Logic, Proofs, and Sets

JWR

Tuesday August 29, 2000

1 Logic

A statement of form

if P, then Q

means that Q is true whenever P is true. The **converse** of this statement is the related statement

if Q, then P.

A statement and its converse do not have the same meaning. For example, the statement

if $x = 2$, then $x^2 = 4$

is true while its converse

if $x^2 = 4$, then $x = 2$

is not generally true (maybe $x = -2$). The following phrases are all synonymous:

- *if P, then Q;*
- *P implies Q;*
- *Q, if P;*
- *P only if Q;*

The mathematical symbol $\implies$ is also used to mean *implies* as in

$$x = 2 \implies x^2 = 4.$$

The **contrapositive** of the statement *if P, then Q* is the statement *if not Q, then not P.* Unlike the converse, an implication and its contrapositive have the same meaning. For example, the two assertions

$$x = 2 \implies x^2 = 4 \quad \text{and} \quad x^2 \neq 4 \implies x \neq 2$$

have exactly the same meaning. The statement

P if and only if Q

has the same meaning as the statement

if P, then Q and if Q, then P.

This statement asserts a kind of equality – that P and Q have the same meaning: P is true exactly when Q is. The phrase *if and only if* is frequently abbreviated *iff*, especially in definitions. The mathematical symbol $\iff$ is also used to mean *if and only if* as in

$$x^2 = 4 \iff x = 2 \text{ or } x = -2.$$

This equation asserts that a number x satisfies the condition $x^2 = 4$ exactly when it satisfies the condition $x = \pm 2$: the two conditions are "equal". Sometimes we say

the conditions P and Q are equivalent

when we mean

P if and only if Q.

This is particularly the case when we have more than two conditions as in the following

Example. For any number x the following conditions are equivalent:

(1) $x^2 - 5x + 6 = 0$.

(2) Either $x = 2$ or $x = 3$.

(3) The number x is an integer between 1.5 and 3.5.

What this means is that if any one of the three conditions is true, then all of them are.

2 Proofs

One of the principal aims of this course is to teach the student how to read and, to a lesser extent, write proofs. A proof is an argument intended to convince the reader that a general principle is true in all situations. The amount of detail that an author supplies in a proof should depend on the audience. Too little detail leaves the reader in doubt; too much detail may leave the reader unable to see the forest for the trees. As a general principle, the author of a proof should be able to supply the reader with additional detail on demand. When a student writes a proof for a teacher, the aim is usually not to convince the teacher of the truth of some general principle (the teacher already knows that), but to convince the teacher that the student understands the proof and can write it clearly.

The "theorems" below show the proper format for writing a proof. In each of them you are supposed to imagine that the theorem to be proved has the indicated form. Notice how the key words *choose, assume, let,* and *therefore* are used in the proof. In these sample formats, the phrase "Blah Blah Blah" indicates a sequence of steps, each one justified by earlier steps. The symbol □ is used to indicate the end of the proof.

Theorem *If P, then Q.*

Proof: Assume P. Blah Blah Blah. Therefore Q. □

Theorem *P if and only if Q.*

Proof: Assume P. Blah Blah Blah. Therefore Q. Conversely, assume Q. Blah Blah Blah. Therefore P. □

Theorem *P(x) for all x.*

Proof: Choose x. Blah Blah Blah. Therefore P(x). □

Theorem *There is an x such that P(x).*

Proof: Let $x = \ldots$. Blah Blah Blah. Therefore P(x). □

Usually P and Q themselves involve the logical phrases *if*, *for all*, *there is.* In this case, the proof reflects that structure by using the corresponding key word *assume*, *choose*, *let.* For example, consider the following

Theorem. *For all a and b, if $a \neq 0$, then there is an x with $ax = b$.*

Proof: Choose a and b. Assume $a \neq 0$. Let $x = b/a$. Then $ax = a(b/a) = b$. Therefore $ax = b$. □

Of course, this proof is quite trivial and is given here only to illustrate the proper use of the key words *choose, assume, let,* and *therefore.* In general, every step in a proof is either an assumption (based on the structure of the theorem to be proved), an abbreviation (used to introduce notation to make the proof easier to read), or follows from earlier statements by the application of previously justified principles.

3 Sets

A set V divides the mathematical universe into two parts: those objects x that **belong** to V and those that don't. The notation $x \in V$ means x belongs to V. The notation $x \notin V$ means that x does not belong to V. The objects that belong to V are called the **elements** of V or the **members** of V. Other words roughly synonymous with the word *set* are *class*, *collection*, and *aggregate*. These longer words are generally used to avoid using the word *set* twice in one sentence. The situation typically arises when an author wants to talk about sets whose elements are themselves sets. One might write " the collection of all finite sets of integers", rather than "the set of all finite sets of integers".

3.1 Defining Sets by Enumeration

The simplest sets are **finite** and these are often defined by simply listing (**enumerating**) their elements between curly brackets. Thus if $V = \{2, 3, 8\}$ then $3 \in V$ and $7 \notin V$. Often an author uses dots as a notational device to mean "et cetera" and indicate that the pattern continues. Thus if

$$V = \{x_1, x_2, \dots, x_n\}, \tag{1}$$

then for any object y, the phrase "$y \in V$" and the phrase "$y = x_i$ for some $i = 1, 2, \dots, n$" have the same meaning; that is, one is true if and only if the other is. Having defined V by (1), we have

$$y \in V \iff y = x_1 \text{ or } y = x_2 \text{ or } \dots \text{ or } y = x_n.$$

In other words, the shorter phrase "$y \in V$" has the same meaning as the more cumbersome phrase "$y = x_1$ or $y = x_2$ or $\dots$ $y = x_n$".

The device of listing some of the elements with dots between curly brackets can also be used to define infinite sets provided that the context makes it clear what the dots stand for. For example, we can define the set of **nonnegative integers** by

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

and the set of **integers** by

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\},$$

and hope that the reader understands that $0 \in \mathbb{N}$, $5 \in \mathbb{N}$, $-5 \notin N$, $\frac{3}{5} \notin \mathbb{N}$, $0 \in \mathbb{Z}$, $5 \in \mathbb{Z}$, $-5 \in \mathbb{Z}$, $\frac{3}{5} \notin \mathbb{Z}$, etc.

3.2 Common Sets

Certain sets are so important that they have names:

$\emptyset$	(the empty set)
$\mathbb{N}$	(the nonnegative integers)
$\mathbb{Z}$	(the integers)
$\mathbb{Q}$	(the rational numbers)
$\mathbb{R}$	(the real numbers)
$\mathbb{C}$	(the complex numbers)

These names are almost universally used by mathematicians today, but in older books one may find other notations. Here are some true assertions: $0 \notin \emptyset$, $\frac{3}{5} \in \mathbb{Q}$, $\sqrt{2} \notin \mathbb{Q}$, $\sqrt{2} \in \mathbb{R}$, $x^2 \neq -1$ for all $x \in \mathbb{R}$, and $x^2 = -1$ for some $x \in \mathbb{C}$ (namely $x = \pm i$).

3.3 Sets and Properties

If V is a set and $P(x)$ is a property that either holds or fails for each element $x \in V$, then we may form a new set W consisting of all $x \in V$ for which $P(x)$ is true. This set W is denoted by

$$W = \{x \in V : P(x)\} \tag{2}$$

and called "the set of all $x \in V$ such that $P(x)$". Some authors write "|" instead of ":" as in

$$W = \{x \in V \mid P(x)\}.$$

This is a very handy notation. Having defined W by (2), we may assert that for all x

$$x \in W \iff x \in V \text{ and } P(x)$$

and that for all $x \in V$

$$x \in W \iff P(x).$$

Since the property $P(x)$ may be quite cumbersome to state, the notation $x \in W$ is both shorter and easier to understand.

Example. If $W = \{x \in \mathbb{N} : x^2 < 6 + x\}$, then $2 \in W$ (as $2^2 < 6 + 2$), $3 \notin W$ (as $3^2 \not< 6 + 3$), and $-1 \notin W$ (as $-1 \notin \mathbb{N}$).

Another notation that is used to define sets is

$$W = \{f(x) : x \in V\}.$$

This is to be understood as an abbreviation for

$$W = \{y : y = f(x) \text{ for some } x \in V\}$$

so that for any y

$$y \in W \iff y = f(x) \text{ for some } x \in V.$$

It may be difficult to decide if $y \in W$: the definition requires us to examine all solutions x of the equation $y = f(x)$.

Example. Using these notations the set W of even nonnegative integers may be denoted by any of the following three notations:

$$\begin{aligned} W &= \{0, 2, 4, \dots\} \\ &= \{m \in \mathbb{N} : m \text{ is divisible by } 2\} \\ &= \{2n : n \in \mathbb{N}\} \end{aligned}$$

Example. $\{x^2 : 2 < x < 3\} = \{y : 4 < y < 9\}$.

Example. $\{x : 2 < x < 3\} \subset \{x : 4 < x^2 < 9\}$, but these are not equal: the latter set contains negative numbers. The subset symbol $\subset$ is explained below.

Crude graphs can be used to get a rough idea of what a set of real numbers is. For example, to graph the set $V = \{x : y_0 < f(x) < y_1\}$ draw the two horizontal lines $y = y_0$ and $y = y_1$, plot the portion of the graph between those lines and project to the x-axis.

Example. $\{x : 1 < x^2 < 4\} = \{x : -2 < x < -1\} \cup \{x : 1 < x < 2\}$. (See Figure 1. The union symbol $\cup$ is explained below.)

To graph the set $W = \{f(x) : x_0 < x < x_1\}$ draw the two vertical lines $x = x_0$ and $x = x_1$, plot the portion of the graph between those lines, and project to the y-axis.

Example. $\{x^2 : -1 < x < 2\} = \{y : 0 \le y < 4\}$. (See Figure 1.)

Exercise. Simplify $\{x^2 : -2 < x < 3\}$.

Answer. $\{x^2 : -2 < x < 3\} = \{y : 0 \le y < 9\}$

Exercise. For each of the numbers $x = 0,\ -1,\ 3,\ 7/9,\ 9/7$ and each of the following sets V_i say whether $x \in V_i$. (There are $5 \times 4 = 20$ questions here.)

$$V_1 = \{1, 2, \dots, 9\} \qquad V_2 = \{x \in \mathbb{Z} : x^2 < 9\}$$

$$V_3 = \{x \in \mathbb{R} : x^2 < 9\} \qquad V_4 = \{x^2 : x \in \mathbb{R},\ \ x < 9\}$$

Answer. $3 \in V_1$; $0, -1 \in V_2$; $0, -1, 7/9, 9/7 \in V_3$; $0, 3, 7/9, 9/7 \in V_4$. In all other cases $x \notin V_i$.

3.4 Subsets

Definition. A set W is a **subset** of a set V, written

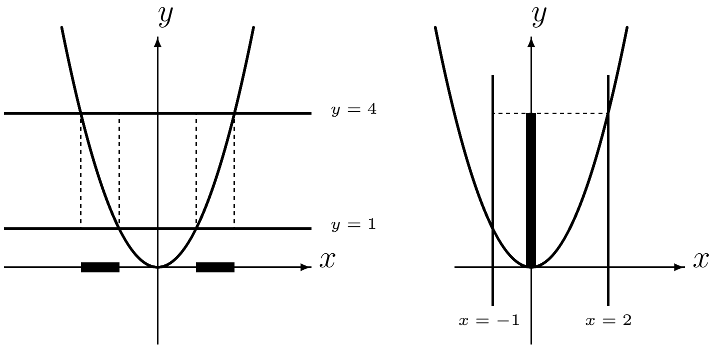
$$W \subset V,$$

iff every element of W is an element of V. The notation $W \not\subset V$ signifies that W is not a subset of V, that is, that there is at least one element of W which is not an element of V. For example,

$$\{1, 3, 4, 7\} \subset \{0, 1, 2, 3, 4, 7, 9\}$$

since every element on the left appears on the right. However,

$$\{1, 3, 4, 7\} \not\subset \{0, 1, 2, 4, 7, 9\}$$



$\{x : 1 \leq x^2 \leq 4\}$ $\{x^2 : -1 \leq x \leq 2\}$

Figure 1: The image and preimage of an interval

since $3 \in \{1, 3, 4, 7\}$ but $3 \notin \{0, 1, 2, 4, 7, 9\}$. To prove that $V \subset W$ we prove

$$x \in V \implies x \in W.$$

Note the following inclusions:

- $\mathbb{N} \subset \mathbb{Z}$ (every nonnegative integer is an integer),
- $\mathbb{Z} \subset \mathbb{Q}$ (every integer is a rational number),
- $\mathbb{Q} \subset \mathbb{R}$ (every rational number is a real number),
- $\mathbb{R} \subset \mathbb{C}$ (every real number is a complex number),
- $\emptyset \subset V$ (The empty set is a subset of every set V).

The last statement is true because *every* element x of the empty set lies in V – or indeed satisfies any other property – since there are no such elements x. However, do not confuse the empty set with the set whose only element is 0;

$$\emptyset \neq \{0\}$$

since $0 \in \{0\}$ but $0 \notin \emptyset$.

The following illustrates the proper format for proving a set inclusion. The phrase 'Blah Blah Blah' indicates a sequence of steps each of which follows from the previous ones.

Theorem $V \subset W$.

Proof: Choose $x \in V$. Blah Blah Blah. Therefore $x \in W$. □

Example. We prove $V \subset W$ where

$$V = \{y \in \mathbb{R} : 0 < y < 4\}, \qquad W = \{x^2 : -2 < x < 3\}.$$

Proof: *Choose* $y \in V$. Then $0 < y < 4$. *Let* $x = \sqrt{y}$. Then $-2 < x < 3$ and $y = x^2$. Hence, $y \in W$ as required. □

Example. Let $V = \{x^2 : x \in \mathbb{N},\ -2 < x < 3\}$ and $W = \{0, 1, 4, 9\}$. Then $W \not\subset V$ as $9 \in W$ but $9 \notin V$.

Exercise. For each of the following pairs of sets (V_i, V_j) decide if $V_i \subset V_j$. If so, prove it; if not, exhibit an x with $x \in V_i$ but $x \notin V_j$. (There are $4 \times (4 - 1) = 12$ problems here.)

$$\begin{aligned}
V_1 &= \{x \in \mathbb{R} : 1 < 3x + 7 < 20\} \\
V_2 &= \{x \in \mathbb{Z} : 1 < 3x + 7 < 20\} \\
V_3 &= \{3x + 7 : x \in \mathbb{R},\ \ 2 < x < 13/3\} \\
V_4 &= \{3x + 7 : x \in \mathbb{R},\ \ -2 < x < 13/3\}
\end{aligned}$$

Answer. It helps if you note that

$$V_1 = \{x \in \mathbb{R} : -2 < x < 13/3\}, \quad V_2 = \{-1, 0, 1, 2, 3, 4\},$$

$$V_3 = \{y \in \mathbb{R} : 13 < y < 20\}, \quad V_4 = \{y \in \mathbb{R} : 1 < y < 20\}.$$

Thus $V_2 \subset V_1$. $V_3, V_4 \not\subset V_1$ as $19 \in V_3, V_4$ but $19 \notin V_2$. Hence $V_3, V_4 \not\subset V_2$. $V_1 \not\subset V_2$ as $1/2 \in V_1$ but $1/2 \notin V_2$. $V_1 \not\subset V_3, V_4$ as $0 \in V_1$ but $0 \notin V_3, V_4$. $V_3 \subset V_4$ but $V_4 \not\subset V_3$ as $2 \in V_4$ but $2 \notin V_3$.

3.5 Boolean Operations

The **intersection**, $V \cap W$, of two sets V and W is the set of objects in both of them:

$$V \cap W = \{z : z \in V \text{ and } z \in W\}.$$

The **union**, $V \cup W$, of two sets V and W is the set of objects in one or the other of them:

$$V \cup W = \{z : z \in V \text{ or } z \in W\}.$$

The **difference**, $V \setminus W$, of two sets V and W is the set of objects in the first and not in the second:

$$V \setminus W = \{z : z \in V \text{ and } z \notin W\}.$$

For example, if

$$V = \{1, 3, 5\}, \quad W = \{2, 3\},$$

then

$$V \cap W = \{3\}, \;\; V \cup W = \{1, 2, 3, 5\}, \;\; V \setminus W = \{1, 5\}.$$

3.6 Equality of Sets

Definition. (Equality of Sets) Two sets V and W are **equal**, written $V = W$, iff $V \subset W$ and $W \subset V$, that is, iff every element of V is an element of W and every element of W is an element of V. To prove that $V = W$ we prove

$$x \in V \iff x \in W.$$

The following illustrates the proper format for proving a set equality. The phrase 'Blah Blah Blah' indicates a sequence of steps each of which follows from the previous ones.

Theorem $V = W$.

Proof: We show $V \subset W$. Choose $x \in V$. Blah Blah Blah. Therefore $x \in W$. This proves $V \subset W$.

We show $W \subset V$. Choose $x \in W$. Blah Blah Blah. Therefore $x \in V$. This proves $W \subset V$. □

Example. Let $f(x) = x^2 - 2x$. We show that $V = W$ where

$$V = \{y \in \mathbb{R} : -1 \le y < 8\}, \quad W = \{f(x) : -1 < x < 4\}.$$

Proof: *We show $V \subset W$. Choose $y \in V$.* Then $-1 \le y < 8$. Let $x = 1 + \sqrt{1+y}$. Then $y = f(x)$ and $-1 < 1 + \sqrt{0} \le x < 1 + \sqrt{9} = 4$. Hence $y \in W$. *This proves $V \subset W$.*

We show $W \subset V$. Choose $y \in W$. Then $y = f(x) = x^2 - 2x = (x-1)^2 - 1$ for some x with $-1 < x < 4$. There are two possibilities:

case (1) $-1 < x < 1$. In this case, $-2 < x - 1 < 0$ so $0 < (x-1)^2 < 4$ so $-1 < y = (x-1)^2 - 1 = f(x) < 3 < 8$

case (2) $1 \le x < 4$. In this case, $0 \le x - 1 < 3$ so $0 \le (x-1)^2 < 9$ so $-1 \le y = (x-1)^2 - 1 = f(x) < 8$

In either case $y \in V$. *This proves $W \subset V$.* □

If you draw the graph of $y = x^2 - 2x$, you'll see how I picked the numbers, but the logic of the proof has nothing to do with the graph.

Exercise. Let $V = \{n \in \mathbb{N} : n^2 + 7 < 6n\}$ and $W = \{2, 3, 4\}$. Prove that $V = W$.

Answer. We show $W \subset V$. Choose $n \in W$. If $n = 2$ then $n^2 + 7 = 11 < 12 = 6n$. If $n = 3$ then $n^2 + 7 = 16 < 18 = 6n$. If $n = 4$ then $n^2 + 7 = 23 < 24 = 6n$. In any case $n \in V$. This shows $W \subset V$. We show $V \subset W$. Choose $n \in V$. Then $n^2 + 7 < 6n$ and $n \in \mathbb{N}$. Hence $3 - \sqrt{2} < n < 3 + \sqrt{2}$. Since n is an integer, we must have $n \in W$. This shows $V \subset W$.

4 Sample worked problem

The quality of your writing will constitute an important component of your grade. You should never assume that your reader knows anything about a problem beyond what appears on the work you hand in. In particular, when you write homework you should not assume that the reader has access to the book – if you write only a problem number the reader will not know what the problem asks. Here is a solution to problem 6 on page 28 in the style that I want.

Problem 6. *Suppose that*

$$m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}, \qquad n = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k} \tag{1}$$

where $p_1, p_2, \dots, p_k$ are distinct primes and the exponents $a_1, \dots, b_k$ are nonnegative integers. Then the greatest common divisor (m, n) of the integers m and n is given by the formula

$$(m, n) = p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k} \tag{2}$$

where $c_i = \min(a_i, b_i)$ for $i = 1, 2, \dots, k$. For example,

$$(2^3 5^2 7^1, 2^5 3^8 5) = (2^3 3^0 5^2 7^1, 2^5 3^8 5^1 7^0) = 2^3 3^0 5^1 7^0 = 2^3 5.$$

Proof: Denote the right hand side of (2) by f. According to the definition on page 23 we must show three things:

(a) $f > 0$.

(b) $f|m$ and $f|n$.

(c) if $d|m$ and $d|n$ then $d|f$.

Condition (a) holds because $p_i > 1$ according to the definition of prime number given on page 26 and a product (in particular a power) of positive numbers is positive. Condition (b) holds because $m = fr$ and $n = fs$ where

$$r = p_1^{a_1 - c_1} p_2^{a_2 - c_2} \cdots p_k^{a_k - c_k}, \qquad s = p_1^{b_1 - c_1} p_2^{b_2 - c_2} \cdots p_k^{b_k - c_k}.$$

(The numbers r and s are integers because the exponents are nonnegative: $c_i = \min(a_i, b_i) \le a_i$ and $c_i = \min(a_i, b_i) \le b_i$.) To prove (c) assume that $d|m$ and $d|n$; we must show that $d|f$. By property (c) of Lemma 1.5.2 any prime which divides d also divides m and n so the unique prime factorization (see Theorem 1.5.8) of d has the form

$$d = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}.$$

As $d|m$ and $d|n$ there are integers u and v with $m = du$ and $n = dv$. From $u|m$ and $v|n$ it follows (again by property (c) of Lemma 1.5.2) that

$$u = p_1^{x_1} p_2^{x_2} \cdots p_k^{x_k}, \qquad v = p_1^{y_1} p_2^{y_2} \cdots p_k^{y_k}$$

where $x_1, \dots, y_k$ are nonnegative integers. Thus

$$m = du = p_1^{e_1+x_1} p_2^{e_2+x_2} \cdots p_k^{e_k+x_k}, \qquad n = dv = p_1^{e_1+y_1} p_2^{e_2+y_2} \cdots p_k^{e_k+y_k}. \quad (3)$$

By the uniqueness of the prime factorization (Theorem 1.5.8) and (1) and (3) we get

$$a_1 = e_1 + x_1,\ a_2 = e_2 + x_2,\ \dots,\ a_k = e_k + x_k$$

and

$$b_1 = e_1 + y_1,\ b_2 = e_2 + y_2,\ \dots,\ b_k = e_k + y_k.$$

Hence $e_i \le a_i$ and $e_i \le b_i$ so $e_i \le c_i = \min(a_i, b_i)$ for $i = 1, 2, \dots, k$. Thus $f = dz$ where

$$z = p_1^{c_1-e_1} p_2^{c_2-e_2} \cdots p_k^{c_k-e_k};$$

in other words $d|f$ as required. □

Note that I can follow the above proof without having the book before me. I can even infer from what is written above that part (c) of Lemma 1.5.2 says that *If $x|y$ and $y|z$, then $x|z$.* The above proof is too detailed for a book (it is hard to see the forest for the trees) but appropriate for a student assignment (the teacher is in no doubt that the student understands).