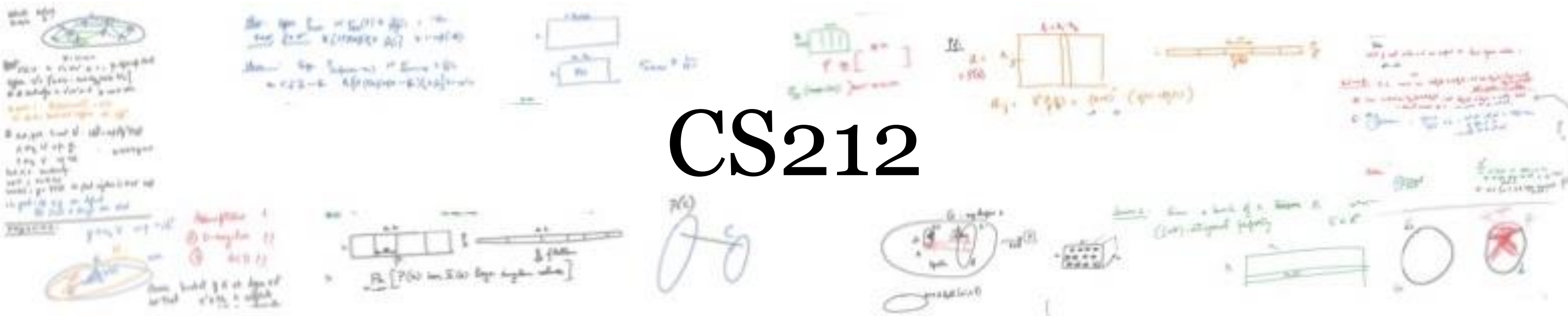


CS212

Mathematical Foundations of Computer Science

Lecture 3: Proofs by Contradiction and Induction

Outline

- Different types of Proofs
- Proof by Contradiction
- Principle of Mathematical Induction
- Examples

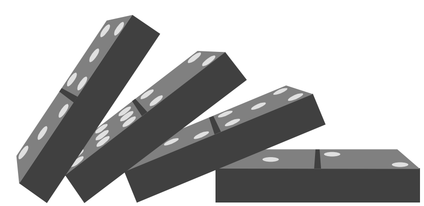
Types of Proofs

- Direct Proof

$$\boxed{\text{Axioms}} \Rightarrow S_1 \Rightarrow S_2 \Rightarrow S_3 \Rightarrow \boxed{\text{Proposition}}$$

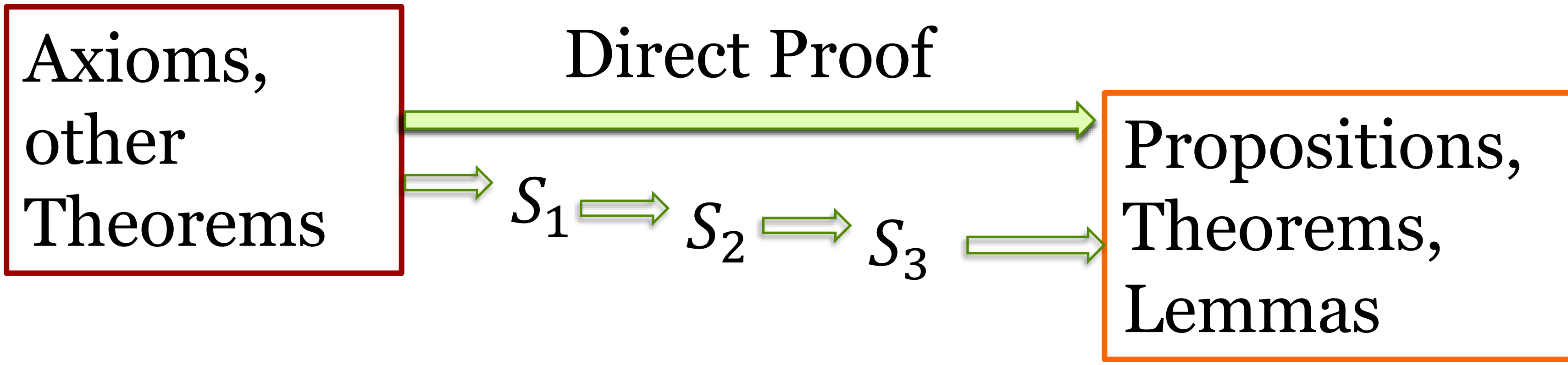
- Proof by Cases
- Proof by Contrapositivity

- Proof by Contradiction



- Proof by Mathematical Induction

Direct Proofs



Eg. Axioms $A_1, A_2, .. A_k$ implies propositions S_1, S_2, S_3 which in turn implies required Theorem/ Proposition.

Most high school proofs are direct proofs (e.g. Pythagoras theorem, many Geometry proofs).

Proof by Cases

Proposition. If (proposition) P, then (proposition) Q

i.e., to prove $P \Longrightarrow Q$

Proof structure.

Step 1: If P is true, then either (a) P1 is true, or (b) P2 is true
Step 2: Case (a): Show P1 implies Q
Step 3: Case (b) Show P2 implies Q

Can also have several (more than two) cases.

Proof by Cases: An example

Proposition. If $\underbrace{x + y \geq 4}_{P}$, then $\underbrace{\text{at least one of } x, y \geq 2}_{Q}$.

Proof.

Case 1: $x \geq 2$: Proposition Q is true!

Case 2: $x < 2$: $x + y \geq 4 \Rightarrow y \geq 4 - x$

$$> 4 + (-2) \geq 2$$

$-x > -2$

Proposition Q is true. $\square$

$P \overset{?}{\Downarrow} Q$

P ⇒ Case 1: $x \geq 2$ ⇒ P_1 ⇒ Q ✓

P ⇒ Case 2: $x < 2$ ⇒ P_2 ⇒ Q ✓

Proof by Contrapositive

Proposition. If (proposition) P, then (proposition) Q

i.e. to prove P $\Longrightarrow$ Q

Proof structure.

We will prove the contrapositive (logically equivalent statement)

P Q

Eg: x is not a multiple of 3 $\Longrightarrow$ x is not a multiple of 6.

i.e. we will prove that (not Q) implies (not P)

Contrapositive?

$$\neg Q \implies \neg P$$

$\neg$ — negation

$\Rightarrow$ — implies

a) x is a multiple of 3 $\Longrightarrow$ x is a multiple of 6.

b) x is a multiple of 6 $\Longrightarrow$ x is a multiple of 3

c) x is not a multiple of 6 $\Longrightarrow$ x is not a multiple of 3

Warning: Remember contrapositive is not the same as converse!

Proof by Contrapositive

P

Proposition. If $a \times b$ is not a multiple of n, then a is not a multiple of n and b is not a multiple of n.

$P \Rightarrow Q$

Q

Contrapositive : $\neg Q \Rightarrow \neg P$

Proof.

We will prove the contrapositive i.e., we need to prove:

$\neg Q$

If a is a multiple of n **or** b is a multiple of n,
then ab is a multiple of n $\neg P$

Case 1 : a is a multiple of n. Then $a \times b = (k \times n) \times b$

$a = k \times n$ $= (kb) \times n$

$\uparrow$ k is an integer

$\Rightarrow$ ab is a multiple of n

Case 2 : a is not a multiple of n $\Rightarrow$ b is a multiple of n

$b = k' \times n \Rightarrow a \times b = a \times k' \times n = (ak') \times n \Rightarrow$ a multiple of n

Proof by Contradiction

Proposition. If P (is true), then Q (is true).

Proof.

Suppose not i.e. $P \wedge (\neg Q)$
(suppose P is true and Q is false)

Then.....

....

....

it follows that $C \wedge \neg C$
i.e. a contradiction ($\Rightarrow\Leftarrow$)

- Assume proposition is not true.
- Arrive at a contradiction
- Hence, proposition is true (called Modus Tollens in logic)

Hence P $\Longrightarrow$ Q

Infinite Primes

Prime number: Natural number p is a prime number if the only divisors of p are $\{1, p\}$.

$$p \in \{2,3,5,7,11,13,17,19,23, \ldots\}$$

- A natural number that is not prime is called composite
- Every composite number has a prime divisor.

Qn. What is the largest prime?

Theorem. There are infinite primes.

Proof by Contradiction

Theorem. There are infinite primes.

Proof. We will prove by contradiction. Suppose there are only finitely many primes (say n of them). Let $p_1, p_2, \dots p_n$ be all the primes.

Suppose not

$m = p_1 \times p_2 \times \dots \times p_n + 1$

$m > p_1, p_2, -, p_n$

m is not in $\{p_1, -, p_n\}$

Hence m is composite (since $p_1, -, p_n$ are the only prime numbers)

But every composite number has a prime divisor

When we divide m by p_1, remainder is 1. p_1 is not a divisor!

Similarly, $p_2, -, p_n$ are not divisors of m. Hence m has no prime divisor.

Contradiction ($\Rightarrow \Leftarrow$). Hence # primes is infinite. $\boxed{}$