Proofs

Slides by Christopher M. Bourke
Instructor: Berthe Y. Choueiry

Fall 2007

Computer Science & Engineering 235
Introduction to Discrete Mathematics
Sections 1.5, 1.6, and 1.7 of Rosen
cse235@cse.unl.edu

Introduction I

> *"A proof is a proof. What kind of a proof? It's a proof. A proof is a proof. And when you have a good proof, it's because it's proven." –Jean Chrétien*

> *"Mathematical proofs, like diamonds, are hard and clear, and will be touched with nothing but strict reasoning." –John Locke*

Mathematical proofs are, in a sense, the only truly absolute knowledge we can have. They provide us with a guarantee as well as an explanation (and hopefully some deep insight).

Introduction II

Mathematical proofs are necessary in computer science for several reasons.

- An algorithm must always be proven *correct*.
- You may also want to show that its more *efficient* than other method. This requires a proof.
- Proving certain properties of data structures may lead to new, more efficient or simpler algorithms.
- Arguments may entail assumptions. It may be useful and/or necessary to make sure these assumptions are actually valid.

Introduction
Terminology

- A *theorem* is a statement that can be shown to be true (via a proof).
- A *proof* is a sequence of statements that form an argument.
- *Axioms* or *postulates* are statements taken to be self-evident, or assumed to be true.
- *Lemmas* and *corollaries* are also (certain types of) theorems. A *proposition* (as opposed to a proposition in logic) is usually used to denote a fact for which a proof has been omitted.
- A *conjecture* is a statement whose truth value is unknown.
- The *rules of inferences* are the means used to draw conclusions from other assertions. These form the basis of various methods of proof.

Theorems
Example

Consider, for example, Fermat's Little Theorem.

Theorem (Fermat's Little Theorem)

If p is a prime which does not divide the integer a, then $a^{p-1} = 1 (\mathrm{mod}\ p)$.

What is the assumption? Conclusion?

Proofs: A General How To I

An argument is *valid* if whenever all the hypotheses are true, the conclusion also holds.

From a sequence of assumptions, $p_1, p_2, \ldots, p_n$, you draw the conclusion p. That is;

$$(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \rightarrow q$$

Proofs: A General How To II

Usually, a proof involves proving a theorem via intermediate steps.

Example

Consider the theorem "If $x > 0$ and $y > 0$, then $x + y > 0$." What are the assumptions? Conclusion? What steps would you take?

Each step of a proof must be justified.

Rules of Inference

Recall the handout on the course web page `http://www.cse.unl.edu/~cse235/files/LogicalEquivalences.pdf` of logical equivalences.

Table 1 (page 66) contains a Cheat Sheet for Inference rules.

Rules of Inference

Modus Ponens

Intuitively, *modus ponens* (or *law of detachment*) can be described as the inference, "p implies q; p is true; therefore q holds".

In logic terms, modus ponens is the tautology

$$(p \wedge (p \to q)) \to q$$

Notation note: "therefore" is sometimes denoted $\therefore$, so we have, p and $p \to q$, $\therefore q$.

Rules of Inference

Addition

Addition involves the tautology

$$p \to (p \vee q)$$

Intuitively, if we know p to be true, we can conclude that either p or q are true (or both).

In other words, $p \therefore p \vee q$.

Example

I read the newspaper today, therefore I read the newspaper or I ate custard.[1]

[1] Note that these are not mutually exclusive.

Rules of Inference

Simplification

Simplification is based on the tautology

$$(p \wedge q) \to p$$

so that we have $p \wedge q$, $\therefore p$.

Example

Prove that if $0 < x < 10$, then $x \geq 0$.

- $0 < x < 10 \equiv (x > 0) \wedge (x < 10)$
- $(x > 0) \wedge (x < 10)$ implies that $x > 0$ by simplification.
- $x > 0$ implies $(x > 0) \vee (x = 0)$ by addition.
- $(x > 0) \vee (x = 0) \equiv (x \geq 0)$.

Rules of Inference

Conjunction

The *conjunction* is almost trivially intuitive. It is based on the tautology

$$((p) \wedge (q)) \to (p \wedge q)$$

Note the subtle difference though. On the left hand side, we independently know p and q to be true. Therefore, we conclude that the right hand side, a *logical conjunction* is true.

Rules of Inference
Modus Tollens

Similar to modus ponens, *modus tollens* is based on the tautology

$$\big(\neg q \wedge (p \rightarrow q)\big) \rightarrow \neg p$$

In other words, if we know that q is not true and that p implies q then we can conclude that p does not hold either.

Example

If you are a UNL student you are a cornhusker. Don Knuth was not a cornhusker. Therefore, we can conclude that Knuth was not a UNL student.

Rules of Inference
Contrapositive

The tautology

$$(p \rightarrow q) \rightarrow (\neg q \rightarrow \neg p)$$

is called the *contrapositive*.

If you are having trouble proving that p implies q in a *direct* manner, you can try to prove the contrapositive instead!

Rules of Inference
Hypothetical Syllogism

Based on the tautology

$$\big((p \rightarrow q) \wedge (q \rightarrow r)\big) \rightarrow (p \rightarrow r)$$

Essentially, this shows that rules of inference are, in a sense, *transitive*.

Example

If you don't get a job you won't make any money. If you don't make any money, you will starve. Therefore, if you don't get a job, you will starve.

Rules of Inference
Disjunctive Syllogism

A *disjunctive syllogism* is formed on the basis of the tautology

$$\big((p \vee q) \wedge \neg p\big) \rightarrow q$$

Reading this in English, we see that if either p or q hold and we know that p does *not* hold; we can conclude that q must hold.

Example

The sky is either clear or cloudy. Well, it isn't cloudy, therefore the sky is clear.

Rules of Inference
Resolution

For *resolution*, we have the following tautology.

$$\big((p \vee q) \wedge (\neg p \vee r)\big) \rightarrow (q \vee r)$$

Essentially, if we have two true disjunctions that have mutually exclusive propositions, then we can conclude that the disjunction of the two non-mutually exclusive propositions is true.

Example I

The best way to become accustomed to proofs is to see many examples.

To begin with, we give a *direct* proof of the following theorem.

Theorem

The sum of two odd integers is even.

Example I

Proof

Let n, m be odd integers. Every odd integer x can be written as $x = 2k + 1$ for some other integer k. Therefore, let $n = 2k_1 + 1$ and $m = 2k_2 + 1$. Then consider

$$\begin{aligned} n + m &= (2k_1 + 1) + (2k_2 + 1) & \\ &= 2k_1 + 2k_2 + 1 + 1 & \text{Associativity/Commutativity} \\ &= 2k_1 + 2k_2 + 2 & \text{Algebra} \\ &= 2(k_1 + k_2 + 1) & \text{Factoring} \end{aligned}$$

By definition, $2(k_1 + k_2 + 1)$ is an even number, therefore, $n + m$ is even.

Example II

Assume that the statements

- $(p \rightarrow q)$
- $(r \rightarrow s)$
- $r \vee p$

to be true. Assume that q is false.

Show that s must be true.

Example II

Proof

Proof.

- Since $p \rightarrow q$ and $\neg q$ are true, $\neg p$ is true by modus tollens (i.e. p must be false).
- Since $r \vee p$ and $\neg p$ are true, r is true by disjunctive syllogism.
- Since $r \rightarrow s$ is true and r is true, s is true by modus ponens.
- Q.E.D.[2]

□

[2] Latin, "quod erat demonstrandum" meaning "that which was to be demonstrated"

If And Only If

If you are asked to show an equivalence (i.e. $p \iff q$, "if and only if"), you *must* show an implication in *both* directions.

That is, you can show (independently or via the same technique) that $p \Rightarrow q$ and $q \Rightarrow p$.

Example

Show that x is odd if and only if $x^2 + 2x + 1$ is even.

If And Only If

Example Continued

Proof.

$$\begin{aligned} \text{x is odd} &\iff x = 2n + 1, n \in \mathbb{Z} & \text{by definition} \\ &\iff x + 1 = 2n + 2 & \text{algebra} \\ &\iff x + 1 = 2(n + 1) & \text{factoring} \\ &\iff x + 1 \text{ is even} & \text{by definition} \\ &\iff (x + 1)^2 \text{ is even} & \text{since } x \text{ is even iff } x^2 \text{ is even} \\ &\iff x^2 + 2x + 1 \text{ is even} & \text{algebra} \end{aligned}$$

□

Fallacies

Even a bad example is worth something—it teaches us what *not* to do.

A theorem may be true, but a bad proof doesn't testify to it.

There are three common mistakes (actually probably many more). These are known as *fallacies*

- Fallacy of affirming the conclusion.
  $$(q \wedge (p \rightarrow q)) \rightarrow p$$
  is *not* a tautology.
- Fallacy of denying the hypothesis.
  $$(\neg p \wedge (p \rightarrow q)) \rightarrow \neg q$$
- Circular reasoning. Here, you use the conclusion as an assumption, avoiding an actual proof.

Fallacies

Sometimes bad proofs arise from illegal operations rather than poor logic. Consider this classically bad proof that $2 = 1$:

Let $a = b$

$$\begin{array}{lcll} a^2 & = & ab & \text{Multiply both sides by } a \\ a^2 + a^2 - 2ab & = & ab + a^2 - 2ab & \text{Add } (a^2 - 2ab) \text{ to both sides} \\ 2(a^2 - ab) & = & a^2 - ab & \text{Factor, collect terms} \\ 2 & = & 1 & \text{Divide both sides by } (a^2 - ab) \end{array}$$

So what's wrong with the proof?

Proofs With Quantifiers

Rules of inference can be extended in a straightforward manner to quantified statements.

- **Universal Instantiation** – Given the premise that $\forall x P(x)$, and $c \in X$ (where X is the universe of discourse) we conclude that $P(c)$ holds.
- **Universal Generalization** – Here we select an arbitrary element in the universe of discourse $c \in X$ and show that $P(c)$ holds. We can therefore conclude that $\forall x P(x)$ holds.
- **Existential Instantiation** – Given the premise that $\exists x P(x)$ holds, we simply give it a name, c and conclude that $P(c)$ holds.
- **Existential Generalization** – Conversely, when we establish that $P(c)$ is true for a specific $c \in X$, then we can conclude that $\exists x P(x)$.

Proofs With Quantifiers

Example

Example

Show that the premise "A car in this garage has an engine problem," and "Every car in this garage has been sold" imply the conclusion "A car which has been sold has an engine problem."

- Let $G(x)$ be "x is in this garage."
- Let $E(x)$ be "x has an engine problem."
- Let $S(x)$ be "x has been sold."
- The premises are as follows.
- $\exists x(G(x) \wedge E(x))$
- $\forall x(G(x) \rightarrow S(x))$
- The conclusion we want to show is $\exists x(S(x) \wedge E(x))$

Proofs With Quantifiers

Example Continued

proof

(1)	$\exists x(G(x) \wedge E(x))$	Premise
(2)	$G(c) \wedge E(c)$	Existential Instantiation of (1)
(3)	$G(c)$	Simplification from (2)
(4)	$\forall x(G(x) \rightarrow S(x))$	Second Premise
(5)	$(G(c) \rightarrow S(c)$	Universal Instantiation from (4)
(6)	$S(c)$	Modus ponens from (3) and (5)
(7)	$E(c)$	Simplification from (2)
(8)	$S(c) \wedge E(c)$	Conjunction from (6), (7)
(9)	$\exists x(S(x) \wedge E(x))$	Existential Generalization from (8) $\square$

Types of Proofs

- Trivial Proofs
- Vacuous Proofs
- Direct Proofs
- Proof by Contrapositive (indirect proof)
- Proof by Contradiction (indirect proof, a.k.a. refutation)
- Proof by Cases (sometimes using WLOG)
- Proofs of equivalence
- Existence Proofs (Constructive & Nonconstructive)
- Uniqueness Proofs

Trivial Proofs I

(*Not* trivial as in "easy")

Trivial proofs: conclusion holds without using the hypothesis.

A trivial proof can be given when the conclusion is shown to be (always) true. That is, if q is true then $p \rightarrow q$ is true.

Example

Prove that if $x > 0$ then $(x + 1)^2 - 2x > x^2$.

Trivial Proofs II

Proof.

Its easy to see that

$$\begin{aligned}(x+1)^2 - 2x &= (x^2+2x+1) - 2x \\ &= x^2+1 \\ &\geq x^2\end{aligned}$$

and so the conclusion holds *without using the hypothesis*. □

Vacuous Proofs

If a premise p is false, then the implication $p \to q$ is (trivially) true.

A *vacuous proof* is a proof that relies on the fact that no element in the universe of discourse satisfies the premise (thus the statement exists in a *vacuum* in the UoD).

Example

If x is a prime number divisible by 16, then $x^2 < 0$.

No prime number is divisible by 16, thus this statement is *true* (counter-intuitive as it may be)

Direct Proof

Most of the proofs we have seen so far are *direct proofs*.

In a direct proof, you assume the hypothesis p and give a direct series of implications using the rules of inference as well as other results (proved independently) to show the conclusion q holds.

Proof by Contrapositive

(Indirect Proofs)

Recall that $p \to q$ is logically equivalent to $\neg q \to \neg p$. Thus, a proof by contrapositive can be given.

Here, you assume that the conclusion is false and then give a series of implications (etc.) to show that such an assumption implies that the premise is false.

Example

Prove that if $x^3 < 0$ then $x < 0$.

Proof by Contrapositive

Example

The contrapositive is "if $x \geq 0$, then $x^3 \geq 0$."

Proof.

If $x = 0$, then trivially, $x^3 = 0 \geq 0$.

$$\begin{aligned} x > 0 &\Rightarrow x^2 > 0 \\ &\Rightarrow x^3 \geq 0 \end{aligned}$$

□

Proof by Contradiction

To prove a statement p is true, you may assume that it is *false* and then proceed to show that such an assumption leads to a contradiction with a known result.

In terms of logic, you show that for a known result r,

$$\neg p \to (r \wedge \neg r)$$

is true, which leads to a contradiction since $(r \wedge \neg r)$ cannot hold.

Example

$\sqrt{2}$ is an irrational number.

Proof by Contradiction

Example

Proof.

Let p be the proposition "$\sqrt{2}$ is irrational." We start by assuming $\neg p$, and show that it will lead to a contradiction.

$\sqrt{2}$ is rational $\Rightarrow$ $\sqrt{2} = \frac{a}{b}$, $a, b \in \mathbb{R}$ and have no common factor (proposition r).

Squarring that equation: $2 = \frac{a^2}{b^2}$.

Thus $2b^2 = a^2$, which implies that a^2 is even.

a^2 is even $\Rightarrow$ a is even $\Rightarrow$ $a = 2c$.

Thus, $2b^2 = 4c^2 \Rightarrow b^2$ is even $\Rightarrow$ b is even.

Thus, a and b have a common factor 2 (i.e., proposistion $\neg r$).

$\neg p \rightarrow r \wedge \neg r$, which is a contridiction.

Proof by Cases

Sometimes it is easier to prove a theorem by breaking it down into *cases* and proving each one separately.

Example

Let $n \in \mathbb{Z}$. Prove that

$$9n^2 + 3n - 2$$

is even.

Proof by Cases

Example

Proof.

Observe that $9n^2 + 3n - 2 = (3n + 2)(3n - 1)$ is the product of two integers. Consider the following cases.

Case 1: $3n + 2$ is even. Then trivially we can conclude that $9n^2 + 3n - 2$ is even since one of its two factors is even.

Case 2: $3n + 2$ is odd. Note that the difference between $(3n + 2)$ and $(3n - 1)$ is 3, therefore, if $(3n + 2)$ is odd, it must be the case that $(3n - 1)$ is even. Just as before, we conclude that $9n^2 + 3n - 2$ is even since one of its two factors is even. $\square$

Existence & Uniqueness Proofs I

A *constructive existence proof* asserts a theorem by providing a specific, concrete example of a statement. Such a proof *only* proves a statement of the form $\exists x P(x)$ for some predicate P. It *does not* prove the statement for all such x.

A *nonconstructive existence proof* also shows a statement of the form $\exists x P(x)$, but it does not necessarily need to give a specific example x. Such a proof usually proceeds by contradiction—assume that $\neg \exists x P(x) \equiv \forall x \neg P(x)$ holds and then get a contradiction.

Existence & Uniqueness Proofs II

A *uniqueness proof* is used to show that a certain element (specific or not) has a certain property. Such a proof usually has two parts, a proof of existence ($\exists x P(x)$) and a proof of uniqueness (if $x \neq y$, then $\neg P(y)$). Together, we have the following

$$\exists x \big(P(x) \wedge \forall y (y \neq x \rightarrow \neg P(y)) \big)$$

Counter Examples

Sometimes you are asked to *disprove* a statement. In such a situation, you are actually trying to *prove* the negation.

With statements of the form $\forall x P(x)$, it suffices to give a *counter example* since the existence of an element x such that $\neg P(x)$ is true proves that $\exists x \neg P(x)$ which is the negation of $\forall x P(x)$.

Counter Examples

Example

Example

Disprove: $n^2 + n + 1$ is a prime number for all $n \geq 1$

A simple counter example is $n = 4$. Then $n^2 + n + 1 = 4^2 + 4 + 1 = 21 = 3 \cdot 7$ which is clearly not prime.

Counter Examples

A word of caution

No matter how many you give, you can never *prove* a theorem by giving examples (unless the universe of discourse is finite—why?).

Counter examples can only be used to disprove universally quantified statements.

Do not give a proof by simply giving an example.

Proof Strategies I

Example: Forward chaining, backward chaining

If there were a single strategy that always worked for proofs, mathematics would be easy.

The best advice I can give is:

- Beware of fallacies and circular argument (i.e., begging the question)
- Don't take things for granted, try proving assertions *first* before you take them as fact.
- Don't peek at proofs. Try proving something for yourself before looking at the proof.
- The best way to improve your proof skills is practice.

Questions?