

Contents

1	Proof Techniques	1
1.1	Direct Proof	1
1.2	Proof by Cases	1
1.3	Counterexample	2
1.4	Contradiction	3
1.5	Proving by Contrapositive	4
2	Logic	5
2.1	Preliminary Definitions	5
2.2	Implication	6
2.3	Normal Forms	6
2.4	First-Order Logic	9
3	Sets and Notation	13
3.1	Membership vs. Subsets	13
3.2	Set Operations	14
3.3	Power Sets	15
3.4	Product	16
3.5	Proof by Set-Element Method	17
3.6	Set Algebra	20
4	Relations	23
4.1	Cartesian Products	23
4.2	Reflexivity	23
4.3	Symmetry and Transitivity	23
4.4	Equivalence Relation	23
4.5	Equivalence Classes	24
5	Functions	26
5.1	Formal Definition	26
5.2	Injectivity	26
5.3	Surjectivity	26
5.4	Bijectivity	28

1 Proof Techniques

1.1 Direct Proof

We directly use our hypotheses to reason that our conclusion is correct.

Practice Problem(s)

Claim: Prove that for all integers n , if n is odd, then n^2 is odd.

Solution(s)

Let n be an arbitrary integer. Suppose n is an odd integer. By definition, $n = 2k + 1$ for some $k \in \mathbb{Z}$.

Then $n^2 = (2k + 1)^2 = (2k + 1)(2k + 1) = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 = 2m + 1$, where $m = 2k^2 + 2k$. m is an integer since it is the sum and product of integers.

Thus, n^2 is odd. Since n was arbitrary, this holds for all integers.

1.2 Proof by Cases

Proof by exhaustion, also known as proof by cases, is a method of mathematical proof in which the statement to be proved is split into a finite number of cases and each case is solved to show that, for every possible “angle” in the domain of a claim, we can exhaustively show that the claim can be proved.

Practice Problem(s)

1. Prove the claim that there exists irrational $x, y \in \mathbb{R}$ such that x^y is rational.
2. Let's agree that given any two people, they have either met or not. If every pair of people in a group has met, we'll call the group a club. If every pair of people in a group has not met, we'll call it a group of strangers.

Prove that every collection of 6 people includes a club of 3 people or a group of 3 strangers.^a

^a*Mathematics for Computer Science* Eric Lehman. 1.7.

Solution(s)

1. Claim: There exists irrational $x, y \in \mathbb{R}$ such that x^y is rational.

Proof: Consider $z = \sqrt{2}^{\sqrt{2}}$

Case 1: z is rational. Let $x = y = \sqrt{2}$, then we are done.

Case 2: z is irrational. Let $x = z$ and $y = \sqrt{2}$ and we get $\sqrt{2}^{\sqrt{2} * \sqrt{2}} = \sqrt{2}^2 = 2$, which is rational.

2. Claim: Every collection of 6 people includes a club of 3 people or a group of 3 strangers.

Proof: Let x denote one of the six people. Since the remaining number of people is 5, which is an odd number, either more or less than half of the people know x .

At least 3 have met x :

- If in those 3, no one knows each other, that is a group of 3 strangers, so the theorem holds.
- If in those 3, at least two people know each other, those two and x are a club of 3 people, so the theorem holds.

At least 3 have not met x :

- If in those 3, everyone knows each other, that is a club of 3 people, so the theorem holds.
- If in those 3, some pair has not met, that pair and x are a group of 3 strangers.

Since the theorem holds in all possible cases, it is always true.

1.3 Counterexample

Counterexamples help us prove that a certain claim is not true. A counterexample is a tangible example, that fits appropriately within the domain of a problem, that disproves the claim being made. Note that not every negative statement can be shown by counterexample (e.g., statements of the form “there does not exist...”).

However, you **cannot** prove a claim by showing one example of it. Counterexamples are used to *disprove*. (Alternatively, used to prove an inequality, as of sets.)

For example, the claim “all CS22 students like dinosaurs” can be disproved by finding a student who does not like dinosaurs. Finding this counterexample, however, will not prove that no 22 students like dinosaurs.

Practice Problem(s)

1. Prove or disprove the claim that for all sets A and B , $\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)$.
2. Prove or disprove via counterexample: $\forall x \in \mathbb{Z}, -1 \leq x \leq 1 \rightarrow x^2 = x$.

3. Consider set A as being the set of positive even integers. $(A_1, A_2) \in R$ if $A_1 = 3 \cdot A_2$. Example, $(18, 6) \in R$. Prove via counterexample that $(A_1, A_2) \in R \wedge (A_2, A_3) \in R \not\rightarrow (A_1, A_3) \in R$.

Solution(s)

1. Consider $A = \{1\}$ and $B = \{2\}$, then $\{1, 2\} \in \mathcal{P}(A \cup B)$ but $\{1, 2\} \notin \mathcal{P}(A) \cup \mathcal{P}(B)$.
2. Counterexample: $x = -1$, then $x^2 = x$ is $(-1)^2 = 1 \neq -1$, so the statement is incorrect.
3. Counterexample: To follow the condition to be in R , an example could be $A_1 = 9$, $A_2 = 3$, and $A_3 = 1$. Then $(A_1, A_3) \in R$ must be incorrect as $A_1 = 9 \cdot A_3$. Because the hypothesis is true in our example and the conclusion is false in our example then the statement in the question is true.

1.4 Contradiction

To prove the *negation* of a statement $\neg p$, we show that it is impossible for p to hold. This is known as *proof by contradiction*. It proceeds as follows:

1. Assume p is true.
2. Given p is true, use a direct proof to obtain a contradiction.
3. Since p being true leads us to a contradiction, p must be false, i.e., $\neg p$ must be true.

Occasionally, we can also use a similar technique to prove a positive (i.e., not negated) statement. *Before using contradiction, see if a direct approach would suffice.*

Here is how we would prove a (positive) proposition p by contradiction:

1. Assume p is not true.
2. Given p is false, use a direct proof to obtain a contradiction.
3. Since p being false leads us to a contradiction, p must be true.

Practice Problem(s)

1. Prove that there is no least positive real number.
2. Prove "If $3n + 2$ is odd, then n is odd." via contradiction.
3. Show that if n is an integer and $n^3 + 5$ is odd, then n is even using

- a) a proof by contraposition.
- b) a proof by contradiction.
4. Consider a set $A = \{a_1, \dots, a_n\}$ with cardinality n . Consider $f : \mathcal{P}(A) \rightarrow \{0, 1\}^n$ where $f(X) = s_1 s_2 \dots s_n$ and $s_i = 1$ if $a_i \in X$ and $s_i = 0$ if $a_i \notin X$.
- Prove the claim that if $f(X_1) = f(X_2)$ then $X_1 = X_2$.

Solution(s)

- Suppose, by contradiction, that there was a least positive real number x . Since x is a positive real number, $x/2$ is also a positive real number, but $x/2 < x$. We have a contradiction, so there must be no least positive real number.
- Suppose that n is even, and assume that $3n + 2$ is odd. Then, we let $n = 2k$ for some integer k . This implies that $3n + 2 = 3(2k) + 2 = 6k + 2$ which is even, leading to a contradiction to the assumption that $3n + 2$ is odd. Thus, n must be odd.
- The contrapositive statement would be "if n is odd, then $n^3 + 5$ is even," so we will prove this statement. Let $n = 2k + 1$ for some integer k . Then $n^3 + 5 = (2k + 1)^3 + 5 = 8k^3 + 12k^2 + 6k + 1 + 5 = \underbrace{8k^3 + 12k^2 + 6k + 6}_{=2a, a \in \mathbb{Z}} = 2a$ is even. We've proven the contrapositive statement, which is equivalent to the original statement, so we have proved the original statement as well.
 - Suppose by contradiction that n is odd. Then $n = 2k + 1$ for some integer k . Then, $n^3 + 5 = (2k + 1)^3 + 5$ is even as shown in the previous problem, which yields a contradiction to the assumption that $n^3 + 5$ is odd.
- For this problem, a direct approach may be applied. Assume that $f(X_1) = f(X_2)$. By assumption, $f(X_1) = s_1 s_2 \dots s_n = f(X_2)$, where $s_1 s_2 \dots s_n$ is a binary string of n digits. Because each digit $s_i = 1$ if and only if $a_i \in X_1$ and $a_i \in X_2$, and $s_i = 0$ otherwise, $X_1 = X_2$.

1.5 Proving by Contrapositive

Alternatively, to prove "if p then q " we suppose that q is false and show that p must be false. This is called a proof by contrapositive. Given a proposition, "if p then q ", the proposition "if $\neg q$ then $\neg p$ " is called the **contrapositive** of the first proposition.

Practice Problem(s)

Prove for all integers n , if n^2 is even then n is even.

Solution(s)

Let n be an arbitrary integer. We show that if n^2 is even, then so is n , by contrapositive.

Suppose n is not even, and so is odd. Then

$$n = 2k + 1 \quad \text{for some integer } k.$$

So

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

Let $k' = 2k^2 + 2k$. Then k' is an integer since it is a sum and product of integers. So

$$n^2 = 2k' + 1,$$

and hence n^2 is odd and therefore not even. Since n was arbitrary, this holds for all integers n .

Samples of different proof types can be found in the resources section of the [22 website](#).

2 Logic

2.1 Preliminary Definitions

1. A **propositional formula** is a condensed representation of a truth table using logical operators and variables. We call a propositional formula a *proposition* for short.
2. The term **logical expression** is often used synonymously with the word proposition.
3. Two propositions are **logically equivalent** when they represent the same truth table. We can prove propositions are logically equivalent by either comparing their truth tables or using logical rewrite rules. A full list of the rules you can use is on our course website.
4. A **valid proposition** is one that evaluates to true on any choice of inputs; it is true no matter what. It is also sometimes called a tautology. The classic example of a valid proposition is $b \vee \neg b$ (thanks, Shakespeare).
5. A proposition is **satisfiable** if it evaluates to true on *some* choice of inputs; that is, that there is some assignment of the input variables to true and false that makes the proposition true.
6. A proposition is **unsatisfiable** if it is false on any choice of inputs; it is false no matter what. It is also sometimes called a contradiction. The classic example of an unsatisfiable proposition is $p \wedge \neg p$.

Let's now review the interpretation of each of the following logical operators:

P	Q	P	$P \wedge Q$	$P \vee Q$	$P \oplus Q$	$P \rightarrow Q$	$P \leftrightarrow Q$
T	T	F	T	T	F	T	T
T	F	F	F	T	T	F	F
F	T	T	F	T	T	T	F
F	F	T	F	F	F	T	T

2.2 Implication

In the formula $P \rightarrow Q$, we call P the **hypothesis** and Q the **conclusion**. $P \rightarrow Q$ is logically equivalent to $\neg P \vee Q$. In words, this means that for $P \rightarrow Q$ to be true, Q must be true or P must be false.

This choice can seem a little strange at first. Why is $P \rightarrow Q$ true when P is false? Consider the following statement: "If it is raining, I will bring my umbrella." Here are the events that could possibly occur.

- It rains, and I bring my umbrella. That seems fine. The statement is consistent with the situation.
- It rains, and I don't bring my umbrella. The statement does not fit with the situation.
- It doesn't rain, and I bring my umbrella. This situation doesn't seem to directly conflict with the statement. After all, what if I brought my umbrella to block the sun instead? As a result, we say the statement is still consistent with the situation.
- It doesn't rain, and I don't bring my umbrella. The statement seems consistent with this situation, too.

The only scenario where the statement doesn't fit is the second, which is why $P \rightarrow Q$ is only false when P is true and Q is false.

- $\neg Q \rightarrow \neg P$ is called the **contrapositive** of $P \rightarrow Q$ and is logically equivalent. As a result, we have a useful proof technique: to prove the statement "if p, then q" we can instead prove "if not q, then not p."
- $Q \rightarrow P$ is called the **converse** of $P \rightarrow Q$. It is **not** logically equivalent to $P \rightarrow Q$. If both a statement and its converse are true, then the biconditional $P \leftrightarrow Q$ is true.

2.3 Normal Forms

We say a proposition is in **DNF (disjunctive normal form)** when it is the disjunction (clauses ORed together (\vee)) of conjunctions (literals ANDed together (\wedge)).

We say a proposition is in **CNF (conjunctive normal form)** when it is the conjunction (clauses ANDed together (\wedge)) of disjunctions (literals ORed together (\vee)).

Here's a truth table, and propositions in DNF and CNF that represent it:

P	Q	R	$?$
T	T	T	F
T	T	F	T
T	F	T	F
T	F	F	T
F	T	T	F
F	T	F	F
F	F	T	T
F	F	F	T

DNF: $(P \wedge Q \wedge \neg R) \vee (P \wedge \neg Q \wedge \neg R) \vee (\neg P \wedge \neg Q \wedge R) \vee (\neg P \wedge \neg Q \wedge \neg R)$

CNF: $(\neg P \vee \neg Q \vee \neg R) \wedge (\neg P \vee Q \vee \neg R) \wedge (P \vee \neg Q \vee \neg R) \wedge (P \vee \neg Q \vee R)$

If we have an arbitrary truth table, here are two ways we can think about describing it:

- Listing the true rows.
- Listing the false rows.

Since every row must be either true or false, both of these ways will uniquely describe our truth table.

These two ways correspond to DNF and CNF, respectively. To write a proposition in DNF, we can think about it like this: we find all rows where our proposition should evaluate to true, and we say that we must be in one of those rows. On the other hand, to write a proposition in CNF, we find all rows where our proposition should evaluate to false, and say we are not in any of those rows.

For DNF, we \wedge the true variables and negations of the false variables (to be in the row, the inputs must exactly correspond to the row). For CNF, we \vee the false variables and the negations of the true variables (to not be in the row, we just need at least one variable to be different).

In this way, we can represent any truth table in DNF or CNF. We can also rewrite any logical expression to be in DNF or CNF.

Practice Problem(s)

1. Suppose we define a new operation \star on logical propositions such that

$$x \star y \equiv \neg(x \wedge y)$$

Create a truth table for each of the following expressions, and state which logical operator the expression is equivalent to.

- $x \star x$
- $(x \star y) \star (x \star y)$

- $(x \star x) \star (y \star y)$
- $(x \star (x \star y)) \star (y \star (y \star x))$

2. Write two propositions corresponding to the following truth table: one in DNF and one in CNF.

P	Q	R	$?$
T	T	T	T
T	T	F	T
T	F	T	F
T	F	F	F
F	T	T	F
F	T	F	T
F	F	T	T
F	F	F	T

Solution(s)

1. • From the definition of \star , we can deduce that $x \star x \equiv \neg(x \wedge x) \equiv \neg x$. Thus, our truth table is the same as the truth table for $\neg x$.

x	$\neg x$	$x \star x$
T	F	F
F	T	T

- We know that $(x \star y) \star (x \star y) \equiv \neg(x \wedge y) \star \neg(x \wedge y) \equiv \neg(\neg(x \wedge y) \wedge \neg(x \wedge y))$. Using DeMorgan's Law, we get $(x \wedge y) \vee (x \wedge y) \equiv x \wedge y$, so our truth table is

x	y	$x \wedge y$	$(x \star y) \star (x \star y)$
T	T	T	T
T	F	F	F
F	T	F	F
F	F	F	F

- Using the identity derived in the first part, we know that $(x \star x) \star (y \star y) \equiv \neg x \star \neg y \equiv \neg(\neg x \wedge \neg y)$. Using DeMorgan's Law, we get $x \vee y$. So, our truth table is

x	y	$x \vee y$	$(x \star x) \star (y \star y)$
T	T	T	T
T	F	T	T
F	T	T	T
F	F	F	F

- Using the identity derived in the second part, we see that

$$\begin{aligned}
(x \star (x \star y)) \star (y \star (y \star x)) &\equiv (x \star \neg(x \wedge y)) \star (y \star \neg(y \wedge x)) \\
&\equiv \neg(x \wedge \neg(x \wedge y)) \star \neg(y \wedge \neg(y \wedge x)) \\
&\equiv \neg(x \wedge (\neg x \vee \neg y)) \star \neg(y \wedge (\neg y \vee \neg x)) \\
&\equiv \neg(\neg(x \wedge (\neg x \vee \neg y)) \wedge \neg(y \wedge (\neg y \vee \neg x))) \\
&\equiv \neg(\neg((x \wedge \neg x) \vee (x \wedge \neg y)) \wedge \neg((y \wedge \neg y) \vee (y \wedge \neg x))) \\
&\equiv \neg(\neg(x \wedge \neg y) \wedge \neg(y \wedge \neg x)) \\
&\equiv (x \wedge \neg y) \vee (y \wedge \neg x) \\
&\equiv x \oplus y
\end{aligned}$$

We see that this is the same expression as exclusive or.

x	y	$x \oplus y$	$(x \star (x \star y)) \star (y \star (y \star x))$
T	T	F	F
T	F	T	T
F	T	T	T
F	F	F	F

2. **DNF** : $(P \wedge Q \wedge R) \vee (P \wedge Q \wedge \neg R) \vee (\neg P \wedge Q \wedge \neg R) \vee (\neg P \wedge \neg Q \wedge R) \vee (\neg P \wedge \neg Q \wedge \neg R)$

2.4 First-Order Logic

In propositional logic, we only consider “atomic” propositions, represented by propositional variables like p and q . First-order logic is more expressive: it allows us to write propositions *about* particular data (like numbers).

In particular, first-order logic lets us write expressions that make assertions about particular entities. Such expressions are called **predicates**; you can think of these a bit like functions from the data in question to the values “true” and “false.” For instance, we might define a predicate $\text{Odd}(n)$ that holds of a natural number $n : \mathbb{N}$ if and only if n is odd. Predicates are syntactically represented by *predicate variables* (like Odd), with the value of which they are being asserted written in parentheses after the predicate variable.

A given predicate can only make assertions about a certain *kind* of object: for instance, it wouldn’t really make sense to apply the predicate Odd above to an irrational number like $\sqrt{2}$. We therefore define for each predicate a **domain**, the collection of all the possible values of which the predicate can be asserted. (The domain of Odd would be \mathbb{N} .)

Given some predicate, we may wish to make claims about whether it holds of *any*, or of *all*, elements in its domain. **Quantifiers** allow us to express such claims in first-order logic. There are two quantifiers of note:

1. Universal quantifier: denoted by the \forall symbol, it represents that a predicate holds for *every* element in its domain.
2. Existential quantifier: denoted by the \exists symbol, it represents that a predicate holds for

some element in its domain.

For instance, the formula $\forall n : \mathbb{N}, \text{Odd}(n)$ asserts that every natural number is odd (this is false!). On the other hand, $\exists n : \mathbb{N}, \text{Odd}(n)$ asserts that at least one odd natural number exists (this is true!).

Note that a universal quantification over an empty domain is always true, while an existential quantification over an empty domain is always false.

We can also chain quantifiers in sequence to represent a more complex proposition.

Example

Problem: Render *Goldbach's conjecture*, that every integer greater than 2 is the sum of two primes, in first-order logic.^a

We first can reformulate this in English in a way that better matches our first-order syntax: “For every even integer n greater than 2, there exist primes p and q such that $n = p + q$ ”.
Note: the TAs find this to be especially helpful!

We can then define some predicates. Let G be the predicate on natural numbers defined by $G(n) := n \geq 2$; that is, $G(n)$ is true just in case $n \geq 2$. Let P be the predicate on natural numbers such that $P(n)$ holds just in case n is prime.

We can thus describe the conjecture in first-order logic as follows:

$$\forall n : \mathbb{N}, G(n) \rightarrow \exists p, q : \mathbb{N}, P(p) \wedge P(q) \wedge n = p + q$$

Note that the order of quantifiers is essential. If we switched the order of the quantifiers, we would essentially assert that there are two prime numbers whose sum is equal to every number greater than 2. (This is clearly false!)

Note also the different ways we “restrict” universal and existential quantifiers (so that we are only considering n satisfying G and so that the witnesses p and q must have property P). If we switched the \rightarrow and \wedge symbols in the above, our formula would be incorrect! (Think about why.)

^a*Mathematics for Computer Science* Eric Lehman. 3.6.

Practice Problem(s)

1. For following questions, assume these definitions:

- Sets:
 - T : The set of CS22 TAs.
- Predicates:

- $D(x)$ “ x double majors at Brown”
- $M(x, y)$ “ x and y share a major in common.”
- $F(x, y)$ “ x and y are friends.”

- Functions

- $n(x)$: The number of majors x studies.

- Constants

- r : Rob, cs22 professor (also known as the Last Logician)!

Using the above definitions, translate these sentences into First-Order logic.

- a) Every TA on the 22 staff double majors.
- b) A TA on staff is friends with every other TA on staff.
- c) Every TA on staff is friends with Rob. (<3).
- d) TAs that study the same major are friends.
- e) There is a TA who doesn't have the same major as anyone else on staff.
- f) There is a TA that studies more majors than any other TA on staff.

2. Translate the following sentences into first-order logic. You may only use \mathbb{N} as a domain of quantification. You may use the relations $=$, $<$, \leq , $>$, and \geq ; functions $+$, $-$, and \times ; and one-place predicate Prime. You may not use any quantifiers or connectives other than those we have discussed in this guide.

- a) The difference of any two natural numbers is no greater than their sum.
- b) No prime number is square.
- c) (Challenge) There is a *unique*^a natural number that is less than every other natural number.

^aI.e., it is the only natural number with this property.

Solution(s)

1.
 - a) $\forall t \in T, D(t)$
 - b) $\exists t_1 \in T, (\forall t_2 \in T, t_1 \neq t_2 \rightarrow F(t_1, t_2)).$
 - c) $\forall t \in T, F(t, r)$

d) $\forall t_1, t_2 \in T, M(t_1, t_2) \rightarrow F(t_1, t_2)$

e) $\exists t_1 \in T, (\forall t_2 \in T, t_1 \neq t_2 \rightarrow \neg M(t_1, t_2))$

f) $\exists t_1 \in T, (\forall t_2 \in T, t_1 \neq t_2 \rightarrow n(t_1) > n(t_2))$

2. a) $\forall n_1, n_2 \in \mathbb{N}, n_1 - n_2 \leq n_1 + n_2$

b) $\forall p \in \mathbb{N}, \text{Prime}(p) \rightarrow (\forall n \in \mathbb{N}, \neg(n \times n = p))$

c) $\exists n_1 \in \mathbb{N}, [(\forall n_2 \in \mathbb{N}, \neg(n_1 = n_2) \implies (n_1 < n_2)) \wedge (\forall n_3 \in \mathbb{N}, (\forall n_4 \in \mathbb{N}, \neg(n_3 = n_4) \implies n_3 < n_4) \implies n_1 = n_3)]$

3 Sets and Notation

A set is a collection of objects without order or repetition.

3.1 Membership vs. Subsets

If an object s is a member of a set S , we say $s \in S$. If a set T is a subset of a set S , we write $T \subseteq S$. This means that every member of T is also a member of S .

Practice Problem(s)

1. A is any set. Which of the following is **always true**?
 - i. $A \subseteq A$
 - ii. $\{\} \subseteq A$
 - iii. $\{\} \in A$
2. A is any set and $\mathcal{P}(A)$ is the set of all subsets of A . Which of the following is **always true**?
 - i. $A \in \mathcal{P}(A)$
 - ii. $A \subseteq \mathcal{P}(A)$
 - iii. $\emptyset \in \mathcal{P}(A)$
 - iv. $\emptyset \subseteq \mathcal{P}(A)$
 - v. $\{A, \emptyset\} \subseteq \mathcal{P}(A)$
3. S is the set of students in CS22. B is the set of students at Brown. Duncan is a student in CS22. Which of the following is **always true**?
 - i. $S \subseteq B$
 - ii. Duncan $\subseteq S$
 - iii. Duncan $\in S$
 - iv. {Duncan} $\subseteq B$

Solution(s)

1. i. and ii. are always true.
2. i., iii., iv., and v. are always true.
3. i., iii., and iv. are always true.

3.2 Set Operations

- The union $A \cup B$ of two sets A and B is the set of all elements that are in A or B .
- The intersection $A \cap B$ of two sets A and B is the set of all elements that are in A and B .
- The set difference $B \setminus A$ of two sets A and B is the set of all elements that are in B , but that are not in A .
- The complement \overline{A} of a set A is the set of all elements that are *not* in A (where “all elements” refers to all elements in some universal set U .)
- The cardinality $|A|$ of a set A is the number of elements of A . Remember that sets have no duplicates!

Practice Problem(s)

1. For this problem, let

$$A = \{-3, -1, 0, 6\}$$

$$B = \{x \in \mathbb{Z} : x^2 \leq 5\}$$

$$C = \{x \in \mathbb{Z} : \exists y \in \mathbb{Z} \text{ s.t. } 3y = x\}$$

$$D = \{x \in \mathbb{Z} : \exists y \in \mathbb{Z} \text{ s.t. } y^2 \leq x\}$$

Find the following sets (not all sets are finite):

- i. $A \cup B$
- ii. $A \cap \overline{C}$
- iii. $B \cap D$
- iv. $A \setminus C$
- v. $B \setminus (C \cup D)$
- vi. $C \cap D$
- vii. $C \cup D$

Find the cardinalities of the following sets:

- i. A
- ii. $(B \setminus C) \setminus D$
- iii. $(A \cup B) \cap (C \cap D)$

Solution(s)

1.
 - i. $\{-3, -2, -1, 0, 1, 2, 6\}$
 - ii. $\{-1\}$
 - iii. $\{0, 1, 2\}$
 - iv. $\{-1\}$
 - v. $\{-2, -1\}$
 - vi. The set of all non-negative multiples of 3.
 - vii. The set containing both all negative multiples of 3 and all non-negative integers.
2.
 - i. 4
 - ii. 2 (The set is $\{-2, -1\}$)
 - iii. 2 (The set is $\{0, 6\}$)

3.3 Power Sets

The *power set* of a set S , denoted $\mathcal{P}(S)$, is the set of all subsets of S . The power set of S has cardinality $2^{|S|}$. We proved this last result by noticing that there are the same number of subsets of a set of size n as there are binary strings of length n (see the sample [bijective proof](#) on the website).

Practice Problem(s)

1. Let A, B, C, D be the sets from above, find the following sets:
 - i. $\mathcal{P}(A \cap B)$
 - ii. $\mathcal{P}(A) \cap \mathcal{P}(D)$
 - iii. $\mathcal{P}(B) \setminus \mathcal{P}(C)$
 - iv. $\mathcal{P}(\mathcal{P}(\emptyset))$

Solution(s)

1.
 - i. $\{\emptyset, \{0\}, \{-1\}, \{0, -1\}\}$
 - ii. $\{\emptyset, \{0\}, \{6\}, \{0, 6\}\}$
 - iii. $\mathcal{P}(B) \setminus \{\emptyset, \{0\}\} = \{\{-2\}, \{-1\}, \{1\}, \{2\},$
 $\{-2, -1\}, \{-2, 0\}, \{-2, 1\}, \{-2, 2\},$
 $\{-1, 0\}, \{-1, 1\}, \{-1, 2\}, \{0, 1\},$
 $\{0, 2\}, \{1, 2\}, \{-2, -1, 0\}, \{-2, -1, 1\},$
 $\{-2, -1, 2\}, \{-2, 0, 1\}, \{-2, 0, 2\}, \{-2, 1, 2\},$
 $\{-1, 0, 1\}, \{-1, 0, 2\}, \{-1, 1, 2\}, \{0, 1, 2\},$
 $\{-2, -1, 0, 1\}, \{-2, -1, 0, 2\}, \{-2, -1, 1, 2\},$
 $\{-2, 0, 1, 2\}, \{-1, 0, 1, 2\}, \{-2, -1, 0, 1, 2\}\}$
 - iv. $\{\emptyset, \{\emptyset\}\}$

3.4 Product

The product of two sets A and B , denoted $A \times B$, is the set of all ordered pairs (a, b) for $a \in A$, $b \in B$. The product of a single set, A , is the set of all ordered pairs (a, a) where $a \in A$.

Practice Problem(s)

1. Let A, B, C, D be the sets from above, find the following sets:
 - i. $A \times B$
 - ii. $B \times \{\emptyset\}$
 - iii. $C \times \emptyset$
 - iv. $\emptyset \times \emptyset$
2. Prove that $(\mathbb{Z} \times \mathbb{N}) \cap (\mathbb{N} \times \mathbb{Z}) = \mathbb{N} \times \mathbb{N}$.
3. Disprove the following claim: $|A \times A| < |\mathcal{P}(A)|$ for any arbitrary finite set A .
4. Disprove the following claim: for any two finite sets A and B , $|\mathcal{P}(A \times B)| = |\mathcal{P}(A) \times \mathcal{P}(B)|$.

Solution(s)

1.
 - i. The set of all ordered pairs (a, b) for $a \in A$ and $b \in B$.

- ii. The set of all ordered pairs (b, \emptyset) for $b \in B$.
 - iii. \emptyset
 - iv. \emptyset
2. To prove this, essentially the only time $(\mathbb{Z} \times \mathbb{N})$ intersects with $(\mathbb{N} \times \mathbb{Z})$ is when the first value in the ordered pair is a natural number since the integer needs to be equal to the natural number, which will be a natural number since integers encompass the natural numbers. This follows for the exact same reason for the second value in the ordered pair, meaning the intersection between $(\mathbb{Z} \times \mathbb{N})$ and $(\mathbb{N} \times \mathbb{Z})$ is $\mathbb{N} \times \mathbb{N}$.
 3. To disprove this, let's use a counterexample of $A = \{a, b\}$, then the set $A \times A$ contains the elements $(a, a), (a, b), (b, a), (b, b)$. $\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$, meaning both have 4 elements in their sets, meaning the cardinality of $A \times A$ is not strictly less than the cardinality of $\mathcal{P}(A)$.
 4. To disprove this claim, let's consider the two sets $A = \{a\}$ and $B = \{b\}$. $A \times B = (a, b)$ so the cardinality of the power set of $A \times B$ is $2^1 = 2$. The power set of A would be equal to $\{\emptyset, \{a\}\}$, and the power set of B would be equal to $\{\emptyset, \{b\}\}$, so $\mathcal{P}(A) \times \mathcal{P}(B) = \{(\emptyset, \emptyset), (\emptyset, b), (a, \emptyset), (b, \emptyset)\}$, meaning its cardinality is 4, disproving the claim made above.

3.5 Proof by Set-Element Method

How do you prove that some set A equals some set B ? First show that $A \subseteq B$ and then you show that $B \subseteq A$. If every element in A is also an element in B and every element in B is also an element of A , then A must equal B .

To show that $A \subseteq B$ you consider an arbitrary element in A and show it is also in B . In use, this looks like the following:

1. Let x be an element of set A .
2. Prove that x is also an element of B .
3. Conclude that $A \subseteq B$.

Example

Claim: $A \cap (A \cup B) = A$.

Proof. We show that both $A \cap (A \cup B) \subseteq A$ and $A \subseteq A \cap (A \cup B)$.

We first prove the subclaim that $A \cap (A \cup B) \subseteq A$.

Consider any $x \in A \cap (A \cup B)$. By definition of intersection, this means that $x \in A$ and $x \in A \cup B$. Because every arbitrary x in $x \in A \cap (A \cup B)$ is in A , we can conclude that

$$A \cap (A \cup B) \subseteq A.$$

We then prove the subclaim that $A \subseteq A \cap (A \cup B)$.

Consider any $x \in A$. By definition of union, we can reason that $x \in A \cup B$. Because we know that $x \in A \wedge x \in (A \cup B)$, by definition of intersection, we conclude $x \in A \cap (A \cup B)$. It follows that because every arbitrary x in A is in $A \cap (A \cup B)$, $A \subseteq A \cap (A \cup B)$.

Therefore, by the set element method we have proved that $A \cap (A \cup B) = A$. □

Practice Problem(s)

1. Prove the claim that $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$ via the set element method.
2. Prove the following properties using the set-element method.
 - a) $\overline{(A \cup B)} = \overline{A} \cap \overline{B}$
 - b) $\overline{(A \cap B)} = \overline{A} \cup \overline{B}$
3. Prove or disprove each of the following. To prove equality, use the set-element method.
 - a) $A \cup (B \cap C) = (A \cup B) \cap C$
 - b) $\overline{A} \cup (A \cap B) = \overline{A} \cup B$
 - c) $A \cap (B \setminus C) = (A \setminus B) \cap (A \setminus C)$

Solution(s)

1. *Claim:* $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$

Proof. We show that both $\mathcal{P}(A) \cap \mathcal{P}(B) \subseteq \mathcal{P}(A \cap B)$ and $\mathcal{P}(A \cap B) \subseteq \mathcal{P}(A) \cap \mathcal{P}(B)$.

We first prove the subclaim that $\mathcal{P}(A) \cap \mathcal{P}(B) \subseteq \mathcal{P}(A \cap B)$.

Consider an element $x \in \mathcal{P}(A) \cap \mathcal{P}(B)$. By definition of intersection, this means that $x \in \mathcal{P}(A)$ and $x \in \mathcal{P}(B)$. By the definition of a power set, this means that x is a subset containing only elements from both A and B . By definition of intersection, it follows that $x \in \mathcal{P}(A \cap B)$ for every arbitrary $x \in \mathcal{P}(A) \cap \mathcal{P}(B)$. So, we can conclude that $\mathcal{P}(A) \cap \mathcal{P}(B) \subseteq \mathcal{P}(A \cap B)$.

We then prove the subclaim that $\mathcal{P}(A \cap B) \subseteq \mathcal{P}(A) \cap \mathcal{P}(B)$.

Consider an element $x \in \mathcal{P}(A \cap B)$. By definition of a power set, this means that x is

a subset of the set $A \cap B$. By the definitions of intersection and power sets, x must be a subset that can only contain elements that exist in both A and B . So, we know that $x \in \mathcal{P}(A) \wedge x \in \mathcal{P}(B)$. By definition of intersection, it follows that $x \in \mathcal{P}(A) \cap \mathcal{P}(B)$ for every arbitrary $x \in \mathcal{P}(A \cap B)$, so we can conclude that $\mathcal{P}(A \cap B) \subseteq \mathcal{P}(A) \cap \mathcal{P}(B)$.

Therefore, by the set-element method we have proved that $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$. \square

2. a) *Claim:* $\overline{(A \cup B)} = \bar{A} \cap \bar{B}$

Proof. We show that both $\overline{(A \cup B)} \subseteq \bar{A} \cap \bar{B}$ and $\bar{A} \cap \bar{B} \subseteq \overline{(A \cup B)}$

We first prove the subclaim that $\bar{A} \cap \bar{B} \subseteq \overline{(A \cup B)}$

Suppose $x \in \bar{A} \cap \bar{B}$

This means that $x \in \bar{A} \wedge x \in \bar{B}$

From this we see that $\neg(x \in A)$ and $\neg(x \in B)$.

For the sake of contradiction, suppose $x \in A \cup B$

Then we know that $x \in A \vee x \in B$

But in either way, we will contradict one of the propositions in $\neg(x \in A)$ and $\neg(x \in B)$.

Thus we conclude that $x \in \overline{(A \cup B)}$.

We then prove the subclaim that $\overline{(A \cup B)} \subseteq \bar{A} \cap \bar{B}$.

Suppose $x \in \overline{(A \cup B)}$

This means that $\neg(x \in A \cup B)$

$x \in A \cup B$ can be rewritten as $x \in A \vee x \in B$ so $\neg(x \in A \vee x \in B)$

Using DeMorgan's Law, $x \notin A \wedge x \notin B$

$x \notin A \wedge x \notin B$ can be rewritten as $x \in \bar{A} \wedge x \in \bar{B}$

This means that $x \in \bar{A} \cap \bar{B}$

\square

b) *Claim:* $\overline{(A \cap B)} = \bar{A} \cup \bar{B}$

Proof. We show that both $\overline{(A \cap B)} \subseteq \bar{A} \cup \bar{B}$ and $\bar{A} \cup \bar{B} \subseteq \overline{(A \cap B)}$

We first prove the subclaim that $\overline{(A \cap B)} \subseteq \bar{A} \cup \bar{B}$.

Consider an element $x \in \overline{(A \cap B)}$. By definition of set complement, $x \notin A \cap B$, which is the same as writing $\neg(x \in A \wedge x \in B)$. Using DeMorgan's logical equivalence laws, this becomes $\neg(x \in A) \vee \neg(x \in B)$. So, $x \notin A \vee x \notin B$. By the definitions of union and set complement, $x \in \bar{A} \cup \bar{B}$ for every arbitrary $x \in \overline{(A \cap B)}$

We then prove the subclaim that $\bar{A} \cup \bar{B} \subseteq \overline{(A \cap B)}$

Consider an element $\overline{A \cup B} \subseteq \overline{(A \cap B)}$. By the definitions of set complement and union, this becomes $x \notin A \vee x \notin B$. We can write this as $\neg(x \in A) \vee \neg(x \in B)$. By DeMorgan's logical equivalence laws, this becomes $\neg(x \in A \wedge x \in B)$. By the definitions of set complement and intersection, we can write this as $x \in \overline{(A \cap B)}$ for every arbitrary $x \in \overline{A \cup B}$.

Therefore, by the set element method, we have proved that $\overline{(A \cap B)} = \overline{A \cup B}$. □

3. a. *Claim:* $A \cup (B \cap C) = (A \cup B) \cap C$

Proof. Let $x \in A \cup (B \cap C)$. Then either $x \in A$ or $x \in B \cap C$. Assume $x \in A$ and $x \notin B \cap C$. This means that $x \notin B$ and $x \notin C$. This is not an element of the right hand side, since $x \notin C$, so the sets are not equal. □

b. *Claim:* $\overline{A} \cup (A \cap B) = \overline{A} \cup B$

Proof. Let $x \in \overline{A} \cup (A \cap B)$. Then either $x \in \overline{A}$ or $x \in A \cap B$. In either case, $x \in \overline{A} \cup B$ because if $x \in \overline{A}$, then $x \in \overline{A} \cup B$. On the other hand, if $x \in A \cap B$, then $x \in B$ so $x \in \overline{A} \cup B$. Thus, $\overline{A} \cup (A \cap B) \subseteq \overline{A} \cup B$.

For the other direction, assume $x \in \overline{A} \cup B$. Then either $x \in \overline{A}$ or $x \in B$. Either way, if $x \in \overline{A}$, then $x \in \overline{A} \cup (A \cap B)$, and if $x \in B$ but $x \in A$, then $x \in \overline{A} \cup (A \cap B)$. Thus, $\overline{A} \cup B \subseteq \overline{A} \cup (A \cap B)$.

Since both sets contain each other, they must be the same set, so they are equal. □

c. LHS: let $x \in$ LHS. Then, $x \in A, x \in B, x \in \overline{C}$

RHS: let $x \in$ RHS. Then, $x \in A, x \in \overline{B}, x \in \overline{C}$.

Therefore, the sets are not equal.

3.6 Set Algebra

1. Conversion of one side of the equation to the other (or conversion of both sides to an identical expression) using stated laws of set algebra. (See list of [set identities](#) on course website!)
2. Conclusion based on the biconditionality of the steps taken.

Note: Do not assume equality before applying set identities! Either rewrite one side to look like the other or rewrite both sides separately to look like the same expression.

Example

Claim: $(A \cap B) \cup (A \setminus B) = A \cap (B \cup (A \setminus B))$.

Proof:

$$\begin{aligned}
 & (A \cap B) \cup (A \setminus B) \\
 &= (A \cap B) \cup (A \cap \overline{B}) && \text{(Set Difference Law)} \\
 &= A \cap (B \cup \overline{B}) && \text{(Distributive Law)} \\
 &= A \cap U && \text{(Complement Law)} \\
 &= A && \text{(Identity Law)} \\
 &= A \cap (A \cup B) && \text{(Absorption)} \\
 &= A \cap (B \cup A) && \text{(Commutativity)} \\
 &= A \cap ((B \cup A) \cap U) && \text{(Identity Law)} \\
 &= A \cap ((B \cup A) \cap (B \cup \overline{B})) && \text{(Complement Law)} \\
 &= A \cap (B \cup (A \cap \overline{B})) && \text{(Distributive Law)} \\
 &= A \cap (B \cup (A \setminus B)) && \text{(Set Difference Law)}
 \end{aligned}$$

□

Practice Problem(s)

Use the set equalities [here](#) to show the below.

1. $(A \cup B) \cap \overline{(A \cap B)} = (B \setminus A) \cup (A \setminus B)$.
2. $(A \cap \overline{B}) \cup B = A \cup B$.
3. $(A \setminus B) \setminus (B \setminus C) = (A \cup B) \setminus (A \cap B)$.

Solution(s)

$$1. (A \cup B) \cap \overline{(A \cap B)} = (B \setminus A) \cup (A \setminus B).$$

Proof.

$$\begin{aligned}
 (A \cup B) \cap \overline{(A \cap B)} &= (A \cup B) \cap (\overline{A} \cup \overline{B}) && \text{(De Morgan's Law)} \\
 &= (A \cap (\overline{A} \cup \overline{B})) \cup (B \cap (\overline{A} \cup \overline{B})) && \text{(Distributive Law)} \\
 &= (A \cap \overline{B}) \cup (B \cap \overline{A}) && \text{(Complement Law)} \\
 &= (A \setminus B) \cup (B \setminus A). && \text{(Set Difference Law)}
 \end{aligned}$$

□

$$2. (A \cap \overline{B}) \cup B = A \cup B.$$

Proof.

$$\begin{aligned}
 & (A \cap \overline{B}) \cup B \\
 &= (A \cup B) \cap (\overline{B} \cup B) && \text{(Distributive Law)} \\
 &= (A \cup B) \cap U && \text{(Complement Law)} \\
 &= A \cup B && \text{(Identity Law)}
 \end{aligned}$$

□

$$3. (A \setminus B) \setminus (B \setminus C) = (A \cup B) \setminus (A \cap B).$$

Proof.

$$\begin{aligned}
 & (A \setminus B) \setminus (B \setminus C) \\
 &= (A \cap \overline{B}) \cap \overline{(B \cap \overline{C})} && \text{(Set Difference Law)} \\
 &= (A \cap \overline{B}) \cap (\overline{B} \cup C) && \text{(DeMorgan's Law)} \\
 &= ((A \cap \overline{B}) \cap \overline{B}) \cup ((A \cap \overline{B}) \cap C) && \text{(Distributive Law)} \\
 &= (A \cap (\overline{B} \cap \overline{B})) \cup (A \cap (\overline{B} \cap C)) && \text{(Associative Law)} \\
 &= (A \cap \overline{B}) \cup (A \cap (\overline{B} \cap C)) && \text{(Idempotent Law)} \\
 &= A \cap (\overline{B}) \cup (\overline{B} \cap C) && \text{(Distributive Law)} \\
 &= A \cap \overline{B} && \text{(Absorption Law)} \\
 &= A \setminus B && \text{(Set Difference Law)} \\
 &= (A \cap \overline{B} \cup B) \cap ((A \cap \overline{B} \cup \overline{A}) && \text{(Distributive Law)} \\
 &= ((A \cup B) \cap (\overline{B} \cup B)) \cap ((A \cup \overline{A}) \cap (\overline{B} \cup \overline{A})) && \text{(Distributive Law)} \\
 &= ((A \cup B) \cap U) \cap (U \cap \overline{B} \cup \overline{A}) && \text{(Complement Law)} \\
 &= (A \cup B) \cap (\overline{B} \cup \overline{A}) && \text{(Identity Law)} \\
 &= (A \cup B) \cap \overline{(A \cap B)} && \text{(DeMorgan's Law)} \\
 &= (A \cup B) \setminus (A \cap B) && \text{(Set Difference Law)} \quad \square
 \end{aligned}$$

4 Relations

4.1 Cartesian Products

A *binary* (or *two-place*) *relation* R consists of a set A , called the *domain*; a set B , called the *codomain*; and a subset of the Cartesian product $A \times B$ called the *graph*. If we say that a relation R is *on* a set A , we mean that both its domain and codomain are A .

Always remember to specify the set(s) on which the relation is defined!

We write aRb or $(a, b) \in R$ to mean that a is related to b by R .

4.2 Reflexivity

A relation R on A is *reflexive* if for all $a \in A$, $(a, a) \in R$. In other words, a relation is reflexive if *every element* in the set A is related to itself in R . This is why it's important to specify a set when talking about a relation: you can't tell if a relation is reflexive if you don't know which elements have to be related to themselves (and every element must be!).

4.3 Symmetry and Transitivity

A relation R is *symmetric* if for all a, b in its domain, the following holds: **if** $(a, b) \in R$, **then** $(b, a) \in R$.

A relation R is *transitive* if for all a, b, c in its domain, the following holds: **if** $(a, b) \in R$ and $(b, c) \in R$, **then** $(a, c) \in R$. Remember that a , b , and c do not need to be different elements.

It's important to note that the definitions of symmetry and transitivity are phrased as if-then statements. A relation is symmetric/transitive *unless* it violates the appropriate if-then condition. To violate the condition, you must simultaneously satisfy the if-clause, and violate the then-clause.

Consider the following example of a relation that is not transitive: the ordered pairs $(1, 2)$ and $(2, 1)$ are in the relation (this satisfies the if-clause of the transitivity definition) but there is no pair $(1, 1)$ in the relation (this violates the then-clause).

As another illustrative example: any empty relation is reflexive, symmetric, and transitive, as there are no ordered pairs in the empty relation to satisfy the if-clause of the definitions.

4.4 Equivalence Relation

An *equivalence relation* is a relation that is reflexive, symmetric, and transitive.

4.5 Equivalence Classes

Let R be an equivalence relation on A . Then the *equivalence class* of $a \in A$ is defined as

$$[a]_R := \{x \mid x \in A, (x, a) \in R\}.$$

Note that a is not unique (unless it is the only element in its equivalence class.) Rather, any element in the same equivalent class can serve equally well as the representative for the class. An equivalence relation splits a set into equivalence classes. In other words, it forms partitions.

A *partition* of a set A is a collection of nonempty subsets B_1, \dots, B_k of A such that

1. $B_1 \cup \dots \cup B_k = A$, and
2. $B_i \cap B_j = \emptyset \quad \forall i, j$ where $i \neq j$.

Practice Problem(s)

1. Consider the set B of all students at Brown. For each of the following relations on B , state if they are reflexive, symmetric, or transitive. If they are an equivalence relation, then list the equivalence classes.
 - i. Two students are related if they are the same age (e.g. 21).
 - ii. s_1 and s_2 are students and $(s_1, s_2) \in R$ if s_1 is younger than s_2 .
 - iii. Two students are related if they are studying anthropology.
 - iv. Two students are related if they go to Brown.
2. Let $A = \{1, 2, 3\}$. Consider the following relations on $\mathcal{P}(A)$. State if they are reflexive, symmetric, or transitive. If they are an equivalence relation, then list the equivalence classes.
 - i. $(S_1, S_2) \in R$ if $|S_1| = |S_2|$.
 - ii. $(S_1, S_2) \in R$ if $S_1 \subseteq S_2$.
 - iii. $(S_1, S_2) \in R$ if S_1 and S_2 share an element.

Solution(s)

1.
 - i. This is an equivalence relation, and the equivalence classes are the different ages of the students.
 - ii. Transitive.
 - iii. Symmetric and transitive.

iv. Equivalence relation. The entire set B is one equivalence class.

2. i. Equivalence relation. The equivalence classes are

$$\{\{\emptyset\}, \{\{1\}, \{2\}, \{3\}\}, \{\{1, 2\}, \{1, 3\}, \{2, 3\}\}, \{\{1, 2, 3\}\}\}$$

ii. Reflexive and transitive.

iii. Reflexive and symmetric.

5 Functions

5.1 Formal Definition

A *function* $f : A \rightarrow B$ is a relation on A and B with the following property: for every $a \in A$ there exists exactly one pair (a, b) in the relation, where $b \in B$.

We call A the domain and B the codomain.

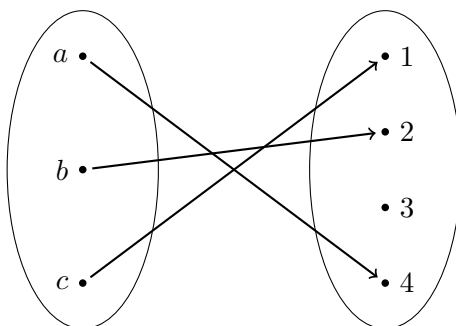
It's important to note that a function is characterized not only by the “rule” that maps inputs to outputs, but also by the domain and codomain.

Additionally, we call the set of all $b \in B$ such that there exists $a \in A$ where $f(a) = b$ the *image* of f . In other words, the image is the set of all elements mapped to by f .

5.2 Injectivity

A function is injective if for all $b \in B$, there exists at most one $a \in A$ such that $f(a) = b$. In other words, no two distinct elements map to the same thing!

If a function $f : A \rightarrow B$ is injective, we know that $|A| \leq |B|$. This is because every element in A needs some unmatched element in B , so B needs to have at least as many elements as A !



There are two ways to prove that a function is injective:

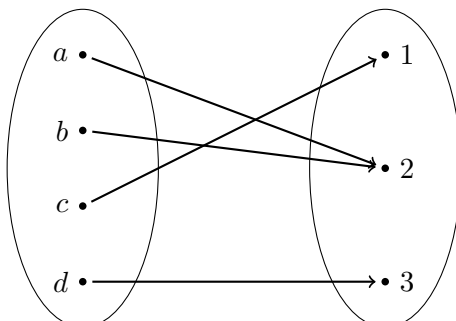
1. Consider two arbitrary elements a and b of the domain, and show that if $f(a) = f(b)$, then we must have $a = b$.
2. Consider two arbitrary distinct elements $a \neq b$ in the domain. Show that they must map to distinct outputs $f(a) \neq f(b)$.

5.3 Surjectivity

A function is surjective if for all $b \in B$, there exists at *least* one $a \in A$ such that $f(a) = b$. In other words, no element in the codomain gets left behind: there is always some element

that maps to it. Equivalently, a function is surjective if the image of the function is the entire codomain.

If a function $f : A \rightarrow B$ is surjective, we know that $|A| \geq |B|$. This is because every element in B needs some element in A to map to it, so A needs to have at least as many elements as B .



To prove that a function is surjective, consider an arbitrary element in the codomain, and construct the specific element in the domain that maps to it.

Practice Problem(s)

1. Let $S = \{0, 1\}$, $T = \{t : t \subseteq S \times S\}$, and R be the set of all possible functions from S to S .
 - i. Can an injection from T to R exist? If so, give one such injection and prove that this mapping is indeed injective. If not, prove why such a mapping cannot exist.
 - ii. Can a surjection from T to R exist? If so, give one such surjection and prove that this mapping is indeed surjective. If not, prove why such a mapping cannot exist.

Solution(s)

1.
 - i. An injection from T to R can not exist. First, we recognize that $T = \{t | t \subseteq S \times S\} = \mathcal{P}(S \times S)$. Since $|T| = |\mathcal{P}(S \times S)| = 2^{|S \times S|} = 2^4 = 16$ and $|R| = 4$ (each of the 2 inputs have 2 possible outputs creating 4 possible functions from S to S). Since there are 16 elements in T and a well-defined function must map each element in T to some element in R , it is not possible for each element in R to be mapped to by a distinct element.
 - ii. A surjection from T to R exists. Suppose $f_0, f_1, f_2, f_3 \in R$ are the 4 functions from S to S . We construct a mapping $g : T \rightarrow R$ where $g(t) = f_{|t| \pmod{4}}$. For example, $g(\{(0, 0), (0, 1), (1, 0)\}) = f_3$ since $|\{(0, 0), (0, 1), (1, 0)\}| \pmod{4} = 3 \pmod{4} = 3$. Given that we can construct subsets of $S \times S$ with 1, 2, 3, and 4 elements, every function in R is mapped to by at least 1 element of T .

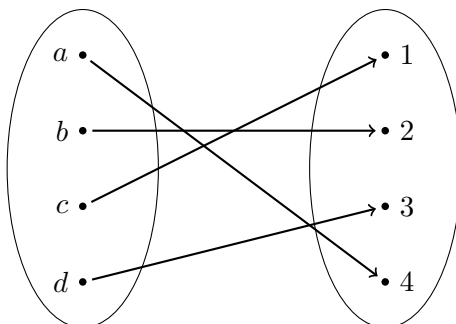
5.4 Bijection

A bijection is a function that is both injective and surjective. Thus, to prove that a function is a bijection, prove that it is injective and surjective.

If we combine our results from injectivity and surjectivity, we know that the cardinality of the domain must be less than or equal to that of the codomain (by injectivity), and that the cardinality of the domain must be greater than or equal to that of the codomain (by surjectivity.) Thus, the cardinalities of the two sets must be equal. This is a powerful result:

There exists a bijection between two sets if and only if they have equal cardinality.

Thus, to prove that the sizes of two sets are equal, it suffices to prove that there exists a bijection between them.



Practice Problem(s)

1. For each of the following, state if it is a function- if it is a function, conclude if it is injective and/or surjective.
 - a) $f : \mathbb{Z} \rightarrow \mathbb{Z}$ where $f(x) = x^2$
 - b) $f : \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$ where $f(x) = x^2$. \mathbb{Z}^+ denotes the positive integers.
 - c) $f : \mathbb{Z} \rightarrow \mathbb{Z}$ where $f(x) = \sqrt{x}$.
 - d) $f : A \rightarrow B$, where $f(\text{student}) = \text{the dorm that the student lives in}$, A represents the set of first year students at Brown, and B represents the set of first year dorms at brown.
 - e) $f : A \rightarrow B$, where $f(\text{student}) = \text{the banner ID of student}$, A represents the set of students at Brown, and B represents the set containing the Banner IDS of all current students at brown.
 - f) $f : \text{People in the World} \rightarrow \{0, 1\}$ where $f(\text{person}) = 1$ if they are Prof. Lewis and 0 otherwise.

- g) $f : A \rightarrow \mathbb{Z}$, where A represents the set of libraries at Brown and $f(\text{Library}) =$ number of books in the library.
- h) $f : S \rightarrow \mathcal{P}(S)$ where $f(S) = \{S\}$.
- i) $f : \mathcal{P}(\{1, 2, 4\}) \rightarrow \{0, 1, 2, 3\}$ where $f(X) = |X|$.
2. Let X be a set with n elements. Let B be the set of bit strings of length n . B can be expressed as $\{0, 1\}^n$. Prove that there is a bijection between $\mathcal{P}(X)$ and B , then conclude that $|\mathcal{P}(X)| = 2^n$.
3. Let A , B , and C be sets, and let $f : B \rightarrow C$ and $g : A \rightarrow B$ be functions. Let $h : A \rightarrow C$ be the composition, $f \circ g$, that is, $h(x) = f(g(x))$ for $x \in A$. Respond true or false to the following claims:
- (a) If h is surjective, then f must be surjective.
- (b) If h is surjective, then g must be surjective.
- (c) If h is injective, then f must be injective.
- (d) If h is injective and f is total, then g must be injective.

Solution(s)

1. a) $f : \mathbb{Z} \rightarrow \mathbb{Z}$ where $f(x) = x^2$
- A function but not injective or surjective.
- b) $f : \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$ where $f(x) = x^2$. \mathbb{Z}^+ denotes the positive integers.
- Function, Injection.
- c) $f : \mathbb{Z} \rightarrow \mathbb{Z}$ where $f(x) = \sqrt{x}$.
- Not a function.
- d) $f : A \rightarrow B$, where $f(\text{student}) =$ the dorm that the student lives in, A represents the set of first year students at Brown, and B represents the set of first year dorms at brown.
- Function, Surjection.
- e) $f : A \rightarrow B$, where $f(\text{student}) =$ the banner ID of student, A represents the set of students at Brown, and B represents the set containing the Banner IDS of all current students at brown.
- Function, Bijection.

f) $f : \text{People in the World} \rightarrow \{0, 1\}$ where $f(\text{person}) = 1$ if they are Prof. Lewis and 0 otherwise.

Function, Surjection

g) $f : A \rightarrow \mathbb{Z}$, where A represents the set of libraries at Brown and $f(\text{Library}) =$ number of books in the library.

Function, Injection

h) $f : S \rightarrow \mathcal{P}(S)$ where $f(S) = \{S\}$.

Function, Injection

i) $f : \mathcal{P}(\{1, 2, 4\}) \rightarrow \{0, 1, 2, 3\}$ where $f(X) = |X|$.

Function, Surjection

2. Let X be a set with n elements. Let B be the set of bit strings of length n . B can be expressed as $\{0, 1\}^n$. Prove that there is a bijection between $\mathcal{P}(X)$ and B , then conclude that $|\mathcal{P}(X)| = 2^n$.

In order to prove that the number of bit strings of length n is equal to the number of subsets of X , we will construct a bijection between these two sets. First, fix an ordering of the elements of X , say

$$X = \{x_1, x_2, \dots, x_n\}.$$

Define the function $f : \{0, 1\}^n \rightarrow \mathcal{P}(X)$ where

$$f((a_1, a_2, \dots, a_n)) = \{x_i : a_i = 1\}.$$

This function maps a bit string to the subset of X consisting of exactly those elements x_i whose positions correspond to 1's in the string. For example, if $X = \{x_1, x_2, x_3, x_4, x_5\}$ and we consider the bit string 10011, represented by $(1, 0, 0, 1, 1)$, then

$$f((1, 0, 0, 1, 1)) = \{x_1, x_4, x_5\}.$$

We now show that f is both injective and surjective, and therefore bijective.

Injective: Suppose that two bit strings $u, v \in \{0, 1\}^n$ both map to the same subset $S \in \mathcal{P}(X)$. Since S is defined by the positions of 1's in the string, if $f(u) = f(v) = S$, then u and v must have 1's in exactly the same positions. But bit strings only contain 0's and 1's, and both u and v are the same length n , so they must be identical. Therefore, f is injective.

Surjective: Consider a subset $S \in \mathcal{P}(X)$. Since S consists of elements of X , which we

ordered as x_1, \dots, x_n , we can construct an n -tuple $b = (b_1, b_2, \dots, b_n)$ where

$$b_i = \begin{cases} 1 & \text{if } x_i \in S, \\ 0 & \text{if } x_i \notin S. \end{cases}$$

By definition of f , we then have $f(b) = S$. Thus, every subset S is mapped to by some bit string, and f is surjective.

Since f is both injective and surjective, it is bijective. We have therefore created a bijection between the set of bit strings of length n and $\mathcal{P}(X)$. Thus, these two sets have equal cardinality. Finally, because there are 2 choices (0 or 1) for each of the n positions in a bit string, we know that

$$|\{0, 1\}^n| = 2^n.$$

Therefore,

$$|\mathcal{P}(X)| = 2^n.$$

3. Let A , B , and C be sets, and let $f : B \rightarrow C$ and $g : A \rightarrow B$ be functions. Let $h : A \rightarrow C$ be the composition, $f \circ g$, that is, $h(x) = f(g(x))$ for $x \in A$. Respond true or false to the following claims:

- (a) If h is surjective, then f must be surjective.

True

- (b) If h is surjective, then g must be surjective.

False

- (c) If h is injective, then f must be injective.

False

- (d) If h is injective and f is total, then g must be injective.

True