CSE 311: Foundations of Computing I

Proof Techniques

What Is This?

Each of the following is as close as we can get to giving you a template (and a completely worked out example) for every proof technique we will discuss this quarter.

However, there is a large **WARNING** associated with these templates! It might be tempting to memorize the structure(s) of these templates rather than learn what they mean well enough to duplicate them on your own. **DON'T DO IT**!!! These are meant as a way to help you ease into proof writing as we introduce more and more complicated strategies. There isn't (and will never be) an algorithm or formula for writing proofs.

Contents

1 Direct Proofs

1.1 Technique Outlines

Proving a $\forall$ Statement

Prove $\forall x\ P(x)$.	Prove $\forall x\ (x = 5 \lor x \neq 5)$.
Let x be arbitrary.	Let x be arbitrary.
Now, x represents an arbitrary element, and we can just use it. Prove $P(x)$ by some other strategy.	Note that by the law of excluded middle, $x = 5$ or $x \neq 5$.
Since x was arbitrary, the claim is true.	Since x was arbitrary, the claim is true.

Proving an $\exists$ Statement

Prove $\exists x\ P(x)$.	Prove $\exists x$ Even(x).
[Find an x for which $P(x)$ is true. This is not actually part of the proof, but it's necessary to continue.] Let $x = \boxed{\text{expression that satisfies } P(x)}$.	[We can choose any even number here. We'll go with 2, because it's simplest.] Let $x = \boxed{2}$.
Now, explain why $P(x)$ is true.	Note that 2 is even, by definition, because $2 \times 1 = 2$.
Since $P(x)$ is true, the claim is true.	Since 2 is even, the claim is true.

Disproving a Statement

Disprove $P(x)$.	Disprove Odd(4).
We show that $P(x)$ is false by proving its negation: $\boxed{\text{the negation of } P(x)}$.	We show that 4 is not odd by showing it's even.
Prove $\neg P(x)$ using some other proof strategy.	Note that 4 is even, by definition, because $2 \times 2 = 4$.
Since $\neg P(x)$ is true, $P(x)$ is false.	Since 4 is even, it is not odd.

1.2 Example

Prove $\forall x\ \forall y\ \exists z\ (zx = y)$ **Domain: Non-Zero Reals**

Proof: Let x and y be arbitrary. Choose $z = \frac{y}{x}$. Note that $x \times \frac{y}{x} = y$. This is valid, because $x \neq 0$. Thus, we've found a z (yx) such that the claim is true.

Commentary: We started off the proof with "Let x and y be arbitrary". This is so that the claim works for any x and y we are provided. We're not allowed to assume anything special about x or y, but if we use them as if they are any particular number, the claim will be true for *any* x and y.
The "choose" line is used to prove the existential quantifier by pointing out a value that works. We have to follow that up with a justification of *why* the choice we made works.
The last line just sums up what we've done.

2 Implication Proofs

2.1 Technique Outlines

Proving an $\rightarrow$ (Directly)

Prove $A \rightarrow B$.	Prove that if $x \leq 4$ is an even, positive integer, then it's a power of two.
Suppose A is true. Prove B using the additional assumption that A is true. It follows that B is true. Therefore, $A \rightarrow B$.	Suppose $x \leq 4$ is even, positive integer. Since x is a positive integer, $x > 0$. Furthermore, since $x \leq 4$, it must be that $x = 2$ or $x = 4$. Note that $2 = 2^1$ and $4 = 2^2$; so, both possibilities are powers of two. It follows that x must be a power of two. So, if x is an even positive integer at most four, then x is a power of two.

Proving an $\rightarrow$ (Contrapositive)

Prove $A \rightarrow B$.	Prove that if $x^2 - 6x + 9 \neq 0$, then $x \neq 3$.
We go by contrapositive. Suppose $\neg B$ is true. Prove $\neg A$ using the additional assumption that $\neg B$ is true. So, $\neg A$ is true. Therefore, $A \rightarrow B$.	We go by contrapositive. Suppose $x = 3$. Then, $x^2 - 6x + 9 = 3^2 - 6 \times 3 + 9 = 0$. So, $x^2 - 6x + 9 = 0$. Thus, if $x^2 - 6x + 9 \neq 0$, then $x \neq 3$.

2.2 Examples

Prove $\forall x\, \forall y\, ((x + y = 1) \to (xy = 0))$ **Domain: Non-negative Integers**

Proof: Let x and y be arbitrary non-negative integers.

We prove the implication by contrapositive. Suppose $xy \neq 0$. Then, it must be the case that neither x nor y is zero, because $0 \times a = 0$ for any a. So, $x > 0$ and $y > 0$, which is the same as $x \geq 1$ and $y \geq 1$.

Adding inequalities together, we see that $x + y \geq 2$. It follows that $x + y > 1$ which means $x + y \neq 1$ which is what we were trying to show.

So, the original claim is true.

Commentary: The hardest thing about proof by contrapositive is to understand when to use it. There are two "clear" situations to try it in:

(1) If there are a lot of negations in the statement. (See the example above in the previous section.) Contrapositive adds a bunch of negations into each part of the implication which means if there are already a lot of them, it removes them!

(2) If you try the direct proof and get stuck (or feel like you have to use proof by contradiction). A very common mistake is to use proof by contradiction when a proof by contrapositive would be much more clear!

Prove $\forall x\, \forall y\, ((x < y) \to (\exists z\, x < z \wedge z < y))$ **Domain: Rationals**

Proof: Let x, y be arbitrary rational numbers such that $x < y$.

Since x, y are both rational, we have $x = \dfrac{p_x}{q_x}$ and $y = \dfrac{p_y}{q_y}$ for integers p_x, q_x, p_y, q_y such that $q_x \neq 0$ and $q_y \neq 0$.

Suppose for contradiction that there are no rationals between x and y. Note that $x \neq y$; so, it cannot be the case that $p_x = p_y$ and $q_x = q_y$.

Define $z = \dfrac{p_z}{q_z} = \dfrac{\frac{p_x}{q_x} + \frac{p_y}{q_y}}{2} = \dfrac{\frac{p_x q_y}{q_x q_y} + \frac{p_y q_x}{q_x q_y}}{2} = \dfrac{p_x q_y + p_y q_x}{2 q_x q_y}$.

First, note that $p_x q_y + p_y q_x$ is an integer (because it's a linear combination of integers). Second, note that $2q_x q_y$ is a *non-zero* integer, because $q_x, q_y \neq 0$.

Furthermore, note that $\dfrac{p_z}{q_z}$ is the *average* of x and y. Since $x \neq y$, the average must be larger than x and less than y.

It follows that z is a rational number such that $x < z < y$, which is what we were trying to prove.
So, the implication is true, as is the entire statement.