CS 441 Discrete Mathematics for CS
Lecture 6

Informal proofs

Milos Hauskrecht
milos@cs.pitt.edu
5329 Sennott Square

Proofs

- The truth value of some statements about the world are obvious and easy to assess
- The truth of other statements may not be obvious, …
  …. But it may still follow (be derived) from known facts about the world

Proof: shows that the truth value of such a statement follows from (or can be inferred) from the truth value of other statements

Important questions:
- When is the argument correct?
- How to construct a correct argument, what method to use?

Theorems

- **Theorem:** a statement that can be shown to be true.
  - **Typically the theorem looks like this:**

$$\underbrace{(p1 \wedge p2 \wedge p3 \wedge \ldots \wedge pn)}_{\textbf{Premises}} \rightarrow \underbrace{q}_{\textbf{conclusion}}$$

- **Example:**

  Fermat's Little theorem:

  Premises (hypotheses)

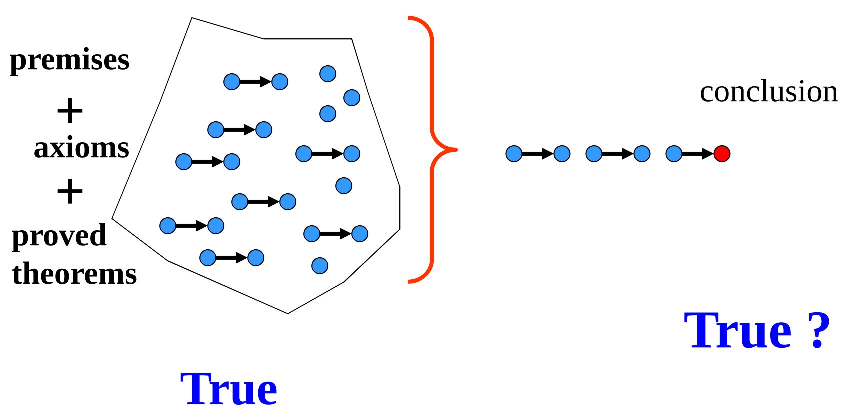
  – If p is a prime and a is an integer not divisible by p,

  then: $a^{p-1} \equiv 1 \bmod p$

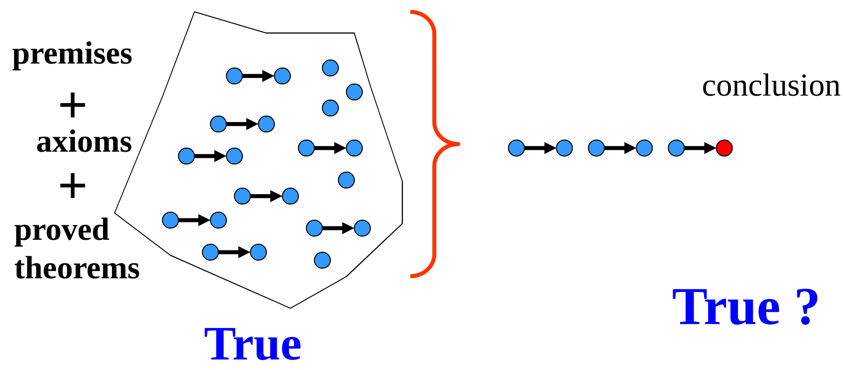
  conclusion

Formal proofs

Allow us to infer from **new True statements** from **known True statements**



Formal proofs



Steps of the proof for statements in the propositional logic are argued using:

- **Equivalence rules**
- **Rules of inference (e.g. modus ponens)**

Proofs using rules of inference

Translations:

- **Assumptions:** $\neg p \wedge q$, $r \rightarrow p$, $\neg r \rightarrow s$, $s \rightarrow t$
- **We want to show:** t

Proof:

- 1. $\neg p \wedge q$ Hypothesis
- 2. $\neg p$ Simplification
- 3. $r \rightarrow p$ Hypothesis
- 4. $\neg r$ Modus tollens (step 2 and 3)
- 5. $\neg r \rightarrow s$ Hypothesis
- 6. s Modus ponens (steps 4 and 5)
- 7. $s \rightarrow t$ Hypothesis
- 8. t Modus ponens (steps 6 and 7)
- **end of proof**

Informal proofs

Proving theorems in practice:

- The steps of the proofs are not expressed in any formal language as e.g. propositional logic
- **Steps are argued less formally** using English, mathematical formulas and so on
- One must always watch the consistency of the argument made, logic and its rules can often help us to decide the soundness of the argument if it is in question

- **We use (informal) proofs to illustrate different methods of proving theorems**

Methods of proving theorems

Basic methods to prove the theorems:

- **Direct proof**
  - $p \rightarrow q$ is proved by showing that if p is true then q follows
- **Indirect proof**
  - Show the contrapositive $\neg q \rightarrow \neg p$. If $\neg q$ holds then $\neg p$ follows
- **Proof by contradiction**
  - Show that $(p \wedge \neg q)$ contradicts the assumptions
- **Proof by cases**
- **Proofs of equivalence**
  - $p \leftrightarrow q$ is replaced with $(p \rightarrow q) \wedge (q \rightarrow p)$

Sometimes one method of proof does not go through as nicely as the other method. You may need to try more than one approach.

Direct proof

- $p \rightarrow q$ is proved by showing that if p is true then q follows
- **Example:** Prove that "If n is odd, then n^2 is odd."

Proof:

- Assume the hypothesis is true, i.e. suppose n is odd.
- Then $n = 2k + 1$, where k is an integer.

$$n^2 = (2k + 1)^2$$
$$= 4k^2 + 4k + 1$$
$$= 2(2k^2 + 2k) + 1$$

- Therefore, n^2 is odd. □

Indirect proof

- To show $p \rightarrow q$ prove its contrapositive $\neg q \rightarrow \neg p$
- Why? **$p \rightarrow q$ and $\neg q \rightarrow \neg p$ are equivalent !!!**
- Assume $\neg q$ is true, show that $\neg p$ is true.

Example: Prove If $3n + 2$ is odd then n is odd.

Proof:

- Assume n is even, that is $n = 2k$, where k is an integer.
- Then: $3n + 2 = 3(2k) + 2$

$$= 6k + 2$$
$$= 2(3k+1)$$

- Therefore $3n + 2$ is even.
- We proved **¬ "n is odd" → ¬ "3n + 2 is odd".** This is equivalent to **"3n + 2 is odd" → "n is odd".** □

Proof by contradiction

- We want to prove $p \rightarrow q$
- The only way to reject (or disprove) $p \rightarrow q$ is to show that $(p \wedge \neg q)$ can be true
- However, if we manage to prove that either q or $\neg$ p is True then we contradict $(\mathbf{p} \wedge \neg \mathbf{q})$
  - **and subsequently** $\mathbf{p} \rightarrow \mathbf{q}$ must be true
- Proof by contradiction. Show that the assumption $(\mathbf{p} \wedge \neg \mathbf{q})$ **leads either to** q or $\neg$ p which generates a contradiction.

Proof by contradiction

- We want to prove $p \rightarrow q$
- To reject $\mathbf{p} \rightarrow \mathbf{q}$ show that $(\mathbf{p} \wedge \neg \mathbf{q})$ can be true
- To reject $(\mathbf{p} \wedge \neg \mathbf{q})$ show that either **q or** $\neg$ **p** is True

Example: Prove If **3n + 2 is odd** then **n is odd**.

Proof:

- Assume **3n + 2 is odd** and **n is even**, that is n = 2k, where k an integer.

Proof by contradiction

- We want to prove $p \to q$
- To reject $\mathbf{p \to q}$ show that $\mathbf{(p \wedge \neg q)}$ can be true
- To reject $\mathbf{(p \wedge \neg q)}$ show that either **q or ¬ p** is True

Example: Prove If **3n + 2 is odd** then n is odd.

Proof:

- Assume **3n + 2 is odd** and n is even, that is n = 2k, where k an integer.
- Then: $3n + 2 = 3(2k) + 2$
  $= 6k + 2$
  $= 2(3k + 1)$
- Thus **3n + 2 is even.** This is a contradiction with the assumption that **3n + 2 is odd.** Therefore **n is odd**. □

Vacuous proof

We want to show $p \to q$

- Suppose p (the hypothesis) is always false
- Then $p \to q$ is always true.

Reason:

- $F \to q$ is always T, whether q is True or False

Example:

- Let P(n) denotes "if $n > 1$ then $n^2 > n$" is TRUE.
- Show that P(0).

Proof:

- For n=0 the premise is False. Thus P(0) is always true.

Trivial proofs

We want to show $p \rightarrow q$

- Suppose the conclusion q is always true
- Then the implication $p \rightarrow q$ is trivially true.
- **Reason:**
- $p \rightarrow T$ is always T, whether p is True or False

Example:

- Let P(n) is "if a >=b then $a^n >= b^n$"
- Show that P(0)

Proof:

$a^0 >= b^0$ is 1=1 trivially true.

Proof by cases

- We want to show $p1 \vee p2 \vee \ldots \vee pn \rightarrow q$
- Note that this is equivalent to
  - $(p1 \rightarrow q) \wedge (p2 \rightarrow q) \wedge \ldots \wedge (pn \rightarrow q)$
- **Why?**
- $p1 \vee p2 \vee \ldots \vee pn \rightarrow q$ <=> (useful)
- $\neg (p1 \vee p2 \vee \ldots \vee pn) \vee q$ <=> (De Morgan)
- $(\neg p1 \wedge \neg p2 \wedge \ldots \wedge \neg pn) \vee q$ <=> (distributive)
- $(\neg p1 \vee q) \wedge (\neg p2 \vee q) \wedge \ldots \wedge (\neg pn \vee q)$ <=> (useful)
- $(p1 \rightarrow q) \wedge (p2 \rightarrow q) \wedge \ldots \wedge (pn \rightarrow q)$

Proof by cases

We want to show $p1 \vee p2 \vee \ldots \vee pn \rightarrow q$

- Equivalent to $(p1 \rightarrow q) \wedge (p2 \rightarrow q) \wedge \ldots \wedge (pn \rightarrow q)$

Prove individual cases as before. All of them must be true.

Example: Show that $|x||y|=|xy|$.

Proof:

- 4 cases:
- $x >=0, y>=0$
- $x>= 0, y <0$
- $x<0, y>=0$ |
- $x<0, , y <0$ |

Proof by cases

We want to show $p1 \vee p2 \vee \ldots \vee pn \rightarrow q$

- Equivalent to $(p1 \rightarrow q) \wedge (p2 \rightarrow q) \wedge \ldots \wedge (pn \rightarrow q)$

Prove individual cases as before. All of them must be true.

Example: Show that $|x||y|=|xy|$.

Proof:

- 4 cases:
- $x >=0, y>=0$ $xy >0$ and $|xy|=xy=|x||y|$
- $x>= 0, y <0$ $xy < 0$ and $|xy|=-xy =x (-y)=|x||y|$
- $x<0, y>=0$ $xy < 0$ and $|xy|=-xy =(-x) y=|x||y|$
- $x<0, , y <0$ $xy >0$ and $|xy|= (-x)(-y) =|x||y|$
- All cases proved.

Proof of equivalences

We want to prove $p \leftrightarrow q$

- Statements: p if and only if q.
- Note that $p \leftrightarrow q$ is equivalent to $[(p \to q) \wedge (q \to p)]$
- Both implications must hold.

Example:

- Integer is odd if and only if n^2 is odd.

Proof of $(p \to q)$:

- $(p \to q)$ If n is odd then n^2 is odd
- we use a direct proof
- Suppose n is odd. Then n = 2k + 1,where k is an integer.
- n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1
- Therefore, n^2 is odd.

Proof of equivalences

We want to prove $p \leftrightarrow q$

- Note that $p \leftrightarrow q$ is equivalent to $[(p \to q) \wedge (q \to p)]$
- Both implications must hold.

- Integer is odd if and only if n^2 is odd.

Proof of $(q \to p)$:

- $(q \to p)$: if n^2 is odd then n is odd
- we use an indirect proof $(\neg p \to \neg q)$ is a contrapositive
- n is even that is n = 2k,
- then n^2 = 4k^2= 2(2k^2)
- Therefore n^2 is even. Done proving the contrapositive.

Since both $(p \to q)$ and $(q \to p)$ are true the equivalence is true

Proofs with quantifiers

- **Existence proof – sentences expressed with an existential quantifiers**
  - **Constructive**
    - Find an example (through search) that shows the statement holds.
  - **Nonconstructive**
    - Show the statement holds for one example but we do not have the witness example. Typically relies on the proof by contradiction – negate the existentially quantified statement and show that it implies a contradiction.

Proofs with quantifiers

- **Universally quantified statements**
  - **Prove the property holds for all examples**
  - **can be tricky**
  - **proof by cases to divides the proof to the different subgroups may help**
  - **Counterexamples:**
    - use to disprove universal statements
    - Similar to constructive proofs for existentially