MAT 2534 Discrete Math

Joe Wells
Virginia Tech

Spring 2023
Last Updated: March 31, 2023

Contents

2 The Logic of Compound Statements

2.1 Logical Form and Logical Equivalence

Definition 2.1.1

A **statement** (or a **proposition**) is a sentence which is either true or false, but not both.

Example 2.1.2

- “$1 + 2 = 3$” is a true statement.
- “$1 + 2 = 4$” is a false statement.
- “$x + 2 = 5$” is neither true nor false since x is unspecified. Usually when we are solving for x, we are trying to find an x-value that makes the statement true.

To make life simpler when breaking down compound statements, we introduce some logical notation:

symbol	**English translation**
$\vee$	“or”
$\wedge$	“and”
$\neg$ or $\sim$	“not”

Remark. “not” should be interpreted generally as negating a statement, which is more commonly how one would use it in English.

The order of operations for these symbols is simply reading them left-to-right, and one can include parentheses to override the order (just like in the usual “PEDMAS” or whatever permutation of those letters you had learned previously).

Example 2.1.3

Let p and q be the following statements.:

$$p : \text{Trey drinks water.}$$
$$q : \text{Sandy eats cookies.}$$

Interpret $p \vee q$, $p \wedge q$, $\neg p \vee q$ in plain English.

- $p \vee q$ means “Trey drinks water or Sandy eats cookies.”
- $p \wedge q$ means “Trey drinks water and Sandy eats cookies.”
- $\neg p \vee q$ means “Trey does not drink water or Sandy eats cookies.”

Let’s analyze the logical form of some common expressions.

“Neither a nor b”	means	not a and not b.
“a but not b”	means	a and not b
“$a \geq 2$”	means	$a > 2$ or $a = 2$
“$1 \leq b < 5$”	means	$1 \leq b$ and $b < 5$.

2.1.1 Truth Values

When considering a sentence comprised of several component statements, we want to know if the entire compound sentence is actually a statement (i.e. has a well-defined truth value). In order to do this, we'll need to analyze how the logical symbols (i.e. logical connectives) relate to the validity of the compound statement.

Example 2.1.4

Let x be a fixed real number and consider the sentence $2 < x < 5$, which we know is "$x > 2$ and $x < 5$". Fix a couple of different x-values and record the truthfulness of the three statements $x > 2$, $x < 5$, and $2 < x < 5$ in a *truth table.*

x-value	$x > 2$	$x < 5$	$2 < x < 5$
-1	F	T	F
3	T	T	T
7	T	F	F

The reasonable interpretation is that $p \wedge q$ is only true if *both* p and q are true statements.

Definition: Conjunction

If p and q are both statements, then the **conjunction** of p and q is the statement $p \wedge q$. The truth table for conjunctions is below.

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Example 2.1.5

Let x be a fixed real number and consider the sentence $x \leq 2$, which we know is "$x < 2$" or "x=2". Let's fix a couple of different x-values and record the truthfulness of $x < 2$, $x = 2$, and $x \leq 2$ in a *truth table*:

x-value	$x < 2$	$x = 2$	$x \leq 2$
-1	T	F	T
2	F	T	T
7	F	F	F

The reasonable interpretation of the logical connective $\vee$ is that $p \vee q$ is true precisely when *at least one* of p and q is true.

Definition: Disjunction

If p and q are both statements, then the **disjunction** of p and q is the statement $p \vee q$. The truth table for conjunctions is below.

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

Remark. Common English tends to use an "exclusive or." At a restaurant, when asked "Soup or salad?" we implicitly understand it to mean that you can have either soup or salad, but not both. In logic, disjunction represents an "inclusive or", which would allow for "soup, salad, or both" as valid answers. While this is a bit of a conventional choice, by comparing the final column of the conjunctive and disjunctive truth tables, we see that the inclusivity keeps them similar. Sometimes the symbol $\oplus$ will be used to denote an exclusive or (although we will not use that in these notes).

Definition: Negation

If p is any statement, then the **negation** of p is the statement $\neg p$. The truth table for negation is below.

p	$\neg p$
T	F
F	T

Now that we know about the basic logical connectives, let's fill in their truth tables.

Example 2.1.6: Exclusive Or

Let p and q be statements. Then "exclusive or" says "p or q, but not both". In symbols, this is written

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

Fill out a truth table for this compound statement above.

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

This truth table agrees with what we expect - the compound statement is only true precisely when one of the statements (and not both) is true.

Exercise 2.1.7: 3-variable truth table

Complete the following truth table for the statement: $p \wedge \neg(q \vee r)$.

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

Definition

Two statements P and Q (involving all of the same variables) are called **logically equivalent** if and only if they have the same truth values. Symbolically we write $P \equiv Q$.

Example 2.1.8: Commutative "and"

Let p and q be logical statements. Use a truth table to verify that $p \wedge q$ and $q \wedge p$ are logically equivalent.

p	q	$p \wedge q$	$q \wedge p$
T	T	T	T
T	F	F	F
F	T	F	F
F	F	F	F

Exercise 2.1.9: double negation

Show that p and $\neg(\neg p)$ are logically equivalent.

Example 2.1.10: Negation is Not Distributive

Show that $\neg(p \vee q) \not\equiv (\neg p) \vee (\neg q)$.

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

Noting that the truth values tables for conjunctions and disjunctions have opposite truth values, it seems that one may be the negation of the other. Indeed, this is the case.

Proposition 2.1.11: DeMorgan's Laws

Let p and q be statements. Then we have the following logical equivalences.

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

Exercise 2.1.12

Verify the above using truth tables.

Definition: Tautology and Contradiction

A **tautology** is a statement (call it $\mathbf{t}$) that is always true and a **contradiction** is a statement (call it $\mathbf{c}$) that is always false.

Example 2.1.13

Let p be a statement. Show that $p \vee \neg p$ is a tautology and $p \wedge \neg p$ is a contradiction.

Using a truth table, we have

p	$\neg p$	$p \vee \neg p$	$p \wedge \neg p$
T	F	T	F
F	T	T	F

2.1.2 Table of Logical Equivalences

Theorem 2.1.14

Let p, q, and r be statements, let $\mathbf{t}$ be a tautology, and let $\mathbf{c}$ be a contradiction. We then have the following table of equivalences:

Commutative Laws	$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$
Associative Laws	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	$(p \vee q) \vee r \equiv p \vee (q \vee r)$
Distributive Laws	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
Identity Laws	$p \wedge \mathbf{t} \ \equiv p$	$p \vee \mathbf{c} \equiv p$
Negation Laws	$p \vee \neg p \equiv \mathbf{t}$	$p \wedge \neg p \equiv \mathbf{c}$
Double Negative Laws	$\neg(\neg p) \equiv p$	
Idempotent Laws	$p \wedge p \equiv p$	$p \vee p \equiv p$
Universal Bound Laws	$p \vee \mathbf{t} \equiv \mathbf{t}$	$p \wedge \mathbf{c} \equiv \mathbf{c}$
De Morgan's Laws	$\neg(p \wedge q) \equiv \neg p \vee \neg q$	$\neg(p \vee q) \equiv \neg p \wedge \neg q$
Absorption Laws	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
Negation of $\mathbf{t}$ and $\mathbf{c}$	$\neg\mathbf{t} \equiv \mathbf{c}$	$\neg\mathbf{c} \equiv \mathbf{t}$

2.2 Conditional Statements

Consider the following promise made by your instructor to his broccoli-averse child.

If you eat your dinner, then I will give you cookies for dessert.

If the child eats dinner and your instructor gives the child cookies for dessert, then the promise is upheld.
If the child eats dinner and your instructor does not gives the child cookies for dessert, then the promise is not upheld.
If the child does not eat dinner, then cookies or not, it would be unfair to claim that the instructor did not uphold the promise.

Definition: If p then q

If p, q are statements, then "if p, then q" is called the **conditional of q by p** and is denoted $p \Rightarrow q$. p is called the **hypothesis** and q is called the **conclusion**. The truth table for the conditional is below.

p	q	$p \Rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

When the hypothesis is false, the conditional statement is called **vacuously true**.

Remark. One could also write $q \Leftarrow p$, but since English is read left-to-right, we will typically avoid using the left-pointing arrow.

Since $p \to q$ is only false when p is true and q is false, then the following observation is immediate.

Exercise 2.2.1

Let p, q be statements. Use a truth table to show that $(p \Rightarrow q) \equiv (\neg p \vee q)$.

It then follows from DeMorgan's Laws that

Proposition 2.2.2: Negation of a conditional statement

If p, q are statements, then $\neg(p \Rightarrow q) \equiv (p \wedge \neg q)$.

2.2.1 Related Conditionals

When it comes to order of operations, $\Rightarrow$ is performed last. In other words, everything to the left of $\Rightarrow$ implies everything to the right of $\Rightarrow$.

Example 2.2.3: Division Into Cases

Let p, q, r be statements. Show that $(p \vee q) \Rightarrow r$ is logically equivalent to $(p \Rightarrow r) \wedge (q \Rightarrow r)$.

p	q	r	$p \vee q$	$(p \vee q) \Rightarrow r$	$p \Rightarrow r$	$q \Rightarrow r$	$(p \Rightarrow r) \wedge (q \Rightarrow r)$
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	F
T	F	T	T	T	T	T	T
T	F	F	T	F	F	T	F
F	T	T	T	T	T	T	T
F	T	F	T	F	T	F	F
F	F	T	F	T	T	T	T
F	F	F	F	T	T	T	T

Definition: Converse, Inverse, Contrapositive

Given statements p, q and the conditional statement, $p \Rightarrow q$, there are three closely-related conditionals:

- The **converse** is $p \Leftarrow q$.
- The **inverse** is $\neg p \Rightarrow \neg q$.
- The **contrapositive** is $\neg p \Leftarrow \neg q$.

Example 2.2.4

Consider the following conditional statement:

If my car is in the repair shop, then I cannot get to class.

Write the converse, inverse, and contrapositive statements.

- [Converse] If I cannot get to class, then my car is in the repair shop.
- [Inverse] If my car is not in the repair shop, then I can get to class.
- [Contrapositive] If I can get to class, then my car is not in the repair shop.

Notice that some of these sound like they could be logically equivalent to one another. The contrapositive, for example, may be logically equivalent to the original statement. The converse, however, doesn't seem like it should be - there may be other reasons that one cannot attend class that are independent of the car needing repairs.

Proposition 2.2.5: Conditional Equivalences

Let S be the conditional statement $p \Rightarrow q$.

1. S is logically equivalent to the contrapositive of S.
2. The converse of S is logically equivalent to the inverse of S.

Proof. We only prove the first statement and leave the second as an exercise.

$$\begin{aligned} p \Rightarrow q &= \neg p \vee q && \text{(Exercise 2.2.1)} \\ &= \neg p \vee \neg(\neg q) && \text{(Double Negative Law)} \\ &= \neg(\neg q) \vee \neg p && \text{(Commutative Law)} \\ &= (\neg) q \Rightarrow p && \text{(Exercise 2.2.1)} \end{aligned}$$

□

2.2.2 Englishy Phrases

One may use the phrase that p happens "only if" q happens. In other words, if q doesn't occur, then p doesn't occur. This is now phrased like the contrapositive, so it must be equivalent to $p \Rightarrow q$. We record this and some other typical phrases below

p implies q	means	"$p \Rightarrow q$"
p only if q	means	"$p \Rightarrow q$"
p if q	means	"$p \Leftarrow q$"
p is a sufficient condition for q	means	"$p \Rightarrow q$"
p is a necessary condition for p	means	"$p \Leftarrow q$"

2.2.3 Biconditional Statements

Definition: Biconditional

If p, q are logical statements, then the **biconditional of** p **and** q, denoted $p \Leftrightarrow q$, is true when p and q have the same truth values, and false when p and q have opposite truth values.

p	q	$p \Leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Example 2.2.6

Show that that $(p \Leftrightarrow q) \equiv ((p \Rightarrow q) \wedge (p \Leftarrow q))$.

p	q	$p \Leftrightarrow q$	$p \Rightarrow q$	$p \Leftarrow q$	$(p \Rightarrow q) \wedge (p \Leftarrow q)$
T	T	T	T	T	T
T	F	F	F	T	F
F	T	F	T	F	F
F	F	T	T	T	T

Because of this connection, we often use the following English phrases to mean a biconditional

"p if and only if q."
"p iff q."
"p is necessary and sufficient for q."

Exercise 2.2.7

Let p, q be statements. Find the negation of $p \Leftrightarrow q$.

2.3 Valid and Invalid Arguments

Definition: argument, validity

An **argument** is a sequence of statements. All statements in an argument, except for the final one are called **premises**. The final statement is called the **conclusion**. The symbol $\therefore$ is read "therefore" and is normally placed before the conclusion. An argument is said to be **valid** when it satisfies the following criterion: if the premises are all true, then the conclusion is also true.

Example 2.3.1

Determine whether the following argument is valid.

If we meet death, then we say "not today."
The phrase "not today" was not spoken.
Therefore, we did not meet death.

The argument above can be simplified with symbols and variables.

$$\begin{array}{rl} & p \Rightarrow q \\ & \neg q \\ \therefore & \neg p \end{array}$$

and so we set up a truth table.

		Premise 1	Premise 2	Conclusion
p	q	$p \Rightarrow q$	$\neg q$	$\neg p$
T	T	T	F	F
T	F	F	T	F
F	T	T	F	T
F	F	T	T	T

There is only one row in the truth table where all premises are true, and that row also has a true conclusion, so it must be valid.

The above example highlights that we only need to fill out the truth tables along the **critical rows**, which are the rows where all premises are true. This simplifies things when checking validity in more complicated arguments.

Example 2.3.2: Division of Cases

Determine the validity of the following argument:

$$\begin{array}{rl} & p \vee q \\ & p \Rightarrow r \\ & q \Rightarrow r \\ \therefore & r \end{array}$$

			Premise 1	Premise 2	Premise 3	Conclusion
p	q	r	$p \vee q$	$p \Rightarrow r$	$q \Rightarrow r$	r
T	T	T	T	T	T	T
T	T	F	T	F		
T	F	T	T	T	T	T
T	F	F	T	F		
F	T	T	T	T	T	T
F	T	F	T	T	F	
F	F	T	F			
F	F	F	F			

Exercise 2.3.3

Determine the validity of the following argument:

$$\begin{array}{rl} & p \wedge q \Rightarrow \neg r \\ & p \vee \neg q \\ & \neg q \Rightarrow p \\ \therefore & \neg r \end{array}$$

					Premise 1		Premise 2	Premise 3	Conclusion
p	q	r	$p \wedge q$	$\neg r$	$p \wedge q \Rightarrow \neg r$	$\neg q$	$p \vee \neg q$	$\neg q \Rightarrow p$	$\neg r$
T	T	T							
T	T	F							
T	F	T							
T	F	F							
F	T	T							
F	T	F							
F	F	T							
F	F	F							

2.3.1 Rules of Inference

Definition: rule of inference

A **rule of inference** is a form of argument that is valid.

Remark. Example **??** (Division of Cases) is a rule of inference.

The two most common rules of inference are

Definition: Modus Ponens, Modus Tollens

Modus ponens is an argument of the form

$$\begin{array}{rl} & p \Rightarrow q \\ & p \\ \therefore & q \end{array}$$

and **modus tollens** is an argument of the form

$$\begin{array}{ll} & p \Rightarrow q \\ & \neg q \\ \therefore & \neg p \end{array}$$

Remark. Modus ponens is Latin for "method of affirming" and *modus tollens* is Latin for "method of denying." Notice that *modus tollens* really uses the contrapositive $\neg q \Rightarrow \neg p$.

Exercise 2.3.4

Use a truth table to show that both modus ponens and modus tollens are valid argument forms.

Example 2.3.5: Recognizing Modus Ponens and Modus Tollens

Use *modus ponens* or *modus tollens* to provide the correct logical conclusion to the following arguments.

a.

If the Golden Globes are fair, then Anya Taylor-Joy will win the award for Best Actress in a Musical or Comedy.
Anya Taylor-Joy did not win the award.
Therefore ____________

b.

If you see White Walkers, then Winter is coming.
You see White Walkers.
Therefore ____________

a. The Golden Globes are not fair. *(modus tollens)*

b. Winter is coming. *(modus ponens)*

Example 2.3.6: Rule of Inference: Elimination

The following argument forms are valid (and checking this is an exercise for the reader):

$$\boxed{\begin{array}{ll} & p \vee q \\ & \neg p \\ \therefore & q \end{array}} \qquad \boxed{\begin{array}{ll} & p \vee q \\ & \neg p \\ \therefore & q \end{array}}$$

In plain English, these say that, if you can rule one of two cases out, then you can conclude that the other case is true.

Suppose you have the polynomial $p(x) = 3x^2 - 15x$ and you are looking for any roots that occur when $x > 0$. After factoring, you get $p(x) = 3x(x - 5)$, and $p(x) = 0$ precisely when $3x = 0$ or $x - 5 = 0$. Since you only care about $x > 0$, then the other root you are looking for is $x = 5$.

A real number x satisfies $3x = 6$ or $x - 5 = 0$.
We observe that $3x \neq 6$.
Therefore $x - 5 = 0$.

Example 2.3.7: Rule of Inference: Specialization

The following argument forms are valid (and checking this is an exercise for the reader):

$$\boxed{\begin{array}{ll} & p \wedge q \\ \therefore & p \end{array}} \qquad \boxed{\begin{array}{ll} & p \wedge q \\ \therefore & q \end{array}}$$

In plain English, these say that, if you know two things are true, then in particular you know that one of those two things is true.

Suppose you are tasked with hiring someone who is fluent in Spanish. A resumè comes across your desk with someone who is fluent in both Spanish and Mandarin. Since they know Spanish, you offer them the job.

A person is fluent in Spanish and in Mandarin.
In particular, a person is fluent in Spanish.

Example 2.3.8: Rule of Inference: Transitivity

The following argument form is valid (and checking this is an exercise for the reader):

$$\boxed{\begin{array}{ll} & p \Rightarrow q \\ & q \Rightarrow r \\ \therefore & p \Rightarrow r \end{array}}$$

In plain English, this says that, if scenario p leads to scenario q and scenario q leads to scenario r, then scenario p leads to scenario r.

If the Philidelphia Eagles beat the Cincinnati Bengals, then they will win the Super Bowl.
If a team wins the Super Bowl, then they will receive the Vince Lombardi Trophy.
Therefore, if the Eagles beat the Bengals, then they will receive the Lombardi Trophy.

Example 2.3.9: Contradiction Rule

Show that the following argument form is valid.

$$\boxed{\begin{array}{ll} & \neg p \Rightarrow \mathbf{c} \\ \therefore & p \end{array}}$$

(where **c** is a contradiction.) In plain English, what this says is that if an assumption leads to a contradition, then that assumption must be false.

			Premise	Conclusion
p	$\mathbf{c}$	$\neg p$	$\neg p \Rightarrow \mathbf{c}$	p
T	F	F	T	T
F	F	T	F	

Example 2.3.10

What happens when you assume that zero is both an even number and an odd number?

Let p, q, r be the following statements.

p: zero is even
q: zero is odd
r: zero is divisible by 2.

We know the following to always be true: if a number is even, then it is divisible by 2; if a number is odd, then it is not divisible by 2. So, if we assume that zero is both even and odd, then we are assuming the following compound statement, which we'll simply denote $\neg\mathcal{P}$.

$$\neg\mathcal{P}\text{: } (p \wedge q) \wedge (p \Rightarrow r) \wedge (q \Rightarrow \neg r)$$

Using our Table of Logical Equivalences, we have that

$$\begin{aligned}
&(p \wedge q) \wedge (p \Rightarrow r) \wedge (q \Rightarrow \neg r) \\
&\equiv (p \wedge q) \wedge (\neg p \vee r) \wedge (\neg q \vee \neg r) && \text{(Exercise 2.2.1)} \\
&\equiv [p \wedge (\neg p \vee r)] \wedge [q \wedge (\neg q \vee \neg r)] && \text{(Associativity/Commutativity)} \\
&\equiv [(p \wedge \neg p) \vee (p \wedge r)] \wedge [(q \wedge \neg q) \vee (q \wedge \neg r)] && \text{(Distributive)} \\
&\equiv [p \wedge r] \wedge [q \wedge \neg r] && \text{(Absorption)} \\
&\equiv (p \wedge q) \wedge (r \wedge \neg r) && \text{(Associativity/Commutativity)} \\
&\equiv \mathbf{c} && \text{(Universal Bound)}
\end{aligned}$$

Since $\neg\mathcal{P} \equiv \mathbf{c}$, then $\neg\mathcal{P} \Rightarrow \mathbf{c}$ is true. By the Contradiction Rule, then we logically conclude that $\mathcal{P}$ is true. In symbols $\mathcal{P}$ is given by

$$\begin{aligned}
\mathcal{P} &\equiv \neg\neg\mathcal{P} && \text{(double negation)} \\
&\equiv \neg(p \wedge q) \vee \neg(p \Rightarrow r) \vee \neg(q \Rightarrow \neg r) && \text{(DeMorgan's)}
\end{aligned}$$

In words, this says that

zero is not both even and odd
or zero is even and not divisible by 2
or zero is odd and is divisible by 2

These last two are clearly false since our baseline assumption was that even numbers are those divisible by 2, so the true statement is precisely that zero cannot be both even and odd.

2.3.2 Fallacies

Definition: fallacy

A **fallacy** is an error in reasoning that results in an invalid argument.

Remark. An argument is invalid precisely when all premises are true, but the conclusion is false.

Example 2.3.11: Ambiguous Premises

Ambiguous premises can arise in many ways. For example, using words with multiple meanings and equivocating them.

6 is an odd number of legs for a horse.
Odd numbers cannot be divided by 2.
Therefore 6 cannot be divided by 2.

The word "odd" in line 1 is a synonym for "unusual" and in line 2 it is being used to describe a number not divisible by 2.

Example 2.3.12: Ambiguous Premises

Ambiguous premises can arise in many ways. For example, using words that cannot be quantified:

If you have a good understanding of Discrete Math, then you will do well on the exam.
You have a good understanding of Discrete Math
Therefore, you get an "A" on the exam.

"Doing well" on a test is ambiguous – arguably a grade of "B" or "C+" would be considered "doing well" to most.

Example 2.3.13: Circular Reasoning

Circular reasoning occurs when you use the conclusion as a premise.

You can't give me a "C" – I'm an "A" student.

You cannot claim to be an "A" student until you receive an "A" grade.

Example 2.3.14: Jumping to the Conclusion

Jumping to the conclusion happens when some premises are missing.

Drake and Rihanna have been seen together in public.
Therefore Drake and Rihanna are dating.

Example 2.3.15: Converse Error

Show that the following argument is invalid.

If Zeke is a cheater, then Zeke sits in the back of the classroom.
Zeke is sitting in the back of the classroom.
Therefore, Zeke is a cheater.

Let's assign some variables b, c to the above statements

c : "Zeke is a cheater"
b : "Zeke sits in the back"

Then we have the following truth table

		Premise 1	Premise 2	Conclusion
c	b	$c \Rightarrow b$	b	c
T	T	T	T	T
T	F	F		
F	T	T	T	**F**
F	F	T	F	

This is called the "converse error" beause it implicitly assumes that $q \Rightarrow p$ is logically equivalent to $p \Rightarrow q$, which is not the case.

Example 2.3.16: Inverse Error

Show that the following argument is invalid.

If this polygon $\mathcal{P}$ is a square, then it has four sides.
$\mathcal{P}$ is not a square.
Therefore $\mathcal{P}$ does not have four sides.

There are plenty of 4-sided polygons that are not squares, so already this argument seems problematic. Let's assign some variables s, f to the above statements

s : "$\mathcal{P}$ is a square"
f : "$\mathcal{P}$ has four sides"

Then we have the following truth table

		Premise 1	Premise 2	Conclusion
s	f	$s \Rightarrow f$	$\neg s$	$\neg f$
T	T	T	F	
T	F	F		
F	T	T	F	
F	F	T	T	**F**

This is called the "inverse error" because it implicitly assumes that $\neg p \Rightarrow \neg q$ is logically equivalent to $p \Rightarrow q$, which is not the case.

2.3.3 Sound Arguments

Definition

An argument is called **sound** if is it valid *and* the premises are all actually true. An argument is **unsound** otherwise.

The above is more of a philosophical distinction than one detectable in a truth table. For example, consider the two following arguments

If an animal is a fluffy god, then it has fur.
An animal does not have fur.
Therefore it is not a dog.

If a potato is green, then it is from Mars.
A potato is not from Mars.
Therefore that is not green.

Both of the above arguments are examples of *modus tollens* and are thusly valid. However, the one on the left is sound (ignore the pedantry of “hair vs. fur”, but the one on the right is not – any discussion of Martian potatoes is pretty outlandish and absurd at present.

Remark. Don’t eat green potatoes. Not only are they almost certainly not from Mars, they carry a high risk of solanine poisoning.

3 The Logic of Quantified Statements

3.1 Predicates and Quantified Statements I

Definition: Predicate, Domain

A **predicate** is a sentence that contains a finite number of variables and becomes a statement when specific values are substituted for the variables. The **domain** of a predicate is the collection of values that may be substituted in place of the variable(s).

Example 3.1.1

Let $P(x)$ be the predicate $x^2 > x$ and let D be the domain $\mathbb{R}$ - the set of real numbers. Assess the truth values of the following statements: $P(-1), P(1), P(10)$.

$$\begin{array}{rll} P(-1)\text{:} & (-1)^2 = 1 > -1 & \text{True} \\ P(1)\text{:} & (1)^2 = 1 \not> 1 & \text{False} \\ P(10)\text{:} & (10)^2 = 100 > 10 & \text{True} \end{array}$$

Exercise 3.1.2

Let $P(x, y)$ be the predicate $y \geq x$ and let D be the domain $\mathbb{R} \times \mathbb{R}$ (that is, x and y are both real numbers). Assess the truth values of the following statements: $P(0, 1)$, $P(1, 1)$, $P(1, 0.9)$.

Definition: Truth set

If $P(x)$ is a predicate and x has domain D, then the **truth set** of $P(x)$ is the set of all elements of D that make $P(x)$ true when they are substituted for x. The truth set of $P(x)$ is denoted

$$\{x \in D \mid P(x)\}.$$

The symbol $\in$ is short for "in" in English.

Definition

The following short-hand notation is used for some commonly-occuring sets.

$\mathbb{N}$	The natural numbers: $0, 1, 2, 3, \ldots$
$\mathbb{Z}$	The integers: $\ldots, -2, -1, 0, 1, 2, \ldots$
$\mathbb{Z}^+$	The positive integers: $1, 2, 3, 4, \ldots$
$\mathbb{Q}$	The rational numbers (i.e. all possible fractions)
$\mathbb{R}$	The real numbers

Remark. Some people take the convention that 0 is not a natural number, and some take the convention that that 0 is a positive integer. These competing conventions are commonplace, and it's not often a big deal in practice if an author doesn't make their particular conventions explicit at the onset. Nevertheless, mathematicians are human and need something to argue about, so your instructor will staunchy insist that anyone who doesn't adhere to his conventions is patently wrong.

Example 3.1.3

Let $P(x)$ be the predicate $x^2 < 10$. Find the truth set for P when the domain D is ...

a. ... $\mathbb{N}$.

b. ... $\mathbb{Z}$.

c. ... $\mathbb{Z}^+$.

d. ... $\mathbb{R}$.

a. The natural numbers x which make $P(x)$ true are $\{0, 1, 2, 3\}$

b. The integers x which make $P(x)$ true are $\{-3, -2, -1, 0, 1, 2, 3\}$

c. The positive integers $\mathbb{Z}^+$ which make $P(x)$ true are $\{1, 2, 3\}$

d. The real numbers $\mathbb{R}$ which make $P(x)$ true are $\{x \in \mathbb{R} \mid -3 < x < 3\}$

3.1.1 The Universal Quantifier: ∀

Definition: universal statement, counterexample

Let $P(x)$ be a predicate and let D be the domain of x. A **universal statement** is a statement of the form

For every x in D, $P(x)$ is true. (In symbols, $\forall x \in D, P(x)$)

The universal statement $\forall x \in D, P(x)$ is true if and only if it is true for every x in D. The universal statement is false if there is at least one x' in D where $P(x')$ is false. Such an x' is called a **counterexample**.

Remark. Sometimes it is also written as $\forall x \in D(P(x))$

Example 3.1.4

Let $P(x)$ be the predicate $x^2 \geq x$. Determine whether or not the universal statements are true or false.

1. $\forall x \in \mathbb{Z}, P(x)$
2. $\forall x \in \mathbb{R}, P(x)$

1. This is true.
2. This is false. When $x = \frac{1}{2}$, then $x^2 = \frac{1}{4} \ngeq x$, so $x = \frac{1}{2}$ is a counterexample. In fact, any x in the interval $0 < x < 1$ will be a counter-example.

Example 3.1.5: Method of Exhaustion

Let D be the following set of prime numbers

$$D = \{29, 41, 47, 53, 59\}$$

and let $P(x)$ be the predicate "x divided by 6 has a remainder of 5." Is the universal statement $\forall x \in D, P(x)$ true?

Statements about prime numbers are often nontrivial, but since we only have a few, we can check them all explicitly:

$$\begin{aligned}29 &= 4(6)+5\\41 &= 6(6)+5\\47 &= 7(6)+5\\53 &= 8(6)+5\\59 &= 9(6)+5\end{aligned}$$

so the universal statement is true.

3.1.2 The Existential Quantifier: $\exists$

Definition: existential statement

Let $P(x)$ be a predicate and let D be the domain of x. An **existential statement** is a statement of the form

$$\text{There exists some } x \text{ in } D \text{ for which } P(x) \text{ is true. (In symbols, } \exists x \in D, P(x))$$

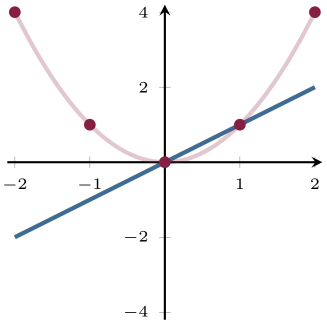
The existential statement $\exists x \in D, P(x)$ is true if and only if it is true for at least one x in D. It is false if and only if it is false for every x in D.

Example 3.1.6

Let $P(x)$ be the predicate $x^2 < x$. Determine whether or not the existential statements are true or false.

1. $\exists x \in \mathbb{R}, P(x)$
2. $\exists x \in \mathbb{Z}, P(x)$

1. This is true. When $x = \frac{1}{2}$, then $x^2 = \frac{1}{4} < \frac{1}{2} = x$.
2. This is false. We don't yet have a means of proving it, but you can be convinced by comparing the graphs of $y = x$ and $y = x^2$ (where x, y are integers).



In English, of course, there are numerous ways in which we can communicate these quantifiers. Below is an incomplete list of such things.

$\forall$	“for each”, “for all”, “for every”, “for arbitrary”, “for any”
$\exists$	“some”, “there is”, “at leat one”, “can find a”

Remark. It’s also worth noting that, in symbolic logic, the quantifiers are always written first, but in English the quantifier may come at the end. For example

$$\text{“}x^2 \geq 0 \text{ for every } x \in \mathbb{R}.\text{”}$$

3.1.3 Universal Conditional Statement

Definition: universal conditional statement

Let $P(x)$, $Q(x)$ be predicates with the same domain D. A **universal conditional statement** is a statement of the form

$$\text{For every } x \text{ in } D, \text{ if } P(x) \text{ is true, then } Q(x) \text{ is true. (In symbols, } \forall x \in D, P(x) \Rightarrow Q(x)\text{)}$$

The universal conditional statement $\forall x \in D, P(x) \Rightarrow Q(x)$ is true if and only if $P(x) \Rightarrow Q(x)$ is true for every x in D. It is false if and only if it is false for at least one x in D (which occurs when $P(x)$ is true and $Q(x)$ is false).

Example 3.1.7

Which of the following conditionals are true for the domain $\mathbb{R}$?

1. $x^2 > 4 \implies x > 2$
2. $x^2 > 4 \iff |x| > 2$

For simplicity we use the following notation:

$P(x)$	$x^2 > 4$
$Q(x)$	$x > 2$
$R(x)$	$\lvert x\rvert > 2$

1. $x^2 > 4 \implies x > 2$ is false. This universal conditional has the form

   $$\forall x \in \mathbb{R}, P(x) \implies Q(x).$$

   But $P(-3)$ is true and $Q(-3)$ is false, so $x = -3$ is a counterexample.
2. $x^2 > 4 \iff |x| > 2$ is true. This universal conditional has the form

   $$\forall x \in \mathbb{R}, P(x) \iff R(x).$$

3.1.4 Implicit Quantification

As is often the case, many times the quantifier is not ever stated explicitly, which we refer to as **implicit quantification**. It is up to you, the reader, to correctly determine which quantifier applies here.

Example 3.1.8: Implicit Quantification

"The sum of even integers is even."

"For all integers x and for all integers y, if x and y are even, then $x + y$ is even."

$$\forall x \in \mathbb{Z}, \forall y \in \mathbb{Z}, x \text{ even} \wedge y \text{ even} \implies (x + y) \text{ even}$$

Example 3.1.9: Sentences: Informal to Formal

For each of the following statements, identify the predicate(s), domain(s), and variable(s). Then rewrite the sentence formally using logical symbols and quantifiers.

1. Whenever an integer is non-zero, its square is positive.
2. Every integer is even if its square is even.
3. $a^2 + 2 = 6$ for some integer a.
4. There's at least one ghost in this classroom right now.

1. *Whenever an integer is non-zero, its square is positive.*

$$\begin{aligned} P(x)&: \quad x \neq 0 \\ Q(x)&: \quad x^2 > 0 \\ D&: \quad \mathbb{Z} \end{aligned}$$

With the above notation, this sentence is written

$$\forall x \in \mathbb{Z},\ P(x) \implies Q(x).$$

. . . .

Alternatively, one could take

$$\begin{aligned} P(x)&: \quad x^2 > 0 \\ D&: \quad \text{nonzero integers} \end{aligned}$$

in which case the sentence is written

$$\forall x \in D,\ P(x).$$

---

2. *Every integer is even if its square is even.*

$$\begin{aligned} P(x)&: \quad x \text{ is even} \\ Q(x)&: \quad x^2 \text{ is even} \\ D&: \quad \mathbb{Z} \end{aligned}$$

With the above notation, this sentence can be written

$$\forall x \in \mathbb{Z},\ Q(x) \implies P(x).$$

3. *$a^2 + 2 = 6$ for some integer a.*

$$\begin{aligned} P(x)\colon &\quad x^2 + 2 = 6 \\ D\colon &\quad \mathbb{Z} \end{aligned}$$

With the above notation, this sentence can be written

$$\exists a \in \mathbb{Z},\ P(x).$$

4. *There's at least one ghost in this classroom right now.*

$$\begin{aligned} P(x)\colon &\quad x \text{ is in this classroom right now} \\ D\colon &\quad \text{Ghosts} \end{aligned}$$

With the above notation, this sentence can be written

$$\exists a \in D\, P(x).$$

Exercise 3.1.10: Sentences: Informal to Formal

For each of the following statements, identify the predicate(s), domain(s), and variable(s). Then rewrite the sentence formally using logical symbols and quantifiers.

1. Some people have tattoos.
2. Among all basketball players, some are tall.
3. Somebody in your group likes the orange Starburst.
4. There is an even prime number.
5. No Tech student has class on Sundays.
6. Integers are also real numbers.
7. All dogs go to heaven.
8. If a real number is rational, then so is its multiplicative inverse.
9. The sum of even integers is even.
10. Any factor of 4 is also a factor of 8.
11. John likes the taste of every Starburst.
12. For any Starburst flavor, there's someone out there who likes the taste it.

3.1.5 Relationship between $\forall$ and $\wedge$; Relationship between $\exists$ and $\vee$

Suppose $D = \{x_1, x_2, x_3, \ldots, x_n\}$ is a finite domain and $P(x)$ is some predicate. Using the method of exhaustion, one can verify the claim $\forall x \in D, P(x)$ by checking that $P(x_1)$, $P(x_2)$, ..., and $P(x_n)$ are all true. In other words

$$\forall x \in D, P(x) \equiv P(x_1) \wedge P(x_2) \wedge \cdots \wedge P(x_n)$$

Similarly, by exhaustion, one can verify the claim $\exists x \in D, P(x)$ by checking that at least one of $P(x_1)$, $P(x_2)$, ..., or $P(x_n)$ is true. In other words

$$\exists x \in D, P(x) \equiv P(x_1) \vee P(x_2) \vee \cdots \vee P(x_n)$$

Exercise 3.1.11

Rewrite the following statements in terms of $\wedge$ and $\vee$.

1. Every integer x with $-1 \leq x \leq 1$ satisfies $x^3 = x$.
2. There is a natural number $x < 4$ for which $x^3 = x$.

In both of these, let $P(x)$ be the statement $x^3 = x$.

1. $\forall x \in \{-1, 0, 1\}, P(x) \equiv P(-1) \wedge P(0) \wedge (P1)$
2. $\exists x \in \{0, 1, 2, 3\}, P(x) \equiv P(0) \vee P(1) \vee P(2) \vee P(3)$

3.2 Predicates and Quantified Statements II

3.2.1 Negating Universal and Existential Statements

Recall that the statement

$$\forall x \in D, P(x)$$

is false precisely when there is some x in D where $P(x)$ is false. Thus, its negation

$$\neg(\forall x \in D, P(x))$$

is true precisely where there is some x in D where $P(x)$ is false. And $P(x)$ is false precisely when $\neg P(x)$ is true. This observation (and the equivalent one when negating an existential statement) yields the following:

Theorem 3.2.1: Negation of Universal/Existential Statements

Let $P(x)$ be a predicate with domain D. Then we have the following:

$$\neg\left(\forall x \in D, P(x)\right) \equiv \exists x \in D, \neg P(x)$$
$$\neg\left(\exists x \in D, P(x)\right) \equiv \forall x \in D, \neg P(x)$$

Example 3.2.2

Negate the following statements.

1. All cats have wings.
2. $y^2 = -7$ for some integer y.
3. Someone in this classroom has a cat with wings.
4. $x^2 > 1$ for all real numbers x.
5. No mathematicians are interesting.
6. Not all students have an iPhone.

3.2.2 Conditionals - Related Conditionals and Negations

There are, of course, universal conditionals that are related to the usual universal conditional $\forall x \in D, P(x) \implies Q(x)$.

Definition: Related Universal Conditionals

Let $P(x), Q(x)$ be predicates with domain D and consider the conditional statement $\forall x \in D, P(x) \implies Q(x)$. The **contrapositive** is

$$\forall x \in D, \neg Q(x) \implies \neg P(x).$$

The **converse** is

$$\forall x \in D, Q(x) \implies P(x).$$

The **inverse** is

$$\forall x \in D, \neg P(x) \implies \neg Q(x).$$

Proposition 3.2.3: Negation of Universal Conditional Statement

Let $P(x), Q(x)$ be predicates with domain D. Then we have the following:

$$\neg\left(\forall x \in D, P(x) \implies Q(x)\right) \equiv \exists x \in D, P(x) \wedge \neg Q(x).$$

Proof.

$$\begin{aligned}
\neg\left(\forall x \in D, P(x) \implies Q(x)\right) &\equiv \exists x \in D, \neg\left(P(x) \implies Q(x)\right) && \text{(Theorem ??)}\\
&\equiv \exists x \in D, \neg\left(\neg P(x) \vee Q(x)\right) && \text{(Exercise 2.2.1)}\\
&\equiv \exists x \in D, \neg\neg P(x) \wedge \neg Q(x) && \text{(DeMorgan's Law)}\\
&\equiv \exists x \in D, P(x) \vee \neg Q(x) && \text{(Double Negative Law)}
\end{aligned}$$

□

Example 3.2.4

Negate the following conditional statements:

1. $\forall x,\ \text{if } x < -1,\ \text{then } x^2 > 1$
2. Whenever VT students attend a football game, they sing ”Enter Sandman”.

Example 3.2.5

Consider the statement

Whenever VT students attend football games, they sing ”Enter Sandman”.

Write the contrapositive, converse, and inverse. Then negate each of these.

1. (Contrapositive) If VT students don’t sing “Enter Sandman”, then they do not attend football games.

(Contrapositive Negation) INCOMPLETE

2. (Converse) INCOMPLETE
   (Converse Negation) INCOMPLETE

3. (Inverse) INCOMPLETE
   (Inverse Negation) INCOMPLETE

3.3 Statements with Multiple Quantifiers

As is often the case in math, one typically involves multiple variables with multiple quantifiers. Anyone who has already taken a calculus class and has seen the formal definition of a limit has experienced this.

> A function f has a limit L at $x = a$ if it has the following property; for every $\varepsilon > 0$, there exists $\delta > 0$ such that
>
> $$0 < |x - a| < \delta \implies |f(x) - L| < \varepsilon.$$

3.3.1 ∀∀ and ∃∃ Statements

In short, two consecutive universal quantifiers (and likewise for two existential quantifiers) can be commuted.

Example 3.3.1

Write the following sentence formally and rearrange the order of the quantifiers.

Every student must do all homework problems.

Symbolically, the above sentence is

$$\forall x \in \{\text{students}\}, \forall y \in \{\text{homework problems}\}, x \text{ must do } y.$$

Changing the order

$$\forall y \in \{\text{homework problems}\}, \forall y \in \{\text{students}\}, y \text{ must do } x$$

which translates to

All homework problems must be done by everyone

and this has the same meaning as the original statement.

Example 3.3.2

Write the following sentence formally and rearrange the order of the quantifiers.

Some kid is stealing cookies from one of the boxes.

Symbolically, the above sentence is

$$\exists x \in \{\text{kids}\}, \exists y \in \{\text{boxes of cookies}\}, x \text{ stole from } y.$$

Changing the order

$$\exists y \in \{\text{boxes of cookies}\}, \exists y \in \{\text{kids}\}, y \text{ stole from } x.$$

which translates to

There is a box from which some kid stole cookies.

and this has the same meaning as the original statement.

3.3.2 ∀∃ and ∃∀ Statements

When mixing quantifiers, the order matters.

$\forall x, \exists y, P(x,y)$	For every x there is some y for which $P(x,y)$ is true.
$\exists x, \forall y, P(x,y)$	There is a x for which $P(x,y)$ is true for every y.

Example 3.3.3

Write the following symbolically, rearrange the quantifiers, and translate it back into plain English. How do the quantifiers change the meaning?

Everybody is good at something.

In symbols, this would read

$$\forall x \in \{\text{people}\}, \exists y \in \{\text{things}\}, x \text{ is good at } y.$$

Switching the order of the quantifiers, we get

$$\exists y \in \{\text{things}\}, \forall x \in \{\text{people}\}, x \text{ is good at } y.$$

which translates to

There is one thing that everyone is good at (i.e., everyone is good at the same thing).

and this sentence is not equivalent to the original sentence.

It's good to think about how order of quantifiers changes a proof strategy. In the ∀∃ case, for each x that you're given, you can find a y that makes $P(x,y)$ true. Usually, y will somehow be related to x, so different x's have different corresponding y values. In the ∃∀ case, we need can find some x with the feature that, no matter what y-value you pick, $P(x,y)$ is true – the y in this case is actually completeley unrelated to x.

Example 3.3.4: Translating Informal to Formal - Math Statements Edition

Translate each of the following mathematical sentences into symbolic language. Then discuss how one might go about proving the statement true.

1. Every nonzero real number has a reciprocal.
2. There is a real number which has no reciprocal.
3. There is a smallest positive integer.
4. There is no smallest positive rational number.

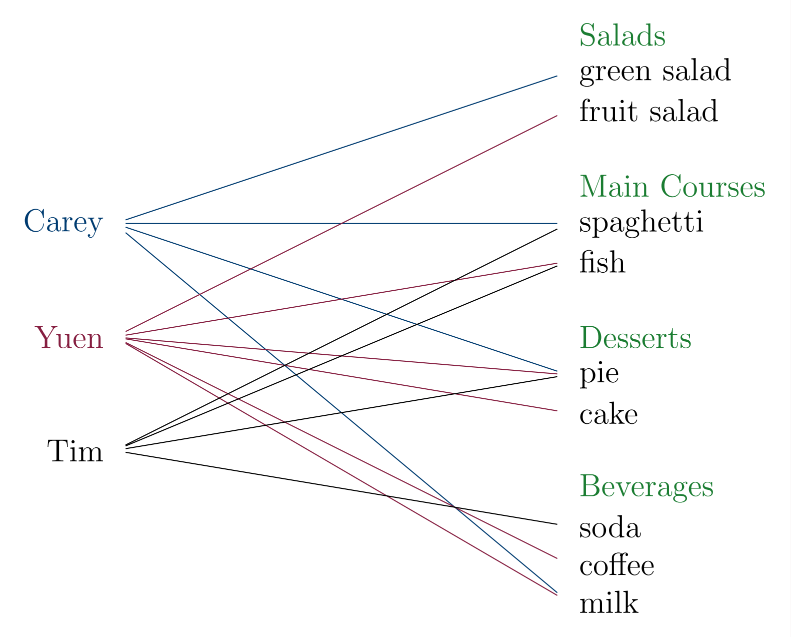
1. $\forall x \in \{\text{nonzero reals}\}, \exists y \in \mathbb{R}, xy = 1.$
   To prove this, given x, we would choose $y = \frac{1}{x}$ (which is again a nonzero real number). Then it follows that $xy = x\left(\frac{1}{x}\right) = 1$.
2. $\exists x \in \mathbb{R}, \forall y \in \mathbb{R}, xy \neq 1.$
   To prove this we just have to find one x-value. Taking $x = 0$ works because, no matter which real number y we try, we always have that $xy = 0y = 0 \neq 1$.
3. $\exists x \in \{\text{positive integers}\}, \forall y \in \{\text{positive integers}\}, x \leq y.$

To prove this we just have to find a smallest positive integer. Indeed, taking $x = 1$ works since any other positive integer y has the property that $1 = x \leq y$.

4. $\forall x \in \{\text{positive rationals}\}, \exists y \in \{\text{positive rationals}\}, 0 < y < x$.
   To prove this, given x, we should choose $y = \frac{1}{2}x$. Since x is positive and rational, so is y. Then it follows that $0 < y\frac{1}{2}x < x$.

Exercise 3.3.5

Three people, Carey, Yuen, and Tim, are going to eat at a buffet. The buffet has four main areas: salads, main courses, desserts, and beverages. The figure below shows which person (P) selected which item (I) from each area (A).



Rewrite each of the following statements informally and find its truth value.

1. $\exists I, \forall P, P$ chose I.
2. $\exists P, \forall I, P$ chose I.
3. $\exists P, \forall A, \exists I$ in A, P chose I.
4. $\forall P, \forall A, \exists I$ in A, P chose I.

Theorem 3.3.6: Negations of Multiple Quantifiers

Let $P(x, y)$ be a predicate and D, E the domains for x, y, respectively. Then

$$\neg\left(\forall x \in D, \exists y \in E, P(x, y)\right) \equiv \exists x \in D, \forall y \in E, \neg P(x, y)$$
$$\neg\left(\exists x \in D, \forall y \in E, P(x, y)\right) \equiv \forall x \in D, \exists y \in E, \neg P(x, y)$$

Example 3.3.7

Negate each of the following statements.

1. $\forall x \in \mathbb{R}, \exists y \in \mathbb{R}$ such that $xy < 0$.

2. $\forall \varepsilon \in \{\text{positive reals}\}, \exists \delta \in \{\text{positive reals}\}$ such that, if $0 < |x - a| < \delta$, then $|f(x) - L| < \varepsilon$.

1. $\exists x \in \mathbb{R}$ such that $\forall y \in \mathbb{R}$, $xy \geq 0$.
2. $\exists \varepsilon \in \{\text{positive reals}\}$ such that $\forall \delta \in \{\text{positive reals}\}$, $0 < |x - a| < \delta$ and $|f(x) - L| \geq \varepsilon$.

4 Elementary Number Theory and Methods of Proof

4.1 Direct Proof and Counterexample I: Introduction

Recall the following:

1. The integers are closed under addition. (The sum of two integers is again an integer.)
2. The integers are closed under multiplication. (The product of two integers is again an integer.)

Definition: even and odd integers

even-odd-int An integer is said to be **even** precisely when it is twice another integer. An integer is said to be **odd** if and only if it is not even. Symbolically,

$$\begin{aligned} n \text{ is even} &\iff \exists k \in \mathbb{Z} \text{ such that } n = 2k. \\ n \text{ is odd} &\iff \exists k \in \mathbb{Z} \text{ such that } n = 2k+1. \end{aligned}$$

Since even/oddness is an existential statement, any proof requires only finding a single integer k.

Example 4.1.1

Use the definitions of even and odd to prove the following statements.

1. 0 is even.
2. -401 is odd.
3. If a, b are integers, $6a^2b$ is even.

1.

> *Proof.* Choosing $k = 0$, we have that $0 = 2(0) = 2k$. Therefore 0 is even. □

2.

> *Proof.* Choosing $k = -201$, we have that $-401 = 2(-201) + 1 = 2k + 1 =$. Therefore -401 is odd. □

3. Notice that this statement nas multiple quantifiers $\forall a \in \mathbb{Z}, \forall b \in Z, \exists k \in \mathbb{Z}$ such that $6a^2b = k$.

> *Proof.* Let $a, b \in \mathbb{Z}$ and choose $k = 3a^2b$. As the integers are closed under multiplication, k is an integer. We have that $6a^2b = 2(3a^2b) = 2k$, therefore $6a^2b$ is even. □

Definition: prime and composite numbers

An positive integer p is prime if and only if $p > 1$ and for any integers m, n with $p = mn$, then one of m or n is p. An integer is **composite** if and only if $p > 1$ and there are integers $1 < m, n < p$ for which $p = mn$. Symbolically,

$$\begin{aligned} p \text{ is prime} &\iff p > 1 \text{ and } \forall m, n \in Z^+, \text{ if } p = mn \text{ then } m = p \\ &\qquad \text{or } n = p. \\ p \text{ is composite} &\iff p > 1 \text{ and } \exists m, n \in Z^+ \text{ such that } 1 < m, n < p \\ &\qquad \text{and } p = mn. \end{aligned}$$

Example 4.1.2

Prove each of the following claims.

1. 1 is not prime.
2. 2468 is composite.
3. 5 is prime.

1.

> *Proof.* By definition, a prime number is strictly greater than 1. Therefore 1 is not prime. □

2.

> *Proof.* Choose $m = 2$ and $n = 1234$, which satisfies $1 < m < n < 2468$. Since $2468 > 1$ and $2468 = 2(1234) = mn$, then 2468 is a composite number. □

3. This proof is actually more difficult than you might expect – how do you prove this holds for every possible integer? The missing ingredient is that we also want $1 \leq m, n \leq p$.

4.1.1 Proving an Existential Statement

To prove an existential statement $\exists x \in D | Q(x)$:

Proving an Existential Statement

1. Produce an x.
2. Show that $x \in D$, the domain.
3. Show that $Q(x)$ is true.

Example 4.1.3

Prove the following statement:

There is an even number that can be written in two ways as a sum of two prime numbers.

First we look at this statement somewhat symbolically:

$\exists x \in \mathbb{Z}^+$ such that $\exists p_1, p_2, q_1, q_2 \in$ {prime numbers} where $x = p_1 + p_2$ and $x = q_2 + q_2$ and p_1, p_2 are different from q_1, q_2.

For scratch work, by simply trying out a few small-numbered examples, we see that $20 = 3 + 17 = 7 + 13$. Using this, we write the proof.

> *Proof.* Notice that the positive integer 20 satisfies $20 = 3 + 17$ and $20 = 7 + 13$. Since and $3, 17, 7, 13$ are all distinct prime numbers, then we have proven the desired claim. □

Definition: Constructive and Nonconstructive Proofs

A **constructive** proof of existence involves

1. finding an x in our domain for which $Q(x)$ is true or
2. giving an set of directions for finding such an x in the domain.

A **nonconstructive proof** of existence involves showing either:

1. the existence of a value x that makes $Q(x)$ true is guaranteed by an axiom or a previously proved theorem
2. the assumption that there is no such x leads to a contradiction

You've probably seen a non-constructive proof before; below is one such proof.

Example 4.1.4: non-constructive proof

Prove the claim:

The polynomial $p(x) = x^5 - x + 1$ has a real root.

We first rewrite this symbolically: $\exists x \in \mathbb{R}$ such that $p(x) = 0$.

> *Proof.* Recall from calculus that polynomials are continuous functions. Since $p(-2) = -29$ and $p(1) = 1$ and $-29 < 0 < 1$, then by the Intermediate Value Theorem, there is a real number $x \in (-2, 1)$ for which $p(x) = 0$. □

4.1.2 Disproving Universal Statements

Disproof by Counterexample

To disprove a statement of the form "$\forall x \in D, P(x) \implies Q(x)$", find a counterexample, i.e. some $x \in D$ for which $P(x)$ is true and $Q(x)$ is false.

Example 4.1.5

Prove or disprove the following claim:

For all real numbers a, b, if $a < b$ then $a^2 < b^2$.

> *Disproof.* Let $a = -10$ and $b = 1$. Then $a = -10 <= 1$, but $a^2 = 100 \geq 1 = b^2$. □

4.1.3 Proving a Universal Statement

We've already seen the Method of Exhaustion before, which works well for small finite domains. In practice

Direct Proof of Universal Statement

1. Express the statement to be proved in the form $\forall x \in D$, if $P(x)$, then $Q(x)$.
2. Let x be a particular but arbitrarily chosen element of the domain for which $P(x)$ is true.
3. Show that the conclusion $Q(x)$ is true by using definitions and previously established rules.

The last item is doing *a lot* of heavy lifting here - that's absolutely the hard part and there's no one-size-fits-all strategy for doing it – this is where you, the human, have to think.

Example 4.1.6

Prove the statement:

The sum of two even integers is even.

We first acknowledge that, symbolically, this statement is $\forall x \in Z, \forall y \in Z$ if x is even and y is even, then $x + y$ is even. For scratch work, recalling the definition of even and odd **??**, we know that, if x, y are even, there are integers k, ℓ for which

$$x = 2k \text{ and } y = 2\ell \implies x + y = 2k + 2\ell = 2(k + \ell)$$

and these rearrangement rules give us the clue into the proof.

> *Proof.* Suppose x and y are arbitrary even integers. Then (by definition) there exist integers k and ℓ such that $x = 2k$ and $y = 2\ell$. It follows then that $x + y = 2k + 2\ell = 2(k + \ell)$. Since the integers are closed under addition, $k + \ell$ is an integer, and therefore $x + y$ is an even integer. □

HERE IT WOULD BE GOOD TO TIE IN THE PROOF FROM TEXTBOOK PAGES 148/149 AND THE DISCUSSION OF MODUS PONENS

4.1.4 Disproving an Existential Statement

Proving the Negation

To disprove a statement of the form $\exists x \in D$ such that $P(x)$:

1. Negate the statement. $(\forall x \in D, \neg P(x))$
2. Prove the negated universal statement.
3. Conclude that the original statement must be false, since the negation is true and the original statement and the negation have opposite truth values.

Example 4.1.7

Show that the following statement is false:

There is a positive integer n such that $n^2 + 3n + 2$ is prime.

Proving that this statement is false is equivalent to proving that its negation is true. The negation of this statement is

For every positive integer n, $n^2 + 3n + 2$ is composite (i.e. not prime).

We begin with some scratch work. Notice that we can factor this quadratic

$$n^2 + 3n + 2 = (n + 1)(n + 2)$$

and neither of the factors are 1.

Proof. Let n be an arbitrary positive integer. Then

$$n^2 + 3n + 2 = (n+1)(n+2)$$

and since $n > 0$ (by definition), then neither $n+1 = 1$ nor $n+2 = 1$. Therefore $n^2 + 3n + 2$ cannot be a prime number. □

Sometimes when we cannot prove a result directly using definitions.

4.1.5 Proof by Cases

Proof by Cases

1. Divide the situation into cases which exhaust all possibilities.

2. Show that for all cases the statement is true.

Example 4.1.8

Prove that for all integers n, $n^2 - 3n$ is even.

It's not present that $n^2 - 3n$ becomes twice some integer, but maybe if we know more about n we can say more. Let's do some scratch work.

$$\begin{aligned} n = 2k \quad &\implies \quad n^2 - 3n = (2k)^2 - 3(2k) = 2(2k^2 - 3k) \\ n = 2k+1 \quad &\implies \quad n^2 - 3n = (2k+1)^2 - 3(2k+1) = 4k^2 + 4k + 1 - 6k - 3 \\ & \quad = 4k^2 - 2k - 2 = 2(2k^2 - k - 2) \end{aligned}$$

Proof. Suppose that n is an even integer. Then there exists another integer k for which $n = 2k$. It follows that

$$n^2 - 3n = 2(2k^2 - 3k).$$

Since $\mathbb{Z}$ is closed under addition and multiplication, $2k^2 - 3k$ is an integer. Therefore $n^2 - 3n$ is even.
Suppose now that n is an odd integer. Then there exists another integer ℓ for which $n = 2\ell$. It follows that

$$n^2 - 3n = 2(2k^2 - k - 2).$$

Since $\mathbb{Z}$ is closed under addition and multiplication, $2k^2 - k - 2$ is an integer. Therefore $n^2 - 3n$ is even.
We conclude that, regardless of the parity of n, $n^2 - 3n$ is an even integer. □

4.2 Direct Proof and Counterexample II: Writing Advice

Guidelines for Writing Proofs

1. Begin by writing the statement which you wish to prove.
2. Identify the domain, hypotheses and conclusion.
3. Clearly mark the beginning of your proof with the word Proof.
4. Make your proof self-contained.
5. Write your proof in complete, grammatically correct sentences.
6. Keep your reader informed about the status of each statement in your proof.
7. Give a reason for each assertion in your proof.
8. Include connecting words and phrases to make your argument clear.
9. Display equations and inequalities.
10. Make sure that the conclusion has been explicitly shown.
11. Clearly mark the end of your proof, usually with a symol like □ or ■.

(Note that if you use LaTeX, then typing `\begin{proof}...\end{proof}` *will handle items 3 and 11 for you.*

4.2.1 Common Mistakes in Proof-Writing

Example 4.2.1: Arguing from examples

Prove: The sum of any two even integers is even.

> *Proof.* This is true because if $m = 14$ and $n = 6$, which are both even, then $m + n = 20$, which is also even. □

Example 4.2.2: Using the same letter to mean two different things

Prove: the sum of any two even integers is even.

> *Proof.* Let m and n be particular but arbitrarily chosen even integers. Then $m = 2k$ and $n = 2k$ for some integer k.
>
> $\vdots$
>
> □

Example 4.2.3: Jumping to a conclusion

Prove: The sum of any two even integers is even.

> *Proof.* Let m and n be particular but arbitrarily chosen even integers. Then by the definition of even, $m = 2k_1$ and $n = 2k_2$ for some integers k_1 and k_2. Thus, $m + n = 2k_1 + 2k_2$. So $m + n$ is even. □

Example 4.2.4: Circular reasoning

Prove: The product of odd integers is odd.

> *Proof.* *Suppose m and n are odd integers. When any odd integers are multiplied, their product is odd. Hence mn is odd.* □

Example 4.2.5: Confusion between what is known and what is still to be shown

Prove: The product of two odd integers is odd.

> *Proof.* Suppose m and n are any odd integers. We must show that mn is odd. This means that there exists an integer s such that $mn = 2s + 1$.
> Also by the definition of odd, there exist integers a and b such that $m = 2a+1$ and $n = 2b+1$.
> Then $mn = (2a + 1)(2b + 1) = 2s + 1$.
> So, since s is an integer, mn is odd by definition of odd. □

This following issues are not serious on their own, but each reflects imprecise thinking that sometimes leads to problems later in a proof.

Example 4.2.6: Use of ***any*** rather than ***some***

Prove: The square of any odd integer is odd.

> *Proof.* Suppose m is a particular but arbitrarily chosen odd integer. By definition of odd, $m = 2a + 1$ for any integer a.
> $\vdots$
> □

Example 4.2.7: Use of ***if*** rather than ***because***

Prove: The square of any odd integer is odd.

> *Proof.* Suppose m is a particular but arbitrarily chosen odd integer. If m is odd, $m = 2a + 1$ for any integer a. $\vdots$
> □

4.3 Direct Proof and Counterexample III: Rational Numbers

Definition: rational numbers

A real number r is a **rational number** if and only if, there are integer a, b with $b \neq 0$ such that $r = \frac{a}{b}$. A real number that is not rational is called **irrational**.

Remark. The set of rational numbers is typically denoted $\mathbb{Q}$, and the irrational numbers are denoted $\mathbb{R} \setminus \mathbb{Q}$ or $\mathbb{R} - \mathbb{Q}$.

Remark. The name rational number comes from the fact that we can write a *ratio*nal number as a *ratio* of integers.

We'll take the following as fact

Fact. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ have the "zero product property.":

If x, y are nonzero numbers, then xy is nonzero.
If the product of numbers $xy = 0$, then at least one of x and y is zero.

Proposition 4.3.1: Properties of $\mathbb{Q}$

$\mathbb{Q}$ has the following properties:

1. $\mathbb{Q}$ is closed under addition. (The sum of two rational numbers is rational).
2. $\mathbb{Q}$ is closed under multiplication. (The product of two rational numbers is again rational).

Proof. Let x, y be arbitrary rational numbers. By definition, we must have integers a_1, a_2 and nonzero integers b_1, b_2 such that

$$x = \frac{a_1}{b_1} \qquad \text{and} \qquad y = \frac{a_2}{b_2}.$$

1. Notice that

$$x + y = \frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2}{b_1 b_2} + \frac{a_2 b_1}{b_1 b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2}.$$

   Since the integers are closed under addition and multiplication, then $a_1 b_2 + a_2 b_1$ and $b_1 b_2$ are integers. Since b_1, b_2 are nonzero, then $b_1 b_2$ is also nonzero by the zero product property for $\mathbb{Z}$. Thus $x + y$ is rational.

2. Left as an exercise for the reader.

□

Proposition 4.3.2

Every integer is a rational number.

In order to prove this, we begin by noting that this statement can be written in logical symbols as

$$\forall z \in \mathbb{Z}, z \text{ is rational.}$$

which again becomes

$$\forall z \in \mathbb{Z}, \exists a \in \mathbb{Z}, \exists b \in \mathbb{Z}, \text{ such that} z = \frac{a}{b} \text{ and } b \neq 0$$

Now we know that this is a universal statement, so we need to let z be fixed but arbitrary and then show that we can choose a and b appropriately.

> *Proof.* Let x be an arbitrary integer, and choose integers $a = x$ and $b = 1$. Then we have that
>
> $$x = \frac{x}{1} = \frac{a}{b}$$
>
> so x is a rational number, by definition. □

Example 4.3.3

Prove or disprove:

Given any rational number x, there is an integer y for which xy is an integer.

Symbolically, this statement is

$$\forall x \in \mathbb{Q}, \exists y \in \mathbb{Q}, \text{ such that } xy \in \mathbb{Z}$$

which means that x is arbitrary and we get to choose y (in a way that probably relies on x).

> *Proof.* Let x be an arbitrary rational number. By definition, we can write $x = \frac{a}{b}$ where $a, b \in \mathbb{Z}$ and $b \neq 0$. Choose $y = b$. With this choice, we have that
>
> $$xy = \left(\frac{a}{b}\right)(b) = \frac{a}{1} = a$$
>
> and a is an integer, whence xy is an integer. □

Alternate proof idea.

> *Proof.* Let x be an arbitrary rational number and choose $y = 0$. Then we have that $xy = x(0) = 0$ and since 0 is an integer, xy is an integer. □

Example 4.3.4

Proe or disprove:

The irrational numbers are closed under addition.

Symbolically, this statement is

$$\forall x \in \mathbb{R} - \mathbb{Q}, \forall y \in \mathbb{R} - \mathbb{Q}, x - y \in \mathbb{R} - \mathbb{Q}$$

> *Disproof.* Choose $x = \pi$ and $y = -\pi$, two irrational numbers. Then $x + y = \pi - \pi = 0$, an integer, hence we've found a counterexample to the claim. □

4.4 Direct Proof and Counterexample IV: Divisibility

Definition: divides

Let n, d be integers. We say that d **divides** m if $d \neq 0$ and there exists some integer k for which $n = dk$. Notationally, we write this as $d \mid n$.

Remark. Do not confuse the "divides" sign with the fraction. $d \mid n$ is equivalent to saying that $\frac{n}{d}$ is an integer.

Remark. If $d \mid n$, we may also say

- n is **divisible** by d.
- n is a **multiple** of d.
- d is a **divisor** of n.
- d is a **factor** of n.

Example 4.4.1

Prove or Disprove:

Let a, b, c be integers. If $a|b$ and $a|c$, then $a|(b+c)$.

Proof. Let a, b, c be arbitrary integers and suppose both that $a|b$ and $a|c$. By definition of divisibility, we must have that a is nonzero and that there are integers k, ℓ for which

$$b = ak \quad \text{and} \quad c = a\ell.$$

By routine algebraic manipulation, we see that

$$b + c = ak + a\ell = a(k + \ell)$$

and we note that $k + \ell$ is an integer since $\mathbb{Z}$ is closed under addition. Since $a \neq 0$, then we must have that $a|(b+c)$. □

Example 4.4.2

Prove or Disprove:

Let a, b, c be integers. If $a|(b+c)$, then $a|b$ and $a|c$.

Disproof. □

Example 4.4.3

Prove or Disprove:

Let a, b, c be integers. If $a|b$ and $a|(b+c)$, then $a|c$.

Proof. □

Example 4.4.4

Prove or Disprove:

Let a, b, c be integers. If $a|b$ and $b|c$, then $a|bc$.

Proof. □

Example 4.4.5

Prove or Disprove:

Let a, b, c be integers. If $a|bc$, then $a|b$ and $a|c$.

Disproof. □

Example 4.4.6

Prove or Disprove:

Let a, b, c be integers. If $a|b$ and $a|bc$, then $a|c$.

Disproof. □

Example 4.4.7: Easy Test for Division by 9

Prove or Disprove:

If a number n's digits sum to a multiple of 9, then n is divisible by 9.

To prove this, we will have to appeal to the following result, whose proof will be reserved for a later section.

Lemma ??

For any positive integer m, $10^m - 1$ is divisible by 9.

Proof. Let n be the $k+1$-digit number "$a_k a_{k-1} \cdots a_2 a_1 a_0$", by which we mean that

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_2 10^2 + a_1 10 + a_0. \tag{1}$$

Through routine algebraic manipulation (which we've tried to color-code for simplicity for the reader) Equation (1) can be rewritten as

$$\begin{aligned} n &= a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0 && (2) \\ &= a_k + a_k(10^k - 1) + a_{k-1} + a_{k-1}(10^{k-1} - 1) + \cdots + a_1 + a_1(10 - 1) + a_0 && (3) \\ &= a_k(10^k - 1) + a_{k-1}(10^{k-1} - 1) + \cdots + a_1(10 - 1) + (a_k + a_{k-1} + \cdots + a_1 + a_0) && (4) \end{aligned}$$

and Lemma **??** guarantees the existence of integers $m_1, \ldots, m_k$ for which Equation (4) becomes

$$\begin{aligned} n &= (a_k + a_{k-1} + \cdots + a_1 + a_0) + a_k(9m_k) + a_{k-1}(9m_{k-1}) + \cdots + a_1(9m_1) && (5) \\ &= 9(a_k 9m_k) + 9(a_{k-1}m_{k-1}) + \cdots + 9(a_1 m_1) + (a_k + a_{k-1} + \cdots + a_1 + a_0) && (6) \end{aligned}$$

At long last, we now suppose that $a_k + a_{k-1} + \cdots + a_1 + a_0$ is divisible by 9. It follows from the definition that there is some integer m_0 for which

$$a_k + a_{k-1} + \cdots + a_1 + a_0 = 9m_0.$$

By substituting this into Equation (6), we obtain

$$\begin{aligned} n &= 9(a_k m_k) + 9(a_{k-1}m_{k-1}) + \cdots + 9(a_1 m_1) + 9m_0 \\ &= 9(a_k m_k + a_{k-1}m_{k-1} + \cdots + a_1 m_1 + m_0) \end{aligned}$$

As $\mathbb{Z}$ is closed under addition and multiplication, this complicated expression is just 9 times an integer, whence n must be divisible by 9. □

4.7 Indirect Argument: Contradiction and Contraposition

4.7.1 Contradiction

Proof By Contradiction

To prove a claim...

1. Assume instead that the claim is false.
2. Show that this assumption leads logically to a contradiction.
3. Conclude that the claim must actually be true.

Remark. Althought it isn't necessary, it's often polite to clue the reader in on the fact that you're about to prove this by contradiction.

Example 4.7.1: Infinity Integers

Prove the following claim:

There is no largest integer.

> *Proof.* Tending towards a contradiction, suppose that there is a largest integer, call it N. Choose $M = N + 1$, another integer. Then we have that $M > N$. But since N was assumed to be the largest, then we also have that $N \geq M$. Clearly N cannot be the largest and not the largest integer.
>
> $$N \geq M > N + 1$$
>
> Ridiculous. Contradiction.
> Therefore there is no largest integer. □

Example 4.7.2

Prove the following claim:

The sum of any nonzero rational number and irrational number is irrational.

4.7.2 Contraposition

Proof By Contraposition

To prove a claim...

1. Express the statement as $\forall x \in D$, $P(x) \Rightarrow Q(x)$.
2. Write the contrapositive statement $\forall x \in D$, $\neg Q(x) \Rightarrow \neg P(x)$.
3. Use a direct proof on the contrapositive.
4. Conclude that the claim must actually be true by logical equivalence of the contrapositive.

Example 4.7.3

Prove the following claim:

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

Notice that the contrapositive is: For all integers n, if n is odd, then n^2 is odd. That proof seems to write itself.

Proof. We approach via contraposition. Let n be an arbitrary integer and suppose that n is odd. Then there is some integer k for which $n = 2k + 1$. Then

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

Since $2k^2 + 2k$ is an integer, then n^2 is odd.
This verifies the claim. □

We want to prove that $\sqrt{2}$ is irrational. However, the proof of this is somewhat involved. First we'll prove a smaller result whose proof is a bit technical. In doing so, we'll make the proof of the square root of 2 much easier.

Lemma 4.7.4

For every rational number x, there exist integers a, b with $b \neq 0$ and a, b not both even such that $x = \dfrac{a}{b}$.

Proof. Let x be an arbitrary rational number. We have three cases: $x = 0$, $x > 0$, and $x < 0$. Since $0 = \frac{0}{1}$, the first case is obvious. We now prove only the case that $x > 0$, noting that the proof of the negative case follows identically by replacing x with $-x$.
Suppose that x is positive. There are integers k_0, ℓ_0 with $\ell_0 \neq 0$ such that

$$x = \frac{k_0}{\ell_0}$$

We may presume that k_0, ℓ_0 are both positive. If they were both negative, we could take $x = \frac{-k_0}{-\ell_0}$ and continue with the remainder of the proof.
If k_0, ℓ_0 are not both even choose $a = k_0$ and $b = \ell_0$. If k_0, ℓ_0 are both even, then there are integers k_1, ℓ_1 such that

$$\begin{aligned} k_0 &= 2k_1 && \text{where } 1 \leq k_1 < k_0 \\ \ell_0 &= 2\ell_1 && \text{where } 1 \leq \ell_1 < \ell_0 \end{aligned}$$

and thus

$$x = \frac{k_0}{\ell_0} = \frac{2k_1}{2\ell_1} = \frac{k_1}{\ell_1}.$$

If k_1, ℓ_1 are not both even, then we choose $a = k_1$ and $b = \ell_1$. If k_1, ℓ_1 are both even, then there are integers k_2, ℓ_2 such that

$$\begin{aligned} k_1 &= 2k_2 && \text{where } 1 \leq k_2 < k_1 < k_0 \\ \ell_1 &= 2\ell_2 && \text{where } 1 \leq \ell_2 < \ell_1 < \ell_0 \end{aligned}$$

and thus

$$x = \frac{k_0}{\ell_0} = \frac{k_1}{\ell_1} = \frac{2k_2}{2\ell_2} = \frac{k_2}{\ell_2}.$$

If k_1, ℓ_1 are not both even, then we choose $a = k_1$ and $b = \ell_1$. If k_1, ℓ_1 are both even, then we repeat this procedure. As there are only finitely many integers x, y satisfying $1 \leq x < k_0$ and $1 \leq y < \ell_0$, this procedure must terminate after only finitely-many steps. Suppose the n^{th} step is the terminal step. Then we have that there exist integers a, b such that

$$\begin{aligned} k_n &= 2a && \text{where } 1 \leq a < k_n < k_{n-1} < \cdots < k_2 < k_1 < k_0 \\ \ell_n &= 2b && \text{where } 1 \leq b < \ell_n < \ell_{n-1} < \cdots < \ell_2 < \ell_1 < \ell_0 \end{aligned}$$

and thus

$$x = \frac{k_0}{\ell_0} = \frac{k_1}{\ell_1} = \cdots = \frac{k_{n-1}}{\ell_{n-1}} = \frac{k_n}{\ell_n} = \frac{a}{b}.$$

As n was chosen to represent the last step in this repeating procedure, we must have that a, b are not both even, as desired. □

Example 4.7.5: Irrationality of $\sqrt{2}$

Prove the following claim:

$\sqrt{2}$ is irrational.

Proof. Seeking a contradiction, suppose that $\sqrt{2}$ is rational. Then, from Lemma 4.7.4 there are integers a, b with $b \neq 0$ and a, b not both even such that

$$\sqrt{2} = \frac{a}{b}$$

Squaring both sides of this equation yields

$$2 = \frac{a^2}{b^2}$$

and rearranging produces

$$b^2 = 2a^2 \tag{7}$$

whence we see that b^2 is even. By Example 4.7.3, it follows that b is an even number, and thus Lemma 4.7.4 implies that a is odd.
Since b is even, there is some integer k for which $b = 2k$. Substituting this into Equation 7, we get

$$\begin{aligned} (2k)^2 &= 2a^2 \\ 4k^2 &= 2a^2 \\ 2k^2 &= a^2 \end{aligned}$$

and thus a^2 is even. By Example 4.7.3, it follows that a is an even number, which contradicts the fact that a was odd.
Therefore, we conclude that $\sqrt{2}$ is, in fact, irrational. □

Example 4.7.6

Prove or disprove the following claim:

$$7p + 21q = 1 \text{ for some integers } p \text{ and } q.$$

Disproof. The claim is false - there are no integers p, q for which $7p + 21q = 1$. To see this, suppose to the contrary that there are integers p, q for which this is true. Then we have that

$$1 = 7p + 21q = 7(p + 3q).$$

As $p + 3q$ is an integer, then 7 must divide 1. But this contradicts the previously-proven fact that all divisors of 1 must be less than (or equal to) 1. □

5 Sequences, Mathematical Induction, and Recursion

5.1 Sequences

One of the most important tasks in mathematics is to recognize and categorize regular patterns.

Definition: sequence, index

A **sequence** is an ordered list of objects (or events):

$$a_1, a_2, .., a_k$$

Each individual element a_k is called a **term**. The k in "a_k" is called the **index** and indicates its position in the sequence. Notationally, we often write $\{a_n\}_{n=1}^{k}$ or $(a_n)_{n=1}^{k}$ to denote a sequence.

Remark. Note that a sequence's index doesn't have to start at 1 (in computer science, these often start at 0). One can always perform a **index shift** to rewrite a sequence starting at $k = 1$, so there's not loss of generality in using this convention.

Definition: T

he number of ordered elements in a sequence is called its **length**. An infinite sequence has an initial term, but continues indefinitely having no final term. A finite sequence has a final term a_m, where m is some natural number.

Definition: explicit formula

An **explicit formula** or **general formula** for a sequence $\{a_n\}$ is a rule that shows how the value of a_k depends on k.

Example 5.1.1

Write the first four terms of the following sequences.

1. The sequence $\{a_k\}$ where $a_k = \dfrac{k}{10+k}$ for all integers $k \geq 1$.
2. The sequence $\{b_j\}$ where $b_j = \dfrac{5-j}{5+j}$ for all integers $j \geq 3$.
3. The sequence $\{c_i\}$ where $c_i = \dfrac{(-1)^i}{3^i}$ for all integers $i \geq 0$.

1.
2.
3.

Remark. The third sequence above is known as an **alternating sequence**.

Example 5.1.2

Given the first few terms of the sequence, find an explicit formula for it.

1. The sequence $\{a_n\}_{n=0}^{\infty}$ given by $1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}, \frac{1}{32}, \frac{1}{64}, \ldots$

2. The sequence $\{b_j\}_{n=1}^{\infty}$ given by $1, 4, 9, 16, 25, 36, 49, 64, \ldots$

1. $a_n = \frac{1}{2^n}$
2. $b_j = j^2$

Definition: sum of a sequence

If m and n are integers and $m \leq n$, the symbol $\displaystyle\sum_{k=m}^{n} a_k$ is the **sum** of all terms from a_m to a_n. That is,

$$\sum_{k=m}^{n} a_k = a_m + a_{m+1} + ... + a_n.$$

Remark. It's important to observe that one can rewrite sums by "splitting off" some number of terms.

$$a_m + \left(\sum_{k=m+1}^{n} a_k\right) = \sum_{k=m}^{n} a_k = \left(\sum_{k=m}^{n-1} a_k\right) + a_n.$$

This strategy may come in handy when we get to induction.

Example 5.1.3

Calculate the following:

1. $\displaystyle\sum_{k=0}^{3} \frac{1}{2^k}$
2. $\displaystyle\sum_{j=1}^{2} \frac{(-1)^j}{j+1}$

1. $\displaystyle\sum_{k=0}^{3} \frac{1}{2^k} = \frac{1}{2^0} + \frac{1}{2^1} + \frac{1}{2^2} + \frac{1}{2^3} = 1\frac{7}{8} = \frac{15}{8}.$
2. $\displaystyle\sum_{j=1}^{2} \frac{(-1)^j}{j+1} =$

Definition: product of a sequence

If m and n are integers and $m \leq n$, the symbol $\displaystyle\prod_{k=m}^{n} a_k$ is the **product** of all terms from a_m to a_n. That is,

$$\prod_{k=m}^{n} a_k = a_m \cdot a_{m+1}.$$

Example 5.1.4

Calculate the following:

1. $\displaystyle\prod_{k=0}^{3} \frac{1}{2^k}$
2. $\displaystyle\prod_{j=1}^{2} \frac{(-1)^j}{j+1}$

1. $\displaystyle\prod_{k=0}^{3} \frac{1}{2^k} = \frac{1}{2^0} \cdot \frac{1}{2^1} \cdot \frac{1}{2^2} \frac{1}{2^3} = \frac{1}{2^6} = \frac{1}{64}$
2. $\displaystyle\prod_{j=1}^{2} \frac{(-1)^j}{j+1} =$

Definition: factorial

For each positive integer n, the quantity n **factorial**, denoted $n!$, is defined to be the product of all integers from 1 to n:

$$n! = n \cdot (n-1) \cdot (n-2) ... 3 \cdot 2 \cdot 1,$$

where we define $0! = 1$.

Example 5.1.5

Simplify the following expressions.

1. $\dfrac{5!}{2!3!}$
2. $\dfrac{(n+1)!}{n!}$
3. $\dfrac{n!}{(n-3)!}$
4. $n + \dfrac{(n-1)}{2!} + \dfrac{(n-2)}{3!} + \dfrac{(n-3)}{4!} + ... + \dfrac{1}{n!}$

1. $\dfrac{5!}{2!3!} = \dfrac{1 \cdot 2 \cdot 2 \cdot 3 \cdot 4 \cdot 5}{1 \cdot 2 \cdot 1 \cdot 2 \cdot 3} = \dfrac{4 \cdot 5}{1 \cdot 2} = 10$
2. $\dfrac{(n+1)!}{n!} = n$
3. $\dfrac{n!}{(n-3)!} = n(n-2)(n-1)$
4. $n + \dfrac{(n-1)}{2!} + \dfrac{(n-2)}{3!} + \dfrac{(n-3)}{4!} + ... + \dfrac{1}{n!} =$

Writing Sequences and Summations Explicitly

Example 5.1.6

Condense the following using notation from above.

1. $1, -\frac{1}{4}, \frac{1}{9}, -\frac{1}{16}, \frac{1}{25}, -\frac{1}{36}$
2. $\left(\frac{1}{n}\right)\left(\frac{2}{n+1}\right)\left(\frac{3}{n+2}\right)\cdots\left(\frac{n+1}{2n}\right)$
3. The sum of the first n odd integers
4. The sum of the first $n^2 - 1$ factorials (starting with 1!)

1. $\{a_n\}_{n=1}^{\infty}$ where $a_n = (-1)^{n+1}\frac{1}{n^2}$
2. $\displaystyle\prod_{k=0}^{n} \frac{k+1}{n+k}$
3. $\displaystyle\sum_{k=0}^{n-1} 2k+1$
4. $\displaystyle\sum_{k=1}^{n^2-1} k!$

5.2 Mathematical Induction I: Proving Formulas

Definition: Principle of Mathematical Induction

Let $P(n)$ be a predicate that is defined for integers n, and let N_0 be a fixed integer. Suppose the following two statements are true.

1. $P(N_0)$ is true.
2. For all integers $k \geq N_0$, if $P(k)$ is true, then $P(k+1)$ is true.

Then $P(n)$ is true for all $n \geq N_0$.

Proof By Induction

Consider a statement of the form

For every integer $n \geq N_0$, the property $P(n)$ is true.

To show this

1. [Base Step] Show that $P(N_0)$ is true.
2. [Inductive Step] Show that, for every integer $k \geq N_0$, if $P(k)$ is true, then $P(k+1)$ is true. Notice that this is a standard universal conditional. So to actually do it:
    - Let k be an arbitrary integer with $k \geq N_0$.
    - Suppose $P(k)$ is true (this is the "induction hypothesis").
    - Deduce that $P(k+1)$ must be true.

Example 5.2.1: Sum of the first n integers.

Show that, for every $n \geq 1$,

$$\sum_{i=1}^{n} i = 1 + 2 + 3 + 4 + \cdots + n = \frac{n(n+1)}{2}$$

First we identify the predicate $P(n)$ as meaning

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

. The base case will be to verify that $P(1)$ is true. When we get to the induction step, we keep in mind that we want to see that $P(k+1)$ is true:

$$\sum_{i=1}^{k+1} i = \frac{(k+1)(k+2)}{2}$$

.

Proof. Let the property $P(n)$ be the equation

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

.

Base Step. To see that $P(1)$ is true, note that the left-hand side of the equation is 1 and the right-hand side is $\frac{1(1+1)}{2} = \frac{2}{2} = 1$. Hence $P(1)$ is true.

Inductive Step. Let k be an arbitrary integer with $k \geq 1$. Suppose that $P(k)$ is true, that is

$$\sum_{i=1}^{k} i = 1 + 2 + 3 + 4 + \cdots + k = \frac{k(k+1)}{2}.$$

Now, we have that

$$\begin{aligned}
\sum_{i=1}^{k+1} &= 1 + 2 + 3 + 4 + \cdots + k + (k+1) \\
&= \left(\sum_{i=1}^{k} i\right) + (k+1) \\
&= \frac{k(k+1)}{2} + (k+1) && \text{(apply induction hypothesis)} \\
&= \frac{k(k+1)}{2} + \frac{2(k+1)}{2} \\
&= \frac{(k+1)(k+2)}{2}
\end{aligned}$$

hence $P(k+1)$ is true.

Therefore $P(n)$ holds for all $n \geq 1$. □

Example 5.2.2: Sum of a geometric sequence.

Let a, r be real numbers with $r \neq 1$. A **geometric sequence** is a sequence of the form

$$\{a, ar, ar^2, ar^3, ar^4, \ldots\}$$

Show that, for every $n \geq 0$,

$$\sum_{i=0}^{n} ar^i = \frac{a(1 - r^{n+1})}{1 - r}$$

Scratch Work.

First we identify the predicate $P(n)$ as meaning

$$\sum_{i=0}^{n} ar^i = a + ar + ar^2 + ar^3 + \cdots + ar^n = \frac{a(1 - r^{n+1})}{1 - r}$$

The base case will be to verify that $P(0)$ is true. When we get to the induction step, we keep in mind that we want to see that $P(k+1)$ is true:

$$\sum_{i=0}^{k+1} ar^i = \frac{a(1+r^{k+2})}{(1-r)}.$$

Proof. Let $P(n)$ denote the equation

$$\sum_{i=0}^{n} ar^i = a + ar + ar^2 + ar^3 + \cdots + ar^n = \frac{a(1-r^{n+1})}{1-r}$$

Base Step. To see that $P(0)$ is true, note that the left-hand side of the equation is a and the right-hand side is $\frac{a(1-r^{0+1})}{1-r} = a$.

Inductive Step. Let k be an arbitrary integer with $k \geq 0$. Suppose that $P(k)$ is true, that is

$$\sum_{i=0}^{k} ar^i = \frac{a(1-r^{k+1})}{1-r}.$$

Now, we have that

$$\begin{aligned}
\sum_{i=0}^{k+1} ar^i &= a + ar + ar^2 + ar^3 + \cdots + ar^k + ar^{k+1} \\
&= \left(\sum_{i=0}^{k} ar^i\right) + ar^{k+1} \\
&= \frac{a(1-r^{k+1})}{1-r} + ar^{k+1} && \text{(apply induction hypothesis)} \\
&= \frac{a(1-r^{k+1})}{1-r} + \frac{ar^{k+1}(1-r)}{1-r} \\
&= \frac{a(1-r^{k+1})}{1-r} + \frac{a(r^{k+1}-r^{k+2})}{1-r} \\
&= \frac{a(1-r^{k+1}+r^{k+1}-r^{k+2})}{1-r} \\
&= \frac{a(1-r^{k+2})}{1-r}
\end{aligned}$$

hence $P(k+1)$ is true.
Therefore $P(n)$ holds for all $n \geq 0$. □

Example 5.2.3: Sum of the first n odd integers

Prove that, for every $n \geq 1$,

$$\sum_{i=1}^{n} (2i-1) = 1 + 3 + 5 + \cdots + (2n-1) = n^2.$$

Proof. Let $P(n)$ denote the equation

$$\sum_{i=1}^{n}(2i-1) = 1+3+5+\cdots+(2n-1) = n^2.$$

Base Step. To see that $P(1)$ is true, note that the left-hand side of this equation is $2(1)-1=1$ and the right-hand side of the equation is $(1)^2=1$.
Inductive Step. Let k be an arbitrary integer with $k \geq 1$. Suppose that $P(k)$ is true, that is

$$\sum_{i=1}^{k}(2i-1) = k^2.$$

Now, we have that

$$\begin{aligned}
\sum_{i=1}^{k+1}(2i-1) &= 1+3+5+\cdots+(2k-1)+(2(k+1)-1) \\
&= \left(\sum_{i=1}^{k}(2i-1)\right)+(2(k+1)-1) \\
&= k^2+(2(k+1)-1) && \text{(apply induction hypothesis)} \\
&= k^2+2k+1 \\
&= (k+1)^2
\end{aligned}$$

hence $P(k+1)$ is true.
Therefore $P(n)$ holds for all $n \geq 1$. □

5.3 Mathematical Induction II: Application

Example 5.3.1: Proving Divisibility

Prove that $n^3 - n$ is divisible by 3 for all positive integers n.

Proof. Let $P(n)$ denote the statement

$$n^3 - n \text{ is divisible by } 3.$$

Base Step. To see that $P(1)$ is true, note that $(1)^3 - 1 = 1 - 1 = 0$ and 0 is divisible by any nonzero number.
Inductive Step. Let k be an arbitrary integer with $k \geq 1$. Suppose that $P(k)$ is true, that is

$$k^3 - k \text{ is divisible by } 3.$$

By definition of divisilibty, this means that there exists an integer ℓ such that $k^3 - k = 3\ell$. Now, we have that

$$\begin{aligned}
(k+1)^3 - (k+1) &= (k^3 + 3k^2 + 3k + 1) - (k+1) \\
&= k^3 + 3k^2 + 3k - k \\
&= k^3 - k + 3k^2 + 3k \\
&= (k^3 - k) + 3k^2 + 3k \\
&= 3\ell + 3k^2 + k && \text{(apply induction hypothesis)} \\
&= 3(\ell + k^2 + k)
\end{aligned}$$

and so this quantity is divisible by 3. Thus $P(k+1)$ is true.
Therefore $P(n)$ is true for all $n \geq 1$. □

Exercise 5.3.2

For any positive integer n, $10^n - 1$ is divisible by 9.

Example 5.3.3: Proving Inequalities

$n! > 2^n$ for all integers $n \geq 4$.

Proof. Let the property $P(n)$ be the inequality

$$n! > 2^n.$$

Base Step. To see that $P(4)$ is true, note that $4! = 24 > 16 = 2^4$.
Inductive Step. Let k be an arbitrary integer with $k \geq 4$. Suppose that $P(k)$ is true, that is

$$k! > 2^k.$$

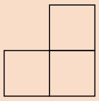
We'll also remark that, since $k \geq 4$, then of course $k + 1 \geq 3 > 2$. Now we have that

$$\begin{aligned} (k+1)! &= (k!)(k+1) \\ &> 2^k(k+1) && \text{(apply induction hypothesis)} \\ &> 2^k(2) && \text{(by our remark)} = 2^{k+1} \end{aligned}$$

hence $P(k + 1)$ is true.
Therefore, $P(n)$ is true for all $n \geq 4$. □

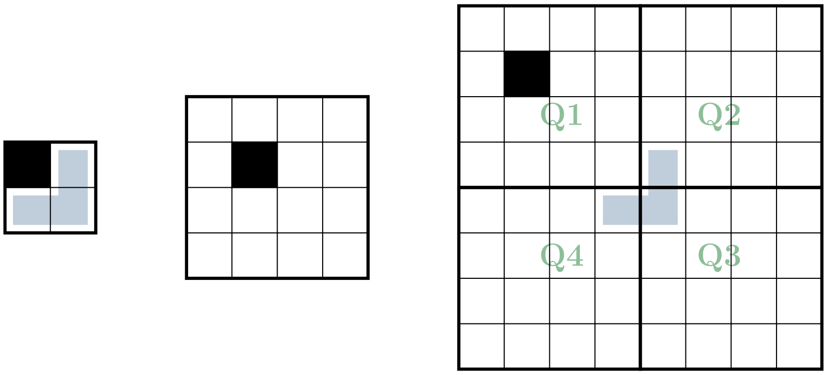
Example 5.3.4: Covering a Board with L-Shaped Trominoes

An **L-shaped tromino** is comprised of three squares arranged in an L-shape, like so:



Show that, for all integers $n \geq 1$, any $2^n \times 2^n$ checkerboard with one square removed can be covered by L-shaped trominoes.

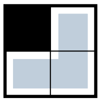
Scratch work



Proof. Let $P(n)$ be the property

Any $2^n \times 2^n$ checkerboard with one square removed can be covered by L-shaped trominoes.

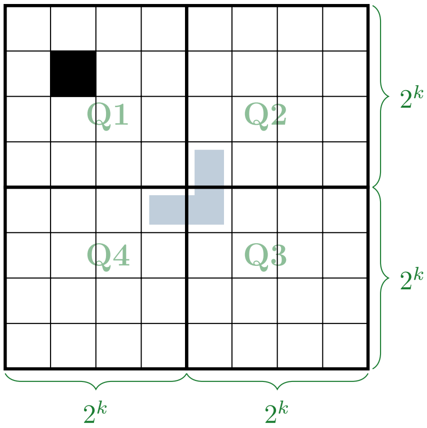
Base Step. To see that $P(1)$ is true,



Inductive Step. Let k be an arbitrary integer with $k \geq 1$. Suppose that $P(k)$ is true, that is

Any $2^k \times 2^k$ checkerboard with one square removed can be covered by L-shaped trominoes.

Consider a $2^{k+1} \times 2^{k+1}$ checkerboard with one square removed. Notice that this checkerboard is comprised of four $2^k \times 2^k$ checkerboards. Let **Q1** the quadrant containing the missing square and label the other quadrants **Q2**, **Q3**, **Q4**. By the induction hypothesis, quadrant **Q1** can be covered by L-shaped trominoes. Now place an L-shaped tromino so that one square lies in each of the remaining quadrants **Q2**, **Q3**, **Q4** (see figure below).



In this way, the uncovered tiles form three more $2^k \times 2^k$ checkerboards, each with a single square removed. Applying the induction hypothesis to each of these quadrants, we must have that all of **Q2**, **Q3**, **Q4** can be covered by L-shaped trominoes. That is to say, $P(k+1)$ is true.

Therefore $P(n)$ is true for every integer $n \geq 1$. □

5.4 Strong Mathematical Induction and the Well-Ordering Principle for the Integers

Definition: Principle of Strong Mathematical Induction

Let $P(n)$ be a predicate that is defined for integers n, and let N_0, N_1 be fixed integers with $N_0 \leq N_1$. Suppose the following two statements are true.

1. $P(N_0), P(N_0+1), P(N_0+2), \ldots, P(N_1)$ are true.
2. For all integers $k \geq N_1$, if $P(N_0), P(N_0+1), \ldots, P(N_1), \ldots, P(k)$ are true, then $P(k+1)$ is true.

Then $P(n)$ is true for all $n \geq N_0$.

In words, the "base step" is possibly actually a finite number of cases (not just a singular case), and the "inductive step" requires that *all* preceding cases (from the basis steps onward) are true. In practice, you may not actually need to use all preceding cases to verify the inductive step.

Theorem 5.4.1: Divisibility by Primes

Any integer greater than 1 is divisible by a prime.

The strategy is this: if a number is composite, then it is the product of two numbers that are smaller, so as long as one of those numbers is divisible by a prime, then this composite number will be as well.

Proof. Let n be an arbitrary integer and let $P(n)$ be the predicate "n is divisible by a prime."
Base step. Since $N_0 = N_1 = 2$ is prime, then N_0 is divisible by 2. Hence $P(N_0)$ is true.
Inductive step. Let $k \geq 2$ be some integer an suppose that $P(2)$, $P(3)$, $\ldots$, $P(k)$ are all true. We have two cases for $k+1$:

($k+1$ is prime). If $k+1$ is prime, then $k+1$ is divisible by itself, hence $P(k+1)$ is true.

($k+1$ is composite). If $k+1$ is composite, then there are two integers, a, b for which $k = ab$ and $1 \leq a \leq k$ and $1 \leq b \leq k$. By the inductive hypothesis, a (and b) is divisible by a prime p. Since $p|a$ implies that $p|(ab)$, then $p|k+1$, hence $P(k+1)$ is true.

□

Example 5.4.2: Recursive Sequence/Explicit Sequence

Let $\{a_n\}_{n=0}^{\infty}$ be the recursively-defined sequence

$$a_0 = 0,\ a_1 = 4,$$
$$\text{and } a_n = 6a_{n-1} - 5a_{n-2} \text{ for all } n \geq 2.$$

Show that, for all $n \geq 0$, $a_n = 5^n - 1$.

For scratch, we compute the first few terms of the sequence to confirm:

$$\begin{aligned}
a_0 &= 0 = 5^0 - 1\\
a_1 &= 4 = 5^1 - 1\\
a_2 &= 6a_1 - 5a_0 = 6(4) - 5(0) = 24 = 5^2 - 1\\
a_3 &= 6a_2 - 5a_1 = 6(24) - 5(4) = 124 = 5^3 - 1\\
a_4 &= 6a_3 - 5a_2 = 6(124) - 5(24) = 624 = 5^4 - 1
\end{aligned}$$

The claim seems reasonable. Since the recursive sequence begins with two terms, our base case should reflect this similarly: using $N_0 = 0, N_1 = 1$.

Proof. Let n be an arbitrary natural number, $\{a_n\}$ the recursive sequence defined above, and let $P(n)$ be the predicate "$a_n = 5^n - 1$."
Base steps. Take $N_0 = 0$ and $N_1 = 1$. We see that

$$a_{N_0} = a_0 = 0 = 5^0 - 1 \qquad \text{and} a_{N_1} = 4 = 5^1 - 1$$

hence $P(N_0)$ and $P(N_1)$ are true.
Inductive step. Let $k \geq 1$ and suppose that $P(0), P(1), \ldots, P(k)$ are all true, that is $a_j = 5^j - 1$ for $j = 0, 1, \ldots, k$. We then have that

$$\begin{aligned} a_{k+1} &= 6a_k - 5a_{k-1} \\ &= 6(5^k - 1) - 5(5^{k-1} - 1) \\ &= 6(5^k) - 6 - 5^k + 5 \\ &= 5(5^k) - 1 \\ &= 5^{k+1} - 1. \end{aligned}$$

Therefore $P(k+1)$ is true. □

5.4.1 Well-Ordering Principle for the Integers

Well-Ordering Principle

Let N_0 be a fixed integer and let S be a nonempty set of integers, all of which are greater than N_0. Then S has a least element.

Theorem 5.4.3: Quotient–Remainder Theorem (Existence)

Given any integer n and any positive integer d, there exist integers q, r such that

$$n = dq + r \qquad \text{and} \qquad 0 \leq r < d.$$

Proof. Let n be an arbitrary, but fixed, integer and let d be an arbitrary, but fixed, positive integer. Let S be the set of all *nonnegative* integers of the form $n - dk$ where k is an integer. To be clear about the notation, S is the nonnegative integers among

$$\{\ldots, n - d(-2), n - d(-1), n - d(0), n - d(1), n - d(2), \ldots\}.$$

We note that S is nonempty: If $n \geq 0$, then $n - d(0) = n \geq 0$. If $n < 0$, then $n - d(n) = n(1 - d) \geq 0$. So, since S contains only integers greater than or equal to 0, then by the well-ordering principle, there must be a least integer $r \geq 0$ within this set, which corresponds to a specific integer q satisfying

$$r = n - dq \implies n = dq + r.$$

Now we only need to verify that $r < d$. To the contrary, assume instead that $r \geq d$. We have that$r > r - d \geq 0$. Then

$$r - d = n - dq - d = n - d(q + 1)$$

and so $r - d$ is an element of S which is smaller that r, contradicting that r was the least element of S. Therefore, $r < d$. □

5.6 Defining Sequences Recursively

Definition: recursive sequence

A **recurrence relation** for a sequence $\{a_n\}$ is a formula that relates each term a_k to certain predecessorts a_{k-1}, a_{k-2}, etc.

Example 5.6.1: Fibonacci Sequence

Let $\{F_n\}_{n=0}^{\infty}$ be the infinite recursive sequence defined by

$$\begin{array}{ll} F_0 = 0,\ F_1 = 1 & \text{(the initial conditions) and} \\ F_k = F_{k-1} + F_{k-2} \text{ for } k \geq 2. & \text{(the recursive formula).} \end{array}$$

Find F_2, F_3, F_4

Example 5.6.2

Define a sequence $b_0, b_1, b_2, ..$ recursively as follows:

$$\begin{array}{ll} b_0 = 2 & \text{(the initial condition) and} \\ b_k = 1 - (b_{k-1})^k \text{ for } k \geq 1 & \text{(the recursive formula).} \end{array}$$

Find b_1, b_2, b_3.

$$b_1 = 1 - (b_0)^1 = 1 - 2^1 = 1 - 2 = -1$$
$$b_2 = 1 - (b_1)^2 = 1 - (-1)^2 = 1 - 1 = 0$$
$$b_3 = 1 - (b_2)^3 = 1 - (0)^3 = 1 - 0 = 1$$

6 Set Theory

6.1 Set Theory: Definitions and the Element of Proof

Definition: set,element

A **set** is an unordered list of items, called **elements**. If A is a set and a is an element of the set, we write $a \in A$. If a is not an element of the set, we write $a \notin A$.

Remark. An element of a set cannot appear twice.

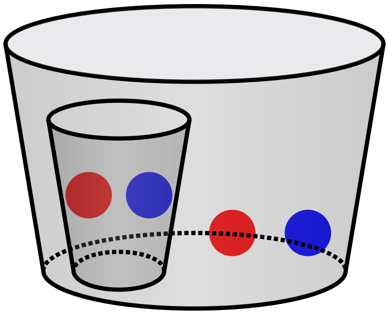
We typically write a set using curly braces and listing the elements.

Example 6.1.1

Examples of sets.

1. $S = \{1, 3, 19\}$
2. *[The natural numbers]* $\mathbb{N} = \{0, 1, 2, 3, 4, 5, \ldots\}$
3. *[The empty set]* $\emptyset = \{\}$
4. $T = \{1, 2, \{1, 2\}\}$

The last example above appears to violate the remark that an element cannot appear twice, but in fact the elements of T are 1, 2, and $\{1, 2\}$. *A set can be an element of another set* (but we musn't be naïve – there famously cannot be a set containing all sets). You can make sense of this by thinking about a situation in which one is carrying a bucket of balls, and within that bucket is a smaller container which also contains a couple of balls. If you reach into the large bucket and grab an object at random, you can grab either a ball or a small container.



Sometimes sets are infinite (and writing it out explicitly is impossible) or sometimes sets are finite but we really want to communicate the pattern of the elements within the set.

Definition: set-builder notation

Let X be some set (called the **universe**) and let $P_1(x), P_2(x), \ldots$ be some properties (or predicates). One can define a set A using **set-builder notation**

$$A = \{x \in X \;:\; P_1(x) \text{ is true}, P_2(x) \text{ is true} \ldots\}.$$

This is read

“A is the set of all elements in X such that $P_1(x), P_2(x), \ldots$ are all true” or

$$\text{“}A \text{ is the set of all elements in } X \text{ with properties } P_1(x), P_2(x), \ldots\text{”}$$

Remark. If this feels like a truth set, it's because it is.

Example 6.1.2

Define $P(x) : x$ is prime, $Q(x) : x < 20$, and $R(x) : x$ is even. Determine the elements of the following sets:

1. $A = \{x \in \mathbb{Z}^+ \mid Q(x)\}$
2. $B = \{x \in \mathbb{Z}^+ \mid P(x) \wedge Q(x)\}$
3. $C = \{x \in \mathbb{Z}^+ \mid P(x) \wedge R(x)\}$

1. $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19\}$
2. $\{2, 3, 5, 7, 11, 13, 17, 19\}$
3. $\{2\}$

Loosely-speaking, the set-builder notation allows us to define a set within a set. Formally, this is called a subset.

Definition: subset

Let A be a set. We say that B is a **subset** of A, denoted $B \subseteq A$, if and only if

$$\forall x \in A, \text{ if } x \in B \text{ then } x \in A$$

A subset B is called a **proper subset** of A, denoted $B \subsetneq A$, if and only if

$$B \subseteq A \text{ and } \exists x \in A \text{ such that } x \notin B.$$

In other words, B is a proper subset of A if and only if B is a subset of A and $B \neq A$.

Remark. There are some competing notations about subsets. Some authors will prefer to make the subset notation look the same as $\leq$ and $<$ notations, using $\subset$ for a proper subset. Others will use $\subset$ for a subset and $\subsetneq$ for a proper subset. We shy away from using the $\subset$ symbol at all because is very similar to the letter C when hand-written.

If we treat A and B as regions of the plane, we can think about a **Venn diagram** which relates these sets.

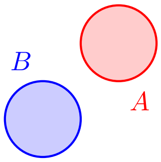


Figure 1: $B \not\subseteq A$ and $A \not\subseteq B$

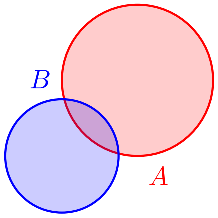


Figure 2: $B \not\subseteq A$ and $A \not\subseteq B$

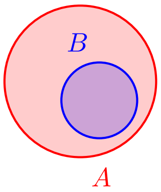


Figure 3: $B \subsetneq A$ and $A \not\subseteq B$

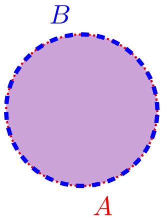


Figure 4: $A \subseteq B$ and $B \subseteq A$

Example 6.1.3

Let $A = \{1, 3, 5, 9\}, B = \{1, 2, 3, 4, 5, 7, 9\}$.

1. Is A a subset of B?
2. Is A a proper subset of B?

1. Yes. Every element of A is also contained in B.

$$\{1, 2, 3, 4, 5, 7, 9\}$$

2. Yes. There are elements of B that are not contained in A.

$$\{1, 2, 3, 4, 5, 7, 9\}$$

For small sets, it is easy to just compare elements explicitly and check whether one is a subset of another. But for large sets – especially ones described in terms of set-builder notation – this can become more complicated. Look at the definition of subset more closely

$$B \subseteq A \iff [\forall x \in A, x \in B \implies x \in A]$$

This yields the following technique

Element Method for Subsets

?? Let A, B be sets. To show that $B \subseteq A$.

1. Suppose $x \in B$, where x is arbitrary.
2. Show that $x \in A$.

Example 6.1.4

For any integer k, we define the set

$$k\mathbb{Z} := \{x \in \mathbb{Z} \ : \ x \text{ is a multiple of } k\}.$$

Show that $6\mathbb{Z} \subseteq 2\mathbb{Z}$.

In order to show that this is true, we need to show that any multiple of 6 is also a multiple of 2.

> *Proof.* Let $x \in \mathbb{Z}$ be arbitrary and suppose that $x \in 6\mathbb{Z}$, i.e., x is a multiple of 6. Then, by definition, there is some integer n for which $x = 6n = 2(3n)$. Since $3n$ is an integer, we see that such an x is also a multiple of 2, and therefore $x \in 2\mathbb{Z}$. □

Figure 4 suggests to us the following definition

Definition

Two sets A and B are said to be **equal** if and only if both are subsets of each other. Symbolically,

$$A = B \iff (A \subseteq B) \wedge (B \subseteq A).$$

Example 6.1.5

Using the notation from Example 6.1.4, let A be the set

$$A = \{x \in \mathbb{Z} \ : \ x \in 2\mathbb{Z} \wedge x \in 3\mathbb{Z}\}.$$

Show that $A = 6\mathbb{Z}$.

Showing $6\mathbb{Z} \subseteq A$. Let x be an arbitrary integer and suppose $x \in 6\mathbb{Z}$. Then by definition $x = 6k$ for some integer k. But $x = 6k = 2(3k)$ showing both that $x \in 2\mathbb{Z}$. Moreover, $x = 6k = 3(2k)$ so $x \in 3\mathbb{Z}$. Therefore $x \in A$ and thus $6\mathbb{Z} \subseteq A$.
[Showing $A \subseteq 6\mathbb{Z}$] Let x be an arbitrary integer and suppose $x \in A$. Then, by definition of A, $x \in 2\mathbb{Z}$ and $x \in 3\mathbb{Z}$. Since $x \in 3\mathbb{Z}$, there is some integer k for which $x = 3k$. Since $x \in 2\mathbb{Z}$, then x is even, and since 3 is not even, it must be that k is even, i.e., that there is an integer ℓ for which $x = 3(2\ell) = 6\ell$. Therefore $x \in 6\mathbb{Z}$ and thus $A \subseteq 6\mathbb{Z}$
Since $A \subseteq 6\mathbb{Z}$ and $6\mathbb{Z} \subseteq A$, then $A = 6\mathbb{Z}$. □

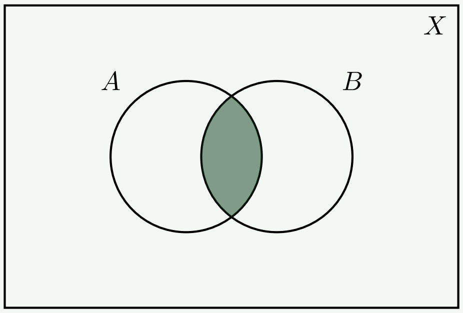
6.1.1 Set Operations

Definition

Let A and B be subsets of the same universal set X.

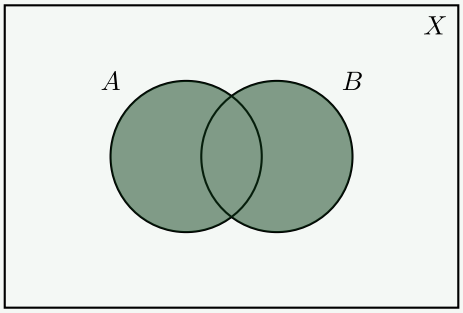
1. The **intersection of** A **and** B, denoted $A \cap B$, is the set of all elements common to both A and B.

$$A \cap B = \{x \in X \ : \ x \in A \text{ and } x \in B\}$$



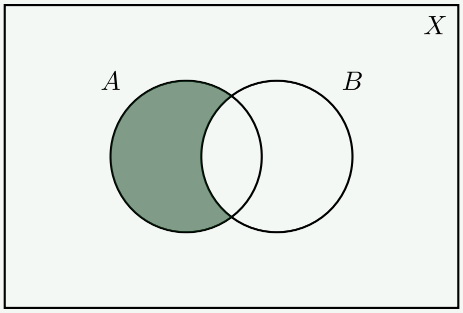
2. The **union of** A **and** B, denoted $A \cup B$, is the set of all elements contained in either A or B.

$$A \cup B = \{x \in X \ : \ x \in A \text{ or } x \in B\}$$



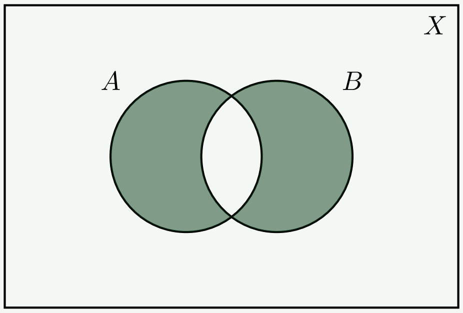
3. The **difference of A minus B** (sometimes called the **relative complement of B in A**), denoted $A - B$, is the set of all elements in A that are not contained in B.

$$A - B = \{x \in X \;:\; x \in A \text{ and } x \notin B\}$$



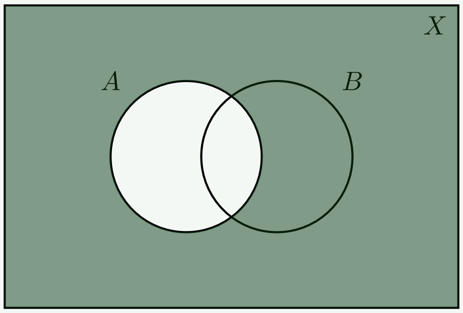
4. The **symmetric difference of A and B**, denoted $A \Delta B$, is the set of all elements in either A or B, but not in both.

$$A \Delta B = \{x \in X \;:\; x \in A \cup B \text{ and } x \notin A \cap B\}$$



5. The **complement of A in X**, denoted A^c, is the set of all elements not in A.

$$A^c = \{x \in X \;:\; x \notin A\}$$



Remark. When taking the union or intersection of a large (possibly infinite) number of sets

$A_1, A_2, \ldots, A_n$, it's common to simplify notation

$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \cdots \cup A_n$$

$$\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \cdots \cap A_n$$

To be completely clear about this notation, if $A_1, \ldots, A_n$ are subsets of the same universe X, then

$$\bigcup_{i=1}^{n} A_i = \{x \in X \ : \ x \in A_1 \vee x \in A_2 \vee \ldots \vee x \in A_n\},$$

$$\bigcap_{i=1}^{n} A_i = \{x \in X \ : \ x \in A_1 \wedge x \in A_2 \wedge \ldots \wedge x \in A_n\}.$$

Example 6.1.6

Let $A = \{1, 2, 3, 4\}$, $B = \{2, 4, 6, 8\}$, $C = \{x \in \mathbb{Z} \mid x \text{ is prime}\}$, and $X = \mathbb{Z}$. Find each of the following:

1. $A \cap C$
2. $B - A$
3. A^c
4. $A^c \cap B$
5. $(A \cap C) \cup B$

1. $A \cap C = \{2, 3\}$
2. $B - A = \{6, 8\}$
3. $A^c = \{\ldots, -3, -2, -1, 0, 5, 6, 7, 8, \ldots\}$
4. $A^c \cap B = \{6, 8\}$
5. $(A \cap C) \cup B = \{2, 3\} \cup B = \{2, 3, 4, 6, 8\}$

Definition: disjoint sets

Two sets A and B are called **disjoint** if and only if they have no elements in common, i.e., if and only if $A \cap B = \emptyset$. A possibly-infinite collection of sets $\{A_1, A_2, \ldots\}$ is said to be **pairwise disjoint** if A_i and A_j are disjoint whenever $i \neq j$.

Definition: partition

Let A be a set and let $\{B_1, B_2, \ldots\}$ be a possibly-infinite collection of *nonempty* subsets of A. This collection is a **partition of** A if and only if

1. The B_i are pairwise disjoint, and
2. $A = \bigcup_{i} B_i$.

Example 6.1.7

Let $A = \{2, 3, 5, 7, 11, 13\}$, $B_1 = \{2, 3, 5\}$, $B_2 = \{7, 11\}$, and $B_3 = \{13\}$. Is $\{B_1, B_2, B_3\}$ a partition of A?

Yes. By inspection, we see that B_1, B_2, B_3 are all mutually disjoint. It is equally straightforward to see that $A = B_1 \cup B_2 \cup B_3$.

Example 6.1.8

Find a partition of $\mathbb{Z}$.

Consider the possible remainders when dividing an integer by 3. The possible options are o, 1, 2. In other words, every integer has one of the following forms:

$$3k, \qquad 3k+1, \qquad \text{or } 3k+2$$

Moreover, after dividing by 3, no integer can have two different remainders, so any integer of the form $3k$ cannot be written as an integer of the form $3k+1$, etc. With this in mind, we defined the following subsets of integers:

$$\begin{aligned} T_0 &= \{n \in \mathbb{Z} \ : n = 3k \text{ for } k \in \mathbb{Z}\} \\ T_1 &= \{n \in \mathbb{Z} \ : n = 3k+1 \text{ for } k \in \mathbb{Z}\} \\ T_2 &= \{n \in \mathbb{Z} \ : n = 3k+2 \text{ for } k \in \mathbb{Z}\} \end{aligned}$$

By our discussion above

1. $T_0 \cap T_1 = T_0 \cap T_2 = T_1 \cap T_2 = \emptyset$
2. $\mathbb{Z} = T_0 \cup T_1 \cup T_2$

and therefore $\{T_0, T_1, T_2\}$ is a partition of $\mathbb{Z}$.

Definition: power set

Given a set A, the **power set of** A, $\mathscr{P}(A)$ is the set of all subsets of A.

Example 6.1.9

Find $\mathscr{P}(A)$ given $A = \{x, y\}$

. The possible subsets of A are $\emptyset, \{x\}, \{y\}, \{x, y\}$. Thus

$$\mathscr{P}(A) = \{\emptyset, \{x\}, \{y\}, \{x, y\}\}.$$

6.1.2 Logic as Set Theory

The definitions of union, intersection, and complements appear to play the roles of $\vee$, $\wedge$, and $\neg$. In fact, the connection is so strong that one can essentially restate the table of logical equivalences in terms of these operations. (Note that the empty set corresponds to a contradiction, and a tautology corresponds to a tautology; which makes sense if one thinks about truth sets).

Theorem 6.1.10

Let P, Q, and R be sets in the same universe X. We then have the following table of set equalities:

Commutative Laws	$P \cap Q = Q \cap P$	$P \cup Q = Q \cup P$
Associative Laws	$(P \cap Q) \cap R) = P \cap (Q \cap R)$	$(P \cup Q) \cup R = P \cup (Q \cup R)$
Distributive Laws	$P \cap (Q \cup R) = (P \cap Q) \cup (P \cap R)$	$P \cup (Q \cap R) = (P \cup Q) \cap (P \cup R)$
Identity Laws	$P \cap X = P$	$P \cup \emptyset = P$
Complement Laws	$P \cup P^c = X$	$P \cap P^c = \emptyset$
Double Complement Laws	$(P^c)^c = P$	
Idempotent Laws	$P \cap P = P$	$P \cup P = P$
Universal Bound Laws	$P \cup X = X$	$P \cap \emptyset = \emptyset$
De Morgan's Laws	$(P \cap Q)^c = P^c \cup Q^c$	$(P \cup Q)^c = P^c \cap Q^c$
Absorption Laws	$P \cup (P \cap Q) = P$	$P \cap (P \cup Q) = P$
Complement of X and $\emptyset$	$X^c = \emptyset$	$\emptyset^c = X$

This set framework ends up being quite a bit more powerful than one might would think. Notice that we can start to come up with a correspondence between some natural numbers and sets:

$$0 \leftrightsquigarrow \emptyset, \qquad 1 \leftrightsquigarrow \{\emptyset\}.$$

Russel and Whitehead, in their *Principia Mathematica* (published in 3 volumes from 1910-1913) famously spend a few hundred pages getting to this point. Their work builds the rest of the natural numbers through the use of a **successor function**, S, as follows: For any natural number n

$$S(n) = n \cup \{n\}$$

What this does is extends the correspondence between $\mathbb{N}$ and sets

$$\begin{aligned}
&0 \leftrightsquigarrow \emptyset \\
&1 \leftrightsquigarrow S(0) = \emptyset \cup \{\emptyset\} = \{\emptyset\} \\
&2 \leftrightsquigarrow S(1) = \{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\} \\
&3 \leftrightsquigarrow S(2) = \{\emptyset, \{\emptyset, \{\emptyset\}\}\} \\
&\vdots
\end{aligned}$$

Moreover, notice the successor function allows us to define “addition” between two natural numbers in a recursive fashion:

$$\begin{aligned} m + 0 &= m \\ m + S(n) &= S(m+n) \end{aligned}$$

For example

$$\begin{aligned} 2 + 2 &= 2 + S(1) \\ &= S(2+1) \\ &= S(2+S(0)) \\ &= S(S(2+0)) \\ &= S(S(2)) \\ &= S(3) \\ &= 4 \end{aligned}$$

So what this shows us is that sets with the union/intersection/complement operations are enough to encode basic logic as well as arithmetic. One of the goals of Russel and Whitehead was to completely formalize set theory and make it the logical basis for all modern mathematics. In a sense, the idea was that every true math statement could be thusly distilled down to set theory wherein it could be proven.

In 1931, work of Godel showed that this logical system actually contains true statements which are unprovable (in fact, any logical system which could encode basic arithmetic suffers from this feature). So Russel and Whitehead were sort of doomed to failure in creating a system which would be able to prove everything. However, they did lay the groundwork for a specific branch of mathematics - Type Theory (which your instructor knows absolutely nothing about, but it’s definitely a thing).

6.2 Properties of Sets

Because subsets are defined by an implication " $\implies$ ", there is a natural ordering to reading statements about them so that we may omit extranneous parentheses. "$A \cap B \subseteq C$" means "$(A \cap B) \subseteq C$".

Proposition 6.2.1: Some Subset Relations

Let A, B be sets (in the same universe). Then

1. $A \cap B \subseteq A$ and $A \cap B \subseteq B$
2. $A \subseteq A \cup B$ and $B \subseteq A \cup B$
3. if $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$
4. [Set Difference Law] $A - B = A \cap B^c$

Proof. We use the Element Method of Proof.

1. Suppose $x \in A \cap B$. Then, $x \in A$ and $x \in B$. Therefore $A \cap B \subseteq A$ and $A \cap B \subseteq B$.
2. Let A, B be sets. If $x \in A$, then $x \in A \vee x \in B$, hence $x \in A \cup B$. Therefore $A \subseteq A \cup B$. If $x \in B$, then $x \in A \vee x \in B$, hence $x \in A \cup B$. Therefore $B \subseteq A \cup B$.
3. Let A, B, C be sets wth $A \subseteq B$ and $B \subseteq C$. Suppose that $x \in A$. Then, since $A \subseteq B$, $x \in B$. Moreover, since $B \subseteq C$, then $x \in C$. We have shown that $x \in A \implies x \in C$ and therefore $A \subseteq C$.
4. Let A, B be sets. We have to show both that $A - B \subseteq A \cap B^c$ and that the opposite containment is true.

   [$\subseteq$] Suppose that $x \in A - B$. Then $x \in A$ and $x \notin B$, hence $x \in A$ and $x \in B^c$, and thus $x \in A \cap B^c$. Therefore $A - B \subseteq A \cap B^c$.

   [$\supseteq$] Suppose now that $x \in A \cap B^c$. Then $x \in A$ and $x \in B^c$, that is, $x \in A$ and $x \notin B$, and thus $x \in A - B$. Therefore $A \cap B^c \subseteq A - B$.

□

The subset relations of the preceding proposition combined with the Table of Set Equalities gives us another way to try to prove our favorite statement.

Example 6.2.2

Prove the following statement using the element method, and then again with the Table of Set Equalities and Proposition 6.2.1: *For all sets* A, B, C,

$$A \cap (B - C) \subseteq (A \cap B) - (A \cap C).$$

First the Element Method.

> *Proof.* Suppose $x \in A \cap (B - C)$. Then $x \in A$ and $x \in B - C$, hence $x \in B$ and $x \notin C$. Since $x \in A$ and $x \in B$, then $x \in A \cap B$. Also, since $x \notin C$, then in particular, $x \notin (A \cap C)$. It follows that $x \in (A \cap B) - (A \cap C)$ and therefore $A \cap (B - C) \subseteq (A \cap B) - (A \cap C)$. □

Using the table/proposition:

Proof. Let A, B, C be sets. Then

$$\begin{aligned}
A \cap (B - C) &= A \cap (B \cap C^c) && \text{(thm:subset-relations)} \\
&= A \cap B \cap C^c && \text{(associative)} \\
&= \emptyset \cup (A \cap B \cap C^c) && \text{(identity)} \\
&= (A \cap A^c \cap B) \cup (A \cap B \cap C^c) && \text{(Complement law)} \\
&= (A \cap B \cap A^c) \cup (A \cap B \cap C^c) && \text{(commutative)} \\
&= (A \cap B) \cap (A^c \cup C^c) && \text{(distributive)} \\
&= (A \cap B) \cap (A \cap C)^c && \text{(DeMorgan's)} \\
&= (A \cap B) - (A \cap C) && \text{(thm:subset-relations)}
\end{aligned}$$

Since $A \cap (B - C) = (A \cap B) - (A \cap C)$, then in particular $A \cap (B - C) \subseteq (A \cap B) - (A \cap C)$. □

6.3 Disproofs and Algebraic Proofs

Let $A = \{1, 2, 3\}$ and $B = \{1, 2\}$. Looking at the power set of A, we have

$$\mathscr{P}(A) = \{\ \emptyset,\ \{1\},\ \{2\},\ \{3\},\ \{1,2\},\ \{1,3\},\ \{2,3\},\ \{1,2,3\}\ \}$$

In blue are all of the subsets of B. Moreover, notice the remaining sets in $\mathscr{P}(A)$ can be written in terms of the subsets of B.

$$\begin{aligned} \{3\} &= \emptyset \cup \{3\} \\ \{1,3\} &= \{1\} \cup \{3\} \\ \{2,3\} &= \{2\} \cup \{3\} \\ \{1,2,3\} &= \{1,2\} \cup \{3\} \end{aligned}$$

This observation provides us with the inutition for the inductive step in the proof of the following.

Theorem 6.3.1

For every integer $n \geq 0$, if a set A has n elements, then $\mathscr{P}(A)$ has 2^n elements.

Proof. Let A be a set.
Base Step. Suppose A has zero elements. Then $A = \emptyset$. Moreover, $\mathscr{P}(A) = \mathscr{P}(\emptyset) = \{\emptyset\}$, which is a set with $1 = 2^0$ element (a symbol called "$\emptyset$").
Inductive Step. Suppose now $A = \{a_1, a_2, \ldots, a_k\}$ is any set with k elements and that $\mathscr{P}(A)$ has 2^k elements. Let $B = A \cup \{a_{k+1}\}$ so that B has $k+1$ elements. Notice the following:

- $\mathscr{P}(A)$ and $\mathscr{P}(B) - \mathscr{P}(A)$ are disjoint sets (on the left are subsets of A, on the right are subsets of B which are *not* subsets of A).
- $\mathscr{P}(B) = \mathscr{P}(A) \cup \big(\mathscr{P}(B) - \mathscr{P}(A)\big)$ (this is just the complement law)

so $\mathscr{P}(A)$ and $\mathscr{P}(B) - \mathscr{P}(A)$ provide a partition of $\mathscr{P}(B)$. In this way, we should be able to count both sets separately and add them up.

By the inductive hypothesis, $\mathscr{P}(A)$ has 2^k elements.

Observe that a_{k+1} is the only element of B which is not in A, hence every set in $\mathscr{P}(B) - \mathscr{P}(A)$ must be a set of the form $X \cup \{a_{k+1}\}$ where $X \in \mathscr{P}(A)$. Since $\mathscr{P}(A)$ has 2^k elements, then there must be 2^k sets of the form $X \cup \{a_{k+1}\}$, whence $\mathscr{P}(B) - \mathscr{P}(A)$ also has 2^k elements.

It follows then that $\mathscr{P}(B)$ has

$$\underbrace{2^k}_{\mathscr{P}(A)} + \underbrace{2^k}_{\mathscr{P}(B)-\mathscr{P}(A)} = 2(2^k) = 2^{k+1}$$

elements.

Therefore, for all $n \geq 0$, if A has n elements, then $\mathscr{P}(A)$ has 2^n elements. □

Example 6.3.2

Prove that, for all sets A, B, then $\mathscr{P}(A) \cap \mathscr{P}(B) = \mathscr{P}(A \cap B)$.

Proof. Let X be an arbitrary set. We have the following string of biconditionals

$$\begin{aligned} & X \in \mathscr{P}(A) \cap \mathscr{P}(B) \\ \iff & X \subseteq A \text{ and } X \subseteq B \\ \iff & X \subseteq A \cap B \\ \iff & X \in \mathscr{P}(A \cap B) \end{aligned}$$

This shows that $\mathscr{P}(A) \cap \mathscr{P}(B) \subseteq \mathscr{P}(A \cap B)$ and $\mathscr{P}(A \cap B) \subseteq \mathscr{P}(A) \cap \mathscr{P}(B)$. Therefore,

$$\mathscr{P}(A) \cap \mathscr{P}(B) = \mathscr{P}(A \cap B).$$

□

Example 6.3.3

Prove that, for all sets A, B, then $\mathscr{P}(A) \cup \mathscr{P}(B) \subseteq \mathscr{P}(A \cup B)$. Give an explicit example which shows that the left-hand side may be a proper subset.

Proof. Let X be an arbitrary set. We have the following string of coniditionals

$$\begin{aligned} & X \in \mathscr{P}(A) \cup \mathscr{P}(B) \\ \iff & X \subseteq A \text{ or } X \subseteq B \\ \implies & X \subseteq A \cup B \\ \iff & X \in \mathscr{P}(A \cap B) \end{aligned}$$

This shows that

$$\mathscr{P}(A) \cap \mathscr{P}(B) \subseteq \mathscr{P}(A \cap B).$$

□

To see that it is not necessarily equality, consider

$$\begin{aligned} A &= \{1, 2\} \\ B &= \{2, 3\} \\ A \cup B &= \{1, 2, 3\} \end{aligned}$$

whence

$$\begin{aligned} \mathscr{P}(A) \cup \mathscr{P}(B) &= \{\ \emptyset,\ \{1\},\ \{2\},\ \{3\},\ \{1, 2\},\ \{2, 3\}\ \} \\ \mathscr{P}(A \cup (B) &= \{\ \emptyset,\ \{1\},\ \{2\},\ \{3\},\ \{1, 2\},\ \{2, 3\},\ \{1, 3\},\ \{1, 2, 3\}\ \} \end{aligned}$$

6.4 Boolean Algebras, Russell's Paradox, and the Halting Problem

We saw that set theory and logic both seemed to contain some certain structure. So since the same structure appears in multiple separate contexts, that must mean that it's important. As such, we give a name to this feature, which is named after the 19th century English mathematician George Boole.

Definition: boolean algebra

A **Boolean algebra** is a set B together with two operations, generally denoted $\oplus$ and $\otimes$, such that for all $a, b \in B$, both

$$a \oplus b \in B, \qquad a \otimes b \in B$$

and the following properties hold:

1. Commutative Laws: For all $a, b \in B$,

   (a) $a \oplus b = b \oplus a$ (b) $a \otimes b = b \otimes a$

2. Associative Laws: For all $a, b, c \in B$,

   (a) $(a \oplus b) \oplus c = a \oplus (b \oplus c)$ (b) $(a \otimes b) \otimes c = a \otimes (b \otimes c)$

3. Distributive Laws: For all $a, b, c \in B$,

   (a) $a \oplus (b \otimes c) = (a \oplus b) \otimes (a \oplus c)$ (b) $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$

4. Identity Laws: There exist distinct elements $\mathrm{Id}_\oplus$ and $\mathrm{Id}_\otimes$ in B such that for all $b \in B$,

   (a) $b \oplus \mathrm{Id}_\oplus = b$ (b) $b \otimes \mathrm{Id}_\otimes = b$

5. Complement Laws: For each $b \in B$, there exists an element in B, denoted $\overline{b}$ and called the complement or negation of b, such that

   (a) $b \oplus \overline{b} = \mathrm{Id}_\otimes$ (b) $b \otimes \overline{b} = \mathrm{Id}_\oplus$

A Boolean algebra is sometimes shortened to the ordered triple $(B, \oplus, \otimes)$.

Remark. Many use the symbols $+, \times, 0, 1$ instead of $\oplus, \otimes, \mathrm{Id}_\oplus, \mathrm{Id}_\otimes$, respectively. While this makes a lot of sense, I'm going to continue with my chosen notation so as not to confuse symbols (since it could be that B is a set of numbers in which case distinguishing between "+" in the Boolean algebra operation vs. "+" in the usual set operation.

Example 6.4.1

$\big(\{\text{logical statements}\}, \vee, \wedge\big)$ is a Boolean algebra where the complement/negation is given by $\overline{p} = \neg p$, and the "identity elements" are $\mathrm{Id}_\vee = \mathbf{c}$ (contradiction) and $\mathrm{Id}_\wedge = \mathbf{t}$ (tautology).

It is straightforward to check the Boolean algebra properties.

- Commutative Laws:
- Associative Laws:

- Distributive Laws:
- Identity Laws:
- Complement Laws:

Example 6.4.2

$\big(\{\text{subsets of a universe } X\}, \cup, \cap\big)$ is a Boolean algebra where the complement/negation is given by $\overline{A} = A^c$, and the identity elements are $\mathrm{Id}_\cup = \emptyset$ and $\mathrm{Id}_\cap = X$.

- Commutative Laws:
- Associative Laws:
- Distributive Laws:
- Identity Laws:
- Complement Laws:

Example 6.4.3

Let $B = \{0, 1\}$ and define the following operations on B:

$$\begin{aligned} x \oplus y &= xy + x + y \pmod 2 \\ x \otimes y &= xy \pmod 2 \\ \overline{x} &= x + 1 \pmod 2 \\ \mathrm{Id}_\oplus &= 0 \pmod 2 \\ \mathrm{Id}_\otimes &= 1 \pmod 2 \end{aligned}$$

Is $(B, \oplus, \otimes)$ a Boolean algebra?

It is! We check the properties in the definition of a Boolean algebra. By commutativity and associativity of the real numbers yield commutativity of $\oplus$ and $\otimes$ almost immediately. The others can be checked with a table.

- Distributive Laws:

a	b	c	$a \oplus (b \otimes c)$	$(a \oplus b) \otimes (a \oplus c)$
0	0	0	0	0
0	0	1	0	0
0	1	0	0	0
0	1	1	1	1
1	0	0	1	1
1	0	1	1	1
1	1	0	1	1
1	1	1	1	1

a	b	c	$a \otimes (b \oplus c)$	$(a \otimes b) \oplus (a \otimes c)$
0	0	0	0	0
0	0	1	0	0
0	1	0	0	0
0	1	1	0	0
1	0	0	0	0
1	0	1	1	1
1	1	0	1	1
1	1	1	1	1

- Identity Laws:

b	$\text{Id}_\oplus$	$b \oplus \text{Id}_\oplus$
0	0	0
1	0	1

b	$\text{Id}_\otimes$	$b \otimes \text{Id}_\otimes$
0	1	0
1	1	1

- Complement Laws:

b	$\overline{b}$	$b \oplus \overline{b}$	$\text{Id}_\otimes$
0	1	1	1
1	0	1	1

b	$\overline{b}$	$b \otimes \overline{b}$	$\text{Id}_\oplus$
0	1	0	1
1	0	0	1

Theorem 6.4.4: Properties of a Boolean Algebra

Let B be any Boolean algebra.

1. *Uniqueness of the Complement Law*
   For all a and x in B, if $a \oplus x = \text{Id}_\otimes$ and $a \otimes x = \text{Id}_\oplus$, then $x = \overline{a}$.
2. *Uniqueness of* $\text{Id}_\oplus$ *and* $\text{Id}_\otimes$
   If there exists $x \in B$ such that $a \oplus x = a \quad \forall a \in B$, then $x = \text{Id}_\oplus$.
   If there exists $y \in B$ such that $a \otimes y = a \quad \forall a \in B$, then $y = \text{Id}_\otimes$.
3. *Double Complement Law*
   For all $a \in B$, $\overline{(\overline{a})} = a$.
4. *Idempotent Law*
   For all $a \in B$,

   (a) $a \oplus a = a$ (b) $a \otimes a = a$

5. *Universal Bound Law*
   For all $a \in B$,

   (a) $a \oplus \text{Id}_\otimes = \text{Id}_\otimes$ (b) $a \otimes \text{Id}_\oplus = \text{Id}_\oplus$

6. *De Morgan's Laws*
   For all $a, b \in B$,

   (a) $\overline{a \oplus b} = \overline{a} \otimes \overline{b}$ (b) $\overline{a \otimes b} = \overline{a} \oplus \overline{b}$

7. *Absorption Laws*
   For all $a, b \in B$,

   (a) $(a \oplus b) \otimes a = a$ (b) $(a \otimes b) \oplus a = a$

8. *Complements of* $\text{Id}_\oplus$ *and* $\text{Id}_\otimes$

   (a) $\overline{\text{Id}_\oplus} = \text{Id}_\otimes$ (b) $\overline{\text{Id}_\otimes} = \text{Id}_\oplus$

Proof. 1.

2.

3.

4. Let $a \in B$. Then

$$\begin{aligned} a \oplus a &= (a \oplus a) \otimes \mathrm{Id}_{\otimes} && \text{(Identity Law)} \\ &= (a \oplus a) \otimes (a \oplus \overline{a}) && \text{(Complement Law)} \\ &= a \oplus (a \otimes \overline{a}) && \text{(Distributive Law)} \\ &= a \oplus \mathrm{Id}_{\oplus} && \text{(Complement Law)} \\ &= a && \text{(Identity Law)} \end{aligned}$$

(and the proof that $a \otimes a = a$ is nearly identical with symbols swapped).

5.

□

Example 6.4.5

Let $B = \{1, 2, 3, 4, 6, 8, 12, 24\}$ and define the following operations on B:

$$x \oplus y = \mathrm{lcm}(x, y)$$
$$x \otimes y = \gcd(x, y)$$
$$\overline{x} = \frac{24}{x}$$

Is $(B, \mathrm{lcm}, \gcd)$ a Boolean algebra?

This is much harder to tell by simply looking at it, and checking with tables – while not unreasonable for a computer, is not practical by hand (each distributive law will use 216 rows, for example).

The first task might be to try to better understand this collection. What are $\mathrm{Id}_{\oplus}$ and $\mathrm{Id}_{\ominus}$? This should be inferrable from the Complement Law, since $a \oplus \overline{a} = \mathrm{Id}_{\otimes}$. But writing out this relatively short table, we have

b	$\overline{b}$	$b \oplus \overline{b}$
1	24	24
2	12	12
3	8	24
4	6	12
6	4	12
8	3	24
12	2	12
24	1	24

But the third column is not constant, so there cannot be a unique choice of $\mathrm{Id}_{\otimes}$, which violates one of the Boolean Algebra Properties. Therefore $(B, \mathrm{lcm}, \gcd)$ is not a Boolean algebra.

7 Properties of Functions

7.1 Functions Defined on General Sets

Definition

Let A, B be sets. The **Cartesian product of A and B** is the set

$$A \times B = \{(a, b) \; : \; a \in A \text{ and } b \in B\}$$

Example 7.1.1: Cartesian Plane

The Cartesian plane, usually denoted $\mathbb{R}^2$ or $\mathbb{R} \times \mathbb{R}$ is the collection of all ordered pairs of real numbers (x, y).

You've probably always thought about a function f via its graph $y = f(x)$. But what is the graph of the function other than ordered pairs of the form $(x, f(x))$ where the inputs $x \in \mathbb{R}$ and the outputs $f(x) \in \mathbb{R}$. This is the motivation to keep in mind as we work on introducing the formal definition of a limit.

Definition

A **binary relation of A and B** is a subset R of $A \times B$. The symbol xRy, read "x is related to y" means $(x, y) \in R$.

We can graph a binary relation in the same way that we graph a function.

Example 7.1.2

Let $A = B = \mathbb{R}$ and let $R = \{(x, y) \; : \; x = y^2 \vee x = -y^2\}$

Definition: function

A **function** from a set A to a set B, denoted $f : A \to B$, is a relation of A (the **domain**) and B (the **codomain**) with the following properties:

1. every element in A is related to some element in B.

$$\forall a \in A, \exists b \in B \text{ such that} aRb$$

2. no element in A is related to more than one element in B.

$$\forall a \in A \text{ and } \forall b_1, b_2 \in B, \text{ if } aRb_1 \text{ and } aRb_2 \text{ then } b_1 = b_2.$$

When the relation is a function f, we usually write $f(a) = b$ instead of aRb.

Example 7.1.3

Let $f \subseteq \mathbb{N} \times \mathbb{R}$ be the relation given by

$$\big\{(n, x) \;:\; n^2 - x = 0\big\}$$

Let $g \subseteq \mathbb{N} \times \mathbb{R}$ be the relation given by

$$\big\{(n, x) \;:\; n^2 + x^2 = 10\big\}$$

Are either of f or g functions?

f is a function since its defining equation can be rewritten as $x = n^2$, so every unique $n \in \mathbb{N}$ is mapped to only one $x \in \mathbb{R}$.
g is not a function, since both $(5, \sqrt{75})$ and $(5, -\sqrt{75})$ are in the relation. Notably the defining equation can be rearranged to $x = \sqrt{100 - n^2}$ or $x = -\sqrt{100 - n^2}$, so there are two real numbers paired with n when $n \neq 0, 10$.

7.1.1 Arrow Diagram

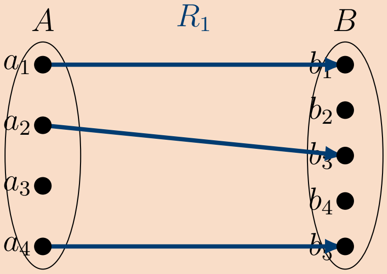
Definition: arrow diagram

Given a relation R of A and B, an **arrow diagram** is formed by drawing an arrow from $a \in A$ to $b \in B$ if and only if aRb.

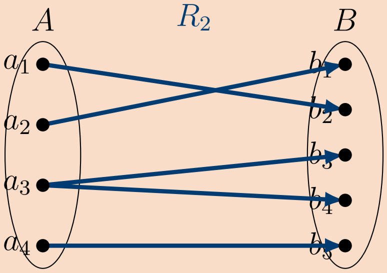
Example 7.1.4: Arrow Diagrams

Draw the arrow diagram for each of the following relations:

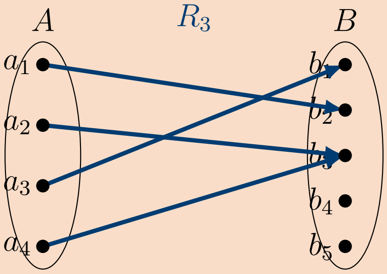
1. $R_1 = \{(a_1, b_1), (a_2, b_3), (a_4, b_5)\}$



2. $R_2 = \{(a_1, b_2), (a_2, b_1), (a_3, b_3), (a_3, b_4), (a_4, b_5)\}$



3. $R_3 = \{(a_1, b_2), (a_2, b_3), (a_3, b_1), (a_4, b_3)\}$



7.1.2 Range, Preimage

Definition: range, preimage

Let $f : A \to B$ be a function. The **range of** f, sometimes denoted $f(A)$, is the set

$$\text{Range}(f) = \{b \in B \ : \ b = f(a) \text{ for some } a \in A\}.$$

Given a subset $\tilde{B} \subseteq B$, the **preimage of** $\tilde{B}$ **under** f is the set

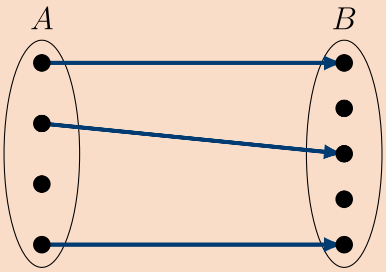
$$\text{Preim}(\tilde{B}) = \left\{a \in A \ : \ f(a) = \tilde{b} \text{ for some } \tilde{b} \in \tilde{B}\right\}.$$

Remark. The preimage of $\tilde{B}$ under f is quite commonly written as $f^{-1}(\tilde{B})$, but so as to avoid confusion, we'll not utilize such notation here.

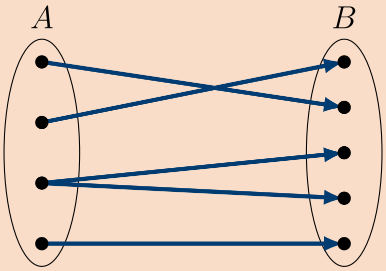
Example 7.1.5: Function or Not?

Determine which of the following mappings are functions.

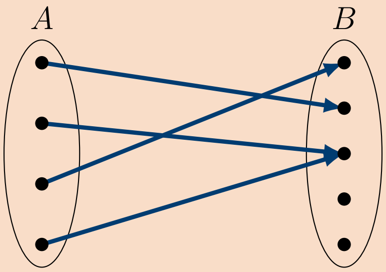
1. f



2. g



3. h



1. f is not a function because there is an element of A that is not paired with an element of B.
2. g is not a function because there is an element of A that is paired with two different elements of B.
3. h is a function because every element of A is paired with a unique element of B.

Definition

Two functions $f : X \to Y$ and $g : X \to Y$ are **equal** if and only if $f(x) = g(x)$ for every $x \in X$.

Remark. Note that this is equivalent to saying that the sets

$$\{(x,y) \in X \times Y \ : f(x) = y\}$$
$$\{(x,y) \in X \times Y \ : g(x) = y\}$$

are equal

Example 7.1.6

Determine which of the following pairs of functions, f and g, are equal:

1. $f : \mathbb{Q} \to \mathbb{Q}$ given by $f(x) = \dfrac{1}{x^2+1}$,
   $f : \mathbb{R} \to \mathbb{R}$ given by $\beta(x) = \dfrac{1}{x^2+1}$.
2. $f : \mathbb{Z} - \{1\} \to \mathbb{Z}$, $f(x) = \dfrac{x^2-1}{x-1}$,
   $g : \mathbb{Z} \to \mathbb{Z}$ given by $g(x) = x + 1$.
3. $f : \mathbb{Z} \to \mathbb{Z}$ given by $f(x) = \dfrac{x^3+x}{x^2+1}$,
   $g : \mathbb{Z} \to \mathbb{Z}$ given by $g(x) = x$.

1. f and g are not equal because $f(\pi)$ is undefined, but $g(\pi)$ is defined.
2. f and g are not equal because $f(1)$ is undefined, but $g(1)$ is defined.
3. Noting that $\dfrac{x^3+x}{x^2+1} = \dfrac{x(x^2+1)}{x^2+1} = x$, we see that $f(x) = g(x)$ for all $x \in \mathbb{Z}$. Thus $f = g$.

7.2 One-to-One, Onto, and Inverse Functions

Definition: L

et $f : A \to B$ be a function. f is said to be **one-to-one** or **injective** if and only if

$$\text{for all } a_1, a_2 \in A, \text{ if } f(a_1) = f(a_2) \text{ then } a_1 = a_2.$$

The tagline is that *"two distinct inputs cannot have the same output."*
f is said to be **onto** or **surjective** if and only if

$$\text{for all } b \in B, \text{ there is some } a \in A \text{ for which } f(a) = b.$$

The tagline is that *the range of f is all of B.*
f is said to be **bijective** if and only if it is both one-to-one and onto.

Example 7.2.1

Give examples of functions that are all combinations of one-to-one (or not) and onto (or not).

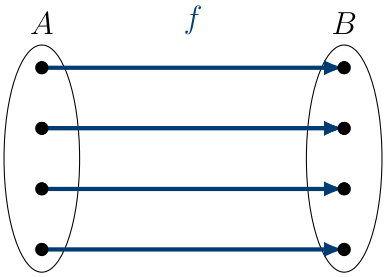


Figure 5: f is both one-to-one and onto.

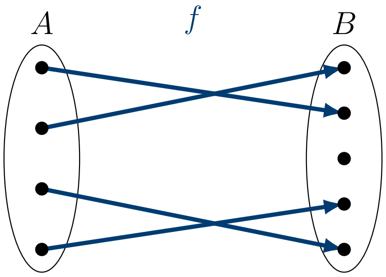


Figure 6: f is one-to-one, but not onto.

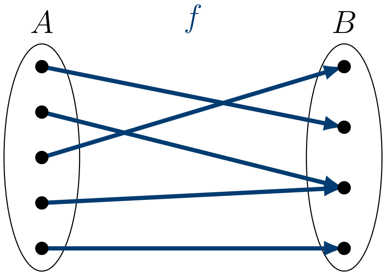


Figure 7: f is not one-to-one, but is onto.

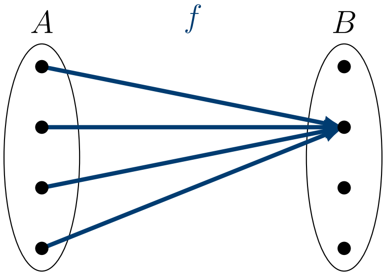


Figure 8: f is neither one-to-one nor onto.

Let's look at the previous examples and reverse the arrows in each case.

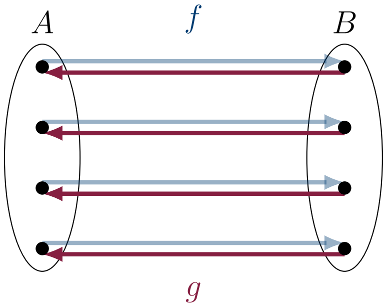


Figure 9: f is both one-to-one and onto.
g is both one-to-one and onto.

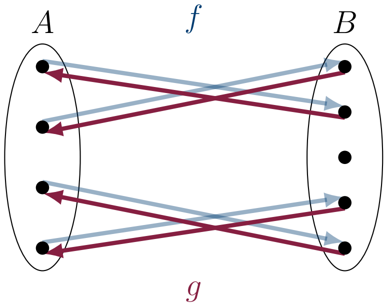
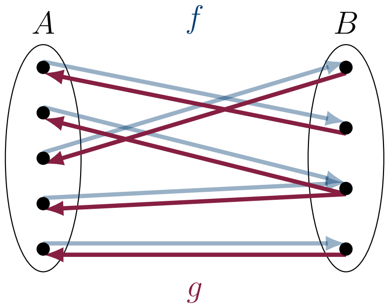
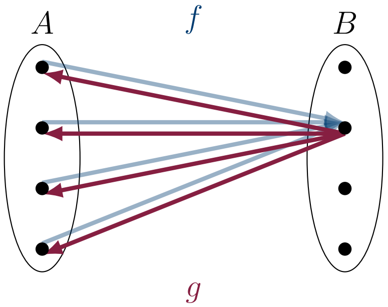


Figure 10: f is one-to-one, but not onto.
g is not a function because
it fails the first condition in the definition.





f is not one-to-one, but is onto.
g is not a function (it fails the second condition of the definition).

f is neither one-to-one nor onto.
g is not a function (it fails both conditions in the derivative).

Naïvely, we would want to define an inverse function by just reversing the arrows. What we see is that the "inverse" only exists in the case that f is one-to-one and onto. Explicitly,

Definition: L

et $f : A \to B$ be a function. The function $f^{-1} : B \to A$ is called an inverse if it has the following property:

$$\text{For all } a \in A, b \in B,\ f^{-1}(b) = a \text{ if and only if } f(a) = b.$$

Theorem 7.2.2

For any function $f : A \to B$, $f^{-1} : B \to A$ exists if and only if f is bijective.

Because of the above theorem, bijections are sometimes referred to as **invertible** functions.

7.3 Composition of Functions

7.4 Cardinality with Applications to Computability

8 Properties of Relations

8.1 Relations on Sets

8.2 Reflexivity, Symmetry, and Transitivity

8.3 Equivalence Relations

8.5 Partial Order Relations

Index