Contents

1 Logic **1**

1.1 Key Concept Review . . . 1
1.1.1 Propositional Logic . . . 1
1.1.2 Logic Proofs . . . 3
1.1.3 First Order Logic . . . 5
1.2 Technique: Translating Between Logic and English . . . 6
1.3 Technique: Writing Truth Tables . . . 8
1.4 Technique: Showing Logical Equivalence . . . 9
1.4.1 By Truth Tables . . . 9
1.4.2 By Logic Algebra . . . 10
1.5 Technique: Writing a Propositional Formula in DNF . . . 10
1.6 Technique: Checking the Validity of Rules of Inference . . . 11
1.6.1 By Truth Tables . . . 11
1.6.2 By Equivalence . . . 12
1.6.3 By Reasoning Through it . . . 12
1.7 Technique: Logic Proofs . . . 12

2 Math Foundations **14**

2.1 Key Concept Review . . . 14
2.1.1 Math Basics . . . 14
2.1.2 Set Theory Basics . . . 15
2.1.3 Relations and Functions . . . 21
2.1.4 Equivalence Relations . . . 24
2.2 Technique: Proving $\forall$ . . . 26
2.3 Technique: Proving If . . . 27
2.3.1 Directly Proving If . . . 27
2.3.2 Proving If by Contrapositive . . . 28
2.4 Technique: Proving Iff . . . 28
2.5 Technique: Proving $\exists$ . . . 28
2.6 Technique: Proving Or . . . 29
2.7 Technique: Using Or in a Proof (Proof by Cases) . . . 29
2.8 Technique: Proof by Contradiction . . . 29
2.9 Technique: Induction . . . 30
2.9.1 Strong Induction . . . 32
2.10 Technique: Proving Sets are Equal . . . 32
2.10.1 By the Set Element Method . . . 32
2.10.2 By Set Algebra . . . 33

1 Logic

We begin with some review content on logic.

1.1 Key Concept Review

The following section gives an overview of the key concepts we covered in logic.

1.1.1 Propositional Logic

In the beginning of logic, we covered propositional logic.

Definition 1 (Proposition)**.** *A* ***proposition*** *is a statement that is true or false.*

For example, “grass is green" is a proposition. We will let capital letters—typically P, Q, R etc.—stand for specific propositions as in “Let P be the proposition: grass is green.”

Definition 2 (Propositional Variable)**.** *A* ***propositional variable*** *is a variable used to represent a proposition.*

We will let lower case letters—typically p, q, r, etc.—stand for propositional variables. This is similar to the way that we use variables, like x, to stand for numbers in algebraic formulas like $x = 5x + 5$. However, unlike in algebra where, typically, our goal is to solve for x, here we will use propositional variables to assert things that are true no matter which proposition we let the propositional variable stand for.

Definition 3 (Connective)**.** *A* ***connective*** *takes in propositions and outputs new propositions.*

For example, the *and* connective (notated $\wedge$) takes propositions P and Q and forms the proposition P *and* Q (notated $P \wedge Q$). Likewise, connectives can also take in propositional variables—for instance the *and* of p and q is $p \wedge q$. We will say that a proposition that is output by a connective is **compound**, otherwise, the proposition is **atomic**. We will mainly deal with the connectives *and* ($\wedge$), *or* ($\vee$), *not* ($\neg$), *implies* ($\rightarrow$) and *if and only if* ($\leftrightarrow$). *implies* is also often written as *if-then* and *if and only if* is often written as *iff*.

Definition 4 (Propositional Formula)**.** *A* ***propositional formula*** *is a statement consisting of connectives and propositional variables.*

Example

$p \wedge q$ and $p \wedge q \vee \neg q$ are propositional formulas.

Definition 5 (Truth Table)**.** *A **truth table** shows the truth of a propositional formula as a function of its atomic propositions.*

For instance, the truth table of $p \wedge q$ shows if $p \wedge q$ is true or false for each of the possible truth values of p and q.

Example

The below gives the truth table corresponding to the above-mentioned connectives.

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \oplus q$	$p \to q$	$p \leftrightarrow q$
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

The connectives $\to$ and $\leftrightarrow$ go by several different names in English and you should be able to recognize all of them. If $p \to q$ is true then we say that p **implies** q, that p is **sufficient** for q, that q is **necessary** for p and that p **only if** q. If $p \leftrightarrow q$ is true then we say that p is **necessary and sufficient** for q and we will often use q as a **definition** of p.

Example

Let B be the proposition "Ellis goes to the beach" and S be the proposition "it is sunny." Then "Ellis goes to the beach only if it is sunny" translates to $B \to S$ (and not $S \to B$): being sunny is necessary for Ellis to go to the beach but it does not guarantee that he goes. On the other hand, "Ellis goes to the beach if it is sunny" translates to $S \to B$.

Just as in algebra where $\cdot$ is applied before $+$ (so $xy + xz$ means $(xy) + (xz)$), connectives have an **order of operations**: $\neg$ is applied first, then $\wedge$, then $\vee$, then $\to$ and finally $\leftrightarrow$. For example, $p \wedge q \vee \neg p \to q$ means $((p \wedge q) \vee (\neg p)) \to q$. When in doubt, use parentheses.

Definition 6 (Logical Equivalence)**.** *Two propositional formulas are **equivalent** if they always have the same truth value.*

In particular, two formulas are equivalent if no matter what propositions we substitute into the variables, the two propositions have the same truth value. We denote the equivalence of two formulas with $\equiv$.

The connectives $\wedge$, $\vee$ and $\leftrightarrow$ are **associative**, meaning

$$p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$$
$$p \vee (q \vee r) \equiv (p \vee q) \vee r$$
$$p \leftrightarrow (q \leftrightarrow r) \equiv (p \leftrightarrow q) \leftrightarrow r$$

and so we simply write $p \wedge q \wedge r$, $p \vee q \vee r$ and $p \leftrightarrow q \leftrightarrow r$ without parentheses. Note that $\to$ is *not* associative: $p \to (q \to r) \not\equiv (p \to q) \to r$.

Definition 7 (Disjunctive Normal Form (DNF))**.** *A **literal** is an atomic proposition or the negation of one. A **cube** is the "and" of literals. We say a formula is in **disjunctive normal form (DNF)** when it is the "or" of cubes.*

Example

The following is a formula in DNF.

$$(p \wedge q \wedge \neg r) \vee (p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge \neg q \wedge \neg r)$$

For any formula, there is an equivalent formula in DNF.

A formula in DNF only uses the connectives $\neg$, $\wedge$ and $\vee$. Furthermore, since $p \wedge q \equiv \neg(\neg p \vee \neg q)$, we can replace every $\wedge$ in a DNF formula with $\neg$s and $\vee$s. Putting these two facts together gives the following.

For any formula, there is an equivalent formula that uses only $\neg$ and $\vee$.

Example

$p \to q$ is equivalent to the DNF formula $(p \wedge q) \vee (\neg p \wedge q) \vee (\neg p \wedge \neg q)$ which is in turn equivalent to the formula $\neg(\neg p \vee \neg q) \vee \neg(\neg\neg p \vee \neg q) \vee \neg(\neg\neg p \vee \neg\neg q)$ which uses only $\neg$ and $\vee$.

Definition 8 (Satisfiable Formula)**.** *A propositional formula is **satisfiable** if there is at least one truth value assignment for which it is true.*

Example

$p \wedge (\neg p \vee \neg q)$ is satisfiable because it is true when p is true and q is false (which can be checked with a truth table).

Definition 9 (Tautology)**.** *A propositional formula is a **tautology** if it is true for all truth value assignments of its atoms.*

Example

$p \vee \neg p$ is a tautology because no matter what the truth value of p is, $p \vee \neg p$ is true (as could be checked with a truth table).

1.1.2 Logic Proofs

Proofs in logic give a way of breaking down complex logical inference into simple steps.

The basic step of a logic proof is a valid rule of inference

Definition 10 (Rule of Inference)**.** *A **rule of inference** takes in propositions of a specified form and outputs another proposition of a specified form.*

We notate a rule of inference as

$$\begin{array}{l} \text{input 1} \\ \text{input 2} \\ \ldots \\ \hline \therefore \text{output} \end{array}$$

Example

Modus ponens is a rule of inference which takes in two propositions of the form p and $p \to q$ and outputs a proposition of the form q. We denote such a rule with:

$$\begin{array}{l} p \\ \underline{p \to q} \\ \therefore q \end{array}$$

Definition 11 (Valid Rule of Inference)**.** *A **valid** rule of inference is one where whenever all of its input propositions are true, so is its output proposition.*

Example

Modus ponens is a valid rule of inference because if p and $p \to q$ are true, then q is also true.

Example

The inference rule

$$\begin{array}{l} q \\ \underline{p \to q} \\ \therefore p \end{array}$$

is not valid because if p is false and q is true then the inputs (q and $p \to q$) to the inference rule are true but the output is false (p).

Definition 12 (Logic Proof)**.** *A **proof** (in logic) of a conclusion from a set of premises is a sequence of propositions where each is either a premise or the output of a valid inference rule applied to earlier propositions and the last written proposition is the conclusion.*

Example

We can use the valid inference rules

$$\text{(R1)}\ \frac{p \quad p \to q}{\therefore q} \qquad \text{(R2)}\ \frac{p \quad q}{\therefore p \wedge q}$$

to prove the conclusion $p \wedge q$ from the premises p and $p \to q$ as follows.

(1)	$p \to q$	(premise)
(2)	p	(premise)
(3)	q	(R1 applied to (1), (2))
(4)	$p \wedge q$	(R2 applied to (2), (3))

A conclusion can be proven from a set of premises if and only if the inference rule from the premises to the conclusion is valid.

1.1.3 First Order Logic

The above concepts make up what is called propositional logic. If we add the concept of predicates and quantifiers to propositional logic, we get first order logic.

Definition 13 (Predicate)**.** *A **predicate** takes in one or more variables and outputs a proposition.*

Example

$x \geq y$ and "x is a fruit" are both predicates.

Definition 14 (Quantifier)**.** ***Quantifiers** take in a predicate and a domain and output a proposition.*

There are two quantifiers that we study: the universal quantifier (notated with $\forall$) and the existential quantifier (notated with $\exists$). The universal quantifier outputs the proposition stating that the predicate is true for all elements of the domain. The existential quantifier outputs the proposition stating that the predicate is true for some element of the domain. To notate this on domain d with predicate $p(x)$, we write $\forall x \in d\ p(x)$ and $\exists x \in d\ p(x)$. If the domain is clear, we drop "$\in d$".

When we write complex expressions with quantifiers, the **scope** of a quantifier $\forall x$ or $\exists x$ is the part of the expression where x refers to the x of $\forall$ or $\exists$. If the scope is not clear from the form of the expression, then we denote it with parenthesis as in $\forall x\ (<\textit{the scope of } x>)$. A variable is **free** if it is not in the scope of a quantifier and **bound** otherwise.

Example

In the expression $p(x) \wedge \forall y\ (p(y) \wedge q(y))$ the variable x in "$p(x)$" is free and both occurrences of "y" are bound in "$(p(y) \wedge q(y))$". Here, the scope of $\forall y$ is $p(y) \wedge q(y)$.

Definition 15 (Formula)**.** *A* ***(predicate) formula*** *consists of variables, connectives and quantifiers where all predicates' variables are bound.*

The idea of proofs, rules of inference and logical equivalence all carry over to first order logic. Some equivalences that are specific to first order logic are the following.

$$\forall \textbf{ Negation. } \neg\forall x\ p(x) \equiv \exists x\ \neg p(x)$$
$$\exists \textbf{ Negation. } \neg\exists x\ p(x) \equiv \forall x\ \neg p(x)$$
$$\forall \textbf{ Commutativity. } \forall x\ \forall y\ p(x,y) \equiv \forall y\ \forall x\ p(x,y)$$
$$\exists \textbf{ Commutativity. } \exists x\ \exists y\ p(x,y) \equiv \exists y\ \exists x\ p(x,y)$$

However, a $\forall$ and an $\exists$ *cannot* be swapped: $\exists x\ \forall y\ p(x,y) \not\equiv \forall y\ \exists x\ p(x,y)$.

Example

Let the domain be all people and let $P(x,y)$ be the predicate "x loves y." Then $\exists x\ \forall y\ P(x,y)$ says that somebody loves everybody whereas $\forall y\ \exists x\ P(x,y)$ says that everybody is loved by somebody. The first implies the second but not vice versa: it could be that everybody is loved by somebody even though no single person loves everybody.

1.2 Technique: Translating Between Logic and English

One of the key ideas we covered is that statements in English are ambiguous but logic is precise. As such, being able to translate to logic from English and vice versa are key skills.

Example

Goldbach's conjecture states that every even integer greater than 2 is the sum of two primes. Here, we translate this to first-order logic.

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 $n = p + q$".

We can then define some predicates. Let G be the predicate on natural numbers such that $G(n)$ holds just in case n is even and $n > 2$. 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:

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

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.)

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
     - e: Ellis, 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 Ellis. (<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 ×; 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.

[a] I.e., it is the only natural number with this property.

1.3 Technique: Writing Truth Tables

In order to draw truth tables for complex propositional formulas

1. Create a column for each of the atoms (p, q, etc.).
2. Create a column for each of the connectives, working "inside" to "outside."
3. Create / fill in a row for each possibility of the atoms.
4. Fill in the columns for each of the connectives.

Example

Suppose we want to write the truth table for $(p \vee q) \wedge \neg p$. Then, we do the following.

Step 1:

p	q

Step 2:

p	q	$\neg p$	$p \vee q$	$(p \vee q) \wedge \neg p$

Step 3:

p	q	$\neg p$	$p \vee q$	$(p \vee q) \wedge \neg p$
T	T			
T	F			
F	T			
F	F			

Step 4:

p	q	$\neg p$	$p \vee q$	$(p \vee q) \wedge \neg p$
T	T	F	T	F
T	F	F	T	F
F	T	T	T	T
F	F	T	F	F

1.4 Technique: Showing Logical Equivalence

In order to show that two logical formulas are equivalent, we can either write a truth table or do logic algebra.

1.4.1 By Truth Tables

To check logical equivalence with a truth table, we write the truth table of both expressions and check if they always have the same truth value for any assignment of truth values to the expressions atoms.

Note that writing truth tables to check logical equivalence only works for propositional logic (because we can only draw truth tables for formulas without quantifiers—at least not without making a row for every element of the domain).

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.

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

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

1.4.2 By Logic Algebra

To check logical equivalence using logic algebra, we start with one side of the equivalence and apply known equivalence to transform it into the right side of the equivalence.

Practice Problem(s)
Use logic algebra and (only) the equivalences

$$\begin{aligned}
\textbf{Double Negation.}\ & \neg\neg p \equiv p \\
\textbf{De Morgan's Law I.}\ & \neg(p \wedge q) \equiv \neg p \vee \neg q \\
\textbf{De Morgan's Law II.}\ & \neg(p \vee q) \equiv \neg p \wedge \neg q \\
\forall\ \textbf{Negation.}\ & \neg\forall x\ p(x) \equiv \exists x\ \neg p(x) \\
\exists\ \textbf{Negation.}\ & \neg\exists x\ p(x) \equiv \forall x\ \neg p(x) \\
\textbf{If Rewritten.}\ & p \to q \equiv \neg p \vee q \\
\textbf{Iff Rewritten.}\ & p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)
\end{aligned}$$

to show the logical equivalence

$$\neg\forall x \left(p(x) \wedge q(x)\right) \ \equiv\ \exists x \left(\neg p(x) \ \vee\ \neg q(x)\right)$$

1.5 Technique: Writing a Propositional Formula in DNF

Given a logical formula, we can find an equivalent formula in DNF by drawing its truth table and then taking the "or" of the cubes which "correspond" to the rows of the truth table where the formula is true.

Example
Suppose we have a mystery propositional formula with the following truth table.

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

Then the following is a formula in DNF which is equivalent to our mystery formula:

$$(p \wedge q \wedge \neg r) \vee (p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge \neg q \wedge \neg r)$$

Here, for example, $(p \wedge q \wedge \neg r)$ is the cube which corresponds to the second row of the truth table.

Practice Problem(s)
Write a formula in DNF that is equivalent to the proposition with the following truth table.

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

1.6 Technique: Checking the Validity of Rules of Inference

One can show that a rule of inference is valid by writing the truth table of the input and output of the inference rule, by showing the input is equivalent to the output or by direct reasoning.

1.6.1 By Truth Tables

To check if a rule of inference is valid by writing a truth table: write the truth table and check if whenever all of the input to the rule of inference is true, so too is the output.

Example
The following is a valid rule of inference:

$$\begin{array}{l} p \vee q \\ \neg p \\ \hline \therefore q \end{array}$$

Why? Consider the following truth table for $\neg p$ and $p \vee q$.

p	q	$p \vee q$	$\neg p$
T	T	T	F
T	F	T	F
F	T	T	T
F	F	F	T

We can see that the only row where all inputs to the inference rule ($p \vee q$ and $\neg p$) are true is the third row but in the third row the output (q) is true.

1.6.2 By Equivalence

If the input of a rule of inference is equivalent to its output then the rule is valid. This is because equivalent formulas always have the same truth value, so whenever the input is true the output is true (and, in fact, whenever the input is false the output is also false). When the rule has several inputs, we take the "and" of the inputs.

Example

The following is a valid rule of inference:

$$\frac{p \wedge q}{\therefore \neg(\neg p \vee \neg q)}$$

Why? By De Morgan's Law and Double Negation we have $\neg(\neg p \vee \neg q) \equiv \neg\neg p \wedge \neg\neg q \equiv p \wedge q$, so the input is equivalent to the output.

Note that this method only sometimes works: a rule can be valid even when its input is not equivalent to its output. For instance, modus ponens is valid but $p \wedge (p \to q) \not\equiv q$ (when p is false and q is true, q is true but $p \wedge (p \to q)$ is false). Equivalence requires truth to flow both ways while validity only requires it to flow from input to output.

1.6.3 By Reasoning Through it

Often, we can also see if something is valid or not by just informally reasoning through it.

Example

The following is a valid rule of inference:

$$\frac{\begin{array}{c} p \vee q \\ \neg p \end{array}}{\therefore q}$$

Why? If $p \vee q$ is true then one of p and q must be true. However, we know $\neg p$ so p must be false and so it follows that q must be true, meaning that the output of the inference rule is true.

1.7 Technique: Logic Proofs

You should be able to write logic proofs as described above.

Practice Problem(s)

Let the following symbols be defined as:

- S: the set of stars. (You can use this as the domain for quantifiers.)

- *Predicate symbols* represent predicates with variable placeholders that can be filled in with any term (Recall that once a variable is assigned, it represents a proposition):
  - $BL(x)$: "star x is blue"
  - $Y(x)$: "star x is young"
- *Constant symbols* are terms:
  - Sun is a constant symbol representing the specific star, the Sun.

Using the following valid inferences,

R1

$$\frac{\forall x\ p(x)}{\therefore p(c) \text{ for any } c \text{ in the domain}}$$

R2

$$\frac{p(c) \text{ for some } c \text{ in the domain}}{\therefore \exists x\ p(x)}$$

Prove that there exists a star that is not young given the following premises:

- $\neg BL(Sun)$
- $\forall s \in S,\ Y(s) \rightarrow BL(s)$

2 Math Foundations

2.1 Key Concept Review

2.1.1 Math Basics

We make use of the following classes of numbers.

Definition 16 (Natural Numbers)**.** *The* ***natural numbers*** *(notated* $\mathbb{N}$*) are* $1, 2, 3, \ldots$*.*

Definition 17 (Integers)**.** *The* ***integers*** *(notated* $\mathbb{Z}$*) are* $\ldots, -2, -1, 0, 1, 2, \ldots$*.*

Definition 18 (Rational Numbers)**.** *The* ***rational numbers*** *(notated* $\mathbb{Q}$*) are those that can be expressed as* x/y *where* x, y *are integers and* $y \neq 0$*; otherwise the number is* ***irrational****.*

Definition 19 (Real Numbers)**.** *The* ***real numbers*** *(notated* $\mathbb{R}$*) are all the other numbers on the number line.*

All of the above numbers exhibit **closure** under addition and multiplication. In particular, if you add or multiply any two numbers of the same class, you get another number which is still in that class. For example, multiplying 2 rationals together results in a rational number.

We further subdivide the integers as follows.

Definition 20 (Even Integers)**.** *Integer* x *is* ***even*** *if there is an integer* k *such that* $x = 2k$*.*

> **Example**
> 6 is even because it can be written as $2 \cdot 3$ and 3 is an integer.

Definition 21 (Odd Integers)**.** *Integer* x *is* ***odd*** *if there is an integer* k *such that* $x = 2k + 1$*.*

> **Example**
> 7 is odd because it can be written as $2 \cdot 3 + 1$ and 3 is an integer.

Any integer is either even or odd.

Definition 22 (Divides)**.** x ***divides*** y *if there is an integer* k *such that* $y = xk$*.*

Example

3 divides 12 because $12 = 3 \cdot 4$ and 4 is an integer.

Definition 23 (Prime)**.** *An integer x* ***is prime*** *if $x \geq 2$ and is only divided by x and 1; otherwise x is* ***composite****.*

Example

7 is prime because it is only divided by 1 and 7.

Definition 24 (Proof (in Math))**.** *A* ***proof*** *of a proposition in math is ultimately just a proof in logic; however the rules of inference are often implicit, the proof is written in English and all premises are not stated (but rather include all known proven facts in math).*

Henceforth, we'll use "proof" to refer to a proof in math.

Definition 25 (Propositions in Math)**.** *A* ***theorem*** *is a particularly interesting mathematical proposition that has been proven. A less interesting proposition is a* ***lemma*** *or* ***claim*** *or* ***remark*** *or* ***note*** *or* ***proposition****. A proposition thought to be true is a* ***conjecture*** *and a proposition that is easy to prove from a known proposition is a* ***corollary****.*

2.1.2 Set Theory Basics

Definition 26 (Sets)**.** *A* ***set*** *is an unordered collection of elements.*

We write the set consisting of elements $a_1, a_2, \ldots$ as $\{a_1, a_2, \ldots\}$. We use capital letters (like "A") to refer to sets. We denote that element a is in a set A with $a \in A$. Similarly, if a is not in set A then we write $a \notin A$.

Example

$A = \{1, 2, 3, 5\}$ is a set and $2 \in A$ but $6 \notin A$.

Similarly, each of the above classes of numbers are sets and $-1 \in \mathbb{Z}$ but $-1 \notin \mathbb{N}$.

We can concisely describe the set consisting of all x that satisfy the predicate $p(x)$ as $\{x : p(x)\}$. We also denote by $\{x \in A : p(x)\}$ the set consisting of all x in the set A which satisfy the predicate $p(x)$.

Example

We can concisely denote the integers as $\{x : x \text{ is an integer}\}$ and all even integers as $\{x \in \mathbb{Z} : x \text{ is even}\}$.

We can also build a set out of the outputs of a function. Given a predicate $p(x)$ and a function $f(x)$, we denote by $\{f(x) : p(x)\}$ the set of all outputs of $f(x)$ on those x which satisfy $p(x)$.

Example

$\{2k : k \in \mathbb{Z}\}$ is the set of all even integers and $\{k^2 : k \in \mathbb{N}\} = \{1, 4, 9, 16, \ldots\}$ is the set of all perfect squares.

Definition 27 (Subset)**.** *Set A is a **subset** of set B if every element of A is in B.*

We denote A is a subset of B with $A \subseteq B$.

Example

$\{1, 3, 5\} \subseteq \{1, 2, 3, 4, 5, 6\}$.

Definition 28 (Empty Set)**.** *The **empty set** is the set with no elements, denoted with $\emptyset$ or $\{\}$.*

Definition 29 (Set Cardinality)**.** *The **cardinality** (a.k.a. size) $|A|$ of a set A is the number of elements of A.*

Example

$|\{1, 3, 8\}| = 3$.

Definition 30 (Set Operations)**.** *A **set operation** takes in one or more sets and outputs a new set.*

We work with the following 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. If the intersection of A and B is the empty set, then we say that A and B are **disjoint**.
- 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 universe U.)

Example

Given sets $A = \{1, 2, 3, 4\}$ and $B = \{3, 4, 5, 6\}$ we have

- $A \cup B = \{1, 2, 3, 4, 5, 6\}$

- $A \cap B = \{3, 4\}$
- $A \setminus B = \{1, 2\}$
- $\bar{A}$ is all integers other than 1, 2, 3 and 4, assuming our universe is $\mathbb{Z}$.

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 followings sets:

   i. A

   ii. $(B \setminus C) \setminus D$

   iii. $(A \cup B) \cap (C \cap D)$

Definition 31 (Power Set)**.** *The **power set** of a set A, denoted $\mathcal{P}(A)$, is the set of all subsets of A.*

Example

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

The power set of set A has cardinality $2^{|A|}$.

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. $\mathcal{P}(\mathcal{P}(\varnothing))$
2. Prove that $|A| < |\mathcal{P}(A)|$ for any arbitrary finite set A.

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. $\{\text{Duncan}\} \subseteq B$

Definition 32 (Cardinality k Subsets)**.** *Given set A and integer k at least 0, we denote with $\binom{A}{k}$ the set containing **all subsets of A of cardinality** k.*

Example
Given $A = \{1, 2, 3\}$, we have $\binom{A}{2} = \{\{1, 2\}, \{2, 3\}, \{1, 3\}\}$.

Definition 33 (Sequences)**.** *A **sequence** is a collection of ordered elements.*

We denote the sequence of $a_1, a_2, \ldots$ as $(a_1, a_2, \ldots)$. We also refer to a sequence with n elements as an n-tuple or just tuple for short and when $n = 2$ as an ordered pair.

Example
$(1, 2)$ and $(2, 1)$ are both sequences but $(1, 2)$ is not the same sequence as $(2, 1)$ (since order matters for sequences).

Definition 34 (Set Product)**.** *The **set product** of two sets A and B is the set $\{(a, b) : a \in A \wedge b \in B\}$ of all ordered pairs (i.e. 2-element sequences).*

Example
Given $A = \{1, 2\}$ and $B = \{3, 4\}$ we have $A \times B = \{(1, 3), (1, 4), (2, 3), (2, 4)\}$.

Definition 35 (k-Way Set Product)**.** *The **k-way product** of sets $A_1, A_2, \ldots, A_k$ is the set $A_1 \times A_2 \times \ldots \times A_k = \{(a_1, a_2, \ldots, a_k) : a_1 \in A_1 \wedge a_2 \in A_2 \wedge \ldots \wedge a_k \in A_k\}$ of all k-tuples whose ith element is in A_i.*

When all of the sets are the same set A, we write the k-way product of A with itself as A^k.

Example
$\{1, 2\} \times \{3\} \times \{4, 5\} = \{(1, 3, 4), (1, 3, 5), (2, 3, 4), (2, 3, 5)\}$ and $\{0, 1\}^2 = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$.

Definition 36 (Bit Strings)**.** *The **n-bit bit strings** are the elements of $\{0, 1\}^n$.*

For short, we write an n-tuple of bits $(b_1, b_2, \ldots, b_n)$ as $b_1 b_2 \ldots b_n$.

Example
$\{0, 1\}^3 = \{000, 001, 010, 011, 100, 101, 110, 111\}$.

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, $|\mathcal{P}(A \times B)| = |\mathcal{P}(A) \times \mathcal{P}(B)|$.

Graphs can be formalized using set theory and then analyzed with proofs.

Definition 37 (Graphs)**.** *A **graph** consists of two sets V and E where E satisfies $E \subseteq \binom{V}{2}$.*

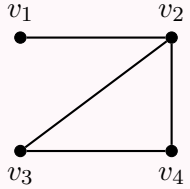
We refer to V as the vertices of the graph and E as the edges. If $\{u, v\} \in E$ then we say that u and v are **adjacent**.

Definition 38 (Cliques)**.** *A **clique** is a subset of the vertices which are all adjacent to one another.*

Definition 39 (Independent Set)**.** *An **independent set** is a subset of the vertices, no two of which are adjacent.*

Example

The graph with $V = \{v_1, v_2, v_3, v_4\}$ and $E = \{\{v_1, v_2\}, \{v_2, v_3\}, \{v_3, v_4\}, \{v_4, v_2\}\}$ is drawn below.



Here $\{v_2, v_3, v_4\}$ is a clique of 3 vertices and $\{v_1, v_3\}$ is an independent set of 2 vertices.

2.1.3 Relations and Functions

Definition 40 (Relations)**.** *A **relation** R with domain X and codomain Y is a subset of $X \times Y$. We say that a relation R is on set A if both its domain and codomain are A.*

Example

Given domain $\mathbb{Z}$ and codomain $\mathbb{Z}$, we have that $R = \{(1,2),(2,4),(3,9)\}$ is a relation.

Definition 41 (Partial Functions)**.** *A relation f with domain A and codomain B is a **partial function** if for all $a \in A$ and any $b, b' \in B$, if $(a,b) \in f$ and $(a,b') \in f$ then $b = b'$.*

Suppose we draw the domain A on the left and codomain B on the right and an arrow from the $a \in A$ to $b \in B$ if $(a,b) \in f$. Then, informally, a partial function is one with at most one arrow out of each element of A.

Definition 42 (Functions)**.** *A relation f is a **(total) function** with domain A and codomain B if it is a partial function and for every $a \in A$ there is some $b \in B$ such that $(a,b) \in f$.*

Informally, a function is one with exactly one arrow out of each element of A.

We denote that f is a function with domain A and codomain B with $f : A \to B$.

Definition 43 (Image)**.** *The **image** of $f : A \to B$ on $A' \subseteq A$ is $\{b \in B : \exists a \in A' \;\; f(a) = b\}$, that is, all elements of B to which f maps something in A'.*

The **range** of f is its image on A; that is, all elements that are mapped to by f.

Definition 44 (Pre-Image)**.** *The **pre-image** of $f : A \to B$ on $B' \subseteq B$ is $\{a \in A : \exists b \in B' \;\; f(a) = b\}$, that is, all elements of A from which f maps something to in B'.*

Definition 45 (Injective Functions)**.** *A function $f : A \to B$ is **injective** if for any $a, a' \in A$ and $b \in B$, if $f(a) = b$ and $f(a') = b$ then $a = a'$.*

Informally, a function is injective if it has at most one arrow into each element of B, as below.

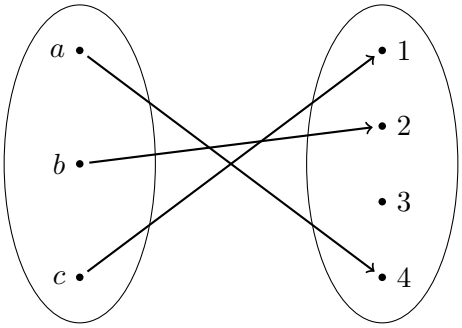


Figure 1: Injective Function

Definition 46 (Surjective Functions)**.** *A function $f : A \to B$ is **surjective** if, for every $b \in B$, there is some $a \in A$ such that $f(a) = b$.*

Informally, a function is surjective if it has at least one arrow into each element of B, as below.

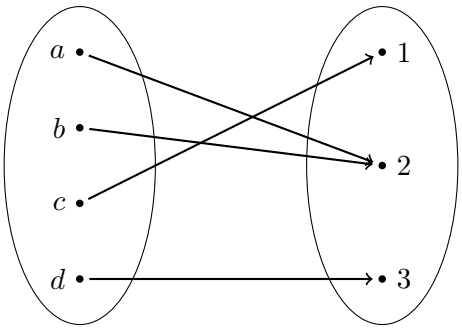


Figure 2: Surjective Function

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. [a]

   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.

[a] *HW3 Problem 1* CSCI0220 2022 Spring

Definition 47 (Bijective Functions)**.** *A function f is **bijective** if it is both injective and surjective. Such a function is also called a **bijection**.*

Informally, a function is bijective if it has exactly one arrow into each element of B, as below.

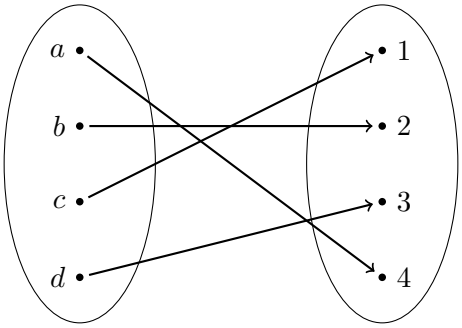


Figure 3: Bijective Function

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) $f : \mathbb{Z} \to \mathbb{Z}$ where $f(x) = x^2$

   b) $f : \mathbb{Z}^+ \to \mathbb{Z}^+$ where $f(x) = x^2$. $\mathbb{Z}^+$ denotes the positive integers.

   c) $f : \mathbb{Z} \to \mathbb{Z}$ where $f(x) = \sqrt{x}$.

   d) $f : A \to B$, 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.

   e) $f : A \to B$, 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.

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

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

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

   i) $f : \mathcal{P}(\{1, 2, 4\}) \to \{0, 1, 2, 3\}$ 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 $f : B \to C$ and $g : A \to B$ be functions. Let $h : A \to C$ 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.

2.1.4 Equivalence Relations

Definition 48 (Reflexive Relations)**.** *Relation R on A is **reflexive** if for every $a \in A$ we have $(a, a) \in R$.*

In other words, a relation is reflexive if *every element* in the set A is related to itself in R.

Definition 49 (Symmetric Relations)**.** *A relation R on A is **symmetric** if for all $a, b \in A$ we have if $(a, b) \in R$, then $(b, a) \in R$.*

Definition 50 (Transitive Relations)**.** *A relation R on A is **transitive** if for all $a, b, c \in A$ we have 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.

Example

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).

Example

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.

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.

Definition 51 (Equivalence Relations)**.** *A relation R on A is an **equivalence relation** if it is reflexive, symmetric and transitive.*

To prove that a relation is an equivalence relation, we prove each of the three properties, each of which is a $\forall$ statement (and so we fix arbitrary elements) whose body is an if-then (and so we suppose the "if" and show the "then").

Example

Claim: $R = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x - y \text{ is even}\}$ is an equivalence relation on $\mathbb{Z}$.

Proof. We show that R is reflexive, symmetric and transitive.

Reflexive: Let x be an arbitrary integer. Then $x - x = 0 = 2 \cdot 0$ is even, so $(x, x) \in R$.

Symmetric: Let x and y be arbitrary integers and suppose $(x, y) \in R$, so $x - y$ is even. Then $x - y = 2k$ for some integer k. But then $y - x = 2(-k)$ where $-k$ is an integer, so $y - x$ is even and $(y, x) \in R$.

Transitive: Let x, y and z be arbitrary integers and suppose $(x, y) \in R$ and $(y, z) \in R$, so $x - y$ and $y - z$ are even. Then $x - y = 2k$ and $y - z = 2k'$ for some integers k and k'. But then $x - z = (x - y) + (y - z) = 2k + 2k' = 2(k + k')$ where $k + k'$ is an integer, so $x - z$ is even and $(x, z) \in R$.

Since R is reflexive, symmetric and transitive, it is an equivalence relation. □

Definition 52 (Equivalence Class)**.** *Let R be an equivalence relation on A. Then the* ***equivalence class*** *of $a \in A$ is defined as*

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

In other words, the equivalence class of a is all things that a is related to.

Example

If $R = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x = y\}$ then $[5]_R = \{5\}$. If $R = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : |x| = |y|\}$ then $[5]_R = \{-5, 5\}$. If $R = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x - y \text{ is even}\}$ then $[5]_R = \{x \in \mathbb{Z} : x \text{ is odd}\}$.

The following lemma says that any element of an equivalence class can serve as its "representative."

Lemma. Let R be an equivalence relation on A and let $a, b \in A$. If $b \in [a]_R$ then $[a]_R = [b]_R$.

An equivalence relation splits a set into its equivalence classes. To make this precise, we need the following definition.

Definition 53 (Partition)**.** *A* ***partition*** *of a set A is a set of disjoint subsets $\{A_1, A_2, \ldots\}$ of A such that $A_1 \cup A_2 \cup \ldots = A$.*

Example

$\{\{1,3,5\},\{2,8\},\{4\},\{6\},\{7\},\{9\}\}$ is a partition of $\{1,2,3,4,5,6,7,8,9\}$.

Theorem. Let R be an equivalence relation on A. Then the distinct equivalence classes $\{[a]_R : a \in A\}$ are a partition of A.

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.

2.2 Technique: Proving $\forall$

In order to prove a proposition of the form "$\forall x \in d \;\; p(x)$" we fix an arbitrary element of the domain d and then show that $p(x)$ holds for this arbitrary element.

Theorem. For all even integers n, we have n^2 is even.

Proof. Let n be an arbitrary even integer. Since n is even, we know that

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

But then

$$n^2 = (2k)^2 = 4k^2 = 2 \cdot 2k^2.$$

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

$$n^2 = 2k'$$

where k' is an integer. Thus n^2 is even. Since n was arbitrary, n^2 is even for all even integers n. □

2.3 Technique: Proving If

A proposition of the form "if p then q" can either be proven "directly" or by contrapositive.

2.3.1 Directly Proving If

In order to prove "if p then q", we assume that p is true, and then show that q is true.

Theorem. For all integers x, y, if x and y are odd, then $x + y$ is even.

Proof. Let x and y be arbitrary integers. Suppose x and y are odd. Then

$$x = 2k + 1 \quad \text{and} \quad y = 2k' + 1$$

for some integers k, k'. So

$$x + y = 2k + 2k' + 2 = 2(k + k' + 1).$$

Let $k'' = k + k' + 1$. Then k'' is an integer since it is the sum of integers. Thus

$$x + y = 2k'',$$

and therefore $x + y$ is even. Since x and y were arbitrary, this holds for all integers x, y. □

Practice Problem(s)
Claim: For all integers n, if n is odd, then n^2 is odd.

Proof. 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.

□

2.3.2 Proving If 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.

Theorem. For all integers n, if n^2 is even then n is even.

Proof. 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. □

2.4 Technique: Proving Iff

In order to prove a proposition of the form "p iff q" we show if p then q and also if q then p.

2.5 Technique: Proving $\exists$

In order to prove a proposition of the form "$\exists x \in d \;\; p(x)$", we provide an example of a c in d for which $p(c)$ is true.

However, the name we give to such a c depends on the form of $\exists x \in d \;\; p(x)$. If we are showing something directly written as $\exists x \in d \;\; p(x)$, then we refer to c as a **witness**. If we are showing $\neg \forall x \in d \; p(x)$ then this is equivalent to showing $\exists x \in d \;\; \neg p(x)$ which is the same as $\exists x \in d \;\; q(x)$ for $q(x) = \neg p(x)$. However, in this case we refer to c as a **counterexample**.

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: $\forall x \in \mathbb{Z}, -1 \leq x \leq 1 \to x^2 = x$.
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 $(A_1, A_2) \in R \wedge (A_2, A_3) \in R \not\to (A_1, A_3) \in R$.

2.6 Technique: Proving Or

In order to prove a proposition of the form "$p \vee q$" we assume p is not true and show q.

Theorem. For all integers n, we have that n or $n(n+1)$ is even.

Proof. Let n be an arbitrary integer. To show n or $n(n+1)$ is even, suppose n is not even. Then n is odd, so

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

Then

$$n(n+1) = (2k+1)(2k+2) = 4k^2 + 6k + 2 = 2(2k^2 + 3k + 1).$$

Let $k' = 2k^2 + 3k + 1$. Then k' is an integer (by closure of integers under addition and multiplication). Thus

$$n(n+1) = 2k',$$

and so $n(n+1)$ is even. Therefore, n is even or $n(n+1)$ is even. Since n was arbitrary, this holds for all integers n. □

2.7 Technique: Using Or in a Proof (Proof by Cases)

If we know a proposition of the form "$p \vee q$" and we would like to show a proposition r then we show if p then r and also if q then r. This is called **proof by cases**.

2.8 Technique: Proof by Contradiction

To prove any proposition p, we assume that p is not true and then show $q \wedge \neg q$ for some proposition q. This is called a **proof by contradiction** because $q \wedge \neg q$ is called a contradiction.

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 $A = \{a_1, ..., a_n\}$ with cardinality n. Consider $f : \mathcal{P}(A) \to \{0, 1\}^n$ where $f(X) = s_1 s_2 ... s_n$ 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 $X_1 = X_2$.

2.9 Technique: Induction

To prove a proposition of the form $\forall n \in \mathbb{N}\ p(n)$, we can use induction. To show $\forall n \in \mathbb{N}\ p(n)$ by induction we use the following template.

1. State that the proof uses induction on n

2. State the predicate $p(n)$

3. Prove the **base case**: show $p(1)$

4. Prove the **induction step**: show for arbitrary $n \in \mathbb{N}$ if $p(n)$ then $p(n + 1)$

5. Conclude "by induction" that $p(n)$ holds for all $n \in \mathbb{N}$

In the induction step, we are showing if $p(n)$ then $p(n + 1)$. The way we show this, as described above, is to assume $p(n)$ and then show $p(n + 1)$. The assumption of $p(n)$ is often referred to as the **inductive hypothesis**.

Example

For example, say we are trying to prove that $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ is true for all $n \in \mathbb{N}$.

1. State that the proof uses induction on n.

   The proof uses induction on n.

2. State the predicate $P(n)$.

   Let $P(n)$ be the predicate that $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

3. Show that the base case is true.

   We will first show $P(1)$ is true. $\sum_{i=1}^{1} i = 1$ and $\frac{1(1+1)}{2} = 1$ so they are equal as needed.

4. Show the induction step. In particular, assume the inductive hypothesis is true for

some arbitrary natural number and then show $P(n+1)$.

Assume $P(k)$ is true for some arbitrary natural number k.

5. Show that $P(k+1)$ is true given the inductive hypothesis.

   We will now show that the sum of all integers from 1 to $k+1$ equals $\frac{(k+1)(k+2)}{2}$.

   We know that the sum of all integers from 1 to $k+1$ equals the sum of all integers from 1 to k, plus $(k+1)$ itself.

   By our inductive hypothesis, the sum of all integers from 1 to k equals $\frac{k(k+1)}{2}$.

   Therefore,

$$\begin{aligned} 1+2+\cdots+k+(k+1) &= (1+2+\cdots+k)+(k+1) \\ &= \frac{k(k+1)}{2}+(k+1) \\ &= \frac{k(k+1)+2(k+1)}{2} \\ &= \frac{(k+1)(k+2)}{2}. \end{aligned}$$

   This completes the inductive step, as needed. □

6. Conclude the proof.

   Therefore, as $P(1)$ is true and $P(k)$ implies $P(k+1)$ for all $k \in \mathbb{N}$, $P(n)$ is true for all natural numbers n.

Practice Problem(s)

1. Show that $6 \mid (n^3 - n)$ for all $n \in \mathbb{N}$.

2. Recall that the Fibonacci numbers are defined by $f_0 = 0, f_1 = f_2 = 1$ and the recursive relation $f_{n+1} = f_n + f_{n-1}$ for all $n \geq 1$. Challenging exercise:

   Show that f_n and f_{n+1} are 'relatively prime' for all $n \geq 1$. That is, they share no factor in common other than the number 1.

3. Use induction to show that $12^n + 2(5^{n-1})$ is divisible by 7 for all $n \geq 1$.

More generally, our induction doesn't have to start from 1 but can start from any $n_0 \geq 1$. In particular, induction still works if our goal is to show $\forall n \geq n_0 \;\; p(n)$ where here this quantification is over all natural numbers at least n_0.

2.9.1 Strong Induction

Strong induction strengthens induction in the sense that it makes it easier to prove $p(n+1)$. In particular, strong induction is the same as regular induction but we assume a stronger inductive hypothesis of $p(k)$ for all $k \leq n$ when we are showing $p(n+1)$. Here, this quantification is over the domain of all natural numbers between n_0 and n.

Why would we need to do that? Sometimes, you can't just rely on the fact that $P(n)$ is true. Maybe you also need $P(n-1)$ to be true, or perhaps also $P(n-2)$, or even $P(n/2)$. While writing out your inductive step, if you realize that $P(n)$ isn't enough to prove $P(n+1)$, odds are, you need strong induction.

Practice Problem(s)

1. Define the sequence S as follows: $S_1 = 1$, $S_2 = 3$, $S_n = S_{n-1} * S_{n-2}$ for integers $n \geq 3$. Prove that S_n is odd for all positive integers n.

2. Prove that every positive integer greater than one can be factored as a product of primes, using strong induction.

2.10 Technique: Proving Sets are Equal

In order to prove that 2 sets are equal we can either use the set element method or set algebra.

2.10.1 By the Set Element Method

In order to prove that two sets A and B are equal by the set element method, we show $A \subseteq B$ and $B \subseteq A$. To show $A \subseteq B$, we consider an arbitrary $a \in A$ and show that it is also in B. To show $B \subseteq A$, we consider an arbitrary $b \in B$ and show that it is also in A.

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 $x \in A \cap (A \cup B)$ 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) $A \cap (B \setminus C) = (A \setminus B) \cap (A \setminus C)$

2.10.2 By Set Algebra

In order to show that 2 sets are equal by set algebra, we apply known equalities between sets to convert one side of the equation to the other. This is very similar to showing logical equivalence by logic algebra.

Example

We can show $(A \cap B) \cup (A \setminus B) = A \cap (B \cup (A \setminus B))$ using the set equalities here as follows.

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. $(A \setminus B) \setminus (B \setminus C) = A \setminus B$.