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 2
- 1.1 Technique Outlines . . . 2
- 1.2 Example . . . 2

2 Implication Proofs 3
- 2.1 Technique Outlines . . . 3
- 2.2 Examples . . . 4

3 Contradiction Proofs 5
- 3.1 Technique Outlines . . . 5
- 3.2 Example . . . 5

4 Set Proofs 6
- 4.1 Technique Outlines . . . 6
- 4.2 Example . . . 7

5 Induction Proofs 8
- 5.1 Technique Outlines . . . 8
- 5.2 Example . . . 9

6 Strong Induction Proofs 10
- 6.1 Technique Outline . . . 10
- 6.2 Example . . . 11

7 Structural Induction Proofs 13
- 7.1 Technique Outline . . . 13
- 7.2 Example . . . 13

8 Irregularity Proofs 14
- 8.1 Technique Outline . . . 14
- 8.2 Example . . . 14

9 Diagonalization Proofs 15
- 9.1 Technique Outline . . . 15
- 9.2 Example . . . 15

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. Now, x represents an arbitrary element, and we can just use it. Prove $P(x)$ by some other strategy. Since x was arbitrary, the claim is true.	Let x be arbitrary. Note that by the law of excluded middle, $x = 5$ or $x \neq 5$. 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 $x = \boxed{\text{expression that satisfies } P(x)}$. Now, explain why $P(x)$ is true. Since $P(x)$ is true, the claim is true.	[We can choose any even number here. We'll go with 2, because it's simplest.] Let $x = \boxed{2}$. Note that 2 is even, by definition, because $2 \times 1 = 2$. 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: $\boxed{\text{the negation of } P(x)}$. Prove $\neg P(x)$ using some other proof strategy. Since $\neg P(x)$ is true, $P(x)$ is false.	We show that 4 is not odd by showing it's even. Note that 4 is even, by definition, because $2 \times 2 = 4$. 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.	Suppose $x \leq 4$ is even, positive integer.
Prove B using the additional assumption that A is true.	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 B is true. Therefore, $A \rightarrow B$.	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.	We go by contrapositive. Suppose $x = 3$.
Prove $\neg A$ using the additional assumption that $\neg B$ is true.	Then, $x^2 - 6x + 9 = 3^2 - 6 \times 3 + 9 = 0$.
So, $\neg A$ is true. Therefore, $A \rightarrow B$.	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 $\forall x\ \forall y\ ((x < y) \to (\exists z\ x < z \land z < y))$ **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 $2 q_x q_y$ 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.

3 Contradiction Proofs

3.1 Technique Outlines

<table>
<tr><th colspan="2">Proving a Statement By Contradiction</th></tr>
<tr><td>Prove P.</td><td>Prove if a is a non-zero rational and b is irrational, then ab is irrational.</td></tr>
<tr><td>Assume for the sake of contradiction that $\neg P$ is true.

Prove Q and prove $\neg Q$ for some Q by some other strategy using $\neg P$ as an assumption.

However, Q and $\neg Q$ cannot both be true; so since the only assumption we made was $\neg P$, it must be the case that $\neg P$ is false. Then, P is true. Since x was arbitrary, the claim is true.</td><td>Suppose a is rational (and non-zero) and b is irrational. Now, assume for the sake of contradiction that ab is rational.

By definition of rational, we have $p, q \neq 0$ such that $ab = \frac{p}{q}$. Re-arranging the equation, we have $b = \frac{p}{aq}$. Note that this is valid because $a \neq 0$. Furthermore, we found numbers $p' = p$ and $q' = aq$ where $q' \neq 0$ (because $a, q \neq 0$.). So, it follows that b is rational!

However, we know that b can't *both* be rational and irrational; so, our assumption (ab is rational) must be false. So, ab is irrational.</td></tr>
</table>

3.2 Example

Prove $\forall x \left((x > 0) \to \left(x + \frac{1}{x} \geq 2\right)\right)$ **Domain: Reals**

Proof: Let $x > 0$ be arbitrary.

Suppose for contradiction that $x + \frac{1}{x} < 2$.

Then, multiplying both sides by x, we have $(x^2+1 < 2x) \to (x^2-2x+1 < 0)$. Factoring gives us $(x-1)^2 < 0$.

However, every square must be at least zero; so, this is a contradiction. It follows that $x + \frac{1}{x} \geq 2$, as claimed.

4 Set Proofs

4.1 Technique Outlines

Proving $S = T$

Prove $S = T$.

[If one of the sets has a complement in it, then make sure to define the universal set: $\mathcal{U}$.]

Make incremental changes to the definition of the set via a series of equalities. The idea is to use the theorems we have for logic to prove things about the sets.

Prove $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

$$\begin{aligned} A \cap (B \cup C) &= \{x : x \in (A \cap (B \cup C))\} && \text{[By definition of containment]} \\ &= \{x : x \in A \wedge x \in (B \cup C)\} && \text{[By definition of } \cap\text{]} \\ &= \{x : x \in A \wedge (x \in B \vee x \in C)\} && \text{[By definition of } \cup\text{]} \\ &= \{x : (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C)\} && \text{[By distributivity of } \wedge, \vee\text{]} \\ &= \{x : (x \in A \cap B) \vee (x \in A \cap C)\} && \text{[By definition of } \cap\text{]} \\ &= \{x : x \in ((A \cap B) \cup (A \cap C))\} && \text{[By definition of } \cup\text{]} \\ &= (A \cap B) \cup (A \cap C) && \text{[By definition of containment]} \end{aligned}$$

Proving $S \subseteq T$

Prove $S \subseteq T$.

Suppose $x \in S$.

Use some other proof strategy to show that $x \in T$. Usually, this is a series of implications that looks very much like proving $S = T$.

So, $x \in T$. Since all elements of S are also in T, it follows that $S \subseteq T$.

Prove $A \cap (B \cap C) \subseteq A \cup (B \cup C)$.

Suppose $x \in A \cap (B \cap C)$.

Then, by definition of intersection, $x \in A$, $x \in B$, and $x \in C$. Since x is contained in all three, we also have $x \in A \vee (x \in B \vee x \in C)$. So, by definition of union, we have $x \in A \cup (B \cup C)$.

It follows that $A \cap (B \cap C) \subseteq A \cup (B \cup C)$.

Proving $S = T$

Prove $S = T$.

We prove that $S \subseteq T$ and $T \subseteq S$ to show that $S = T$.

Prove $S \subseteq T$.

Prove $T \subseteq S$.

Since $S \subseteq T$ and $T \subseteq S$, $S = T$.

4.2 Example

Prove $S = T$

Let $S = \{x \in \mathbb{R} \mid x^2 > x + 6\}$ and $T = \{x \in \mathbb{R} \mid x > 3 \vee x < -2\}$.

Proof: To prove that $S = T$, we first prove that $S \subseteq T$, and then we prove that $T \subseteq S$.
Let x be an arbitrary element of S. Then, it follows that $x \in \mathbb{R}$ and $x^2 > x + 6$. Using algebra, we can simplify this inequality to $x^2 - x - 6 > 0$. Factoring, we get $(x - 3)(x + 2) > 0$. Since $(x - 3)(x + 2)$ is positive, it must either be the case that both factors are positive or both factors are negative.

Case I (Both are positive): Then, we have $x - 3 > 0$ and $x + 2 > 0$. Rearranging these equations, we see that $x > 3$ and $x > -2$. It follows that in this case, $x \in T$, because $x > 3$.

Case II (Both are negative): Then, we have $x - 3 < 0$ and $x + 2 < 0$. Rearranging these equations, we see that $x < 3$ and $x < -2$. It follows that in this case, $x \in T$, because $x < -2$.

Since in either case **if $x \in S$, then $x \in T$, we have $S \subseteq T$.**
Now, we prove that $T \subseteq S$. Let $x \in T$. Then, either $x > 3$ or $x < -2$. We take this in two cases:

Case I ($x > 3$): If $x > 3$, then $x - 3 > 0$ and $x + 2 > 0$. It follows that $(x - 3)(x + 2) > 0$, because both factors are greater than 0. So, $x \in S$.

Case II ($x < -2$): If $x < -2$, then $x + 2 < 0$ and $x - 3 < 0$. It follows that $(x - 3)(x + 2) > 0$, because both factors are less than 0. So, $x \in S$.

Since in either case **if $x \in T$, then $x \in S$, we have $T \subseteq S$.**
Since $S \subseteq T$ and $T \subseteq S$, we have $S = T$, which is what we were trying to prove.