Proofs

Sections 1.5, 1.6 and 1.7 of Rosen

Fall 2010

CSCE 235 Introduction to Discrete Structures

Course web-page: cse.unl.edu/~cse235

Questions: cse235@cse.unl.edu

Outline

- Motivation
- Terminology
- Rules of inference:
  - Modus ponens, addition, simplification, conjunction, modus tollens, contrapositive, hypothetical syllogism, disjunctive syllogism, resolution,
  - Examples
- Fallacies
- Proofs with quantifiers
- Types of proofs:
  - Trivial, vacuous, direct, by contrapositive (indirect), by contradiction (indirect), by cases, existence and uniqueness proofs; counter examples
- Proof strategies:
  - Forward chaining; Backward chaining; Alerts

Motivation (1)

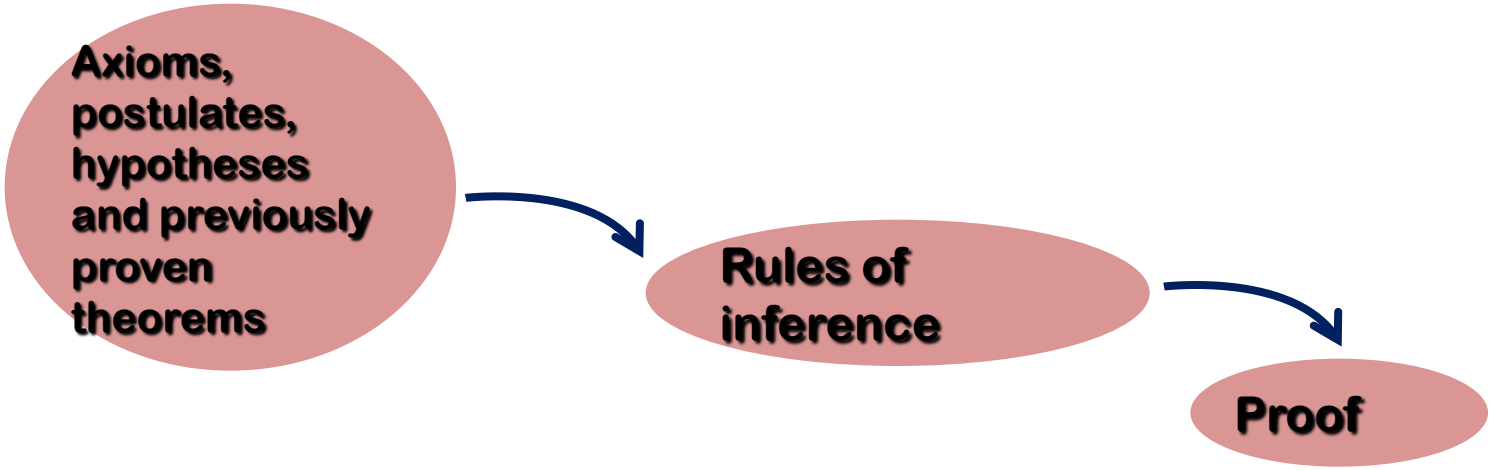
- "Mathematical proofs, like diamonds, are hard and clear, and will be touched with nothing but strict reasoning." *-John Locke*
- Mathematical proofs are, in a sense, the only true knowledge we have
- They provide us with a guarantee as well as an explanation (and hopefully some insight)

Motivation (2)

- Mathematical proofs are necessary in CS
  - You must always (try to) prove that your algorithm
    - terminates
    - is sound, complete, optimal
    - finds optimal solution
  - You may also want to show that it is more efficient than another method
  - Proving certain properties of data structures may lead to new, more efficient or simpler algorithms
  - Arguments may entail assumptions. You may want to prove that the assumptions are valid

Proofs and theorems

A theorem is a statement that can be shown to be true. A proof is the means of doing so.



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
- A lemma (plural lemmas or lemmata) is a theorem useful within the proof of a theorem
- A corollary is a theorem that can be established from theorem that has just been proven
- A proposition is usually a 'less' important theorem
- A conjecture is a statement whose truth value is unknown
- The rules of inference are the means used to draw conclusions from other assertions, and to derive an argument or a proof

Theorems: Example

- Theorem
  - Let a, b, and c be integers. Then
    - If $a|b$ and $a|c$ then $a|(b+c)$
    - If $a|b$ then $a|bc$ for all integers c
    - If $a|b$ and $b|c$, then $a|c$
- Corrolary:
  - If a, b, and c are integers such that $a|b$ and $a|c$, then $a|mb+nc$ whenever m and n are integers
- What is the assumption? What is the conclusion?

Proofs: A General How to (1)

- An argument is valid
  - If, whenever all the hypotheses are true,
  - Then, the conclusion also holds
- From a sequence of assumptions, p_1, p_2, …, p_n, you draw the conclusion p. That is:

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

Proofs: A General How to (2)

- 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?
  - What is the conclusion?
  - What steps should we take?
  - Each intermediate step in the proof must be justified.

Outline

- Motivation
- Terminology
- **Rules of inference**
  - **Modus ponens, addition, simplification, conjunction, modus tollens, contrapositive, hypothetical syllogism, disjunctive syllogism, resolution,**
  - **Examples**
- Fallacies
- Proofs with quantifiers
- Types of proofs
- Proof strategies

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 terminology, modus ponens is the <u>tautology:</u>

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

- Note: 'therefore' is sometimes denoted $\therefore$, so we have:

$$p \rightarrow q \equiv p \therefore q$$

Rules of Inference: Addition

- Addition involves the tautology

$$p \rightarrow (p \vee q)$$

- Intuitively,
  - if we know that p is 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
  - Note that these are <u>not</u> mutually exclusive

Rules of Inference: Simplification

- Simplification is based on the tautology

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

- So we have: $(p \wedge q) \therefore p$
- Example: Prove that if $0 < x < 10$, then $x \geq 0$

1. $0 < x < 10 \equiv (0 < x) \wedge (x < 10)$
2. $(x > 0) \wedge (x < 10) \rightarrow (x > 0)$ by simplification
3. $(x > 0) \rightarrow (x > 0) \vee (x = 0)$ by addition
4. $(x > 0) \vee (x = 0) \equiv (x \geq 0)$ Q.E.D.

Rules of inference: Conjunction

- The conjunction is almost trivially intuitive. It is based on the following tautology:

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

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

Rules of Inference: Modus Tollens

- Similar to the modus ponens, modus tollens is based on the following tautology

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

- 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 UNL student, then you are cornhusker
  - Don Knuth is not a cornhusker
  - Therefore we can conclude that Don Knuth is not a UNL student.

Rules of Inference: Contrapositive

- The contrapositive is the following tautology

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

- Usefulness
  - If you are having trouble proving the p implies q in a direct manner
  - You can try to prove the contrapositive instead!

Rules of Inference: Hypothetical Syllogism

- Hypothetical syllogism is based on the following tautology

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

- Essentially, this shows that the rules of inference are, in a sense, transitive
- Example:
  - If you don't get a job, you won't have money
  - If you don't have money, you will starve.
  - Therefore, if you don't get a job, you'll starve

Rules of Inference: Disjunctive Syllogism

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

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

- Reading this in English, we see that
  - If either *p* or *q* hold and we know that p does not hold
  - Then we can conclude that *q* must hold
- Example
  - The sky is either blue or grey
  - Well it isn't blue
  - Therefore, the sky is grey

Rules of Inference: Resolution

- For resolution, we have the following tautology

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

- 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

Proofs: Example 1 (1)

- 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

Proofs: Example 1 (2)

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

$$n+m = (2k_1+1)+(2k_2+1)$$

$$= 2k_1+ 2k_2+1+1 \qquad \textit{Associativity/Commutativity}$$

$$= 2k_1+ 2k_2+2 \qquad \textit{Algebra}$$

$$= 2(k_1+ k_2+1) \qquad \textit{Factoring}$$

- By definition $2(k_1+k_2+1)$ is even, therefore n+m is even *QED*

Proofs: Example 2 (1)

- Assume that the statements below hold:
  - $(p \rightarrow q)$
  - $(r \rightarrow s)$
  - $(r \vee p)$
- Assume that q is false
- Show that s must be true

Proofs: Example 2 (2)

1. $(p \rightarrow q)$
2. $(r \rightarrow s)$
3. $(r \vee p)$
4. $\neg q$
5. $(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$ by modus tollens on 1 + 4
6. $(r \vee p) \wedge \neg p) \rightarrow r$ by disjunctive syllogism 3 + 6
7. $(r \wedge (r \rightarrow s)) \rightarrow s$ by modus ponens 2 + 6

QED□

QED= Latin word for "quod erat demonstrandum" meaning "that which was to be demonstrated."

$\hfill\Box$

If and Only If

- If you are asked to show an equivalence

  $p \leftrightarrow q$ "if an 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 iff x^2+2x+1 is even

Example (iff)

x is odd $\leftrightarrow x=2k+1, k \in \mathbb{Z}$	*by definition*
$\leftrightarrow x+1 = 2k+2$	*algebra*
$\leftrightarrow x+1 = 2(k+1)$	*factoring*
$\leftrightarrow x+1$ is even	*by definition*
$\leftrightarrow (x+1)^2$ is even	*Since x is even iff x^2 is even*
$\leftrightarrow x^2+2x+1$ is even	*algebra*
	QED

Outline

- Motivation
- Terminology
- Rules of inference
- **Fallacies**
- Proofs with quantifiers
- Types of proofs
- Proof strategies

Fallacies (1)

- Even a bad example is worth something: it teaches us what not to do
- There are three common mistakes (at least..).
- These are known as fallacies
  1. Fallacy of affirming the conclusion

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

  2. Fallacy of denying the hypothesis

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

  3. Circular reasoning. Here you use the conclusion as an assumption, avoiding an actual proof

Little Reminder

- Affirming the antecedent: Modus ponens

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

- Denying the consequent: Modus Tollens

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

- Affirming the conclusion: Fallacy

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

- Denying the hypothesis: Fallacy

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

Fallacies (2)

- Sometimes, bad proofs arise from illegal operations rather than poor logic.
- Consider the bad proof 2=1
- Let: $a = b$

a^2	$= ab$	*Multiply both sides by a*
$a^2 + a^2 - 2ab$	$= ab + a^2 - 2ab$	*Add $a^2 - 2ab$ to both sides*
$2(a^2 - ab)$	$= (a^2 - ab)$	*Factor, collect terms*
2	$= 1$	*Divide both sides by $(a^2 - ab)$*

So, what is wrong with the proof?

Outline

- Motivation
- Terminology
- Rules of inference
- Fallacies
- **Proofs with quantifiers**
- Types of proofs
- Proof strategies

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 $c \in$ UoD (where UoDis the universe of discourse), we conclude that P(c) holds
- **Universal Generalization**: Here, we select an arbitrary element in the universe of discourse $c \in$ UoD 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, we establish that P(c) holds for a specific $c \in$ UoD, then we can conclude that $\exists x P(x)$

Proofs with Quantifiers: Example (1)

- Show that "A car in the garage has an engine problem" and "Every car in the garage has been sold" imply the conclusion "A car has been sold has an engine problem"
- Let
  - G(x): "x is in the garage"
  - E(x): "x has an engine problem"
  - S(x): "x has been sold"
- Let UoD be the set of all cars
- 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 (2)

1.	$\exists x\,(G(x) \wedge E(x))$	*1st premise*
2.	$(G(c) \wedge E(c))$	*Existential instantiation of (1)*
3.	$G(c)$	*Simplification of (2)*
4.	$\forall x\,(G(x) \rightarrow S(x))$	*2nd premise*
5.	$G(c) \rightarrow S(c)$	*Universal instantiation of (4)*
6.	$S(c)$	*Modus ponens on (3) and (5)*
7.	$E(c)$	*Simplification from (2)*
8.	$S(c) \wedge E(c)$	*Conjunction of (6) and (7)*
9.	$\exists x\,(S(x) \wedge E(x))$	*Existential generalization of (8)*

QED

Outline

- Motivation
- Terminology
- Rules of inference:
- Fallacies
- Proofs with quantifiers
- **Types of proofs:**
  - **Trivial, vacuous, direct, by contrapositive (indirect), by contradiction (indirect), by cases, existence and uniqueness proofs; counter examples**
- **Proof strategies:**
  - **Forward chaining; Backward chaining; Alerts**

Types of Proofs

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

Trivial Proofs (1)

- Conclusion holds without using the premise
- 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
- Examples
  - 'If CSE235 is easy implies that the Earth is round'
  - Prove 'If $x>0$ then $(x+1)^2 - 2x \geq x^2$'

Trivial Proofs (2)

- Proof. It is easy to see:

  $(x+1)^2 - 2x$

  $= (x^2 + 2x + 1) - 2x$

  $= x^2 + 1$

  $\geq x^2$

- Note that the conclusion holds without using the hypothesis.

Vacuous Proofs

- If the premise p is false
- Then the implication $p \rightarrow q$ is always 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 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 Proofs

- 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 (sequence) of implications
  - Using the rules of inference
  - As well as other results (proved independently)
  - To show that the conclusion q holds.

Proof by Contrapositive (indirect proof)

- Recall that $(p \rightarrow q) \equiv (\neg q \rightarrow \neg p)$
- This is the basis for the proof by contraposition
  - You assume that the conclusion is false, then
  - Give a series of implications 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:
  1. If $x=0 \rightarrow x^3=0 \geq 0$
  2. If $x>0 \rightarrow x^2>0 \rightarrow x^3>0$

QED

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 a contradiction with a known result
- In terms of logic, you show that
  - for a known result r,
  - $(\neg p \rightarrow (r \wedge \neg r))$ is true
  - Which yields a contradiction $c = (r \wedge \neg r)$ cannot hold
- Example: $\sqrt{2}$ is an irrational number

Proof by Contradiction: Example

- Let p be the proposition '$\sqrt{2}$ is an irrational number'
- Assume $\neg p$ holds, and show that it yields a contradiction
- $\sqrt{2}$ is rational

$\rightarrow \sqrt{2} = a/b$, $a, b \in \mathbb{R}$ and a, b have no common factor (proposition r)

Definition of rational numbers

$\rightarrow 2 = a^2/b^2$ *Squarring the equation*

$\rightarrow (2b^2 = a^2) \rightarrow (a^2$ is even$) \rightarrow (a = 2c)$ *Algebra*

$\rightarrow (2b^2 = 4c^2) \rightarrow (b^2 = 2c^2) \rightarrow (b^2$ is even$) \rightarrow (b$ is even$)$ *Algebra*

$\rightarrow$ (a, b are even) $\rightarrow$ (a, b have a common factor 2) $\rightarrow \neg r$

$\rightarrow (\neg p \rightarrow (r \wedge \neg r))$, which is a contradiction

So, ($\neg p$ is false) $\rightarrow$ (p is true), which means $\sqrt{2}$ is irrational

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

- Observe that $9n^2+3n-2=(3n+2)(3n-1)$
- n is an integer $\rightarrow$(3n+2)(3n-1) is the product of two integers
- **Case 1**: Assume 3n+2 is even

  $\rightarrow$ $9n^2+3n-2$ is trivially even because it is the product of two integers, one of which is even
- **Case 2**: Assume 3n+2 is odd

  $\rightarrow$ 3n+2-3 is even $\rightarrow$ 3n-1 is even $\rightarrow$ $9n^2+3n-2$ is even because one of its factors is even □

Types of Proofs

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

Proofs By Equivalence (Iff)

- If you are asked to show an equivalence

  $p \leftrightarrow q$ "if an 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 iff x^2+2x+1 is even

Example (iff)

x is odd $\leftrightarrow x=2k+1, k \in \mathbb{Z}$ *by definition*

$\leftrightarrow x+1 = 2k+2$ *algebra*

$\leftrightarrow x+1 = 2(k+1)$ *factoring*

$\leftrightarrow x+1$ is even *by definition*

$\leftrightarrow (x+1)^2$ is even *Since x is even iff x^2 is even*

$\leftrightarrow x^2+2x+1$ is even *algebra*

QED

Existence Proofs

- 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 is 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
    - Then get a contradiction

Uniqueness Proofs

- 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
  1. A proof of existence: $\exists x P(x)$
  2. A proof of uniqueness: if $x \neq y$ then $\neg P(y)$)
- Together we have the following:

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

Counter Examples

- Sometimes you are asked to disprove a statement
- In such a situation you are actually trying to prove the negation of the statement
- With statements of the form $\forall x\ P(x)$, it suffices to give a counter example
  - because the existence of an element x for which $\neg P(x)$ holds 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 counterexample is n=4.
- In fact: for n=4, we have

  $n^2+n+1 = 4^2+4+1$

  $= 16+4+1$

  $= 21 = 3 \times 7$, which is clearly not prime

  QED

Counter Examples: A Word of Caution

- No matter how many examples you give, you can never prove a theorem by giving examples (unless the universe of discourse is finite—why?—which is in called an exhaustive proof)
- Counter examples can only be used to disprove universally quantified statements
- Do not give a proof by simply giving an example

Proof Strategies

- Example: Forward and backward reasoning
- If there were a single strategy that always worked for proofs, mathematics would be easy
- The best advice we can give you:
  - Beware of fallacies and circular arguments (i.e., begging the question)
  - Don't take things for granted, try proving assertions first before you can take/use them as facts
  - Try proving something for yourself before looking at the proof
  - The best way to improve your proof skills is PRACTICE.