Department Of Computer Science, CUI Lahore Campus

CSC102 - Discrete Structures

By

Mahwish Waqas

Lecture Outline

- Proofs
  - Vacuous Proof
  - Trivial Proof
  - Direct Proof
  - Indirect Proof
    - Proof by Contraposition
    - Proof by Contradiction

Proofs

- Proof:

  A proof is a valid argument that establishes the truth of a mathematical statement.
- Proofs are essential in mathematics and computer science.
- Some applications of proof methods
  - Proving mathematical theorems
  - Designing algorithms and proving they meet their specifications
  - Verifying computer programs
  - Establishing operating systems are secure
  - Making inferences in artificial intelligence
  - Showing system specifications are consistent
  - …

Terminology

- Theorem: A statement that can be shown true. Sometimes called facts.
- Lemma: A less important theorem that is useful to prove a theorem.
- Proof: Demonstration that a theorem is true. A convincing explanation of why the theorem is true.
- Axiom: A statement that is assumed to be true.
- Corollary: A theorem that can be proven directly from a theorem that has been proved.
- Conjecture: A statement that is being proposed to be a true statement.

Stating Theorems

- Theorem: If $x > y$, where x and y are positive real numbers, then $x^2 > y^2$.
- Theorem: For all positive real numbers x and y, if $x > y$, then $x^2 > y^2$.

Theorem

- Conditional statement (review):
  - $p \rightarrow q$ is true unless p is true and q is false.

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Methods of Proving Theorems

- Vacuous Proof
- Trivial Proof
- Direct Proof
- Indirect Proof
  - Contraposition
  - Contradiction

Vacuous Proof

- Consider an implication: $p \rightarrow q$
- If it can be shown that p is false, then the implication is always true.
  - By definition of an implication
- Note that you are showing that the **hypothesis is false.**

Vacuous Proof Example

- Assume P(n) is “if n > 0, then n^2 > 0”. Show that P(0) is true.

Vacuous Proof Example

- Assume P(n) is “if n > 0, then n^2 > 0”. Show that P(0) is true.

- **Proof:**

  P(0) is “if 0 > 0, then 0^2 > 0”.

  Since the hypothesis of P(0) is false, then P(0) is true.

- **Vacuous proof:**

  p $\rightarrow$ q is true when p is false.

Vacuous Proof Example

- If n is both odd and even then $n^2 = n + n$

Trivial Proof

- Consider an implication: $p \rightarrow q$
- If it can be shown that q is true, then the implication is always true.
  - By definition of an implication
- Note that you are showing that the **conclusion is true**.

Trivial Proof Example

- Assume P(n) is “if ab > 0, then $(ab)^n$ > 0”. Show that P(0) is true.

Trivial Proof Example

- Assume P(n) is “if ab > 0, then $(ab)^n$ > 0”. Show that P(0) is true.

- **Proof:**

  P(0) is “if ab >0, then $(ab)^0$ > 0”.

  $(ab)^0$ = 1 > 0

  Since the conclusion of P(0) is true, P(0) is true.

- **Trivial proof**:

  p $\rightarrow$ q is true when q is true.

Trivial Proof Example

- If n is the sum of two prime numbers, then either n is odd or n is even.
- If x is in CSD101 then x is a student.

Direct Proof

- A direct proof of a conditional statement p → q is constructed when the first step is the assumption that *p* is true; use axioms, definitions, and previously proven theorems, together with rules of inference, with the final step showing that *q* must also be true.

- A direct proof shows that a conditional statement $p \rightarrow q$ is true by showing that if *p* is true, then *q* must also be true, so that the combination *p* true and *q* false never occurs.

Direct Proof

- Direct proof of p $\rightarrow$ q:
- Assume p is true.

These steps are constructed using

Rules of inference

Axioms

Lemmas

Definitions

Proven theorems

…

Direct Proof

- q must be true.

Direct Proof

- Odd Number:
  n is odd if $n = 2k + 1$ for some k of type integer.

- Even Number:
  n is even if $n = 2k$ for some k of type integer.

Direct Proof

- Theorem:

  If n is an odd integer, then n^2 is odd.

Direct Proof

- Theorem:

  If n is an odd integer, then n^2 is odd.
- Proof:

  Assume n is an odd integer.

  By definition, ∃ integer k,

  such that n = 2k + 1

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

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

  Let m = 2k^2 + 2k.

  n^2 = 2m + 1

  So, by definition, n^2 is odd.

Direct Proof

- **Theorem:**

  If n and m are both perfect squares then nm is also a perfect square.

- **Definition:**

  An integer a is perfect square if $\exists$ integer b such that $a = b^2$.

Direct Proof

- Theorem:

  If n and m are both perfect squares then nm is also a perfect square.

- Proof:

  Assume n and m are perfect squares.

  By definition, ∃ integers s and t

  such that n = s^2 and m = t^2.

  nm = s^2t^2 = $(st)^2$

  Let k = st.

  nm = k^2

  So, by definition, nm is a perfect square.

Definition:
An integer a is perfect square if ∃ integer b such that a= b^2.

Direct Proof

- Prove If n and m are odd integers then $n + m$ is even.

Example

- Theorem:

  The sum of two rational numbers is rational.

- Proof:

  Assume r and s are rational.

  $\exists$ p,q $r = p/q$ $q \neq 0$

  $\exists$ t,u $s = t/u$ $u \neq 0$

  $r+s = p/q + t/u = (pu+tq) / (qu)$

  Since $q \neq 0$ and $u \neq 0$ then $qu \neq 0$.

  Let $m=(pu+tq)$ and $n=qu$ where $n \neq 0$.

  So, $r+s = m/n$, where $n \neq 0$.

  So, r+s is rational.

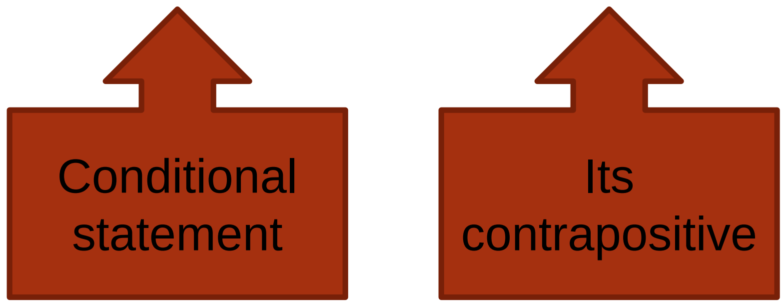
Definition:
The real number r is rational if r=p/q, $\exists$ integers p and q that $q \neq 0$.

Proof Techniques

- **Direct proof** leads from the hypothesis of a theorem to the conclusion.
- Proofs of theorems that do not start with the hypothesis and end with the conclusion, are called **indirect proofs**.

Proof By Contraposition

$$\mathbf{p} \to \mathbf{q} \equiv \neg\mathbf{q} \to \neg\mathbf{p}$$



- In a proof by contraposition of $p \to q$, we take $\neg q$ as a hypothesis and we show that $\neg p$ must follow.
- Thus, show that if $\neg q$ is true, then $\neg p$ is true
- Proof by contraposition is an indirect proof.

Proof By Contraposition

- Proof by contraposition of $p \rightarrow q$:
- Assume $\neg q$ is true.

These steps are constructed using

Rules of inference

Axioms

Lemmas

Definitions

Proven theorems

…

- $\neg p$ must be true.

Proof by contraposition

Proof By Contraposition (Example)

- Theorem:

  If n is an integer and $3n + 2$ is odd, then n is odd.

Proof By Contraposition (Example)

- Theorem:

  If n is an integer and $3n + 2$ is odd, then n is odd.

- Proof (by contraposition):

  Assume n is even.

  ∃ integer k, such that n = 2k

  3n+2 = 3(2k)+2 = 2(3k+1)

  Let m = 3k+1.

  3n+2 = 2m

  So, 3n+2 is even.

  By contraposition, if 3n+2 is odd, then n is odd.

Proof By Contraposition (Example)

- Theorem:

  If n = ab, where a and b are positive integers, then

  b $\leq \sqrt{n}$ or a $\leq \sqrt{n}$.

- Proof (by contraposition):
- Assume b $>\sqrt{n}$ and a $>\sqrt{n}$.

  ab > $(\sqrt{n})$. $(\sqrt{n})$

  ab > n

  So, n $\neq$ ab.

  By contraposition, if n = ab, then b $\leq \sqrt{n}$ or a $\leq \sqrt{n}$.

Example

- Theorem:

  If n is an integer and n^2 is even, then n is even.

  Direct proof or proof by contraposition?

- Proof (direct proof):

  Assume n^2 is an even integer.

  n^2 = 2k (k is integer)

  n = ± $\sqrt{2k}$

  ???

  dead end!

Example

- Theorem:

  If n is an integer and n^2 is even, then n is even.

  Direct proof or proof by contraposition?

- Proof (By contraposition):

  Assume n is an odd integer.

  n = 2k+1 (k is integer)

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

  Assume integer m = 2 k^2 + 2k.

  n^2 = 2m + 1

  So, n^2 is odd.

  By contraposition, If n^2 is even, then n is even.

Proof By Contradiction

- How to prove a proposition by contradiction?
  - Assume the proposition is false.
  - Using the assumption and other facts to reach a contradiction.
  - This is another kind of indirect proof.

Proof By Contradiction

- Proof by contradiction of $p \rightarrow q$:
- Assume p and ¬q is true.

These steps are constructed using
Rules of inference
Axioms
Lemmas
Definitions
Proven theorems
…
Proof by contradiction

contradiction

Proof By Contradiction (Example)

- Prove if $3n + 5$ is even then n is odd.

Proof By Contradiction (Example)

- Prove if $3n + 5$ is even then n is odd.
- Proof (proof by contradiction):

Assume $3n + 5$ is even and n is even.

n = 2k (k is some integer)

3n+5 = 3(2k) + 5 = 6k + 5 = 2(3k + 2) + 1

Assume m = 3k+2.

3n+5 = 2m + 1

So, 3n+5 is odd.

Which contradicts over assumption that $3n + 5$ is even

So by contradiction, if $3n + 5$ is even then n is odd.

Proof By Contradiction (Example)

- Prove if n^2 is odd then n is odd.

Proof By Contradiction (Example)

- Prove if n^2 is odd then n is odd.
- Proof (proof by contradiction):

Assume n^2 is odd and n is even.

∃ integer k n = 2k

n^2 = 4k^2 = 2(2k^2)

Let m = 2k^2

n^2 = 2m

So, n^2 is even.

Which contradicts over assumption that is “n^2 is odd ”.

So by contradiction, if n^2 is odd then n is odd.

Proof By Contradiction (Example)

- Prove that the difference of any rational number and any irrational number is irrational.

Proof By Contradiction (Example)

- Prove The difference of any rational number and any irrational number is irrational.
- Proof:

[We take the negation of the theorem and suppose it to be true.] Suppose ∃ a rational number x and an irrational number y such that (x − y) is rational. By definition of rational, we have

$x = a/b$ for some integers a and b with $b \neq 0$.

and $x - y = c/d$ for some integers c and d with $d \neq 0$.

$$x - y = c/d$$

$$a/b - y = c/d$$

$$y = a/b - c/d$$

$$= (ad - bc)/bd$$

But (ad − bc) are integers and $bd \neq 0$. Therefore, by definition of rational, y is rational. This contradicts the supposition that y is irrational. [Hence, the supposition is false and the theorem is true.]

Proof By Contradiction (Example)

- Prove that $\sqrt{2}$ is not rational by contradiction.

Proof By Contradiction (Example)

- Prove that $\sqrt{2}$ is not rational by contradiction.
- Proof (proof by contradiction):

Assume $\sqrt{2}$ is rational.
∃ a , b $\sqrt{2}$ = a/b b ≠ 0
If a and b have common factor, remove it by dividing a and b by it
2 = a^2 / b^2
2 b^2 = a^2
So, a^2 is even and by previous theorem, a is even.
∃ k a = 2k.
2 b^2 = 4 k^2
b^2 = 2 k^2
So, b^2 is even and by previous theorem, b is even.
∃ m b = 2m.
So, a and b have common factor 2 which contradicts the Assumption.

Definition:
The real number r is rational if r=p/q, ∃ integers p and q that q ≠ 0.

Practice Exercise and Chapter Reading

- Q – 1,2,3,6,9,10,17,18,19
- ***Chapter 1***, Kenneth H. Rosen, Discrete Mathematics and Its Applications, Section 1.7