Informal proofs. Types of proofs.

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

Course administration

• Homework 2 is due today

• Homework 3:
  • out today and due on September 24, 2009

• Recitations tomorrow
  will cover topics/problems related to Homework 3

• Course web page:
  http://www.cs.pitt.edu/~milos/courses/cs441/
Proofs

• The truth value of some statement about the world is obvious and easy to assign
• The truth of other statements may not be obvious, … … But it may still follow (be derived) from known facts about the world

To show the truth value of such a statement follows from other statements we need to provide a correct supporting argument
- a proof

Theorems and proofs

• Theorem: a statement that can be shown to be true.

Typically the theorem looks like this:

\[(p_1 \land p_2 \land p_3 \land \ldots \land p_n) \rightarrow q\]

Premises (hypotheses) conclusion

• Example:
  Fermat’s Little theorem:
  – If p is a prime and a is an integer not divisible by p, then: \( a^{p-1} \equiv 1 \mod p \)
Theorems and proofs

- **Theorem**: a statement that can be shown to be true.
  - Typically the theorem looks like this:
    \[(p_1 \land p_2 \land p_3 \land \ldots \land p_n) \rightarrow q\]

- **Example**: Fermat’s Little theorem:
  - If \( p \) is a prime and \( a \) is an integer not divisible by \( p \),
  - then: \( a^{p-1} \equiv 1 \mod p \)

Formal proofs

**Proof:**
- Provides 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
**Formal proofs**

- **Formal proofs:**
  - show that steps of the proofs follow logically from the set of hypotheses and axioms

In the class we assume formal proofs in the propositional logic

**Rules of inference**

**Rules of inference:** logically valid inference patterns

**Example:**

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

\[ p \rightarrow q \]

\[ \therefore q \]

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

<table>
<thead>
<tr>
<th>( p )</th>
<th>( q )</th>
<th>( p \rightarrow q )</th>
</tr>
</thead>
<tbody>
<tr>
<td>False</td>
<td>False</td>
<td>True</td>
</tr>
<tr>
<td>False</td>
<td>True</td>
<td>True</td>
</tr>
<tr>
<td>True</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>True</td>
<td>True</td>
<td>True</td>
</tr>
</tbody>
</table>
Proofs using rules of inference

Translations:
- Assumptions: \( \neg p \land q, \; r \rightarrow p, \; \neg r \rightarrow s, \; s \rightarrow t \)
- Hypothesis: \( t \)

Proof:
- 1. \( \neg p \land q \) 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 step in the proof may consist of multiple derivations, portions of the proof may be skipped or assumed correct,
- Axioms may not be explicitly stated.
- 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 \((p \land \neg q)\) contradicts the assumptions

• **Proof by cases**

• **Proofs of equivalence**
  - \( p \leftrightarrow q \) is replaced with \( (p \rightarrow q) \land (q \rightarrow p) \)

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.
  
  \[
  n^2 = (2k + 1)^2 \\
  = 4k^2 + 4k + 1 \\
  = 2(2k^2 + 2k) + 1
  \]

• Therefore, $n^2$ is odd. ❑
Direct proof

• Direct proof may not be the best option. It may become hard to prove the conclusion follows from the premises.

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

Proof:
• Assume that $3n + 2$ is odd,
  – thus $3n + 2 = 2k + 1$ for some $k$.
• Then $n = (2k – 1)/3$
• ?
Indirect proof

- To show \( p \rightarrow q \) prove its contrapositive \( \neg q \rightarrow \neg p \)
- Why is this correct?

\[ p \rightarrow q \text{ and } \neg q \rightarrow \neg p \text{ are equivalent} \]

Assume \( \neg q \) is true, show that \( \neg p \) is true.

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

**Proof:**

**Contrapositive:** If \( n \) is even then \( 3n + 2 \) is even.

**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:
- Contrapositive: If $n$ is even then $3n + 2$ is even.
- Assume $n$ is even, that is $n = 2k$, where $k$ is an integer.

\[3n + 2 = 3(2k) + 2\]
\[= 6k + 2\]
\[= 2(3k+1)\]
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:
• Contrapositive: If $n$ is even then $3n + 2$ is even.
• 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 $\neg "n \text{ is odd}" \Rightarrow \neg "3n + 2 \text{ is odd}"$. This is equivalent to $"3n + 2 \text{ is odd}" \Rightarrow "n \text{ is odd}"$. □
Proof by contradiction

- We want to prove $p \rightarrow q$
- The only way to reject (or disprove) $p \rightarrow q$ is to show that $(p \land \neg q)$ can be true

- However, if we manage to prove that either $q$ or $\neg p$ is True then we contradict $(p \land \neg q)$
  - and subsequently $p \rightarrow q$ must be true

- Proof by contradiction. Show that the assumption $(p \land \neg q)$ leads either to $q$ or $\neg p$ which generates a contradiction.

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 $k$ is an integer.
Proof by contradiction

• We want to prove \( p \rightarrow q \)
• To reject \( p \rightarrow q \) show that \( (p \land \neg q) \) can be true
• To reject \( (p \land \neg q) \) 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 \( k \) is 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. \( \square \)
**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 $a \geq b$ then $a^n \geq b^n$”
- Show that $P(0)$

Proof:
- $a^0 \geq b^0$ is $1=1$ trivially true.
Proof by cases

• We want to show $p_1 \lor p_2 \lor \ldots \lor p_n \rightarrow q$

• Note that this is equivalent to

$(p_1 \rightarrow q) \land (p_2 \rightarrow q) \land \ldots \land (p_n \rightarrow q)$

• Why?

Proof by cases

• We want to show $p_1 \lor p_2 \lor \ldots \lor p_n \rightarrow q$

• Note that this is equivalent to

$(p_1 \rightarrow q) \land (p_2 \rightarrow q) \land \ldots \land (p_n \rightarrow q)$

• Why?

• $p_1 \lor p_2 \lor \ldots \lor p_n \rightarrow q \iff$ (useful)

• $\neg (p_1 \lor p_2 \lor \ldots \lor p_n) \lor q \iff \quad$ (De Morgan)

• $(\neg p_1 \land \neg p_2 \land \ldots \land \neg p_n) \lor q \iff$ (distributive)

• $(\neg p_1 \lor q) \land (\neg p_2 \lor q) \land \ldots \land (\neg p_n \lor q) \iff \quad$ (useful)

• $(p_1 \rightarrow q) \land (p_2 \rightarrow q) \land \ldots \land (p_n \rightarrow q)$
**Proof by cases**

We want to show \( p_1 \lor p_2 \lor \ldots \lor p_n \to q \)

- Equivalent to \( (p_1 \to q) \land (p_2 \to q) \land \ldots \land (p_n \to q) \)

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

**Example:** Show that \(|x||y|=|xy|\).

**Proof:**

- 4 cases:
  - \( x \geq 0, y \geq 0 \) \( xy > 0 \) and \(|xy|=xy|=|x||y|\)
  - \( x \geq 0, y < 0 \) \( xy < 0 \) and \(|xy|=-xy=x (-y)=|x||y|\)
  - \( x<0, y \geq 0 \) \( xy < 0 \) 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 \( (p \to q) \land (q \to p) \)
- 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 $[(p \rightarrow q) \land (q \rightarrow p)]$
- 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 an 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:**
  - Are used to disprove universal statements