## Logic, Sets, and Proofs

## David A. Cox and Catherine C. McGeoch <br> Amherst College

## 1 Logic

Logical Statements. A logical statement is a mathematical statement that is either true or false. Here we denote logical statements with capital letters $A, B$. Logical statements be combined to form new logical statements as follows:

| Name | Notation |
| :--- | :--- |
| Conjunction | $A$ and $B$ |
| Disjunction | $A$ or $B$ |
| Negation | not $A$ |
|  | $\neg A$ |
| Implication | $A$ implies $B$ |
|  | if $A$, then $B$ |
|  | $A \Rightarrow B$ |
| Equivalence | $A$ if and only if $B$ |
|  | $A \Leftrightarrow B$ |

Here are some examples of conjunction, disjunction and negation:
$x>1$ and $x<3: \quad$ This is true when $x$ is in the open interval $(1,3)$.
$x>1$ or $x<3$ : This is true for all real numbers $x$.
$\neg(x>1)$ : This is the same as $x \leq 1$.
Here are two logical statements that are true:

$$
\begin{gathered}
x>4 \Rightarrow x>2 \\
x^{2}=1 \Leftrightarrow(x=1 \text { or } x=-1) .
\end{gathered}
$$

Note that " $x=1$ or $x=-1$ " is usually written $x= \pm 1$.

Converses, Contrapositives, and Tautologies. We begin with converses and contrapositives:

- The converse of " $A$ implies $B$ " is " $B$ implies $A$ ".
- The contrapositive of " $A$ implies $B$ " is " $\neg B$ implies $\neg A$ "

Thus the statement " $x>4 \Rightarrow x>2$ " has:

- Converse: $x>2 \Rightarrow x>4$.
- Contrapositive: $x \leq 2 \Rightarrow x \leq 4$.

Some logical statements are guaranteed to always be true. These are tautologies. Here are two tautologies that involve converses and contrapositives:

- $(A$ if and only if $B) \Leftrightarrow((A$ implies $B)$ and ( $B$ implies $A)$ ). In other words, $A$ and $B$ are equivalent exactly when both $A \Rightarrow B$ and its converse are true.
- $(A$ implies $B) \Leftrightarrow(\neg B$ implies $\neg A)$. In other words, an implication is always equivalent to its contrapositive. This is important to know.

There are many other tautologies. Some are pretty obvious, such as

$$
(A \text { or } B) \Leftrightarrow(B \text { or } A)
$$

(similarly for "and"), while others take a bit of thought, such as the following:

| Statement | Equivalent statement | Description |
| :--- | :--- | :--- |
| $A$ or $(B$ and $C)$ | $(A$ or $B)$ and $(A$ or $C)$ | "or" distributes over "and" |
| $A$ and $(B$ or $C)$ | $(A$ and $B)$ or $(A$ and $C)$ | "and" distributes over "or" |
| $\neg(A$ or $B)$ | $\neg A$ and $\neg B$ | De Morgan's law for "or" |
| $\neg(A$ and $B)$ | $\neg A$ or $\neg B$ | De Morgan's law for "and" |
| $A \Rightarrow(B \Rightarrow C)$ | $(A$ and $B) \Rightarrow C$ | conditional proof |

In a course that discusses mathematical logic, one uses truth tables to prove the above tautologies.

## 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 some 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 of all complex numbers is $\mathbb{C}$.
- The set with no elements is $\emptyset$, the empty set.

Another important set is the set of natural numbers, denoted $\mathbb{N}$. In our book,

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

However, you should be aware that in some other books, $\mathbb{N}=\{0,1,2,3, \ldots\}$.

## Basic Definitions and Notation about Sets.

- $x \in S: x$ 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: $\mathbb{Z} \subseteq \mathbb{R} \subseteq \mathbb{C}$ and $\mathbb{Z} \subseteq \mathbb{Z}$.
- $S \nsubseteq T$ : This means $\neg(S \subseteq T)$, i.e., some element of $S$ is not an element of $T$. Example: $\mathbb{R} \nsubseteq \mathbb{Z}$.
- $S \subset T$ : This means $S \subseteq T$ and $S \neq T$. 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 $S \subseteq T$ and $T \subseteq S$.

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 $\{x \mid x \in \mathbb{R}$ and $x>0\}$. We read "" as "such that".

Operations on Sets. Let $S$ and $T$ be sets.

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

$$
S \cup T=\{x \mid x \in S \text { or } x \in T\} .
$$

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

$$
S \cap T=\{x \mid x \in S \text { and } x \in T\} .
$$

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 $S \backslash T$.

## 3 Variables and Quantifiers

Often we are working with elements of a fixed set. In calculus, this fixed set is often the real numbers $\mathbb{R}$ or an interval $[a, b] \subseteq \mathbb{R}$. In linear algebra, the fixed set is often $\mathbb{R}^{n}, \mathbb{C}^{n}$ or an abstract vector space $V$ (all of these terms will eventually be defined). In the discussion that follows, this fixed set will be denoted $U$.

A variable such as $x$ represents some unspecified element from the fixed set $U$. Example: If $\mathbb{Z}$ is the fixed set, then " $x$ is even" is a statement that involves the variable $x$, and " $x>y$ " involves $x$ and $y$.

When a logical statement contains one or more variables, then the truth of the statement depends on which particular members of the fixed set are plugged in for the variables.

We combine quantifiers with statements involving variables to form statements about members of the fixed set $U$. If $P(x)$ is a statement depending on the variable $x$ from the fixed set $U$, then there are two basic types of quantifiers:

- $\forall x \in U(P(x))$. This universal quantifier means that for all (or for every or for each or for any) value of $x$ in $U, P(x)$ is true. Example: $\forall x \in \mathbb{R}(2 x=$ $(x+1)+(x-1))$.
- $\exists x \in U(P(x))$. This existential quantifier means that there exists a (or there is at least one) value of $x$ in $U$ for which $P(x)$ is true. Example: $\exists x \in \mathbb{Z}(x>5)$.

If the fixed set $U$ is understood, it may be omitted from the quantifier. For example, assuming that the fixed set is $\mathbb{Z}$, then the above statement can be written more simply as $\exists x(x>5)$.

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

Statements with Variables and Sets. A statement depending on a variable, such as $P(x)$, 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 $x$ of the fixed set for which the statement $P(x)$ 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 fixed set is assumed to be $\mathbb{Z}$, it can be left out of the definition, so that $S=\{n \mid n>5\}$.

We can recast set inclusions using quantifiers. Thus

$$
\begin{array}{ll}
S \subseteq T & \text { is equivalent to } \\
& \forall x(x \in S \Rightarrow x \in T) \\
\text { is equivalent to } & \forall x \in S(x \in T)
\end{array}
$$

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 and statements, proving $S \subseteq T$ means working with one element 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: For the fixed set is $\mathbb{R}$, we can understand $\neg \forall x(x>0)$ as follows:

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

The last statement is clearly true (take $x=-1$, for example), hence our original statement is true.

## 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 the rules of logic.

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.

Direct Proof. The simplest way to prove $A \Rightarrow B$ is to assume $A$ (the "hypothesis") and prove $B$ (the "conclusion"). See Proof 2 in Section 5 for a direct proof of $n$ is even $\Rightarrow n^{2}$ is even.

Proof by Contradiction. One way to prove $A \Rightarrow B$ is to assume that $A$ is true and $B$ is false. In other words, you assume that the hypothesis is true but the conclusion is false. Then you try to derive a contradiction. See Proof 2 is Section 5 for a proof by contradiction of $n^{2}$ is even $\Rightarrow n$ is even.

Proof by Contrapositive. A closely related strategy to prove $A \Rightarrow B$ is to instead prove its contrapositive $\neg B \Rightarrow \neg A$. Hence the stategy is to assume that $B$ is false and prove that this implies that $A$ is also false.

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 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 fixed set, but don't assume anything more about it. Show as a conclusion that the statement must be true for that (arbitrary) value of $x$.
- If you have a statement of the form $\forall x(P(x)$ or $Q(x))$ or $\exists x(P(x)$ or $Q(x))$, then you can rewrite the statement $P(x)$ or $Q(x)$ using any logical tautology. The same is true if "or" is replaced by "and", "implies" or "if and only if". Example: By the contrapositive tautology, proving $\forall x\left(x \geq 1 \Rightarrow x^{2} \geq 1\right)$ is equivalent to proving $\forall x\left(x^{2}<1 \Rightarrow x<1\right)$.


## Proof Strategies for Sets.

- (Membership) Strategy to prove $x \in S$ : Show that $x$ has the properties that define membership in $S$.
- (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 $T \subseteq S$.


## 5 Sample Proofs

Here we give two simple 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:

$$
\begin{array}{llll}
x \in A \cup(B \cap C) & \text { implies } & x \in A \text { or } x \in B \cap C & \text { Def } \cup \\
& \text { implies } & x \in A \text { or }(x \in B \text { and } x \in C) & \text { Def } \cap \\
& \text { implies } & (x \in A \text { or } x \in B) \text { and }(x \in A \text { or } x \in C) & \text { Dist } \\
& \text { implies } & x \in A \cup B \text { and } x \in A \cup C & \text { Def } \cup \\
\text { implies } & x \in(A \cup B) \cap(A \cup C) & \text { Def } \cap .
\end{array}
$$

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.

Proof 2. Prove that $\forall n \in \mathbb{Z}$ ( $n$ is even $\Leftrightarrow n^{2}$ 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.

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

$$
n^{2}=(2 m)^{2}=(2 m)(2 m)=2\left(2 m^{2}\right),
$$

which shows that $n^{2}$ is even.
Proof that $n^{2}$ is even $\Rightarrow n$ is even: Now 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 $n=2 m+1$ for some $m \in \mathbb{Z}$. Then

$$
n^{2}=(2 m+1)^{2}=(2 m+1)(2 m+1)=4 m^{2}+4 m+1=2\left(2 m^{2}+2 m\right)+1
$$

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

