CS 441 Discrete Mathematics for CS
Lecture 8

Methods of Proof

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

Course administration

- **Homework 1 and Homework 2:**
- **Due today**

- **Homework 3**
  out today, due next week on Friday

- **Course web page:**
  http://www.cs.pitt.edu/~milos/courses/cs441/

Theorems and proofs

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

    $(p1 \wedge p2 \wedge p3 \wedge \ldots \wedge pn) \rightarrow q$

    Premises (hypotheses) — conclusion

- **Example:**

  Fermat's Little theorem:
  - If p is a prime and a is an integer not divisible by p, then: $a^{p-1} \equiv 1 \bmod p$

Proofs

Proof:

- an argument supporting the validity of the statement
- proof of the theorem:
  - shows that the conclusion follows from premises
  - may use:
    - Premises
    - Axioms
    - Results of other theorems

Formal proofs:

- steps of the proofs follow logically from the set of premises and axioms
- we assumed ***formal proofs*** in propositional logic

Rules of inference

Rules of inference: logically valid inference patterns

Example;

- **Modus Ponens**, or the Law of Detachment
- Rule of inference

$$\begin{array}{l} p \\ \underline{p \rightarrow q} \\ \therefore q \end{array}$$

- Given p is true and the implication $p \rightarrow q$ is true then q is true.

Rules of inference

Rules of inference: logically valid inference patterns

Example;

- **Modus Ponens**, or the Law of Detachment
- Rule of inference

$$\begin{array}{l} p \\ \underline{p \rightarrow q} \\ \therefore q \end{array}$$

- Given p is true and the implication $p \rightarrow q$ is true then q is true.

p	q	$p \rightarrow q$
False	*False*	*True*
False	*True*	*True*
True	*False*	*False*
True	*True*	*True*

Rules of inference

Rules of inference: logically valid inference patterns

Example;

- **Modus Ponens**, or the Law of Detachment
- Rule of inference
$$\begin{array}{l} p \\ \underline{p \rightarrow q} \\ \therefore q \end{array}$$
- Given p is true and the implication $p \rightarrow q$ is true then q is true.

p	q	$p \rightarrow q$
False	*False*	*True*
False	*True*	*True*
True	*False*	*False*
True	*True*	*True*

Rules of inference

Rules of inference: logically valid inference patterns

Example;

- **Modus Ponens**, or the Law of Detachment
- Rule of inference
$$\begin{array}{l} p \\ \underline{p \rightarrow q} \\ \therefore q \end{array}$$
- Given p is true and the implication $p \rightarrow q$ is true then q is true.

p	q	$p \rightarrow q$
False	*False*	*True*
False	*True*	*True*
True	*False*	*False*
True	*True*	*True*

Applying rules of inference

Text:

- It is not sunny this afternoon and it is colder than yesterday.
- We will go swimming only if it is sunny.
- If we do not go swimming then we will take a canoe trip.
- If we take a canoe trip, then we will be home by sunset.

Propositions:

- p = It is sunny this afternoon, q = it is colder than yesterday, r = We will go swimming , s= we will take a canoe trip
- t= We will be home by sunset

Translation:

- **Assumptions:** $\neg p \wedge q$, $r \rightarrow p$, $\neg r \rightarrow s$, $s \rightarrow t$
- **Hypothesis:** t

Proofs using rules of inference

Translations:

- **Assumptions:** $\neg p \wedge q$, $r \rightarrow p$, $\neg r \rightarrow s$, $s \rightarrow t$
- **Hypothesis:** 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

General 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 premise (hypothesis) is true, i.e. suppose n is odd.
- Then $n = 2k + 1$, where k is an integer.

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.

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

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 is this correct?

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:

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.

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

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.**

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 **$(p \wedge \neg q)$**
  - **and subsequently $p \rightarrow q$** must be true
- Proof by contradiction. Show that the assumption **$(p \wedge \neg q)$** **leads either to** q or $\neg p$ which generates a contradiction.

Proof by contradiction

- We want to prove $p \rightarrow q$
- To reject **$p \rightarrow q$** show that **$(p \wedge \neg q)$** can be true
- To reject **$(p \wedge \neg q)$** 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 $p \rightarrow q$
- To reject **$p \rightarrow q$** show that **$(p \wedge \neg q)$** can be true
- To reject **$(p \wedge \neg q)$** 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.
- Then: $3n + 2 = 3(2k) + 2$
  $= 6k + 2$
  $= 2(3k + 1)$
- Thus **3n + 2 is…**

Proof by contradiction

- We want to prove $p \rightarrow q$
- To reject **$p \rightarrow q$** show that **$(p \wedge \neg q)$** can be true
- To reject **$(p \wedge \neg q)$** 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.
- 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 $p \rightarrow q$

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

Reason:

- $F \rightarrow q$ 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?**

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:
- $x >=0, y>=0$ $xy >0$ 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 $[(p \rightarrow q) \wedge (q \rightarrow p)]$
- Both implications must hold.

Example:

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

Proof of $(p \rightarrow q)$:

- **$(p \rightarrow q)$** 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 $[(p \rightarrow q) \wedge (q \rightarrow p)]$
- Both implications must hold.

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

Proof of $(q \rightarrow p)$:

- $(q \rightarrow p)$: if n^2 is odd then n is odd
- we use an indirect proof $(\neg p \rightarrow \neg q)$ 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 $(p \rightarrow q)$ and $(q \rightarrow p)$ are true the equivalence is true

Proofs with quantifiers

- **Existence proof**
  - **Constructive**
    - Find the example that shows the statement holds.
  - **Nonconstructive**
    - Show it holds for one example but we do not have the witness example (typically ends with one example or other example)

- **Counterexamples:**
  - use to disprove a universal statements