

More Proofs

Dr. Holmes

September 4, 2009

1 Summary of Proof Strategies

1.1 Basic Logical Concepts

contradiction: I'm introducing a symbol \perp for a sentence which is false, read "contradiction".

negation: If P is a sentence, $\neg P$ means "It is not the case that P ", " P is false", "not P ".

conjunction: If P and Q are sentences, $P \wedge Q$ means " P and Q ".

disjunction: If P and Q are sentences, $P \vee Q$ means " P or Q (or both)". This is the default meaning of "or" in mathematical English.

implication: If P and Q are sentences, $P \rightarrow Q$ is read "if P then Q " or " P implies Q ". This is understood to be false only if P is true and Q is false: it is exactly equivalent to $\neg(P \wedge \neg Q)$ or to $\neg P \vee Q$. This is the default meaning of "if...then..." or "implies" in mathematical English.

biconditional: If P and Q are sentences, $P \leftrightarrow Q$ means " P if and only if Q ", or " P implies Q and Q implies P ". This is abbreviated " P iff Q ".

universal quantifier: $(\forall x.P(x))$ means "for all x , $P(x)$ " and $(\forall x \in A.P(x))$ means "for all x in the set A , $P(x)$ ".

existential quantifier: $(\exists x.P(x))$ means "for some x , $P(x)$ " or "there exists an x such that $P(x)$ ", and $(\exists x \in A.P(x))$ means "for some x in the set A , $P(x)$ ", or "there exists an x in A such that $P(x)$ ".

1.2 Proving sentences of these forms

In this subsection we have techniques for proving statements of each of these logical forms, and sample outlines of what such a proof (in a highly formalized style) would look like.

contradiction: To prove \perp , prove A and prove $\neg A$ (for some sentence A) [we certainly hope that we cannot do this except under bad assumptions!]

negation: To prove $\neg A$, assume A and prove \perp (which you can only do by proving some B and $\neg B$).

Goal: $\neg A$

Assume: A

Goal: contradiction

[proof of B]

[proof of $\neg B$]

completing a contradiction: B might be any statement.

conjunction: To prove $P \wedge Q$, prove P , then prove Q .

Goal: $P \wedge Q$

Goal 1: P

[proof of P]

Goal 2: Q

[proof of Q]

Notice that the single conjunction goal unpacks into two goals which each need to be proved separately.

disjunction: To prove $P \vee Q$, do one of four things (you do not need to do more than one!):

Method 1: Assume $\neg P$ (for the sake of argument) then prove Q ; when done with this proof of Q , one no longer can use the assumption $\neg P$, which is local to that proof.

Goal: $P \vee Q$

Assume: $\neg P$

Goal: Q
[proof of Q]

Notice that the assumption $\neg P$ and any conclusion proved using $\neg P$ (including the local conclusion Q) can only be used in the indented part of the proof.

Method 2: Assume $\neg Q$ (for the sake of argument) then prove P ; when done with this proof of P , one no longer can use the assumption $\neg Q$, as above.

Goal: $P \vee Q$
Assume: $\neg Q$
Goal: P
[proof of P]

Notice that the assumption $\neg Q$ and any conclusion proved using $\neg Q$ (including the local conclusion P) can only be used in the indented part of the proof.

Method 3: Notice that it is enough just to prove P .

Goal: $P \vee Q$
Goal: P
[proof of P]

Method 4: Notice that it is enough just to prove Q .

Goal: $P \vee Q$
Goal: Q
[proof of Q]

implication: To prove $P \rightarrow Q$, assume P (for the sake of argument), then prove Q . The assumption P can only be used in this local proof of Q .

Goal: $P \rightarrow Q$
Assume: P
Goal: Q
[proof of Q]

The assumption P and anything proved using it can only be used in the indented part of the proof.

An alternative strategy (proof by contrapositive) is to assume $\neg Q$ and then prove $\neg P$.

Goal: $P \rightarrow Q$

Assume: $\neg Q$

Goal: $\neg P$

[proof of $\neg P$]

biconditional: To prove $P \leftrightarrow Q$ one needs a proof with two parts: in the first part one assumes P for the sake of argument then proves Q ; in the second part one assumes Q for the sake of argument then proves P .

Goal: $P \leftrightarrow Q$

Part 1: Assume: P

Goal: Q

[proof of Q]

Part 2: Assume: Q

Goal: P

[proof of P]

One or both of the embedded proofs of $P \rightarrow Q$ and $Q \rightarrow P$ could be replaced with proofs by contrapositive.

universal quantifier: To prove $(\forall x.P(x))$, introduce an arbitrary object a (about which we may make no special assumptions; we should not have ever mentioned it before), and prove $P(a)$. After the end of this proof we should not refer to this a again.

To prove $(\forall x \in A.P(x))$, introduce an arbitrary object a (about which we may make no special assumptions; we should not have ever mentioned it before), assume $a \in A$ and prove $P(a)$. After the end of this proof we should not refer to this a again.

existential quantifier: To prove $(\exists x.P(x))$, find an object t such that you can prove $P(t)$.

To prove $(\exists x \in A.P(x))$, find an object t such that you can prove $t \in A$ and you can prove $P(t)$.

proof by contradiction: To prove any statement A at all: assume $\neg A$ and deduce a contradiction.

Goal: A

Assume: $\neg A$

Goal: contradiction

[proof of B]

[proof of $\neg B$]

where B can be any statement.

1.3 Using theorems, assumptions or conclusions of these forms

contradiction: If you have assumed or concluded \perp , you may assume or conclude any further conclusion A that you want (a false statement implies anything).

negation: If you have assumed or concluded $\neg\neg A$, you may conclude A .

The main use of a negative conclusion $\neg A$ is to see if you can also prove A and thus prove a contradiction (\perp).

Here is a proof fragment where a negative hyp $\neg A$ is used in this way.

$\neg A$

Goal: $\neg B$

Assume: B

Goal: contradiction

Goal: A (for the sake of a contradiction)

[proof of A]

(the point is that we now have a contradiction because $\neg A$ is already a conclusion above)

conjunction: If you have assumed or concluded $P \wedge Q$, you may also conclude P and you may also conclude Q .

disjunction: If you have assumed or concluded $P \vee Q$ and are trying to prove G , you can complete the proof using proof by cases: (case 1) assume P , then prove G ; (case 2) assume Q , then prove G .

Here is a bit of proof text:

$P \vee Q$

Goal: G

Case 1: Assume: P

Goal: G

[proof of G]

Case 2: Assume: Q

Goal: G

[proof of G]

implication: If you have assumed or concluded $P \rightarrow Q$, and have also assumed or concluded P , you can further conclude Q (rule of modus ponens).

(1) $P \rightarrow Q$

(2) P

Q , from (1) (2) by the rule of modus ponens

If you have assumed or concluded $P \rightarrow Q$, and have also assumed or concluded $\neg Q$, then you can further conclude $\neg P$. (modus tollens)

(1) $P \rightarrow Q$

(2) $\neg Q$

$\neg P$, from (1) (2) by the rule of modus tollens

If you have *just* the assumption or conclusion $P \rightarrow Q$ and it is unclear what to do next, try proving P (because if you do you can further conclude Q), or proving $\neg Q$ (because if you do you can further conclude $\neg P$).

Here is a proof fragment:

$A \rightarrow B$

Goal: $G \dots$

Goal: A (for the sake of proving B)
[proof of A]

B [this follows by m.p. from $A \rightarrow B$ above and the just given proof of A]

[rest of proof of G]

biconditional: Suppose you have assumed or concluded $P \leftrightarrow Q$.

If you have further assumed or concluded P , you can draw the further conclusion Q .

If you have further assumed or concluded Q , you can draw the further conclusion P .

If you have further assumed or concluded $\neg P$, you can draw the further conclusion $\neg Q$.

If you have further assumed or concluded $\neg Q$, you can draw the further conclusion $\neg P$.

universal quantifier: If you have assumed or concluded $(\forall x.P(x))$, you can further conclude $P(t)$ (where t is any object you can name).

If you have assumed or concluded $(\forall x.P(x))$ and also have assumed or concluded $t \in A$, you can further conclude $P(t)$ (where t is any object you can name).

existential quantifier: If you have assumed or concluded $(\exists x.P(x))$, you can introduce a new name w for a witness to this statement and assume $P(w)$. This name should not appear either in any earlier assumptions or conclusions nor in the assertion(s) you are trying to prove.

If you have assumed or concluded $(\exists x \in A.P(x))$, you can introduce a new name w for a witness to this statement and assume $w \in A$ and $P(w)$. This name should not appear either in any earlier assumptions or conclusions nor in the assertion(s) you are trying to prove.

copying assumptions and things proved: Of course if you currently assume A or have already proved A under your current assumptions you can say so:

...

[proof of A]

...

A has already been proved...

OR

...

Assume: A

...

we have A by assumption...

You do need to remember that assumptions can generally only be used in a specific part of a proof.

anything at all follows from a contradiction :

P

$\neg P$

Goal: Q

prove by contradiction...

Assume: $\neg Q$

Goal: contradiction

We have $P \wedge \neg P$ by assumptions above so we are done.

2 Examples of Proofs with Quantifiers

In this section we give proofs in mathematical English (with symbols as needed) with occasional lapses into logical notation to explain what is going on.

Definition: A natural number n is said to be *odd* iff there is a natural number k such that $2k+1 = n$. (This is assuming that natural numbers start with 0: if they start with 1 we need to say $2k - 1 = n$).

Notice that this can be written completely in mathematical notation:

$$(\exists k \in \mathbb{N}. 2k + 1 = n)$$

Theorem: The product of two odd numbers is odd.

Discussion: The underlying logical form of this statement is “For any natural numbers m and n , if m and n are odd, then $m \cdot n$ is odd.”

This could be written

$$(\forall m \in \mathbb{N}.(\forall n \in \mathbb{N}.m \text{ is odd} \wedge n \text{ is odd} \rightarrow m \cdot n \text{ is odd}))$$

Nested universal quantifiers can be collapsed together:

$$(\forall mn \in \mathbb{N}.m \text{ is odd} \wedge n \text{ is odd} \rightarrow m \cdot n \text{ is odd})$$

Though in English we might say “for all natural numbers m and $n \dots$ ”, notice that there is no occurrence of \wedge corresponding to this English use of the word “and”.

Proof: Let p, q be arbitrarily chosen natural numbers [to be plugged in for the variables m, n in the goal].

Goal: p is odd $\wedge q$ is odd $\rightarrow p \cdot q$ is odd.

Discussion: We just applied the strategy for proving a universal statement (twice). We could have called the arbitrarily chosen numbers m and n (so we didn’t have to rename things), and often it is convenient to do so (it would be fine here, for example).

We continue with the strategy for proving an implication.

Assume (1): p is odd $\wedge q$ is odd.

Goal: $p \cdot q$ is odd.

Discussion: A vitally important strategy is to unpack defined concepts. This goal can be restated as “for some k , $m \cdot n = 2k + 1$ ”. So we are proving an existential conclusion: our aim is to find a specific k such that $m \cdot n = 2k + 1$.

Rephrased Goal: Find k such that $m \cdot n = 2k + 1$.

Further Discussion: We can unpack the conjunction of assumptions above into two conclusions “ m is odd” and “ n is odd”. We also unpack the definition of “odd”, so we have existential hypotheses, to which we can introduce witnesses.

We conclude (2) m is odd and (3) n is odd from (1). (2) means “there is a k such that $m = 2k + 1$, so we can introduce a natural number u such that $m = 2u + 1$. (3) means “there is a

k such that $n = 2k + 1$ ", so we can introduce a natural number v such that $n = 2v + 1$. *It is an error commonly made by students to use the same letter for these two witnesses: always use a new letter for a witness to an existential hypothesis.*
 Now $m \cdot n = (2u + 1) \cdot (2v + 1) = 4uv + 2u + 2v + 1 = 2(2uv + u + v) + 1$, so setting $k = 2uv + u + v$ meets our goal. The proof is complete.

Another result which we prove in the same style is (like the previous one) a Math 187 exercise: the composition of two injective functions is injective. I'm going to factor out problems I had in the class presentation with domains and ranges by sticking to real numbers.

Definition: A function $f : \mathbb{R} \rightarrow \mathbb{R}$ is *injective* iff for any $x, y \in \mathbb{R}$, if $f(x) = f(y)$ then $x = y$.

Definition: If f and g are functions from the reals to the reals, $f \circ g$ is the function from the reals to the reals defined by $[f \circ g](x) = f(g(x))$, called the *composition* of f and g .

Theorem: The composition of two injective functions from the reals to the reals will be an injective function from the reals to the reals.

Discussion: This says $(\forall f, g. f \text{ is injective} \wedge g \text{ is injective} \rightarrow f \circ g \text{ is injective})$. It is a universally quantified statement.

Let f and g be arbitrarily chosen functions from the reals to the reals.

Assume (1): f is injective and g is injective.

Goal: $f \circ g$ is injective.

Discussion: What we have done so far is apply the strategy for proving a universally quantified statement, followed by the strategy for proving an implication. We now need to unpack definitions.

Restated Goal: For any x, y real numbers, $[f \circ g](x) = [f \circ g](y) \rightarrow x = y$.

Let x and y be arbitrarily chosen reals.

Assume (2): $[f \circ g](x) = [f \circ g](y)$

Goal: $x = y$

Discussion: You should see familiar logical strategies.

We know that (3) for all x, y , if $f(x) = f(y)$ then $x = y$, and we know that (4) for all x, y , if $g(x) = g(y)$ then $x = y$, from the hypothesis (1) above that f and g are injective (this is another example of the strategy “unpack definitions”).

We deduce $f(g(x)) = f(g(y))$ from (2) and the definition of composition.

we then deduce $g(x) = g(y)$ from (3),

and finally we deduce $x = y$ from (4), completing the proof.

3 The Axiomatic Method Applied to Arithmetic

In our book, we will see an application of the axiomatic method to the theory of real numbers. To introduce this method, we present an application to arithmetic.

In the axiomatic method, we give a list of primitive notions in terms of which everything else is formally defined: we cannot define *every* concept we use, because this would lead to circular definition (or to an infinite regress of definitions).

Further, we give a list of basic assumptions called axioms, from which everything we prove will be deduced. Again, we cannot prove *every* statement we assert, because this would lead to the fallacy of assuming what we are trying to prove (or to an infinite regress of assumptions).

The notions of logic, including the equality relation, are assumed to be part of every theory. So we will not list basic assumptions or results of logic among our primitive notions or axioms (this *can* be done but it would make things harder). Notions of set theory may also be assumed to be part of every theory (and we will in fact assume this) though this might be more controversial. About this, more later.

The primitive concepts of our theory (which is called “Peano arithmetic” or “first-order arithmetic”) are \mathbb{N} (the set of natural numbers), 0, (the natural number 0), S (the successor operation), addition and multiplication.

The axioms are as follows:

I: 0 is a natural number ($0 \in \mathbb{N}$).

II: If x, y are natural numbers, $S(x)$, $x + y$, and $x \cdot y$ are natural numbers. [we have lumped all the closure axioms into one]. [$S(x)$ actually is intended to mean $x + 1$].

III: $S(x) \neq 0$

IV: $S(x) = S(y) \rightarrow x = y$

V: For any sentence $P(n)$ about a natural number variable n , $P(0) \wedge (\forall k \in \mathbb{N}. P(k) \rightarrow P(S(k))) \rightarrow (\forall n \in \mathbb{N}. P(n))$. This is the familiar principle of mathematical induction.

VI: $x + 0 = x$

VII: $x + S(y) = S(x + y)$

VIII: $x \cdot 0 = 0$

IX: $x \cdot S(y) = x \cdot y + x$

Notice that most statements here are implicitly universally quantified, as is the usual style in algebra: e.g., $x + S(y) = S(x + y)$ actually abbreviates $(\forall xy. x + S(y) = S(x + y))$. I am assuming that we can all handle the underlying logic of algebra.

Definition: 1 is defined as $S(0)$. 2 is defined as $S(1)$. 3 is defined as $S(2)$. 4 is defined as $S(3)$. 5 is defined as $S(4)$. 6 is defined as $S(5)$. 7 is defined as $S(6)$. 8 is defined as $S(7)$. 9 is defined as $S(8)$. The symbols 0,1,2,3,4,5,6,7,8,9 are called *digits*: these are all the digits. They are called *numerals* as well, and we stipulate that any notation made up of a numeral n representing a natural number N immediately followed by a digit d representing a natural number D is a numeral and represents $(S(9) \cdot N) + D$. [I hope you enjoy this definition].

Theorem: $S(n) = n + 1$.

Proof: Let n be an arbitrarily chosen natural number. $n + 1 =$ (by def of 1) $n + S(0) =$ (by **VII**) $S(n + 0) =$ (by **VI**) $S(n)$.

Comment: Note that we could now dispense with the unfamiliar $S(x)$ in favor of $x+1$. We will still sometimes use the successor notation. Notice that S is not redundant even if we stop using it completely, since $x + 1$ is defined in terms of 1, which is in turn defined in terms of S .

Equality: The basic properties of equality are presumed to be familiar. $x = x$ is true for any x (reflexive property). If $x = y$ then $y = x$ (symmetric property). If $x = y$ and $y = z$ then $x = z$ (transitive property). Chained equations $x_1 = x_2 = x_3 = \dots = x_{n-1} = x_n$ abbreviate $x_1 = x_2 \wedge x_2 = x_3 = \dots = x_{n-1} = x_n$, and if each equation in the chain is justified we have (by many applications of transitivity) a justification of the assertion $x_1 = x_n$. The substitution property of equality says that if $x = y$ and $P(x)$ then $P(y)$, where $P(x)$ is any statement about x at all. It is interesting to note that it is relatively easy to prove symmetry and transitivity from reflexivity and substitution.

We can easily verify that if we interpret the primitive notions of the theory as the familiar concepts they seem to be in relation to the familiar system of whole numbers, all the axioms are true. What is much more interesting is that all the familiar things that you know about the natural numbers can be proved from these axioms alone.

We formalize mathematical induction as a proof strategy.

Axiom **V** tells us that if we can prove $P(0) \wedge (\forall k \in \mathbb{N}. P(k) \rightarrow P(k+1))$ (here I use the theorem about successor proved above) then we can prove $(\forall n \in \mathbb{N}. P(n))$. So a strategy for proving $P(0) \wedge (\forall k \in \mathbb{N}. P(k) \rightarrow P(k+1))$ is also a strategy for proving $(\forall n \in \mathbb{N}. P(n))$.

This justifies the following proof outline:

Goal: $(\forall n \in \mathbb{N}. P(n))$

Basis Goal: $P(0)$
[proof of $P(0)$]

Induction Step: Let k be an arbitrarily chosen natural number.

Assume (ind hyp): $P(k)$

Induction Goal: $P(k+1)$ [or $P(S(k))$]
[proof of $P(k+1)$]

Of course the induction hypothesis can only be used as an assumption in the proof of the induction goal.

We now prove a familiar theorem as an example, namely the commutativity of addition.

Goal: For any natural numbers m, n , $m + n = n + m$.

Let m be an arbitrarily chosen natural number.

Goal: For any natural number n , $m + n = n + m$.

Discussion: We prove this goal by mathematical induction. We will also have to prove some intermediate statements by mathematical induction (lemmas). In this presentation, unlike the one in class, I will embed the smaller math induction results in the larger one.

Basis Goal: $m + 0 = 0 + m$

Discussion: The basis gets its own induction proof.

Basis Goal: $0 + 0 = 0 + 0$

This follows from the reflexive property of equality/

Induction Step: Let k be an arbitrarily chosen natural number.

Assume (ind hyp): $0 + k = k + 0$

Induction Goal: $0 + S(k) = S(k) + 0$

$0 + S(k) = \text{(VII)}S(0 + k) = \text{(ind hyp)}S(k + 0) = \text{(VI)}S(k) = \text{(VI)}S(k) + 0$. This chain of equalities justifies $0 + S(k) = S(k) + 0$.

Induction Step: Let k be an arbitrarily chosen natural number.

Assume (ind hyp): $m + k = k + m$

Induction Goal: $m + S(k) = S(k) + m$

$m + S(k) = \text{(VII)}S(m + k) = \text{(ind hyp)}S(k + m)$. This would then be equal to $S(k) + m$, completing the proof, if we could show $(\forall pq \in \mathbb{N}. S(p + q) = S(p) + q)$, a statement which looks like a variation of axiom **VII**. So we adopt this statement as a new goal.

Goal (Lemma): $(\forall pq \in \mathbb{N}. S(p + q) = S(p) + q)$

Let p be an arbitrarily chosen real number.

Goal: $(\forall q \in \mathbb{N}. S(p + q) = S(p) + q)$ [we prove this by math induction]

Basis Goal: $S(p + 0) = S(p) + 0$

$S(p + 0) = S(p) = S(p) + 0$, by two applications of **VI**.

Induction Step: Let r be an arbitrarily chosen natural number. [k is already in use!]

Assume (ind hyp): $S(p + r) = S(p) + r$

Induction Goal: $S(p + S(r)) = S(p) + S(r)$

$$S(p + S(r)) \stackrel{\text{(VII)}}{=} S(S(p + r)) \stackrel{\text{(ind hyp)}}{=} S(S(p) + r) \stackrel{\text{(VII)}}{=} S(p) + S(r)$$

The proof of the Lemma is complete. We explained above why completing the proof of the Lemma completes the main proof as well.