Discrete Mathematics 3
Proof Theory Techniques

Dr. Maged Kassab

Introduction to Proofs

A proof : is a valid argument that establishes the truth of a mathematical statement.

There are two types of proofs :

- **Formal proof :** where all steps are supplied and the rules for each step in the argument are given
- **Informal proof :** where more than one rule of inference may be used in each step, where steps may be skipped, where the axioms being assumed and rule of inference used are not explicitly stated.

Introduction to Proofs (Cont.)

- A theorem is a statement that can be shown to be true.
  - Less important theorems sometimes are called propositions.
  - (Theorems can also be referred to as facts or results.)
  - it may be the universal quantification of a conditional statement with one or more premises and a conclusion, or it may be another type of logical statements.

- Proof is a valid argument (sequence of statements) that establishes the truth of a theorem. And the statements to be used in proofs include:

Introduction to Proofs (Cont.)

- A theorem is a statement that can be shown to be true.
  - Less important theorems sometimes are called *propositions.*
  - (Theorems can also be referred to as facts or results.)
  - it may be the universal quantification of a conditional statement with one or more premises and a conclusion, or it may be another type of logical statements.
- Proof is a valid argument (sequence of statements) that establishes the truth of a theorem. And the statements to be used in proofs include:

Introduction to Proofs (Cont.)

- **Axioms** or **postulates** (statement assumed to be true without proof)
  - Ex: If x is positive integer then x+1 is positive integer.
- **Hypothesis** (premises) of the theorem
- Previously proven **theorems**
- **Rules of inference** used to draw conclusions and to move from one step to another

Introduction to Proofs (Cont.)

- Lemma is a less important theorem that is helpful in the proof of other results
- A corollary is a theorem that can be established directly from a theorem that has been proved.
- A conjuncture
  - is a statement that is being proposed to be a true statement, usually on the basis of some partial evidence.
  - When a **proof** of a conjuncture is **found**, the conjuncture becomes a **theorem**

Introduction to Proofs (Cont.)

- Methods of proving theorems:
  - Direct proofs
  - Proof by Contraposition
  - Vacuous Proofs
  - Trivial Proofs
  - Proofs by Contradiction
  - Proof by cases

Methods of proving theorems – Direct proofs

- A direct proof of a conditional statement $p \rightarrow q$ is constructed when the first step is the assumption that p is true; subsequent steps are constructed using 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.
- In a direct proof, we assume that p is true and use axioms, definitions, and previously proven theorems, together with rules of inference, to show that q must also be true.

Methods of proving theorems – Direct proofs

- Definition : The integer n is even if there exists an integer k such that $n = 2k$, and n is odd if there exists an integer k such that $n = 2k + 1$.

- Note that every integer is either even or odd, and no integer is both even and odd.

- Two integers have the same parity when both are even or both are odd; they have opposite parity when one is even and the other is odd.

Methods of proving theorems - Direct proofs

- Example_Give a direct proof of the theorem :

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

- Proof:

We assume that n is odd. (hypothesis)

=> $n = 2k + 1$, where k is some integer. (definition of odd number)

We can square both sides of the equation $n = 2k + 1$ to obtain

a new equation that expresses n^2

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

=> $n^2 = 2r+1$ is odd.

Methods of proving theorems – Direct proofs

- Example Give a direct proof of the theorem :

"if m and n are both perfect squares, then nm is also perfect"

We assume that m and n are both perfect squares :

$m = s^2$ and $n = t^2$

$m.n = s^2.t^2 = (st)^2$

m.n is also perfect

- Can we use this methodology to prove theorems of the form $\forall x(P(x) \rightarrow Q(x))$?

Proofs of theorems of this type that are not direct proofs, that is, that do not start with the premises and end with the conclusion are called indirect proof.

Methods of proving theorems – Proof by Contraposition

- An extremely useful type of indirect proof is known as proof by contraposition ($p \to q$ equivalent to $\neg q \to \neg p$)

- Methodology of Proof by Contraposition : It is proving the conditional statement $p \to q$ by showing that its contrapositive, $\neg q \to \neg p$, is true

Methods of proving theorems – Proof by Contraposition

to prove that $p \to q$

Begin with $\neg q$ is true as a premise

using (axioms, definitions previously proven theorems with rules of inference)

$\neg p$ must be also true

It is showing the contrapositive $\neg q \to \neg p$ is true

Methods of proving theorems – Proof by Contraposition

- **Example** Prove that if n is an integer and $3n + 2$ is odd, then n is odd.
  - Proof:

We assume that the conclusion of the conditional statement "if $3n + 2$ is odd, then n is odd" is false .

=> We assume that n is even. (hypothesis)

=> $n = 2k$, where k is some integer. (definition of even number)

(Substituting $2k$ for n in hypthesis : $3n+2$)

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

Since $r = 3k + 1$ is an integer

=> $3n + 2 = 2r$ is even .

Methods of proving theorems – Proof by Contraposition

- **Example** Use an indirect proof to show that "if n^2 is odd then n is odd"
  - Proof:

The contraposition is "if n is not odd then n^2 is not odd "

=> We Assume that n is not odd i.e., n is even (hypothesis)

=> $n = 2k$, where k is some integer. (definition of even number)

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

Since $r = 2k^2$ is an integer

=> $n^2 = 2r$ (definition of not odd number)

Thus , if n^2 is odd then n is odd is true

Methods of proving theorems – Proof by Contraposition

- Example Prove that if $n = ab$ where a and b are positive integers then $a \le \sqrt{n}$ or $b \le \sqrt{n}$

  - Proof: Let p="$a \le \sqrt{n}$", q="$b \le \sqrt{n}$" and r="$n=ab$"

    We want to prove that $r \rightarrow p \vee q$

    => The contraposition is $\neg(p \vee q) \rightarrow \neg r$ (By definition)

    => $\neg p \wedge \neg q \rightarrow \neg r$ (De Morgan's law)

    Now, assume that $a > \sqrt{n}$ and $b > \sqrt{n}$ ($\neg p \wedge \neg q$)

    => $a.b > \sqrt{n}.\sqrt{n} = n$ (by multiplying above twos)

    => $ab \neq n$

    => $\neg r$ which contradicts the statement $n = ab$

Because the negation of the conclusion of the conditional statement implies that the hypothesis is false, the original conditional statement is true.

Methods of proving theorems – Vacuous Proofs

p	q	$p \to q$
F	F	T
F	T	T
T	F	F
T	T	T

- Vacuous Proofs A conditional statement $p \to q$ is TRUE if p is FALSE. If we can show that p is False, then we have a proof, called *vacuous proof*, of the conditional statement $p \to q$.

- Example Show that the proposition P(0) is true, where P(n) is "If $n > 1$, then $n^2 > n$" and the domain consists of all integers.

➢ Proof: Note that P(0) is "If $0 > 1$, then $0^2 > 0$." We can show P(0) using a vacuous proof. Indeed, the hypothesis $0 > 1$ is false. This tells us that P(0) is automatically true.

- Example Prove that if he is alive and he is dead then the sun is ice cold

➢ Proof: Since the hypothesis is always false the implication is vacuously true.

Methods of proving theorems – Vacuous Proofs

p	q	$p \to q$
F	F	T
F	T	T
T	F	F
T	T	T

- Trivial Proofs A conditional statement $p \to q$ is TRUE if q is True. If we can show that q is True, then we have a proof, called *Trivial proof*, of the conditional statement $p \to q$.

- Example Let $P(n)$ be "If a and b are positive integers with $a \geq b$, then $a^n \geq b^n$ where the domain consists of all nonnegative integers. Show that $P(0)$ is true.

  - Proof: The proposition $P(0)$ is "If $a \geq b$, then $a^0 \geq b^0$." Because $a^0 = b^0 = 1$, the conclusion of the conditional statement "If $a \geq b$, then $a^0 \geq b^0$" is true. Hence, this conditional statement, which is $P(0)$, is true

- Example Prove that if $x=2$ then $x^2 \geq 0$ for all real numbers

  - Proof: Since $x^2 \geq 0$ is true then the implication is trivially true. (we didn't use the fact $x=2$)

1. Propositional Logic

1. Propositional Logic

1. Propositional Logic

1. Propositional Logic

1. Propositional Logic

1. Propositional Logic

1. Propositional Logic

1. Propositional Logic

1. Propositional Logic

1. Propositional Logic

1. Propositional Logic

1. Propositional Logic

1. Propositional Logic

1. Propositional Logic

1. Propositional Logic

1. Propositional Logic

1. Propositional Logic

1. Propositional Logic

1. Propositional Logic

1. Propositional Logic

Introduction to Proofs

A proof : is a valid argument that establishes the truth of a mathematical statement.

There are two types of proofs :

- **Formal proof :** where all steps are supplied and the rules for each step in the argument are given
- **Informal proof :** where more than one rule of inference may be used in each step, where steps may be skipped, where the axioms being assumed and rule of inference used are not explicitly stated.

شكراً لحسن المتابعة