CS 13: Mathematical Foundations of Computer Science

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 ∀ 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 ∃ 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 non-zero reals. 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 in the domain. 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 $\implies$ (Directly)

Prove $A \implies B$.	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, $A \implies B$.	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 $\implies$ (Contrapositive)

Prove $A \implies B$.	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, $A \implies B$.	So, $x^2 - 6x + 9 = 0$. Thus, if $x^2 - 6x + 9 \neq 0$, then $x \neq 3$.

2.2 Examples

Prove $\forall x\ \forall y\ ((x + y = 1) \implies (xy = 0))$ **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 $\forall x\ \forall y\ ((x < y) \implies (\exists z\ x < z \land z < y))$ **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 $q_y \neq 0$.

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 Set Proofs

3.1 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 $T \subseteq S$, $S = T$.

3.2 Example

Prove $S = T$

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

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.

4 Contradiction Proofs

4.1 Technique Outlines

Proving a Statement By Contradiction

Prove P.	Prove if a is a non-zero rational and b is irrational, then ab is irrational.
Assume for the sake of contradiction that $\neg P$ is true.	Suppose a is rational (and non-zero) and b is irrational. Now, assume for the sake of contradiction that ab is rational.
Prove Q and prove $\neg Q$ for some Q by some other strategy using $\neg P$ as an assumption.	By definition of rational, we have $ab = \frac{p}{q}$ for integers p, q, such that $q \neq 0$. Re-arranging the equation, we have $b = \frac{p}{aq}$. (Note that this is valid because $a \neq 0$.) Furthermore, we now have integers $p' = p$ and $q' = aq$ where $q' \neq 0$ (because $a, q \neq 0$.). So, it follows that $b = \frac{p'}{q'}$ is rational!
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.	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.

4.2 Example

Prove $\forall x \left((x > 0) \implies \left(x + \frac{1}{x} \geq 2 \right) \right)$ **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 $(x^2 + 1 < 2x) \implies (x^2 - 2x + 1 < 0)$. 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.

5 Induction Proofs

5.1 Technique Outlines

Proving $\forall(n \in \mathbb{N})\ P(n)$

Prove $\forall(n \in \mathbb{N})\ P(n)$.

Let $P(n)$ be " definition of P(n) here–this must have a truth value! ".
We prove $P(n)$ for all $n \in \mathbb{N}$ by induction on n.

Base Case:

> Prove $P(0)$ is true. This is often done by plugging in 0 and evaluating sides of an (in)equality.

So, $P(0)$ is true.

Induction Hypothesis:

Suppose $P(k)$ is true for some $k \in \mathbb{N}$.

Induction Step:

We want to show $P(k+1)$ is true.

> Prove $P(k+1)$ is true *using* $P(k)$ *as an assumption*. You *must* use the IH (induction hypothesis) somewhere in this proof and cite it when you use it.

So, $P(k) \implies P(k+1)$ for all $k \in \mathbb{N}$.

It follows that $P(n)$ is true for all $n \in \mathbb{N}$ by induction.

5.2 Example

Prove $\forall (n \in \mathbb{N}) \sum_{i=0}^{n} i = \frac{n(n+1)}{2}$

Let $P(n)$ be " $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$ ". We prove $P(n)$ for all $n \in \mathbb{N}$ by induction on n.

Base Case:

Note that $\sum_{i=0}^{0} i = 0 = \frac{0(0+1)}{2}$.

So, $P(0)$ is true.

Induction Hypothesis:

Suppose $P(k)$ is true for some $k \in \mathbb{N}$.

Induction Step:

We want to show $P(k+1)$ is true.

Note that:

$$\begin{aligned}
\sum_{i=0}^{k+1} i &= \left(\sum_{i=0}^{k} i\right) + (k+1) && \text{[Splitting the summation]} \\
&= \left(\frac{k(k+1)}{2}\right) + (k+1) && \text{[By IH]} \\
&= (k+1)\left(\frac{k}{2} + 1\right) && \text{[Factoring]} \\
&= (k+1)\left(\frac{k+2}{2}\right) && \text{[Multiplying by 1]} \\
&= \frac{(k+1)(k+2)}{2} && \text{[Algebra]}
\end{aligned}$$

So, $P(k) \implies P(k+1)$ for all $k \in \mathbb{N}$.

It follows that $P(n)$ is true for all $n \in \mathbb{N}$ by induction.

6 Strong Induction Proofs

6.1 Technique Outlines

Proving $\forall(n \in \mathbb{N})\ P(n)$

Prove $\forall(n \in \mathbb{N})\ P(n)$.

Let $P(n)$ be " definition of P(n) here–this must have a truth value! ".
We prove $P(n)$ for all $n \in \mathbb{N}$ by strong induction on n.

Base Cases:

> Prove $P(0), P(1), \ldots P(x)$ are true up to some specific small $x \in \mathbb{N}$.

So, $P(0), P(1), \ldots, P(x)$ is true.

Induction Hypothesis:

Suppose $P(k)$ is true for all $0 \leq k \leq \ell$ for some $\ell \geq x$.

Induction Step:

We want to show $P(\ell + 1)$ is true.

> Prove $P(\ell + 1)$ is true *using* $P(0), P(1), \ldots P(\ell)$ *as an assumption*. You *must* use the IH (induction hypothesis) somewhere in this proof and cite it when you use it.

So, the strong induction step holds.

It follows that $P(n)$ is true for all $n \in \mathbb{N}$ by induction.

6.2 Example

Let

$$a_n = \begin{cases} 1 & \text{if } n = 0 \\ 1 & \text{if } n = 1 \\ 2a_{n-1} + 3a_{n-2} & \text{if } n \geq 2 \end{cases}$$

Prove $a_n = \frac{1}{2}(3^n - (-1)^{n+1})$ for $n \in \mathbb{N}$

Let P(n) be the statement "$a_n = \frac{1}{2}(3^n - (-1)^{n+1})$" for all $n \in \mathbb{N}$. We prove P(n) by strong induction for all $n \in \mathbb{N}$.

Base Case:

Note that $a_0 = 1 = \frac{1}{2}(3^0 - (-1)^1)$ and $a_1 = 1 = \frac{1}{2}(3^1 - (-1)^2)$.

So, $P(0)$ and $P(1)$ are true.

Induction Hypothesis:

Suppose $P(k)$ is true for all $0 \leq k \leq \ell$ for some $\ell \geq 1$.

Induction Step:

We want to show $P(\ell + 1)$ is true.

By the definition of a_n (where $n \geq 2$), we have: $a_{\ell+1} = 2a_\ell + 3a_{\ell-1}$. By our IH, we have $a_\ell = \frac{1}{2}(3^\ell - (-1)^{\ell+1})$ and $a_{\ell-1} = \frac{1}{2}(3^{\ell-1} - (-1)^\ell)$.
Substituting into $a_{\ell+1}$, we see:

$$\begin{aligned} a_{\ell+1} &= 2\left(\frac{1}{2}(3^\ell - (-1)^{\ell+1})\right) + 3\left(\frac{1}{2}(3^{\ell-1} - (-1)^\ell)\right) \\ &= 3^\ell - (-1)^{\ell+1} + \frac{1}{2}\left(3^\ell - 3(-1)^\ell\right) \\ &= \frac{1}{2}\left(2 \times 3^\ell + 3^\ell - 2(-1)^{\ell+1} - 3(-1)^\ell\right) \\ &= \frac{1}{2}\left(3^{\ell+1} - (-1)^{\ell+1}(2-3)\right) \\ &= \frac{1}{2}\left(3^{\ell+1} - (-1)^{\ell+2}\right) \end{aligned}$$

So, the strong induction step holds.

It follows that $P(n)$ is true for all $n \in \mathbb{N}$ by induction.

7 Structural Induction Proofs

7.1 Technique Outlines

Proving $\forall(T \in \text{Trees})\ P(T)$ for Trees with elements from A

Prove that $\forall(T \in \text{Trees})\ P(T)$

(the domain of trees is usually implicit in the problem and does not explicitly need to be stated)

Let $P(T)$ be " definition of $P(T)$ here–this must have a truth value! ".
We prove $P(T)$ for all $T \in$ Trees by structural induction on T.

Base Case:

> Prove $P(\texttt{Nil})$ is true (and possibly some other base cases if the claim you're proving has multiple base cases).

So, $P(\texttt{Nil}), \ldots$ is true.

Induction Hypothesis:

Suppose $P(L)$ and $P(R)$ is true some trees $L, R \in$ Trees.

Induction Step:

We want to show $P(T)$ is true for $T = \texttt{Tree}(x, L, R)$ for all $x \in A$.

> Prove $P(T)$ is true *using* $P(L), P(R)$ *as an assumption*. You *must* use the IH (induction hypothesis) somewhere in this proof and cite it when you use it.

So, the structural induction step holds.

It follows that $P(T)$ is true for all $T \in$ Trees over A by induction.

7.2 Example

Let

$$\begin{aligned}
\texttt{flip}(\texttt{Nil}) &= \texttt{Nil} \\
\texttt{flip}(\texttt{Tree}(x, L, R)) &= \texttt{Tree}(x, \texttt{flip}(R), \texttt{flip}(L))
\end{aligned}$$

Prove $\texttt{flip}(\texttt{flip}(T)) = T$ for $T \in$ Trees over $\mathbb{Z}$

For all $T \in$ Trees, let $P(T)$ be the statement "$\texttt{flip}(\texttt{flip}(T)) = T$". We prove $P(T)$ by structural induction for all $T \in$ Trees.

Base Case:

Note that by definition of $\texttt{flip}$, $\texttt{flip}(\texttt{flip}(\texttt{Nil})) = \texttt{flip}(\texttt{Nil}) = \texttt{Nil}$.

So, $P(\texttt{Nil})$ is true.

Induction Hypothesis:

Suppose $P(L)$ and $P(R)$ are true for some $L, R \in$ Trees.

Induction Step:

We want to show $P(\texttt{Tree}(x, L, R))$ is true for all $x \in \mathbb{Z}$.

Observe that we have

$$\begin{aligned}
\texttt{flip}(\texttt{flip}(\texttt{Tree}(x, L, R))) &= \texttt{flip}(\texttt{Tree}(x, \texttt{flip}(R), \texttt{flip}(L))) && [\text{Def of } \texttt{flip}] \\
&= \texttt{Tree}(x, \texttt{flip}(\texttt{flip}(L)), \texttt{flip}(\texttt{flip}(R))) && [\text{Def of } \texttt{flip}] \\
&= \texttt{Tree}(x, L, R) && [\text{by IH}]
\end{aligned}$$

So, the structural induction step holds.

It follows that $P(T)$ is true for all $T \in$ Trees by induction.

8 Graph Induction Proofs

8.1 Technique Outlines

Proving $\forall(G \in \text{Graphs})\ P(G)$

Prove that $\forall(G \in \text{Graphs})\ P(G)$

Let $P(G)$ be " definition of $P(G)$ here–this must have a truth value! ".
We prove $P(G)$ by graph induction for all $G \in \text{Graphs}$.

Base Case:

> Prove $P((\varnothing, \varnothing))$ is true. (This is a graph with no vertices and no edges.) You may possibly want to prove some other base cases if the claim you're proving has multiple base cases.

So, $P((\varnothing, \varnothing)), \ldots$ is true.

Induction Hypothesis:

Suppose $P(G)$ is true for all $G = (V, E) \in \text{Graphs}$ which have $|V| = n$, for some $n \in \mathbb{N}$. (These are all graphs with n vertices.)

Induction Step:

We want to show $P(G)$ is true for $G = (V, E) \in \text{Graphs}$ which has $|V| = n + 1$.

> Construct $G' = (V', E')$, a reduced version of G with one fewer vertex, i.e.: $|V'| = |V| - 1 = n$. (You should provide the method for constructing G'. You will likely want G' to have specific, useful properties; if so, you should prove that it is always possible to construct a G' with those properties.)
>
> Since G' has $|V'| = n$, by the induction hypothesis, $P(G')$ is true. You *must* use the IH as an assumption in this proof and cite it when you use it.
>
> Now, return from G' to G. Ideally, you selected G' such that $P(G')$ now provides useful information about G. Using $P(G')$, prove that $P(G)$ holds.

So, the induction step holds.

It follows that $P(G)$ is true for all $G \in \text{Graphs}$ by induction.

8.2 Example

Prove that for all graphs $G = (V, E)$, if $\max_{v \in V} d(v) = k$ then G is $k + 1$-colorable

For all $G \in$ Graphs where $G = (V, E)$, let $P(G)$ be the statement "if $\max_{v \in V} d(v) = k$ then G is $k + 1$-colorable". We prove $P(G)$ by graph induction for all $G \in$ Graphs.

Base Case:

Let $G = (\varnothing, \varnothing)$. There are no vertices, so maximum degree is 0 and G can be colored in 1 color.
Let $G = (V, E)$ with $|V| = 1$ and arbitrary E. One vertex always has degree 0 and can be colored in 1 color.

So, $P(G = (V, E))$ is true when $|V| = 0$ and $|V| = 1$.

Induction Hypothesis:

Suppose $P(G)$ is true for all $G = (V, E) \in$ Graphs which have $|V| = n$, for some $n \in \mathbb{N}$.

Induction Step:

We want to show $P(G)$ is true for $G = (V, E) \in$ Graphs which has $|V| = n + 1$.

Assume $\max_{v \in V} d(v) = k$.

Let $w \in V$ be a vertex with $d(w) = k$. Let $G' = (V', E')$ be G with w removed. (That is, $V' = V \setminus \{w\}, E' = \{e \in E : w \notin e\}$.) This means $|V'| = n$. Let $k' = \max_{v \in V'} d(v) \leq k$.

By the induction hypothesis, G' is $k' + 1$-colorable. Since $k' \leq k$, G' is $k + 1$-colorable.

Add w and its edges back to G'. The new edges are $\{e \in E : w \in e\}$. Since $d(w) = k$, there are k such edges, and w has k neighbors. Those neighbors have at most k distinct colors between them, so one of the $k + 1$ colors can be used for w.

The resulting graph is G and $k + 1$-colorable.

So, the induction step holds.

It follows that $P(G)$ is true for all $G \in$ Graphs by induction.