Logic, Sets, and Proofs

David A. Cox and Catherine C. McGeoch
Amherst College

1 Logic

Logical Statements. 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 in the following ways to form new logical statements.

Operation	Name	Notation	Alternate Notation
and	Conjunction	$A \wedge B$	A and B
or	Disjunction	$A \vee B$	A or B
not	Negation	$\neg A$	not A
implies	Implication	$A \Rightarrow B$	A implies B *or* if A, then B
if and only if	Equivalence	$A \Leftrightarrow B$	A iff B

Equivalent Statements. Here is a list of common logical equivalences. In a proof, you can replace a statement in the first column with the corresponding statement in the second column, and vice versa. Here, T (resp. F) stands for something known to be true (resp. false).

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 $\vee$
$A \vee \mathrm{F}$	A	F is identity for $\vee$
$A \wedge \mathrm{T}$	A	T is identity for $\wedge$
$A \vee \neg A$	T	law of excluded middle
$A \wedge \neg A$	F	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 $\mathbb{N}$. 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 $\{x \mid (x \in \mathbb{R}) \wedge (x > 0)\}$.

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 Quantifiers

A *variable* such as x represents some unspecified element from a fixed set U, often called the *universe*. For a logical statement that involve x, the truth of the statement depends on the particular value of x. Example: $x > 1$ for $x \in \mathbb{R}$. Here, the universe is $\mathbb{R}$. Note that $x > 1$ is true for $x = 2$ but false for $x = 0$.

We combine *quantifiers* to form statements about members of the universe 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,

  $P(x)$ 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 $P(x)$ 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 $\mathbb{Z}$, we can write $\exists x\,(x > 5)$ instead of $\exists x \in \mathbb{Z}\,(x > 5)$.

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

Defining Sets. A logical statement $P(x)$ that depends on 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 $P(x)$ 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. Thus:

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

As a general rule, we prove things about sets by working with the statements 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, proving $S \subseteq T$ means working with elements one at a time.

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 $\neg\forall x\,(x^2 > 0)$ (here $x \in \mathbb{R}$), we compute

$$\begin{array}{lll} \neg\forall x\,(x^2 > 0) & \text{is equivalent to} & \exists x\,(\neg(x^2 > 0)) \\ & \text{is equivalent to} & \exists x\,(x^2 \leq 0). \end{array}$$

The last statement is true, as can be seen by taking $x = 0$.

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 row of the table only requires one premise for the consequence to hold.

Premise I	Premise II	Consequence
A	$A \Rightarrow B$	B
$A \Rightarrow B$	$\neg B$	$\neg A$
$A \vee B$	$\neg B$	A
$\neg A \Rightarrow (B \wedge \neg B)$		A

The bottom row is called *proof by contradiction*.

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, makes $P(x)$ true. Example: To prove $\exists x\,(x > 12)$, you can simply indicate that setting $x = 14$ makes $x > 12$ 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 $P(x)$ must be true for that (arbitrary) value of x.

For a proof involving a compound statement $P(x) \vee Q(x)$ or $P(x) \wedge Q(x)$ or $P(x) \Rightarrow Q(x)$, make sure that both $P(x)$ and $Q(x)$ refer to the *same* value of x. You *cannot* distribute a quantifier across the two parts of a compound statement. For example, the statement

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

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

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

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) Strategy to prove $x \in S$: Show that x has the properties that define membership in S.
- (Non-membership) Strategy to prove $x \notin S$: Here are two strategies:
  - Show directly that x does not have one of the properties that define S.
  - Assume that x is in S, and derive a contradiction.
- (Inclusion) Strategy to prove 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.
- (Equality) Strategy to prove 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 $\mathbb{N} = \{1, 2, 3, \ldots\}$.

A proof by induction has two parts:

- (Base Case) Show that $P(n)$ is true for the smallest value of n, here $n = 1$. This means plugging in $n = 1$ and then showing that $P(1)$ is ture.
- (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 Induction allows you to conclude that $\forall n\,(P(n))$ is true.

In induction, $\mathbb{N}$ can be replaced with a set 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 base case is now the smallest element of the set.

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

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

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

where the underlined number tells us that we have the first, second, third, ..., odd integer. Hence $2n-1$ is the 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 induction.

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 $S_n = n^2$ holds for an arbitrary but fixed value of n. 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 Induction. QED