Logic, Sets, and Proofs

David A. Cox and Catherine C. McGeoch
Amherst College

1 Logic

Logical Operators. A *logical statement* is a mathematical statement that can be assigned a value either *true* or *false*. Here we denote logical statements with capital letters A, B. Logical statements be combined with the following operators to form new logical statements.

Operation name	Notation I	Notation II	Java
AND (Conjunction)	$A \wedge B$	$A \cdot B$	`A && B`
OR (Disjunction)	$A \vee B$	$A + B$	`A || B`
NOT (Negation)	$\neg A$	$\bar{A}$	`!A`
IMPLIES (Implication)	$A \rightarrow B$	if A then B	
IF AND ONLY IF (Equivalence)	$A \leftrightarrow B$	A iff B	`==`

Tautologies. Here is a list of tautologies. In any proof, you can replace a statement in the first column with the corresponding statement in the second column, and vice versa. All of these can be proved by truth tables.

Statement	Equivalent statement	Description
$A \vee B$	$B \vee A$	$\vee$ is commutative
$A \wedge B$	$B \wedge A$	$\wedge$ is commutative
$(A \vee B) \vee C$	$A \vee (B \vee C)$	$\vee$ is associative
$(A \wedge B) \wedge C$	$A \wedge (B \wedge C)$	$\wedge$ is associative
$A \vee (B \wedge C)$	$(A \vee B) \wedge (A \vee C)$	$\vee$ distributes over $\wedge$
$A \wedge (B \vee C)$	$(A \wedge B) \vee (A \wedge C)$	$\wedge$ distributes over $\vee$
$A \vee \text{false}$	A	false is identity for $\vee$
$A \wedge \text{true}$	A	true is identity for $\wedge$
$A \vee \neg A$	true	law of excluded middle
$A \wedge \neg A$	false	contradiction
$A \vee A$	A	$\vee$ is idempotent
$A \wedge A$	A	$\wedge$ is idempotent
$\neg\neg A$	A	double negative
$\neg(A \vee B)$	$\neg A \wedge \neg B$	De Morgan's law for $\vee$
$\neg(A \wedge B)$	$\neg A \vee \neg B$	De Morgan's law for $\wedge$
$A \rightarrow B$	$\neg A \vee B$	rewriting implication
$A \rightarrow B$	$\neg B \rightarrow \neg A$	contrapositive
$A \rightarrow (B \rightarrow C)$	$(A \wedge B) \rightarrow C$	conditional proof
$A \leftrightarrow B$	$(A \rightarrow B) \wedge (B \rightarrow A)$	definition of $\leftrightarrow$

2 Sets

A *set* is a collection of objects, which are called *elements* or *members* of the set. Two sets are *equal* when they have the same elements.

Common Sets. Here are three important sets:

- The set of all *integers* is $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$.
- The set of all *real numbers* is $\mathbb{R}$.
- The set with no elements is $\emptyset$, the *empty set*.

Another important set is the set of *natural numbers*, denoted $\mathbb{N}$ or $\mathcal{N}$. Unfortunately, the meaning of $\mathbb{N}$ is not consistent. In some books,

$$\mathbb{N} = \{1, 2, 3, \ldots\},$$

while in other books,

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}.$$

Basic Definitions and Notation.

- $x \in S$: x is an element or member of S. Example: $2 \in \mathbb{Z}$.
- $x \notin S$: x is not an element of S, i.e., $\neg(x \in S)$. Example: $\frac{1}{2} \notin \mathbb{Z}$.
- $S \subseteq T$: Every element of S is also an element of T. We say that S is a *subset* of T and that T *contains* or *includes* S. Examples: $\mathbb{Z} \subseteq \mathbb{R}$ and $\mathbb{Z} \subseteq \mathbb{Z}$.
- $S \not\subseteq T$: This means $\neg(S \subseteq T)$, i.e., some element of S is not an element of T. Example: $\mathbb{R} \not\subseteq \mathbb{Z}$.
- $S \subset T$: This means $(S \subseteq T) \wedge (S \neq T)$. We say that S is a *proper subset* of T and that T *properly contains* or *properly includes* S. Example: $\mathbb{Z} \subset \mathbb{R}$.

Note that $S = T$ is equivalent to $(S \subseteq T) \wedge (T \subseteq S)$.

Describing Sets. There are two basic ways to describe a set.

- Listing elements: Some sets can be described by listing their elements inside brackets { and }. Example: The set of positive squares is $\{1, 4, 9, 16, \ldots\}$. When listing the elements of a set, order is unimportant, as are repetitions. Thus

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

  since all three contain the same elements, namely 1, 2 and 3.

- Set-builder notation: We can sometimes describe a set by the conditions its elements satisfy. Example: The set of positive real numbers is

$$\{x \in \mathbb{R} \mid x > 0\}.$$

This can also be written $\{x \mid (x \in \mathbb{R}) \wedge (x > 0)\}$. A common alternative notation uses the colon instead of the vertical bar, as in $\{x : (x \in \mathbb{R}) \wedge (x > 0)\}$.

Operations on Sets. Let S and T be sets.

- The *union* $S \cup T$ is the set

$$S \cup T = \{x \mid (x \in S) \vee (x \in T)\}.$$

Thus an element lies in $S \cup T$ precisely when it lies in *at least one* of the sets. Examples:

$$\begin{aligned} \{1,2,3,4\} \cup \{3,4,5,6\} &= \{1,2,3,4,5,6\} \\ \{n \in \mathbb{Z} \mid n \geq 0\} \cup \{n \in \mathbb{Z} \mid n < 0\} &= \mathbb{Z}. \end{aligned}$$

- The *intersection* $S \cap T$ is the set

$$S \cap T = \{x \mid (x \in S) \wedge (x \in T)\}.$$

Thus an element lies in $S \cap T$ precisely when it lies in *both* of the sets. Examples:

$$\begin{aligned} \{1,2,3,4\} \cap \{3,4,5,6\} &= \{3,4\} \\ \{n \in \mathbb{Z} \mid n \geq 0\} \cap \{n \in \mathbb{Z} \mid n < 0\} &= \emptyset. \end{aligned}$$

- The *set difference* $S - T$ is the set of elements that are in S but not in T. Example:

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

A common alternative notation for $S - T$ is $S \setminus T$.

3 Predicates and Quantifiers

A *variable* like x represents some unspecified element from a fixed set U called the *universe*. A *predicate* is a logical statement containing one or more variables. Examples: "x is even" and "$x > y$" are predicates. The truth of the predicate depends on which particular members of the universe are plugged in for the variables.

We combine *quantifiers* with predicates to form statements about members of U. There are two basic types:

- $\forall x \in U\,(P(x))$. This *universal quantifier* means

  for all (*or* for every *or* for each *or* for any) value of x in the universe,

  the predicate $P(x)$ is true. Example: $\forall x \in \mathbb{R}\,(2x = (x+1)+(x-1))$.

- $\exists x \in U\,(P(x))$. This *existential quantifier* means

  there exists a (*or* there is at least one) value of x in the universe

  for which the predicate $P(x)$ is true. Example: $\exists x \in \mathbb{Z}\,(x > 5)$.

If the universe is understood, it may be omitted from the quantifier. For example, assuming that the universe is $\mathbb{Z}$, the above predicate can be written $\exists x\,(x > 5)$.

A general strategy for proving things about predicates with quantifiers is to *work with their elements one at a time.* Even when we are dealing with universal quantifiers and infinite universes, we proceed by thinking about the properties that a particular but arbitrary element of the universe would have.

Predicates and Sets. A predicate $P(x)$ is often used to describe a set in terms of the set-builder notation

$$S = \{x \in U \mid P(x)\}.$$

This means that the set S consists of all elements of the universe for which the predicate is true. Example: The definition $S = \{n \in \mathbb{Z} \mid n > 5\}$ means $n \in S$ if and only if n is an integer greater than 5. If the universe is assumed to be $\mathbb{Z}$, it can be left out of the definition, so that $S = \{n \mid n > 5\}$.

We can recast claims about set inclusions using quantifiers and predicates. Thus:

$$\begin{array}{lll} S \subseteq T & \text{is equivalent to} & \forall x\,((x \in S) \to (x \in T)) \\ & \text{is equivalent to} & \forall x \in S\,(x \in T) \\ S \not\subseteq T & \text{is equivalent to} & \exists x\,((x \in S) \wedge (x \notin T)) \\ & \text{is equivalent to} & \exists x \in S\,(x \notin T). \end{array}$$

As a general rule, we prove things about sets by working with the predicates that define them. We will see later that the equivalences for $S \subseteq T$ lead to a useful proof strategy. As with the case of quantifiers and predicates, proving $S \subseteq T$ means working with elements one at a time.

Sequences of Quantifiers. A sequence of quantifiers may appear in front of a predicate. The order in which the quantifiers appear is very important to the meaning of the statement. Here are some examples, using $\mathbb{Z}$ as universe.

- $\forall x\,\exists y\,(x > y)$. This statement is true. Once you pick an arbitrary x, you can find a particular value for y (such as $x - 1$) that is smaller than x. Remember that "pick an arbitrary x" means that you don't know anything about x except that it belongs to the universe (here the integers).

- $\exists x\, \forall y\, (x > y)$. This statement is false. Once you pick a particular x you can find integers y (such as $x+1$) that are not less than x. Hence not every integer y is less than x.

- $\exists x\, \exists y\, (x \neq y)$. This statement is true. You can pick a particular value of x and then pick a particular y that is not equal to x.

- $\forall x\, \forall y\, (x \neq y)$. This statement is false. Once you pick particular value of x, you will not be able to show that every integer y is different from x (because one of the values for y will be equal to x).

Negations of Quantifiers. It is important to understand how negation interacts with quantifiers. Here are the basic rules.

- $\neg\forall x\, P(x)$ is equivalent to $\exists x\, (\neg P(x))$.

- $\neg\exists x\, P(x)$ is equivalent to $\forall x\, (\neg P(x))$.

Example: To understand $\neg\exists x\, \forall y\, (x > y)$, we compute

$$\begin{aligned} \neg\exists x\, \forall y\, (x > y) \quad & \text{is equivalent to} \quad \forall x\, (\neg\forall y\, (x > y)) \\ & \text{is equivalent to} \quad \forall x\, \exists y\, \neg(x > y)) \\ & \text{is equivalent to} \quad \forall x\, \exists y\, (x \leq y)). \end{aligned}$$

The last statement is clearly true (for any x take $y = x+1$), so our original statement is true. This gives a clear way to see that $\exists x\, \forall y\, (x > y)$ (the second example given in "Sequences of Quantifiers") is false.

4 Proof Strategies

A *proof* starts with a list of *hypotheses* and ends with a *conclusion*. The proof shows the step-by-step chain of reasoning from hypotheses to conclusion. Every step needs to be justified. You can use any of the reasons below to justify a step in your proof:

- A hypothesis.

- A definition.

- Something already proved earlier in the proof.

- A result proved previously.

- A consequence of earlier steps according to a rule of inference. Some rules of inference are listed below.

Be sure to proceed one step at a time. Writing a good proof requires knowing definitions and previously proved results, understanding how the notation and the logic works, and having a bit of insight. It also helps to be familiar with some common strategies for different types of proofs.

Rules of Inference. The table below gives some general rules of inference. Statements in the first two columns are the *premises*; the statement in the third column is called the *consequence.*

These rules of inference say that if you know the premises are both true (either because you are assuming them as hypotheses or because you have already proved them), then you can conclude that the consequence is true as well. The bottom two rows of the table only require one premise for the consequence to hold. These rules of inference can be proved by truth tables.

Premise I	Premise II	Consequence	Name of Rule
A	$A \to B$	B	Modus ponens
$A \to B$	$\neg B$	$\neg A$	Modus tollens
$A \lor B$	$\neg B$	A	Disjunctive syllogism
$\neg A \to (B \land \neg B)$		A	Proof by contradiction
A		Any tautology of A	Equivalent statement

Proof Strategies for Quantifiers. Here is a list of strategies for proving the truth of quantified statements.

- $\exists x \in U\,(P(x))$. Give an example value of the variable x that, when plugged in to the predicate, makes $P(x)$ true. Example: To prove $\exists x\,(x > 12)$, you can simply indicate that setting $x = 14$ makes the predicate true.

- $\forall x \in U\,(P(x))$. Assume (as a hypothesis) that x has the properties of the universe, but don't assume anything more about it. Show as a conclusion that the predicate must be true for that (arbitrary) value of x.

- If you have a statement of the form $\forall x\,(P(x)$ OP $Q(x))$ or $\exists x\,(P(x)$ OP $Q(x))$, where OP is one of the logical operators $\lor$, $\land$, $\to$, or $\leftrightarrow$, then you can rewrite the statement $P(x)$ OP $Q(x)$ using any logical tautology. Example: Proving $\forall x\,((x \geq 1) \to (x^2 \geq 1))$ is equivalent to proving $\forall x\,((x^2 < 1) \to (x < 1))$ by the contrapositive tautology.

In proofs involving compound statements $P(x)$ OP $Q(x)$, both predicates must refer to the *same* value of x. You *cannot* distribute a quantifier across the two parts of a compound statement. For example, the statement

$$\forall x\,((x \text{ is even}) \lor (x \text{ is odd})),$$

is true because, after picking a specific value for x, the value must either even or odd. But if you distribute the quantifier, you would get a different (and false) statement

$$(\forall x\,(x \text{ is even }))\lor(\forall x\,(x \text{ is odd})).$$

It not true that all integers are even, and it is not true that all integers are odd, and the disjunction of two false statements is false.

Proof Strategies for Sets.

- (Membership) Prove that $x \in S$. Show that x has the properties that define membership in S.
- (Non-membership) Prove that $x \notin S$. Here are two strategies:
  - Show that x does not have one of the properties that define S.
  - Assume that x is in S, and derive a contradiction.
- (Inclusion) Prove that S is a subset of T, i.e., $S \subseteq T$. Take an arbitary element x of S. That is, x represents any specific member of S: you can assume x has the properties that define S, but you can't assume anything more about it. Then show that x must also be an element of T using the membership strategy described above. Remember that you can assume that x satisfies the defining properties of S.
- (Proper Inclusion) Prove that S is a proper subset of T, i.e., $S \subset T$. First prove that $S \subseteq T$. Then find a specific example of an element x such that $x \in T$ but $x \notin S$.
- (Equality) Prove that S equals T, i.e., $S = T$. First prove that $S \subseteq T$. Then prove that $T \subseteq S$.

Proofs by Induction. If the universe consists of the natural numbers $\mathbb{N}$, then you can prove a statement of the form $\forall n\,(P(n))$ using induction. Here, we will assume that $\mathbb{N} = \{1, 2, 3, \ldots\}$. There are two proof-by-induction strategies.

A proof by *weak induction* (also called simply *induction*) has two parts:

- (Base Case) Show that $P(n)$ is true for the smallest value of n, here $n = 1$. This means plugging $n = 1$ into the predicate and showing that the predicate holds for this particular value.
- (Inductive Step) Show that $\forall n\,(P(n) \rightarrow P(n+1))$. Recall that a proof involving a universal quantifier starts by referring to an arbitrary value of the universe, here an integer $n \in \mathbb{N}$. Then assume $P(n)$ and show that $P(n+1)$ must be true. That is, your proof must show the chain of reasoning between the hypothesis $P(n)$ and the conclusion $P(n+1)$, for an arbitrary value of n.

After you have proved the two parts of an inductive proof, the Principle of (Weak) Induction allows you to conclude that $\forall n\,(P(n))$ is true.

A proof by *strong induction* (also called *complete induction*) only one part:

- (Inductive Step) Show that $\forall n\,((\forall k < n\,(P(k))) \rightarrow P(n))$. This means you pick an arbitrary $n \in \mathbb{N}$ and assume that $P(k)$ is true for all $k < n$ in $\mathbb{N}$. Then prove that $P(n)$ is true. In other words, with the hypothesis that $P(k)$ holds for all values of k strictly less than n, show the chain of reasoning leading to the conclusion $P(n)$. Note it is a property of the universal quantifier that the statement $\forall k < n(P(k))$ is automatically true if its universe is empty (i.e., if there are no natural numbers $k < n$).

After you have proved the inductive step, the Principle of Strong (or Complete) Induction allows you to conclude that $\forall n\,(P(n))$ is true.

In both weak and strong induction, $\mathbb{N}$ can be replaced with sets of integers such as $\{0, 1, 2, 3, \ldots\}$ or $\{2, 3, 4, \ldots\}$ that have a smallest element and contain $n+1$ whenever they contain n. The basis case in weak induction would plug in the smallest element of the universe rather than 1.

5 Sample Proofs

Here we give some proofs to illustrate various proof strategies.

Proof 1. Let A, B, C be sets. Prove the distribution law for $\cup$ over $\cap$, which states $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Proof. The proof has two parts because we want to prove two sets are equal.

To prove $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$, take $x \in A \cup (B \cap C)$. Then we have a series of implications

$x \in A \cup (B \cap C)$	hence	$(x \in A) \vee (x \in B \cap C)$	Def $\cup$
	hence	$(x \in A) \vee ((x \in B) \wedge (x \in C))$	Def $\cap$
	hence	$((x \in A) \vee (x \in B)) \wedge ((x \in A) \vee (x \in C))$	Dist
	hence	$(x \in A \cup B) \wedge (x \in A \cup C)$	Def $\cup$
	hence	$x \in (A \cup B) \cap (A \cup C)$	Def $\cap$.

This shows that $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$.

For the opposite inclusion $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$, take $x \in (A \cup B) \cap (A \cup C)$. The implications in the first part of the proof are reversible, so that $x \in A \cup (B \cap C)$. This proves $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$, and equality follows. QED

Proof 2. Prove that $\forall n \in \mathbb{Z}\,(n \text{ is even} \leftrightarrow n^2 \text{ is even})$.

Proof. Fix an arbitrary $n \in \mathbb{Z}$. Then we need to prove that n is even $\leftrightarrow n^2$ is even. The proof has two parts because we want to prove an equivalence.

Take $n \in \mathbb{Z}$ and assume n is even. By the definition of even, this means $n = 2m$ for some $m \in \mathbb{Z}$. Then

$$n^2 = (2m)^2 = (2m)(2m) = 2(2m^2),$$

which shows that n^2 is even.

Next take $n \in \mathbb{Z}$ and assume n^2 is even. We prove that n is even by contradiction. So assume n is not even, i.e., n is odd. This means $n = 2m + 1$ for some $m \in \mathbb{Z}$. Then

$$n^2 = (2m+1)^2 = (2m+1)(2m+1) = 4m^2 + 4m + 1 = 2(2m^2 + 2m) + 1,$$

which shows that n^2 is odd. This contradicts our assumption that n^2 is even, and it follows that n must be even. QED

Proof 3. Consider the universe $\mathbb{N} = \{1, 2, 3, \ldots\}$ of natural numbers. Fix $k \in \mathbb{N}$ and define S_k to be the set of natural numbers that are divisible by k. That is,

$$S_k = \{n \in \mathbb{N} \mid \exists m \in \mathbb{N}\, (n = k \cdot m)\}.$$

For example,

$$S_4 = \{4, 8, 12, 16, \ldots\}.$$

Prove that if $k = 2\ell$, then $S_k \subseteq S_\ell$.

Proof. Our hypotheses are listed below. We need to introduce different notation for the sets so we won't confuse their members.

1. $S_k = \{n \in \mathbb{N} \mid \exists m \in \mathbb{Z}\, (n = k \cdot m)\}$.
2. $S_\ell = \{p \in \mathbb{N} \mid \exists q \in \mathbb{Z}\, (p = \ell \cdot q)\}$.
3. $k = 2\ell$.

The conclusion we are aiming for is $S_k \subseteq S_\ell$. Our strategy is to first rewrite this inclusion in terms of predicates and quantifiers to obtain the equivalent statement

$$\forall n \in S_k\, (n \in S_\ell).$$

The proof strategy is thus to take an arbitrary value of n that has the properties that define membership in S_k, and show that n must also have the properties that define membership in S_ℓ. We do this as follows.

Start with an arbitrary value of $n \in S_k$. By the definition of S_k we know that $\exists m \in \mathbb{Z}\, (n = k \cdot m)$ for this n. Therefore $n = k \cdot m$ for some $m \in \mathbb{N}$. Since $k = 2\ell$ (by hypothesis), we conclude that

$$n = k \cdot m = (2\ell) \cdot m = \ell \cdot (2m),$$

where the last equality uses the associative and commutative properties of multiplication that you learned in middle school. Let $q = 2m \in \mathbb{N}$. Then $n = \ell \cdot q$, where $q \in \mathbb{N}$. This implies $n \in S_\ell$ by the definition of S_ℓ.

Therefore we can conclude that $S_k \subseteq S_\ell$. QED

Proof 4. Prove that for all n in the universe $\mathbb{N} = \{1, 2, 3, \ldots\}$, the sum of the first n odd positive integers is equal to n^2.

Before beginning the proof, observe that the first n odd positive integers are

$$2 \cdot \underline{1} - 1 = 1, \quad 2 \cdot \underline{2} - 1 = 3, \quad 2 \cdot \underline{3} - 1 = 5, \ldots, 2\underline{n} - 1.$$

where the underlined number tells us that we have the first, second, third, ..., nth odd integer. Thus the sum of the first n odd positive integers is the number

$$S_n = 1 + 3 + 5 + \cdots + (2n - 1).$$

For example, the fifth odd integer is $2 \cdot 5 - 1 = 9$, so that

$$S_5 = 1 + 3 + 5 + 7 + 9 = 25 = 5^2.$$

We need to prove that $\forall n \, (S_n = n^2)$.

Proof. Our strategy is to use weak induction for the proof.

Base Case: The smallest natural number is 1. We need to show that $S_1 = 1^2$. This is true since plugging $n = 1$ into the definition of S_n gives $S_1 = 1$.

Inductive Step: Our hypothesis is that the predicate holds for an arbitrary but fixed value of n, that is, $S_n = n^2$. Our goal is to show that the conclusion $S_{n+1} = (n+1)^2$ must also hold.

Our strategy is to start from the hypothesis $S_n = n^2$ and use a series of implications justified by algebra. We first add $2(n + 1) - 1$ to each side of $S_n = n^2$ to obtain

$$S_n + 2(n + 1) - 1 = n^2 + 2(n + 1) - 1.$$

Since $2(n + 1) - 1$ is the $(n + 1)$st odd number, the left-hand side is S_{n+1} by the definitions of S_n and S_{n+1}. Hence we can rewrite the above equation as

$$S_{n+1} = n^2 + 2(n + 1) - 1.$$

We will not review the rules of algebra here, but you should be able to explain why the right-hand side of this equation simplifies to $(n + 1)^2$. Hence we obtain

$$S_{n+1} = (n + 1)^2.$$

Our inductive conclusion has been derived from our inductive hypothesis. Therefore $\forall n \, (S_n = n^2)$ is true by the Principle of Weak Induction. QED