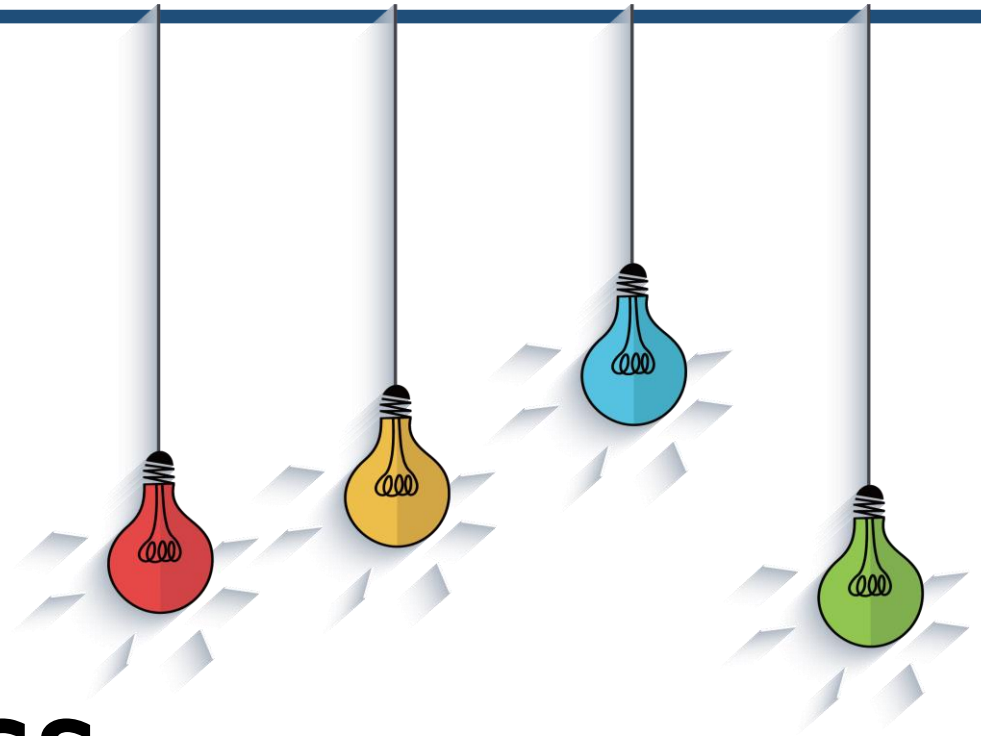
UMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA



IF120
Discrete Mathematics

03 Proofs

Angga Aditya Permana, Januar Wahjudi, Yaya Suryana, Meriske, Muhammad Fahrury Romdendine

REVIEW

- Propositions
- Logics Operators and Truth Table
- Conditional Propositions and Logical Equivalence
- Arguments and Rules of Inference
- Quantifiers

OUTLINE

- Direct Proofs and Indirect Proofs
- Other Proofs Methods
- Proofs Strategy
- Mathematical Induction

Mathematical Systems

- A mathematical system consists of axioms, definitions, and undefined terms.
- **Axioms** are assumed to be true.
- **Definitions** are used to create new concepts in terms of existing ones.
- Some **terms** are not explicitly defined but rather are implicitly defined by the axioms.
- Within a mathematical system we can derive theorems.
- A **theorem** is a proposition that has been proved to be true.
- Special kinds of theorems are referred to as lemmas and corollaries.
- A **lemma** is a theorem that is usually not too interesting in its own right but is useful in proving another theorem.
- A **corollary** is a theorem that follows easily from another theorem.
- An argument that establishes the truth of a theorem is called a **proof**.

Mathematical Systems

- Euclidean geometry furnishes an example of a mathematical system.
- Among the **axioms** are

✓Given two distinct points, there is exactly one line that contains them.

✓Given a line and a point not on the line, there is exactly one line parallel to the line through the point.

- The terms **point** and **line** are **undefined terms** that are implicitly defined by the axioms that describe their properties.
- Among the **definitions** are

✓Two triangles are congruent if their vertices can be paired so that the corresponding sides and corresponding angles are equal.

✓Two angles are supplementary if the sum of their measures is 180°.

Mathematical Systems

- Examples of **theorems** about real numbers are

✓ $x \cdot 0 = 0$ for every real number x.

✓ For all real numbers x, y, and z, if $x \leq y$ and $y \leq z$, then $x \leq z$.

- An example of a **lemma** about real numbers is

✓ If n is a positive integer, then either $n - 1$ is a positive integer or $n - 1 = 0$.

- Theorems are often of the form

$$For\ all\ x_1, x_2, \ldots, x_n, if\ p(x_1, x_2, \ldots, x_n), then\ q(x_1, x_2, \ldots, x_n).$$

- This universally quantified statement is true provided that the conditional proposition

$$if\ p(x_1, x_2, \ldots, x_n), then\ q(x_1, x_2, \ldots, x_n)$$

is true for all $x_1, x_2, \ldots, x_n$ in the domain of discourse.

Direct Proofs

- *Definition*: An integer n is **even** if there exists an integer k such that n = 2k. An integer n is **odd** if there exists an integer k such that n = 2k + 1.

❑ Give a direct proof of the following statement. For all integers m and n, if m is odd and n is even, then m + n is odd.

❖ Let m and n be arbitrary integers, and suppose that m is odd and n is even. We prove that m + n is odd. By definition, since m is odd, there exists an integer k_1 such that $m = 2k_1 + 1$. Also, by definition, since n is even, there exists an integer k_2 such that $n = 2k_2$. Now the sum is $m + n = (2k_1 + 1) + (2k_2) = 2(k_1 + k_2) + 1$. Thus, there exists an integer k (namely $k = k_1 + k_2$) such that $m + n = 2k + 1$. Therefore, m + n is odd.

Direct Proofs

- There are frequently many different ways to prove a statement. We illustrate by giving two proofs of the statement $X \cup (Y - X) = X \cup Y$ for all sets X and Y .
- [First proof] We show that for all x, if $x \in X \cup (Y - X)$, then $x \in X \cup Y$, and if $x \in X \cup Y$, then $x \in X \cup (Y - X)$.

  Let $x \in X \cup (Y - X)$. Then $x \in X$ or $x \in Y - X$. If $x \in X$, then $x \in X \cup Y$. If $x \in Y - X$, then $x \in Y$, so again $x \in X \cup Y$. In either case, $x \in X \cup Y$.

  Let $x \in X \cup Y$. Then $x \in X$ or $x \in Y$. If $x \in X$, then $x \in X \cup (Y - X)$. If $x \notin X$, then $x \in Y$. In this case, $x \in Y - X$. Therefore, $x \in X \cup (Y - X)$. In either case, $x \in X \cup (Y - X)$. The proof is complete.
- [Second proof] Letting U denote the universal set, we obtain

$$
\begin{aligned}
X \cup (Y - X) &= X \cup (Y \cap \bar{X}) && [Y - X = Y \cap \bar{X}] \\
&= (X \cup Y) \cap (X \cup \bar{X}) && [\text{Distributive law}] \\
&= (X \cup Y) \cap U && [\text{Complement law}] \\
&= X \cup Y && [\text{Identity law}].
\end{aligned}
$$

Disproving a Universally Quantified Statement

- Recall that to disprove

$$\forall x\, P(x)$$

  we simply need to find one member x in the domain of discourse that makes P(x) false.

- Such a value for x is called a **counterexample**.

❑ The statement

$$\forall n \in Z^{+} (2^{n} + 1\ is\ prime)$$

  is false.

  A counterexample is n = 3 since $2^3 + 1 = 9$, which is not prime.

Proof by Contradiction

- A **proof by contradiction** establishes p → q by assuming that the hypothesis p is true and that the conclusion q is false and then, using p and ¬q as well as other axioms, definitions, previously derived theorems, and rules of inference, derives a **contradiction**.
- A contradiction is a proposition of the form r ∧ ¬r (r may be any proposition whatever).
- A proof by contradiction is sometimes called an **indirect proof** since to establish p → q using proof by contradiction, we follow an indirect route:

  We derive r ∧ ¬r and then conclude that q is true.
- Proof by contradiction may be justified by noting that the propositions

$$p \rightarrow q \; and \; (p \wedge \neg q) \rightarrow (r \wedge \neg r)$$

  are equivalent.
- The equivalence is immediate from a truth table.

Proof by Contradiction

- We will give a proof by contradiction of the following statement:

$$For\ every\ n\ \in\ Z, if\ n^2\ is\ even, then\ n\ is\ even$$

- We give a proof by contradiction.

  Thus we assume the hypothesis

$$n^2\ is\ even$$

  and that the conclusion is false

$$n\ is\ odd$$

  Since n is odd, there exists an integer k such that n = 2k + 1. Now

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

  Thus n^2 is odd, which contradicts the hypothesis n^2 is even.

  The proof by contradiction is complete.

  We have proved that $for\ every\ n\ \in\ Z, if\ n^2\ is\ even, then\ n\ is\ even.$

Proof by Contradiction

- We will prove that $\sqrt{2}$ is irrational using proof by contradiction.
- We use proof by contradiction and assume that $\sqrt{2}$ is rational.

  Then there exist integers p and q such that $\sqrt{2}$ = p/q.

  We assume that the fraction p/q is in lowest terms so that p and q are not both even.

  Squaring $\sqrt{2}$ = p/q gives 2 = p^2 / q^2, and multiplying by q^2 gives $2q^2 = p^2$.

  It follows that p^2 is even. The last example tells us that p is even.

  Therefore, there exists an integer k such that p = 2k.

  Substituting p = 2k into $2q^2 = p^2$ gives $2q^2 = (2k)^2 = 4k^2$.

  Canceling 2 gives $q^2 = 2k^2$.

  Therefore q^2 is even, and the last example tells us the q is even.

  Thus p and q are both even, which contradicts our assumption that p and q are not both even.

  Therefore, $\sqrt{2}$ is irrational.

Proof by Contrapositive

- Suppose that we give a proof by contradiction of $p \rightarrow q$ in which we deduce $\neg p$.
- In effect, we have proved $\neg q \rightarrow \neg p$.
- [Recall that $p \rightarrow q$ and $\neg q \rightarrow \neg p$ are equivalent.]
- This special case of proof by contradiction is called **proof by contrapositive**.

Proof by Contrapositive

- Use proof by contrapositive to show that

$$for\ all\ x\ \in\ R, if\ x^2\ is\ irrational, then\ x\ is\ irrational.$$

- We begin by letting x be an arbitrary real number.

  We prove the contrapositive of the given statement, which is

$$if\ x\ is\ not\ irrational, then\ x^2\ is\ not\ irrational$$

  or, equivalently,

$$if\ x\ is\ rational, then\ x^2\ is\ rational$$

  So suppose that x is rational.

  Then x = p/q for some integers p and q.

  Now $x^2 = p^2/\ q^2$.

  Since x^2 is the quotient of integers, x^2 is rational.

  The proof is complete.

Proof by Cases & Exhaustive Proof

- **Proof by cases** is used when the original hypothesis naturally divides itself into various cases. Sometimes the number of cases to prove is finite and not too large so we can check them all one by one. We call this type of proof **exhaustive proof**.

❑ Prove that $2m^2+3n^2 = 40$ has no solution in positive integers, that is, that $2m^2+3n^2 = 40$ is false for all positive integers m and n.

❖ If $2m^2+3n^2 = 40$, we must have $2m^2 \leq 40$. Thus $m^2 \leq 20$ and $m \leq 4$.

Similarly, we must have $3n^2 \leq 40$. Thus $n^2 \leq 40/3$ and $n \leq 3$.

Therefore it suffices to check the cases m = 1, 2, 3, 4 and n = 1, 2, 3.

The entries in the table give the value of $2m^2+3n^2 = 40$ for the indicated values of m and n.

Since $2m^2+3n^2 \neq 40$ for m = 1, 2, 3, 4 and n = 1, 2, 3, and $2m^2+3n^2 > 40$ for m > 4 or n > 3, we conclude that $2m^2+3n^2 = 40$ has no solution in positive integers.

		m			
		1	2	3	4
n	1	5	11	21	35
	2	14	20	30	44
	3	29	35	45	59

Proof by Equivalence

- Some theorems are of the form p **if and only if** q.
- Such theorems are proved by using the **equivalence**

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

that is, to prove "p if and only if q," prove "if p then q" and "if q then p."

Proof by Equivalence

- Prove that for every integer n, n is odd if and only if n − 1 is even.
- We first prove that if n is odd then n − 1 is even.

  If n is odd, then n = 2k + 1 for some integer k. Now

  $$n - 1 = (2k + 1) - 1 = 2k$$

  Therefore, n − 1 is even.

  Next we prove that if n − 1 is even then n is odd.

  If n − 1 is even, then n − 1 = 2k for some integer k. Now

  $$n = 2k + 1$$

  Therefore, n is odd.

  The proof is complete.

Existence Proofs

- A proof of

$$\exists x\, P(x)$$

is called an **existence proof**.

❑ Let a and b be real numbers with a < b. Prove that there exists a real number x satisfying $a < x < b$.

❖ It suffices to find one real number x satisfying $a < x < b$.

The real number

$$x = \frac{a+b}{2}$$

halfway between a and b, surely satisfies $a < x < b$.

Resolution Proofs

- **Resolution** is a proof technique proposed by J. A. Robinson in 1965 that depends on a single rule:

$$If\ p \vee q\ and \neg p \vee r\ are\ both\ true, then\ q \vee r\ is\ true$$

- Because resolution depends on this single, simple rule, it is the basis of many computer programs that reason and prove theorems.
- In a proof by resolution, the hypotheses and the conclusion are written as **clauses**.
- A clause consists of terms separated by or's, where each term is a variable or the negation of a variable.

❑ The expression $a \vee b \vee \neg c \vee d$ is a clause.

❑ The expression $x\ y \vee w \vee \neg z$ is not a clause.

Nb: $x\ y$ is a shorten for $x \wedge y$

Resolution Proofs

- We prove the following using resolution:

$$1.\ a \vee b$$
$$2.\ \neg a \vee c$$
$$3.\ \neg c \vee d$$
$$\therefore b \vee d$$

- Applying Resolution Rule to expressions 1 and 2, we derive

$$b \vee c$$

Applying Resolution Rule to expressions 3 and 4, we derive

$$b \vee d$$

the desired conclusion.

Given the hypotheses 1, 2, and 3, we have proved the conclusion $b \vee d$.

- Special cases of Resolution Rule are as follows:

$$If\ p \vee q\ and \neg p\ are\ true, then\ q\ is\ true.$$
$$If\ p\ and \neg p \vee r\ are\ true, then\ r\ is\ true.$$

- We prove the following using resolution:

$$\begin{array}{l} 1.\ a \vee \neg bc \\ 2.\ \neg(a \vee d) \\ \hline \therefore\ \neg b \end{array}$$

- We replace hypothesis 1 with the two hypotheses

$$a \vee \neg b$$
$$a \vee c$$

We use the first of De Morgan's laws to replace hypothesis 2 with the two hypotheses

$$\neg a$$
$$\neg d$$

The argument becomes

$$\begin{array}{l} 1.\ a \vee \neg b \\ 2.\ a \vee c \\ 3.\ \neg a \\ 4.\ \neg d \\ \hline \therefore\ \neg b \end{array}$$

Applying Resolution Rule to expressions 1 and 3, we immediately derive the conclusion ¬b.

Mathematical Induction

- Suppose that we have a propositional function S(n) whose domain of discourse is the set of positive integers.
- Suppose that

  $S(1)\ is\ true;$ (basis step)

  $for\ all\ n \geq 1, if\ S(n)\ is\ true, then\ S(n+1)\ is\ true.$ (inductive step)

  Then S(n) is true for every positive integer n.

- *Definition*: n **factorial** is defined as

$$n! = \begin{cases} 1 & if\ n = 0 \\ n(n-1)(n-2)\ldots 2.1 & if\ n \geq 1 \end{cases}$$

Mathematical Induction

- Use induction to show that

$$n! \geq 2^{n-1} \; for \; all \; n \geq 1 \quad (3.1)$$

- Basis Step (n = 1)

  We must show that (3.1) is true if n = 1. This is easily accomplished, since $1! = 1 \geq 1 = 2^{1-1}$.

  Inductive Step

  We assume that the inequality is true for n ≥ 1; that is, we assume that

$$n! \geq 2^{n-1} \quad (3.2)$$

  is true. We must then prove that the inequality is true for n + 1; that is, we must prove that

$$(n + 1)! \geq 2^{n} \quad (3.3)$$

  is true.

Mathematical Induction

We can relate (3.2) and (3.3) by observing that

$$(n + 1)! = (n + 1)(n!)$$

Now

$$\begin{aligned}(n + 1)! &= (n + 1)(n!) \\ &\geq (n + 1)2^{n-1} && by\ (3.2) \\ &\geq 2 \cdot 2^{n-1} && since\ n + 1 \geq 2 \\ &= 2^n\end{aligned}$$

Therefore, (3.3) is true.

We have completed the Inductive Step.

Since the Basis Step and the Inductive Step have been verified, the Principle of Mathematical Induction tells us that (3.1) is true for every positive integer n.

Mathematical Induction

- Use induction to show that $5^n - 1$ is divisible by 4 for all n ≥ 1.

- Basis Step (n = 1)

  If n = 1, $5^n - 1 = 5^1 - 1 = 4$, which is divisible by 4.

  Inductive Step

  We assume that $5^n - 1$ is divisible by 4. We must then show that $5^{n+1} - 1$ is divisible by 4. We use the fact that if p and q are each divisible by k, then p + q is also divisible by k. In our case, k = 4.

  We relate the $(n + 1)$st case to the nth case by writing

  $$5^{n+1} - 1 = 5^n - 1 + \text{to be determined.}$$

  Now, by the inductive assumption, $5^n - 1$ is divisible by 4. If "to be determined" is also divisible by 4, then the preceding sum, which is equal to $5^{n+1} - 1$, will also be divisible by 4, and the Inductive Step will be complete. We must find the value of "to be determined."

Mathematical Induction

Now

$$5^{n+1} - 1 = 5 \cdot 5^n - 1 = 4 \cdot 5^n + 1 \cdot 5^n - 1$$

Thus, "to be determined" is $4 \cdot 5^n$, which is divisible by 4.

Formally, we could write the Inductive Step as follows.

By the inductive assumption, $5^n - 1$ is divisible by 4 and, since $4 \cdot 5^n$ is divisible by 4, the sum

$$(5^n - 1) + 4 \cdot 5^n = 5^{n+1} - 1$$

is divisible by 4.

Since the Basis Step and the Inductive Step have been verified, the Principle of Mathematical Induction tells us that $5^n - 1$ is divisible by 4 for all n ≥ 1.

PRACTICE

PRACTICE 1

- Prove that for all integers m and n, if m and n are even, then m + n is even.
- Prove that for all rational numbers x and y, x + y is rational.
- Prove that $X \cap Y \subseteq X$ for all sets X and Y.

PRACTICE 2

- Prove that for every n ∈ Z, if n^2 is odd, then n is odd.
- Prove that for all x, y ∈ R, if x is rational and y is irrational, then x + y is irrational.
- Prove that if a and b are real numbers with a < b, there exists a rational number x satisfying a < x < b.

PRACTICE 3

- Use resolution to derive each conclusion.

1.
$$\begin{array}{c} \neg p \vee q \vee r \\ \neg q \\ \neg r \\ \hline \therefore \neg p \end{array}$$

2.
$$\begin{array}{c} \neg p \vee t \\ \neg q \vee s \\ \neg r \vee st \\ p \vee q \vee r \vee u \\ \hline \therefore s \vee t \vee u \end{array}$$

PRACTICE 4

- Using induction, verify that each equation is true for every positive integer n.

1. $1 + 3 + 5 + \cdots + (2n - 1) = n^2$
2. $1(1!) + 2(2!) + \cdots + n(n!) = (n + 1)! - 1$

NEXT WEEK'S OUTLINE

- Functions
- Sequences
- Strings

REFERENCES

- Johnsonbaugh, R., 2005, *Discrete Mathematics*, New Jersey: Pearson Education, Inc.
- Rosen, Kenneth H., 2005, *Discrete Mathematics and Its Applications*, 6th edition, McGraw-Hill.
- Hansun, S., 2021, *Matematika Diskret Teknik*, Deepublish.
- Lipschutz, Seymour, Lipson, Marc Lars, *Schaum's Outline of Theory and Problems of Discrete Mathematics*, McGraw-Hill.
- Liu, C.L., 1995, *Dasar-Dasar Matematika Diskret*, Jakarta: Gramedia Pustaka Utama.
- Other offline and online resources.

Visi

Menjadi Program Studi Strata Satu Informatika **unggulan** yang menghasilkan lulusan **berwawasan internasional** yang **kompeten** di bidang Ilmu Komputer (*Computer Science*), **berjiwa wirausaha** dan **berbudi pekerti luhur**.

INFORMATIKA
UMN
UNIVERSITAS MULTIMEDIA NUSANTARA

Misi

1. Menyelenggarakan pembelajaran dengan teknologi dan kurikulum terbaik serta didukung tenaga pengajar profesional.
2. Melaksanakan kegiatan penelitian di bidang Informatika untuk memajukan ilmu dan teknologi Informatika.
3. Melaksanakan kegiatan pengabdian kepada masyarakat berbasis ilmu dan teknologi Informatika dalam rangka mengamalkan ilmu dan teknologi Informatika.