Basic Proof Techniques

Joshua Wilde, revised by Isabel Tecu, Takeshi Suzuki and María José Boccardi

August 13, 2013

1 Basic Notation

The following is standard notation for proofs:

- $A \Rightarrow B$. A implies B.
- $A \Leftarrow B$. B implies A.
  Note that $A \Rightarrow B$ does not mean $B \Rightarrow A$. Example: If (A) a person eats two hot dogs, she also (B) eats one hot dog. However, if (B) a person eats one hot dog, that does not imply that she also (A) eats two hot dogs.
- $A \Leftrightarrow B$. A implies B and B implies A.
  Another way of saying this is that A holds if and only if (iff) B holds, or that A is equivalent to B.
- $\neg A$. Not A, or the negation of A.
  Example: If A is the event that $x \leq 10$, then $\neg A$ is the event that $x > 10$.

It is common to use mathematical symbols for words while writing proofs in order to write faster. The following are commonly used symbols:

$\forall$ For all, for any

$\exists$ There exists

$\in$ Is contained in, is an element of

$\ni$ Such that, contains as an element

$\subset$ Is a subset of

QED Latin for "quod erat demonstandum", or "which was to be proven". A common way to signal to the reader that you have successfully concluded your proof.

2 Proofs

We seek for ways to prove that $A \Rightarrow B$.

2.1 Direct Proofs

2.1.1 Deductive Reasoning

A direct proof by deductive reasoning is a sequence of accepted axioms or theorems such that $A_0 \Rightarrow A_1 \Rightarrow A_2 \Rightarrow \cdots \Rightarrow A_{n-1} \Rightarrow A_n$, where $A = A_0$ and $B = A_n$. The difficulty is finding a sequence of theorems or axioms to fill the gaps.

Example: Prove the number three is an odd number.

Proof: A number q is odd if there exists an integer m such that $q = 2m + 1$. Let $m = 1$. Then $2m + 1 = 3$. Therefore three is an odd number. QED

2.1.2 Contrapositive

A contrapositive proof is just a direct proof of the negation. It makes use of the fact that the statement $A \Rightarrow B$ is equivalent to the statement $\neg B \Rightarrow \neg A$. For example, if (A) all people with driver's licenses are (B) at least 16 years old, then if you are not $(\neg B)$ 16 years old, then you do not $(\neg A)$ have a driver's license. So proving $A \Rightarrow B$ is really the same as proving $\neg B \Rightarrow \neg A$.

Example: Let x and y be two positive numbers. Prove that if $xy > 9$, then $x > 3$ or $y > 3$.

Proof: Suppose that both $x \leq 3$ and $y \leq 3$. Then $xy \leq 9$. QED (Here A: $xy > 9$, B: $x > 3$ or $y > 3$. In order to prove $A \Rightarrow B$ we proved $\neg B \Rightarrow \neg A$.)

2.2 Indirect Proofs

2.2.1 Contradiction

Suppose that we are trying to prove a proposition A, and we cannot prove it directly. However, we can show that all other alternatives to A are impossible. Then we have indirectly proved that A must be true. Therefore, the we can prove $A \Rightarrow B$ by first assuming that $A \not\Rightarrow B$ and finding a contradiction. In other words, we start off by assuming that A is true but B is not. If this leads to a contradiction, then either B was actually true all along, or A was actually false. But since we assume A is true, then it must be that B is true, and we have a proof by contradiction.

Example: Prove that $\sqrt{2}$ is an irrational number.

Proof: Suppose not. Then $\sqrt{2}$ is a rational number, so it can be expressed in the form $\frac{p}{q}$, where p and q are integers which are not both even. This implies that

$$2 = \frac{p^2}{q^2} \Rightarrow 2q^2 = p^2,$$

which implies that p^2 is even, which in turn implies that q^2 is not even. The fact that p^2 is even also implies that p is even, so there exists a integer m such that $2m = p$. This implies

$$4m^2 = p^2 = 2q^2 \Rightarrow q^2 = 2m^2,$$

which means that q is even, a contradiction. QED

2.2.2 Induction

Induction can only be used for propositions about integers or indexed by integers. Consider a list of statements indexed by the integers. Call the first statement $P(1)$, the second $P(2)$, and the nth statement $P(n)$. If we can prove the following two statements about the sequence, then every statement in the entire sequence must be true:

1. $P(1)$ is true.

2. If $P(k)$ is true, then $P(k+1)$ is true.

Induction works because by 1., $P(1)$ is true. By 2., $P(2)$ is true since $P(1)$ is true. Then $P(3)$ is true by 2. again, and so is $P(4)$ and $P(5)$ and $P(6)$, until we show that all the P's are true. Notice that the number of propositions need not be finite.

Example: Prove that the sum of the first n natural numbers is $\frac{1}{2}n(n+1)$.

Proof: Let $n = 1$. Then $\frac{1}{2}\cdot 1(1+1) = \sum_{j=1}^{1} j = 1$. Now let $n = k$, and assume that $\sum_{j=1}^{k} j = \frac{1}{2}k(k+1)$. We add $k+1$ to both sides to get

$$\sum_{j=1}^{k+1} j = \frac{1}{2}k(k+1) + k + 1 = \left(\frac{1}{2}k + 1\right)(k+1) = \frac{1}{2}(k+1)((k+1)+1).$$

QED

2.3 Epsilon-Delta Arguments

A lot of definitions and proofs in real analysis use the "ϵ and δ" concept. For example, recall the definition of the limit of a function: We write $\lim_{x\to p} f(x) = q$ if for every $\epsilon > 0$ we can find $\delta > 0$ such that $|f(x) - q| < \epsilon$ for all x for which $|x - p| < \delta$.

It is important to get the quantifiers correct: *For every ϵ there exists* δ such that... This means that δ will change with ϵ - for some value ϵ_1 we'll be able to find δ_1 so that the statement holds, and for some other value ϵ_2 we'll find δ_2 which may different from δ_1. The opposite would be "*there exists* δ such that *for every* ϵ it holds that...". Here there is only one δ which has to fit all different values of ϵ.

When we prove a statement involving an ϵ-δ definition, we start by ascribing a fixed, but unknown, value to ϵ ("fix $\epsilon > 0$"). Then we try to find value of δ that makes the statement in question come true. This δ will usually be a function of ϵ. This completes the proof since ϵ could have been anything: For every ϵ we have found a δ such that the statement holds.

When we want to show that a certain ϵ-δ statement does not hold, we usually choose one particular ϵ for which the statement should not be true ("Let $\epsilon = 0.5$"). Then we proceed by contradiction: We pretend there exists some δ that fits our ϵ and show that this leads to a contradiction. Ergo, no δ can fit our particular ϵ. Therefore it is not true that for all ϵ we can find a fitting δ.

Example 1 Prove that $\lim_{x\to 0} x^2 + 1 = 1$.
Proof: Fix $\epsilon > 0$. How small does δ have to be such that $|(x^2+1) - 1| = |x^2| < \epsilon$ for all x for which $|x| < \delta$? $\delta = \sqrt{\epsilon}$ works: If $|x| < \sqrt{\epsilon}$ then $|x|^2 < (\sqrt{\epsilon})^2$. $|x|^2 = |x^2|$ and $(\sqrt{\epsilon})^2 = \epsilon$, therefore $|x^2| < \epsilon$. QED.

Example 2 Show that $f(x) = \begin{cases} 1 \text{ if } x \geq 0 \\ -1 \text{ if } x < 0 \end{cases}$ is not continuous.

Recall that f is continuous at a point p if for every $\epsilon > 0$ we can find $\delta > 0$ such that $|f(x) - f(p)| < \epsilon$ for all x for which $|x - p| < \delta$. f is probably not continuous is at 0. We therefore take $p = 0$ and show that the above definition of continuity does not hold. It suffices to show that for one particular ϵ we

cannot find a fitting δ. We prove this by contradiction.
Proof: Let $\epsilon = 1$. Suppose there exists δ such that $|f(x) - f(0)| < \epsilon$ for all x for which $|x| < \delta$. Plugging in, this means $|f(x) - 1| < 1$ for all x for which $|x| < \delta$. Set $x = -\frac{\delta}{2}$. Then $|x| < \delta$ but $|f(x) - 1| = |-1-1| = 2$ which is not < 1. This contradicts $|f(x) - 1| < 1$ for all x for which $|x| < \delta$. Therefore there exists not δ such that the definition of continuity becomes true. f is not continuous at 0 and therefore not a continuous function. QED.

Exercises

1. Negate the definition of convergence for a sequence. (The definition is in Real Analysis part.)
2. Negate the definition of continuity.
3. Let $f(x) = \begin{cases} 1 \text{ if } x \neq 0 \\ 1.1 \text{ if } x = 0 \end{cases}$. Prove that f is not continuous at 0.
4. Prove that $\lim_{x \to 0} \frac{1}{x} \neq K$ for any number K.
5. Let f and g be two continuous functions from $\mathbb{R}$ to $\mathbb{R}$. Show that $f + g$ is continuous.

3 Homework

Prove the following by direct proof.

1. $n(n+1)$ is an even number.
2. The sum of the first n natural numbers is $\frac{1}{2}n(n+1)$.
3. If $6x+9y=101$, then either x or y is not an integer.

Prove the following by contrapositive.

1. $n(n+1)$ is an even number.
2. If $x+y>100$, then either $x>50$ or $y>50$.

Prove the following by contradiction.

1. $n(n+1)$ is an even number.
2. $\sqrt{3}$ is an irrational number.
3. There are infinitely many prime numbers.

Prove the following by induction.

1. $n(n+1)$ is an even number.
2. $2n \leq 2^n$.
3. $\sum_{i=1}^{n} i^2 = \frac{1}{6}n\,(n+1)\,(2n+1)$.
4. The sum of the first n odd integers is n^2 (This is the first known proof by mathematical induction, attributed to Francesco Maurolico. Just in case you were interested.)

Find the error in the following argument, supposedly by induction:

If there is only one horse, then all the horses are of the same color. Now suppose that within any set of n horses, they are all of the same color. Now look at any set of $n+1$ horses. Number them $1,2,3,\ldots,n,n+1$. Consider the sets $\{1,2,3,\ldots,n\}$ and $\{2,3,4,\ldots,n+1\}$. Each set is a set of n horses, therefore they are all of the same color. But these sets overlap, therefore all horses are the same color.

Prove the following (solution in Analysis solution sheet):

1. Let f and g be functions from $\mathbb{R}^k$ to $\mathbb{R}^m$ which are continuous at x. Then $h=f-g$ is continuous at x.
2. Let f and g be functions from $\mathbb{R}^k$ to $\mathbb{R}^m$ which are continuous at x. Then $h=fg$ is continuous at x.

In first semester micro you will be introduced to preference relations. We say that $x \succeq y$, (read "x is weakly preferred to y") if x is at least as good as y to the agent. From this, we can derive two important relations:

- The strict preference relation, $\succ$, defined by $x \succ y \Leftrightarrow x \succeq y$ but not $y \succeq x$. The strict preference relation is read "x is strictly preferred to y".
- The indifference relation, $\sim$, defined by $x \sim y \Leftrightarrow x \succeq y$ and $y \succeq x$. The indifference relation is read "x is indifferent to y".

We say that a preference relation is rational if:

- $\forall\ x, y$, either $x \succeq y$ or $y \succeq x$.
- $\forall\ x, y, z$, if $x \succeq y$ and $y \succeq z$, then $x \succeq z$.

Prove the following two statements given that preferences are rational:

1. If $x \succ y$ and $y \succ z$, then $x \succ z$.
2. If $x \sim y$ and $y \sim z$, then $x \sim z$.