A Primer for Logic and Proof

Holly P. Hirst and Jeffry L. Hirst

2008-2009 Edition[1]

Contents

Introduction

There is a significant shift in the emphasis of undergraduate mathematics between calculus level courses and analysis and algebra courses. The early courses emphasize the application of mathematical concepts to solve specific problems. In later courses, students combine and manipulate the concepts themselves, usually by studying and creating proofs. This book is designed to help students with the transition from application to proof.

Most students have encountered proofs before entering college. In high school geometry, proofs often take the form of a two column justification. For example, suppose we let $\overline{AB}$ denote the length of the line segment AB. Then we can prove the statement, *If the point P lies on the line segment AB between points A and B, then $\overline{PB} = \overline{AB} - \overline{AP}$,* using the two column justification:

Statement	Justification
1. P lies on AB between A and B	Given
2. $\overline{AP} + \overline{PB} = \overline{AB}$	Definition of between using 1
3. $\overline{PB} = \overline{AB} - \overline{AP}$	Subtraction property of = using 2

This very formal type of proof has the advantage of showing plenty of detail, especially revealing the assumptions and definitions used in the argument. Given the list of allowable assumptions and definitions, we can verify each line of the proof in a mechanical fashion and be certain that it is complete and correct. The drawback of the formal proof is that the wealth of detail can hide the interesting mathematical content.

The first two chapters of this book present formal proof systems for propositional calculus and predicate calculus. Propositional calculus will give us a good sense of the meaning of if... then statements and negation. Predicate calculus adds the expressive power of quantifiers, so we can examine statements like "for all x, $A(x)$ or not $A(x)$." Our formal proof systems will provide a precise, detailed, verifiable method of proof.

Predicate calculus is an excellent scaffold on which to hang additional axioms. In the remaining chapters of the book, we will present good sets of axioms for studying number theory, analysis, algebra, set theory, and graph theory. We will also see how to abbreviate formal proofs and distill clear, correct, and informative informal proofs.

The early emphasis on formal logic proofs distinguishes this book from many texts written for bridge courses. On the other hand, the approach to logic

is very mathematical, and sidesteps many philosophical issues that appear in logic texts. Streamlining the logic presentation leaves time in the semester to complete the transition to informal proof, and to tie the material firmly to the study of abstract mathematics. The level and the style of presentation is directed at beginning undergraduate students.

Chapter 1

Propositional Calculus

The big idea in propositional calculus is to study the structure of simple statements. We will discover connections between the structure and the truth values of these statements, and devise fast methods for determining truth values. Eventually, we will write some formal proofs of statements.

1.1 Building Blocks

Propositions

A proposition is a statement, containing a subject and a verb like a sentence in English. We will eventually work with mathematical statements almost exclusively, but for now any statements can be used.

Example. Here are three examples of propositions.

> 2 is prime.
>
> $4 + 6 = 10$.
>
> Today it is raining.

Propositions can be combined with *connectives* such as *and* and *implies* to create compound propositions.

Example. Here are three examples of compound propositions.

> 2 is prime, and $4 + 6 = 10$.
>
> Today it is raining implies that tomorrow the sun will shine.
>
> Today is Thursday and tomorrow will be sunny implies that yesterday was rainy.

Be careful with multiple connectives! English can be quite ambiguous. Take the last combination of propositions for example. Do both of the first statements together imply yesterday was rainy or is it only the second one? If we are not careful, this ambiguity can cause problems when writing mathematical proofs.

Writing out the entire text of a compound proposition can be tedious, particularly if it contains several propositions. As a shorthand, we will use:

- lower case letters (like a, b, c, etc.) for simple propositions, and
- UPPER CASE LETTERS (like A, B, C, etc.) for compound propositions.

Propositions can be true or false. If we know what truth value to assign one we can utilize this information. Otherwise, we check what happens when the proposition is assumed to be true and then false by using a *truth table*. The following truth tables reveal the meaning of the various connectives.

Connectives

The symbols $\neg$, $\wedge$, $\vee$, $\rightarrow$, and $\leftrightarrow$ are called *propositional connectives*. Their properties are best shown via *truth tables*.

Negation

Symbol: $\neg$

Interpretation: $\neg a$ means "not a"

a	$\neg a$
T	F
F	T

Notice that the proposition a has a column containing all possible truth values, in this case simply T and F. Then the second column contains the truth value for "not a" for each possible value of a. We can read this table as follows: If a is true then not a is false. If a is false, then not a is true. Not too bad. Other books use the symbols $\sim a$ or $!a$ to denote $\neg a$. Let's look at the other connectives.

Conjunction

Symbol: $\wedge$

Interpretation: $a \wedge b$ means "a and b"

Vocabulary: a and b are the *conjuncts* in the compound proposition $a \wedge b$.

a	b	$a \wedge b$
T	T	T
T	F	F
F	T	F
F	F	F

Notice here that all possible combinations of truth values for a and b are listed, along with the corresponding value for the connective. The quick story on the *and* connective is that both propositions need to be true for the conjunction to be true.

Disjunction

Symbol: $\vee$

Interpretation: $a \vee b$ means "a or b"

Vocabulary: a and b are the *disjuncts* in the compound proposition $a \vee b$.

a	b	$a \vee b$
T	T	T
T	F	T
F	T	T
F	F	F

Summarizing, a disjunction is true whenever at least one of the propositions is true. This connective is sometimes called *inclusive or* to differentiate it from *exclusive or* (which is often denoted by $+$). The formula $a + b$ is interpreted as "a or b, but not both."

Implication

Symbol: $\rightarrow$

Interpretation: $a \rightarrow b$ means "if a then b" (in the mathematical sense.)

Vocabulary: In the formula $a \rightarrow b$, the proposition a is referred to as the *hypothesis* (or sometimes as the *premise*). The proposition b is referred to as the *conclusion*.

a	b	$a \rightarrow b$
T	T	T
T	F	F
F	T	T
F	F	T

The truth values for implication seem pretty peculiar at first. Some people might argue that the interpretation is distinctly different from typical English usage. They're probably right. However the truth values do correspond exactly to the way that mathematicians use this symbol. The only time an implication is false is when the hypothesis is true and the conclusion is false. False may imply false and false may imply true, but true cannot imply false.

Mathematical texts use all of the following phrases to represent $a \rightarrow b$:

if a then b,

a implies b,

a is a sufficient condition for b,

b is a necessary condition for a.

Biconditional

Symbol: $\leftrightarrow$

Interpretation: $a \leftrightarrow b$ means "a if and only if b"

a	b	$a \leftrightarrow b$
T	T	T
T	F	F
F	T	F
F	F	T

The biconditional is true exactly when the propositions have the same truth value. In some texts, the phase "a is a necessary and sufficient condition for b" is used for $a \leftrightarrow b$.

Truth tables for compound propositions

We can glue statement letters (or propositions) together with connectives to build *compound propositions*. Using the truth tables from above, we can build truth tables for compound propositions. Be sure to include a row for each possible truth assignment for the statement letters.

Example. Build a truth table for $p \rightarrow (q \vee r)$

p	q	r	$q \vee r$	$p \rightarrow (q \vee r)$
T	T	T	T	T
T	T	F	T	T
T	F	T	T	T
T	F	F	F	F
F	T	T	T	T
F	T	F	T	T
F	F	T	T	T
F	F	F	F	T

Note that each simple proposition is listed first, and all possible combinations of truth values are listed. Each parenthesized subformula is listed, and then the final column contains the truth values for the entire compound statement.

Example. Build a truth table for $\neg(p \rightarrow q)$

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

Now, let's do the same examples using *abbreviated truth tables*. There are two important things to remember here. First, an abbreviated truth table contains exactly the same information as any other truth table; only the bookkeeping is different. Second, in any single row of the abbreviated truth table, every occurrence of a propositional letter receives the same truth value. We mark the column for the main connective with bold type. This column corresponds to the last column of a standard truth table.

Example. Build an abbreviated truth table for $p \to (q \vee r)$

p	$\to$	$(q$	$\vee$	$r)$
T	**T**	T	T	T
T	**T**	T	T	F
T	**T**	F	T	T
T	**F**	F	F	F
F	**T**	T	T	T
F	**T**	T	T	F
F	**T**	F	T	T
F	**T**	F	F	F

In building the preceding abbreviated truth table, we followed the order of the parentheses. First, we wrote the columns for p, q, and r so that every possible combination of truth values was represented. Next, we filled in the column for the $\vee$ in $q \vee r$, and finally we filled in the column for the $\to$ connective.

Example. Build an abbreviated truth table for $\neg(p \to q)$

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

Example. Compare the truth tables for $(a \vee b) \wedge c$ and $a \vee (b \wedge c)$.

$(a$	$\vee$	$b)$	$\wedge$	c
T	T	T	**T**	T
T	T	T	**F**	F
T	T	F	**T**	T
T	T	F	**F**	F
F	T	T	**T**	T
F	T	T	**F**	F
F	F	F	**F**	T
F	F	F	**F**	F

a	$\vee$	$(b$	$\wedge$	$c)$
T	**T**	T	T	T
T	**T**	T	F	F
T	**T**	F	F	T
T	**T**	F	F	F
F	**T**	T	T	T
F	**F**	T	F	F
F	**F**	F	F	T
F	**F**	F	F	F

Note that in the last example, the two formulas have the same proposition letters and connectives in the same order. Only the location of the parentheses is different. However, the truth values for the main connectives do not match in the second and fourth rows. There is a moral here. **Parentheses make a difference!** You can leave out parentheses when the meaning of the statement is clear. However, if you have any doubt, retain the parentheses.

Sometimes books will leave out more parentheses than you might like. In a pinch, you can assume that connectives are evaluated in the following order $\neg$, $\wedge$, $\vee$, $\to$, $\leftrightarrow$, with like connectives evaluated from left to right. For example, the formula $b \wedge a \to b \to c \vee \neg d$ should be parenthesized as $((b \wedge a) \to b) \to (c \vee (\neg d))$.

Translations

Given a key listing the meanings of the propositional symbols, we can translate symbolized statements into English sentences.

Example. Given the interpretations below, translate each of the following sentences into English.

a means "Fritz likes trout."
b means "Waldo is tiny."
c means "Violins don't melt."

(a) Translate: $(a \vee b) \rightarrow c$

Solution: If Fritz likes trout or Waldo is tiny, then violins don't melt.

(b) Translate: $a \leftrightarrow c$

Solution: Fritz likes trout if and only if violins don't melt.

Alternate solution: Fritz liking trout is a necessary and sufficient condition for the non-melting of violins.

(c) Translate: $\neg(b \wedge c)$

Solution: It is not the case that both Waldo is tiny and violins don't melt.

Alternate solution: Waldo isn't tiny or violins melt.

The first translation of $\neg(b \wedge c)$ is a direct substitution of English for formal symbols. The second translation is a direct substitution for the symbols in the formula $\neg b \vee \neg c$. Because $\neg b \vee \neg c$ and $\neg(b \wedge c)$ have matching last columns in their truth tables, we can say that the two translations mean the same thing. In section 1.3, we'll learn that these formulas are logically equivalent. The fact that they are logically equivalent is sometimes called DeMorgan's law. Each translation has redeeming merits. The first translation is more literal, while the second sounds more natural.

We can reverse the process of our previous examples, and translate English into our symbolic language. Be sure to include a key to explain the translation.

Example. Translate: If Fritz is the king of France, then Bert eats trout.

Solution: Let k denote "Fritz is the king of France." Let b denote "Bert eats trout." The sentence "If Fritz is the king of France, then Bert eats trout" translates as

$$k \rightarrow b.$$

Common sense and truth

Sometimes we can use common sense to assign a truth value to a proposition. For example, $2 + 2 = 4$ is true, and $2 + 2 = 5$ is false. Note that these truth

values are actually assumptions based on prior experience, but they are still pretty reasonable. In other cases, we lack sufficient information to reasonably assign truth values. For example, the statement "Waldo has a trout in his hat" is neither obviously true nor obviously false. In situations where we can assign truth values to some (or all) of the proposition letters, we can often determine the truth value of associated compound statements. The process involves looking at appropriate lines in the truth table of the compound statement. Here are some examples.

Example. Given the information below, and using common sense where applicable, try to assign truth values to the following compound statements.

a means "$2 = 5$." (We'll assume this is F.)

b means "7 is an odd prime." (We'll assume this is T.)

c means "Waldo is the milkman's pet trout." (We won't assume any truth value here.)

(a) $a \wedge b$

Solution: F $\wedge$ T is F, so $a \wedge b$ is false.

(b) $a \vee b$

Solution: F $\vee$ T is T, so $a \vee b$ is true.

(c) $b \vee c$

Solution:

b	$\vee$	c
T	**T**	T
T	**T**	F

So $b \vee c$ is true.

(d) $a \leftrightarrow c$

Solution:

a	$\leftrightarrow$	c
F	**T**	F
F	**F**	T

So $a \leftrightarrow c$ depends on truth value of c.

Exercises.

1. Build the truth table for $p \wedge q$.
2. Build the truth table for $p \rightarrow (q \vee r)$
3. Build the truth table for $\neg(p \vee \neg p)$
4. Build the truth table for $p \wedge \neg p$
5. Build the truth table for $(p \wedge q) \rightarrow p$
6. Build the truth table for $p \rightarrow (p \vee q)$
7. Given the interpretations below, translate each of the following sentences into English. p means "$2 + 2 = 5$." q means "3 is prime."

(a) Translate: $p \to q$

(b) Translate: $(\neg p) \vee q$

(c) Translate: $\neg(p \vee q)$

8. Given the interpretations below, translate each of the following sentences into English. d means "Waldo wears a hat." m means "All milkmen like trout." w means "$4 + 8 = 32$." z means "$2 \neq 5$."

   (a) Translate: $d \to (m \vee w)$

   (b) Translate: $z \leftrightarrow w$

   (c) Translate: $z \wedge (w \to z)$

   (d) Translate: $\neg(\neg d \wedge z)$

9. Translate into formal symbols: Either money is green or the sky is blue.

10. Translate into formal symbols: If either $2 \neq 5$ or $4 + 5 = 9$, then $5^2 \neq 25$.

11. Translate into formal symbols: Fritz likes chocolate bunnies and Waldo likes umbrellas.

12. Translate into formal symbols: If 5 is not an odd integer, then 8 is prime.

13. Given the information below, and using common sense where applicable, try to assign truth values to the following compound statements.

    p means "$2 \neq 5$."

    q means "7 is an integer multiple of 2."

    r means "Fritz is a tap-dancing investment banker."

   (a) $p \vee q$

   (b) $p \wedge r$

   (c) $q \to r$

   (d) $r \to (q \to r)$

1.2 Tautologies and Contradictions

Some compound propositions are true (or false) just because of their structure. (See exercises 3, 4, 5, and 6 in section 1.1.) The truth values of these statements don't rely on the interpretation of the propositional letters or on any common sense assignment of truth values to the propositional letters. The semantics of these formulas depends only on their syntax. Because these are special formulas, we give them special names.

Definition. A *tautology* is a compound proposition which is always true. That is, a formula is a tautology if and only if the last column of its truth table contains only Ts.

Example. Show that $p \vee \neg p$ is a tautology.

Solution: We'll check that the main connective column in the truth table for $p \vee \neg p$ contains only Ts.

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

Definition. A *contradiction* is a compound proposition which is always false. That is, a formula is a contradiction if and only if the last column of its truth table contains only Fs.

Example. Show that $p \wedge \neg p$ is a contradiction.

Solution: We'll check that the main connective column in the truth table for $p \wedge \neg p$ contains only Fs.

p	$\wedge$	$(\neg$	$p)$
T	**F**	F	T
F	**F**	T	F

Definition. A *contingency* is a compound proposition which is neither a tautology nor a contradiction. That is, a formula is a contingency if and only if the last column of its truth table contains both Ts and Fs.

Example. Show that $p \rightarrow q$ is a contingency.

Solution: We'll show that the main connective column in the truth table for $p \rightarrow q$ contains at least one T and at least one F.

p	$\rightarrow$	q
T	**T**	T
T	**F**	F
F	**T**	T
F	**T**	F

The first and second rows will fill the bill. We didn't even need to write the last two rows.

Exercises.

1. Show that $a \rightarrow (b \rightarrow a)$ is a tautology.
2. Show that $(a \rightarrow (b \rightarrow c)) \rightarrow ((a \rightarrow b) \rightarrow (a \rightarrow c))$ is a tautology.
3. Show that $(\neg b \rightarrow \neg a) \rightarrow ((\neg b \rightarrow a) \rightarrow b)$ is a tautology.
4. Show that $p \leftrightarrow (p \rightarrow \neg p)$ is a contradiction.
5. Show that $p \wedge p$ is a contingency.
6. Classify each of the following formulas as a tautology, a contradiction, or a contingency. Provide enough of the truth table for the formula to justify your answer. (For tautologies and contradictions, you need the whole table. For contingencies you can get by with just two cleverly selected rows.)

(a) $(p \wedge q) \rightarrow p$

(b) $p \rightarrow (p \vee q)$

(c) $(p \vee q) \rightarrow (p \wedge q)$

(d) $p \leftrightarrow \neg p$

(e) $p \rightarrow (\neg p \rightarrow (q \wedge \neg q))$

(f) $(p \rightarrow q) \vee (q \rightarrow p)$

1.3 Logical Equivalence

Think for a minute about formulas involving the proposition letters p and q. There are lots of formulas of this sort. Each of those formulas has a truth table with exactly four rows. There are only sixteen possible last columns for those truth tables. Consequently, a lot of formulas have truth tables whose last columns match. The following definition extends this notion of matching last columns to situations where the formulas may not contain exactly the same statement letters.

Definition. Two formulas, A and B, are *logically equivalent* if and only if $A \leftrightarrow B$ is a tautology.

Example. Show that $p \rightarrow q$ is logically equivalent to $\neg q \rightarrow \neg p$.

Solution: We'll verify that the main connective column in the truth table for the biconditional constructed from these two formulas contains only Ts.

$(p$	$\rightarrow$	$q)$	$\leftrightarrow$	$((\neg$	$q)$	$\rightarrow$	$(\neg$	$p))$
T	T	T	**T**	F	T	T	F	T
T	F	F	**T**	T	F	F	F	T
F	T	T	**T**	F	T	T	T	F
F	T	F	**T**	T	F	T	T	F

Exercises.

1. Show that $\neg p \wedge \neg q$ is logically equivalent to $\neg(p \vee q)$.
2. Show that $p \wedge q$ is logically equivalent to $\neg(\neg p \vee \neg q)$.
3. Show that p is logically equivalent to $\neg\neg p$.
4. Show that $p \vee (q \rightarrow (s \wedge \neg\neg t))$ is logically equivalent to $p \vee (q \rightarrow (s \wedge t))$.

1.4 Contrapositives and Converses

Mathematicians are often concerned with conditional statements. Given an implication, there are two related formulas which occur so often that they have special names.

Definition. The *contrapositive* of the conditional $P \to Q$ is $\neg Q \to \neg P$.

Example. The contrapositive of $a \to (b \vee c)$ is $\neg(b \vee c) \to \neg a$.

Example. We say that a mapping is 1–1 if $x \neq y$ implies that $f(x) \neq f(y)$. The contrapositive of this implication is: if $f(x) = f(y)$ then $x = y$. (We've eliminated some double negations here. To be excruciatingly technically correct, the contrapositive of $x \neq y \to f(x) \neq f(y)$ is $\neg(f(x) \neq f(y)) \to \neg(x \neq y)$, and the formula $f(x) = f(y) \to x = y$ is logically equivalent to the contrapositive.)

Sometimes the contrapositive of a formula is easier to prove than the original formula. For example, it is much easier to assume that $f(x) = f(y)$ and deduce $x = y$ than it is to assume $x \neq y$ and deduce $f(x) \neq f(y)$. This has little to do with functions and a lot to do with the fact that $x \neq y$ is not usually a particularly useful piece of information. The thing that makes this important is the fact that every formula is logically equivalent to its contrapositive. Consequently, if we want to prove that a mapping is 1–1, it's good enough to prove that if $f(x) = f(y)$ then $x = y$. This works for any conditional statement, and mathematicians spend a lot of time proving conditional statements. The main point of this discussion is recapped in the following theorem.

Theorem (Contrapositive Theorem)**.** Every conditional formula is logically equivalent to its contrapositive.

Proof. Any conditional formula will have the form $P \to Q$. We'll show that this is logically equivalent to $\neg Q \to \neg P$ by checking the truth table for the biconditional statement built from these formulas. We're looking for all Ts in the main connective column.

$(P$	$\to$	$Q)$	$\leftrightarrow$	$(\neg$	Q	$\to$	$\neg$	$P)$
T	T	T	**T**	F	T	T	F	T
T	F	F	**T**	T	F	F	F	T
F	T	T	**T**	F	T	T	T	F
F	T	F	**T**	T	F	T	T	F

The main connective column is all Ts, so the biconditional is a tautology and the formulas are logically equivalent. □

Definition. The *converse* of the conditional $P \to Q$ is $Q \to P$.

Example. The converse of $a \to (b \vee c)$ is $(b \vee c) \to a$.

Example. We say that a mapping is well-defined if every input has a unique output. Thus a mapping is well-defined if $x = y$ implies $f(x) = f(y)$. Look at these formulas:

$f(x)$ is well defined means that $x = y \to f(x) = f(y)$.

$f(x)$ is 1–1 means that $f(x) = f(y) \to x = y$.

We can see that "$f(x)$ is well-defined" is the converse of "$f(x)$ is 1–1."

To prove a biconditional like $p \leftrightarrow q$, a mathematician often proves $p \rightarrow q$ and proves the converse, $q \rightarrow p$. Neither of these steps can be skipped, because a conditional and its converse may not be logically equivalent. For example, you can easily show that $a \rightarrow b$ is not logically equivalent to its converse. Some bizarre formulas, like $a \rightarrow a$ for example, are logically equivalent to their converses, but that's just a fluke. To summarize this section, a conditional is always logically equivalent to its contrapositive. A conditional may or may not be logically equivalent to its converse.

Exercises.

1. Write the contrapositives of the following.
   (a) $p \rightarrow q$
   (b) $(p \vee r) \rightarrow q$
   (c) $(a \wedge b) \rightarrow (c \vee d)$
   (d) If Waldo likes trout, then Elmer is a sailor.
   (e) If $0 \neq 1$, then 4 is a prime.
   (f) If tap-dancing is foolish, then I want to be a fool.
2. Write the converses of the following.
   (a) $p \rightarrow q$
   (b) $(p \vee r) \rightarrow q$
   (c) $(a \wedge b) \rightarrow (c \vee d)$
   (d) If Waldo likes trout, then Elmer is a sailor.
   (e) If $0 \neq 1$, then 4 is a prime.
   (f) If tap-dancing is foolish, then I want to be a fool.
3. Show that $a \rightarrow b$ is not logically equivalent to its converse.
4. Show that $a \rightarrow a$ is logically equivalent to its converse.
5. Find a formula that is logically equivalent to its converse and one that is not. You could be imaginative and pick examples other than those in exercises 3 and 4.

1.5 Analysis of Arguments

We see examples of informal arguments every day. In newspaper editorials, court cases, and advertising, people give lists of reasons and try to convince us of a conclusion. Here's a formal version of the process.

An *argument* is a list of premises which taken all together supposedly imply a conclusion. For example,

$$\begin{array}{l} P_1 \\ P_2 \\ P_3 \\ ... \\ P_n \\ \hline P_{n+1} \end{array}$$

is an argument.

We say that an argument (like the one above) is *logically valid* if and only if $(P_1 \wedge P_2 \wedge P_3 \wedge ... \wedge P_n) \rightarrow P_{n+1}$ is a tautology. Note that the conclusion of a logically valid argument is not necessarily true. Logical validity ensures only that *if* all the premises are true, *then* the conclusion is true.

Example. Show that the following argument is logically valid.

$$\begin{array}{l} p \\ p \rightarrow q \\ \hline q \end{array}$$

Solution: We build the truth table to check.

$(p$	$\wedge$	$(\ p$	$\rightarrow$	$q))$	$\rightarrow$	q
T	T	T	T	T	**T**	T
T	F	T	F	F	**T**	F
F	F	F	T	T	**T**	T
F	F	F	T	F	**T**	F

Looks good. This argument format is so commonly used, that it has a name: *Modus Ponens*. We will see it later in our proof system as a legitimate deduction rule, i.e., if p and $p \rightarrow q$ are both lines in a proof, then q can be used alone.

Exercises.

1. Here are some other common argument forms. Show that they are all logically valid.

   Modus Tollens: $\begin{array}{l} a \rightarrow b \\ \neg b \\ \hline \neg a \end{array}$

   Constructive Dilemma: $\begin{array}{l} p \rightarrow r \\ q \rightarrow r \\ p \vee q \\ \hline r \end{array}$

   Hypothetical Syllogism: $\begin{array}{l} p \rightarrow q \\ q \rightarrow r \\ \hline p \rightarrow r \end{array}$

Disjunctive Syllogism: $\dfrac{\begin{array}{c} s \vee t \\ \neg s \end{array}}{t}$

2. Is the following argument logically valid?

   The chancellor knows.

   If the chancellor doesn't know, then the provost knows.

   If the provost knows, then we're in trouble.

   We're in trouble.

3. Is the following argument logically valid?

   When it rains, I wear a hat.

   It never rains

   I never wear a hat.

4. What statement could be substituted for P to make the following argument valid?

   When it rains, I wear a hat.

   P

   It never rains.

5. Is the following argument logically valid?

   If today is Sunday, then tomorrow is Monday.

   Today is not Sunday.

   Tomorrow is not Monday.

6. Is the following argument logically valid?

   You can afford a used Pinto.

   If you've driven a Ford lately, then you want to buy a Ford.

   If you want to buy a Ford, and you can afford a used Pinto, then you'll buy a used Pinto.

   If you've driven a Ford lately, then you'll buy a used Pinto.

7. Modify one of the premises below to make the argument valid.

It's cold.

If Fritz wears a parka, then its cold.

Fritz is fond of velcro.

Fritz wears a parka.

1.6 A Proof System

So far, we've been primarily concerned with the semantics of propositional calculus. Now, we'll deal with a syntactic notion. For the next several sections, there won't be any truth tables at all. Eventually, we'll connect our study of semantics with our study of syntax.

The syntactic topic we're going to work on is the idea of proof. When a mathematician writes a proof, he justifies a conclusion with a series of intermediate steps. Our proofs will be very formal, so we can specify in advance exactly which steps are allowable. This will help us get a good handle on exactly what constitutes a proof.

The proofs we'll be doing will be fun, provided you keep your cool. Sometimes people get stuck and become frustrated. Ask any practicing mathematician, and he or she can tell you about being seriously stuck on a proof. It's O.K., and (almost) everybody survives. Remember, working on a proof is a worthy endeavor. Sit back and enjoy the process.

The system L

A *proof* is a sequence of formulas with justifications. Each line in a *proof in the system* L must be one of the following:

- an axiom of L,
- the result of applying Modus Ponens,
- a hypothesis (that is, a given formula), or
- a lemma.

The last formula in a proof is called a *theorem.* We write $\vdash_L A$ if A is a theorem. We write $G_1, G_2, ..., G_n \vdash_L A$ if A can be proved in L from the given formulas $G_1, G_2, ..., G_n$.

Axioms

There are three axioms in L:

Axiom 1: $A \to (B \to A)$

Axiom 2: $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$

Axiom 3: $(\neg B \to \neg A) \to ((\neg B \to A) \to B)$

We can use any *instance* of an axiom in a proof. That is, A, B, and C can be uniformly replaced by any formula we like. We'll use $A := p$ to denote replacing A by the formula p. Here are three instances of Axiom 1 and the substitutions used to create them.

$p \to (q \to p)$ results from $A := p$ and $B := q$.

$B \to (A \to B)$ results from $B := A$ and $A := B$.

$A \to (A \to A)$ results from $A := A$ and $B := A$.

$(B \to C) \to (\neg Q \to (B \to C))$ results from $A := B \to C$ and $B := \neg Q$.

Modus Ponens

The rule of inference *Modus Ponens* says that if A and $A \to B$ are lines in a proof, we can write B as a (later) line. Here A and B can represent any formulas.

Rather than mess with a concocted example, let's do a proof!

Our first proof

Theorem L 1. $\vdash_L A \to A$

1. $A \to ((A \to A) \to A)$ — Axiom 1
   $A := A$ and $B := (A \to A)$
2. $(A \to ((A \to A) \to A)) \to ((A \to (A \to A)) \to (A \to A))$ — Axiom 2
   $A := A$, $B := (A \to A)$ and $C := A$
3. $((A \to (A \to A)) \to (A \to A))$ — Modus Ponens
   Lines 1 and 2
4. $A \to (A \to A))$ — Axiom 1
   $A := A$ and $B := A$
5. $A \to A$ — Modus Ponens
   Lines 3 and 4

Technically, the formal proof of $A \to A$ in L consists of just the sequence of five propositions. As a courtesy to the reader, we include the justifications (which axiom or rule of inference we used) and additional information (substitutions and lines).

Lemmas

We've proved $\vdash_L A \to A$. Now we can use any *instance* of $A \to A$ in future proofs. In this case, we say that we're using this theorem as a *lemma.* For example,

Theorem L 2. $\vdash_L (\neg B \to B) \to B$

1. $\neg B \to \neg B$	Theorem L1
	$A := \neg B$
2. $(\neg B \to \neg B) \to ((\neg B \to B) \to B)$	Axiom 3
	$A := B$ and $B := B$
3. $((\neg B \to B) \to B)$	Modus Ponens
	Lines 1 and 2

The use of lemmas is actually just a convenient shortcut. Rather than writing the instance of Theorem L1 as the first line in the preceding proof, we could write the five lines of the proof of Theorem L1, replacing all the uses of A in that proof with $\neg B$. The justification for these lines would be unchanged from our original proof of Theorem L1. In the resulting proof of L2, every single line would be an axiom or a use of modus ponens. However, since we have already written the proof of Theorem L1 once, it seems silly to recopy it. Consequently, we use lemmas.

Proofs using hypotheses

Hypotheses (also called "given" formulas) must be used **exactly** as stated. Here's an example:

Theorem L 3. $A \to (B \to C),\ A \to B \vdash_L A \to C$

1. $A \to (B \to C)$	Given
2. $A \to B$	Given
3. $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$	Axiom 2
4. $(A \to B) \to (A \to C)$	Modus Ponens, lines 1 and 3
5. $A \to C$	Modus Ponens, lines 2 and 4

Here's an important distinction. Hypotheses must be used as stated. Instances of hypotheses are not allowed. For example, in the preceding proof, we cannot just write down $A \to C$ as an instance of the given formula $A \to B$. However, instances of lemmas are allowed.

Thus, we can use an instance of this theorem in a new proof. Here's an instance: $A \to ((B \to A) \to C),\ A \to (B \to A) \vdash_L A \to C$. In this instance, we have used $A := A$, $B := B \to A$, and $C := C$. Let's use this in the following proof.

Theorem L 4. $A \to ((B \to A) \to C) \vdash_L A \to C$

1. $A \to ((B \to A) \to C)$ Given
2. $A \to (B \to A)$ Axiom 1
3. $A \to C$ Theorem L3

$A := A$, $B := B \to A$, and $C := C$

Exercises.

Prove the following theorems. Remember, any theorem with a lower number may be used in the proof. (Using earlier theorems can save a lot of work.)

Theorem L 5. $B \vdash_L A \to B$

Theorem L 6. $A \to (B \to C),\ B \vdash_L A \to C$

Theorem L 7. $A \to (B \to C) \vdash_L B \to (A \to C)$

Theorem L 8. $A \to B,\ B \to C \vdash_L A \to C$

Theorem L 9. $P \to R \vdash_L P \to (Q \to R)$

Theorem L 10. $\vdash_L (\neg B \to \neg A) \to (A \to B)$

Theorem L 11. $\vdash_L \neg\neg B \to B$

Theorem L 12. $\vdash_L B \to \neg\neg B$

1.7 The Deduction Theorem

In this section, we'll learn about a wonderful shortcut, which comes in the form of a theorem.

Theorem (Deduction Theorem, Herbrand 1930)**.** If $G_1, ..., G_n, A \vdash_L B$, then $G_1, ..., G_n \vdash_L A \to B$.

Let's try one.

Theorem L 13. $\vdash_L (A \to (B \to C)) \to (B \to (A \to C))$

First we'll prove $A \to (B \to C), B \vdash_L (A \to C)$.

1. $A \to (B \to C)$ Given
2. B Given
3. $A \to C$ Theorem L6, lines 1 and 2

We've proved $A \to (B \to C),\ B \vdash_L (A \to C)$. Applying the deduction theorem, we obtain $A \to (B \to C) \vdash_L B \to (A \to C)$. A second application of the deduction theorem yields $\vdash_L (A \to (B \to C)) \to (B \to (A \to C))$, completing the proof of Theorem L13.

Let's summarize. To prove $P \to Q$, we can assume P, deduce Q, and then apply the deduction theorem. Look at any math text. Any proof that starts with "Let..." or "Assume that..." is using this technique.

The deduction theorem is not a theorem *of* the system L, it's a theorem *about* the system L. It says that if we have a proof of $P \vdash_L Q$, then we are guaranteed that a proof of $\vdash_L P \to Q$ exists. This has two consequences. First, since the deduction theorem is not really a rule, an axiom, or a theorem of L, it is technically incorrect to use it as a justification for a line in a formal proof. (Some books allow this, and it doesn't cause frequent difficulties. However, it can cause some problems and it's just as easy to write our uses of the deduction theorem outside the formal proof.) Second, the deduction theorem says we could live without this shortcut. If we use the deduction theorem to show that a proof $\vdash_L P \to Q$ exists, then sure enough, a formal proof in L of $P \to Q$ does exist, and that formal proof doesn't use the deduction theorem. The deduction theorem does save time. Proofs that use it are often less than half as long as those that do not.

How does the deduction theorem work?

The idea behind the proof of the deduction theorem is that we can always convert a proof of something of the form $G_1, \ldots, G_n, A \vdash_L B$ into a proof of $G_1, \ldots, G_n \vdash_L A \to B$. For example, we should be able to convert our proof (from page 17) of Theorem L3, namely $A \to (B \to C), A \to B \vdash_L A \to C$, into a proof of $A \to (B \to C) \vdash_L (A \to B) \to (A \to C)$. Furthermore, we want to achieve this conversion in a systematic fashion that could be adapted to any proof. We can achieve this by proving $(A \to B) \to M$ for every line M in the original proof. This doesn't result in a short or elegant proof, but it's very systematic. Here is a proof of $A \to (B \to C) \vdash_L (A \to B) \to (A \to C)$ based on our proof of L3 with some additional explanatory commentary.

Theorem. $A \to (B \to C) \vdash_L (A \to B) \to (A \to C)$.

Line 1 of the proof of L3 was $A \to (B \to C)$, so we will want to prove $(A \to B) \to (A \to (B \to C))$.

1. $A \to (B \to C)$ Given

2. $(A \to B) \to (A \to (B \to C))$ L5, line 1

Good. We got what we wanted. Now, line 2 of the proof of L3 was $A \to B$, so next we want to prove $(A \to B) \to (A \to B)$.

3. $(A \to B) \to (A \to B)$ L1

Got it in one. Line 3 of the proof of L3 was Axiom 2, so we need to prove $(A \to B) \to [(A \to (B \to C)) \to ((A \to B) \to (A \to C))]$.

4. $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$ Axiom 2

5. $(A \to B) \to [(A \to (B \to C)) \to ((A \to B) \to (A \to C))]$ L5, line 4

Line 4 of the proof of L3 was $(A \to B) \to (A \to C)$, so we need to prove $(A \to B) \to [(A \to B) \to (A \to C)]$. The original justification was modus ponens applied to line 1 and line 3. The justification for our new line will be Theorem L3 applied to line 2 (the new version of line 1 from the previous proof) and line 5 (the new version of line 3 from the previous proof).

6. $(A \to B) \to [(A \to B) \to (A \to C)]$ L3, lines 2 and 5

The last line in the proof of L3 is $A \to C$. We need to prove $(A \to B) \to (A \to C)$. The original justification was modus ponens, so we will use L3 again.

7. $(A \to B) \to (A \to C)$ L3, lines 3 and 6

We've proved the line we wanted.

Since every proof in L can be rewritten using just hypotheses, axioms and modus ponens, the techniques used in the preceding theorem can be adapted to any proof. This explains why the deduction theorem always works. For a detailed proof of the deduction theorem, we should really use some form of induction on proof length. For more on this see [8] or [1].

Exercises.

Prove the following theorems. You will enjoy using the deduction theorem.

Theorem L 14. $\vdash_L A \to ((A \to B) \to B)$

Theorem L 15. $\vdash_L \neg A \to (A \to B)$

Theorem L 16. $\vdash_L (A \to B) \to (\neg B \to \neg A)$

Theorem L 17. $\vdash_L A \to (\neg B \to \neg(A \to B))$

1.8 Generalizing L

Our proof system, L, is pretty powerful. It works fine on formulas involving only $\neg$ and $\to$ as connectives. Unfortunately, it doesn't handle $\leftrightarrow$, $\wedge$, and $\vee$. We can get around this problem by using the following abbreviations.

$A \wedge B$ abbreviates $\neg(A \to \neg B)$

$A \vee B$ abbreviates $(\neg A) \to B$, and

$A \leftrightarrow B$ abbreviates $\neg((A \to B) \to \neg(B \to A))$.

Here is an example of how these are used in L.

Theorem L 18. $A, B \vdash_L A \wedge B$

The unabbreviated version of the theorem is $A, B \vdash_L \neg(A \to \neg B)$.

1.	A	Given
2.	B	Given
3.	$A \to (\neg\neg B \to \neg(A \to \neg B))$	L17
4.	$\neg\neg B \to \neg(A \to \neg B)$	Modus Ponens, lines 1 and 3
5.	$B \to \neg\neg B$	L12
6.	$\neg\neg B$	Modus Ponens, lines 2 and 5
7.	$\neg(A \to \neg B)$	Modus Ponens, lines 6 and 4

Is this a reasonable approach to dealing with other connectives? Yes, but only because the abbreviations are logically equivalent to their unabbreviated forms. This can be verified via truth tables, as in the first three exercises below. It's also worth noting that the theorems of L proved in this section do a good job of describing important aspects of mathematical practice. For example, a mathematician who wants to prove a biconditional proves an implication, then proves the converse, and then asserts the biconditional. This is exactly the plan of attack described by Theorem L25.

Exercises.

1. Use a truth table to show that $A \wedge B$ is logically equivalent to $\neg(A \to \neg B)$.
2. Use a truth table to show that $A \vee B$ is logically equivalent to $(\neg A) \to B$.
3. Use a truth table to show that $A \leftrightarrow B$ is logically equivalent to $\neg((A \to B) \to \neg(B \to A))$.
4. Prove the following theorems.

   Theorem L 19. $A \wedge B \vdash_L A$

   Theorem L 20. $A \wedge B \vdash_L B$

   Theorem L 21. $A \vdash_L A \vee B$

   Theorem L 22. $B \vdash_L A \vee B$

   Theorem L 23. $A \leftrightarrow B \vdash_L A \to B$

   Theorem L 24. $A \leftrightarrow B \vdash_L B \to A$

Theorem L 25. $A \to B, B \to A \vdash_L A \leftrightarrow B$

5. This exercise shows that the connective $\wedge$ has an associative property.
   (a) Compare the unabbreviated forms of $A \wedge (B \wedge C)$ and $(A \wedge B) \wedge C$.
   (b) Prove $A \wedge (B \wedge C) \vdash_L (A \wedge B) \wedge C$. (Using L18, L19, and L20 yields a much shorter proof.)
   (c) Prove $(A \wedge B) \wedge C \vdash_L A \wedge (B \wedge C)$. (Using L18, L19, and L20 yields a much shorter proof.)

1.9 Soundness and Completeness of L

As we'll see in the next section, L is not the only possible proof system for propositional calculus. So why have we been working with L? There are two reasons.

The first reason is pedagogical. L deals very well with conditionals and negations. These connectives are the ones most used by mathematicians. Thus, L forces us to concentrate on material with lots of mathematical applications.

The second reason is mathematical. As we'll see in a minute, the theorems of L are exactly the tautologies. So L is related in a pretty wonderful way to the semantics we covered at the beginning of the course. We'll state this relationship in the form of two theorems.

Theorem. [The Soundness Theorem for L] If $\vdash_L A$, then A is a tautology. Also, if $G_1, G_2, ..., G_n \vdash_L A$, then $(G_1 \wedge G_2 \wedge ... \wedge G_n) \to A$ is a tautology.

As a consequence of the Soundness Theorem, every formula we proved in L is a tautology. Let's look at at two examples.

Example. Verify that L19 is a tautology: $\vdash_L (A \wedge B) \to A$

$(A$	$\wedge$	$B)$	$\to$	A
T	T	T	**T**	T
T	F	F	**T**	T
F	F	T	**T**	F
F	F	F	**T**	F

Example. Verify that L11 is a tautology: $\vdash_L \neg\neg B \to B$

$\neg$	$\neg$	B	$\to$	B
T	F	T	**T**	T
F	T	F	**T**	F

Why does the Soundness Theorem always work? Here is a rough sketch of the proof. Suppose that we have a proof in L of A. If we want, we can eliminate any uses of the deduction theorem and any uses of lemmas from our proof, so that the proof consists only of axioms and uses of modus ponens. Start at the beginning of the proof. The first two lines have to be axioms, and all the axioms

of L are tautologies. (See exercises 1, 2, and 3 on page 9.) If the next line is an axiom, then it is a tautology, too. The next line could be an application of modus ponens to previous lines of the form P and $P \to Q$, yielding Q. Since the previous lines, namely P and $P \to Q$, are both tautologies, Q must be a tautology also. Proceeding in this fashion, we can prove that every line in the proof is a tautology, including the last line, which is A. Thus, if L proves A, then A must be a tautology.

Our next theorem is actually the converse of the Soundness theorem.

Theorem. [The Completeness Theorem for L] If A is a tautology, then $\vdash_L A$. Also, if $(G_1 \wedge G_2 \wedge ... \wedge G_n) \to A$ is a tautology, then $G_1, G_2, ..., G_n \vdash_L A$.

We can use the Completeness Theorem for L to show that a formula can be proved in L, *without actually producing the proof!* Actually, this happens all the time in mathematics. Lots of theorems assert the existence of a set, or a function, or a solution to a problem, or even a proof, without actually providing the desired object. People call these theorems "non-constructive existence theorems." This sort of theorem is surprisingly useful. It's sort of like saying, "I know there's a vacuum cleaner in that closet, and I could find it if I really needed it."

Example. Use the Completeness Theorem for L to prove that L can prove $A \to A$ (Theorem L1).

Solution: The truth table for $A \to A$ is:

A	$\to$	A
T	**T**	T
F	**T**	F

$A \to A$ is a tautology, so by the Completeness Theorem, $\vdash_L A \to A$.

This is shorter than our proof in L of Theorem L1, but in some ways less satisfying. Often it is faster (or at least less boring) to produce the proof in L than to write the truth table. For example, write down an instance of Axiom 1 with 10 letters in it. The truth table would contain 2^{10} lines, but the proof in L is just one line. In this case, it is easier to produce the proof than to apply the Completeness Theorem to prove that the proof exists.

One way to prove the Completeness Theorem is to devise an algorithm that converts truth tables into proofs in L. The proof in [8] which is based on [5] uses this technique. Since such an algorithm exists, we could write a computer program that would accept a formula as an input, determine if the formula is a tautology, and if it is, construct and print a proof in L of the formula. Unfortunately, the proofs supplied by the algorithm tend to be extremely long and unintuitive. So far, we are superior to machines at providing short, elegant proofs in L.

Suppose for a moment that $\vdash_L A$. By the Soundness Theorem, A is a tautology. Thus, $\neg A$ is a contradiction. In particular, $\neg A$ is not a tautology. By the contrapositive of the Soundness Theorem, L doesn't prove $\neg A$. Thus, if L proves A, then L doesn't prove $\neg A$. Similarly, if L proves $\neg A$, then L doesn't prove A. Summarizing, we have that L can't ever prove both A and $\neg A$. This

important property of L is called consistency, and is summarized in the following theorem.

Theorem (Consistency of L)**.** L is consistent. That is, there is no formula A such that both $\vdash_L A$ and $\vdash_L \neg A$.

Exercises.

1. Use the Completeness Theorem for L to show that L can prove Theorem L7.

2. Use the Completeness Theorem for L to show that L can prove Theorem L13.

3. Use the Completeness Theorem for L to show that L can prove Theorem L15.

4. Is there a proof in L of $(A \vee B) \rightarrow B$?

5. Is there a proof of $B \vdash_L A \vee B$?

6. Is there a proof of $(A \wedge \neg A) \vdash_L B$?

7. Is there a proof in L of $A \wedge \neg A$?

1.10 Modifying L

As noted in the previous section, L has some nice properties. How can we modify L, retaining soundness and completeness? There are three reasonable approaches: adding an axiom, discarding an axiom, and starting from scratch.

Adding an axiom

Suppose we add a tautology to L as a new axiom. Let's call the new axiom NEW. Suppose also that there is some formula A that we can prove in L, using the new axiom. Then for some *instance* of NEW (call it NEW^*) we have $NEW^* \vdash_L A$. By the Deduction Theorem, $\vdash_L NEW^* \rightarrow A$. Since NEW^* is a tautology, by the Completeness Theorem for L, $\vdash_L NEW^*$. We can put together a short proof of $\vdash_L A$.

1. $NEW*$ Axiom NEW

2. $NEW* \rightarrow A$ Lemma from preceding paragraph

3. A Modus Ponens, lines 1 and 2

So far, anything provable with the new axiom is provable in the original axiom system. Also, anything provable in L must be provable in the new axiom system. Thus, the new axiom system has exactly the same theorems as L.

What does this do for us? The new axiom system satisfies the completeness and soundness theorems. It's another reasonable axiom system. In reality, it's just L with a lemma disguised as an axiom. Big deal.

Suppose now that we add a formula that isn't a tautology as a new axiom. Remember that since we want to treat this new formula just like any other axiom, we have to allow any instance of the new formula to appear as a line in a proof. This always results in an inconsistent theory. (And inconsistent theories don't satisfy the Soundness Theorem.) Let's look at a particular example.

Consider adding $A \to B$ to L as a new axiom. We can show that the resulting theory is inconsistent: Notice that a particular instance of this new axiom is $A \to \neg A$ (where $\neg A$ is substituted for B. However, $A \to \neg A$ is not a tautology, so this new theory is not sound:

A	$\to$	$\neg A$
T	**F**	F
F	**T**	T

Let's summarize. If we add a tautology to L, we get L. If we add a non-tautology to L, we get garbage. It looks like adding axioms is not very profitable.

Discarding an axiom

Axiom 3 is particularly ugly. Can we throw it away? Unfortunately, the resulting theory doesn't satisfy the Completeness Theorem. Here's another way to descibe the situation. Axiom 3 can't be proved from Axiom 1 and Axiom 2. Also, since L is consistent, Axiom 1 and Axiom 2 can't prove the negation of Axiom 3. Logicians would say, "Axiom 3 is *independent* of Axiom 1 and Axiom 2." Independence statements of this sort are often very challenging to prove.

Overall, discarding axioms yields systems that don't satisfy the Completeness Theorem. This isn't such a hot way to modify L.

Starting from scratch

So far, we haven't had much luck. Maybe the best thing is to dump L, and start with a brand new axiom system. Lots of people have done this. Here are two examples.

Axiom System. Kleene's Axiom System for Propositional Calculus [6].

The axioms:

$A \to (B \to A)$
$(A \to (B \to C)) \to ((A \to B) \to (A \to C))$
$(A \wedge B) \to A$
$(A \wedge B) \to B$
$A \to (B \to (A \wedge B))$
$A \to (A \vee B)$

$B \to (A \vee B)$
$(A \to C) \to ((B \to C) \to ((A \vee B) \to C))$
$(A \to B) \to ((A \to \neg B) \to \neg A)$
$\neg\neg A \to A$

Use the above axioms with Modus Ponens. The theorems of this system are exactly the tautologies. In other words, completeness and soundness theorems hold for this system. By using this system, we could avoid using abbreviations to deal with conjunction and disjunction. If we wanted, we could add more axioms to deal with biconditional or any other connectives we might like to append.

Axiom System. Meredith's Axiom System for Propositional Calculus [9].

Here's the (only!) axiom:

$$((((A \to B) \to (\neg C \to \neg D)) \to C) \to E) \to ((E \to A) \to (D \to A))$$

Using the above axiom with Modus Ponens. The theorems of this system are exactly the tautologies. Meredith's system is very elegant with its single axiom and single rule of inference. Unfortunately, it is not so easy to prove theorems in this system or even to recognize instances of the axiom. For an exceptionally challenging exercise, try proving L1 in Meredith's system.

Exercises.

1. Show that Meredith's axiom is a tautology
2. Write down two instances of Meredith's axiom.
3. Prove the following using Kleene's axiom system:
   (a) $A \to A$
   (b) $A \to B, B \to C \vdash A \to C$
   (c) $A \to B \vdash \neg B \to \neg A$

1.11 Assessing Propositional Calculus

Propositional calculus is pretty nice. We've managed to talk about a lot of logic without being terribly technical. Our proof system, L, is slick. It's consistent, and has a deduction theorem, a soundness theorem, and a completeness theorem.

Propositional calculus is useful for analyzing lots of different sorts of arguments. In particular, we can use it to understand the structure of lots of mathematical proofs. For example, we know that mathematicians use the Deduction Theorem every day to prove implications. Also, mathematicians follow the format of L25 to prove biconditional statements.

The big disadvantage of propositional calculus is that it glosses over any fine distinctions. It's just not very expressive. For example, suppose we want to use propositional calculus to formalize the statement "if $n > 0$ then $n + 1 > 0$." If we let P denote $n > 0$ and Q denote $n+1 > 0$, then our formalization is $P \to Q$. This certainly shows us that the statement is an implication, but it hides the fact that the hypothesis and the conclusion are both talking about n. In order to overcome this limitation, we need a logical system that includes variables.

Exercises.

1. Use propositional calculus to formalize the following argument.
   Socrates is a man.
   All men have ugly feet.

   Socrates has ugly feet.

2. Is the argument in exercise 1 valid? Should it be?

Chapter 2

Predicate Calculus

Propositional calculus can express only the simplest of statements. Predicate calculus overcomes this difficulty by introducing variables and quantifiers. Variables will be used to represent an arbitrary object in the set of objects being studied, called the *universe*. Quantifiers will allow us to talk about a property holding *for all* objects or that *there exists* an object for which the property holds. The addition of quantified variables makes the language of predicate calculus sufficiently rich to express almost any mathematical notion.

We'll use our study of propositional calculus as a map for our study of predicate calculus. As before, we need to start by specifying what the formulas look like. Then we can talk about some semantics, looking for a notion that parallels the idea of tautologies. We'll do some formula rewriting, and then turn to proofs. The proof system we concoct will be consistent and have a deduction theorem, a soundness theorem, and a completeness theorem. We'll also cook up some shortcuts to make proofs easier to write. By then, it will be time to start a new chapter.

2.1 Building Blocks

What sort of symbols are used in predicate calculus? Roughly, what do the symbols represent? Here are the answers:

Predicates

We use capital letters, (A, B, C, etc.) to represent predicates. A predicate letter will usually be associated with a list of at least one variable. For example,

$$A(x) \qquad B(x, y, z) \qquad Q(n)$$

are all acceptable constructions. A predicate is used to represent a property of its variable(s) or a relationship between its variables. For example, $P(x, y)$

might represent the statement "$x < y$" or the statement "x and y are kinds of fish."

Sometimes, we'll use special predicate symbols like $=$, $\leq$, or $>$. Rather than writing the symbol in front of the variables, we'll put it between the variables. Thus, we would write $x = y$ rather than $= (x, y)$. Writing the predicate in front is called *prefix notation*. Writing it in the middle is called *infix notation*. No matter which notation we use or which symbols we use, we should specify any intended meaning of the predicate symbols.

Terms

The list after a predicate symbol can include more than just variables. Any *term* can be used in the list. Terms are either variables, constants, or functions applied to terms.

- Variables are small letters (like x, y, and z) representing an arbitrary object from the universe.
- Constants are underlined letters (like $\underline{a}$, $\underline{b}$, and $\underline{c}$) representing a particular object from the universe.
- Functions are small letters (like f, g, and h); functions take as input a list of terms and have a unique output.

Despite the fact that functions and variables are both denoted by small letters, it is easy to keep them straight. Functions have lists associated with them, just like predicates. For example, $f(x, y)$ is a function f applied to the variables x and y. Functions can act on other terms, too. For example, $g(x, \underline{a}, h(z))$ is the function g applied to the variable x, the constant $\underline{a}$, and the function h, where h is a function applied to z.

Functions and predicates differ in one very important respect. The value of a function is an object, while the value of a predicate is a truth value. For example, if we want to represent "the father of x," it makes sense to use a function like $f(x)$. On the other hand, if we want to say "x is a father," we would use a predicate symbol, like $P(x)$. If f(Chelsea) is Bill, then P(Bill) is true.

What sort of objects these terms represents depend upon the context, i.e., the universe of objects that we are examining. If we're talking about numbers, x would represent a number. If we're talking about milkmen, x would represent a milkman. A variable represents a non-specific object, like some milkman. A constant represents a particular object, like "Waldo the milkman who lives up the street." A function represents an object that is somehow related to the objects in its variable list. For example, if x represents a milkman in the universe of milkmen, then $f(x)$ could represent the milkman who took over x's old route. If $\underline{w}$ represents Waldo the milkman, then $f(\underline{w})$ represents the milkman who took over Waldo's old route.

Connectives

The connectives are $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$, and $\neg$. These are the same connectives we used in propositional calculus, and they mean exactly the same thing.

Quantifiers

We'll use $\forall$ and $\exists$ as our quantifier symbols. Quantifier symbols must be followed by a single variable (never a constant or a function).

$\forall x$ is read as "for all x."

$\exists x$ is read as "there exists an x."

We'll build all our formulas from the sorts of symbols listed above, inserting parentheses where we need them. If we need to represent an entire formula with a single letter, we'll just use a capital letter (A, B, C, etc.). If there is any possibility confusing a whole formula with a predicate, we'll be sure to include extra explanation. Usually, we will use $A(x, y, z)$ to represent a formula that includes the variables x, y, and z.

Rather than being really technical about what constitutes a properly constructed formula, let's look at some examples.

2.2 Translations

We can translate English statements into predicate calculus, and vice versa. In either case, we must be careful to specify what the symbols represent.

Predicate calculus into English.

Example. Assuming that the universe consists of the real numbers, and that $\cdot$, $-$, 0, 1, and $=$ have their usual meaning, we'll translate the following into English.

(a) $\forall x(x \cdot 0 = 0)$
For all real numbers x, x times 0 equals 0.

(b) $\forall x(x \cdot x - x = 0 \rightarrow (x = 0 \vee x = 1))$
For all real numbers x, if $x \cdot x - x = 0$ then either $x = 0$ or $x = 1$.

(c) $\forall x \exists y(x \cdot y = 1)$
For all real numbers x, there is a real number y such that $x \cdot y = 1$.

Example. Assuming that the universe consists of the natural numbers $\mathbb{N} = \{0, 1, 2, ...\}$, $f(x)$ means $x + 1$, and $B(x)$ means $x = 0$, translate the following into English.

(a) $\forall x \neg B(f(x))$
For all natural numbers x, it is not true that $x + 1 = 0$.
We can make it sound more natural: For all natural numbers x, $x + 1 \neq 0$.

(b) $\exists x B(f(x))$
There is a natural number x, such that $x + 1 = 0$.

(c) $\exists x \neg B(f(x))$
There is a natural number x, such that $x + 1 \neq 0$.

Most of the translations we have done to this point involved one quantifier. Before proceeding let's consider the following example, which will clarify the convention on how to interpret multiple quantifiers:

Example. Let the universe be the set of all people, and the predicate $L(x, y)$ stand for x loves y (and equivalently, y is loved by x). Here are all of the possible versions with x and y quantified. Notice the careful treatment of the translation in each case. "Loves" is not assumed to be reflexive here.

Both variables quantified with $\forall$:
$\forall x \forall y L(x, y)$: Everyone loves everyone.
$\forall y \forall x L(x, y)$: Everyone is loved by everyone.
These sentences mean the same thing, and this will be true for all interpretations, as we will prove more formally later.

Both variables quantified with $\exists$:
$\exists x \exists y L(x, y)$: Someone loves someone.
$\exists y \exists x L(x, y)$: Someone is loved by someone.
Again, these sentences mean the same thing, and this will be true for all interpretations, as we will prove more formally later.

First variable quantified with $\forall$:
$\forall x \exists y L(x, y)$: Everyone loves someone.
$\forall y \exists x L(x, y)$: Everyone is loved by someone.
These sentences do not mean the same thing. In the first case a more formal translation would be "Every person has someone that they love." In the second case, "Every person has someone who loves them." The order of the variables is important here.

First variable quantified with $\exists$:
$\exists x \forall y L(x, y)$: Someone loves everyone.
$\exists y \forall x L(x, y)$: Someone is loved by everyone.
Again, these sentences do not mean the same thing. In the first case we have "there is someone who loves all people." In the second case, "there is someone who is loved by everyone." Notice also that none of the four alternations of quantifiers means the same thing. Order is extremely important!

English into predicate calculus

Example. Let's begin by formalizing: For all natural numbers n, $n \leq n^2$. We have several choices for formalizing this statement. Let the universe be all

natural numbers. Let $s(x)$ be the function x^2 and $P(x, y)$ be the predicate for $x \leq y$. We can formalize the statement as:

$$\forall x \ P(x, s(x)).$$

On the other hand, we can use the $\leq$ and square symbols with their usual meanings directly and use n as our variable name:

$$\forall n(n \leq n^2).$$

What if we needed the universe to be all real numbers rather than all natural numbers? How could we adapt the first version to handle this? We would need to have a new predicate for "x is a natural number." Let $N(x)$ stand for this:

$$\forall x(N(x) \rightarrow P(x, s(x))).$$

Example. Now let's try a more complex example: Socrates is a man. All men have ugly feet. Socrates has ugly feet. Again, we can proceed in several ways. Let the universe be the set of all people. Let $U(x)$ be the predicate x has ugly feet. Let $M(x)$ be the predicate x is a man. Let $\underline{s}$ be the constant in the universe representing the man Socrates. Then the three statements above translate as follows.

$$M(\underline{s}) \qquad \forall x(M(x) \rightarrow U(x)) \qquad U(\underline{s})$$

Example. Let's look at a statement that uses a function in a non-mathematical universe. Translate: Each man has a father. There are a variety of ways proceed. Let the universe be all men. Let $f(x)$ be the function " father of x." Let $S(x, y)$ mean is that x same person as y. Then we can formalize the statement as

$$\forall x \exists y S(y, f(x)).$$

Exercises.

1. Assuming that the universe consists of all people, $f(x)$ means "father of x," and $B(x)$ means "x is the chancellor," translate the following into English.
   (a) $\forall x \neg B(f(x))$
   (b) $\exists x B(x)$
   (c) $\exists x \neg B(x)$
2. Assuming that the universe consists of all people, $f(x)$ means "father of x," $D(x)$ means "x is tiny," and $\underline{w}$ represents Waldo, translate the following into English.
   (a) $\forall x(D(x))$
   (b) $D(\underline{w})$
   (c) $\forall x(D(f(x)) \rightarrow D(x))$

(d) $\neg\exists x(D(x))$

3. Assuming that the universe is the set of natural numbers, $E(x)$ means "x is even," $O(x)$ means "x is odd," and $S(x)$ means "x is a multiple of 3," translate the following into English.

   (a) $\forall x(E(x) \vee O(x))$

   (b) $\forall x(S(x) \rightarrow O(x))$

   (c) $\exists x(S(x) \wedge \neg E(x))$

   (d) $\forall x(O(x)) \rightarrow \forall x(E(x))$

4. Assume the universe is all real numbers and $L(x, y)$ means x is less than y. Match each formula in the first list with a translation in the second list.

   (a) $\forall x \forall y L(x, y)$

   (b) $\forall y \forall x L(x, y)$

   (c) $\exists x \exists y L(x, y)$

   (d) $\exists y \exists x L(x, y)$

   (e) $\forall x \exists y L(x, y)$

   (f) $\forall y \exists x L(x, y)$

   (g) $\exists x \forall y L(x, y)$

   (h) $\exists y \forall x L(x, y)$

      i. There is a real number that is greater than any real number.

      ii. There is a real number that is less than any real number.

      iii. Given any real number, we can find a greater real number.

      iv. Given any real number, we can find a lesser real number.

      v. If x and y are reals, then x is less than y.

      vi. There are reals x and y such that x is less than y.

5. Formalize: No elbow is an ankle.

6. Assume that the universe is the set of all fish. Using the information below, formalize each of the given statements.

   - $T(x)$ means "x is a trout"
   - $S(x)$ means "x is shiny"
   - $J(x)$ means "x jumps"

   (a) Formalize: All fish are trout.

   (b) Formalize: Some trout are shiny.

   (c) Formalize: Not all trout jump.

   (d) Formalize: No trout jump.

7. Formalize: If x is a non-zero real number, then for some y, $x \cdot y = 1$.

8. Formalize the four statements below, assuming that the universe is all men.

   (a) All men are giants.

   (b) No men are giants.

   (c) Some men are giants.

   (d) Some men are not giants.

9. Repeat exercise 8 assuming that the universe is all living things.

10. Formalize the following:

    (a) Everyone is respected by someone.

    (b) Someone is respected by everyone.

    (c) No one is respected by everyone.

    (d) Someone is respected by no one.

    (e) Everyone should help her neighbors or her neighbors will not help her.

    (f) All parents love their children.

    (g) No number is divisible by zero.

2.3 A brief interlude: Truth

What is truth? Nice question; let's ignore it.

When is a formula true? This seems like an easier question. When we were translating formulas into English, it seemed like it would be easy to assign a truth value to the *translated* formulas. This is a good observation. A formula might be true or false, depending on how we interpret the symbols. Before we can nail down the notion of truth, we need to talk some more about interpretations.

Here's another problem. Suppose our universe is the real numbers and the symbols $=$ and 2 have their usual meaning. Is the formula $\forall x(x = 2)$ true? It's reasonable to say no. We know that $3 \neq 2$, so it is not the case that for all real numbers x, $x = 2$. Now consider the formula $\exists x(x = 2)$. Is this formula true? It's reasonable to say yes, this time. There is a real number x, such that $x = 2$. What about the formula $x = 2$? Is $x = 2$ true or false? It's reasonable to say "none of the above." The truth value of $x = 2$ depends on what you plug in for x. So, we had no problems with truth values for $\forall x(x = 2)$ and $\exists x(x = 2)$, but $x = 2$ gives us fits. Truth must have something to do with quantifiers. We'd like a way to tell if a formula is going to cause problems, just by looking at where the quantifiers are.

So now we have two tasks. First, let's look at how quantifiers act on formulas. Then we'll specify exactly what information we need to generate good translations of formulas. That's what is in the next two sections. Once we have the tools we need, we'll talk about truth.

2.4 Free variables

Usually, when we write quantifiers, we put a pair of parentheses afterwards indicating the part of the formula that the quantifier affects. The stuff in the parentheses is called the *scope* of the quantifier. Let's look at some examples.

Example. Indicate the scope of $\forall x$ in the formula:

$$\forall x(P(x) \to \forall y(R(x) \vee Q(y))) \wedge B(x)$$

Because of the parentheses, the scope of $\forall x$ in this example stops just before the $\wedge$:

$$\forall x\underline{(P(x) \to \forall y(R(x) \vee Q(y)))} \wedge B(x)$$

Example. Indicate the scope of $\forall y$ in the formula:

$$\forall x(P(x) \to \forall y(R(x) \vee Q(y))) \wedge B(x)$$

This time, we can just match the parentheses following the $\forall y$ quantifier.

$$\forall x(P(x) \to \forall y\underline{(R(x) \vee Q(y))}) \wedge B(x)$$

Sometimes, if there are several quantifiers, we leave out some parentheses. If we put the parentheses back in, it's easy to find the scopes.

Example. Indicate the scope of $\forall x$ in the formula:

$$\forall x \exists y(D(x, y)) \wedge B(x)$$

Again, the $B(x)$ is not within the scope of the $\forall x$:

$$\forall x\underline{\exists y(D(x, y))} \wedge B(x)$$

Whenever a variable occurs in the scope of a quantifier on that variable, we say that the occurrence of the variable is *bound*. Any occurrence of a variable which is not bound is called *free*. We could also say this as follows. The quantifier $\forall x$ captures all the xs in its scope. (It ignores any ys or other variables, and it ignores everything that's not in its scope.) Any x that is captured is bound. Any x that isn't bound is free. The terminology is the same for other quantifier and variable combinations, like $\forall y$ or $\exists z$.

Example. Underline the free occurrences of variables in the formula:

$$\forall x(P(x) \to \forall y(R(x) \vee Q(y))) \wedge B(x)$$

Since $P(x)$ and $Q(x)$ occur in the scope of the first $\forall x$ and $Q(y)$ is within the scope of $\forall y$, only the x in $B(x)$ is free. Thus, our answer is:

$$\forall x(P(x) \to \forall y(R(x) \vee Q(y))) \wedge B(\underline{x})$$

Example. Underline the free occurrences of variables in the formula:

$$\exists x \forall y M(x, y, f(x, z)) \vee G(x, y, z)$$

The predicate $M(x, y, f(x, z))$ is included in the scope of quantifiers on the variables x and y. The predicate $G(x, y, z)$ is not in the scope of any quantifier. Underlining the free variables gives us:

$$\exists x \forall y M(x, y, f(x, \underline{z})) \vee G(\underline{x}, \underline{y}, \underline{z})$$

One more piece of terminology. A formula with no free variables is called *closed*. (Some people call closed formulas *sentences*.) Using this terminology, we can see that $\forall x(x = 2)$ is closed, $\exists x(x = 2)$ is closed, and $x = 2$ is not closed.

Exercises.

1. Underline the free occurrences of variables in the following formulas.
   (a) $\forall x(P(x, y) \rightarrow \exists z(P(x, z)))$
   (b) $\exists x \forall y(P(x, y) \vee P(y, x) \vee Q(z, z))$
   (c) $\forall y(P(x, y) \rightarrow \forall x(P(x, y)))$
   (d) $Q(z, 0) \rightarrow \exists x(Q(z, x))$
   (e) $P(f(x), x) \vee \exists y(P(f(y), y))$
   (f) $\exists y(P(x, y) \rightarrow \exists x(P(x, z)))$
   (g) $\exists z \exists w(R(x, y, z))$
   (h) $B(x) \vee \forall x(P(x, y))$
   (i) $\forall z(P(z, f(z)) \vee P(z, y))$
   (j) $\forall x(P(x, g(0, x, y)) \vee B(y) \vee \exists y(B(y)))$
2. Which of the following formulas are sentences?
   (a) $\exists x P(x, y)$
   (b) $\forall y \exists x P(x, y)$
   (c) $\forall y \exists x P(0, y)$
   (d) $\forall y \exists x P(z, y)$
   (e) $\forall y P(0, y)$
   (f) $\forall y P(x, 0)$
   (g) $\exists x P(x, 0)$
   (h) $\exists x P(0, y)$

2.5 Models

Back in section 2, we were given information that we used to translate formulas into English. A list of information used in translations is called a *model*. Our models must include:

- a universe,
- interpretations of all predicate symbols,
- interpretations of all function symbols, and
- interpretations of all constant symbols.

There are a few rules. The interpretations of the predicate symbols must make sense for everything in the universe. The interpretations of the function symbols must be functions that are defined for everything in the universe and take values in the universe. Finally, the constants must be specific elements of the universe.

There is a lot of freedom in defining a model. We can make the predicates, functions, and constants mean pretty much whatever we like. Notice that we don't get to redefine the quantifiers or connectives, though. $\forall x$ always means "for all x", and $\vee$ always means "or". Some things never change.

Example. Construct three different models where the formula

$$\forall x \exists y (P(x, y) \vee B(x))$$

can be interpreted. Give three corresponding translations of the formula.

1. Let the universe be all real numbers, let $P(x, y)$ represent *x is greater than y*, and let $B(x)$ represent *x is rational*. A translation in this model is:

   For all real numbers x, there is a corresponding real number y where either x is greater than y or x is rational.

2. Let the universe be all people, let $P(x, y)$ represent *x is y's father*, and let $B(x)$ represent *x is deceased*. A translation in this model is:

   For all people x, there is a corresponding person y where either x is y's father or x is deceased.

3. Let the universe be cans of soup, let $P(x, y)$ represent *x was canned after y*, and let $B(x)$ represent *x is too old to eat*. A translation in this model is:

   For all cans of soup x, there is a corresponding can y where either x was canned after y or x is too old to eat.

Example. Construct three different models where the formula

$$\forall x \exists y L(f(x, 0), y)$$

can be interpreted. Give three corresponding translations of the formula.

1. Let the universe be real numbers, $f(x, y)$ denote $x \cdot y$ (usual multiplication), 0 denote 0, and $L(x, y)$ denote $x > y$ (usual inequality). A translation in this model is:

   For every real number x, we can find a real number y such that $x \cdot 0 > y$. (Note that this statement is true in this model.)

2. Let the universe be $\{0, 1, 2, 3, \cdots\}$ (natural numbers), and $f(x, y)$ denote $x \cdot y$ (usual multiplication). Note that for every pair of natural numbers, this function gives a natural number value. We couldn't have picked something like $x - y$ here. Let 0 denote 0, and $L(x, y)$ denote $x > y$ (usual inequality). A translation in this model is:

   For every natural number x, we can find a natural number y such that $x \cdot 0 > y$. (Note that this statement is false in this model.)

3. Let the universe be all people and suppose $f(x, y)$ denotes the youngest person in the set $\{y$, the father of $x\}$. Note that for any pair of people chosen, the function yields a person. Let 0 denote Zeno, and let $L(x, y)$ denote "x was born before y was born." A translation in this model is:

   For every person x, we can find a person y such that the younger of x's father and Zeno was born before y was born. (This statement is true in this model, since if x's father is younger than Zeno we can set y to be x, and otherwise we can let y be Einstein.)

Exercises.

1. Construct three different models where the formula

   $$\forall x(S(x) \rightarrow \exists y(C(x, y)))$$

   can be interpreted. Give three corresponding translations of the formula.

2. Construct three different models where the formula

   $$\forall x \exists y(x = y \vee x + 1 > y)$$

   can be interpreted. Be sure to indicate meanings for the predicate $=$, the predicate $>$, the function $x + y$, and the constant symbol 1. Give three corresponding translations of the formula.

3. Construct three different models where the formula

   $$\forall x \exists y(x = y \wedge f(x) = y)$$

   can be interpreted. Give three corresponding translations of the formula.

2.6 Truth and Sentences

Recall that a *sentence* is a formula with no free variables. Generally speaking, it is easy to determine if a sentence is true provided that we are told what the various symbols represent. We say that a sentence A is *true in the model M,* if the translation of A using the information from M is true. Similarly, we say that a sentence B is *false in the model M,* if the translation of B using the information from M is false.

Remember, the definitions above only work for sentences, so any free variables could throw a serious kink in things. Also, it's good to note that these definitions always work, so given any sentence A and any model M, either A is true in M, or A is false in M.

You may feel that these definitions are too informal. That's reasonable. "Tarski's truth definition" is a much more precise way of presenting the same concept. Good sources for more information on Tarski's definition include [8] and [11].

Here are some examples.

Example. Let M be the model where the universe is the collection of people, $C(x)$ means x is a chancellor, and $L(x)$ means x lives on a university campus. Decide if the following sentences are true in M or false in M.

1. $\forall x C(x)$

   "All people are chancellors" is false.

2. $\forall x L(x)$

   "All people live on university campuses" is false.

3. $\exists x(C(x) \wedge L(x))$

   "There is someone who is both a university chancellor and lives on a campus" is true.

4. $\exists x(L(x) \wedge \neg C(x))$

   "There is someone who both lives on a campus and is not a chancellor" is true.

5. $\forall x(L(x) \rightarrow C(x))$

   "Living on a campus implies one is a chancellor" is false.

   Alternately, "every person who lives on a campus is a chancellor" is false.

Example. Let M be the model where the universe is the natural numbers, $C(x)$ means x is a multiple of 10, and $L(x)$ means x is even. Decide if the following sentences are true in M or false in M.

1. $\forall x C(x)$

   "All natural numbers are multiples of 10" is false, since 9 is not a multiple of 10.

2. $\forall x L(x)$

   "All natural numbers are even" is false, since 3 is not even.

3. $\exists x(C(x) \wedge L(x))$

   "There is a natural number that is both even and a multiple of 10" is true. For example, 20 is such a number.

4. $\exists x(L(x) \wedge \neg C(x))$

   "There is a natural number that is both even and not a multiple of 10" is true. For example, 4 is such a number.

5. $\forall x(L(x) \rightarrow C(x))$

   "For all natural numbers, being even implies being a multiple of 10" is false, since 4 is even but not a multiple of 10.

Exercises.

1. Let K be the model where the universe is the natural numbers, $G(x, y)$ means x is greater than y and $h(x)$ represents the function $x+1$. Decide if the following sentences are true in K or false in K. Justify your answers.

   (a) $\forall x \forall y G(x, y)$

   (b) $\forall x G(h(x), x)$

   (c) $\forall x \exists y G(x, y)$

   (d) $\forall y \exists x G(x, y)$

   (e) $\forall x \forall y(G(x, y) \rightarrow \exists z(G(x, z) \wedge G(z, y)))$

2. Let K be the model where the universe is the real numbers, $G(x, y)$ means x is greater than y and $h(x)$ represents the function $x + 1$. Decide if the following sentences are true in K or false in K. Justify your answers.

   (a) $\forall x \forall y G(x, y)$

   (b) $\forall x G(h(x), x)$

   (c) $\forall x \exists y G(x, y)$

   (d) $\forall y \exists x G(x, y)$

   (e) $\forall x \forall y(G(x, y) \rightarrow \exists z(G(x, z) \wedge G(z, y)))$

3. Find a model M where the sentence $\forall x \exists y A(x, y)$ is true, and the sentence $\exists y \forall x A(x, y)$ is false.

4. Can you find a model M where the sentence $\forall x \exists y A(x, y)$ is false, and the sentence $\exists y \forall x A(x, y)$ is true? Explain.

2.7 Truth and free variables

Our definitions of true and false in models only apply to sentences. Now we want to extend these definitions to formulas with free variables. Suppose that $A(x)$ is a formula with the free variable x. Suppose that M is a model.

- We say that $A(x)$ is true in M if $\forall x A(x)$ is true in M.
- We say that $A(x)$ is satisfiable in M if $\exists x A(x)$ is true in M.
- We say that $A(x)$ is false in M if $\exists x A(x)$ is false in M.

Note that if $A(x)$ is true in M, then $A(x)$ is satisfiable in M. The converse of this statement is not always true. In cases where our formulas have more than one free variable, we just tack more quantifiers on the front. For example, $A(x, y, z)$ is true in M if $\forall x \forall y \forall z A(x, y, z)$ is true in M, $A(x, y, z)$ is satisfiable in M if $\exists x \exists y \exists z A(x, y, z)$ is true in M, and $A(x, y, z)$ is false in M if $\exists x \exists y \exists z A(x, y, z)$ is false in M.

Example. Let M be the model where the universe is the real numbers, $G(x, y)$ means $x > y$, and $h(x)$ represents the function $x + 1$. Classify the following formulas as true in M, false in M, or satisfiable in M.

1. $G(x, x)$

   This is false in the model, because there does not exist a real number that is less than itself.

2. $G(x, h(x))$

   This is false in the model, because there does not exist a real number that is greater than one plus itself.

3. $G(0, x)$

   This is satisfiable in the model, because 0 is greater than negative two plus one, so there is a number for which the formula is true. Also, not all real numbers work, so the formula is satisfiable but not true.

4. $G(h(x), 0)$

   This is satisfiable in the model, because one plus one is greater than zero, so there is a number for which the formula is true. Also, not all real numbers work, so this formula is satisfiable but not true.

5. $G(x, y)$

   This is satisfiable in the model, because we can find numbers x and y where $x < y$. Also, not all real numbers would work, so the formula is satisfiable but not true.

Example. Let K be the model where the universe is the natural numbers $\mathbb{N} = \{0, 1, 2, ...\}$, $G(x, y)$ means $x > y$, and $h(x)$ represents the function $x + 1$. Classify the following formulas as true in K, false in K, or satisfiable in K. This is the same set of formulas as in the previous example; note how the truth values are different.

1. $G(x, x)$

   False – same as part 1 above.

2. $G(x, h(x))$

   False – same as part 2 above.

3. $G(0, x)$

   False – not the same as part 3 above because we are now looking at the natural numbers, which do not include the negative numbers.

4. $G(h(x), 0)$

   True – not the same as part 4 above because we are now looking at the natural numbers, which do not include the negative numbers.

5. $G(x, y)$

   Satisfiable but not true– same as part 5 above.

Exercises.

1. Consider the formula $P(x, 0)$. Find a model where this formula is true, a model where it is satisfiable but not true, and a model where it is false.

2. Consider the formula $\forall x S(x, y)$. Find a model where this formula is true, a model where it is satisfiable but not true, and a model where it is false.

3. Consider the formula $\exists y R(x, y)$. Find a model where this formula is true, a model where it is satisfiable but not true, and a model where it is false.

4. Consider the formula $x = 2$. Find a model where this formula is true, a model where it is satisfiable but not true, and a model where it is false. (Hint: Every model in which this statement can be interpreted must contain an element which is represented by the constant symbol 2. Consequently, in a model where the formula is false, the meaning assigned to the predicate symbol = must be different from equality. Some logicians feel that = is such a special symbol that this sort of redefinition should never be allowed.)

2.8 Logical validity

As we have seen, many formulas are true in some models and false in others. Here's a reasonable question: *Are some formulas true in every model?* The examples considered in the preceding sections tend to indicate that the answer is no. We have always been able to contrive models where our formulas are false. However, the examples that we looked at were not a random sample.

Consider the formula:

$$\forall x A(x) \vee \neg \forall x A(x)$$

It is true in all models because without specifying the formula interpretations we can still determine the truth value. The left formula, $\forall x A(x)$, is always going to be translated as *property A is true for all x*. The right formula, $\neg \forall x A(x)$, is always going to be translated as *property A is not true for all x* – which covers the case that property A is never true as well as the case that property A doesn't hold in some cases. It is clear that either the left disjunct or the right disjunct must be true, regardless of the particular interpretations in a given model.

Formulas like the one above are very important. From just the structure of the formula (syntax), we can draw conclusions about the truth of the formula (semantics). It would be nice to have some good vocabulary for talking about these formulas.

We say that a formula is *logically valid* (or just valid) if it is true in every model. We say that a formula is *contradictory* if it is false in every model. Note that some formulas are neither logically valid nor contradictory.

The notion of a *logically valid formula* is particularly important for us. Recall that tautologies were formulas of propositional calculus which were true no matter what truth assignments we made to the statement letters. Similarly, logically valid formulas are true no matter which model we consider. The logically valid formulas play the same role in predicate calculus that the tautologies play in propositional calculus. We have found the parallel to tautologies that was promised at the beginning of the chapter.

In one way, tautologies and logically valid formulas are very different. To show that a formula is a tautology, all we need to do is construct the truth table. To show that a formula is logically valid, we must show that it is true in every possible model, regardless of the choice of the universe or however bizarre the interpretations of the predicates might be. This sounds like a challenging job.

Here are two more definitions that will help us experiment with logically valid formulas. We say that a formula A *logically implies* a formula B if the formula $A \rightarrow B$ is logically valid. We say that a formula A is *logically equivalent* to a formula B if the formula $A \leftrightarrow B$ is logically valid.

Using the preceding definitions, we can show that if A logically implies B and B logically implies A, then A and B are logically equivalent. Suppose that A logically implies B and B logically implies A. Then the formulas $A \rightarrow B$ and $B \rightarrow A$ are logically valid. Pick any model M. Because they are logically valid formulas, both $A \rightarrow B$ and $B \rightarrow A$ must be true in M. On the basis of the truth table for $A \leftrightarrow B$, it follows that $A \leftrightarrow B$ is true in M. This reasoning

holds for any model M we might select, so $A \leftrightarrow B$ is true in every model. By the definition of logical equivalence, this shows that A is logically equivalent to B.

Exercises.

1. Give an example of a logically valid formula.
2. Give an example of two logically equivalent formulas.
3. Give an example of formulas A and B such that A logically implies B, but B does not logically imply A.

2.9 Formulas that aren't logically valid

As noted in the previous section, to show that a formula is logically valid, we must show that it is true in every possible model. Consequently, to show that a formula is not logically valid, all we need to do is construct one model where the formula is not true. We already know how to build models, so this task is not so difficult.

Before doing some examples, we should compare this to our experience with propositional logic. Note that constructing a model to show that a formula is not logically valid corresponds roughly to finding one line in a truth table that shows that a propositional formula is not a tautology. Thus the model building in the following examples is like the "line building" we did in Chapter 1.

Example. Show that $\forall x(A(x) \vee B(x))$ is not logically valid.

Consider the universe of real numbers, and let $A(x)$ mean *x is odd* and $B(x)$ mean *x is an integer multiple of 10*. "All real numbers are either odd or an integer multiple of 10" is false. For example, 4 is neither odd nor an integer multiple of 10. We have found a model in which the sentence is false, so the sentence is not logically valid.

Example. Show that $\forall x \exists y C(x, y)$ does not logically imply $\exists y \forall x C(x, y)$.

We will need to construct a model where $\forall x \exists y A(x, y)$ is true, but $\exists y \forall x A(x, y)$ is false. Here is an entertaining graphical technique for building finite models. Let the universe be $\{0, 1\}$. Draw an arrow from from 0 to 1 and a second arrow from 1 to 0. Let $A(x, y)$ mean that there is an arrow from x to y. For every choice of x, there is an arrow that starts at x, so $\forall x \exists y A(x, y)$ is true in this model. On the other hand, $A(0, 0)$ and $A(1, 1)$ are both false, so $\exists y \forall x A(x, y)$ is false.

Exercises.

1. Show that $\forall x(A(x) \wedge B(x))$ is not logically valid.
2. Show that $\forall x \exists y C(x, y)$ is not logically valid.

3. Show that $\exists x(A(x) \to B(x))$ does not logically imply $(\exists x A(x)) \to (\exists x B(x))$.

4. Show that $\forall x \exists y C(x, y)$ does not logically imply $\exists z C(z, z)$.

5. Show that $(\forall x A(x)) \leftrightarrow (\forall x B(x))$ is not logically equivalent to $\forall x(A(x) \leftrightarrow B(x))$.

6. Show that the formula

$$\exists x \forall y((C(x, y) \wedge \neg C(y, x)) \to (C(x, x) \leftrightarrow C(y, y)))$$

is not logically valid. (Warning: This one is tough.)

2.10 Some logically valid formulas

In the previous section, we found a method for showing that a formula is not logically valid. Our model theoretic method works on any formula, provided that it's not logically valid. This is not very satisfying. What we would really like is a method for showing that a formula is logically valid. Eventually, we will develop a technique for doing just that. In the mean time, it would be nice to have a method for showing that *some* formulas are logically valid. In this section, we will list (an infinite number of) logically valid formulas.

We say that a formula is an *instance of a tautology* if it is the result of uniformly replacing the statement letters in a propositional tautology with formulas of predicate calculus. Note that determining whether or not a formula is an instance of a tautology depends only on its structure. We only consider the shape of the formula, ignoring meaning and models.

The formula $p \to p$ is a tautology, so anything with this pattern is. Here are two instances of tautologies based upon this pattern:

$$\exists x \forall y Q(x, y) \to \exists x \forall y Q(x, y)$$

$$A(x) \to A(x)$$

Similarly, $A \to (B \to A)$ is a tautology, so

$$\forall x \exists y C(x, y) \to (\forall x A(x) \to \forall x \exists y C(x, y))$$

is an instance of a tautology.

Here is the fact that makes instances of tautologies interesting. *Every instance of a tautology is logically valid.* Since we can easily construct instances of tautologies, we can easily list lots of logically valid formulas. We've already seen three:

$$\exists x \forall y Q(x, y) \to \exists x \forall y Q(x, y)$$

$$A(x) \to A(x)$$

$$\forall x \exists y C(x, y) \to (\forall x A(x) \to \forall x \exists y C(x, y))$$

Note that the formula $A(x) \to A(x)$ has a free variable. Since we know it is logically valid, we know it is true in every model. Now $A(x) \to A(x)$ is true in a model M exactly when $\forall x(A(x) \to A(x))$ is true in M. Formulas that are true in every model are logically valid, so $\forall x(A(x) \to A(x))$ is logically valid.

The reasoning of the preceding paragraph works for any formula and any variable. If we know that P is a logically valid formula, then so are the formulas $\forall xP$, $\forall yP$, $\forall x\forall yP$, and so on. We can use this rule to build logically valid formulas that are not instances of tautologies. For example, $A(x) \to A(x)$ is an instance of a tautology, $\forall x(A(x) \to A(x))$ is not an instance of a tautology, but both are logically valid.

Here's another way to build more logically valid formulas. If a formula P is true in a model M, then it is satisfiable in M. Since P is satisfiable in M, the formula $\exists xP$ is true in M. Consequently, if P is logically valid, then so is $\exists xP$. As with adding universal quantifiers, this works for any formula P and any variable x. We can combine this with our previous work to build more complicated logically valid formulas. For example, $\forall x\exists y(C(x,y) \to \neg\neg C(x,y))$ is logically valid, but not an instance of a tautology.

Summarizing, any instance of a tautology is logically valid. Any formula gotten by stringing quantifiers in front of a logically valid formula is logically valid. Not every logically valid formula is an instance of a tautology. Indeed there are logically valid formulas that simply cannot be built using the techniques of this section.

Exercises.

1. Each of the following formulas is logically valid. Mark those that are instances of tautologies.
   (a) $A(x) \to (\forall yB(y) \to A(x))$
   (b) $\forall x(A(x) \to (\forall yB(y) \to A(x)))$
   (c) $A(x) \to (\neg B(y) \vee B(y))$
   (d) $\exists x(A(x) \to (\neg B(y) \vee B(y))$
   (e) $\exists x(\neg\neg A(x) \to (\neg B(y) \vee B(y))$
   (f) $\exists y\exists x(\neg\neg A(x) \to (\neg B(y) \vee B(y))$
2. Each of the following formulas is logically valid. Mark those that are instances of tautologies.
   (a) $C(x,y) \to C(x,y)$
   (b) $\forall x\exists y(C(x,y) \to C(x,y))$
   (c) $\forall x\exists yC(x,y) \to \forall x\exists y\neg\neg C(x,y)$
   (d) $\forall x\exists yC(x,y) \to \neg\neg\forall x\exists yC(x,y)$
   (e) $A(x) \vee \neg A(x)$
   (f) $\forall x(A(x) \vee \neg A(x))$

2.11 Free for...

Here is a summary of what we can do so far. If someone says, "Here is a formula which is not logically valid; show that this is the case," then we build a model where the formula isn't true. If someone says, "Here is a formula which *is* logically valid; show that this is the case," then we check if the formula is an instance of a tautology. If it isn't, we try to build the formula by tacking some quantifiers onto an instance of a tautology. If this works, we're done. Otherwise, we're stuck.

We would like some *guaranteed* method of showing that a formula is logically valid. We know that logically valid formulas are predicate calculus analogs of tautologies. We can show that a formula is a tautology by checking the truth table or writing a proof in L. If we had a proof system for predicate calculus, we could show that a formula is logically valid just by writing a proof.

In order for this scheme to work, our proof system for predicate calculus must have two properties. First, every formula that is provable must be logically valid. In other words, our proof system must be sound. This ensures that we don't get wrong answers. Secondly, every logically valid formula must be provable in the system. In other words, our proof system must be complete. This ensures that we can always get an answer.

In order to even state the axioms we need, we will need to elaborate on our notions of free and bound variables. We need a more sophisticated notion of when a variable is free. In particular, we need to know when we can substitute one variable (or term) for another variable.

Recall that in section 2.4, we said that an occurrence of a variable is *free* if it is not in the scope of a quantifier on that variable. An occurrence which isn't free is called *bound*. Also, recall that a *term* is part of a formula which refers to an object in a model. That is, a term may be a variable, a constant, or the result of applying a function to terms.

Here's the question that we want to answer: "When is it O.K. to plug in a given term for a particular variable in a given formula?" What sort of situations might cause problems? Consider the formula $\forall x P(x, y)$. Note that y is a free variable in this formula, while x is not. We cannot substitute something for x, since the quantifier $\forall$ indicates that the formula must be true for all x. But, since y is free, we have flexibility and should be able to substitute a term in for y.

Here are some examples of substitutions.

$\forall x P(x, z)$ – another variable is allowed. As with any mathematical variable, the particular name is unimportant.

$\forall x P(x, f(\underline{c}, z, w))$ – a function of several constants and variables is also allowed. Think of it as an analogy to a composition of functions.

$\forall x P(x, x)$ – This substitution is not as general as the last. Substituting x in for y changes the meaning of this formula since we now have bound a variable that was previously free.

$\forall x P(x, h(x))$ – As with the last substitution, this one "binds" a variable that was previously free.

When working with formulas in predicate calculus, we will not allow substitutions like the last two. The first two are fine. We can nail this concept down with a single definition. It's a little technical, but that's what makes it precise and useful.

Definition. A term t is free for a variable x in the formula P if x does not occur free within the scope of a quantifier on a variable in t.

We can approximate this definition as follows. It's fine to plug in a term for a free variable if none of the variables in the term are accidentally captured by quantifiers.

Example. Consider the terms x, y, $f(x, y)$, and 3. Determine which of these terms are free for x in each formula below.

1. $\forall y(A(x, y) \vee B(z))$
   (a) x is free for x in $\forall y(A(x, y) \vee B(z))$; x is always free for itself.
   (b) y is not free for x in $\forall y(A(x, y) \vee B(z))$; it would be in the scope of the $\forall y$.
   (c) $f(x, y)$ is not free for x in $\forall y(A(x, y) \vee B(z))$; it would be in the scope of the $\forall y$.
   (d) 3 is free for x in $\forall y(A(x, y) \vee B(z))$; constants can never be captured by quantifiers.
2. $A(x) \vee \forall z(C(z, z) \wedge A(z, y))$

   Terms:
   (a) x is free for x in $A(x) \vee \forall z(C(z, z) \wedge A(z, y))$; $A(x)$ is not in the scope of any quantifiers and x is always free for x in any formula anyway.
   (b) y is free for x in $A(x) \vee \forall z(C(z, z) \wedge A(z, y))$; $A(x)$ is not in the scope of any quantifiers.
   (c) $f(x, y)$ is free for x in $A(x) \vee \forall z(C(z, z) \wedge A(z, y))$; $A(x)$ is not in the scope of any quantifiers.
   (d) 3 is free for x in $A(x) \vee \forall z(C(z, z) \wedge A(z, y))$; $A(x)$ is not in the scope of any quantifiers, and constants can never be captured by quantifiers anyway.
3. $B(y) \rightarrow \forall y(A(x, z) \wedge \exists x C(x, y))$

   Terms:
   (a) x is free for x in the formula $B(y) \rightarrow \forall y(A(x, z) \wedge \exists x C(x, y))$; the only free occurrence of x is in the $A(x, z)$ predicate, and x is always free for x.

(b) y is not free for x in the formula $B(y) \to \forall y(A(x,z) \wedge \exists x C(x,y))$; x occurs free in the $A(x,z)$ predicate, and y will be captured by the $\forall y$ quantifier.

(c) $f(x,y)$ is not free for x in the formula $B(y) \to \forall y(A(x,z) \wedge \exists x C(x,y))$; x occurs free in the $A(x,z)$ predicate, and the y in $f(x,y)$ will be captured by the $\forall y$ quantifier.

(d) 3 is free for x in the formula $B(y) \to \forall y(A(x,z) \wedge \exists x C(x,y))$; constants can never be captured

4. d) $\forall x \exists y D(x,y,z)$

Terms: There are no free occurrences of x to plug in for in this formula. Consequently, every term is free for x in $\forall x \exists y D(x,y,z)$. This is a weird case, but the idea is not too hard. If there is no place to plug in, then you can plug in anything safely.

(a) x is free for x in $\forall x \exists y D(x,y,z)$.

(b) y is free for x in $\forall x \exists y D(x,y,z)$.

(c) $f(x,y)$ is free for x in $\forall x \exists y D(x,y,z)$.

(d) 3 is free for x in $\forall x \exists y D(x,y,z)$.

Here's a summary of all the work done above. In the table below, an OK appears if the term is free for x in the formula. If not, then an X appears.

	x	y	f(x,y)	3
$\forall y(A(x,y) \vee B(z))$	OK	X	X	OK
$A(x) \vee \forall z(C(z,z) \wedge A(z,y))$	OK	OK	OK	OK
$B(y) \to \forall y(A(x,z) \wedge \exists x C(x,y))$	OK	X	X	OK
$\forall x \exists y D(x,y,z)$	OK	OK	OK	OK

Let's summarize some shortcuts. We can plug x in for x in any formula, and not worry. We can plug a constant symbol in for x in any formula, and not worry. Note that we only ever plug terms into free occurrences of variables. We never plug terms of any sort into bounded occurrences of variables.

Exercises.

1. Use the following lists of formulas and terms to solve the exercises below.

Formulas:	Terms
1. $\forall y(A(x,y) \vee B(z))$	(a) x
2. $A(x) \vee \forall z(C(z,z) \wedge A(z,y))$	(b) y
3. $B(y) \to \forall z(A(x,z) \wedge \exists x C(x,y))$	(c) $f(x,y)$
4. $\forall x \exists y D(x,y,z)$	(d) 3

(a) Determine which of the terms are free for y in each formula.

(b) Determine which of the terms are free for z in each formula.

2. Use the following lists of formulas and terms to solve the exercises below.

Formulas:	Terms
1. $\forall x A(x, y, z)$	(a) x
2. $\forall y B(x, y) \vee \forall z C(z, y)$	(b) y
3. $\forall y(B(x, y) \vee \forall z C(z, y))$	(c) $h(z, 3)$
4. $\forall y \forall z(B(x, y) \vee C(z, y))$	(d) $g(x, y, z)$

   (a) Determine which of the terms are free for x in each formula.

   (b) Determine which of the terms are free for y in each formula.

   (c) Determine which of the terms are free for z in each formula.

2.12 A proof system for predicate calculus

Now we're ready to define our proof system for predicate calculus. Our proofs will consist of sequences of formulas of the sort we've been using, with justifications for each line. We need to specify the axioms, the rules of inference, and any abbreviations that we want to use. Since our new axiom system looks a little like L, we'll call it K.

Axioms

Any formulas of predicate calculus may be substituted for A, B, and C in the following schemes. Also, other variables may be substituted for the use of x in Axiom 4 and Axiom 5.

Axiom 1: $A \to (B \to A)$

Axiom 2: $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$

Axiom 3: $(\neg B \to \neg A) \to ((\neg B \to A) \to B)$

Axiom 4: $(\forall x A(x)) \to A(t)$, provided that t is free for x in $A(x)$.

Axiom 5: $\forall x(A \to B) \to (A \to \forall x B)$, provided that x does not occur free in A.

Rules of inference

Modus Ponens (MP): From A and $A \to B$, deduce B.

Generalization (GEN): From A, deduce $\forall x A$.

Abbreviations and Notation

We will use $\exists x A$ to abbreviate $\neg\forall x\neg A$. The connectives $\wedge$, $\vee$, and $\leftrightarrow$ are rewritten using the equivalent $\neg$ and $\rightarrow$ formulations. We will write $\vdash A$ if there is a proof of A in the proof system K.

Before we go any further, we should construct enough instances of axioms that we get a good feel for what axioms are available.

Axiom 1: $A(x) \rightarrow (\forall x A(x) \rightarrow A(x))$

Axiom 1: $\forall x A(x) \rightarrow (\exists x A(x) \rightarrow \forall x A(x))$

Axiom 1: $(\forall x A(x) \rightarrow \exists y C(y)) \rightarrow ((\exists x B(x) \rightarrow (\forall x A(x) \rightarrow \exists y C(y)))$

Axiom 2:$(A(x) \rightarrow (\exists y C(y) \rightarrow \forall z W(z))) \rightarrow$
$((A(x) \rightarrow \exists y C(y)) \rightarrow (A(x) \rightarrow \forall z W(z)))$

Axiom 3: $(\neg\exists x C(x) \rightarrow \neg A(x)) \rightarrow ((\neg\exists x C(x) \rightarrow A(x)) \rightarrow \exists x C(x))$

Axiom 4: $\forall x \exists y B(x, y, z) \rightarrow \exists y B(x, y, z)$

Axiom 4: $\forall x \exists y B(x, y, z) \rightarrow \exists y B(t, y, z)$

Axiom 5: $\forall x(\forall y B(y) \rightarrow \exists y C(x, y)) \rightarrow (\forall y B(y) \rightarrow \forall x \exists y C(x, y))$

Be careful with Axioms 4 and 5. It's vital to pay attention to the extra conditions on free occurrences of x. Here are two examples of common mistakes. First, the formula $\forall x \exists y B(x, y, z) \rightarrow \exists y B(y, y, z)$ is not a correct instance of Axiom 4 because the variable y is not free for x in $\exists y B(x, y, z)$. Second, the formula $\forall x(\exists y A(x, y) \rightarrow B(x)) \rightarrow (\exists y A(x, y) \rightarrow \forall x B(x))$ is not a correct instance of Axiom 5 because x occurs free in $\exists y A(x, y)$.

Proofs in K look a lot like proofs in L. Here is an example of a short proof.

Theorem K 1. $\vdash \forall x(A(x) \rightarrow (B(x) \rightarrow A(x)))$.

1. $A(x) \rightarrow (B(x) \rightarrow A(x))$ Axiom 1
2. $\forall x(A(x) \rightarrow (B(x) \rightarrow A(x)))$ GEN, line 1

Before we do any more proofs, lets remember why we were interested in a proof system. We wanted a good way to show that formulas were logically valid. The following two **very important** theorems say that this is the proof system that we want.

Theorem. [Completeness Theorem for Predicate Calculus] (Gödel 1930) If A is logically valid, then $\vdash A$.

Theorem. [Soundness Theorem for Predicate Calculus] (Gödel 1930) If $\vdash A$, then A is logically valid.

Summarizing, we can prove a formula A if and only if it is logically valid. The relationship between K and the logically valid formulas is exactly the same as the relationship between L and the tautologies.

The proof of the soundness theorem for K is very much like the proof of the soundness theorem for L. One shows that all the axioms are logically valid and that applying MP and GEN to logically valid formulas always yields more logically valid formulas. Then given a proof in K, we can step through line by line, showing that each line in turn is logically valid. In particular, the last line is logically valid, so if a formula can be proved in K, then it is logically valid.

The proof of the completeness theorem for K is completely different from the proof of the completeness theorem for L. Rather than proving the result directly, it is best to prove the contrapositive. Consequently, we would assume that there is no proof of A in K, and then show that A is not logically valid by constructing a model where $\neg A$ is true. Many proofs of the completeness theorem (e.g. [2], [6], [8], and [4]) differ primarily on the method of this construction. The method employed by Henkin [4] actually uses a set of terms as the universe for the model. This is a delightfully twisted idea.

In our discussion of the completeness theorem for L, we noted that it is possible to write a computer program that accepts formulas of L as input, determines whether or not they are tautologies, and then outputs either a row of the truth table showing that the formula is not a tautology or a proof in L of the formula. This is not the case for K. Indeed, there is no computer program that can accept formulas of K as input and determine whether or not they are logically valid. This situation is not due to a lack of talent on the part of programmers. There is a proof that predicate calculus is undecidable, that is no decision program can be created [10]. While there is no program for deciding which formulas are logically valid, we do have a method for supporting our conclusions. Given a logically valid formula we can find a proof of it in K, and given a formula that isn't logically valid we can find a model in which it is not true.

Exercises.

1. Build two instances for each of the axioms, showing the substitution made in each case.

2. Are the following instances of one of the axioms? If so, show the substitution made.

   (a) $\forall x \forall y A(x,y) \rightarrow (\exists x B(x) \rightarrow \forall y A(x,y))$.

   (b) $\forall x \forall y A(x,y) \rightarrow \forall y A(y,y)$.

   (c) $\forall x \forall y A(x,y) \rightarrow \forall y A(x,y)$.

   (d) $\exists x B(x) \rightarrow ((\forall x \exists y C(x,y) \rightarrow A(x)) \rightarrow \exists x B(x))$.

In order to make efficient use of our new proof system, K, we could use some shortcuts. When we learned to write proofs in L, progress was painful until

we learned the Deduction Theorem for L. One of the shortcuts we will learn is a Deduction Theorem for Predicate Calculus. The next four sections consist entirely of shortcuts and proof strategies for our new proof system.

2.13 Dealing with $\forall$

Here is a strategy for manipulating universal quantifiers. To add $\forall x$ to the beginning of a formula, use GEN. To rip $\forall x$ off the front of a formula, use Axiom 4. Here is an easy proof that illustrates both halves of the strategy.

Theorem K 2. $\forall x \forall y A(x,y) \vdash \forall y \forall x A(x,y)$.

1. $\forall x \forall y A(x,y)$ — Given
2. $\forall x \forall y A(x,y) \rightarrow \forall y A(x,y)$ — Axiom 4
3. $\forall y A(x,y)$ — MP, lines 1. and 2.
4. $\forall y A(x,y) \rightarrow A(x,y)$ — Axiom 4
5. $A(x,y)$ — MP, lines 3. and 4.
6. $\forall x A(x,y)$ — GEN, line 5.
7. $\forall y \forall x A(x,y)$ — GEN, line 6.

Be careful! Our strategy only works on **leading** quantifiers whose scope is the whole formula. Other situations require gyrations of a different sort. The next shortcut will make these gyrations easier.

2.14 Rule T

Since Axiom 1, Axiom 2, Axiom 3 and MP are all included in K, every proof in L is also a proof in K. The following rule lets us use all the results we could have proved in L, even if we didn't actually do the proof.

RULE T: Any instance of a tautology may be inserted as a line in a predicate calculus proof.

Theorem K 3. $A(x) \wedge B(x) \vdash A(x)$.

1. $A(x) \wedge B(x)$ — Given
2. $(A(x) \wedge B(x)) \rightarrow A(x)$ — Rule T
3. $A(x)$ — MP, lines 1. and 2.

Any time we introduce a shortcut rule, we need to consider one question. Can every proof done using the shortcut be done without using it? If the answer to the question is no, then proofs done via the shortcut may not be sound. For Rule T, the answer to the question is yes. Actually, any line invoking Rule T can be replaced by a proof using only Axiom 1, Axiom 2, Axiom 3, and MP. This follows immediately from the completeness theorem for L. Roughly, since every tautology can be proved in L, every formula that looks like a tautology (i.e. every instance of a tautology) can be proved using axioms that look like axioms of L (i.e. Axioms 1 through 3.)

The previous paragraph indicates why Rule T is such a powerful shortcut. When we use Rule T, we are making full use of our understanding of L, including the Completeness Theorem for L. On the other hand, misapplications of Rule T are very undesirable. Rule T only allows insertion of instances of tautologies. It does not allow us to insert other logically valid formulas. This is a very good time to review section 2.10 and make sure that you understand exactly what constitutes an instance of a tautology.

2.15 The Deduction Theorem

One of our nicest shortcuts in L was the deduction theorem. We can state (and use) a deduction theorem for predicate calculus, too. We'll state the theorem, give two quick applications, and then discuss its proof a little.

Theorem (Deduction Theorem for K)**.** If there is a proof of $A \vdash B$ with no applications of generalization to any variables that occur free in A, then there is a proof of $\vdash A \to B$.

Theorem K 4. $\vdash \forall x \forall y A(x,y) \to \forall y \forall x A(x,y)$

We have already proved K2: $\forall x \forall y A(x,y) \vdash \forall y \forall x A(x,y)$. The proof, which appears on page 54, contains no applications of GEN to a variable appearing free in $\forall x \forall y A(x,y)$. Actually, you don't need to look at the proof, since there are no free variables in $\forall x \forall y A(x,y)$. Theorem K4 follows by one application of the deduction theorem for K.

Theorem K 5. $\vdash \forall x(A(x) \wedge B(x)) \to \forall x A(x)$

This time, we will formally prove $\forall x(A(x) \wedge B(x)) \vdash \forall x A(x)$, and then apply the deduction theorem.

1. $\forall x(A(x) \wedge B(x))$	Given
2. $\forall x(A(x) \wedge B(x)) \to (A(x) \wedge B(x))$	Axiom 4
3. $A(x) \wedge B(x)$	MP, lines 1 and 2
4. $(A(x) \wedge B(x)) \to A(x)$	Rule T
5. $A(x)$	MP, lines 3 and 4

6. $\forall x A(x)$ GEN, line 5

The only use of GEN in this proof is on the variable x, which does not occur free in the hypothesis. Thus, we can apply the deduction theorem to obtain $\vdash \forall x(A(x) \wedge B(x)) \rightarrow \forall x A(x)$, as desired.

In the preceding proof, we actually used the following restricted version of the deduction theorem:

Corollary. If $A \vdash B$ and A has no free variables, then $\vdash A \rightarrow B$.

The restriction on applications of generalization to variables not occurring free in the hypothesis is a vital part of the statement of the deduction theorem. Without it, our proofs would not be sound. For example, consider the following correct proof of $x = y \vdash x = 0$.

1. $x = y$ Given
2. $\forall y(x = y)$ GEN, line 1
3. $\forall y(x = y) \rightarrow x = 0$ Axiom 4
4. $x = 0$ MP, lines 2 and 3

Note that the application of GEN in line 2 to the variable x, which occurs free in $x = y$, precludes us from applying the deduction theorem. This is a good thing, because if we incorrectly applied the deduction theorem, we could deduce $x = y \rightarrow x = 0$, which could be generalized to $\forall x \forall y(x = y \rightarrow x = 0)$. This formula is not logically valid, since in the model with the natural numbers as its universe and the usual interpretation of $=$ and 0, the implication $1 = 1 \rightarrow 1 = 0$ is false. Just one misapplication of the deduction theorem destroys the soundness of our proof system. Always check for uses of GEN before applying the deduction theorem.

Can every proof done using the deduction theorem be done without using the deduction theorem? Sure! That's essentially what the deduction theorem says. At this point, we have enough tools to do a lot of proofs without too much effort.

Exercises.

Prove the following in K. You may use any theorem with a lower number in your proof.

Theorem K 6. $\vdash (\forall x A(x)) \rightarrow \forall x(A(x) \vee B(x))$

Theorem K 7. $\vdash \forall x(A(x) \rightarrow B(x)) \rightarrow (\forall x A(x) \rightarrow \forall x B(x))$

Theorem K 8. $\vdash \forall x B(x) \rightarrow \forall x(A(x) \rightarrow B(x))$

Theorem K 9. $\vdash \forall x \forall y A(x, y) \rightarrow \forall y \forall x A(y, x)$

Theorem K 10. $\vdash \forall x(A(x) \vee B(x)) \rightarrow (\forall x \neg A(x) \rightarrow \forall x B(x))$

2.16 Adding $\exists x$

If we have $\forall x A(x)$, we ought to be able to prove $\exists x A(x)$. In order to do this, we need to be able to add $\exists x$ to a formula. Here's an example of how to do this using the shortcuts we have so far.

Theorem K 11. $A(x) \vdash \exists x A(x)$

1. $A(x)$	Given
2. $\forall x \neg A(x) \rightarrow \neg A(x)$	Axiom 4
3. $(\forall x \neg A(x) \rightarrow \neg A(x)) \rightarrow (A(x) \rightarrow \neg \forall x \neg A(x))$	Rule T
4. $A(x) \rightarrow \neg \forall x \neg A(x)$	MP, lines 2 and 3
5. $\neg \forall x \neg A(x)$	MP, lines 1 and 4
6. $\exists x A(x)$	Abbreviation of line 5

We can extract the content of the proof of Theorem K11, and create an Add-$\exists x$ Rule that handles even more cases. We need to be careful that the hidden use of Axiom 4 is acceptable. In the following, the clauses requiring that $A(t)$ is the result of replacing every free occurrence of x in $A(x)$ with t and t is free for x in $A(x)$ insure that $\forall x \neg A(x) \rightarrow \neg A(t)$ is a correct instance of Axiom 4. This allows us to modify the proof of K11 to obtain a proof of $\exists x A(x)$ from $A(t)$. Stating the rule will save us from having to mess with contrapositives every time we want to tack on an existential quantifier.

Add $\exists x$ Rule: If $A(t)$ is the result of replacing every free occurrence of x in $A(x)$ with t, and t is free for x in $A(x)$, then from $A(t)$ we may deduce $\exists x A(x)$.

Here is an application of the Add $\exists x$ Rule that makes use of the ability to substitute for a term. In the following, $A(y, y)$ is the result of replacing every free occurrence of x in $A(x, y)$ with y, and y is free for x in $A(x, y)$. Thus the Add $\exists x$ Rule allows us to deduce $\exists x A(x, y)$ from $A(y, y)$.

Theorem K 12. $A(y, y) \vdash \forall y \exists x A(x, y)$

1. $A(y, y)$	Given
2. $\exists x A(x, y)$	Add $\exists x$ Rule, line 1
3. $\forall y \exists x A(x, y)$	GEN, line 2

Exercises.

1. Prove:

   Theorem K 13. $\vdash \forall x A(x) \to \exists x A(x)$

2. Consider the theorem:

   Theorem K 14. $\vdash \forall y A(y) \to \exists x A(x)$

   (a) Prove K14 using the deduction theorem, Axiom 4 and K13.

   (b) Prove K14 using the Add $\exists x$ Rule.

3. Prove:

   Theorem K 15. $\vdash \forall x(A(x) \vee B(x)) \to (\forall x A(x) \vee \exists x B(x))$

4. Prove the following theorems. Like the proof of Theorem K11, these results use the fact that $\exists x A(x)$ is an abbreviation for $\neg\forall x\neg A(x)$. Mathematicians use results like these whenever they "push negations past a quantifier."

   (a)

   Theorem K 16. $\neg\exists x A(x) \vdash \forall x\neg A(x)$

   (b)

   Theorem K 17. $\forall x\neg A(x) \vdash \neg\exists x A(x)$

   (c)

   Theorem K 18. $\exists x\neg A(x) \vdash \neg\forall x A(x)$

   (d)

   Theorem K 19. $\neg\forall x A(x) \vdash \exists x\neg A(x)$

2.17 Removing $\exists x$

So far, we have strategies for adding and removing $\forall x$, and a rule for adding $\exists x$. To complete our survey of techniques for manipulating quantifiers, we need a rule for removing $\exists x$.

Informally, if we have $\exists x A(x)$, we should be able to find some element to plug in for x. If we give that element a temporary name, we could proceed with our proof. The best thing to use as a name is a constant symbol. If we use a constant symbol that already appears in the proof (or appears in some weird axioms that we plan to use later), we will be implicitly making additional assumptions about the element. Consequently, we want to use a **new** constant symbol. Here's the rule, presented more formally.

Rule C: If $\exists x A(x)$ is a previous line in a proof, we may write $A(\underline{c})$ as a line, provided that the following two conditions hold.

1. $\underline{c}$ is a new constant symbol. (That is $\underline{c}$ doesn't show up in any earlier lines of the proof, of in any proper axioms we ever plan to use.)
2. If some variable (say y) appears free in the formula $\exists x A(x)$, then GEN is never applied to y in the proof.

Here is an example of using Rule C in a proof.

Theorem K 20. $\exists x(A(x) \wedge B(x)) \vdash \exists x A(x)$

1. $\exists x(A(x) \wedge B(x))$	Given
2. $A(\underline{c}) \wedge B(\underline{c})$	Rule C, line 1
3. $(A(\underline{c}) \wedge B(\underline{c})) \rightarrow A(\underline{c})$	Rule T
4. $A(\underline{c})$	MP, lines 2 and 3
5. $\exists x A(x)$	Add $\exists x$ Rule, line 4

Why do we need the second condition in Rule C? We need to worry about GEN and Rule C for the same reason that we worry about GEN and the Deduction Theorem. If we do a proof with Rule C and break the second condition, our conclusion may not be sound. For example, consider the following incorrect proof of $\exists x \forall y(x = y)$ from $\forall y(y = y)$.

1. $\forall y(y = y)$	Given
2. $\forall y(y = y) \rightarrow y = y$	Axiom 4
3. $y = y$	MP, lines 1 and 2
4. $\exists x(x = y)$	Add $\exists x$ Rule, line 3
5. $\underline{c} = y$	Rule C, line 4
6. $\forall y(\underline{c} = y)$	**Illegal** use of GEN
7. $\exists x \forall y(x = y)$	Add $\exists x$ Rule, line 6

In line 4, $y = y$ is the result of substituting y for every free occurrence of x in $x = y$, and y is free for x in $x = y$, so this line is a legal application of the Add $\exists x$ Rule. Indeed, this is just like the second line in the proof of K12 with $x = y$ substituted for $A(x, y)$. We pull the substitution trick with the Add $\exists x$ Rule again in line 7. It is legal there, too. The only illegal step is in line 6, where we apply GEN to a variable that appears free in line 4, the formula to which we applied Rule C. That violates the second condition of Rule C, and it is a very bad idea. There is a model where $\forall y(y = y)$ is true, but $\exists x \forall y(x = y)$ is false, so $\forall y(y = y)$ does not logically imply $\exists x \forall y(x = y)$. The illegal use of GEN with Rule C has destroyed the soundness of our proof system.

We've seen the bad effects of violating the conditions of Rule C. However, if we can prove A using Rule C correctly, then we can prove A without using

Rule C. Consequently, correct uses of the shortcut Rule C do not mess up the completeness and soundness theorems for our proof system. One way to prove this is to construct an algorithm that converts proofs that use the shortcut to proofs that do not. This sort of argument closely resembles a proof of the deduction theorem, and is used in [8].

Exercises.

Use Rule C to prove the following:

Theorem K 21. $\vdash \exists x A(x) \rightarrow \exists x(A(x) \vee B(x))$

Theorem K 22. $\vdash \exists x \forall y A(x, y) \rightarrow \forall y \exists x A(x, y)$

Theorem K 23. $\vdash \exists x(A(x) \rightarrow B(x)) \rightarrow (\forall x A(x) \rightarrow \exists x B(x))$

Theorem K 24. $\vdash \exists x B(x) \rightarrow \exists x(A(x) \rightarrow B(x))$

Theorem K 25. $\vdash \neg \forall x A(x) \rightarrow \exists x(A(x) \rightarrow B(x))$ (Hint: Use K19)

Theorem K 26. $\vdash (\forall x A(x) \rightarrow \exists x B(x)) \rightarrow \exists x(A(x) \rightarrow B(x))$ (Hint: Use K24 and K25, rather than Rule C.)

2.18 Proof strategies in predicate calculus

Predicate calculus looks a lot like propositional calculus, except for the addition of quantifiers. We have some excellent tools for dealing with quantifiers. To add $\forall x$ we use GEN, and to add $\exists x$ we use the aptly named Add $\exists x$ Rule. To remove $\forall x$ we use Axiom 4, and to remove $\exists x$ we use Rule C. A very rough overall strategy for doing proofs in predicate calculus is:

- Rip off the quantifiers.
- Use Rule T (or whatever) to mess with the guts of the formula.
- Glue the quantifiers back on.

Of course, we also can use techniques from propositional calculus like applying the deduction theorem or proving the contrapositive as a lemma. Here are some problems that use a variety of methods.

Exercises.

Theorem K 27. $\vdash \forall x A(x,x) \rightarrow \forall x \exists y A(x,y)$

Theorem K 28. $\vdash \forall y \exists x (\neg A(y,x) \vee A(y,y))$

Theorem K 29. $\vdash \exists x (A(x) \vee B(x)) \rightarrow (\exists x A(x) \vee \exists x B(x))$

Theorem K 30. $\vdash (\exists x A(x) \vee \exists x B(x)) \rightarrow \exists x (A(x) \vee B(x))$.

Theorem K 31. $\vdash \exists x (A(x) \wedge B(x)) \rightarrow (\exists x A(x) \wedge \exists x B(x))$

Theorem K 32. $\vdash (\forall x A(x) \wedge \exists x B(x)) \rightarrow \exists x (A(x) \wedge B(x))$

Theorem K 33. $\vdash (\forall x A(x) \vee \forall x B(x)) \rightarrow \forall x (A(x) \vee B(x))$

Theorem K 34. $\vdash \forall x (A(x) \wedge B(x)) \rightarrow (\forall x A(x) \wedge \forall x B(x))$

Theorem K 35. $\vdash (\forall x A(x) \wedge \forall x B(x)) \rightarrow \forall x (A(x) \wedge B(x))$

Theorem K 36. $\vdash (\exists x A(x) \rightarrow \forall x B(x)) \rightarrow \forall x (A(x) \rightarrow B(x))$

Hints: You may find the following strategies useful for the preceding exercises.

K27: Deduction theorem.

K28: Rule T, followed by Add $\exists x$ Rule.

K29: $P \vee Q$ abbreviates $\neg P \rightarrow Q$.

K30: Prove the contrapositive.

K31: Deduction theorem and Rule C.

K32: Deduction theorem and Rule C.

K33: Prove the contrapositive.

K34: Deduction theorem.

K35: Deduction theorem.

K36: Prove the contrapositive.

Chapter 3

Transition to Informal Proofs

We just spent the whole last chapter talking about predicate calculus. Two of the important theorems we discussed were the Completeness Theorem and the Soundness Theorem. These two theorems can be summarized as follows: *The formulas that are provable in predicate calculus are exactly the logically valid formulas.*

These results indicate both the main weakness and the main strength of predicate calculus. On the one hand, the only formulas we can prove are the logically valid formulas, which will always be true in every model. However, most of the interesting formulas in mathematics state properties that are peculiar to the integers, or the reals, or to some other entertaining *specific* model. For example,

$$\forall x(P(x) \vee \neg P(x))$$

is true in absolutely every model, but

$$\forall x((P(x) \wedge B(x)) \rightarrow O(x))$$

is not logically valid. However, consider the following model:

Universe := natural numbers

P(x) := x is prime

B(x) := x is bigger than 2

O(x) := x is odd

In this model (a *particular* model), the second statement above translates to: *All prime natural numbers bigger than 2 are odd.* This is a true statement, but since it is not logically valid, we need new axioms in order to prove it.

Now we want to address a new question: *What additional axioms do mathematicians use?* In a sense, we are asking about what sort of objects mathematicians work on, and what properties of these objects they use to describe them. By considering important properties, we are avoiding some pithy philosophical questions, and asking some more pragmatic questions. For example, rather than asking "What is a natural number?", we will ask "What important properties of natural numbers are useful in mathematical proofs?" The philosophical questions are very interesting, but, after all, our goal is to write better proofs.

If we actually knew all along that predicate calculus could not prove mathematically interesting statements and that we would eventually tack on bunches of new axioms, why did we spend a whole chapter on predicate calculus? Remember that any formula provable in predicate calculus is provable in any theory with added axioms. Thus, the theorems of predicate calculus are the common core of first order mathematical theories. Also, the shortcut methods we used don't exclude the use of additional axioms, so the proof techniques we learned in the last chapter will apply to all sorts of interesting mathematical proofs. Predicate calculus is a sort of scaffold on which we can hang any axiom systems that interest us.

Any theory that consists of the axioms of K together with additional (often called non-logical) axioms using predicates and variables from K is called a *first order theory*. In the next two sections, we will take a look at first order theories describing the nature of equality and the natural numbers.

3.1 The Theory of Equality

Here is a simple example of a first order theory. The goal is to describe our understanding of what equality means. Suppose that we use the symbol $x = y$ to represent some binary predicate (like $A(x, y)$). Let E denote the axioms of predicate calculus (K) together with the following axioms (numbered to avoid confusion with Axioms 1 through 5 in k):

Axiom 6 (Reflexivity of equality) $\forall x(x = x)$
Axiom 7 (Substitutivity of equality) For every formula $A(x, y)$, with free variable x, if y is free for x in $A(x, x)$ then

$$x = y \rightarrow (A(x, x) \rightarrow A(x, y)).$$

If we can prove a formula B in predicate calculus using the additional axioms 6 and 7, we will write $\vdash_E B$. In this case, we say that B is a theorem of E, and that E proves B. It's interesting to note that these two axioms actually do a pretty good job of describing the way that equality acts. In particular, Axiom 7 captures the sort of substitution steps that are commonly used in elementary algebra. In this sense, a lot of elementary algebra has more to do with the equality predicate than with functions or numbers. Here are several instances of Axiom 7.

$x = y \to (P(x, x, z) \to P(x, y, z))$

$y = z \to (R(y) \to R(z))$

$y = z \to (x = y \to x = z)$

$x = y \to (x = x \to y = x)$

$x = 2 \to (x \cdot y = 6 \to 2 \cdot y = 6$

$x = y \to (x + 2 = x + 2 \to x + 2 = y + 2)$

Note that Axiom 7 can't be used on quantified variables, so the following statement is *not* an instance of Axiom 7: $x = y \to (\forall x P(x, x, z) \to \forall x P(x, y, z))$. Remember that all the axioms of L and K are axioms of E. Consequently, all of the theorems we proved using L and K are theorems of E. Now it is time to try our hand at a proof that uses the new axioms.

Theorem E 1. $\vdash_E \forall x \forall y(x = y \to y = x)$ (Mathematicians would paraphrase this by saying *equality is symmetric.*)

Proof:

1. $x = y \to (x = x \to y = x)$	Axiom 7
2. $x = x \to (x = y \to y = x)$	L7, line 1
3. $\forall x(x = x)$	Axiom 6
4. $\forall x(x = x) \to x = x$	Axiom 4
5. $x = x$	MP, lines 3 and 4
6. $x = y \to y = x$	MP, lines 2 and 5
7. $\forall y(x = y \to y = x)$	GEN, line 6
8. $\forall x \forall y(x = y \to y = x)$	GEN, line 7

Exercises.

Prove the following in E.

Theorem E 2. $\vdash_E x = y \to (y = z \to x = z)$ (This is often called the *transitive law of equality.*)

Theorem E 3. $\vdash_E (x = y \wedge x = z) \to y = z$ (This is an axiom of Euclid: *things equal to the same thing are equal to each other.*)

Theorem E 4. $\vdash_E x = y \to \forall z(f(z, x) = f(z, y))$

Note that Theorem E4 holds regardless of the choice of $f(x, z)$. For example, we could replace $f(x, z)$ by $x + z$, $x - z$, $x \cdot z$, x^z, z^x, or any other two place function.

3.2 Formal Number Theory

indexnumber theory

In this section, we will discuss an axiom system for formal number theory. By formal number theory, we mean a theory that describes arithmetic on the natural numbers. The mathematical objects we are trying to describe with our new axioms are the counting numbers $\{0, 1, 2, ...\}$ and various familiar functions on them, like addition and multiplication.

Rather than trying to cook up a reasonable set of axioms from scratch, we can rely on the expertise of some other mathematicians. The following axioms were used by Kleene [6] and Mendelson [8]. We'll call our axiom system PA, short for Peano's Axioms for Arithmetic. The function x' is read as *successor* and is intended to represent $x + 1$.

indexaxiom systems!number theory The axiom system PA consists of the axioms of E and the eight following axioms.

Axiom 8: $\forall x \forall y(x = y \rightarrow x' = y')$

Axiom 9: $\forall x(0 \neq x')$

Axiom 10: $\forall x \forall y(x' = y' \rightarrow x = y)$

Axiom 11: $\forall x(x + 0 = x)$

Axiom 12: $\forall x \forall y(x + (y') = (x + y)')$

Axiom 13: $\forall x(x \cdot 0 = 0)$

Axiom 14: $\forall x \forall y(x \cdot (y') = (x \cdot y) + x)$

Axiom 15: If $A(x)$ is a formula of PA, then

$$A(0) \rightarrow (\forall n(A(n) \rightarrow A(n')) \rightarrow \forall n A(n)).$$

We can easily paraphrase what these axioms say. Axioms 8, 9 and 10 say that equality acts the way we expect equality to act related to numbers and successors. Axiom 9 says that 0 is the least counting number. Axiom 10 says that 0 is the additive identity. Axioms 11 and 12 outline the behavior of addition, and Axioms 13 and 14 do the same for multiplication. Axiom 15 says that we can use induction to prove facts about the counting numbers. All in all, this seems like a very reasonable list of properties of the natural numbers.

The language of PA is very expressive. That is, lots of properties of the natural numbers can be written as formulas of PA. Here are some examples.

Example. Each of the following mathematical concepts is presented with its formalization in PA. Note that these are just formulas representing properties of natural numbers, not provable statements.

1. x is even: $\exists k(x = 2 \cdot k)$

   (2 is an abbreviation for $0''$.)

2. x is odd: $\exists k(x = 2 \cdot k + 1)$
   (1 is an abbreviation for $0'$.)
3. $y|x$ (y divides x evenly): $\exists k(x = y \cdot k)$)
4. $x \leq y$ (x is less than or equal to y): $\exists k(x + k = y)$
5. $x < y$ (x is strictly less than y): $\exists k(x + k = y \wedge k \neq 0)$
   ($k \neq 0$ is an abbreviation for $\neg(k = 0$.)
6. x is a prime number: $1 < x \wedge \forall y(y|x \rightarrow (y = 1 \vee y = x))$
   ($y|x$ is an abbreviation for $\exists k(x = y \cdot k)$, as shown in part 3.)

Besides being able to express a multitude of number theoretical concepts, PA can actually prove gobs of facts about the natural numbers. Here are some additional statements and their formalizations, each of which can be proved in PA.

Example. Each of the following mathematical statements is presented with its formalization in PA. Each of these properties of natural numbers can be proved from the axioms of PA. Since GEN is included in PA, we can also prove closed versions of these statements with universal quantifiers in the front.

1. Addition is commutative: $x + y = y + x$
2. Addition is associative: $x + (y + z) = (x + y) + z$
3. Multiplication is distributive over addition: $x \cdot (y + z) = x \cdot y + x \cdot z$
4. Strict inequality is transitive: $x < y \rightarrow (y < z \rightarrow x < z)$
5. Inequality is preserved by addition: $x \leq y \rightarrow x + z \leq y + z$
6. Strict inequality is preserved by addition: $x < y \rightarrow x + z < y + z$
7. Inequality is preserved by multiplication: $x \leq y \rightarrow x \cdot z \leq y \cdot z$
8. Strict inequality is preserved by nonzero multiplication:
   $z \neq 0 \rightarrow (x < y \rightarrow x \cdot z < y \cdot z)$
9. Inequalities can be added: $(w \leq x \wedge y \leq z) \rightarrow w + y \leq x + z$
10. Inequalities can be multiplied: $(w \leq x \wedge y \leq z) \rightarrow w \cdot y \leq x \cdot z$

We keep asserting that statements can be proved in PA without providing the proof. There is a reason for this. Generally speaking, the proofs are somewhat long and complicated, though the next two examples aren't too bad.These first two results give a formal proof that $0 \cdot n = 0$. From Axiom 13, we know that $n \cdot 0 = 0$, but since commutativity of multiplication is not one of our axioms, we have the prove the new statement. Indeed, this can be used as an initial step in a proof that multiplication is commutative. (See the exercises.) Remember that in our proofs in PA, we can use axioms of PA, and results from L, K and E.

Theorem PA 1. $\vdash_{PA} \forall n(0 \cdot n = 0 \rightarrow 0 \cdot (n') = 0)$.

Proof: We will prove that $0 \cdot n = 0 \vdash_{PA} 0 \cdot (n') = 0$, and then apply the Deduction Theorem and GEN.

1. $0 \cdot n = 0$ Given
2. $\forall x \forall y(x \cdot (y') = (x \cdot y) + x)$ Axiom 14
3. $\forall x \forall y(x \cdot (y') = (x \cdot y) + x) \rightarrow \forall y(0 \cdot (y') = (0 \cdot y) + 0)$ Axiom 4
4. $\forall y(0 \cdot (y') = (0 \cdot y) + 0)$ MP, lines 2 and 3
5. $\forall y(0 \cdot (y') = (0 \cdot y) + 0) \rightarrow (0 \cdot (n') = (0 \cdot n) + 0)$ Axiom 4
6. $0 \cdot (n') = (0 \cdot n) + 0$ MP, lines 4 and 5
7. $\forall x(x + 0 = x)$ Axiom 11
8. $\forall x(x + 0 = x) \rightarrow (0 \cdot n) + 0 = 0 \cdot n$ Axiom 4
9. $(0 \cdot n) + 0 = 0 \cdot n$ MP, lines 7 and 8
10. $(0 \cdot (n') = (0 \cdot n) + 0) \rightarrow ((0 \cdot n) + 0 = 0 \cdot n \rightarrow 0 \cdot (n') = 0 \cdot n)$ Theorem E2
12. $(0 \cdot n) + 0 = 0 \cdot n \rightarrow 0 \cdot (n') = 0 \cdot n$ MP, lines 6 and 10
13. $0 \cdot (n') = 0 \cdot n$ MP, lines 9 and 12
14. $(0 \cdot (n') = 0 \cdot n) \rightarrow (0 \cdot n = 0 \rightarrow 0 \cdot (n') = 0)$ Theorem E2
15. $0 \cdot n = 0 \rightarrow 0 \cdot (n') = 0$ MP, lines 13 and 14
16. $0 \cdot (n') = 0$ MP lines 1 and 15

Our proof of $0 \cdot n = 0 \vdash_{PA} 0 \cdot (n') = 0$ used no applications of GEN to n, so by the Deduction Theorem, we have $\vdash_{PA} 0 \cdot n = 0 \rightarrow 0 \cdot (n') = 0$. Using this as a lemma and applying GEN to n, we obtain a proof of Theorem PA1.

Theorem PA 2. $\vdash_{PA} \forall n(0 \cdot n = 0)$.

Proof: Our proof will use Theorem PA1 and the induction axiom from PA. In informal terms, line 3 of the following proof is the base case and line 4 is the induction step.

1. $\forall x(x \cdot 0 = 0)$ Axiom 13
2. $\forall x(x \cdot 0 = 0) \rightarrow 0 \cdot 0 = 0$ Axiom 4
3. $0 \cdot 0 = 0$ MP, lines 1 and 2
4. $\forall n(0 \cdot n = 0 \rightarrow 0 \cdot (n') = 0)$ Theorem PA1
5. $0 \cdot 0 = 0 \rightarrow (\forall n(0 \cdot n = 0 \rightarrow 0 \cdot (n') = 0) \rightarrow \forall n(0 \cdot n = 0))$ Axiom 15
6. $\forall n(0 \cdot n = 0 \rightarrow 0 \cdot (n') = 0) \rightarrow \forall n(0 \cdot n = 0)$ MP, lines 3 and 5
7. $\forall n(0 \cdot n = 0)$ MP lines 4 and 6

Exercises.

1. Translate the following statements into formulas of PA. (Note that each of these could actually be proven in PA, but that is not part of this exercise.)
   (a) For every x, there is a number y such that $x^2 = y$.
   (b) 2 is not a square.
   (c) There is a natural number which is not a square.
   (d) Multiplication is commutative
   (e) Multiplication is associative.
2. Translate the following statements into formulas of PA. (Note that PA can prove each of these statements, but that is not part of this exercise.)
   (a) If x is even, then $x + 1$ is odd.
   (b) If x is odd, then $x + 1$ is even.
   (c) For every x, either x is even, or x is odd.
   (d) For every x, there is a y such that $x < y$.
   (e) There are infinitely many primes. (A formal proof of this statement in PA would be many hundreds of lines long.)
3. Prove:

   Theorem PA 3. $\forall n(n = 0 + n)$
4. Prove:

   Theorem PA 4. $\forall x \forall y(x + y = y + x)$
5. Prove:

   Theorem PA 5. $\forall x \forall y(x \cdot y = y \cdot x)$
6. Using the formalizations in the examples, formalize the statement "if x is prime and even, then $x = 2$." Prove this statement in PA.

3.3 More about induction

Consider the induction argument we used to prove Theorem PA2. We prove that $0 \cdot n = 0$ for all n via the following three steps:

1. Base case: $(n = 0)$ We proved $0 \cdot 0 = 0$.
2. Induction step: Assuming $0 \cdot n = 0$, we deduced $0 \cdot n' = 0$. This proof was actually carried out in Theorem PA1, and then used in the proof of Theorem PA2.

3. Conclusion: By virtue of the induction axiom (Axiom 15), we concluded that $0 \cdot n = 0$ for all n.

In the induction step, the assumed statement $0 \cdot n = 0$ is called the *induction hypothesis.* If we rewrite the proof in a less formal fashion, we can include the main steps of the proof of Theorem PA1 and still give the reader a good idea of the overall structure of the argument.

Theorem. $\forall n(0 \cdot n = 0)$.

Proof. We will use induction and axioms of PA.
Base case: $0 \cdot 0 = 0$ by Axiom 13 of PA.
Induction step: Assume $0 \cdot n = 0$. We will prove that $0 \cdot (n') = 0$.

$$\begin{aligned} 0 \cdot (n') &= 0 \cdot n + 0 && \text{Axiom 14} \\ &= 0 \cdot n && \text{Axiom 11} \\ &= 0 && \text{Induction hypothesis} \end{aligned}$$

By the transitivity of equality, we have shown $0 \cdot (n') = 0$, as desired.
Conclusion: By induction, it follows that $\forall n(0 \cdot n = 0)$. □

Note that this proof has significant advantages over the proof in the previous section. It contains both the proof of Theorem PA1 and Theorem PA2, but is much shorter. It is much easier to read than the formal proof, but still highlights the main axioms used in the formal proof. By suppressing some of the logical machinations of the formal proof, it actually reveals more of the unalloyed mathematical content of PA.

Clearly, less formal proofs do a better job of serving the interests of mathematicians. On the other hand, it is also much more difficult to spot errors in informal proofs. Whenever we are unsure of a step, it is nice to be able to rely on the technical precision of formal proof to verify the correctness of details.

The format of an induction argument can be modified in a variety of ways. For example, the following theorem of PA essentially says that we can shift the starting point of an induction argument.

Theorem PA 6. If $A(x)$ is a formula of PA, then

$$A(k) \to (\forall n(k \leq n \to (A(n) \to A(n'))) \to \forall n(k \leq n \to A(n))).$$

Note that Theorem PA6 has a formal proof in PA, though we will not bother to write it up. Also, in the statement of the theorem, we use $k \leq n$ as an abbreviation for $\exists x(k + x = n)$, applying our work from part 4 of the example on page 67.

We can use Theorem PA6 to create informal proofs in exactly the same way that we used Axiom 15 before. We will call these proofs by *induction with a shifted starting point.* If we want to prove that $A(n)$ holds for all $n \geq k$, we can use the following three steps.

1. Base case: $(n = k)$ Prove that $A(k)$ holds.

2. Induction step: Assume the induction hypothesis, namely that both $k \leq n$ and $A(n)$ hold. Deduce $A(n')$.

3. Conclusion: By induction, we conclude that $\forall n(k \leq n \rightarrow A(n))$.

This type of induction argument is particularly handy for proving results about summations. You may have seen the following notation in a calculus course.

$$\sum_{i=0}^{k} f(i) = f(0) + f(1) + f(2) + \cdots + f(k).$$

The starting point of the summation can be a value other than 0. For example,

$$\sum_{i=2}^{5} \frac{1}{i} = \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5}.$$

Shifting the starting points and endpoints allow us to rewrite sums in various convenient formats. For example,

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

Note that for *finite* summations, and rearrangement of the terms yields the same final sum.

Using our new notation, we can state a nice theorem which we will then prove by an informal induction argument with a shifted starting point. Since this is the first result that we will prove using strictly informal methods, we will call it Theorem 1.

Theorem 1. For all $n \geq 1$, $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

Before writing the proof, we should do some scratch work. We will need to use induction with the starting point $k = 1$. In the induction step, our induction hypothesis will be that $n \geq 1$ and $\sum_{i=1}^{n} i = n(n+1)/2$. We will want to prove that $\sum_{i=1}^{n'} i = n'(n'+1)/2$, that is, $\sum_{i=1}^{n+1} i = (n+1)(n+2)/2$. Now $\sum_{i=1}^{n+1} i = (\sum_{i=1}^{n} i) + (n+1)$, so after applying the induction hypothesis we just need to show that $n(n+1)/2 + (n+1) = (n+1)(n+2)/2$. We can prove this by rewriting the second $(n+1)$ on the left side of the equation as $2(n+1)/2$ to achieve a common denominator, and then adding fractions and simplifying. Now we have all the elements of the proof. A little reorganization and we will have a nice informal proof. We are done with the scratch work; here we go with the proof.

Proof. We will use induction with a shifted starting point.

Base case: Note that $\sum_{i=1}^{1} i = 1 = \frac{1(1+1)}{2}$, so the theorem holds for $n = 1$.

Induction step: Suppose that $1 \leq n$, and $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$. Then,

$$\begin{aligned}
\sum_{i=1}^{n+1} i &= \left(\sum_{i=1}^{n} i\right) + n + 1 \\
&= \frac{n(n+1)}{2} + n + 1 \qquad \text{(by the induction hypothesis)} \\
&= \frac{n(n+1)}{2} + \frac{2(n+1)}{2} \\
&= \frac{n(n+1) + 2(n+1)}{2} \\
&= \frac{(n+1)(n+2)}{2}.
\end{aligned}$$

Conclusion: By induction, we have shown $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$ for all $n \geq 1$. □

It is possible to formalize and prove Theorem 1 in PA. This would be a very involved process. First, we would have to find a formula in the language of PA that asserts that x is the sum of the natural numbers between 1 and n. this is no trivial feat in itself. Then we would have to decide how to formalize division by 2. Once we had a proper formalization of the theorem, we would still need to carry out the shifted induction argument. The induction step uses some algebra that we would need to backtrack and prove. This could all be done, but the insight gained by this process is not terribly interesting to the typical mathematician. Our informal proof does a good job of justifying the result without drowning us in the details.

Exercises.

1. Prove the following using informal induction arguments. You may use any previously proved theorems of PA, the algebraic properties in the example on page 67, and basic high school algebra facts.

   Theorem 2. $\sum_{k=0}^{n} 2^k = 2^{n+1} - 1$

   Theorem 3. $\sum_{k=1}^{n} 2k = n^2 + n$

   Theorem 4. $k \geq 1 \rightarrow 8|(9^k - 1)$

   Theorem 5. $n \geq 3 \rightarrow n^2 \leq 5n!$

2. Consider the theorem:

   Theorem 6. The sum of the first n odd numbers is n^2.

(a) Rewrite Theorem 6 using summation notation. (Hint: Every odd number is of the form $2k + 1$ for some k.)

(b) Prove Theorem 6 using an informal induction argument.

3. Find a formula in the language of PA with the free variables n and x that formalizes the statement "x is the sum of the natural numbers less than or equal to n."

4. *Strong induction* consists of the axiom scheme

$$A(0) \to (\forall n(\forall x(x \leq n \to A(x)) \to A(n')) \to \forall n A(n)).$$

The only difference from a standard induction argument is that in the induction step we are allowed to use all the preceding cases as the induction hypothesis. Thus, in proving $A(n')$, we may make use of $A(n)$, $A(n-1)$, $A(n-2)$, and so on. The strong induction scheme is a theorem of PA. It can also be proved with a shifted starting point.

The Fibonacci sequence is a sequence of integers defined by the formulas $f_1 = 1$, $f_2 = 1$, and $f_n = f_{n-1} + f_{n-2}$ for $n \geq 3$. Use strong induction to prove the following theorems:

Theorem 7. Prove that for all $n \geq 1$, $f_n \leq 2^n$.

Theorem 8. Prove that for all $n \geq 5$, $f_n \geq n$.

Theorem 9. Prove that for all $n \geq 9$, $f_n \geq 3n$.

3.4 Inductive Pitfalls

In the last section, we proved Theorem 1 which states that for all $n \geq 1$, $\sum_{i=1}^{n} i = n(n+1)/2$. It is possible to prove this theorem without using induction. Supposedly Gauss cooked up the following proof in order to solve a problem in elementary school.

Alternate Proof. Let $S_n = \sum_{i=1}^{k} i$. This sum can be written from smallest to largest or from largest to smallest:

$$\begin{aligned} S_n &= 1 + \quad 2 + 3 + \ldots + \quad n \\ S_n &= n + \quad (n-1) + (n-2) + \ldots + \quad 1 \end{aligned}$$

Adding these two equations term by term gives:

$$2S_n = (1+n) + (2+(n-1)) + (3+(n-2)) + \ldots + (n+1)$$

which is the same as

$$2S_n = (n+1) + (n+1) + (n+1) + \ldots + (n+1) = n(n+1).$$

Dividing both sides by 2, gives our result:

$$S_n = \frac{k(k+1)}{2}. \quad \square$$

Very clever boy, that Gauss! His use of dots in the middle of a sum is acceptable. Using dots as part of the argument can lead to difficulties. Here is an example of a bad use of dots.

Non-Theorem 1. $3^n \geq n!$.

Non-Proof. Consider the following cases:

n=0: $1 = 3^0 \geq 0! = 1$

n=1: $3 = 3^1 \geq 1! = 1$

n=2: $9 = 3^2 \geq 2! = 2$

n=3: $27 = 3^3 \geq 3! = 6$

$\vdots$

Proceeding in this fashion yields our result. $\square$

Not!!! In fact, this statement is also true for $n = 4$, 5, and 6. At $n = 7$ it fails, since $2187 = 3^7 < 7! = 5040$. Indeed, the theorem is false for all numbers above 6. Beware the abuse of dots. A collection of base cases does not make a valid argument. On the other hand, leaving out the base case can also cause difficulties, as shown by the next erroneous example.

Non-Theorem 2. $\sum_{i=1}^{n} i = \frac{n^2+n+2}{2}$

Non-Proof. Assume the statement is true for $n = k$, so $\sum_{i=1}^{k} i = \frac{k^2+k+2}{2}$, and consider

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

Expanding out the binomials and combining terms over the common denominator gives:

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

We know this is not correct! We proved the correct statement as Theorem 1. What went wrong? No base case. One last non-theorem will show us that not only must we consider the base case, but we must be sure we have the right base case.

Non-Theorem 3. All horses are the same color.

Non-Proof. We prove this theorem by induction on the number of horses.

Base case: One horse is the same color as itself.

Induction step: Assume that any set of k horses contains horses of one color. Consider a set, S, of $k+1$ horses. Choose any two horses x and y from S with $x \neq y$. To finish we must show x and y are the same color.

To accomplish this, look at the sets:

$$A = S \ / \{x\}$$

$$B = S \ / \{y\}$$

A and B are sets of k horses, and thus by the induction hypothesis each contains horses of one color. Now choose any z contained in $A \cap B$. z and y are both in A and are therefore the same color. z and x are both in B and are therefore the same color as well. Thus x is the same color as y. □

What is wrong here? We know that the statement is false! Somehow induction was not properly done. The error is a subtle one. We chose horses $x \neq y$ out of our set of horses S – that's two horses – and then we chose another horse z from S. That makes three horses in the smallest S possible for the induction step to make sense. So the base case should have been two horses, which is false! The moral of this example is: *Think very carefully about the base step.*

Now that we have mastered induction and seen some errors to avoid, it is very tempting to use our new hammer on every nail we see. Induction is not always the most direct approach to proving a theorem. In an induction proof, if the induction hypothesis is not used in the proof of the induction step, then induction can be avoided. The direct proof will resemble the proof of the induction step with the base case omitted. The next exercise illustrates this situation. Our erroneous proof of Non-theorem 2 looked like an induction step with the base case omitted, but in that argument we used the induction hypothesis. In the exercise, we can shorten the proof while avoiding the error.

Exercise.

1. Consider the theorem:

   Theorem 10. n is odd $\rightarrow n^2 - 1$ is divisible by 4.

   (a) Prove this theorem by induction. (Your induction step will not require the use of the induction hypothesis.)

   (b) Prove this theorem without using induction.

3.5 Proofs by Contradiction

Sometimes when we want to prove $P \rightarrow Q$, the easiest thing to do is to assume that $P \rightarrow Q$ is false, and derive a contradiction. By assuming the negation of

$P \to Q$, we are actually assuming both P and $\neg Q$, so we have two hypotheses to get us started. The fact that deducing a contradiction suffices to prove $P \to Q$ is a consequence of the following theorem about proofs in K.

Theorem (Proof by Contradiction)**.** If Γ is a collection of formulas with no free variables, and for some formula B there is a proof of $\Gamma, \neg A \vdash B \wedge \neg B$, and if that proof contains no applications of generalization to variables that occur free in A, then $\Gamma \vdash A$.

Proof. If there is a proof of $\Gamma, \neg A \vdash B \wedge \neg B$ with no inappropriate uses of GEN, then by the deduction theorem $\Gamma \vdash \neg A \to (B \wedge \neg B)$. Using this as a lemma, we have the following formal proof of $\Gamma \vdash A$.

1. $\neg A \to (B \wedge \neg B)$	Lemma
2. $(\neg A \to (B \wedge \neg B)) \to (\neg(B \wedge \neg B) \to A)$	Rule T
3. $\neg(B \wedge \neg B) \to A$	MP, lines 1 and 2
4. $\neg(B \wedge \neg B)$	Rule T
5. A	MP, lines 3 and 4

Thus, given the deduction of the contradiction $B \wedge \neg B$ from the assumption of $\neg A$, we may deduce that A holds. □

The inclusion of Γ in the theorem allows us to apply proof by contradiction in systems with additional axioms, like E and PA. Note that whenever we do proofs by contradiction, we must exhibit the same care concerning generalization that we use in applications of the deduction theorem. To see the importance of this, consider the following incorrect proof of $0' \neq 0'$. We begin by giving a correct formal proof of $\neg(x \neq 0') \vdash_{PA} 0 = 0' \wedge 0 \neq 0'$.

1. $\neg(x \neq 0')$	Given
2. $\neg(x \neq 0') \to x = 0'$	Rule T
3. $x = 0'$	MP, lines 1 and 2
4. $\forall x(x = 0')$	GEN, line 3
5. $\forall x(x = 0') \to 0 = 0'$	Axiom 4
6. $0 = 0'$	MP, lines 4 and 5
7. $\forall x(0 \neq x')$	Axiom 9 of PA
8. $\forall x(0 \neq x') \to 0 \neq 0'$	Axiom 4
9. $0 \neq 0'$	MP, lines 7 and 8
10. $0 = 0' \wedge 0 \neq 0'$	L18, lines 6 and 9

Due to the use of generalization on the variable x in line 2, we are blocked from applying proof by contradiction. If we ignored the restrictions of the theorem and just charged ahead, we would incorrectly conclude that $\vdash_{PA} x \neq 0$. Using this as a lemma, we could apply generalization and Axiom 4 and obtain the the consequences $\forall x(x \neq 0')$ and $0' \neq 0'$. The only error in this reasoning is the use of proof by contradiction in a situation with the wrong sort of application of generalization.

Now that we have a formal justification for proof by contradiction, we should look at examples of informal arguments based on this principle. Remember that the negation of $P \to Q$ is logically equivalent to $P \wedge \neg Q$.

Theorem 11. If n^2 is even, then n is even.

Proof. We will assume the negation of the theorem, giving us n^2 is even and n is not even. We expect to find a contradiction. Since n is not even, it is not a multiple of 2, so there is a k such that $n = 2 \cdot k + 1$. Thus,

$$\begin{aligned} n^2 = n \cdot n &= (2k+1) \cdot (2k+1) \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1 \end{aligned}$$

Note that $2k^2 + 2k$ is simply another natural number; call it j. Thus we have $n^2 = 2j + 1$, and so n^2 is odd. This contradicts our assumption that n^2 is even, so we have shown that n^2 is even implies n is even. □

Theorem 12. At a party of more than two people, there are at least two people who have the same number of friends at the party.

Proof. We will prove this by contradiction. Assume that there are n people at the party and that no two people have the same number of friends at the party. This means that we can match each person to their number of friends and list them in order:

person 1: 0 friends present

person 2: 1 friend present

person 3: 2 friends present

$\vdots$

person n: $n - 1$ friends present

Since person n has $n - 1$ friends present, every person at the party is a friend of person n. In particular, person 1 is a friend of person n. However, person 1 has 0 friends at the party, so person 1 is no friend of person n. Contradiction! So there are at least two people with the same number of friends present. □

Besides doing party tricks, proof by contradiction can be used to prove the next interesting theorem about prime numbers. Recall from item 6 in the example on page 67 that n is prime if and only if both $n > 1$ and if k divides n then $k = 1$ or $k = n$.

Theorem 13. There are infinitely many primes.

Proof. We will prove this theorem by contradiction. Assume that there are finitely many primes, say n of them. We can list them in order:

$$2 = p_1 < p_2 < p_3 < \cdots < p_n.$$

Now consider the natural number $q = p_1 \cdot p_2 \cdots p_n + 1$. Note that $p_n < p_n + 1 \leq p_1 \cdot p_2 \cdots p_n + 1 = q$, so $p_n < q$. Because p_n is the biggest prime, q is not a prime.

Since q is not prime and $1 < q$, we know q has a prime factorization using some of the n listed primes, say k of them:

$$q = p_{i_1} \cdot p_{i_2} \cdots p_{i_k}.$$

We have two different expressions for q. Equating them yields

$$p_1 \cdot p_2 \cdots p_n + 1 = p_{i_1} \cdot p_{i_2} \cdots p_{i_k}.$$

Choose any prime from the prime factorization on the right, say p_{i_1}. Our number p_{i_1} divides the right side of this equation, so it must also divide the left side. Because p_{i_1} is a prime, it appears in the list $p_1, p_2, \ldots p_n$, and so p_{i_1} divides $p_1 \cdot p_2 \cdots p_n$. Since p_{i_1} divides the first term of the left side, and it divides the entire left side, it must divide the second term on the left, so p_{i_1} must divide 1. Thus $p_{i_1} = 1$, contradicting the assumption that p_{i_1} is a prime! Thus there must not be a largest prime, and so there are infinitely many. □

We used two *facts* in this proof that deserve further discussion:

If $a + b = c$, $p|a$ and $p|c$ then $p|b$.

q is not prime, then it has a prime factorization.

These are both worthy of proofs themselves. They are certainly not obvious from our basic axioms or from the definitions of divisibility and prime. A mathematician would prove these results first, perhaps as *lemmas*, and then cite them in the main proof. Let's prove these lemmas.

Lemma 1. If $a + b = c$, $p|a$ and $p|c$ then $p|b$.

Proof. Let $a + b = c$. Then subtracting a from both sides of this equation gives $b = c - a$. Since $p|a$ and $p|c$, $p|(c - a)$. Because $c - a$ is b, this implies that $p|b$. □

Lemma 2. Every natural number greater than 1 is either prime or has a prime factorization.

Proof. We will prove this result by induction.

Base case: $n = 2$ is prime.

Induction step: Assume all numbers greater than 2 and less than k are prime or have prime factorizations. We must show that k is either prime or has a prime factorization. There are two cases: either k is prime or k is not prime. If k is prime, we've attained our conclusion, so we'll assume k is not prime.

By the definition of prime number, k is not prime implies that we can find m and d each strictly between 1 and k so that $k = m \cdot d$. Note that $m < k$ and $d < k$, so by the induction hypothesis, m and d are either prime or have prime factorizations. Since m is a product of one or more primes and d is a product of one or more primes, $k = m \cdot d$ is a product of two or more primes. Summarizing, in this case k has a prime factorization, completing the proof of the induction step, and the entire proof. □

Theorem 14. If $2^n - 1$ is prime, then n is prime.

Proof. We'll assume that $2^n - 1$ is prime and that n is not prime, and look for a contradiction. Since n is not prime, there are factors x and y such that $n = x \cdot y$, and $1 < x$, $y < n$.

So

$$\begin{aligned} 2^n - 1 = 2^{xy} - 1 &= (2^x)^y - (1)^y \\ &= (2^x - 1)((2^x)^{y-1} + (2^x)^{y-2} + ... + 1). \end{aligned}$$

Since we can factor in this way, we have found a factorization of $2^n - 1$, but $2^x - 1$ is not equal to either or $2^n - 1$ because x is not equal to either 1 or n. So $2^n - 1$ has a factorization different from 1 and itself. Thus $2^n - 1$ cannot be prime, contradicting our initial assumption. □

Wow! This proof uses a very weighty fact of algebra, which we will leave as an exercise:

Theorem 15. $x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + ... + 1)$

Every proof by contradiction can be proved directly. In fact, a direct proof of the contrapositive often is more succinct than a proof by contradiction, but still allows us to utilize the negation of the conclusion. Consider the following theorem and proof.

Theorem 16. If $n > 2$ then there is no m such that $n|m$ and $n + m = nm$.

Proof. We will prove the contrapositive: If there is an m such that $n+m = nm$ and $n|m$ then $n \leq 2$. Assume that $n + m = nm$ and $n|m$. Since $n|m$, we can find a k such that $m = nk$. Thus $m + n = nk + n = n(k + 1)$ and $nm = n \cdot nk$. Since $m + n = nm$, we have $n(k + 1) = n \cdot nk$, so $k + 1 = nk$. Subtracting k from both sides and factoring yields $1 = k(n - 1)$, so $k = 1$ and $n - 1 = 1$. Since $m = nk$, we have $m = 2$ as desired.

Exercises.

1. Prove Theorem 15.

2. Prove the following theorems. You may wish to use proofs by contradiction.

   Theorem 17. If n^2 is odd, then n is odd.

   Theorem 18. The sum of the cubes of two consecutive natural numbers cannot be equal to the cube of the next largest number.

   Theorem 19. If m and n are odd then $x^2 - 2mx + 2n = 0$ has no natural number solution, x.

   Theorem 20. If for all m, $1 < m \leq \sqrt{p}$ implies m does not divide p, then p is prime.

   Theorem 21. There are at least two people in the world with exactly the same number of hairs on their heads.

3.6 Other Strategies

Many strategies for informal proofs follow directly from their formal counterparts. Here are a few examples:

Existence: To show something exists, we must either cite it, (i.e., give an example) or show that it has to occur without actually producing it. This latter situation is called an *indirect* proof, and is sometimes accomplished through a proof by contradiction: Assume that it doesn't exist and derive a contradiction.

Uniqueness: To show that something is unique, it is almost always easiest to assume that there are two with the same properties and then prove that the two are equal.

If and Only If Statements (iff or $\leftrightarrow$): From propositional logic, we know that to accomplish the proof of $A \leftrightarrow B$, we can prove both $A \rightarrow B$ and $B \rightarrow A$. The two directions might use very different approaches. It is unusual for such a statement to be proven without dividing it into the two cases.

Showing that two Expressions are Equal: We have seen direct proofs of $A = B$. Sometimes, it is not obvious how to accomplish this. There are other, equivalent forms of equality that may be easier to prove:

$A - B = 0$
$(A \geq B) \wedge (B \geq A)$
$\frac{A}{B} = 1, B \neq 0$

Composite Statements: If either the hypothesis or the conclusion is composite, i.e., is a compound statement, we must be careful when deciding what to assume and what to prove:

1. $(A \wedge B) \rightarrow C$. We assume both A and B are true and proceed to prove C if using a direct method. To use contrapositive methods, be careful! The conclusion becomes $\neg(A \wedge B)$ which we know from propositional logic is logically equivalent to $\neg A \vee \neg B$.
2. $(A \vee B) \rightarrow C$. This is really two proofs: $A \rightarrow C$ and $B \rightarrow C$.
3. $C \rightarrow (A \wedge B)$. Assume C and show both $C \rightarrow A$ and $C \rightarrow B$. Again we need to be careful constructing the contrapositive; the hypothesis will be $\neg A \vee \neg B$.
4. $C \rightarrow (A \vee B)$. This is logically equivalent to $C \rightarrow (\neg A \rightarrow B)$ and also logically equivalent to $C \rightarrow (\neg B \rightarrow A)$. You can pick whichever form seems best at the moment and start your proof with two hypotheses.

Here are some exercises to sharpen your proof writing skills.

Exercises.

1. Give informal proofs of the following theorems.

   Theorem 22. There are natural numbers a, b, and c such that $a^2 + b^2 = c^2$.

   Theorem 23. There is a natural number n such that $2^n + 7^n$ is prime.

   Theorem 24. Every natural number has a unique prime factorization.

   Theorem 25. Every pair of natural numbers has a common multiple.

   Theorem 26. There is a unique integer n for which $2n^2 - 3n - 2 = 0$.

   Theorem 27. If n is a multiple of 3, then either n is odd or n is a multiple of 6.

   Theorem 28. If $n \neq 0$ then either n is a multiple of 2 or $n = 2k + 1$ for some k.

   Theorem 29. No natural number is both even and odd.

   Theorem 30. If b is a multiple of 2 and a multiple of 5 then b is a multiple of 10.

   Theorem 31. If $a|b$, $b|c$, and $c|a$, then $a = b = c$.

   Theorem 32. $m^2 = n^2$ iff $m = n$.

   Theorem 33. If $m \cdot n = \frac{(m+n)^2}{2}$ then $n = m = 0$.

Theorem 34. 3 must divide the sum of any three consecutive numbers.

Theorem 35. If $3|n$ then 3 divides the sum of the digits of n.

Theorem 36. For any number with at least two trailing zeros, if 4 divides the number obtained by deleting the trailing zeros, the 4 divides the original number.

Theorem 37. If X is a set with $n \geq 2$ elements, then X has $\frac{1}{2}n(n-1)$ subsets with exactly 2 elements.

Theorem 38. For $n \geq 1$, the equation $\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \cdots + \frac{1}{n\cdot(n+1)} = \frac{n}{n+1}$ holds.

Theorem 39. Every set with n elements has exactly 2^n subsets.

Theorem 40. For every n, the number $n^3 - n$ is divisible by 3.

Theorem 41. $\forall n > 0\big(8|(5^n + 2 \cdot 3^{n-1} + 1)\big)$.

Theorem 42. $\sum_{k=1}^{n} k \cdot k! = (n+1)! - 1$.

Theorem 43. $\forall n \geq 5\ (2^n > n^2)$.

Theorem 44. If $a|b$ and $b|a$ then $a = b$.

Theorem 45. $\sum_{k=1}^{n} k^3 = \frac{n^2(n+1)^2}{4}$.

2. The greatest common divisor of m and n, denoted by $\gcd(m,n)$, is the largest number that divides both m and n. The least common multiple of m and n, denoted by $\text{lcm}(m,n)$ is the smallest number that both m and n divide. Prove:

Theorem 46. For all a and b, if $a \neq 0$ and $b \neq 0$ then $\text{lcm}(a,b) = \frac{ab}{\gcd(a,b)}$.

Chapter 4

Alternation of Quantifiers – Sequences

In this section we will study sequences and sequence convergence. The statements in this chapter will involve the alternation of quantifiers, so let's review some of what we did formally.

Remember that $\forall x \exists y$ has a different meaning from $\exists y \forall x$. In the first, we are required to produce *for each x, a corresponding y*, and in the second we are required to produce *a single y that works for every x*. Let's review this idea with an example:

Let the universe be the set of people Tom, Dick and Harry. Consider the predicate $P(x, y) = x$ likes y. Then all possible alternating quantifiers are:

$\forall x \exists y(P(x, y))$ which translates to everyone likes someone.

In particular for our universe we would have to identify someone Tom likes, someone Dick likes and someone Harry likes. The "someones" could all be the same or different - doesn't matter.

$\forall y \exists x(P(x, y))$ which translates to everyone is liked by someone.

In particular for our universe we would have to identify some person Tom, Dick and Harry all like. Here it has to be the same person for all three.

$\exists x \forall y(P(x, y))$ which translates to someone likes everyone.

We have to identify one person who likes everyone of Tom, Dick and Harry.

$\exists y \forall x(P(x, y))$ which translates to someone is liked by everyone.

We have to identify one person who is liked by all of Tom, Dick and Harry.

Having this under our belts, notice the occurances of alternating quantifiers in the basic definitions about sequences below.

4.1 Sequences, Bounds and Convergence

We start with a definition of sequence.

Definition. A **sequence** is a mapping from $\mathbb{N} \to \mathbb{R}$, for which every n in $\mathbb{N}$ is mapped to a unique a_n in $\mathbb{R}$, i.e., the sequence is a function from $\mathbb{N}$ into $\mathbb{R}$.

When a_n is the n-th term, we write the sequence as

$$\langle a_n \rangle$$

where n takes on every value in $\mathbb{N}$, unless otherwise stated.

Here are some examples to investigate:

$\langle n \rangle$: $0, 1, 2, 3, 4, \ldots, n, \ldots$

$\langle 2^{-n} \rangle$: $1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \ldots, \frac{1}{2^n}, \ldots$

$\langle 2^{-n} \rangle_1^\infty$: $\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, ..., \frac{1}{2^n}, \ldots$

$\langle (-1)^n \rangle_0^\infty$: $1, -1, 1, -1, 1, -1, 1, \ldots$

$\langle n \rangle_3^\infty$: $3, 4, 5, 6, \ldots, n, \ldots$

Let's start by investigating convergence of sequences. What does this mean? We say that a sequence converges if it eventually settles down to some real value, L. By this we mean that we want the sequence to stay close to L after it settles down, i.e., it can't start to drift away again. We don't care how far out in the sequence we have to look before we see this trend.

In calculus we used a simple approach for estimating L for a given series. We looked at the dominating terms:

$a_n = \frac{n}{2n+1}$ is about the same as $\frac{n}{2n}$ when n is really large, so we expect the series to settle down near $\frac{1}{2}$ for large n.

$a_n = \frac{n}{n^2+1}$ is about the same as $\frac{n}{n^2}$ when n is really large, so we expect the series to behave like $\frac{1}{n}$ as n gets really large. Thus this sequence is getting really close to 0.

$a_n = n$ grows larger and larger, so it never settles down to a finite number. In this case, we could say that a_n doesn't converge or that $a_n \to \infty$.

$a_n = sin(n)$ oscillates back and forth, so it never settles down to any number, and it doesn't grow larger and larger. Here we would say that a_n doesn't converge.

How can we say this mathematically and precisely?

Definition. $\langle a_n \rangle$ **converges** to $L < \infty$, written $a_n \to L$, if and only if

$$\forall \epsilon > 0 \; \exists N \in \mathbb{N} \; \forall m > N \; (|a_m - L| < \epsilon).$$

Notice the alternation of quantifiers $\forall\exists$. We are required for a given ϵ to produce an index N after which the terms in the sequence are within ϵ of L. We'll use this idea to build some proofs later in this section.

The last example above doesn't converge, but it does stay trapped between 1 and -1. This leads to another definition (actually three definitions in one).

Definition. indexsequence!bounds $\langle a_n \rangle$ is **bounded from above** if and only if $\exists U\ \forall n\ (a_n \leq U)$. The sequence $\langle a_n \rangle$ is **bounded from below** if and only if $\exists L\ \forall n\ (a_n \geq L)$. The sequence $\langle a_n \rangle$ is **bounded** if and only if $\exists U\ \exists L\ \forall n\ (L \leq a_n \leq U)$.

Notice the alternation of quantifiers here again, this time $\exists\forall$. So we are required to produce a bounding number that works for all elements of the sequence. Let's use the definitions to prove some convergence results:

Theorem 1. $\langle \frac{n}{2n+1} \rangle$ converges to $\frac{1}{2}$.

So how do we get started? Suppose we have the ϵ. Then we need to give an N so that $m > N$ gives:

$$\left| \frac{m}{2m+1} - \frac{1}{2} \right| < \epsilon$$

Working backwards from here, we see that

$$\left| \frac{2m - (2m+1)}{2(2m+1)} \right| < \epsilon$$

$$\frac{1}{2(2m+1)} < \epsilon$$

Solving this for ϵ gives

$$\frac{1}{2\epsilon} < 2m + 1$$

So it looks like

$$m > \frac{\frac{1}{2\epsilon} - 1}{2}$$

would give us what we need.

How do we write this up in a proper proof?

Proof. Fix $\epsilon > 0$, and consider $N = \frac{\frac{1}{2\epsilon} - 1}{2}$. Let $m > N$. Then

$$\begin{aligned} |a_m - L| &= \left| \frac{m}{2m+1} - \frac{1}{2} \right| \\ &= \left| \frac{-1}{2(2m+1)} \right| \\ &= \frac{1}{2(2m+1)} \\ &< \frac{1}{2\left[2\left(\frac{\frac{1}{2\epsilon}-1}{2}\right)+1\right]} \\ &= \frac{1}{\frac{1}{\epsilon}} = \epsilon. \end{aligned}$$

Thus, for any given $\epsilon > 0$, we have shown how to produce an N such that if $m > N$ then $|a_m - L| < \epsilon$. $\square$

Theorem 2. $\langle \frac{n}{2n+1} \rangle$ is bounded.

This is an easy theorem to prove; we simply have to come up with two numbers, a lower bound and an upper bound, for the sequence. Looking at the first few numbers in the sequence gives:

$$\langle \frac{n}{2n+1} \rangle : 0, \frac{1}{3}, \frac{2}{5}, \frac{3}{7}, ...$$

Notice that this peaks at 1 and then the numbers are all less than 1 and greater than 0. So the proof is going to be quite simple:

Proof. Consider the sequence $\langle \frac{n}{2n+1} \rangle$, and let $U = 1$ and $L = 0$. Clearly, for every n, $0 \leq \frac{n}{2n+1} \leq 1$, so $L \leq \frac{n}{2n+1} \leq U$ and thus the sequence is bounded. $\square$

Theorem 3. If $a_n = \begin{cases} 2^{-n} & \text{if } n \text{ is even} \\ 3^{-n} & \text{if } n \text{ is odd} \end{cases}$ then $\langle a_n \rangle$ converges to 0.

This sequence is more complicated. How do we handle this case? First of all, what does this sequence look like?

$$1, \frac{1}{3}, \frac{1}{2^2}, \frac{1}{3^3}, \frac{1}{2^4}, \frac{1}{3^5}, ...$$

So it's components of the two sequences:

$$1, \frac{1}{2}, \frac{1}{2^2}, \frac{1}{2^3}, \frac{1}{2^4}, \frac{1}{2^5}, ...$$

$$1, \frac{1}{3}, \frac{1}{3^2}, \frac{1}{3^3}, \frac{1}{3^4}, \frac{1}{3^5}, ...$$

Let's look at the convergence of these two sequences first. Clearly they both converge to 0. Starting with 2^{-n} let's work backwards again to see if we can write N in terms of ϵ. We'll come back to theorem 3 afterwards.

Theorem 4. $\langle 2^{-n} \rangle$ converges to 0.

$$\left|2^{-N} - 0\right| < \epsilon$$

$$2^{-N} < \epsilon$$

One way to solve for N would be to take the $\log_2$ of both sides:

$$-N < \log_2 \epsilon$$

$$N > -\log_2 \epsilon$$

Ok; so recapping, the proof should work as follows: Fix ϵ, and let $N = -\log_2 \epsilon$. Algebra should get us

$$\left|2^{-N} - 0\right| < \epsilon$$

Let's write this out formally, just to be sure:

Proof. (Theorem 4) Choose an arbitrary $\epsilon > 0$, and consider $N = -\log_2 \epsilon$. For the sequence $\langle 2^{-n} \rangle$ and $m > N$, we need to show that

$$\left|2^{-m} - 0\right| < \epsilon.$$

We have

$$\left|2^{-m} - 0\right| = 2^{-m}.$$

Since $m > N$ and $N = -\log_2 \epsilon$, we have that $m > -\log_2 \epsilon$, so:

$$\left|2^{-m} - 0\right| < 2^{\log_2 \epsilon} = \epsilon. \quad \square$$

The proof for convergence of $\langle 3^{-n} \rangle$ should work the same way using an N of $-\log_3 \epsilon$. How do we combine these to prove Theorem 2? We need to find an N that works regardless of whether the later term is 2^{-m} or 3^{-m}.

So what we really need to do is to choose the larger N given ϵ, i.e., choose the larger of $-\log_2 \epsilon$ and $-\log_3 \epsilon$. This will guarantee that we are far enough out on the sequence so that the terms are within ϵ of 0. Which if these two logs is larger? That depends on ϵ, and since we don't want to make any assumptions regarding ϵ, we will simply let $N = max\{-\log_2 \epsilon, -\log_3 \epsilon\}$.

Here is the proof of Theorem 3:

Proof. (Theorem 3) Choose an arbitrary $\epsilon > 0$, and consider the number N defined by $N = max\{-\log_2 \epsilon, -\log_3 \epsilon\}$. For the sequence $\langle a_n \rangle$ and $m > N$, we need to show that

$$|a_m - 0| < \epsilon.$$

Consider the following cases:

When m is even, we can say that $N \geq -\log_2 \epsilon$, so we have that $m > N$ implies $m > \log_2 \epsilon$. Thus

$$|a_m - 0| = \left|2^{-m} - 0\right| < 2^{\log_2 \epsilon} = \epsilon.$$

When m is odd, we can say that $N \geq -\log_3 \epsilon$, so we have that $m > N$ implies $m > \log_3 \epsilon$. Thus

$$|a_m - 0| = \left|3^{-m} - 0\right| < 3^{\log_3 \epsilon} = \epsilon. \quad \square$$

In the proofs above, simple algebra allowed us to solve for N in terms of ϵ. Sometimes bounding the sequence by another, simpler sequence is a better approach.

Theorem 5. $\langle \frac{2n^2}{n^3+1} \rangle$ converges to 0.

How should we proceed? We could try to solve $\frac{2N^2}{N^3+1} < \epsilon$ for N in terms of ϵ. This would be very messy:

$$\frac{2N^2}{N^3+1} < \epsilon$$
$$2N^2 < \epsilon \cdot (N^3+1)$$
$$2N^2 - \epsilon \cdot (N^3+1) < 0$$

Yuk! It's cubic in N.

A better approach: Note that

$$\frac{2N^2}{N^3+1} < \frac{2N^2}{N^3} = \frac{2}{N}$$

because we have made the denominator smaller by subtracting 1, and hence the fraction is larger.

This implies that if we find an N that works for the series with general term $\frac{2}{N}$ then it will also work for the series with general term $\frac{2N^2}{N^3+1}$. Why? The inequality tells us that no matter what index we are interested in, $\frac{2N^2}{N^3+1}$ is below $\frac{2}{N}$, so if we find the place on $\frac{2}{N}$ where all subsequent terms are within ϵ of L, all subsequent terms of $\frac{2N^2}{N^3+1}$ will also be within ϵ of L.

So we have a new question: What N works for $\langle \frac{2}{N} \rangle$? Let's try the algebraic way of getting N in terms of ϵ:

$$\frac{2}{N} - 0 < \epsilon$$
$$\frac{2}{\epsilon} < N$$

How do we put this all together in our proof?

Proof. Choose an arbitrary $\epsilon > 0$, and consider $N = \frac{2}{\epsilon}$. For the sequence $\langle \frac{2n^2}{n^3+1} \rangle$ and $m > N$, we need to show that

$$\left| \frac{2m^2}{m^3+1} - 0 \right| < \epsilon.$$

We have

$$\left| \frac{2m^2}{m^3+1} - 0 \right| = \frac{2m^2}{m^3+1} < \frac{2}{m}.$$

Since $m > N$ and $N = \frac{2}{\epsilon}$, we have that $m > \frac{2}{\epsilon}$, so:

$$\left| \frac{2m^2}{m^3+1} - 0 \right| < \frac{2}{m} < \frac{2}{\frac{2}{\epsilon}} = \epsilon. \quad \square$$

Exercise 4.1. Do the following sequences converge? If so, to what? Are they bounded? If so, by what? Provide proofs for those that converge and/or are bounded.

a. $a_n = 1 + \frac{1}{n}$

b. $a_n = \frac{1+(-1)^n}{2}$

c. $a_n = 1 + \frac{1}{2} + \frac{1}{3} + ... + \frac{1}{n}$

d. $a_n = \frac{2n}{3n+1}$

e. $a_n = \frac{3n+7}{n}$

f. $a_n = \frac{n^2}{n+1}$

g. $a_n = \frac{n^2}{2n^2+1}$

h. $a_n = (-1)^n 2^{-n}$

i. $a_n = \frac{\sin(n)}{n}$

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

k. $a_n = \frac{5n}{4-n}$ (where $n \geq 5$)

4.2 More on Convergence and Boundedness

Now that you have worked with some specific sequences, we will think about general properties of sequences. To start, try to find examples for the following exercises.

Exercise 4.2. Find examples for each, if possible:

a. A sequence that is bounded but does not converge.

b. $\langle a_n \rangle$ and $\langle b_n \rangle$ do not converge but $\langle a_n + b_n \rangle$ does.

c. $\langle a_n \rangle$ and $\langle b_n \rangle$ do not converge but $\langle a_n \cdot b_n \rangle$ does.

d. A sequence that is not bounded.

e. $\langle |a_n| \rangle$ converges to A but $\langle a_n \rangle$ does not converge.

f. Is there a sequence that converges to two different numbers?

g. Is there a convergent sequence that is not bounded?

These ideas lead to us to conjecture some theorems:

Theorem 6. Every convergent sequence is bounded.

How shall we start this one? Let the limit be A and note that eventually (for m's greater than some N) $|a_m - A| < 1$, or

$$A - 1 < a_m < A + 1.$$

Why? We are using the definition for the specific case of $\epsilon = 1$. Thus a lower bound can be found by choosing the smallest number from the set $\{a_1, a_2, ..., a_n, A-1\}$ and an upper bound can be found by choosing the largest number from the set $\{a_1, a_2, ..., a_n, A + 1\}$.

Proof. Suppose $|a_n|$ converges to A. Choose $\epsilon = 1$; then there is an N such that $m > N$ implies

$$A - 1 < a_m < A + 1.$$

Let $L = min\{a_1, a_2, ..., a_n, A - 1\}$ and $U = max\{a_1, a_2, ..., a_n, A + 1\}$. Then for all n, $L < a_n < U$. □

Theorem 7. The limit of a convergent sequence is unique.

So how will we prove this? In the standard way: Assume there are 2 limits and show that they must be equal. This is not so easy as it sounds. Here is a proof. Notice that we are using a specific ϵ again.

Proof. We will prove this by contradiction. Assume $\langle a_n \rangle$ converges to A and also to B, and assume that $A < B$. Let $\epsilon = \frac{1}{2}(B - A)$. Since $\langle a_n \rangle$ converges to A, we know that there is an N_1 such that for all $m > N_1$ we have $|a_m - A| < \epsilon$ or

$$A - \epsilon < a_m < A + \epsilon.$$

Similarly, since $\langle a_n \rangle$ converges to B, we know that there is an N_2 such that for all $m > N_2$ we have $|a_m - B| < \epsilon$ or

$$B - \epsilon < a_m < B + \epsilon.$$

As long as we are beyond both N_1 and N_2, we have:

$$A + \epsilon = A + \frac{1}{2}(B - A) = B - \frac{1}{2}(B - A) = B - \epsilon$$

This is a contradiction, since $B - \epsilon < a_m < A + \epsilon$. □

This is not the only way to prove this theorem. Can you develop another proof?

Theorem 8. If $\langle a_n \rangle$ converges to A and $\langle b_n \rangle$ converges to B then $\langle a_n + b_n \rangle$ converges to $A + B$.

So how do we approach this? We need

$$|(a_N + b_N) - (A + B)| < \epsilon$$

or

$$|(a_N - A) + (b_n - B)| < \epsilon.$$

Can we say that $|a_N - A| < \frac{\epsilon}{2}$ and $|b_N - B| < \frac{\epsilon}{2}$? Sure! The definition says that we have the result for all ϵ, so we also have it for any $\frac{\epsilon}{2}$. Here is the proof:

Proof. Choose $\epsilon > 0$. Since $\langle a_n \rangle$ converges to A, we know that there is an N_1 such that for all $m > N_1$ we have $|a_m - A| < \frac{\epsilon}{2}$.

Similarly, since $\langle b_n \rangle$ converges to B, we know that there is an N_2 such that for every $m > N_2$ we have $|b_m - B| < \frac{\epsilon}{2}$.

Let $N = max\{N_1, N_2\}$. Then for all $m > N$, we have

$$|(a_m + b_m) - (A + B)| \leq |a_m - A| + |b_m - B| < \epsilon. \quad \square$$

Here are some more theorems to prove.

Theorem 9. If $\langle a_n \rangle$ converges to A then $\langle c \cdot a_n \rangle$ converges to cA.

Theorem 10. If $\langle a_n \rangle$ converges to A then $\langle c + a_n \rangle$ converges to $c + A$.

Theorem 11. $\langle a_n \rangle$ converges to A iff $\langle a_n - A \rangle$ converges to 0.

Theorem 12. If $\langle a_n \rangle$ converges to A, $\langle b_n \rangle$ converges to A and for all n the inequality $a_n \leq c_n \leq b_n$ holds, then $\langle c_n \rangle$ converges to A as well.

Theorem 13. If $\langle a_n \rangle$ converges to A, $\langle b_n \rangle$ converges to B and for all n the inequality $a_n \leq b_n$ holds, then $A \leq B$.

Theorem 14. $\langle a_n \rangle$ converges to A inplies that $\langle |a_n| \rangle$ converges to $|A|$.

Theorem 15. If $\langle a_n \rangle$ converges to 0 and $\langle b_n \rangle$ is bounded, then $\langle a_n \cdot b_n \rangle$ converges to 0.

Theorem 16. If $\langle a_n \rangle$ converges to A and $\langle b_n \rangle$ converges to B then $\langle a_n \cdot b_n \rangle$ converges to $A \cdot B$.

Theorem 17. If $\langle a_n \rangle$ converges to A and $\langle b_n \rangle$ converges to B, with $B \neq 0$ and $\forall n, b_n \neq 0$, then $\langle \frac{a_n}{b_n} \rangle$ converges to $\frac{A}{B}$.

4.3 A Note on Divergent Sequences

Are there sequences that don't converge? Yes! We already saw that $\langle n \rangle$ diverges to ∞ and that $\langle \sin(n) \rangle$ doesn't ever settle down. How can we prove that a sequence diverges? To understand this, we need to examine the negation of the definition of convergence. Let's start with a more formal version of the definition:

$\langle a_n \rangle$ **converges** iff $\exists L \; \forall \epsilon > 0 \; \exists N \in \mathbb{N} \; \forall m > N \; (|a_m - L| < \epsilon)$.

The negation is:
$\langle a_n \rangle$ **diverges** iff $\neg \exists L \; \forall \epsilon > 0 \; \exists N \in \mathbb{N} \; \forall m > N \; (|a_m - L| < \epsilon)$.

Now let's use our knowledge of negation and quantifiers to push the negation all the way to the interior of the formula:

$\langle a_n \rangle$ **diverges** iff $\forall L \; \exists \epsilon > 0 \; \forall N \in \mathbb{N} \; \exists m > N \; (|a_m - L| \geq \epsilon)$.

So we need to show that if we choose an arbitrary L, there is an ϵ that works for all N. Let's try a simple one:

Theorem 18. The sequence $\langle n \rangle$ diverges.

To do this proof, choose an arbitrary L. We need find an ϵ so that we end up with

$$|N - L| \geq \epsilon,$$

and it needs to work for some $m > N$ no matter what N is chosen. If we choose $\epsilon = \frac{1}{2}$ and we pick an arbitrary N we can find a number $m > N$, namely $m = N+1+L$ so that $|m-L| \geq \epsilon$, since $|a_m - L| = |m-L| = |N+1+L-L| = N+1 \geq \frac{1}{2}$.

Proof. Choose an arbitrary L, let $\epsilon = \frac{1}{2}$, and choose an arbitrary N. Then consider $m = N + 1 + L$:

$$|m - L| = |N + 1 + L - L| = N + 1 \geq \frac{1}{2} = \epsilon. \quad \square$$

When a bounded sequence diverges, its values tend to oscillate within a restricted range. It is often easiest to start the proof by selecting a value b and a quantity ϵ such the sequence bounces above $b + \epsilon$ infinitely many times and below $b - \epsilon$ infinitely many times. For any L there are two possible cases. If $L \geq b$ (so L is high), then for any N there is an $m > N$ such that $b - \epsilon > a_m$ (so a_m is low) and consequently, $|a_m - L| \geq b - a_m > \epsilon$. On the other hand, if $L < b$ (so L is low), then for any N there is an $m > N$ such that $b + \epsilon < a_m$ (so a_m is high) and consequently, $|a_m - L| \geq a_m - b > \epsilon$. Of course, the initial choices of b and ϵ will depend on the sequence.

Exercise 4.3. Prove that the following sequences diverge.

a. $a_n = n + 5$

b. $a_n = n^2$

c. $a_n = n!$

Exercise 4.4. Prove that the following bounded sequences diverge.

a. $a_n = (-1)^n$

b. $a_n = \cos(n\pi/2)$

c. $a_n = \sin(n)$

   Hint: For any N, obtain m by rounding $N \cdot 2\pi$ up to the next largest integer (i.e. $m = \lceil N \cdot 2\pi \rceil$). If we view m as an angle in radians it will correspond to an angle between 0 and 1 radians. Thus $m + 1$ will be an angle between 1 and 2 radians, so $\sin(m + 1) \geq .8$. Also, $m + 4$ will be between 4 and 5 radians, so $\sin(m + 4) \leq -.75$.

Exercise 4.5. Prove that the sequence $a_n = n \sin(n)$ diverges. (Hint: Use the hint from exercise 4.4c.)

Chapter 5

Introduction to set theory

Most upper level mathematics courses use at least some notation from set theory and many apply results and techniques from set theory. The logical expertise that you have gained in the preceding chapters is directly applicable to the study of sets.

Naïve set theory and axiomatic set theory are the Scylla and Charybdis of this topic. On the one hand, naïve set theory concentrates on the portion of set theory that is most frequently applied by mathematicians. Unfortunately, it glosses over some problems with existence of sets that can lead to paradoxes. Axiomatic set theory is engineered specifically to address these existence problems. As appealing as a purely axiomatic approach is, the usual formulation of the axioms treats many of the central constructs of set theory as abbreviations, sidestepping the material which is most useful in everyday practice.

We will try to thread a course between the two extremes, mentioning axioms when they are pertinent and introducing many of the concepts you will need for your future courses. With any luck, we won't be drawn down or chewed up.

5.1 Familiar sets and symbols

We can start our discussion of sets by listing a few very familiar concrete examples. Attaching a nice symbol to each of these sets will make it easier to talk about them later.

Natural numbers: $\mathbb{N} = \{0, 1, 2 \dots\}$

Integers: $\mathbb{Z} = \{\cdots -1, -2, 0, 1, 2 \dots\}$

Rational numbers: $\mathbb{Q} = \{\frac{a}{b} \mid a \in \mathbb{Z} \wedge b \in \mathbb{N} \wedge b \neq 0\}$.

A few rational numbers: $\frac{1}{3}$, $\frac{2}{6}$, $\frac{-1}{12}$, 0, 7

Real numbers: $\mathbb{R}$

A few real numbers: 0, -6, $\frac{1}{3}$, $\sqrt{3}$, π

The fancy script used for these set symbols is called "blackboard bold." The idea is that it is easier to draw two close lines with a piece of chalk than it is to draw one wide line. The particular letters seem to make some sense. $\mathbb{N}$ for **n**atural numbers and $\mathbb{R}$ for **r**eal numbers are obvious choices. Since every rational number can be written as a **q**uotient, $\mathbb{Q}$ seems reasonable. Finally, the german word for number is *Zahl*, so $\mathbb{Z}$ fur die Zahlen steht.

Various authors may or may not include 0 in the set of natural numbers. Since we would like $\mathbb{N}$ to be a model of the Peano axioms, and those axioms include a constant symbol for 0, we should definitely include 0. People who don't care about the Peano axioms will sometimes leave it out. It is always safest to double check what the particular book says.

The formula $x \in y$ means "x is an element of y." We will also write $x \notin y$ as an abbreviation for $\neg(x \in y)$. Combined with our letters for common sets, this notation provides a very convenient shorthand. Rather than saying "2 is a natural number and π is not a natural number," we can write $2 \in \mathbb{N}$ and $\pi \notin \mathbb{N}$.

The formula $A \subset B$ is read "A is a subset of B." $A \subset B$ means that every element of A is also an element of B. More formally, $A \subset B$ means $\forall t(t \in A \to t \in B)$. Note that this tells us that to prove that $A \subset B$, we should start with an arbitrary element t and prove the implication $t \in A \to t \in B$. Depending on the situation, we might prove the implication directly, prove the contrapositive, or do a proof by contradiction.

Notation for subsets varies from book to book. Some books use $A \subseteq B$ to denote $A \subset B$ and then use $A \subset B$ for $A \subseteq B \wedge A \neq B$. We will use $A \subsetneq B$ to denote $A \subseteq B \wedge A \neq B$. The formula $A \subsetneq B$ is read "A is a proper subset of B." All these symbols can be reversed in the same fashion as $<$ and $>$, so $A \subset B$ means exactly the same thing as $B \supset A$. We can also write $A \not\subset B$ as an abbreviation of $\neg(A \subset B)$, and make similar negated forms of all the preceding notation.

Although both $\in$ and $\subset$ denote forms of containment, they denote different sorts of containment. Consider the set $A = \{1, \{2\}, \{1, 2\}\}$. The set A has exactly three elements. We can see that $1 \in A$ and $\{1, 2\} \in A$, since 1 is the first element in our listing of A and $\{1, 2\}$ is the third. While $\{2\} \in A$ (look for it in the list), $2 \notin A$ (it's not in the list). Here 2 and $\{2\}$ are very different objects. We can also say that $\{1, \{2\}\} \subset A$, because each element of $\{1, \{2\}\}$ (namely 1 and $\{2\}$) is also an element of A. On the other hand, $\{1, 2\} \not\subset A$, because $2 \notin A$.

The formula $A = B$ is read "A equals B." We are not monkeying with the meaning of equality here. That is, equality is assumed to be the familiar relationship satisfying the axioms of E. In particular, substitutivity of equality holds, so $A = B$ implies $\forall t(t \in A \leftrightarrow t \in B)$. Furthermore, we will adopt the following axiom asserting the converse of the preceding implication.

Axiom of Extensionality: For all sets A and B, if A and B have the same elements, then $A = B$. Formally, $\forall t(t \in A \leftrightarrow t \in B) \to A = B$.

We can use the axiom of extensionality as a blueprint for proofs involving equality. The proof of the next theorem illustrates this and also provides us with new tools for dealing with set equality.

Theorem 47. $A = B$ if and only if both $A \subset B$ and $B \subset A$.

Proof. First, suppose $A = B$. By substitutivity of equality, $\forall t(t \in A \leftrightarrow t \in B)$. Thus $\forall t(t \in A \rightarrow t \in B)$, so $A \subset B$. Similarly, $B \subset A$. Summarizing, we have shown that $A = B$ implies $A \subset B \wedge B \subset A$.

Now suppose that $A \subset B \wedge B \subset A$. Fix t. Since $A \subset B$, we know that $t \in A \rightarrow t \in B$. Since $B \subset A$, we know that $t \in B \rightarrow t \in A$. Thus, $\forall t(t \in A \leftrightarrow t \in B)$. By the Axiom of Extensionality, $A = B$. Summarizing, we have shown that $A \subset B \wedge B \subset A$ implies $A = B$. □

We have one last bit of notation to introduce in this section. The set containing no elements is called the empty set, and is denoted by $\emptyset$. We have an axiom that says exactly this.

Empty Set Axiom: The empty set contains no elements. Formally, $\forall t(t \notin \emptyset)$.

Here are three little brain teasers involving the empty set.

Theorem 48. For every set A, $\emptyset \subset A$.

Proof. Fix t. Since $t \notin \emptyset$, we know that $t \in \emptyset \rightarrow t \in A$. Thus, $\forall t(t \in \emptyset \rightarrow t \in A)$, which is the definition of $\emptyset \subset A$. □

Theorem 49. $\emptyset \neq \{\emptyset\}$.

Proof. Note that $\emptyset \in \{\emptyset\}$, but by the Empty Set Axiom, $\emptyset \notin \emptyset$. Thus $\emptyset$ and $\{\emptyset\}$ don't have the same elements, so by the contrapositive of substitutivity of equality, they are not equal. □

The method used in proof of Theorem 49 is useful in many situations. By substitutivity of equality, $A = B$ implies $\forall t(t \in A \leftrightarrow t \in B)$. The contrapositive of this is that $\neg\forall t(t \in A \leftrightarrow t \in B)$ implies $A \neq B$. Of course, the formula $\neg\forall t(t \in A \leftrightarrow t \in B)$ is equivalent to $\exists t(t \in A \not\leftrightarrow t \in B)$, which is the same as saying that there is a t such that t is in one of the sets but not the other. Summarizing, to prove that two sets are not equal, we just need to find one element that is in one of the sets but not in the other.

Theorem 50. $\emptyset$ is unique. That is, for any set A, if $\forall t(t \notin A)$, then $A = \emptyset$.

Proof. If $\forall t(t \notin A)$, then $\forall t(t \in A \leftrightarrow t \in \emptyset)$. By the Axiom of Extensionality, $A = \emptyset$. □

Exercises.

1. Prove: For all A and B, if $A \subsetneq B$ then $B \neq \emptyset$. (Hint: $A \subsetneq B$ means that $A \subset B$ and $A \neq B$. In light of the Axiom of Extensionality, what does $A \neq B$ imply?)

2. Prove: For all A and B, if $A \subset \emptyset$ then $A = \emptyset$.

3. The subset relation is almost, but not quite, an equivalence relation. The three parts of this exercise fill in the details.

   (a) Prove that $\subset$ is a reflexive relation. (That is, show that for all A, $A \subset A$.)

   (b) Prove that $\subset$ is a transitive relation. (That is, show that if $A \subset B$ and $B \subset C$, then $A \subset C$, for all A, B, and C.)

   (c) Prove that $\subset$ is not a symmetric relation. (That is, show that it is not the case that for all sets A and B, if $A \subset B$ then $B \subset A$. Your proof should consist of two concrete sets that violate symmetry.)

5.2 Operators on sets

In this section, we will explore the set theoretic operations of union, intersection and power set. Union and intersection can be treated as the familiar operations on two sets, or they can be generalized to operations on many sets. These generalized forms are frequently useful in the study of algebra and analysis. We will start with the binary union operator.

Definition. The *union* of two sets consists of all the elements that are in either set (or both). More formally, $A \cup B = \{x \mid x \in A \vee x \in B\}$. This is the union operator that you probably saw the first time you learned any set theory.

Example. The binary union operator is the one that you probably saw the first time you learned any set theory. If $A = \{0, 2\}$ and $B = \{2, 3, 4\}$, then $A \cup B = \{0, 2, 3, 4\}$.

Definition. The *union* of a collection of sets consists of all the elements that are in at least one of the sets in the collection. More formally, if I is a set of sets, then $\cup I = \{x \mid \exists y(y \in I \wedge x \in y)\}$.

Example. We can rewrite the previous example using the unary union operator. If $A = \{0, 2\}$ and $B = \{2, 3, 4\}$ and $I = \{A, B\}$, then $\cup I = A \cup B = \{0, 2, 3, 4\}$.

The unary union operator can be used to find the union of one set. The set $\cup\{A\}$ consists of all those those x such that there is a $y \in \{A\}$ such that $x \in y$. Since the only y satisfying $y \in \{A\}$ is A itself, $\cup\{A\}$ consists of all those x such that $x \in A$. That is, $\cup\{A\} = A$. One slick way to think about this is to

write $\cup\{A\} = A \cup A = A$. Repeating the A in the middle expression is perfectly acceptable here.

The unary operator can also be used to find the union of zero sets. The set $\cup\emptyset$ consists of all those x such that there is a $y \in \emptyset$ such that $x \in y$. Since there is no $y \in \emptyset$, no x can satisfy these requirements. Consequently, $\cup\emptyset = \emptyset$. You might think that as in the previous paragraph, we could just write $\cup\emptyset = \emptyset \cup \emptyset = \emptyset$. These equations are true, but highly misleading. If we really imitate the preceding paragraph, we would write $\cup\{\emptyset\} = \emptyset \cup \emptyset = \emptyset$. (Note the change in the first in the first term.) Since we know that $\cup\emptyset$ is also empty, we have $\cup\{\emptyset\} = \cup\emptyset$. In general, for a set A, the union $\cup\{A\}$ may or may not be A. For more on this, see exercise 13.

The big advantage of the unary union operator is that it allows us to avoid dots. Given a sequence of sets $A_1, A_2, A_3, \ldots$, we could write the union of all these sets as either $A_1 \cup A_2 \cup A_3 \cup \ldots$ (using binary union and nasty dots) or as $\cup\{A_i \mid i \in \mathbb{N}\}$ (using the more elegant unary union). The two notations describe the same set, but the one without dots relies less on our intuitive understanding of the underlying pattern in the sequence of sets.

Example. For each $n \in \mathbb{N}$, define $Z_n = \{i \in \mathbb{Z} \mid -n \leq i \leq n\}$. For example, $Z_0 = \{0\}$, $Z_1 = \{-1, 0, 1\}$, $Z_2 = \{-2, -1, 0, 1, 2\}$, and so on. We'll call each Z_n a *balanced interval*, and let $B = \{Z_n \mid n \in \mathbb{N}\}$ be the set of all balanced intervals. Note that B is a set of sets of integers, so it makes sense to take its union.

Theorem. $\cup B = \mathbb{Z}$.

Proof. To prove the equality, we'll prove containment in each direction. First, suppose $j \in \cup B$. Then for some $n \in \mathbb{N}$, $j \in Z_n$. Since $Z_n \subset \mathbb{Z}$, we must have $j \in \mathbb{Z}$. Summarizing, we have shown that $\cup B \subset \mathbb{Z}$. To complete the proof, suppose $k \in \mathbb{Z}$. Since $-|k| \leq k \leq |k|$, we know that $k \in Z_{|k|}$. Since $Z_{|k|} \in B$, we must have $k \in \cup B$. Consequently $\mathbb{Z} \subset \cup S$. By Theorem 47, the claim holds. □

The intersection symbol can also be used as either the traditional binary operator or as a unary operator. The following definitions and examples closely parallel those for unions

Definition. The intersection of two sets consists of all the elements that are in both sets. More formally, $A \cap B = \{x \mid x \in A \wedge x \in B\}$.

Example. With this intersection symbol, we are back to something you probably saw a long time ago. If $A = \{0, 2\}$ and $B = \{2, 3, 4\}$, then $A \cap B = \{2\}$.

Definition. The intersection of a nonempty collection of sets consists of all the elements that are in every one of the sets in the collection. More formally, if I is a set of sets, then $\cap I = \{x \mid \forall y(y \in I \rightarrow x \in y)\}$.

Example. We can rewrite the preceding example using the unary notation. If $A = \{0, 2\}$ and $B = \{2, 3, 4\}$ and $I = \{A, B\}$, then $\cap I = A \cap B = \{2\}$.

We can use the unary notation to take the intersection of one set. The intersection $\cap\{A\}$ consists of all those elements x that are elements of every $y \in \{A\}$. Since the only y in $\{A\}$ is A itself, this simplifies to the collection of those elements x that are in A. Thus $\cap\{A\} = A$. As we did with union, we could write $\cap\{A\} = A \cap A = A$.

The definition of the unary intersection specifies that the collection of sets that we are intersecting is nonempty. Consequently, we can't take the intersection of zero sets. This turns out to be a good thing. Suppose we think of V as being the collection of all those elements x such that $\forall y(y \in \emptyset \to x \in y)$. Since $y \in \emptyset$ is false for every y, the implication $y \in \emptyset \to x \in y$ is true, regardless of the choice of x and y. Consequently, V would contain every set x and be a so-called "universal set." Axiomatic set theory denies the existence of a universal set in order to avoid a paradox. We should follow suit, avoid universal sets, and avoid trying to find the intersection of zero sets.

As with the unary union operator, the unary intersection operator really shines when we want to take intersections of large collections of sets. As an example, we will return to our consideration of balanced intervals.

Example. Let B be the set of balanced intervals in $\mathbb{Z}$ used in the example for unions.

Theorem. $\cap B = \{0\}$.

Proof. To prove the equality, we'll prove containment in each direction. First suppose that $t \in \cap B$. Then for every $Z_n \in B$, t must be an element of Z_n. In particular, $t \in Z_0 = \{0\}$. Thus $t = 0$, and so t is an element of the set on the right side of the equality. To prove the reverse containment, suppose t is an element of the set on the right side of the equality. Clearly, $t = 0$. For every $n \in \mathbb{N}$, we know $-n \leq 0 \leq n$, so $0 \in Z_n$. Since $0 \in Z_n$ for every $Z_n \in B$, we have $0 \in \cap B$. Since $t = 0$, we also have $t \in \cap B$. □

There are some very nice connections between union and intersection. For example, the binary operators differ only in their logical operator. Compare these equations:

$$A \cup B = \{x \mid x \in A \vee x \in B\}$$
$$A \cap B = \{x \mid x \in A \wedge x \in B\}$$

The unary operators have a similar connection. This is especially notable if we switch to bounded quantifier notation.

$$\cup I = \{x \mid \exists y(y \in I \wedge x \in y)\} = \{x \mid \exists y \in I(x \in y)\}$$

$$\cap I = \{x \mid \forall y(y \in I \to x \in y)\} = \{x \mid \forall y \in I(x \in y)\}$$

The ZF set theory axioms include a Union Axiom which asserts the existence of unions. There is no axiom in ZF for intersections, nor is there technically a function symbol for intersection. The Axiom of Separability can be used to prove the existence of intersections. As we noted before, ZF denies the existence of $\cap\emptyset$. In particular, the existence of a universal set violates the Axiom of Regularity.

We complete this section with one more unary set operator. Here is the definition followed by two short examples.

Definition. The *power set* of a set X is denoted by $\mathcal{P}(X)$ and is the set of all subsets of X. Formally, $\mathcal{P}(X) = \{y \mid y \subset X\}$.

Example. If $A = \{0, 2\}$, then $\mathcal{P}(A) = \{\emptyset, \{0\}, \{2\}, \{0, 2\}\}$. It is not too hard to show that if X has n elements, then $\mathcal{P}(X)$ has 2^n elements. We are lucky that A was a pretty small set.

Example. Suppose B is the set of balanced intervals from $\mathbb{Z}$ as described earlier.

Theorem. $B \subsetneq \mathcal{P}(\mathbb{Z})$.

Proof. For each n, $Z_n \in \mathcal{P}(\mathbb{Z})$, so $B \subset \mathcal{P}(\mathbb{Z})$. Additionally, $\{0, 3, 5\} \subset \mathbb{Z}$ and $\{0, 3, 5\} \notin B$, so $B \neq \mathcal{P}(\mathbb{Z})$. □

Exercises.

1. Prove: For all A, B, and C, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
2. Prove: For all sets A, $\forall t(t \in A \to t \subset \cup A)$.
3. Suppose that for all $n \in \mathbb{N}$, $X_n = \{n, n + 1, n + 2, \dots\}$. Let $A = \{X_n \mid n \in \mathbb{N}\}$.
   (a) Find $\cup A$.
   (b) Find $\cap A$.
4. Prove: For all A, B, and C, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
5. Prove: For all sets A, $\forall t(t \in A \to \cap A \subset t)$.
6. Prove: $\forall X(\cup \mathcal{P}(X) = X)$.
7. (a) Prove if $\emptyset \in A$ then $\cap A = \emptyset$.
   (b) Prove $\forall X(\cap \mathcal{P}(X) = \emptyset)$.
8. Prove: $\forall X(X \subset \mathcal{P}(\cup X))$.
9. Find a set X such that $X = \mathcal{P}(\cup X)$.
10. Find $\mathcal{P}(\emptyset)$.
11. Prove that $\cup \emptyset = \emptyset$.
12. Find the following sets: $\mathcal{P}(\emptyset)$, $\mathcal{P}(\mathcal{P}(\emptyset))$, $\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset)))$
13. A set S is called *transitive* if $\forall x \forall y((x \in y \wedge y \in S) \to x \in S)$. (So S is transitive if $\in$ is a transitive relation on the elements of S.)
    (a) Prove that S is transitive if and only if $\cup S \subset S$.

(b) Prove that $\emptyset$ is transitive. (Hint: You could use the definition or part 13a.)

(c) Prove that $\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \dots\}$ is transitive.

(d) Prove that $\{\emptyset, \{\{\emptyset\}\}\}$ is not transitive.

5.3 Cartesian products and functions

The notation (a, b) is used to denote an *ordered pair* of objects. We say that $(a, b) = (x, y)$ if and only if $a = x$ and $b = y$. Note that ordered pairs are different from sets with two elements. While $\{0, 1\} = \{1, 0\}$ because the sets have the same elements, $(0, 1) \neq (1, 0)$ because the first components don't match. In axiomatic set theory, ordered pairs are encoded by sets. For more about this, see exercise 4.

Sets of ordered pairs are used to represent a myriad of constructs in mathematics. We can think of the points in the real plane as a set of ordered pairs of coordinates. We can also view the graph of a function or even the function itself as a set ordered pairs.

Definition. If X and Y are sets, then the *cartesian product* $X \times Y$ is the set of all ordered pairs with a first coordinate from X and a second component from Y. More formally, $X \times Y = \{(x, y) \mid x \in X \wedge y \in Y\}$.

Definition. We say a set f of ordered pairs is *single-valued* if and only if

$$\forall x \forall y_1 \forall y_2 (((x, y_1) \in f \wedge (x, y_2) \in f) \rightarrow y_1 = y_2).$$

A *function* is a set of ordered pairs that is single valued. Rather than writing $(x, y) \in f$, we often use the convenient abbreviation $f(x) = y$.

Requiring f to be single-valued insures that the equality in the abbreviation is transitive, as we would expect. In particular, if $f(x) = y_1$ and $f(x) = y_2$, then $y_1 = y_2$ holds. For any function f from $\mathbb{R}$ to $\mathbb{R}$, the fact that f is single-valued is equivalent to saying that every vertical line in the plane hits the graph of f in at most one point. So for functions on the reals, the preceding definition says "functions must satisfy the vertical line test." On the other hand, for functions of other sorts, the vertical line test makes less sense. For functions that are (for example) linear transformations on $\mathbb{R}^3$, or complex valued holomorphisms, or automorphisms on finite groups, the idea of a "vertical line" doesn't make a lick of sense. However, we can certainly talk about all these functions being single-valued.

Example. Consider the set $F = \{(0, 1), (1, 2), (2, 1)\}$. Since each first coordinate appears in only one ordered pair, F is a function. Because $(0, 1) \in F$, we can write $F(0) = 1$. Similarly we can write $F(1) = 2$ and $F(2) = 1$. If you plot the three pairs in F as points in the real plane, you will see that they satisfy the vertical line test.

Example. Consider $X = \{(1,0),(2,1),(1,2)\}$. X is not a function, because $(1,0)$ and $(1,2)$ witness that X is not single-valued. These pairs indicate that $X(1) = 0$ and $X(1) = 2$, and that would cause problems. As in the previous example, you could draw a picture here to illustrate the situation.

Example. Consider $Y = \{(a,b),(b,c),(a,c)\}$, where none of the letters are equal. Since this is practically identical to the preceding example, Y is not a function. We can demonstrate this by just pointing out that $Y(a) = b$ and $Y(a) = c$, so Y is not single-valued. Since we're not dealing with numbers here, drawing a picture would require making some assumptions about a, b, and c. Unless we identify the letters with numbers, the "vertical line test" doesn't make much sense.

Example. Suppose $S = \{(x, x^2) \mid x \in \mathbb{R}\}$. S is the familiar squaring function on the real numbers, often described using the equation $S(x) = x^2$.

Example. Consider $T = \{(x^2, x) \mid x \in \mathbb{R}\}$. Since $(1,-1)$ and $(1,1)$ are both elements of T, T is not single-valued. Because we are working in the reals, we could say that T fails the vertical line test.

When we think of functions as sets of ordered pairs, the concepts of domain and range become completely transparent. Consider the following definition.

Definition. If f is a function, the *domain* of f is defined by the equation

$$\mathsf{dom}(f) = \{x \mid \exists y (x,y) \in f\}.$$

The *range* of f is defined by the equation

$$\mathsf{ran}(f) = \{y \mid \exists x (x,y) \in f\}.$$

If X is the domain of f and Y is any set containing the range of f, then we often write $f : X \to Y$, which is read "f maps X to Y." In this case, the set Y is referred to as the *codomain* of f.

Example. If $S = \{(x, x^2) \mid x \in \mathbb{R}\}$, then $\mathsf{dom}(S) = \mathbb{R}$, and $\mathsf{ran}(S) = \{y \in \mathbb{R} \mid y \geq 0\}$. We could write $S : \mathbb{R} \to \mathbb{R}$. Note that in this case, the indicated codomain is $\mathbb{R}$ even though the range is a smaller set.

Notation alert: Consider the familiar square root function on the real numbers. We can defined it by $g = \{(x, \sqrt{x}) \mid x \in \mathbb{R} \wedge x \geq 0\}$. If we're working on the reals, then the square root is not defined on negative numbers and so $\mathsf{dom}(g) = \{x \in \mathbb{R} \mid x \geq 0\}$. Despite this, it is not too unusual to see someone write

$$g : \mathbb{R} \to \mathbb{R} \text{ is defined by } g(x) = \sqrt{x}$$

and claim that the *implicit domain* is $\mathsf{dom}(g) = \{x \in \mathbb{R} \mid x \geq 0\}$. In other words, figuring out the actual domain and the precise definition of the function is left up to the reader. Referring to this as sloppy writing will not win you any

friends, but it is perfectly reasonable to politely ask for clarification when you see it.

Using ordered pairs to define functions also cleans up the notion of what it means for functions to be onto and/or one to one. The relevant definitions and some examples follow.

Definition. If $f : X \to Y$ (where $\mathsf{dom}(f) = X$ and Y is a codomain of f), and $T \subset Y$, we say f *maps* X *onto* T if $\mathsf{ran}(f) = T$.

Note: To prove that $\mathsf{ran}(f) = T$, we could prove containment both directions. In practice, one direction is almost always given to us. See the next example.

Example. Suppose $S : \mathbb{R} \to [0, \infty)$ is defined by $S(x) = x^2$. Prove that S maps $\mathbb{R}$ onto $[0, \infty)$. (Here $[0, \infty)$ is the interval notation for the set $\{y \in \mathbb{R} \mid y \geq 0\}$.)

Proof. Since $[0, \infty)$ is the codomain of S, we know $\mathsf{ran}(S) \subset [0, \infty)$. It remains to show the opposite containment. Suppose $t \in [0, \infty)$. Then $\sqrt{t}$ is a well-defined real number . Since

$$S(\sqrt{t}) = (\sqrt{t})^2 = t,$$

$t \in \mathsf{ran}(S)$. Thus $t \in [0, \infty)$ implies $t \in \mathsf{ran}(S)$, and so $[0, \infty) \subset \mathsf{ran}(S)$. By Theorem 1, $\mathsf{ran}(S) = [0, \infty)$, so S maps $\mathbb{R}$ onto $[0, \infty)$. □

Definition. Suppose $f : X \to Y$. We say f is one to one (also written 1–1) when no two distinct range elements are mapped to the same range element. More formally, f is one to one means

$$\forall x_1 \forall x_2 (x_1 \neq x_2 \to f(x_1) \neq f(x_2)).$$

Any one to one function from a set X into a set Y matches each element of X with a unique partner in Y. When we match students with student identifier numbers, or match books with call numbers, or give everyone an individual bag of chips for their lunch, we are implementing one to one functions. In applying the definition, generally it is easiest to prove the contrapositive of the implication. In practice, to prove that f is one to one, we usually prove

$$\forall x_1 \forall x_2 (f(x_1) = f(x_2) \to x_1 = x_2)$$

Example. Consider $f : [0, \infty) \to \mathbb{R}$ defined by $f(x) = \sqrt{x}$. Prove that f is one to one.

Proof. Suppose x_1 and x_2 are elements of $[0, \infty)$ such that $f(x_1) = f(x_2)$. By the definition of f, $\sqrt{x_1} = \sqrt{x_2}$. Squaring both sides of the equation shows that $x_1 = \pm x_2$. Since x_1 and x_2 are both nonnegative, $x_1 = x_2$. □

Example. Consider $S : \mathbb{R} \to [0, \infty)$ defined by $S(x) = x^2$. Show that S is not one to one.

Proof. Note that $S(-1) = 1 = S(1)$. Thus S is not one to one. □

Concrete constructions (like the one in the preceding example) are the best possible approach to proving many existential statements. It is much better to write $S(-1) = 1 = S(1)$ rather than $S(-x) = x^2 = S(x)$, because when $x = 0$, $S(-0) = 0^2 = S(0)$ fails to show that S is not one to one.

The definitions of one to one functions and single-valued are sufficiently similar to cause some confusion. When you write them next to each other, they look very different:

f is one to one: $\forall x_1 \forall x_2 \forall y((f(x_1) = y \wedge f(x_2) = y) \rightarrow x_1 = x_2)$

f is single-valued: $\forall x\ \forall y_1 \forall y_2((f(x) = y_1 \wedge f(x) = y_2) \rightarrow y_1 = y_2)$

We have slightly modified the formula for one to one here, but this version is equivalent to the one above. Note that the definition of one to one has two xs and one y, while the definition of single-valued has one x and two ys. A relation (from $\mathbb{R}$ to $\mathbb{R}$) that is not single-valued fails the vertical line test, while a function that is not one to one fails a horizontal line test.

Exercises

The following problems use these sets of ordered pairs:

$f = \{(n, n^2) \mid n \in \mathbb{N}\}$

$g = \{(x, x^2) \mid x \in \mathbb{Z}\}$

$h = \{(x^2, x) \mid x \in \mathbb{Z}\}$

$r = \{(n, n + 3) \mid n \in \mathbb{N}\}$

$s = \{(x, x + 3) \mid x \in \mathbb{Z}\}$

1. (a) Prove that f is single-valued.
   (b) Prove that h is not single-valued. (Use a concrete example.)
2. (a) Prove that f is one to one.
   (b) Prove that g is not one to one. (Use a concrete example.)
3. Both r and s are functions.
   (a) Find the domain and range of r.
   (b) Is r one to one and onto $\mathbb{N}$? Justify your answer.
   (c) Find the domain and range of s.
   (d) Is s one to one and onto $\mathbb{Z}$? Justify your answer.
4. In axiomatic set theory, we encode ordered pairs by sets. This amounts to asserting that the ordered pair notation is just a shorthand for a particular set. An encoding suggest by Kuratowski [7] is $(a, b) = \{\{a, b\}, a\}$.
   (a) Using Kuratowski's encoding and the Axiom of Extensionality, prove that $(a, b) = (c, d)$ if and only if $a = c$ and $b = d$. (That is, show that the set encoding (a, b) has exactly the same elements as the set encoding (c, d) if and only if $a = c$ and $b = d$.)

(b) Using Kuratowski's encoding, prove that $X \times Y \subset \mathcal{P}(X \cup \mathcal{P}(X \cup Y))$.

5. The Axiom of Regularity implies that $\forall x(x \notin x)$. Show that the Axiom of Regularity implies that no set with exactly one element can represent an ordered pair in the Kuratowski encoding.

6. Find an example of sets a, b, c, and d such that $\{\{a\}, b\} = \{\{c\}, d\}$ but it is not the case that $a = b$ and $c = d$. (This shows that $(a, b) = \{\{a\}, b\}$ doesn't work as an encoding of ordered pairs.)

5.4 Inverse functions, images, and pre-images

In this section, we will use our set theoretic representation of functions to explore the the concept of inverse functions. We start with a traditional definition of an inverse function and a couple of examples.

Definition. Suppose that f is a function with $\mathsf{dom}(f) = X$ and $\mathsf{ran}(f) = Y$. We say that the function $g : Y \to X$ is the *inverse of* f and write $g = f^{-1}$ provided that the following hold:

$$\forall x \in X(g(f(x)) = x) \quad \text{and} \quad \forall y \in Y(f(g(y)) = y).$$

It is easy to see that this definition is symmetric. That is, $f = g^{-1}$ if and only if $g = f^{-1}$. It is also possible to prove that if f has an inverse, then that inverse is unique. See exercise 1.

Example. Let $\mathbb{R}^+ = \{x \in \mathbb{R} \mid x \geq 0\}$ and consider the function $f : \mathbb{R}^+ \to \mathbb{R}^+$ defined by $f(x) = x^2$. Let $g : \mathbb{R}^+ \to \mathbb{R}^+$ be defined by $g(x) = \sqrt{x}$. (Note that $\sqrt{x}$ is the positive square root of x.) We claim that $g = f^{-1}$. This is verified by the following sequences of equalities, which hold for all x and y in $\mathbb{R}^+$.

$$g(f(x)) = g(x^2) = \sqrt{x^2} = |x| = x$$

$$f(g(y)) = f(\sqrt{y}) = (\sqrt{y})^2 = y$$

Example. Suppose $f : \mathbb{R} \to \mathbb{R}^+$ is defined by $f(x) = x^2$, and $g : \mathbb{R}^+ \to \mathbb{R}$ is defined by $g(x) = \sqrt{x}$. Since

$$g(f(-1)) = g((-1)^2) = g(1) = \sqrt{1} = 1,$$

$g(f(-1)) \neq -1$, so g is not f^{-1}. If we redefined g as the negative square root, $g(f(1))$ would not equal 1, so we still would not have an inverse. Indeed, the fact that $f(1) = 1 = f(-1)$ bars us from being able to find an inverse for $f(x) = x^2$ on this domain.

The preceding example has two morals. First, domains matter in finding inverses. Second, functions that are not one to one don't have inverses. Maybe we should stir in some set theory. If we think of the function f as a set of ordered pairs, we can build a new set g by flipping the order of all the pairs. If this new set is a function, then it ought to be the inverse of f. Our second moral gives us an indication of when the flipped set is a function. The next theorem says that this is a very good indication indeed.

Theorem 51. Suppose that f is a function with $\mathsf{dom}(f) = X$ and $\mathsf{ran}(f) = Y$. Define $g = \{(y, x) \mid (x, y) \in f\}$. Then g is a function if and only if f is one to one.

Proof. Suppose that f and g are as in the theorem. Then f is not one to one if and only if there are values x_1 and x_2 in X such that $x_1 \neq x_2$ and $f(x_1) = f(x_2)$. This holds if and only if there is a $y \in Y$ such that $x_1 \neq x_2$, $(x_1, y) \in f$, and $(x_2, y) \in f$. By the definition of g, this is equivalent to $x_1 \neq x_2$, $(y, x_1) \in g$, and $(y, x_2) \in g$. But this is equivalent to asserting that g is not single-valued, i.e. that g is not a function. □

Before the last theorem, we said that the flipped set should be the inverse function, provided that it is a function at all. We still need to prove that.

Theorem 52. Suppose f is a function. Define $g = \{(y, x) \mid (x, y) \in f\}$. Then g is a function if and only if $g = f^{-1}$.

Proof. Suppose f is a function with with $\mathsf{dom}(f) = X$ and $\mathsf{ran}(f) = Y$. Also suppose g is the set of pairs defined above. If g is the inverse function of f, then g is certainly a function. Consequently, we need only prove the converse. Suppose g is a function. Note that $(x, y) \in f$ if and only if $(y, x) \in g$. In function notation, this means $f(x) = y$ if and only if $g(y) = x$. First, suppose $x \in X$ and $f(x) = y$. Then $g(f(x)) = g(y) = x$. Similarly, if $y \in Y$ and $g(y) = x$, then $f(g(y)) = f(x) = y$. Summarizing, g is the inverse of f. □

Sometimes we want to apply a function to every element of a set. As a slick shorthand, rather than writing $\{f(x) \mid x \in X\}$, we can just write $f(X)$. People also have a shorthand for all the elements that f maps into a set. Here are both of these shorthand notations in one definition.

Definition. Suppose $f : X \to Y$ is a function. If $U \subset X$, the image of U under f is defined by $f(U) = \{f(x) \mid x \in U\}$. If $V \subset \mathsf{ran}(f)$, then the pre-image of V under f is defined by $f^{-1}(V) = \{x \in X \mid f(x) \in V\}$.

Notation alert: The pre-image of a set under f is often defined even when the inverse function f^{-1} does not exist. Consequently, $f^{-1}(V)$ (for a set V) may denote a perfectly well defined set even when $f^{-1}(y)$ (for an element y of $\mathsf{ran}(f)$) may be complete gibberish.

Example: Define the function $f : \{0, 1, 2, 3\} \to \{a, b, c\}$ by the set of ordered pairs $f = \{(0, a), (1, c), (2, c), (3, b)\}$. So $f(0) = a$, $f(1) = c$, and so on. Then

$$f(\{0, 1\}) = \{f(0), f(1)\} = \{a, c\}$$

and

$$f^{-1}(\{b, c\}) = \{x \mid f(x) \in \{b, c\}\} = \{x \mid f(x) = b \ \vee \ f(x) = c\} = \{1, 2, 3\}.$$

Exercises

1. Prove that if an inverse exists for a function, it must be unique.
2. Suppose $f : \mathbb{Z} \to \mathbb{Z}$ is defined by $f(x) = 3x + 2$.
   (a) Prove that f is one to one.
   (b) Prove that f does not map $\mathbb{Z}$ onto $\mathbb{Z}$.
   (c) Find a formula for f^{-1}, the inverse of f. Your formula should be of the form $f^{-1}(x) =$ *some algebraic expression involving* x.
   (d) Find the domain of f^{-1}.
3. Prove that if f is a function and $U \subset \mathsf{dom}(f)$, then $f^{-1}(f(U)) \supset U$. (Note that f^{-1} is denoting a pre-image in this problem, not an inverse function.)
4. Show that in problem 3, we can't replace the subset symbol by equality. Do this by giving an example of a function f and a set $U \subset \mathsf{dom}(f)$ for which $f^{-1}(f(U)) \supsetneq U$.
5. Prove that if f is a function and $V \subset \mathsf{ran}(f)$, then $f(f^{-1}(V)) = V$.

5.5 Sizes of sets

Consider the following tables, which define the functions f and g.

x	1	2	5	7
$f(x)$	t	a	r	e

x	1	2	5
$g(x)$	t	a	r

Note that the function f is one to one and maps the set $\{1, 2, 5, 7\}$ onto the set $\{t, a, r, e\}$. So f matches each element of $\{1, 2, 5, 7\}$ with an element of $\{t, a, r, e\}$. As a consequence of this, it is reasonable to conclude that the set $\{1, 2, 5, 7\}$ is the same size as the set $\{t, a, r, e\}$.

Why bother with f? Each of these sets contains four elements, so of course they are the same size. Note that in counting the elements, we actually match each element with one of the numbers 1, 2, 3, and 4. Consequently, as we count the elements in each set, we are actually defining a one to one and onto map between the set and $\{1, 2, 3, 4\}$. When we count the elements in the two sets, we are actually constructing two functions. If we compose one of those functions with the inverse of the other, we get a one to one function mapping one of the sets onto the other. In some sense, counting the elements is just a process for constructing a function like f.

Now g witnesses that the sets $\{1, 2, 5\}$ and $\{t, a, r\}$ are the same size. Since g can also be viewed as a one to one map from $\{1, 2, 5\}$ into $\{t, a, r, e\}$, this also shows us that the set $\{t, a, r, e\}$ is at least as big as the set $\{1, 2, 5\}$. Note that

in the previous sentence, when we expand the codomain of g, we get a function *into* $\{t, a, r, e\}$, not *onto* $\{t, a, r, e\}$.

The next definition sets up some nice shorthand notation for this notion of size of sets.

Definition. Let A and B be sets. If there is a one to one function from A into B, we say that B is at least as big as A, and write $A \preccurlyeq B$ (or $B \succcurlyeq A$). If there is a one to one function from A onto B, then we say that A and B are the same size, and write $A \sim B$.

The really beautiful thing about this definition is that it allows us to compare the sizes of infinite sets. Here are two examples.

Theorem 53. $\mathbb{N} \preccurlyeq \mathbb{Z}$, that is, the integers are at least as big as the natural numbers.

Proof. The function $f : \mathbb{N} \to \mathbb{Z}$ defined by the equation $f(n) = n$ is a one to one map of $\mathbb{N}$ into $\mathbb{Z}$. Verification that this function is one to one is left as an easy exercise. □

Theorem 54. $\mathbb{N} \sim \mathbb{Z}$, that is, the integers and the natural numbers are the same size.

Proof. The function $g : \mathbb{N} \to \mathbb{Z}$ defined by the formula below is a one to one map of $\mathbb{N}$ onto $\mathbb{Z}$.

$$g(n) = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even} \\ -\frac{n+1}{2} & \text{if } n \text{ is odd} \end{cases}$$

Verification that this function is one to one and onto is left as an exercise. □

Sometimes cooking up these one to one and onto functions is quite challenging. The next theorem provides perhaps one of the most useful shortcuts in the set theory literature. Unfortunately, the proof of this theorem is beyond the scope of this book, but you can find a proof in [3], if you are interested.

Theorem 55 (Cantor-Berstein Theorem)**.** If $A \preccurlyeq B$ and $B \preccurlyeq A$, then $A \sim B$.

Although the Cantor-Berstein Theorem looks like a trivial statement about inequalities, the notation is hiding its remarkable power. It really says that there is some systematic method for converting a pair of one to one functions into a single function that is one to one and onto. Very handy indeed. Here is an example.

Alternate proof of Theorem 54. The function $f : \mathbb{N} \to \mathbb{Z}$ defined by the equation $f(n) = n$ is a one to one map of $\mathbb{N}$ into $\mathbb{Z}$. Let $h : \mathbb{Z} \to \mathbb{N}$ be the function defined by:

$$h(z) = \begin{cases} 2^z & \text{if } z \geq 0 \\ 3^{|z|} & \text{if } z < 0 \end{cases}$$

Then h is a one to one map of $\mathbb{Z}$ into $\mathbb{N}$. By the Cantor-Berstein Theorem, $\mathbb{N} \sim \mathbb{Z}$. □

So far, all the infinite sets that we have examined were the same size. This is a complete fluke. In the case of finite sets, the power set of a set is always larger than the original set. Cantor proved that this is true for infinite sets, too! If we write $X \prec Y$ for $(X \preccurlyeq Y \wedge X \not\sim Y)$, we can state the next theorem very elegantly.

Theorem 56. $\forall X(X \prec \mathcal{P}(X))$. That is, for every set X, the power set of X is strictly larger than X.

Proof. Fix a set X. We need to show that $X \preccurlyeq \mathcal{P}(X) \wedge X \not\sim \mathcal{P}(X)$. To prove the first conjunct, note that the function $f : X \to \mathcal{P}(X)$ defined by $f(x) = \{x\}$ for each $x \in X$ is a one to one function.

It remains to show that $X \not\sim \mathcal{P}(X)$. Suppose that $g : X \to \mathcal{P}(X)$ is one to one. We will show that g cannot be onto. Let $y = \{t \in X \mid t \notin g(t)\}$. Note that $y \in \mathcal{P}(X)$. However, y cannot be in the range of g. To see this, suppose for a moment that there is some $x \in X$ such that $g(x) = y$. Then $x \in g(x)$ if and only if $x \in y$. By the definition of y, $x \in y$ if and only if $x \notin g(x)$. Concatenating the biconditionals, we have $x \in g(x)$ if and only if $x \notin g(x)$, a clear contradiction. Thus y is not in the range of g, and so g is not onto. Since g was an arbitrary one to one function, there can be no function mapping X into $\mathcal{P}(X)$ which is both one to one and onto. That is, $X \not\sim \mathcal{P}(X)$. □

If we plug the natural numbers in for X in the preceding theorem and then iterate this process, we get a nice chain of infinite sets of strictly increasing sizes.

$$\mathbb{N} \prec \mathcal{P}(\mathbb{N}) \prec \mathcal{P}(\mathcal{P}(\mathbb{N})) \prec \mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N}))) \prec \dots$$

We say that a set X is *countable* if $X \sim \mathbb{N}$. All the sets to the right of $\mathbb{N}$ in the list are *uncountable*. It is possible to prove that $\mathcal{P}(\mathbb{N}) \sim \mathbb{R}$, so the real numbers are uncountable. For details of that proof, see Corollary 3.23 in [3]. For a direct argument that $\mathbb{N} \not\sim \mathbb{R}$, see exercise 6. By contrast, Theorem 54 shows that the integers are countable and exercise 4 shows that the rationals are countable. Summarizing, there are infinitely many different sizes of infinite sets, and familiar infinite sets include both countable and uncountable examples.

Exercises

1. Give a proof that the function defined in the proof of Theorem 53 is one to one.

2. Give a detailed proof that the function defined in the first proof of Theorem 54 is indeed one to one and onto.

3. Give a detailed proof that the function h defined in the alternate proof of Theorem 54 (following the statement of the Cantor-Berstein theorem) is one to one.

4. Prove that the rationals are countable. (Hint: It is easiest to use the Cantor-Berstein Theorem to prove that $\mathbb{Q} \sim \mathbb{N}$.)

5. Prove that the function f in the proof of Theorem 56 is one to one.

6. Use a proof by contradiction to show that $\mathbb{N} \not\sim \mathbb{R}$. Assume that $\mathbb{N} \sim \mathbb{R}$ and so there a function f that maps $\mathbb{N}$ one to one onto $\mathbb{R}$. Describe a method of constructing a single real number r that differs from each $f(n)$ in the $n + 1^{\text{st}}$ decimal place. Since this real is not in the range of f, this contradicts the claim that f is onto.

5.6 Dangers of naïve set theory

Around 1901, Bertrand Russell asked the following question:

Let $X = \{t \mid t \notin t\}$. Is X an element of X?

There are two obvious responses: yes and no.

Suppose the answer is yes, so we think that X is an element of X. Formally, we have $X \in X$. Like all elements of X, the set X must satisfy the formula that defines X, so $X \notin X$. Summarizing, we have $X \in X$ and $X \notin X$. This is problematic.

No worries, we must have just guessed wrong. Suppose the answer is no, so we think that X is not an element of X. Formally, we have $X \notin X$. Thus, X is a set which satisfies the formula $t \notin t$. Consequently, $X \in X$. Summarizing, we have $X \notin X$ and $X \in X$. This is particularly problematic, since we just ran out of obvious responses.

Here's a not so obvious response to Russell's question. Before asking about whether X was an element of X, Russell said "Let $X = \{t \mid t \notin t\}$." How do we know that the set X exists? Maybe there is no set X such that $\forall t(t \in X \leftrightarrow t \notin t)$. Perhaps we should be a bit more careful about how we use set-builder notation.

The way logicians solved this problem was to write down a list of axioms describing the behavior of sets, with special attention to questions of existence. These axioms are called the Zermelo-Fraenkel axioms for set theory and are usually referred to as ZF.

The proper axioms of ZF are:

1. Axiom of Extensionality
2. Empty Set Axiom
3. Pairing Axiom
4. Union Axiom
5. Power Set Axiom
6. Separation Axiom
7. Infinity Axiom
8. Replacement Axiom

9. Regularity Axiom

Most people add the axiom of choice to this list, and work in ZFC.

As a general rule of thumb, as long as you stick to subsets of sets that you know already exist (e.g. sets of natural numbers or sets of continuous functions on the reals), you will (hopefully) never run into a Russell-style paradox. If you think you have, we would all like to hear about it.

Exercises

1. Prove that for all x, $\mathcal{P}(x) \not\subset x$. (Use a proof by contradiction. Suppose $\mathcal{P}(x) \subset x$ and define the set $U = \{t \in x \mid x \notin t\}$. Then U is a perfectly good subset of x, whose existence could be proved in ZF by means of the separation axiom. Consequently, either $x \in U$ or $x \notin U$. Show that neither possibility can hold.)

Bibliography

[1] Herbert B. Enderton, *A mathematical introduction to logic*, 2nd ed., Harcourt/Academic Press, Burlington, MA, 2001. MR **1801397 (2001h:**03001)

[2] Kurt Gödel, *Die Vollständigkeit der Axiome des logischen Funktionenkalküls*, Monatsh. Math. Phys. **37** (1930), no. 1, 349–360 (German). MR 1549799

[3] John M. Harris, Jeffry L. Hirst, and Michael J. Mossinghoff, *Combinatorics and graph theory*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 2000. MR 1770510

[4] Leon Henkin, *The completeness of the first-order functional calculus*, J. Symbolic Logic **14** (1949), 159–166. MR 0033781 (11,487d)

[5] László Kalmár, *Zurückführung des Entscheidungsproblems auf den Fall von Formeln mit einer einzigen, binären, Funktionsvariablen*, Compositio Math. **4** (1937), 137–144 (German). MR 1556967

[6] Stephen Cole Kleene, *Introduction to metamathematics*, D. Van Nostrand Co., Inc., New York, N. Y., 1952. MR 0051790 (14,525m)

[7] K. Kuratowski, *Sur la notion del l'ordre dans la théorie des ensembles*, Fund. Math. **2** (1921), 161-171.

[8] Elliott Mendelson, *Introduction to mathematical logic*, 4th ed., Chapman & Hall, London, 1997. MR **1630547 (99b:**03002)

[9] Carew A. Meredith, *Single axioms for the systems* (C, N), (C, O) *and* (A, N) *of the two-valued propositional calculus*, J. Computing Systems **1** (1953), 155–164. MR 0055953 (15,1b)

[10] Joseph R. Shoenfield, *Recursion theory*, Lecture Notes in Logic, vol. 1, Association for Symbolic Logic, Urbana, IL, 2001. Reprint of the 1993 original. MR **1813760 (2001m:**03078)

[11] Alfred Tarski, *Logic, semantics, metamathematics. Papers from 1923 to 1938*, Oxford at the Clarendon Press, 1956. Translated by J. H. Woodger. (For truth in models, especially see *Der Wahrheitsbegriff in den formalisierten Sprachen.*) MR 0078296 (17,1171a)

Index