COS210 - Theoretical Computer Science
Proofs

Theorem Proving Techniques

- **Theorem:** mathematical statement that is *true*

  "$\sqrt{2}$ is an irrational number"

  "the computational problem X is in complexity class Y"

  "$P \to Q$"

- **Proof:** sequence of statements that form an argument to show that a theorem is *true*

$$\begin{array}{rl} & P \\ \to & P' \\ \leftrightarrow & P'' \\ & \ldots \\ \to & Q \end{array}$$

How to Approach a Theorem

- Read and understand the theorem
- Consider simple example cases of the theorem
- Check if the theorem can be divided into sub theorems
- Select a suitable proof strategy
- Formally write down all steps of the proof

Proof Strategies

Common strategies we will discuss (non exhaustive list) for proving a theorem, include:

- **Direct proofs**
- **Constructive proofs**
- **Non-constructive proofs**
- **Proofs by contradiction**
- **Proofs by induction**

Direct Proof

Approach the theorem directly

Theorem

$P \rightarrow Q$

by assuming P (the *premise*) is *true* and, through a sequence of logical deductions, showing that Q (*conclusion*) must be *true*.

Direct Proof: Example

Theorem

If n is an odd positive integer, then n^2 is odd as well.

Proof:

Constructive Proof

Existence of a certain object is proven by constructing it

Theorem

There exists an object O with property P

Proof:

- Construct an object O
- Prove that O satisfies P

Constructive Proof: Example

Theorem

For any $a, b \in \mathbb{R}$ *where* $a < b$ *there exists a* $c \in \mathbb{R}$ *such that* $a < c < b$

Proof:

Proof by Contradiction

Proof by contradiction relies on a logical manipulation of the statement to be proven.

Theorem

Statement S is true

Proof by Contradiction:

- Assume that statement S is *false*.
- Then, derive a contradiction.
- The contradiction implies that S cannot be *false*, therefore S is *true*.

Proof by Contradiction

Application to a conditional theorem:

Theorem

If A then B. $(A \implies B)$

Proof:

- Recall that $(A \implies B) = \neg A \vee B$
- Assume that $A \implies B$ is *false*
- So $\neg(A \implies B) = \neg(\neg A \vee B) = A \wedge \neg B$
- We assume $A \wedge \neg B$, derive a contradiction, therefore $A \implies B$ must be *true*

Proof by Contradiction: Example 1

Theorem

Let n be a positive integer. If n^2 is even then n is even.

Proof:

Proof by Contradiction: Example 2

Theorem

The sum of a rational number x and an irrational number y is irrational.

Proof: