CSCI 2300
Fall 2020
Lecture Notes

1 Propositional Logic

1.1 Syntax of propositional logic

Rosen and Zybooks use term *compound proposition* for an expression written using logic. I will use the more common term *propositional formula* instead.

The *syntax* of propositional logic only says what a propositional formula looks like. It does not say what a propositional formula means. We use A, B, C and ϕ (Greek phi) to name arbitrary propositional formulas.

Definition 1.1. A *propositional formula* is defined as follows.

1. Symbols **T** and **F** are propositional formulas.
2. A *propositional variable* is a propositional formula. We will use p, q, r and s, possibly with subscripts, as propositional variables and X for talking about an arbitrary variable.
3. If A and B are propositional formulas then so are
   (a) $A \vee B$,
   (b) $A \wedge B$,
   (c) $\neg A$,
   (d) (A).

For example, each of the following is a propositional formula.

- p
- $p \vee q$

- $p \wedge \neg q$
- $p \wedge q \wedge r$
- $q \vee p \wedge r$
- $(r \wedge \mathbf{T}) \vee \neg q$

Operator $\vee$ is read "or", $\wedge$ is read "and", and $\neg$ is read "not".

Rules of *precedence* and *associativity* determine how you break a propositional formula into subformulas. Higher precedence operators are done first. The following lists operators by precedence, from highest to lowest.

Precedence	
parentheses	high
$\neg$	
$\wedge$	
$\vee$	low

For example, $p \vee q \wedge r$ is understood to have the same structure as $p \vee (q \wedge r)$ since $\wedge$ has higher precedence than $\vee$.

Associativity determines how an expression is broken into subexpressions when it involves two or more occurrences of the same operator. We assume that operators $\vee$ and $\wedge$ are done from left to right. That is, they are *left-associative*. (Associativity is like the wind. A north wind blows from north to south.) For example, $p \vee q \vee r$ has the same structure as $(p \vee q) \vee r$. Associativity does not really matter for $\vee$ and $\wedge$ because they are *associative operators*. That is, $(p \vee q) \vee r$ always has the same meaning as $p \vee (q \vee r)$ and $(p \wedge q) \wedge r$ always has the same meaning as $p \wedge (q \wedge r)$. But associativity does matter for some operators, so it is wise to think about it.

1.2 Meaning of propositional logic

The meaning of a propositional formula can only be defined when the values of all of its variables are given. Each variable can be true or false.

Definition 1.2. A *truth-value assignment* is a set of components of the form $X = V$ where X is a variable and V is either T or F. For example, $\{p$=T, q=F$\}$ is a truth-value assignment. (Note that T and F are possible values of a propositional variable or a propositional formula. Do not confuse them with **T** and **F**, which are propositional formulas.)

Definition 1.3. If a is a truth-value assignment and X is a variable then $a(X)$ is the value (T or F) that a gives for variable X. For example, if a is $\{p$=T, q=F$\}$ then $a(p) =$ T and $a(q) =$ F.

Definition 1.4. Suppose that ϕ is a propositional formula and a is a truth-value assignment that defines every variable that occurs in ϕ. Notation $\phi : a$ indicates the value of ϕ (either T or F) when variables have values given by a. Specifically:

1. $(\mathbf{T} : a) =$ T. That is, symbol **T** is always true; it does not depend on a.
2. $(\mathbf{F} : a) =$ F. That is, symbol **F** is always false; it does not depend on a.
3. If X is a variable then $(X : a) = a(X)$. That is, X has the value that it is given by truth-value assignment a.
4. $(A \vee B : a)$ is T if at least one of $(A : a)$ and $(B : a)$ is T, and is F otherwise. For example, $((p \vee q) : \{p = \mathrm{T}, q = \mathrm{F}\})$ is T because $(p : \{p = \mathrm{T}, q = \mathrm{F}\})$ is T, and we only need one of p and q to be true.
5. $((A \wedge B) : a)$ is T if both of $(A : a)$ and $(B : a)$ are T, and is F otherwise. For example, $((p \wedge q) : \{p = \mathrm{T}, q = \mathrm{F}\})$ is F because $(p : \{p = \mathrm{T}, q = \mathrm{F}\})$ and $(q : \{p = \mathrm{T}, q = \mathrm{F}\})$ are not both T.
6. $(\neg A : a)$ is T if $(A : a$ is F, and is F if $(A : a)$ is T.
7. $((A) : a) = (A : a)$. Parentheses only influence the structure of a propositional formula. A parenthesized formula (A) has the same meaning as A.

You determine the value of a propositional formula by building up larger and larger subexpressions, being careful to follow the rules of precedence and associativity. For example, suppose that $a = \{p$=F, q=T, r=T$\}$. Then

(a) $(q : a) = \mathrm{T}$

(b) $(p : a) = \mathrm{F}$

(c) $(\neg p : a) = \mathrm{T}$ by (b)

(d) $(\neg p \wedge q : a) = \mathrm{T}$ by (a) and (c)

1.3 Additional definitions

Definition 1.5. $A \rightarrow B$ is defined to be an abbreviation for $\neg A \vee B$. Operator $\rightarrow$ is read "implies".

Intuitively, $A \rightarrow B$ means "if A is true then B is true." But that is not its definition. Its definition is that either A is false or B is true (or both). Notice that, if B is true, then $A \rightarrow B$ is true, *by definition*. Also, if A is false, then $A \rightarrow B$ is true, *by definition*.

Operator $\rightarrow$ has lower precedence than $\vee$ and is left-associative. Note that $\rightarrow$ is not an associative operator. $(A \rightarrow B) \rightarrow C$ does not have the same meaning as $A \rightarrow (B \rightarrow C)$.

Definition 1.6. $A \leftrightarrow B$ is defined to be the same as $((A \rightarrow B) \wedge (B \rightarrow A))$. Operator $\leftrightarrow$ is read "if and only if".

Formula $A \leftrightarrow B$ says that A and B have the same value; either both are true or both are false. In fact, $A \leftrightarrow B$ is equivalent to $(A \wedge B) \vee (\neg A \wedge \neg B)$. That is, either A and B are both true or A and B are both false.

Definition 1.6. $A \equiv B$ if $A \leftrightarrow B$ is true for all possible values of the variable in A and B. Read $A \equiv B$ as "A is equivalent to B.".

Operators $\leftrightarrow$ and $\equiv$ have even lower precedence than $\rightarrow$. Here is a complete precedence table, from high to low precedence.

Precedence	
parentheses	high
$\neg$	
$\wedge$	
$\vee$	
$\rightarrow$	
$\leftrightarrow$	
$\equiv$	low

1.4 Truth tables

Since the value of a propositional formula depends on the values of its variables, one way to understand what the formula means is to look at its value for all possible values of the variables. That leads to the idea of a *truth table* of a propositional formula. The following is a truth table for $\neg p \vee q$.

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

There is a row for each possible collection of values of the variables. Under each variable, we write that variable's value. Under each operator, we write the value of the formula having that operator as its main or outermost operator. The column in blue is the value of the entire formula, $\neg p \vee q$.

1.5 Validity

Definition 1.8. Propositional formula ϕ is *valid* if $(\phi : a)$ is true for every truth value assignment a. A valid formula is also called a *tautology*.

For example, operator $\vee$ is commutative. Another way to say that is to say that formula

$$(p \vee q) \leftrightarrow (q \vee p)$$

is valid. Let's check that using a truth table.

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

The validity of

$$(p \vee q) \leftrightarrow (q \vee p)$$

is evident from the blue column of all Ts.

Table 1-1 shows a collection of true equivalences and valid propositional formulas. You can check each one using a truth table.

Valid equivalences give you a way to replace one formula by another. For example, if you see $p \vee q$ in any context, you can replace it by $q \vee p$. In fact, you can replace any variable by any propositional formula in any of the above tautologies (or any other valid propositional formula) and they are still valid, provided (1) you replace every occurrence of a variable by the same propositional formula and (2) you use parentheses to avoid rules of precedence from rearranging the formula. For example, the commutative law for $\wedge$ says that

$$p \wedge q \;\equiv\; q \wedge p.$$

Replacing p by $(w \to v)$ and q by $\neg r$ yields

$$(w \to v) \wedge \neg r \;\equiv\; \neg r \wedge (w \to v)$$

which is also valid. Review of propositional logic

Table 1-1: Some propositional tautologies	
Equivalence	**Name**
$\neg(\neg p) \equiv p$	double negation
$p \vee q \equiv (q \vee p)$	commutative law of $\vee$
$p \wedge q \equiv (q \vee p)$	commutative law of $\wedge$
$(p \vee q) \vee r \equiv p \vee (q \vee r)$	associative law of $\vee$
$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	associative law of $\wedge$
$(p \wedge (q \vee r) \equiv (p \vee q) \wedge (p \vee r)$	distributive law of $\wedge$ over $\vee$
$(p \vee (q \wedge r) \equiv (p \wedge q) \vee (p \wedge r)$	distributive law of $\vee$ over $\wedge$
$\neg(p \vee q) \equiv \neg p \wedge \neg q$	DeMorgan's law for $\vee$
$\neg(p \wedge q) \equiv \neg p \vee \neg q$	DeMorgan's law for $\wedge$
$\neg(p \rightarrow q) \equiv p \wedge \neg q$	DeMorgan's law for $\rightarrow$
$p \rightarrow q \equiv \neg q \rightarrow \neg p$	Law of the contrapositive
$(p \vee q) \rightarrow r \equiv (p \rightarrow r) \wedge (q \rightarrow r)$	cases
$(p \wedge q) \rightarrow r \equiv (p \rightarrow (q \rightarrow r))$	
$p \wedge \neg p \equiv \mathbf{F}$	contradiction 1
$p \equiv (\neg p \rightarrow p)$	contradiction 2
$p \equiv (\neg p \rightarrow \mathbf{F})$	contradiction 3
$p \vee \neg p$	Law of the excluded middle
$p \rightarrow p$	Law of the excluded middle, restated using $\rightarrow$
$\neg(p \wedge \neg p)$	Law of the excluded middle (DeMogan variant)
$p \rightarrow (q \rightarrow p)$	
$\neg p \rightarrow (p \rightarrow q)$	

2 First-Order Logic

First-order logic (also called *predicate logic*) is an extension of propositional logic that is much more useful than propositional logic. It was created as a way of formalizing common mathematical reasoning.

In first-order logic, you start with a nonempty set of values called the *domain of discourse* U. Logical statements talk about properties of values in U and relationships among those values.

2.1 Predicates

In place of propositional variables, first-order logic uses *predicates*.

Definition 2.1. A *predicate* P takes zero or more parameters $x_1, x_2, \ldots, x_n$ and yields either true or false. First-order formula $P(x_1, \ldots, x_n)$ is the value of predicate P with parameters $x_1, \ldots, x_n$. A predicate with no parameters is a propositional variable.

Suppose that the domain of discourse U is the set of all integers. Here are some examples of predicates. There is no standard collection of predicates that are always used. Rather, each of these is like a function definition in a computer program; different programs contain different functions.

- We might define even(n) to be true if n is even. For example even(4) is true and even(5) is false.
- We might define greater(x, y) to be true if $x > y$. For example, greater$(7, 3)$ is true and greater$(3, 7)$ is false.
- We might define increasing(x, y, z) to be true if $x < y < z$. For example, increasing$(2, 4, 6)$ is true and increasing$(2, 4, 2)$ is false.

2.2 Terms

A *term* is an expression that stands for a particular value in U. The simplest kind of term is a *variable*, which can stand for any value in U.

A *function* takes zero or more parameters that are members of U and yields a member of U. Here are examples of functions that might be defined when U is the set of all integers.

- A function with no parameters is called a *constant*. We might define function zero with no parameters to be the constant 0.
- We might define successor(n) to be $n+1$. For example, successor$(2) = 3$.
- We might define sum(m, n) to be $m+n$. For example, sum$(5, 7) = 12$.
- We might define largest(a, b, c) to be the largest of a, b and c. For example, largest$(3, 9, 4) = 9$ and largest$(4, 4, 4) = 4$.

Definition 2.2. A *term* is defined as follows.

1. A *variable* is a term. We use single letters such as x and y for variables.
2. If f is a function that takes no parameters then f is a term (standing for a value in U).
3. If f is a function that takes $n > 0$ parameters and $t_1, \ldots, t_n$ are terms then $f(t_1, \ldots, t_n)$ is a term.

For example, sum(sum(x, y), successor(z)) is a term. (What is its value if $x = 2$, $y = 5$ and $z = 20$?)

The meaning of a term should be clear, provided the values of variables are known. Term sum(x, y) stands for the result that function sum yields on parameters (x, y) (the sum of x and y).

2.3 First-order formulas

Definition 2.3. A *first-order formula* is defined as follows.

1. **T** and **F** are first-order formulas.

2. If P is a predicates that takes no parameters then P is a first-order formula.

3. If $t_1, \ldots, t_n$ are terms and P is a predicate that takes $n > 0$ parameters, then $P(t_1, \ldots, t_n)$ is a first-order formula. It is true if $P(v_1, \ldots, v_n)$ is true, where v_1 is the value of term t_1, v_2 is the value of term t_2, etc.

4. If t_1 and t_2 are terms then $t_1 = t_2$ is a first-order formula. (It is true if terms t_1 and t_2 have the same value.)

5. If A and B are first-order formulas and x is a variable then each of the following is a first-order formula.

   (a) (A)

   (b) $\neg A$

   (c) $A \vee B$

   (d) $A \wedge B$

   (e) $\forall x\, A$

   (f) $\exists x\, A$

The meaning of parentheses, **T**, **F**, $\neg$, $\vee$ and $\wedge$ are the same as in propositional logic. Symbols $\forall$ and $\exists$ are called *quantifiers*. You read $\forall x$ as "for all x, and $\exists x$ as "for some x" or "there exists an x". They have the following meanings.

1. $\forall x\, A$ is true of A is true for all values of x in U.

2. $\exists x\, A$ is true if A is true for at least one value of x in U.

By convention, quantifiers have higher precedence than all of the operators $\wedge$, $\vee$, etc.

Examples of first-order formulas are:

1. $P(\text{sum}(x, y))$ says that, if $v = \text{sum}(x, y)$, then $P(v)$ is true. Its value (true or false) depends on the meanings of predicate P and function sum, as well as on the values of variables x and y.

2. $\forall x(\text{greater}(x, x))$ says that $\text{greater}(x, x)$ is true for every value x in U. Using the meaning of $\text{greater}(a, b)$ given above, $\forall x(\text{greater}(x, x))$ is clearly false, since no x can be greater than itself.

3. $\neg\forall x(\text{greater}(x, x))$ says that $\forall x(\text{greater}(x, x))$ is false. That is true.

4. $\exists y(y = \text{sum}(y, y))$ says that there exists a value y where $y = y + y$. That is true since $0 = 0 + 0$.

5. $\forall x(\exists y(\text{greater}(y, x)))$ says that, for every value v of x, first-order formula $\exists y(\text{greater}(y, v))$ is true. That is true. If $v = 100$, then choose $y = 101$, which is larger than 100. If $v = 1000$, choose $y = 1001$. If $v = 1,000,000$, choose $y = 1,000,001$.

6. $\exists y(\forall x(\text{greater}(y, x)))$ says that there exists a value v of y so that $\forall x(\text{greater}(v, x))$. That is false. There is no single value v that is larger than every integer x.

Operators $\rightarrow$, $\leftrightarrow$ and $\equiv$ have the same meanings in first-order logic as in propositional logic.

2.4 Sentences

Example 1 above uses variable x and y, and its value cannot be determined without knowing the values of x and y. It only makes sense if the values of x and y have already been specified. Think of them as similar to global variables in a function definition in a computer program.

The other examples above do not depend on any variable values. They manage their own variables, and are similar to a function definition that only uses local variables.

We say that variable x is *bound* if it occurs inside A in a first-order formula of the form $\forall x\, A$ or $\exists x\, A$.

Definition 2.4. A first-order formula is a *sentence* if all of its variables are bound.

Table 2-1. Some valid equivalences
$\exists x\, P(x) \vee \neg\exists x\, P(x)$
$\forall x\, P(x) \ \wedge\ \exists y\, Q(y) \ \equiv\ \exists y\, Q(y) \ \wedge\ \forall x\, P(x)$
$\neg(\forall x\, A) \ \equiv\ \exists x(\neg A)$
$\neg(\exists x\, A) \ \equiv\ \forall x(\neg A)$
$\forall x(A \wedge B) \ \equiv\ \forall x\, A \wedge \forall x\, B$
$\forall x\, A \to \exists x\, A$

2.5 Validity

Recall that a propositional formula is *valid* if it is true for all values of the variables that it contains. There is a similar concept of validity for first-order formulas.

Definition 2.5. Suppose that S is a sentence of first-order logic. (That is, it does not contain any unbound variables.) We say that S is *valid* if it is true regardless of the domain of discourse and the meanings of the predicates and functions that it mentions.

One way to get a valid first-order formula is to substitute first-order formulas into a propositional tautology. The following table lists two valid first-order formulas found in that way. Table 2-1 lists a few valid first-order equivalences, the first two of which are examples of substituting a first-order formula into a propositional equivalence.

2.6 Notation

First-order logic notation is usually extended to include common mathematical notation. For example, we write $x > y$ rather than greater(x, y), and $x + y$ rather than sum(x, y). Constants such as 0, 1 and 200 are also usually allowed. Instead of writing even(x), we write "x is even". For example,

$$\forall x(x \text{ is even } \wedge\, y \text{ is even } \to x + y \text{ is even})$$

is true. Those notational changes make first-order logic more readable. Review of first-order logic

3 Theorems and Proofs

A *theorem* is any mathematical statement, such as a formula of first-order logic, that has been proved true. When you are about to prove a theorem, you call it theorem as a way of promising that a proof is about to be produced.

3.1 What is a proof?

There are many different precise definitions of a proof. But most mathematicians accept an informal definition: a proof is a clear and unambiguous argument that a mathematical statement is true that any sufficiently knowledgeable person can check. The key is that a reader must be able to check that each step is correct.

Students who are just learning to do proofs make many different kinds of mistakes, but most fall into one of the following two categories.

1. **The student does not check his or her own work.** The reason can vary from lack of time to lack of understanding to fear of failure.

   A student might take a proof of something else from a book or from notes and make some modifications to it, and then *hope* that the modifications have produced a correct proof, without checking whether that is true. The student who has a lack of understanding cannot check the proof. The student who is afraid of failure will not check the proof out of fear that it might turn out to be incorrect.

   Regardless of your reason for not checking your proof, you can be sure that an unchecked proof is incorrect, for the same reasons that an untested computer program does not work. You will need to find a way to motivate yourself to check your proofs carefully.

2. Mathematics relies on precise definitions. When you do a proof, it is essential for you to use definitions wherever appropriate. **Students often get stuck in a proof because they have forgotten to use definitions**. Any time you cannot see how to proceed, ask yourself if using a definition will help. We will do many examples of that.

3.2 Forward proofs

A *forward proof* reasons from what you know to what you can conclude. Each new conclusion relies on prior knowledge or conclusions.

You have probably been taught a different approach in an algebra class. In a *backwards proof*, you write down what you want to show and then perform some manipulations on it, working backwards to a statement that you already know is true.

In this class, we will do forward proofs, with minor excursions using backwards reasoning. **I expect you to use forward proofs as well.** At least for this class, put aside the backwards proofs that you have learned in algebra.

In this section, I do proofs at two different levels of detail. One of the proof works in small steps and shows everything that you know after each step. The other proof is more typical of what you would write, and what I want to see from you.

3.3 Some definitions

Definition 3.1. Integer n is *even* if there exists an integer m such that $n = 2m$. For example, 6 is even because $6 = (2)(3)$.

Definition 3.2. Integer n is *odd* if there exists an integer m such that $n = 2m + 1$. We will also make use of the fact that, for every n, n is odd if and only if n is not even.

Definition 3.3. Integer n is a *perfect square* if there exists an integer m such that $n = m^2$.

Definition 3.4. Real number x is *rational* if there exist integers n and m where $m \neq 0$ such that $x = n/m$.

3.4 Proof techniques

The remaining subsections discuss common ways of proving particular kinds of first-order formulas.

3.5 Proving $A \to B$

To prove $A \to B$, assume that A is true and show that B is true.

Theorem 3.1. If n is even then n^2 is even.

Detailed Proof.

1. Suppose that n is even.

Known variables:	n
Know:	n is even.
Goal:	n^2 is even.

2. By the definition of an even integer, there exists an integer m such that $n = 2m$.

Known variables:	n, m
Know:	n is even.
Know:	$n = 2m$.
Goal:	n^2 is even.

3. Since $n = 2m$, $n^2 = (2m)^2 = 4m^2 = 2(2m^2)$.

Known variables:	n, m
Know:	n is even.
Know:	$n = 2m$.
Know:	$n^2 = 2(2m^2)$.
Goal:	n^2 is even.

4. So $n^2 = 2(x)$ where $x = 2m^2$. Using the definition of an even number again, n^2 is even.

♢———————————————————————————————♢

Typical Proof. Suppose n is even. By the definition of an even integer, there is an integer m such that $n = 2m$. So

$$n^2 = (2m)^2 = 4m^2 = 2(2m^2).$$

By the definition of an even integer, n^2 is even.

♢———————————————————————————————♢

Theorem 3.2. If n and m are perfect squares then nm is a perfect square.

Detailed Proof.

1. Suppose that n and m are perfect squares.

Known variables:	n, m
Know:	n is a perfect square.
Know:	m is a perfect square.
Goal:	nm is a perfect square.

2. By the definition of a perfect square, there exist integers x and y such that $n = x^2$ and $m = y^2$.

Known variables:	n, m, x, y
Know:	$n = x^2$.
Know:	$m = y^2$.
Goal:	nm is a perfect square.

3. Replacing n by x^2 and m by y^2, $nm = x^2y^2 = (xy)^2$.

Known variables:	n, m, x, y
Know:	$n = x^2$.
Know:	$m = y^2$.
Know:	$nm = (xy)^2$.
Goal:	nm is a perfect square.

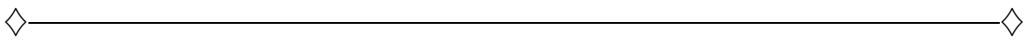
4. So $nm = z^2$ where $z = xy$. Using the definition of a perfect square again, nm is perfect square.

♢———————————————————————————————♢

Typical Proof. Suppose that n and m are perfect squares. By the definition of a perfect square, there exist integers x and y such that $n = x^2$ and $m = y^2$. Replacing n by x^2 and m by y^2,

$$nm = x^2y^2 = (xy)^2.$$

So nm is a perfect square.



3.5.1 Using the contrapositive

You can prove any theorem by proving an equivalent mathematical statement. For example, you can prove $A \to B$ by proving equivalent formula $\neg B \to \neg A$, which is called the *contrapositive* of $A \to B$. Here is an example.

Theorem 3.3. Suppose n is an integer. If $3n + 2$ is odd, then n is odd.

Detailed Proof. We prove the contrapositive: If n is not odd then $3n + 2$ is not odd.

1. We know that an integer x is even if and only if x is not odd. So what we want to prove is equivalent to: If n is even then $3n + 2$ is even.

Known variables:	n
Goal:	If n is even then $3n + 2$ is even.

2. Suppose that n is even.

Known variables:	n
Know:	n is even.
Goal:	$3n + 2$ is even.

3. By the definition of an even integer, there exists an integer m such that $n = 2m$.

Known variables:	n, m
Know:	$n = 2m$.
Goal:	$3n + 2$ is even.

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

Known variables:	n, m
Know:	$n = 2m$.
Know:	$3n + 2 = 2(3m + 1)$.
Goal:	$3n + 2$ is even.

5. Using the definition of an even integer again, $3n + 2$ is even because $3n + 2 = 2z$ where $z = 3m + 1$.

♢———————————————————————————♢

Typical Proof. We prove the contrapositive: If n even then $3n + 2$ is even.

Suppose n is even. Then there exists an integer m such that $n = 2m$.

$$3n + 2 = 3(2m) + 2 = 6m + 2 = 2(3m + 1).$$

Since $3n + 2$ is twice an integer, $3n + 2$ is even.

♢———————————————————————————♢

3.6 Proving and using $A \wedge B$

To prove $A \wedge B$, prove A and prove B.

If you know that $A \wedge B$ is true, then you know that A is true and you know that B is true.

3.7 Proving and using $\neg(A)$

To prove $\neg(A)$, you typically use DeMorgan's laws and the laws for negating quantified formulas to push the negation inward. For example, to prove $\neg(A \wedge B)$, you prove equivalent formula $\neg A \vee \neg B$. To prove $\neg(\forall x A)$, you prove equivalent formula $\exists x(\neg A)$.

The same principle applies when you already know $\neg(A)$. For example, if you know $\neg(A \to B)$, you can conclude equivalent formula $A \wedge \neg B$. You write that down as an additional known fact.

3.8 Proving and using $A \vee B$

To prove $A \vee B$, you usually prove one of the equivalent formulas $\neg A \to B$ or $\neg B \to A$.

Suppose that you know that $A \vee B$ is true and you want to use that to show that C is true. That is, you want to show that $A \vee B \to C$ is true. You typically prove equivalent formula

$$A \to C \ \wedge \ B \to C.$$

That is called *proof by cases*. First, you assume that A is true and show that C is true. Next, you assume that B is true and show that C is true. See Section 3.

3.9 Proving and using $\exists x A$

To prove that something exists, produce it.

Theorem 3.4. There exists an integer n where n is even and n is prime.

Proof. Choose $n = 2$. Notice that n is even and n is prime.

♢———————————————————————————♢

3.9.1 Using existential knowledge

Sometimes, instead of needing to prove $\exists x P(x)$, you already know $\exists x P(x)$. What do you do? You ask somebody else to give you a value x so that $P(x)$ is true. It is not necessary for you to say how to find x. We will encounter many examples of that.

3.10 Proving $\forall x A$

To prove $\forall x P(x)$, prove $P(x)$ for an *arbitrary* value of x.

That does not mean that you can choose the value of x. Rather, someone else chooses x and you must prove that $P(x)$ is true for that value of x. Think of it as a challenge. You say to someone else, give me any value of x that you

like. I will prove that $P(x)$ is true. In mathematics, *arbitrary* always means a value chosen by someone else.

We have actually used this idea above. When the statement of a theorem involves unbound variables, it is assumed to be saying that the statement is true for all values of those variables. Here is the first proof above with the quantifier explicit. The universe of discourse is the set of all integers.

Theorem 3.5. $\forall n(n \text{ is even} \to n^2 \text{ is even})$.

Detailed Proof.

1. Ask someone else to select an arbitrary integer n. (We cannot assume anything about n except that it belongs to the universe of discourse.) We must prove: (n is even $\to n^2$ is even) for that n.

Known variables:	n
Goal:	n is even $\to n^2$ is even.

2. Suppose that n is even.

Known variables:	n
Know:	n is even.
Goal:	n^2 is even.

3. By the definition of an even integer, there exists an integer m such that $n = 2m$.

Known variables:	n
Know:	$\exists m(n = 2m)$.
Goal:	n^2 is even.

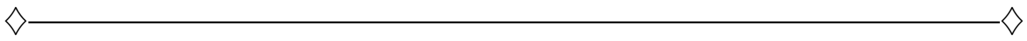
4. Ask someone else to provide the integer m that is asserted to exist.

Known variables:	n, m
Know:	$n = 2m$.
Goal:	n^2 is even.

5. Since $n = 2m$, $n^2 = (2m)^2 = 4m^2 = 2(2m^2)$.

Known variables:	n, m
Know:	$n = 2m$.
Know:	$n^2 = 2(2m^2)$.
Goal:	n^2 is even.

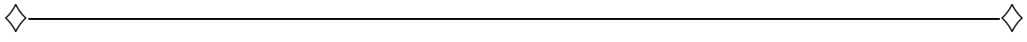
6. So $n = 2(x)$ where $x = 2m^2$. Using the definition of an even number again, n is even.



Typical Proof. Let n be an arbitry even integer. By the definition of an even integer, there exists an integer m such that $n = 2m$. So

$$n^2 = (2m)^2 = 4m^2 = 2(2m^2).$$

Evidently, n^2 is even.



3.10.1 Proof by contradiction

You can prove any theorem by proving an equivalent theorem. We have seen propositional tautology

$$P \equiv (\neg P \to \mathbf{F}).$$

That is, to prove P, assume that P is false and prove that **F** is true. That is called *proof by contradiction*. Let's use proof by contradition to reprove a theorem that we proved above.

Theorem 3.6. For every integer n, if $3n + 2$ is odd, then n is odd.

Detailed Proof.

1. Reasoning by contradiction, we can assume the theorem is false and prove **F**. That is:

Know:	$\neg\forall n(3n + 2$ is odd $\to n$ is odd).
Goal:	**F**.

2. We can push the negation across the quantifier using valid formula $\neg\forall x A \equiv \exists x(\neg A))$.

Know:	$\exists n(\neg(3n+2 \text{ is odd } \rightarrow n \text{ is odd}))$.
Goal:	**F**.

3. Now use the tautology that $\neg(P \rightarrow Q) \equiv P \wedge \neg Q)$.

Know:	$\exists n(3n+2 \text{ is odd } \wedge n \text{ is even})$.
Goal:	**F**.

4. Ask somebody else to select an integer n such that $3n+2$ is odd and n is even.

Known variables:	n
Know:	$3n+2$ is odd.
Know:	n is even.
Goal:	**F**.

5. By the definition of an even integer, saying that n is even is equivalent to saying that there exists an integer m such that $n = 2m$. (Existential information is useful because it allows you to get something in hand, as is done in the next step. So you often want to exploit existential information.)

Known variables:	n
Know:	$3n+2$ is odd.
Know:	$\exists m(n = 2m)$.
Goal:	**F**.

6. Since we know that an integer m exists such that $n = 2m$, we can ask somebody else to give us such an m. Let's do that.

Known variables:	n, m
Know:	$3n+2$ is odd.
Know:	$n = 2m$.
Goal:	**F**.

7. Since we know that $n = 2m$, it seems reasonable to substitute $2m$ for n in expression $3n + 2$ to see what we get. Doing that gives

$$3n + 2 = 3(2m) + 2 = 6m + 2 = 2(3m + 1).$$

So $3n + 2$ is even. Recording that:

Known variables:	n, m
Know:	$3n + 2$ is odd.
Know:	$n = 2m$.
Know:	$3n + 2$ is even.
Goal:	**F**.

8. But $3n + 2$ cannot be both even and odd. Formula ($3n + 2$ is odd $\wedge$ $3n + 2$ is even) is equivalent to **F**. So we have concluded that **F** is true and we are done.

♢———————————————————————————————♢

Typical Proof. By contradiction. Assume there exists an n such that $3n+2$ is odd but n even) Since n is even, there exists an integer m so that $n = 2m$. So

$$3n + 2 = 3(2m) + 2 = 6m + 2 = 2(3m + 1).$$

That means $3n + 2$ is even, contradiction the assumption that $3n + 2$ is odd.

♢———————————————————————————————♢

3.11 Proving $\forall x(\exists y A)$

It is common to encounter theorems whose general form is $\forall x(\exists y P(x, y))$. The proof usually involves finding an algorithm. For any x, the algorithm must find a y so that $P(x, y)$ is true. Here is an example.

Theorem 3.7. For all real numbers x and y, if x and y are both rational numbers then $x + y$ is also a rational number.

Detailed Proof.

1. Ask someone else to select arbitrary real numbers of x and y.

Known variables:	x, y
Goal:	If x and y are rational then $x + y$ is rational.

2. Assume that x and y are rational.

Known variables:	x, y
Know:	x is rational.
Know:	y is rational.
Goal:	$x + y$ is rational.

3. Our knowledge involves the term *rational*. We need to know what that means. From the definition of a rational number, there must exist integers a and b where $b \neq 0$ and $x = a/b$; and there must exist integers c and d where $d \neq 0$ and $y = c/d$.

Known variables:	x, y, a, b, c, d
Know:	a, b, c and d are integers.
Know:	$b \neq 0$.
Know:	$d \neq 0$.
Know:	$x = a/b$.
Know:	$y = c/d$.
Goal:	$x + y$ is rational.

4. Since the goal is to show that $x + y$ is rational, let's replace x by a/b and replace y by c/d in expression $x + y$.

$$x + y = a/b + c/d = ad/bd + bc/bd = (ad + bc)/bd.$$

Known variables:	x, y, a, b, c, d
Know:	a, b, c and d are integers.
Know:	$b \neq 0$.
Know:	$d \neq 0$.
Know:	$x = a/b$.
Know:	$y = c/d$.
Know:	$x + y = (ad + bc)/bd$.
Goal:	$x + y$ is rational.

5. But we have shown that $x + y$ is the ratio of integers $ad + bc$ and bd. Since neither b nor d is 0, bd cannot be 0. So $x + y$ is rational, by the definition of a rational number.

♢———————————————————————————♢

Typical Proof. Let x and y be arbitrary rational numbers. By the definition of a rational number, there exists integers a, b, c and d ($b \neq 0$ and $d \neq 0$) such that $x = a/b$ and $y = c/d$. Then

$$x + y = a/b + c/d = ad/bd + bc/bd = (ad + bc)/bd.$$

Since $x + y$ is the ratio of two integers, $x + y$ is rational. (You can observe that $bd \neq 0$ since the product of two nonzero numbers is nonzero.)

3.12 Proving $A \equiv B$ or $A \leftrightarrow B$

There are two commonly used ways of proving $A \equiv B$.

3.12.1 Using direct equivalences

You can treat $\equiv$ in a way similar to the way you treat $=$ in algebraic equations, performing equivalence-preserving manipulations. Let's use that approach to prove the law of the contrapositive.

Theorem 3.8. $P \to Q \ \equiv \ \neg Q \to \neg P$.

Proof.

$$\begin{array}{lcll} \neg Q \to \neg P & \equiv & \neg(\neg Q) \vee \neg P & \text{(defn of } \to\text{)} \\ & \equiv & Q \vee \neg P & \text{(double negation)} \\ & \equiv & \neg P \vee Q & \text{(commutative law of } \vee\text{)} \\ & \equiv & P \to Q & \text{(defn of } \to\text{)} \end{array}$$

3.12.2 Proving two implications

Sometimes it is preferable to use the definition of $P \leftrightarrow Q$, namely $P \to Q \wedge Q \to P$.

Theorem 3.9. For every integer n, n is odd if and only if n^2 is odd.

Detailed Proof.

1. It suffices to prove

   $$\forall n(n \text{ is odd } \to n^2 \text{ is odd } \wedge\ n^2 \text{ is odd } \to n \text{ is odd}).$$

   That gives two goals. We use tautology $\forall x(A \wedge B) \equiv \forall x A \wedge \forall x B$ and change the variable names so that we can look at the two parts separately without variables from one interfering with the other.

Goal (1):	$\forall n(n \text{ is odd } \to n^2 \text{ is odd}).$
Goal (2):	$\forall m(m^2 \text{ is odd } \to m \text{ is odd}).$

2. Ask someone else to choose arbitrary values of m and n.

Known variables:	n, m
Goal (1):	n is odd $\to n^2$ is odd.
Goal (2):	m^2 is odd $\to m$ is odd.

3. Goal (2) is equivalent to its contrapositive, m is even $\to m^2$ is even. We proved that as Theorem 3.1. That only leaves Goal (1). (We know goal (2), but we can always discard known things to simplify.)

Known variables:	n
Goal (1):	n is odd $\to n^2$ is odd.

4. To prove Goal (1), assume that n is odd.

Known variables:	n
Know:	n is odd.
Goal (1):	n^2 is odd.

5. Since n is odd, there exists an integer k so that $n = 2k + 1$.

Known variables:	n
Know:	$\exists k(n = 2k + 1)$.
Goal (1):	n^2 is odd.

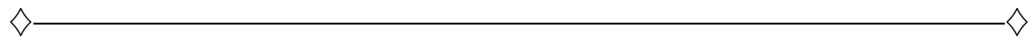
6. Ask someone else to provide a value k such that $n = 2k + 1$.

Known variables:	n, k
Know:	$n = 2k + 1$.
Goal (1):	n^2 is odd.

7. Since $n = 2k + 1$,

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

Since $n^2 = 2z + 1$ for $z = 2k^2 + 2k$, it is evident that n^2 is odd.



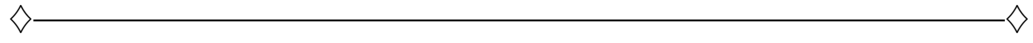
Typical Proof.

(a) (n is odd $\rightarrow$ n^2 is odd) Assume that n is odd. By the definition of an odd integer, there is an integer k such that $n = 2k + 1$. So

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

By the definition of an odd integer, n^2 is odd.

(b) (n^2 is odd $\rightarrow$ n is odd) This is equivalent to (n is even $\rightarrow$ n^2 is even), which we profed earlier as Theorem 3.1.



3.13 Proof by cases

Proof by cases involves proving two or more implications. You must be careful that assumptions made during one of those cases are not still in place when proving another one. Think of this is similar to calling a function in a program. Each time a function is called, a new frame is created, so that calling $f(3)$ does not interfere with a later call to $f(4)$.

Theorem 3.10. For every integer n, $n^2 \geq n$.

Detailed Proof.

1. Ask someone to select an arbitrary integer n.

Known variables:	n
Know:	n is an integer
Goal:	$n^2 \geq n$.

2. Let's break proving the goal into three cases: $n = 0$, $n > 0$ and $n < 0$.

Known variables:	n
Know:	n is an integer
Goal (1):	$n = 0 \to n^2 \geq n$.
Goal (2):	$n > 0 \to n^2 \geq n$.
Goal (3):	$n < 0 \to n^2 \geq n$.
Goal (4):	$n^2 \geq n$.

3. Goal (1) is clearly true since $0^2 \geq 0$. Let's record it among the known facts.

Known variables:	n
Know:	n is an integer
Know (1):	$n = 0 \to n^2 \geq n$.
Goal (2):	$n > 0 \to n^2 \geq n$.
Goal (3):	$n < 0 \to n^2 \geq n$.
Goal (4):	$n^2 \geq n$.

4. Goal (2) is an implication, so we should assume that $n > 0$ and prove that $n^2 \geq n$. But let's prove that as a separate subproof. Knowledge and goals that are local to the proof of goal (2) is numbered 2.1, 2.2, etc., and they can only be used to establish goal (2).

Known variables:	n
Know:	n is an integer
Know (1):	$n = 0 \to n^2 \geq n.$
Goal (2):	$n > 0 \to n^2 \geq n.$
Goal (3):	$n < 0 \to n^2 \geq n.$
Goal (4):	$n^2 \geq n.$
Know (2.1):	$n > 0$
Goal (2.1):	$n^2 \geq n$

5. Since $n > 0$ is an integer, it must be the case that $n \geq 1$.

Known variables:	n
Know:	n is an integer
Know (1):	$n = 0 \to n^2 \geq n.$
Goal (2):	$n > 0 \to n^2 \geq n.$
Goal (3):	$n < 0 \to n^2 \geq n.$
Goal (4):	$n^2 \geq n.$
Know (2.1):	$n \geq 1$
Goal (2.1):	$n^2 \geq n$

Multiplying both sides of fact (2.1) by n preserves the inequality because $n > 0$. That gives $n \cdot n \geq n \cdot 1$, or equivalently, $n^2 \geq n$.

Known variables:	n
Know:	n is an integer
Know (1):	$n = 0 \to n^2 \geq n.$
Goal (2):	$n > 0 \to n^2 \geq n.$
Goal (3):	$n < 0 \to n^2 \geq n.$
Goal (4):	$n^2 \geq n.$
Know (2.1):	$n \geq 1$
Know (2.2):	$n^2 \geq n$
Goal (2.1):	$n^2 \geq n$

6. We have succeeded in proving goal (2). Notice that fact (2.2) cannot be used to establish goal (4) since it depends on the assumption that $n > 0$.

   We can move goal (2) into our knowledge. But we must also throw out parts that were local to the proof of goal (2).

Known variables:	n
Know:	n is an integer
Know (1):	$n = 0 \to n^2 \geq n.$
Know (2):	$n > 0 \to n^2 \geq n.$
Goal (3):	$n < 0 \to n^2 \geq n.$
Goal (4):	$n^2 \geq n.$

7. Now we need to prove goal (3). Assume that $n < 0$. But the square of any number is nonnegative. It follows that $n^2 \geq 0 > n$, and we can move goal (3) into what we know.

Known variables:	n
Know:	n is an integer
Know (1):	$n = 0 \to n^2 \geq n.$
Know (2):	$n > 0 \to n^2 \geq n.$
Know (3):	$n < 0 \to n^2 \geq n.$
Goal (4):	$n^2 \geq n.$

8. Propositional formula

$$((P \to S) \wedge (Q \to S) \wedge (R \to S)) \to ((P \vee Q \vee R) \to S)$$

is a tautology. That means known facts (1), (2) and (3) imply

$$(n = 0 \vee n > 0 \vee n < 0) \to n^2 \geq n.$$

But we know that $(n = 0 \vee n > 0 \vee n < 0)$ is true, and $\mathbf{T} \to S$ is equivalent to S. So we have demonstrated goal (4).

♢———————————————————————————————♢

Typical Proof. The proof is by cases ($n = 0$, $n > 0$ and $n < 0$).

Case 1 ($n = 0$). Then $n^2 \geq n$ because $0^2 \geq 0$.

Case 2 ($n > 0$). The smallest positive integer is 1, so $n > 0$ implies $n \geq 1$. Multiplying both sides of inequality $n \geq 1$ by positive number n gives $n^2 \geq n$.

Case 3 ($n < 0$). $n^2 \geq 0$ for all numbers n. Since, in this case, n is negative, clearly $n^2 \geq n$.

♢———————————————————————————————♢

Theorems and proofs

4 Sets

4.1 Sets

Definition 4.1. A *set* is an unordered collection of things without repetitions. The things in set S are called the *members* of S.

Definition 4.2. A *set enumeration* is one way to describe a set, by writing the members of the set in braces, separated by commas. For example, {2, 5, 9} is a set of three integers.

4.1.1 Finite and infinite sets

It is possible to list the members of a *finite* set. But some sets, such as the set of all positive integers, have infinitely many members. Here are a few common infinite sets.

$\mathcal{N}$	$\{0, 1, 2, 3, \ldots\}$
$\mathcal{Z}$	$\{\ldots, -2, -1, 0, 1, 2, \ldots\}$
$\mathcal{R}$	the set of all real numbers

4.1.2 Set comprehensions

A *set comprehension* is a way to describe the set of all values that have a certain property. Notation

$$\{x \mid p(x)\}$$

stands for the set of all values x such that $p(x)$ is true and notation

$$\{f(x) \mid p(x)\}$$

stands for the set of all values $f(x)$ such that $p(x)$ is true. Notation

$$\{x \in S \mid p(x)\}$$

is shorthand for $\{x \mid x \in S \wedge p(x)\}$ Here are some examples.

Set	Description
$\{x \mid x \in \mathcal{R} \ \wedge \ x^2 - 2x + 1 = 0\}$	$\{-1, 1\}$
$\{x \in \mathcal{R} \mid x^2 - 2x + 1 = 0\}$	$\{-1, 1\}$
$\{x \mid x$ is an even positive integer$\}$	$\{2, 4, 6, \ldots\}$
$\{x^2 \mid x$ is an even positive integer$\}$	$\{4, 16, 36, \ldots\}$

4.1.3 Set notation and operations

Table 4-1 defines notation for sets.

4.1.4 Identities for sets

Table 4-2 list some identities are easy to establish.

4.1.5 Sets of sets

The members of sets can be sets. For example, if $S = \{\{1, 2, 3\}, \{2, 4, 6\}\}$ then $|S| = 2$, since S has exactly two members, {1, 2, 3} and {2, 4, 6}.

Do not confuse $\in$ with $\subseteq$. If $S = \{\{1, 2, 3\}, \{2, 4, 6\}\}$ then

$\{1, 2, 3\} \in S$

$\{1, 2, 3\} \not\subseteq S$

$3 \notin S$

Notice that $\{\} \neq \{\{\}\}$. $|\{\}| = 0$ but $|\{\{\}\}| = 1$ since $\{\{\}\}$ has one member, the empty set.

Sets

Table 4-1	
Notation	**Meaning**
$\|S\|$	$\|S\|$ is the *cardinality* (size) of S, when S is a finite set.
$\{\}$	$\{\}$ is the empty set, which has no members
$x \in S$	$x \in S$ is true if x is a member of set S. For example, $2 \in \{1, 2, 3, 4\}$
$x \notin S$	$x \notin S$ is equivalent to $\neg(x \in S)$
$S \cup T$	$S \cup T = \{x \mid x \in S \vee x \in T\}$. For example, $\{2, 5, 6\} \cup \{2, 3, 7\} = \{2, 3, 5, 6, 7\}$. This is called the *union* of sets S and T.
$S \cap T$	$S \cap T = \{x \mid x \in S \wedge x \in T\}$. For example, $\{2, 5, 6\} \cup \{2, 3, 7\} = \{2\}$. This is called the *intersection* of sets S and T.
$S - T$	$S - T = \{x \mid x \in S \wedge x \notin T\}$. For example, $\{2, 5, 6\} - \{2, 3, 7\} = \{5, 6\}$. This is called the *difference* of sets S and T.
$\overline{S}$	$\overline{S} = U - S$, where U is the domain of discourse. This is called the *complement* of S.
$S \times T$	$S \times T = \{(x, y) \mid x \in S \wedge y \in T\}$. For example, $\{2, 3\} \times \{5, 6\}$ = {(2,5), (2,6), (3,5), (3,6)}. This is called the *cartesian product* of S and T.
$S \subseteq T$	$S \subseteq T$ is true if $\forall x(x \in S \rightarrow x \in T)$. For example, $\{2, 4, 6\} \subseteq \{1, 2, 3, 4, 5, 6\}$. Notice that $\{2, 4, 6\} \subseteq \{2, 4, 6\}$. $S \subseteq T$ is read "S is a subset of T."
$S = T$	Sets S and T are equal if $S \subseteq T$ and $T \subseteq S$. That is, S and T have exactly the same members.

Table 4-2
Some Set Identities
$A \cup \{\} = A$
$A \cap \{\} = \{\}$
$\overline{\overline{A}} = A$
$A \cup B = B \cup A$
$A \cap B = B \cap A$
$A \cup (B \cup C) = (A \cup B) \cup C$
$A \cap (B \cap C) = (A \cap B) \cap C$
$\overline{A \cup B} = \overline{A} \cap \overline{B}$
$\overline{A \cap B} = \overline{A} \cup \overline{B}$
$A - B = A \cap \overline{B}.$
$A \cup (A \cap B) = A$
$A \cap (A \cup B) = A$