SAKARYA ÜNİVERSİTESİ

Discrete Mathematics
LECTURE 6
Proofs

Assistant Professor Gülüzar ÇİT

Outline

- Theorem
- Proof
- Methods of Proving Theorems
  - Direct Proofs
  - Indirect Proofs
    - Proof by Contraposition
    - Trivial Proof
    - Proof by Contradiction
    - Proof by Equivalence
    - Counterexample
- References

Proofs

- **Theorem**
  - a statement that can be shown to be true
  - can also be referred to as **facts** or **results**.
  - universal quantification of a conditional statement with one or more **premises** and a **conclusion**.
  - true with a **proof**.

Proofs…

- **Proof**
  - a valid argument that establishes the truth of a theorem.
  - the statements used in a proof can include **axioms** (or **postulates**), which are statements we assume to be true

aksiyon

varsayımlar

Proofs…

- **Methods of Proving Theorems**
  - Direct Proofs
  - Indirect Proofs
    - Proof by Contraposition
    - Trivial Proof
    - Proof by Contradiction
    - Proof by Equivalence
    - Counterexample

Proofs…

➢ Direct Proof

- A **direct proof** of a conditional statement $p \longrightarrow q$
  - 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.
    inşa edilmiş
  - shows that a conditional statement $p \longrightarrow q$ 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.
  - 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.

Proofs…

- **Direct Proof…**
  - **Example:** Prove that "If n is an odd integer, then n^2 is odd."

$\forall n\, P(n) \longrightarrow Q(n)$
$P(n)$: "*n* is an odd integer"
$Q(n)$: "n^2 is odd"

n is odd $\Longrightarrow n = 2k + 1$ where *k* is some integer
$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 = 2y + 1 \Longrightarrow n^2$ is odd

Proofs…

- **Direct Proof…**
  - **Example:** Prove that "if *m* and *n* are both perfect squares, then *n.m* is also a perfect square"
    - NOTE: An integer *a* is a perfect square if there is an integer *b* such that $a = b^2$

$\forall n\, P(n) \wedge Q(n) \longrightarrow S(n)$
$P(n)$: "*m* is a perfect square"
$\mathrm{Q}(n)$: "*n* is a perfect square"
$P(n) \wedge Q(n)$: "*m* and *n* are both perfect squares"
$S(n)$: "*n.m* is also perfect square"

m is a perfect square $\Longrightarrow m = s^2$
n is a perfect square $\Longrightarrow n = t^2$
$n.m = s^2 t^2 = (st)^2 \Longrightarrow$ *n.m* is a perfect square

Proofs…

- **Indirect Proofs**
  - proofs of theorems that are not direct proofs
  - another method of proving theorems of the form $\forall x\ P(x) \longrightarrow Q(x)$
  - do not start with the premises and end with the conclusion

Proofs…

- **Proof by Contraposition**
  - an extremely useful type of indirect proof
  - make use of the fact that the conditional statement $p \longrightarrow q$ is equivalent to its contrapositive, $\sim q \rightarrow \sim p$
  - This means that the conditional statement $p \longrightarrow q$ can be proved by showing that its contrapositive, $\sim q \rightarrow \sim p$, is true.

Proofs...

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

$\forall n\ P(n) \longrightarrow Q(n)$
$P(n)$: "$3n + 2$ is odd"
$Q(n)$: "n is odd"

$\forall n\ \neg Q(n) \longrightarrow \neg P(n)$
$\sim Q(n)$: "n is even"
$\sim P(n)$: "$3n + 2$ is even"

n is even $\Longrightarrow n = 2k$ where k is some integer
$3n + 2 = 3(2k) + 2 = 2(3k + 1) = 2y \Longrightarrow 3n + 2$ is even

Proofs...

Proof by Contraposition...

- **Example:** Prove that " if $n = ab$, where *a* and *b* are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$ "

$\forall n\, P(n) \longrightarrow Q(n)$
$P(n)$: "$n = ab$"
$Q(n)$: "$a \leq \sqrt{n}$ or $b \leq \sqrt{n}$"

$\forall n\, \neg Q(n) \longrightarrow \sim P(n)$
$\sim Q(n)$: "$a > \sqrt{n}$ and $b > \sqrt{n}$"
$\sim P(n)$: "n $\neq ab$"

$0 < s < t$ and $0 < u < v \Longrightarrow su < tv$
$0 < \sqrt{n} < a$ and $0 < \sqrt{n} < b \Longrightarrow \sqrt{n}.\sqrt{n} < ab \Longrightarrow n \neq ab$

Proofs…

- **Proof by Contraposition…**
  - **Example:** Prove that "if *n* is an integer and n^2 is odd, then *n* is odd"

$\forall n\, P(n) \longrightarrow Q(n)$
$P(n)$: "n^2 is odd"
$Q(n)$: "n is odd"

$\forall n \sim Q(n) \longrightarrow \sim P(n)$
$\sim Q(n)$: "n is even"
$\sim P(n)$: "n^2 is even"

n is even $\implies$ $n = 2k$ where *k* is some integer
$n^2 = (2k)^2 = 4k^2 = 2(2k^2) = 2y \Longrightarrow n^2$ is even

Proofs…

- **Trivial Proof**
  - proof of $p \rightarrow q$ that uses the fact that q is true

  - 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.

$\forall n\ P(n) \longrightarrow Q(n)$
$P(n)$: "$a \geq b$"
$Q(n)$: "$a^n \geq b^n$"

The preposition $P(0)$ is "if $a \geq b$ then $a^0 \geq b^0$
$a^0 = b^0 = 1 \Longrightarrow P(0)$ is TRUE

Proofs…

- **Proof by Contradiction**
  - can be used to prove that a single/conditional statement is true
    - first suppose the statement is false. That is, suppose that the negation of the statement is true.
    - show that this supposition leads logically to a contradiction.
    - conclude that the statement to be proved is true.

Proofs…

- **Proof by Contradiction…**
  - Example: Show that "There is no integer both even and odd."

P : "There is no integer both even and odd"
$\sim P$: "There is at least one integer *n* both even and odd"

To dedude a contradiction suppose $\sim P$ to be true

n is odd $\Longrightarrow n = 2k$
n is even $\Longrightarrow n = 2m + 1$

$n = 2k = 2m + 1 \Longrightarrow k - m = {}^{1}/_{2} \Longrightarrow$not an integer, a contradiction, because the difference between two integer must also be an integer

Proofs…

Proof by Contradiction…

- **Example:** Give a proof by contradiction of the theorem "If $3n + 2$ is odd, then n is odd."

$\forall n \; P(n) \longrightarrow Q(n)$
$P(n)$: "$3n + 2$ is odd"
$Q(n)$: "n is odd"

$p \longrightarrow q \equiv {\sim}p \vee q \equiv \overline{(p \wedge {\sim}\, q)}$

$\Longrightarrow$To construct a proof by contradiction, assume that both p and $\sim q$ are true

$\sim Q(n)$: "n is even" $\Longrightarrow n = 2k$
$P(n)$: "$3n + 2$ is odd" $\Longrightarrow 3n + 2 = 6k + 2 = 2(3k + 1) = 2y$
$\Longrightarrow$even $\Longrightarrow \sim P(n) \Longrightarrow$ CONTRADICTION!...

Proofs…

- **Proof by Equivalence**
  - to prove a theorem that is a biconditional statement, that is, a statement of the form $p \leftrightarrow q$, we show that $p \rightarrow q$ and $q \rightarrow p$ are both true.
  - The validity of this approach is based on the tautology
    - $(p \leftrightarrow q) \leftrightarrow (p \longrightarrow q) \wedge (q \longrightarrow p).$

Proofs...

- **Proof by Equivalence...**
  - Example: Prove the theorem "If *n* is an integer, then *n* is odd if and only if n^2 is odd."

$$\forall n\, P(n) \leftrightarrow Q(n) \equiv \big(P(n) \longrightarrow Q(n)\big) \land \big(Q(n) \longrightarrow P(n)\big)$$

$P(n)$: "n is odd"
$Q(n)$: "n^2 is odd"

$P(n) \longrightarrow Q(n) \Longrightarrow$can be proved by direct proof
Q$(n) \longrightarrow P(n) \Longrightarrow$can be proved by indirect proof

Proofs…

- **Proofs by Equivalence…**
  - Example: Show that these statements about the integer *n* are equivalent:

    P_1: *n* is even.

    P_2: *n* − 1 is odd.

    P_3: n^2 is even.

$$P_1 \leftrightarrow P_2 \leftrightarrow P_3 \equiv (P_1 \rightarrow P_2) \wedge (P_2 \rightarrow P_3) \wedge (P_3 \rightarrow P_1)$$

$(P_1 \rightarrow P_2) \Longrightarrow$ can be proved by direct proof
$(P_2 \rightarrow P_3) \Longrightarrow$ can be proved by direct proof
$(P_3 \rightarrow P_1) \Longrightarrow$ can be proved by indirect proof

Proofs…

- **Counterexample**
  - to show that a statement of the form $\forall x P(x)$, we need only find a counterexample, that is, an example x for which $P(x)$ is false.

Proofs…

- **Counterexample…**
  - Example: Show that the statement "Every positive integer is the sum of the squares of two integers" is false.

$\forall n\, P(n)$: "Every positive integer is the sum of the squares of two integers«

$1: 0^2 + 1^2 = 1$
$2: 1^2 + 1^2 = 1$
$3: 1^2 + 1^2 \neq 3 \Longrightarrow$ counterexample

Proofs…

- **Counterexamples**
  - Example: Show that the statement "If a natural number is divisible by 3 and 2, that natural number is divisible by 12." is false.

$$\forall n\ P(n) \longrightarrow Q(n): (3|x) \land (2|x) \longrightarrow (12|x)$$

$n = 30$: $(3|30)$ ✓ and $(2|30)$ ✓ but $(3|30)$ X $\Longrightarrow$ counterexample

Study Questions

- Prove that "If n is natural number and n is even then $n+1$ is odd."
- Prove that "If n is a natural number and prime then n is odd."

References

- K.H. Rosen, Discrete Mathematics and Its Applications, Seventh Edition, Mc Graw Hill, 2012.
- R.P. Grimaldi, Discrete and Combinatorial Mathematcics, An Applied Introduction, Fifth Edition, Pearson, 2003.
- S.S. Epp, Discrete Mathemtics with Applications, Fouth Edition, 2010.
- N. Yurtay, "Ayrık İşlemsel Yapılar" Lecture Notes, Sakarya University