Introduction to Theory CS: Workshop 2

Proofs

Alvin Chiu

Georgia Tech University

September 11, 2019

Outline

What do we need in a proof?

- A mathematical proof shows that the stated assumptions **logically** imply the conclusion.

What do we need in a proof?

- A mathematical proof shows that the stated assumptions **logically** imply the conclusion.
- **Axioms** are the "rules of the game", which we assume to be true without proof.
- **Logic** is the deductive reasoning we use to go from the axioms and assumptions to the conclusion.

What do we need in a proof?

- A mathematical proof shows that the stated assumptions **logically** imply the conclusion.
- **Axioms** are the "rules of the game", which we assume to be true without proof.
- **Logic** is the deductive reasoning we use to go from the axioms and assumptions to the conclusion.
- Example of how we use logic every week!
  - **Axiom:** If today is Friday, then I don't have to do my homework.
  - **Assumption:** Today is Friday.
  - **Conclusion:** Therefore, I don't have to do my homework!

How should we think about proofs?

- Math Proofs: Statement and Reason vs Structured Proofs
  - A proof is a list of true statements and reasons for that.
  - A proof has a structure to it, using various techniques.

How should we think about proofs?

- Math Proofs: Statement and Reason vs Structured Proofs
  - A proof is a list of true statements and reasons for that.
  - A proof has a structure to it, using various techniques.
- CS Programs: Unstructured vs Structured Programming
  - Assembly (unstructured): run a program through a set of instructions using *goto* statements.
  - C (structured): run a program through subroutines.

Propositional Logic

- We can write statements in terms of logical operations.
  - $P \vee Q = P$ or Q
  - $P \wedge Q = P$ and Q
  - $\neg P =$ not P
  - $P \to Q = \neg P \vee Q =$ If P then Q

Propositional Logic

- We can write statements in terms of logical operations.
  - $P \vee Q = P$ or Q
  - $P \wedge Q = P$ and Q
  - $\neg P =$ not P
  - $P \rightarrow Q = \neg P \vee Q =$ If P then Q
- I am either going to eat at Nave or Brittain Dining Hall.
  - Let P stand for “I eat at Nave” and Q stand for “I eat at Brittain”.
  - This is equivalent to $P \vee Q$.

Propositional Logic

- We can write statements in terms of logical operations.
  - $P \vee Q = P$ or Q
  - $P \wedge Q = P$ and Q
  - $\neg P =$ not P
  - $P \rightarrow Q = \neg P \vee Q =$ If P then Q
- I am either going to eat at Nave or Brittain Dining Hall.
  - Let P stand for "I eat at Nave" and Q stand for "I eat at Brittain".
  - This is equivalent to $P \vee Q$.
- Either Bill is at work and Jane isnt, or Jane is at work and Bill isnt.
  - Let B stand for "Bill is at work" and J stand for "Jane is at work."
  - This is equivalent to $(B \wedge \neg J) \vee (\neg B \wedge J)$.

Direct Proof

- To prove a conclusion of the form $P \to Q$:
  - **Direct Proof:** Assume P is true and then prove that Q is true.

Direct Proof

- To prove a conclusion of the form $P \to Q$:
  - **Direct Proof:** Assume P is true and then prove that Q is true.
- Example: If a and b are even integers, then $a + b$ is an even integer.
  - **Definition:** Let n be an integer. If there exists an integer k such that $n = 2k$, then n is even.
  - By definition of even integer, there exists integer k and l such that $a = 2k$ and $b = 2l$. Then $a + b = 2k + 2l = 2(k + l)$. Since $k + l$ is an integer, $a + b$ is an even integer.

Proof by Contrapositive

- Note that in logic, $P \to Q = \neg Q \to \neg P$. We call $\neg Q \to \neg P$ the **contrapositive** of $P \to Q$.
- To prove a conclusion of the form $P \to Q$:
  - **Proof by Contrapositive:** Assume Q is false ($\neg Q$) and then prove that P is false ($\neg P$).

Proof by Contrapositive

- Note that in logic, $P \to Q = \neg Q \to \neg P$. We call $\neg Q \to \neg P$ the **contrapositive** of $P \to Q$.
- To prove a conclusion of the form $P \to Q$:
  - **Proof by Contrapositive:** Assume Q is false ($\neg Q$) and then prove that P is false ($\neg P$).
- Example: If ab is an even integer, then either a or b is even.

Proof by Contrapositive Example

- If ab is an even integer, then either a or b is even.
- Can you prove this directly using our assumptions?

Proof by Contrapositive Example

- If ab is an even integer, then either a or b is even.
- Can you prove this directly using our assumptions?
  - We don't know that $ab = 2k$ implies that 2 divides a or b yet!

Proof by Contrapositive Example

- If ab is an even integer, then either a or b is even.
- Can you prove this directly using our assumptions?
  - We don't know that $ab = 2k$ implies that 2 divides a or b yet!
- Note that in logic, the statement we want to prove is $P \to (Q \vee R)$. The contrapositive of $P \to (Q \vee R)$ is

$$\neg(Q \vee R) \to \neg P = (\neg Q \wedge \neg R) \to \neg P$$

- We proceed with proof by contrapositive. Assume that a and b are both not even, so they are odd. Let $a = 2m + 1$ and $b = 2n + 1$ for integers m and n. Then

$$ab = (2m+1)(2n+1) = 4mn+2m+2n+1 = 2(2mn+m+n)+1.$$

  Since $2mn + m + n$ is an integer, ab is odd, so it is not even.
- This completes the proof!

Proof by Contradiction

- To prove a conclusion of the form P:
- Assume $\neg P$ is true. Then try to reach a contradiction. Once you have reached a contradiction, you can conclude that $\neg P$ is false.
- A contradiction is when you have the statement $P \wedge \neg P$. Both cannot be true at the same time, so the assumption must be wrong.

Proof by Contradiction

- To prove a conclusion of the form P:
- Assume $\neg P$ is true. Then try to reach a contradiction. Once you have reached a contradiction, you can conclude that $\neg P$ is false.
- A contradiction is when you have the statement $P \wedge \neg P$. Both cannot be true at the same time, so the assumption must be wrong.
- Example: Prove that $\sqrt{2}$ is irrational.
  - **Definition:** A number is *irrational* if it cannot be expressed as a fraction $\frac{p}{q}$ for any integers p and q.
  - If we want to prove this directly, we need to show that $\sqrt{2} \neq \frac{p}{q}$ for ALL integers p and q! That doesn't sound fun.

Proof by Contradiction Example

Instead, we use proof by contradiction! Assume that $\sqrt{2} = \frac{p}{q}$ for some integers p and q, where p and q share no common factors (otherwise, we would just simplify the fraction).

- By algebra, $\sqrt{2} = \frac{p}{q} \implies 2 = \frac{p^2}{q^2} \implies p^2 = 2q^2$
- Since $p^2 = 2q^2$ and q^2 is an integer, p^2 is even.
- Since p^2 is even, p must also be even. Let $p = 2r$ for some integer r.
- Then $p^2 = 4r^2 = 2q^2 \implies 2r^2 = q^2$.
- Hence, q^2 is even, So q is even.
- Both p and q are even, so they share a common factor of 2. But we assumed they shared no common factors! So we have a contradiction.

Thus, $\sqrt{2}$ is irrational.

Mathematical Induction

- To prove a conclusion of the form "For all $n \in \mathbb{N}$, $P(n)$":
  - **Base Case:** Prove that $P(1)$ is true.
  - **Induction Step:** Prove that for all $k \in \mathbb{N}, P(k) \implies P(k+1)$.
- Example: Prove that $1 + 2^1 + \cdots + 2^n = 2^{n+1} - 1$.
  - **Base Case:** $P(1)$ is true, since $1 + 2^1 = 2^2 - 1$.
  - **Induction Step:** Assume $1 + \cdots + 2^k = 2^{k+1} - 1$. Then

$$1 + \cdots + 2^k + 2^{k+1} = 2^{k+1} - 1 + 2^{k+1} = 2^{k+2} - 1$$

  - This completes the induction!

Recap

- A proof is a logical argument using true statements.
- A proof is more than just a list of statements and reasons, it has structure to it.
- There are many techniques used in proofs. In more complex proofs, multiple techniques are often used!
  - Direct Proof
  - Proof by Contrapositive
  - Proof by Contradiction
  - Mathematical Induction