# Proof Techniques

Lecture 2

September 11, 2017

# Definitions, Theorems, and other Mathematical Creatures

- A **definition** describes the objects and notions that we talk about.
  - Definitions should be precise; as precise as, for example, Java class definitions.
- A **theorem** is a specially interesting statement proven true.
- A **lemma** is a statement that is special only because proving it assists in proving another, more significant statement.
- A **corollary** is a statement whose proof follows from the proof of a theorem.

# Proofs

- A proof is a logical argument that a statement is true.
- It is a sequence of statements; each statement follows(?) from previous statements, definitions, or already-proven results.
  - As you will see, writing a proof is pretty much like writing a program.
  - You first have to spend some time thinking about how to approach the problem, and then you have to write your program/proof using precise language.
  - Just like a program, a proof is often divided into sub-proofs.

# Example

**Theorem** *For any two sets $A$ and $B$, $\overline{A \cup B} = \overline{A} \cap \overline{B}$.*

**Proof.** (Write your own proof here and then see the text p. 20)

# Proof Techniques

- Some of the commonly used proof techniques in the theory of computation:
  1. Proof by construction
  2. Proof by contradiction
  3. Proof by induction

# 1. Proof by Construction

- Used to prove that a particular type of object exists.
- The proof demonstrates how the object is to be constructed.
- Example
  - **Definition** *A graph is* ***$k$-regular*** *if every node in the graph has degree $k$.*
  - **Theorem** *For each even number $n$ greater than 2, there exists a 3-regular graph with $n$ nodes.*
  - **Proof.** (Write your proof here and then see the text p. 21.)

# 2. Proof by Contradiction

- Strategy: Assume the statement is false and show that this leads to a contradiction.
- Example:
  - **Theorem** $\sqrt{2}$ *is irrational.*
  - **Proof.** (Write your proof here and then see the text p. 22.)

# 3. Proof by Induction

- Used to prove that all elements of some infinite set have a certain property.
- For now, consider only the infinite set, $\mathbb{N}$, of natural numbers.
- Strategy: If $\mathcal{P}$ is the property under consideration, then
  - Prove that $\mathcal{P}(1)$ is true. This is called the **basis**.
  - Prove that, for $k \in \mathbb{N}$, $\mathcal{P}(k)$ implies $\mathcal{P}(k+1)$. This is called the **induction step**.
    - The assumption that $\mathcal{P}(k)$ is true is called the **induction hypothesis**.
- Why does it work?
  - The domino effect.

# Example

**Theorem** *For any* $n \in \mathbb{N}$, $1 + 2 + 3 + \cdots + n = \dfrac{n(n+1)}{2}$.

# Example

**Theorem** *For any* $n \in \mathbb{N}$, $1 + 2 + 3 + \cdots + n = \dfrac{n(n+1)}{2}$.

**Proof.** We shall prove the theorem by using induction on $n$.

# Example

**Theorem** *For any* $n \in \mathbb{N}$, $1 + 2 + 3 + \cdots + n = \dfrac{n(n+1)}{2}$.

**Proof.** We shall prove the theorem by using induction on $n$.

*Basis:* For $n = 1$, the L.H.S. is 1 and the R.H.S is $\dfrac{1(1+1)}{2} = \dfrac{2}{2} = 1$. Since the L.H.S. = R.H.S., then the statement is true for $n = 1$.

# Example

**Theorem** *For any* $n \in \mathbb{N}$, $1 + 2 + 3 + \cdots + n = \dfrac{n(n+1)}{2}$.

**Proof.** We shall prove the theorem by using induction on $n$.

*Basis:* For $n = 1$, the L.H.S. is 1 and the R.H.S is $\dfrac{1(1+1)}{2} = \dfrac{2}{2} = 1$. Since the L.H.S. = R.H.S., then the statement is true for $n = 1$.

*Induction Hypothesis:* Assume the statement is true for some $k \in \mathbb{N}$. That is, assume that $1 + 2 + 3 + \cdots + k = \dfrac{k(k+1)}{2}$.

# Example (Cont'd)

*Induction Step:* We need to show that

$$1+2+3+\cdots+k+(k+1)=\frac{(k+1)(k+2)}{2}.$$

$$1+2+3+\cdots+k+(k+1)$$

$$=\frac{k(k+1)}{2}+(k+1) \text{ (By the induction hypothesis.)}$$

$$=\frac{k(k+1)+2(k+1)}{2}$$

$$=\frac{(k+1)(k+2)}{2} \text{ (By factoring out } (k+1).)$$

Thus, or any $n\in\mathbb{N}$, $1+2+3+\cdots+n=\frac{n(n+1)}{2}$.

# Points to take home

- Definitions, theorems, lemmas, and corollaries.
- Proofs.
- Proof by construction.
- Proof by contradiction.
- Proof by induction.

# Next time

- Formal languages.