Proof by Contradiction and Proof by Induction

CSC165 Week 5

Lindsey Shorser, Winter 2021

Proof Techniques so far:

- Direct Proof of an implication
- Proof of a ∀ statement
- Proof of a ∃ statement
- Proof of the contrapositive
- Proof by cases

New Proof Techniques:

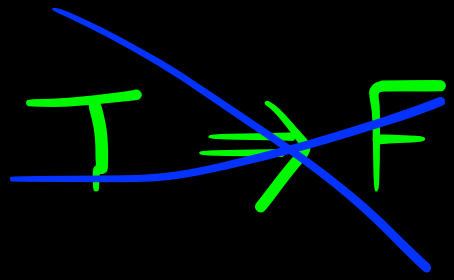
- Proof by contradiction
- Proof by Induction

Proof by Contradiction — General Structure

We want to show that statement A is true.

- Assume ¬A is true.

Show that ¬A $\Longrightarrow$ a contradiction.



Given a correct implication, this must mean that ¬A is false.

Therefore, A is true.

Q.E.D.

Example: Prove that there are infinitely many prime numbers.

Example: Prove that there are infinitely many prime numbers.

Strategy: Assume that there ~~is not infinitely many~~ are finitely many prime numbers.

Example: Prove that there are infinitely many prime numbers.

Strategy: Assume that there is not infinitely many prime numbers.

Want to show: There is no largest prime number.

Example: Prove that there are infinitely many prime numbers.

Strategy: Assume that there is not infinitely many prime numbers.

Want to show: There is no largest prime number.

$$\neg \left(\forall x \in \mathbb{N},\ \exists n \in \mathbb{N},\ \text{Prime}(n) \wedge (x < n) \right)$$

Proof: We want to show that there are infinitely many prime numbers in a proof by contradiction.

Assume that there are not infinitely many prime numbers.

So $\exists x \in \mathbb{N}, \forall n \in \mathbb{N}, \neg \text{Prime}(n) \vee (x \geq n)$

Proof: We want to show that there are infinitely many prime numbers in a proof by contradiction.

Assume that there are not infinitely many prime numbers.

So $\exists x \in \mathbb{N}, \forall n \in \mathbb{N}, \neg \text{Prime}(n) \vee (x \geq n)$

We will try proof that the last bracket is true and thereby get a contradiction.

Proof: We want to show that there are infinitely many prime numbers in a proof by contradiction.

Assume that there are not infinitely many prime numbers.

So $\exists x \in \mathbb{N}, \forall n \in \mathbb{N}, \neg Prime(n) \vee (x \geq n)$

Let $p_1, p_2, \ldots p_n$ be a complete list of all prime numbers.

Let $x = (p_1)(p_2)(p_3)\ldots(p_n) + 1$

What do we know about $x = (p_1)(p_2)(p_3)\ldots(p_n) + 1$?

$p_1 \nmid x$

because when we divide x by p1 we get a remainder of 1. The same is true for p2, ..., pn

$p_2 \nmid x$

$\vdots$

$p_n \nmid x$

The only factors of x are 1 and itself.

Therefore, x is prime and bigger than p1, ..., pn. So this contradicts the idea that p1,...,pn is a complete list of all primes.

Therefore, we can always find a prime that is bigger than any given set of primes.

What do we know about $x = (p_1)(p_2)(p_3)\ldots(p_n) + 1$?

The Unique Factorization Theorem says that all natural numbers > 1 can be written uniquely as a product of prime numbers with multiplicities (exponents).

$6 = 2^1 3^1$

$100 = 2^2 5^2$

x is a prime number because its only factors are 1 and itself. Also, it is bigger than all of the primes in the list (p1,...pn) and so it is not on the list

This contradicts the idea that $p_1,\ldots,p_n$ is a complete list of prime numbers.

Therefore, $\forall x \in \mathbb{N}, \exists n \in \mathbb{N}, \text{Prime}(n) \wedge (x < n)$ Q.E.D.

Proof by Induction — General Structure

We want to prove that the statement P(n) is true for all natural numbers n.

In other words, we want to prove $\forall n \in \mathbb{N}, P(n)$.

Step 1: Base case $n = 0$

Prove P(0) (or any other case that should be verified first.

Step 2: Induction hypothesis

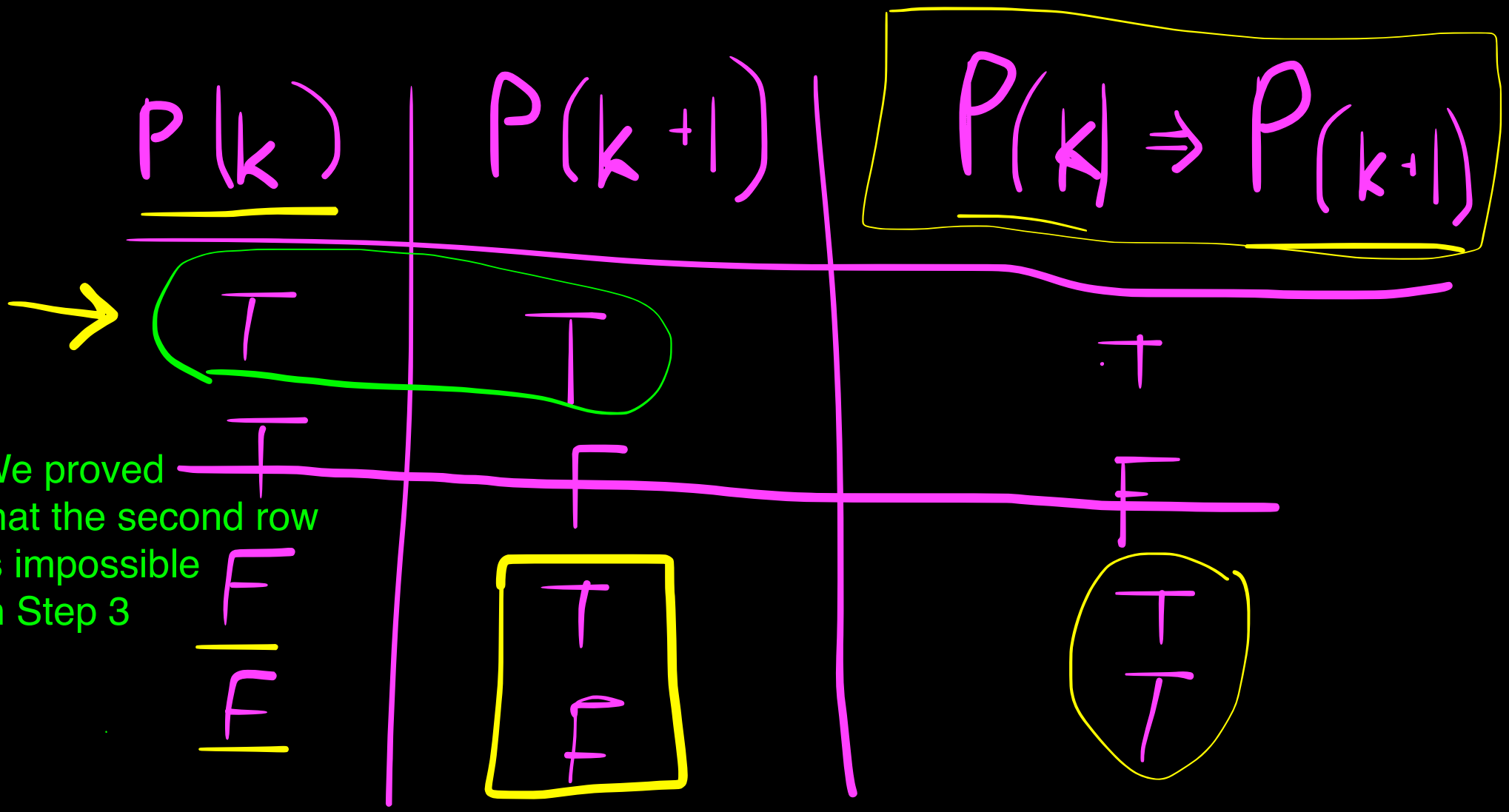
Since we want to show that $P(k) \Longrightarrow P(k+1)$,

We assume P(k) is true. (let n = k)

Step 3: Let n = k+1 and Prove P(k+1)

This is where we use the induction hypothesis P(k) to prove P(k+1) must also be true.

Why do we need to prove the base case?



We proved that the second row is impossible in Step 3

To eliminate the possibility that we are in rows 3 or 4, we prove that the base case is true, so P(k) is true for at least one value of k.

Example: $\forall n \in \mathbb{N}, n \geq 3 \implies 2n+1 < 2^n$

$P(n) = 2n+1 < 2^n$ <-- the base case has to be n=3

$Q(n) = n \geq 3 \implies 2n+1 < 2^n$ <-- This is still true for n<=3

→ $Q(k) \implies Q(k+1)$

Example: $\forall n \in \mathbb{N}, n \geq 3 \Longrightarrow 2n+1 < 2^n$ (Method 1)

We want to show that $\forall n \in \mathbb{N}$, P(n) is true.

Base Case: P(3) Let n = 3

$n = 3$

$LHS = 2(3)+1 = 7 < 8 = 2^3 = RHS$

Induction Hypothesis: Assume P(k) Let n = k

$\exists k \in \mathbb{N}, \; 2k+1 < 2^k$

Proof of P(k+1): Let n = k+1

$LHS = 2(k+1)+1 = (2k+1)+2 < 2^k + 2$ (by induction hypothesis)

Since $k \geq 3 \Longrightarrow 2^k + 2 < 2^k + 2^k = 2(2^k) = 2^{k+1}$

Q.E.D

LHS: 2(k+1) + 1 (where n = k+1 and we start with 2n+1)

= 2k + 2 + 1

= (2k+1) + 2

< 2^k + 2 (by induction hypothesis: 2k+1 < 2^k)

$< 2^k + 2^k$ because k > = 3 ==> k >=1

= 2^k + 2^k

= 2(2^k)

RHS: = 2^{k+1}

LHS = Left Hand Side, RHS = Right Hand Side

Example: $\forall n \in \mathbb{N}, n \geq 3 \implies 2n+1 < 2^n$ (Method 2)

We want to show that $\forall n \in \mathbb{N}$, Q(n) is true.

Three cases:

- $n < 3$ P(0) is true because 0 < 3, same with P(1) and P(2)
- $n = 3$ P(3): LHS = 7, RHS = 8. Therefore LHS < RHS
- $n > 3$ We will prove this by proving the implication that Q(k) ==> Q(k+1)

P(4) base case?

Induction Hypothesis: Assume Q(k) Let $n = k \in \mathbb{N}$

Assume k >= 3 ==> 2k+1 < 2^k

Proof of Q(k+1):

Assume k+1 >= 3 ==> k >= 2 The rest is like the proof of P(k+1).