B$, and $\exists$ some injective function from $B \to A$, then $\exists$ some bijective function from $A \to B$. It follows that the two sets have the same cardinality: $|A| = |B|$.

Sets

- $P(A) = \{S : S \subseteq A\}$
- For a finite set A, if $|A| = k$, then $|P(A)| = 2^k$
- *Cartesian Product*: $A \times B = \{(a, b) : a \in A \wedge b \in B\}$
- The dual of a statement about sets is one with each $\cup$ swapped with $\cap$, each $\cap$ swapped with $\cup$, each $\mathbb{U}$ (universal set) swapped with $\varnothing$, and each $\varnothing$ swapped with $\mathbb{U}$.
- Set equality: The formal definition: $A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$.

Types of Proof

Direct Proof

Directly show that if p is true, then q is true as well.

- This includes proof by induction.

1. Write the proposition
2. Start with a true hypothesis
   Through definitions, axioms, and properties, work your way to a conclusion
3. End with a true conclusion

Indirect Proof

Proofs of an equivalent implication. For example, the contrapositive of a statement can be used to prove that statement.

- Proof by Contradiction

Assume a counterexample can be found. Then there is an element in the domain that either:

- Makes the hypothesis true   Makes the conclusion false

This leads to a contradiction.

Subtypes of Proof (?)

Element-wise Proofs

Show that for *any* arbitrary element inside a set, some relation holds.

- $A \subseteq B$: $\forall x \in A, x \in B$
- $A = B$: $A \subseteq B \wedge B \subseteq A$

Proof Tips

- Use the definitions to express things that reveal fundamental properties
- Use variables that represent **any** element in the domain
- Do not use the same variable for two different things
- Apply rules/properties that apply to every element in the domain
- The resulting conclusions should be true for any element in the domain.

Set-Builder Notation

$S = \{\text{domain} \mid \text{predicate}\}$

- $\{x \in \mathbb{N} : x \text{ is even}\}$
- $\{x \in \mathbb{N} : x \bmod 2 = 0\}$

Graphs

Isomorphism

Two graphs, A and B are said to be isomorphic if $\exists\ f : A_V \to B_V$, such that the same vertices stay connected. Denoted as $A \cong B$.

Two graphs that are isomorphic must have:

- The same number of:
  - Vertices (of any given degree)
  - Edges
  - Cycles/Circuits (of any given length)
- Same connectedness
- Same degree sequence (list of degrees in decreasing order)
- Cycle types

A graph is *connected* if there is a path between every pair of vertices in the graph. (this might be slightly wrong, you should probably read the question closely)

(Spanning) Trees

A graph, B is said to be a *spanning* graph of A if $\forall v \in A_V, v \in B_V$. There may be variation in edges.

A *tree* is a graph where each vertex only has one incoming edge, except for one (the root).

Tree Facts:

- Any tree with n vertices has $n - 1$ edges.
- Any *connected* graph with n vertices and $n - 1$ edges is necessarily a tree.

Minimal Spanning Trees:

- A spanning tree with the least total weight.
- If a graph has unique edge weights, it has a unique MST; otherwise, it may have many correct MSTs

Prim's Algorithm:

1. Start at any vertex, highlight it.
2. Identify all edges coming out of that vertex and choose the edge with the least weight.
3. While we still have unvisited vertices:
   a. Identify all edges coming out of all visited vertices to unvisited vertices
   b. Choose the edge with the minimum cost

Kruskal's Algorithm:

1. Start with an empty graph T
2. While we still have less than $n - 1$ edges:
   a. Identify an edge of minimum weight in G
   b. If adding this edge to T doesn't form a cycle, then add it to T and delete it from G

Adjacency Matrices

- Raising an adjacency matrix to the n-th power tells how many walks of length n there are between two vertices.
- Adding $M^1 + M^2 + M^3 + \dots + M^k$ gives the number of nontrivial walks of length k or less.

Relations can be expressed as graphs.
- A relation R is transitive $\Leftrightarrow M^2 \leq M$, where M is the adjacency matrix for R.

Trails, Walks, Cycles
- *Walk*: a list of alternating vertices and edges.
  - In a simple graph, there is no need to indicate the edges.
  - The length of a walk is its number of edges.
  - A walk is trivial if its length is 0.
  - A walk is *closed* if it starts and ends on the same vertex.
- *Trail*: a walk with no repeated edges.
- *Circuit*: a closed trail.
- *Path*: a walk with no repeated vertices.
- *Cycle*: a nontrivial circuit in which the only repeated vertex is the first/last one.

Eulerianness
- A trail or circuit is *Eulerian* if it uses every edge in the graph exactly once (allowing for revisiting vertices).
- A graph is Eulerian if it has an Eulerian trail/circuit containing every edge (technically, semi-Eulerian if only a trail).
- A graph is only Eulerian if every vertex has an even degree.
- A graph is semi-Eulerian if only 0 or 2 vertices have an odd degree.
- A Hamiltonian cycle is one that visits each vertex exactly once (allowing for revisiting edges).

Counting

	Order matters	Order does not matter
Repetitions are allowed	Ordered list (permutations with repetitions)	Unordered list or bag (combination with repetitions)
Repetitions are not allowed	Permutations (ordered list without repetition)	Combination or set (unordered list without repetition)

- *Rule of Products*: If there are n ways to do task A and m ways to do task B regardless of how A was performed, then there are $m \cdot n$ ways to do AB.
- *Rule of Sums*: If there are n ways to do task A and m ways to do task B, then there are $m + n$ ways to do task A or B but not both.
- *Choose*: $\binom{n}{r} = \frac{n!}{r!(n-r)!}$ *Permute*: $P(n, r) = \frac{n!}{(n-r)!}$

Example Problem

$\sqrt{2} \notin \mathbb{Q}$ - by contradiction.
- Suppose not. That is, $\exists p, q \in \mathbb{Z} \neq 0$ s.t. $\sqrt{2} = \frac{p}{q}$, s.t. (1) p, q do not share a factor.
- Then $2 = \frac{p^2}{q^2} \Rightarrow 2q^2 = p^2$.
- By definition of even, p^2 is even.
- This implies p is even. (proof omitted)
- Then, $p = 2a, a \in \mathbb{Z} \Rightarrow 2 = \frac{4a^2}{q^2} \Rightarrow q^2 = 2a^2$.
- By definition of even, q^2 is even.
- This implies q is even.
- Since both are even, they both have a common factor 2.
- This contradicts (1): p, q do not share a factor. ■

There are infinitely many prime numbers - by contradiction.
- Fact (1): Any integer $n > 1$ is divisible by some prime number.
- Fact (2): For any integer, a, and any prime number, p, if $p \mid a \Rightarrow p \nmid a + 1$
- Assume there is a finite number of prime numbers. Then, let p be the largest prime number.
- Then, we can write all the prime numbers in ascending order as such: $2, 3, 5, 7, 11, ..., p$.
- Let another integer, $n = (2 * 3 * 5 * 7 * ... * p) + 1$.
- We know by (2) that since n is divisible by every prime number, $n + 1$ is divisible by no prime number.
- But by (1), $n + 1$ must be divisible by some prime number.
- This contradicts our assumption that p is the largest prime number. Therefore, there are infinitely many prime numbers. ■

How many ways to rearrange the letters in the word "MISSISSIPPI":
- 11 letters means 11! permutations, but this is an overcount
- Each set of identical letters is overcounted, so divide by those permutations:
- $\frac{11!}{4! \cdot 4! \cdot 2! \cdot 1!}$

How many sequences (x, y, z) of non-negative integers satisfy $x + y + z = 10$?
- The solution is a sequence of three numbers in $\mathbb{Z}^{\geq 0}$ that add up to 10. Note:
  - Order matters, because it is a sequence
  - Repeats are allowed
  - This is not an unordered list structure
- How many binary sequences of length 12 have exactly two 1's and ten 0's?
- Precisely equal to the desired answer.
- The number of binary sequences of length $r + n - 1$ containing exactly r 0's is $\binom{r+n-1}{r}$.

How many outcomes frrom four throws of a six-sided die sum to 14?
1. Count solutions where all $x_i \geq 1$.
2. Count solutions where some $x_j \geq 7$.
3. Required answer is (1) - (2).

$x_1 + x_2 + x_3 + x_4 = 14$.

1:
- The minimum number that appears on a die is 1, so 4 out of 14 is already guaranteed.
- The same as counting solutions where $y_i \geq 0$ for the equation $y_1 + y_2 + y_3 + y_4 = 10$.
- We know that the number of solutions with $y_i \geq 0$ is $\binom{10+4-1}{10} = 286$.

2: Count solutions where at least one $x_j \geq 7$ for $x_1 + x_2 + x_3 + x_4 = 14$.
- Equivalent to "How many bags of 14 pieces of fruit can be bought from a store that sells apples, bananas, oranges, and pears, if we get at least 7 of one kind and one of each other kind?"
- One way to pick 7 apples, 1 banana, 1 orange, and 1 pear.
  - How many ways to pick the remaining 4 pieces of fruit to fill the bag?
  - Equivalent to $z_1 + z_2 + z_3 + z_4 = 4$.
  - $\binom{4+4-1}{4}$.
- One way to pick 1 apple, 7 bananas, 1 orange, and 1 pear.
- So on, and so forth...
- Resulting quantity is $\binom{4+4-1}{4} \cdot 4$.

3: Required answer is (1) - (2).

$(A \cap B) \cup (A \cap C) = A \cap (B \cup C)$ - element-wise.
By definition of set equality, we must prove two things:
1. $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$
2. $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$

For 1: Let $x \in (A \cap B) \cup (A \cap C)$. By definition of $\cup$, we consider two possible cases:
1. $x \in A \cap B$
   - By definition of $\cap$, $x \in A \land x \in B$.
   - By definition of $\cup$, $x \in B \Rightarrow x \in B \cup C$.
   - By definition of $\cap$, since $x \in A \land x \in B \cup C, x \in A \cap (B \cup C)$.
2. $x \in A \cap C$.
   - By definition of $\cap$, $x \in A \land x \in C$.
   - By definition of $\cup$, $x \in C \Rightarrow x \in B \cup C$.
   - By definition of $\cap$, since $x \in A \land x \in B \cup C, x \in A \cap (B \cup C)$.

Therefore, $x \in (A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$.■

For 2: Let $x \in A \cap (B \cup C)$. By definition of $\cap$, we know $x \in A \land x \in (B \cup C)$. By definition of $\cup$, we consider two possible cases:
1. $x \in A \land x \in B$.
   - By definition of $\cap$, $x \in A \cap B$.
   - By definition of $\cup$, $x \in (A \cap B) \cup (A \cap C)$.
2. $x \in A \land x \in C$.
   - By definition of $\cap$, $x \in A \cap C$.
   - By definition of $\cup$, $x \in (A \cap B) \cup (A \cap C)$.

Therefore, $x \in A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.■

Since we have proved (1) and (2), $(A \cap B) \cup (A \cap C) = A \cap (B \cup C)$.■