The Process of Mathematical Proof

Introduction. Mathematical proofs use the rules of logical deduction that grew out of the work of Aristotle around 350 BC. In Math 213 and other courses that involve writing proofs, there may have been an *unspoken* assumption that you and everyone else would instinctively follow those rules. Along the way you have likely acquired an understanding of what is — and is not — acceptable mathematical argument. To make sure that everyone starts this course from the same logical point of view, this document discusses explicitly the ground rules of mathematical proof. You may find it a handy reference, especially at the start, to check your reasoning.

A fundamental precept of deductive reasoning is the *law of the excluded middle*: every statement is either true or false, never both. Mathematics classifies statements about mathematical ideas and sets as true or false. The most basic true statements are the *axioms* of the particular branch of mathematics under study. They are assumptions that specify the basic relations among the fundamental *undefined objects* of the theory. Math 216 deals with abstract algebraic structures, and as an example the first axiom appears on p. 4 of the text:

Well-Ordering Principle: Every nonempty subset of the set $\mathbf{Z}^+$ of positive integers has a smallest element.

Another example you've already seen if you have taken Math 215 is the *associative law of addition* in a vector space V over a field F:

$$\text{for all vectors } u, v, w \in V,\ u + (v + w) = (u + v) + w.$$

Among the true statements in a mathematical theory besides the axioms are *definitions*, which introduce more objects in terms of the fundamental ones. For instance, recall that the negative $-v$ of a vector in V is by definition $(-1)v$. (If you haven't yet taken Math 215, think of V as a real vector space such as $\mathbf{R}^3$.)

Mathematical systems consist of axioms, definitions, and further true statements that are deducible from the basic axioms and definitions: lemmas, theorems, propositions (little theorems) and corollaries (simple consequences of theorems and propositions). For example, the following proposition is a simple con-

sequence of the axioms for a vector space V.

(1) if $\alpha v = 0$, then either the scalar α or the vector v must be zero.

Tautologies. The simplest true statements in any theory are *tautologies*, which are true by virtue of their form or meaning. An example is the statement that for every real number x, $x = \frac{1}{2}(2x)$. In mathematical systems, such statements are seldom very interesting. However, logical tautologies do provide the *standard argument forms* for valid mathematical proofs. Those forms involve the basic logical connectives *or*, *and*, *not*, *if...then* and *if and only if.* Recall that *or* has the *inclusive* meaning:

- *P or Q* (symbolically, $P \vee Q$) is true precisely in case at least one of the statements P or Q holds true.

Such assignment of truth values applies to the other connectives as well:

- *P and Q* (symbolically, P & Q or $P \wedge Q$) is true precisely in case *both* P and Q are true.
- *not P* (symbolically, $\neg P$) is true precisely in case P is false.
- *If P then Q* (equivalently, *P implies Q* or, symbolically, $P \Rightarrow Q$) is true in all cases *except* when P is true but Q is false.
- *P if and only if Q* (symbolically, $P \Longleftrightarrow Q$) is true precisely in case P and Q have the same truth values — that is, both are true or both are false.

Direct Proof. Logical tautologies provide the *argument forms* for proofs. The most common of those is *modus ponens*:

$$\big[(P \Rightarrow Q) \ \& \ P\big] \Rightarrow Q.$$

Most mathematical theorems are *if...then* assertions: $P \Rightarrow Q$, where P is the *hypothesis* and Q is the *conclusion.* Modus ponens allows you to conclude that a statement Q holds if you know that a statement P is true and there is a theorem that $P \Rightarrow Q$.

Since $P \Rightarrow Q$ is true in all cases except for P true and Q false, the most common way to prove a theorem $P \Rightarrow Q$ is to *suppose* the truth of the hypothesis P and to show that the truth of the conclusion Q must then follow. This usually proceeds by means of repeated use of modus ponens on a sequence of intermediate results $P \Rightarrow P_1$, $P_1 \Rightarrow P_2, \ldots, P_{n-1} \Rightarrow P_n$, and $P_n \Rightarrow Q$.

Another common method of proof uses the logical equivalence of $P \Rightarrow Q$ and $\neg Q \Rightarrow \neg P$. (The statement $\neg Q \Rightarrow \neg P$ is the *contrapositive* of $P \Rightarrow Q$.) This argument form rests on the fact that

$$(P \Longrightarrow Q) \Longleftrightarrow (\neg Q \Longrightarrow \neg P)$$

is a tautology. Use of this method to prove $P \Rightarrow Q$ starts by assuming the denial of the conclusion Q, and then reasoning to establish the denial of the hypothesis P.

An example is the argument on p. 4 of the text to justify the method of *proof by mathematical induction* of a statement $S(n)$ about natural numbers n. In Theorem 0.2 that method takes the form $P \Rightarrow Q$, where

- P is "(i) $S(1)$ is true and (ii) $S(m+1)$ is true whenever $S(m)$ is true for $m \geq 1$,"
- Q is "$S(n)$ is true for all natural numbers n."

(Study the statement of Theorem 0.2 to check that it really is expressible in this way!)

The proof of Theorem 0.2 begins by assuming $\neg Q$, that is, that $S(n)$ fails to hold for at least one positive integer n. It then uses the above *well-ordering principle* for the positive integers, on the set $T = \{n \mid n \in \mathbf{Z}^+ \text{ and } S(n) \text{ is false}\}$. From the assumption that $S(n)$ is false for at least one positive integer n, it follows that T is nonempty. The well-ordering principle then guarantees the existence of a smallest element n_0 in T, that is, a smallest positive integer n_0 for which $S(n)$ is false. By hypothesis (i), $n_0 \neq 1$, so $n_0 - 1$ is still a positive integer, and of course is *smaller* than n_0. Then $S(n_0 - 1)$ must be *true*, because n_0 is the *smallest* positive integer for which S is false. But in that case, P is false (that is, $\neg P$ holds), since P is false for the positive integer $m = n_0 - 1$. Why? Because (ii) is violated:

$S(n_0 - 1)$ is true, but $S(n_0 - 1 + 1) = S(n_0)$ is *not*. Theorem 0.2 then follows by an appeal to the above argument form: $\neg Q$ implies $\neg P$ is equivalent to $P \Rightarrow Q$.

Compare the last paragraph to the text's remarks, which suggest that the argument amounts to a proof by contradiction. That isn't quite right, as the following discussion of *indirect proof* aims to explain.

Indirect proof. This method rests on the tautology

$$\Big[R \;\&\; (\neg(P \Longrightarrow Q) \Longrightarrow \neg R)\Big] \Longrightarrow \Big[P \Longrightarrow Q\Big], \tag{2}$$

which may not be immediately clear but is easy to establish by making its truth table. More informally, the logic goes as follows. If

R holds (so that $\neg R$ is false),

and

$\neg(P \Longrightarrow Q)$ implies $\neg R$,

then

$\neg(P \Longrightarrow Q)$ must be false: that is, $(P \Longrightarrow Q)$ must be true!

The falsity of $\neg(P \Longrightarrow Q)$ comes from the fact that a true statement cannot imply the false statement $\neg R$.

A proof of a theorem $P \Longrightarrow Q$ by contradiction starts by assuming the truth of both P and $\neg Q$ (the denial of the conclusion Q that you want to establish). This amounts to assuming the denial of $P \Rightarrow Q$, which is logically equivalent to $P \;\&\; \neg Q$. (Remember the fourth bullet on p. 2: $P \Longrightarrow Q$ is true in *all other situations*.) If from this start you can derive the denial of some known true statement R, then you have established the hypothesis of (2), so also then have established its conclusion — precisely what you want to prove! The following famous argument (which reputedly cost Pythagoras his life!) illustrates these ideas.

Theorem. The real number $\sqrt{2}$ is irrational.

Proof. Here, $P \Rightarrow Q$ is the statement

$$\text{If } x = \sqrt{2} \text{ then } x \text{ is not a rational number.}$$

The proof starts by assuming to the contrary that $\sqrt{2}$ is a rational number, that is, $\neg(P \Rightarrow Q)$. You also assume (as the statement R) that $\sqrt{2} = p/q$, where p and

q are relatively prime (that is, *have no common prime factors*), so that the rational number is in lowest terms. You then square the equation to obtain $2q^2 = p^2$. This says at once that *2 is a factor of p*, so $p = 2k$ for some integer k say. But then

$$2q^2 = p^2 = 4k^2 \Longrightarrow q^2 = 2k^2,$$

which implies that *2 is also a factor of q*. Thus, the prime 2 *is a common factor* of p and q, that is, $\neg R$ holds. This reasoning thus establishes that $\neg(P \Rightarrow Q)$ implies $\neg R$. In view of (2), that is enough to complete the proof of the theorem by contradiction: $P \Rightarrow Q$ holds.

Multiple Conclusions. To prove a theorem of the form $P \Rightarrow (Q \vee R)$, you normally start by supposing that P holds and assuming the negation of Q or R. You then argue to establish the *truth* of the other alternative. This method of proof rests on the tautology

(3) $$\big[(P \;\&\; \neg Q) \Longrightarrow R\big] \Longrightarrow \big[P \Longrightarrow (Q \vee R)\big],$$

which may not be obvious, but can be seen as follows. The only way it could be false would be for

(4) $$(P \;\&\; \neg Q) \Longrightarrow R \text{ to be true}$$

but $P \Longrightarrow (Q \vee R)$ to be false (second bullet on p. 2 again). That in turn would require P to be true but $Q \vee R$ to be false. But by the first bullet on p. 2, the only way for $Q \vee R$ to be false is for *both* Q and R *to be false*. That would make $(P \;\&\; \neg Q) \Longrightarrow R$ false, because $P\&\neg Q$ would be true, but R would be false. That conflicts with (4), so it's impossible for (3) to be false!

This is the approach to proving (1) above in linear algebra.

Counterexamples. Almost as important as being able to prove theorems is the ability to construct counterexamples. If someone asserts that the square of every prime is odd, for instance, nothing is quite as effective as asking the person to consider the prime 2! Most mathematical theorems implicitly involve the universal quantifier *for all*, the symbol for which is $\forall$. For instance, the elementary linear algebra theorem (1) is really the formal statement that

> for all α and all v, if α is a scalar and v is a vector and $\alpha v = 0$, then $\alpha = 0$ or $v = 0$.

The logical role of counterexamples comes from the *denial* of a statement that begins with "for all."

- The negation of *for all x P(x)* is: *there exists at least one x such that* $\neg P(x)$, that is, *there exists at least one x for which* $P(x)$ *is false.*

Thus *to show the falsehood of a universally quantified conjecture* of the form for all x $P(x)$, *you need only produce a single x for which* $P(x)$ *is false*. The fact that the square of the single prime 2 is even thus suffices to disprove the conjecture above that the square of every prime is odd. Note: if you became confused and thought that to disprove the conjecture you had to establish that *for all* primes p the square of p is even, you would be stymied!

The law of double negation — that the negation of the negation of P is tautologically equivalent to P — gives the following rule for the denial of an existence assertion.

- The negation of *there exists at least one x such that* $Q(x)$ is: *for all x* $\neg Q(x)$, that is, *for all x* $Q(x)$ *is false.*

The definition of limit. Both the above kinds of denial arise in working with functions $f : R \to R$ that have no limit at a point $x = c$. Recall the definition of $\lim_{x \to c} f(x) = L$:

(5) For every $\varepsilon > 0$, there is some $\delta > 0$ such that for all x
if $0 < |x - c| < \delta$, then $|f(x) - L| < \varepsilon$.

The following symbolic rendering of (5) underscores its complexity.

$$\exists L \ \forall \varepsilon \ \exists \delta \ \forall x \ \big[(0 < |x - a| < \delta) \Longrightarrow |f(x) - L| < \varepsilon\big].$$

To show that a certain function fails to have a limit at a point a, you have to negate (5). According to the negation rules above, that amounts to establishing the following.

> For every real number L, there is some $\varepsilon > 0$ such that for all $\delta > 0$ there is at least one real number x for which
>
> $$0 < |x - a| < \delta \text{ and yet } |f(x) - L| > \varepsilon.$$

Example. The function f with formula $f(x) = 1/x$ has no limit at $x = 0$. To show that from (5), consider any real number L. Then you must show that for some particular value of ε, for any $\delta > 0$ there is some real number x for which $0 < |x - 0| < \delta$ but $|1/x - L| > \varepsilon$. (As Math 273 explains, it is enough to use $\varepsilon = 1$ and to pick some $x \neq 0$ in the interval $(-1, 1)$.)

While the *content* of this example is unrelated to the subject matter of Math 216, in writing up proofs and counterexamples you may sometimes need to apply the *process* of negating universally or existentially quantified statements.