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: $A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$.

Useful Properties

1. Connectedness of a relation - strong & weak

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.

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

Function Proofs

They basically involve proving either:

- Surjectivity
- Injectivity
- Both (Invertibility)

Logical Equivalence proofs

Show that two statements are logically equivalent using logic laws.

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

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

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

Example Proofs

$\sqrt{2} \notin \mathbb{Q}$ - 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 is no greatest even integer - by contradiction.

- Suppose not. That is, there is some greatest even integer, n.
- Then, by closure under addition, $n + 2 = k \in \mathbb{Z}$.
- By definition of even, $n = 2a, a \in \mathbb{Z}$.
- By substitution, $n + 2 = 2a + 2$.
- By distributive property, $2a + 2 = 2(a + 1)$.
- By definition of even, $2(a + 1)$ is even $\Rightarrow n + 2$ is even.
- Since $n + 2 > n$ and $n + 2$ is even, this contradicts our original assumption that there must be a greatest even integer. ■

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. ■

$A \cap B \subseteq A$ **- element-wise.**
- Let A and B be any sets.
- Let x be any element of $A \cap B$.
- By definition of $\cap$, $x \in A \land x \in B$.
- Since our choice of x was arbitrary, this implies every element in $A \cap B$ is also in A.
- Therefore, $A \cap B \subseteq A$.■

$A \subseteq C \land B \subseteq C \Rightarrow A \cup B \subseteq C$ **- element-wise.**
- Let sets A, B, C be any sets s.t. $A \subseteq C \land B \subseteq C$.

The goal here is to prove that for every element x, $x \in A \cup B \Rightarrow x \in C$.
- By definition of $\cup$, we consider two possible cases:
  - $x \in A$
    - Since $A \subseteq C$, by definition of $\subseteq$, $x \in C$.
  - $x \in B$
    - Since $B \subseteq C$, by definition of $\subseteq$, $x \in C$.
- In both cases, $x \in C$; therefore, $A \cup B \subseteq C$.■

$(A \cap B) \cup (A \cap C) = A \cap (B \cup C)$ **- 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), $(A \cap B) \cup (A \cap C) = A \cap (B \cup C)$.■

Prove that $g : \mathbb{Q} \to \mathbb{Q}$ with the rule $g(x) = 5x - 1$ is surjective - function proof.
- Let $y \in \mathbb{Q}$ (the codomain).
- We wish to show that $\exists x \in \mathbb{Q}, g(x) = y$.
- By substitution, $5x - 1 = y$.
- By algebra, $x = \frac{y+1}{5}$.
- We also wish to show that $x \in \mathbb{Q}$.
- By closure under addition, $y + 1 \in \mathbb{Z}$.
- By definition of $\mathbb{Q}$, $\frac{y+1}{5} = \frac{p}{q}, p, q \in \mathbb{Z} \Rightarrow \frac{y+1}{5} \in \mathbb{Q}$.

Prove that $f : \mathbb{Z} \to \mathbb{Z}$ with the rule $f(x) = 5x + 7$ is injective - function proof.
- Let $a, b \in \mathbb{Z}$ s.t. $f(a) = f(b)$. (Show they must be the same number)
- Then, $5a + 7 = 5b + 7$.
- By subtraction, $5a = 5b$.
- Since both sides are divisible by 5, the Division Theorem says the quotient must be unique.
- Therefore, $a = b$.■

Prove that there are infinite integers - proof by contradiction.
- Assume not. That is, assume there is some integer n, s.t. $\forall m \in \mathbb{Z}, n > m$.
- Consider $n + 1$. By closure over addition, $n + 1$ must be an integer as well.
- This contradicts our assumption that n was the largest integer. Therefore, there are infinitely many integers. ■

Prove that the composition of two injective functions is itself an injective function - direct.
- Let $f : X \to Y, g : Y \to Z$, where g, y are both injective functions.
- By definition of injectivity, $g(x_1) = g(x_2) \Rightarrow x_1 = x_2$, and $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$. (variable names might not be acceptable here)
- Applying the composition, we want to show that $g(f(a)) = g(f(b)) \Rightarrow a = b$.
- By definition of injectivity, g being injective implies $f(a) = f(b)$.
- By definition of injectivity, f being injective implies $a = b$.■

Prove that the composition of two injective functions is itself an injective function - contradiction.
- Assume not. That is, $\exists$ distinct x_1, x_2 s.t. (1) $\ g(f(x_1)) = g(f(x_2))$.
- By definition of injectivity, g being injective implies $f(x_1) = f(x_2)$.
- By definition of injectivity, f being injective implies $x_1 = x_2$.
- But this contradicts (1) - our assumption that x_1 and x_2 are distinct. Therefore, $g \circ f(x)$ is injective. ■

This proof is basically just the direct proof again. Unsure if the one shown on 3/4 is correct…

Other
- Remainder Theorem: any a mod some b has exactly one remainder.
- What other theorems??