Proof Techniques

Lecture 2

October 10, 2021

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.

Direct Proofs

- $P \to Q$: Assume P and (recursively) prove Q.
- $P \wedge Q$: Prove P and prove Q.
- $P \leftrightarrow Q$: Recall that this is just $(P \to Q) \wedge (Q \to P)$.
- $\forall x[P(x) \to Q(x)]$: Prove that $P(x) \to Q(x)$ for an arbitrary x.
  - In particular, consider an arbitrary x such that $P(x)$.

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)

Example (cont'd)

Proof.

Let A and B be two sets. We need to prove

1. $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$ and
2. $\overline{A} \cap \overline{B} \subseteq \overline{A \cup B}$

We show the first. Let $x \in \overline{A \cup B}$. By definition of complementation, $x \notin A \cup B$. Hence, by definition of union, $x \notin A$ and $x \notin B$. By definition of complementation again, $x \in \overline{A}$ and $x \in \overline{B}$. Thus, by definition of intersection, $x \in \overline{A} \cap \overline{B}$. Since x is an arbitrary member of $\overline{A \cup B}$, it follows that $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$.

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 integer 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.)

Proof by Construction (cont'd)

Proof. Let n be an even integer greater than 2. Consider the graph $G_n = (V_n, E_n)$, where

- $V_n = \{1, 2, \ldots, n\}$ and
- E_n is the smallest set satisfying the following conditions.
  1. $\{i, i+1\} \in E_n$, for $1 \leq i < n$;
  2. $\{1, n\} \in E_n$; and
  3. $\{i, i+n/2\} \in E_n$, for $1 \leq i \leq n/2$

Proof by Construction (cont'd)

We claim that G_n is 3-regular. To prove this claim, let $u \in V_n$. We consider four exhaustive and mutually exclusive cases.

1. $u = 1$. In this case, u is in exactly three edges: $\{1, 2\}$ (by the first condition), $\{1, n\}$ (by the second condition), and $\{1, 1 + n/2\}$ (by the third condition).

2. $u = n$. In this case too, u is in exactly three edges: $\{n - 1, n\}$ (by the first condition), $\{1, n\}$ (by the second condition), and $\{n/2, n\}$ (by the third condition).

3. $2 \leq u \leq n/2$. Again, u is in exactly three edges: $\{u, u + 1\}$ and $\{u - 1, u\}$ (by the first condition) and $\{u, u + n/2\}$ (by the third condition).

4. $n/2 + 1 \leq u \leq n - 1$. Again, u is in exactly three edges: $\{u, u + 1\}$ and $\{u - 1, u\}$ (by the first condition) and $\{u - n/2, u\}$ (by the third condition).

2. Proof by Contradiction

- We would like to prove a statement P.
- Assume $\neg P$.
- Find some statement Q, and prove both Q and $\neg Q$.
- By the rule of conjunction, we can derive $Q \wedge \neg Q$.
- Since, we have proved that $\neg P \rightarrow (Q \wedge \neg Q)$, and since $Q \wedge \neg Q$ is false, it must be that $\neg P$ is false.
- Hence P.

Proof by Contradiction Example

Theorem $\sqrt{2}$ *is irrational.*

Proof.

- Assume that $\sqrt{2}$ is rational.
- Thus, there are integers a and b such that $\sqrt{2} = \frac{a}{b}$.
- In particular, let $\frac{a}{b}$ be the simplest fractional representation of $\sqrt{2}$.
  - That is, the only common factor of a and b is 1.
- Hence, $2 = \frac{a^2}{b^2}$.
- It follows that $a^2 = 2b^2$, which means that a^2 is even.
- But, then, a is also even.

Proof by Contradiction Example (cont'd)

- Hence, there is an integer m with $a = 2m$.
- Now, since $a^2 = 2b^2$, it follows that $(2m)^2 = 2b^2$.
- Thus, $b^2 = 2m^2$.
- It follows that b is even.
- Consequently, there is an integer n such that $b = 2n$.
- But than a and b have a common factor other than 1, namely 2; which is a **contradiction**.
- Thus, our only assumption, that $\sqrt{2}$ is rational, must be false.

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.