Proof Techniques

This handouts contains a collection of proof techniques used in CSE 311. Some problems will require multiple techniques, and some techniques may be used as steps in other techniques.

1. Proving $\exists$

To prove an exists statement, simply choose an object in the domain that satisfies the desired property and show it satisfies that property.

Tips:

- The hard part of these proofs is usually finding the object. One technique is to suppose an object x satisfies the property, and then using that to deduce as much information about x as possible.

Example

Show that there is an even prime integer.

Proof. Let $p = 2$. Then p is even and p is prime, so there exists an even prime integer. □

2. Proving an Implication ("if-then") Statement

To prove an "if A then B" statement, start with "Suppose A" and show that in this case B must hold.

Tips:

- It's rare that you just prove an implication statement on its own, it's usually surrounded by a "for all" quantifier in some way.
- Try writing down the premise, leaving blank space, and writing the conclusion at the end.
- The definition of $A \subseteq B$ is an implication (inside a $\forall$) so you'll use this technique frequently with sets.

Example

Show that for any integer x, if x is even then $-x$ is even.

Proof. Let x be an arbitrary integer. Suppose x is even. By the definition of even there exists an integer k such that $x = 2k$. By Algebra, $-x = 2(-k)$. Since $-k$ is an integer, by definition we have $-x$ is even. □

3. Proof By Counter-example (Disproving $\forall$)

Recall that for any predicate P in any domain that $\neg\forall x\ P(x) \equiv \exists x\ \neg P(x)$. So disproving a $\forall$ claim is the same as *proving* an exists statement.

To disprove a $\forall$ claim, choose an object in the domain that doesn't satisfy the desired property and show it doesn't satisfy that property. This is called a *counter-example*, and may take some experimentation to construct.

Tips:

- Sometimes it's helpful to try to prove the "forall" statement and see where it breaks down. When you get stuck, try to construct an object that causes the problem you're having with the proof.
- As with proving an $\exists$ statement, you can try supposing you had an object x that worked as a counterexample and try to deduce as much about that object as possible.

Example

Show that not all integers are positive or negative.

Proof. Let $x = 0$. Then x is not positive and x is not negative, hence it is not the case that x is positive or negative. Thus, not all integers are positive or negative. □

4. Proof By Cases

Sometimes an argument won't always have one series of steps that works for every scenario you need to consider. If this happens we must divide it into cases, which are a set of statements such that at least one always hold. You assume each statement in turn and in each case show that your conclusion holds. If you can do this for every statement, then the conclusion always holds. Usually the cases are mutually exclusive as well, but this isn't necessary.

Tips:

- If you can't make any progress on a proof, try asking yourself if there any cases where the proof would work easily. Make these one of your cases. Then see what happens when none of those cases hold. It might not bring you closer to a solution, but it does give you more specificity for what the situation looks like when the proof is hard.
- As you do more proofs, you'll naturally start considering cases automatically. Ask what if x is even or odd? What if x is positive or non-negative? If some value can take on some small finite number of values, is it feasible to just consider each of those values as a separate case?

Example

Show that for any integer x, that $x^2 \equiv x \pmod 2$.

Proof. Let x be arbitrary. Let $r = x\%2$ meaning $x \equiv r \pmod 2$. Note that since $0 \leq r < 2$ that either $r = 0$ or $r = 1$. There are two cases

Case 1: $r = 0$**.** If $r = 0$, then $x \equiv 0 \pmod 2$. Multiplying both sides of this congruence by x we have $x^2 \equiv 0 \pmod 2$. Since both are congruent to 0, we have $x^2 \equiv x \pmod 2$.

Case 2: $r = 1$**.** If $r = 1$ then $x \equiv 1 \pmod 2$. Multiplying both sides of this congruence by x we have $x^2 \equiv x \pmod 2$.

These cases are exhaustive, so the claim that $x^2 \equiv x \pmod 2$ must hold. Since x was arbitrary, it holds for all x. □

5. Proof By Contrapositive

Recall that any implication statement has a *contrapositive*. The contrapositive of "if A then B" is "if $\neg B$ then $\neg A$". Sometimes if you're having trouble proving an if-then statement, try proving the contrapositive instead.

Example

Show that for any integer x, if x^2 is odd then x is odd.

Proof. We argue by contrapositive. That is, we show instead that if x is not odd then x^2 is not odd, which is the same as saying if x is even then x^2 is even.

Let x be an arbitrary integer and suppose x is even. Then by definition there exists an integer k such that $x = 2k$. Then by Algebra, $x^2 = (2k)^2 = 4k^2 = 2(2k^2)$. Since $2k^2$ is an integer, by definition we have x^2 is even. This shows the claim. □

Note, an alternative proof would be to use the previous example's result. Why does this work?

6. Proof by Contradiction

Occasionally, the easiest way to prove a theorem is by assuming its negation and showing that we can prove a false statement under that assumption. Since (hopefully) it's impossible to prove false statements, our only conclusion can be that the original statement was actually true (rather than its negation being true).

Many proofs by contradiction can actually be modified to use some other proof technique instead, such as proof by contrapositive. You should avoid the tendency to use this technique as much as possible.

Tips:

- Trying proof by contradiction can often be helpful during scratch work. For example, if you're proving a claim $\forall x\ (P(x) \to Q(x))$, then the negation is $\exists x\ (P(x) \wedge \neg Q(X))$. This means if you're trying to prove "all objects with property P have property Q", try assuming there was an object x that satisfied P but not Q, and see if that leads to a contradiction.
- Proof by contradiction is often helpful when proving "forall" claims. If you're showing all objects have some property, then assume there was an object that didn't satisfy the property and call it x. See if you can deduce anything weird about x that could lead to a contradiction.

Example

Show that there is no largest integer.

Proof. Suppose, for the sake of contradiction, that there were a larger integer. Call it x. Then $x + 1 > x$. But x is the largest integer, so $x + 1 \leq x$. It can't be true that $x + 1 > x$ and $x + 1 \leq x$, so this is a contradiction. Thus, our assumption that there was a largest integer must be false. □

Try turning the above claim from a "not exists" statement into a "for all" statement. Try proving it again without proof by contradiction.

7. Proving a Biconditional

A biconditional ($p \leftrightarrow q$) can be proven in two ways. Either show $p \to q \wedge q \to p$ (see the "Proving an implication" section) or transform p into q applying an "if-and-only-if" rule (or equivalence) at each step.

Tips:

- Showing two sets are equal is the biconditional we have to prove the most often.

- For the proof to be logically correct, you have to say "if and only if" or "equivalent to" (or something similar) at each step. Otherwise you're implicitly saying the first implies the second (but you don't say the second implies the first, which you also need).
- We strongly recommend writing the two separate implications (it's very easy to miss that an explanation only works one way).

Example

Let n be a positive integer. Show that $x \equiv 3 \pmod{n}$ if and only if $x \equiv n + 3 \pmod{n}$.

Proof. Let x be an arbitrary integer, and n be an arbitrary positive integer.

$x \equiv 3 \pmod{n}$ if and only if $n|(x-3)$ (by definition of mod). Which is true if and only if there is an integer k such that $nk = x - 3$. Which is true if and only if $n(k-1) = x - n - 3$ (by subtracting n). $k - 1$ is an integer if and only if k is, so the above holds if and only if $n|(x - [n+3])$, which (by definition of mod) holds if and only if $x \equiv n + 3 \pmod{n}$. □

Try proving this claim again by proving the implications separately.

8. Proof By Induction

To show a claim holds for all natural numbers (or all natural numbers greater than a fixed value) one often wants induction. To show a claim holds for all elements of a recursively-defined set, one often wants structural induction.

Tips:

- While all the induction variants are equally powerful, often one technique is much easier than the others to use.
- Induction is useful for summations, products, and recursion – anything where the claim for k appears as part of the claim for $k + 1$.

Example

See the templates in the induction templates handout.