

A Catalog of Proof Techniques

October 23, 2000

Handout 7

The following handout summarizes the various proof techniques that we are going to cover in this course. I hope you will find this useful (here and in later classes) when when you are asked to prove something and have to think about what proof technique to apply.

Direct Proof

This proof technique is the most basic in which you use the laws of inference to prove the desired result in a direct manner. As an example suppose that you want to prove that $p \rightarrow q$ for propositions p and q . In a direct proof you first assume that p is true and then show that from this assumption it can be shown that q must also be true. Of course, this technique can also be applied to prove statements that are not implications.

WARNING: When writing a direct proof avoid the fallacy of circular reasoning in which part of your proof is actually based on the truth of the statement being proved.

Indirect Proof

This proof technique gives an alternate method to a direct proof for showing that $p \rightarrow q$. In this technique one proves that $p \rightarrow q$ by instead proving the contrapositive, $\neg q \rightarrow \neg p$. Typically one proves $\neg q \rightarrow \neg p$ directly (although other techniques can be used).

Proof by Contradiction

To prove that proposition p is true using this technique, you show that $\neg p \rightarrow F$. This is a very general proof technique that can be used in many settings. For example, we used this technique to prove that $\sqrt{2}$ is not rational. It can also be used to prove $p \rightarrow q$ by showing that

$$\neg(p \rightarrow q) \iff \neg(\neg p \vee q) \iff (p \wedge \neg q) \rightarrow F.$$

In other words, you show that it is not possible for both p to be true and q to be false, and thus it follows that $p \rightarrow q$.

Note that when proving $p \rightarrow q$, the techniques of using an indirect proof and proof by contradiction are very closely related. Namely, in a proof by contradiction typically you suppose that p and $\neg q$ are true and then use the steps of the proof that $\neg q \rightarrow \neg p$ to reach the desired contradiction.

Proving $p \leftrightarrow q$

Although this is not a proof technique, these type of proofs are used so commonly that they merit a section of their own. The two most common method of writing $p \leftrightarrow q$ are: “ p if and only if (iff) q ” and “ p is necessary and sufficient for q ”.

To prove that $p \leftrightarrow q$ you must show *both* that:

1. $q \rightarrow p$ (i.e. p if q , or equivalently p is necessary for q), and
2. $p \rightarrow q$ (i.e. p only if q , or equivalently p is sufficient for q).

The proof technique used in proving these two “subproofs” can be independently selected. For example, you may directly show that $q \rightarrow p$ and indirectly show that $p \rightarrow q$.

WARNING: Be sure not to prove the same implication using two different proof techniques! For example if you prove that $p \rightarrow q$ and $\neg q \rightarrow \neg p$ then you have *not* shown that $p \leftrightarrow q$, but rather you have given two ways of showing that $p \rightarrow q$.

Proof By Cases

This proof technique is useful when you want to prove that $p \rightarrow q$ when p can be decomposed into cases p_1, p_2, \dots, p_n where $p \leftrightarrow (p_1 \vee p_2 \vee \dots \vee p_n)$. Since $[(p_1 \vee p_2 \vee \dots \vee p_n) \rightarrow q] \leftrightarrow [(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \dots \wedge (p_n \rightarrow q)]$, to prove $p \rightarrow q$ it suffices to independently prove (using whatever proof technique is most appropriate for each) the n implications given by $p_i \rightarrow q$ for $1 \leq i \leq n$.

WARNING: Do not forget to demonstrate/prove that $p \leftrightarrow (p_1 \vee p_2 \vee \dots \vee p_n)$. Also, try not to generate more cases than necessary.

Proving That A Set of Propositions are Equivalent

As in proof by cases, here we break the problem of proving that propositions p_1, p_2, \dots, p_n are logically equivalent into a set of subcases. While one could proceed by showing that all pairs of propositions are logically equivalent this technique would be unnecessarily tedious. Instead, one can select n (properly chosen) implications to prove. Namely, since

$$[p_1 \leftrightarrow p_2 \leftrightarrow \dots \leftrightarrow p_n] \iff [(p_1 \rightarrow p_2) \wedge (p_2 \rightarrow p_3) \wedge \dots \wedge (p_{n-1} \rightarrow p_n) \wedge (p_n \rightarrow p_1)],$$

to prove that p_1, p_2, \dots, p_n are logically equivalent, it suffices to prove that $p_i \rightarrow p_{i+1}$ for $1 \leq i \leq n-1$, and that $p_n \rightarrow p_1$. Again, each of these n implications can be proven by any of the proof techniques discussed here.

WARNING: Be sure that the “chain” of implications returns to the proposition where it started and that it passes through *each* of the propositions that you would like to prove equivalent.

Constructive Existence Proof

Here the goal is to prove that $\exists x P(x)$ where $P(x)$ is a propositional function. In a constructive proof, one finds an a and then proves that $P(a)$ is true.

WARNING: Be sure to argue that a is in the universe of discourse (if not immediately obvious). Also be sure to prove that $P(a)$ is true (using another proof technique.)

Non-Constructive Existence Proof

Here too the goal is to prove that $\exists x P(x)$. However, in a non-constructive proof you never find an a such that $P(a)$ can be shown to be true. For example, you could use a proof by contradiction to show that

$$\neg \exists x P(x) \leftrightarrow \forall x \neg P(x) \rightarrow F.$$

Mathematical Induction

This proof technique is most commonly used to prove a statement such as $\forall x P(x)$ where $P(x)$ is a propositional function and the universe of discourse for x is typically the integers greater than or equal to a constant c (where c is typically 0 or 1). It is important the the universe of discourse has the well-ordering property.

An inductive proof has two steps. In the *basis step* you must prove that $P(c)$ is true. The second step is the *inductive step*. In *weak induction*, the inductive step consist of showing the proposition $P(n) \rightarrow P(n + 1)$ is true for all $n \geq c$. In *strong induction*, the inductive step consists of showing the proposition

$$[P(c) \wedge P(c + 1) \wedge \cdots \wedge P(n)] \rightarrow P(n + 1)$$

is true for all $n \geq c$.

WARNING: Although it is *usually* trivial, do not forget to prove the base case! (There are false claims for which the inductive step holds but the base case does not.)

Remember that to prove a recursive program correct, typically you can use induction on the number of recursive calls made. To prove that an iterative program correct, these are the steps to follow:

- Clearly state the loop invariant “ p ” that you will use.
- Use induction to prove that p is a loop invariant.
- Now use your loop invariant to prove that the given program is partially correct with respect to the given initial and final assertions.
- Finally, prove the given program is correct with respect to the given initial and final assertions (i.e. show that it always terminate).

Diagonalization (TO BE COVERED)

Diagonalization is used to show that the cardinality of one set, say set A , is larger than the cardinality of another set, say set B . For example, to show that the real numbers are uncountable we must show that the cardinality of the reals is larger than the cardinality of the natural numbers.

In such proofs you typically begin by assuming that A and B have the same cardinality (i.e. there is a one-to-one correspondence between them), and then show that this leads to a contradiction. (Thus we are using a proof by contradiction.) The diagonalization technique is used to prove that some element of A was not included in the one-to-one correspondence, thus contradicting the fact that the relation given between A and B was a one-to-one correspondence.

Pigeonhole Principle (TO BE COVERED)

This principle, in its most general form, states that if there are m objects (or pigeons) and only n categories (or pigeon holes) into which these objects are classified, then there must be at least $\lceil \frac{m}{n} \rceil$ objects that fall into the same category.