Discrete Mathematics, KOM1062 Lecture #3

Instructor: Dr. Yavuz Eren

Lecture Book: **"Discrete Mathematics, Seventh Edt., Kenneth H. Rosen, 2007, McGraw Books Discrete Mathematics and Applications, Susanna S. Epp, Brooks, 4th Edt., 2011".**

Spring 2024

Introduction to Proofs

- A proof is a valid argument that establishes the truth of a mathematical statement.
- A proof can use the hypotheses of the theorem, if any, axioms assumed to be true, and previously proven theorems. Using these ingredients and rules of inference, the final step of the proof establishes the truth of the statement being proved.
- The arguments (as been considered before)to show that statements involving propositions and quantified statements are true were formal proofs, where all steps were supplied, and the rules for each step in the argument were given.
- However, formal proofs of useful theorems can be extremely long and hard to follow. In practice, the proofs of theorems designed for human consumption are almost always informal proofs, where more than one rule of inference may be used in each step, where steps may be skipped, where the axioms being assumed and the rules of inference used are not explicitly stated.
- Informal proofs can often explain to humans why theorems are true, while computers are perfectly happy producing formal proofs using automated reasoning systems.
- Understanding the techniques used in proofs is essential both in mathematics and in computer science
- Formally, a **theorem is a statement that can be shown to be true.**
- Less important theorems sometimes are called **propositions.**
- A proof is 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**
- A less important theorem that is helpful in the proof of other results is called a **lemma**
- A **corollary is a** theorem that can be established directly from a theorem that has been proved.
- **A conjecture is** a statement that is being proposed to be a true statement, usually on the basis of some partial evidence, a heuristic argument, or the intuition of an expert.

- Many theorems assert that a property holds for all elements in a domain, such as the integers or the real numbers. Although the precise statement of such theorems needs to include a universal quantifier, the standard convention in mathematics is to omit it. For example, the statement

  If $x>y$, where x and y are positive real numbers, then $x^2>y^2$.

  really means

  For all positive real numbers x and y, if $x>y$, then $x^2>y^2$.

Proving Methods

To prove a theorem of the form $\forall x(P(x) \rightarrow Q(x))$, *our goal is to show that* $P(c) \rightarrow Q(c)$ is true, where *c is an arbitrary element of the domain, and then apply universal generalization.* In this proof, we need to show that a conditional statement is true. Because of this, we now focus on methods that show that conditional statements are true. Recall that $p \rightarrow q$ *is true unless p is* true but *q is false. Note that to prove the statement* $p \rightarrow q$, *we need only show that q is true if p* is true.

Direct Proof:

•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, so that the combination p true and q false never occurs. 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.

•You will find that direct proofs of many results are quite straightforward, with a fairly obvious sequence of steps leading from the hypothesis to the conclusion. However, direct proofs sometimes require particular insights and can be quite tricky.

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.*

Ex. 1(83): Give a direct proof of the theorem "If *n is an odd integer, then* n^2 *is odd."*
Solution:

Ex. 2(83): Give a direct proof that if m and n are both perfect squares, then nm is also a perfect square.
(An integer a is a perfect square if there is an integer b such that $a = b^2$.)
Solution:

Proof by Contraposition:

•Direct proofs lead from the premises of a theorem to the conclusion.
•They begin with the premises, continue with a sequence of deductions, and end with the conclusion. However, we will see that attempts at direct proofs often reach dead ends.
•We need other methods of proving 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 proofs.
•An extremely useful type of indirect proof is known as proof by contraposition.
•Proofs by contraposition make use of the fact that the conditional statement $p \rightarrow q$ *is equivalent to its* contrapositive, $\neg q \rightarrow \neg p$. *This means that the conditional statement* $p \rightarrow q$ *can be proved by* showing that its contrapositive, $\neg q \rightarrow \neg p$, *is true. In a proof by contraposition of* $p \rightarrow q$, *we* take $\neg q$ *as a premise, and using axioms, definitions, and previously proven theorems, together* with rules of inference, we show that $\neg p$ *must follow.*

Ex. 3(83): Prove that if *n is an integer and 3n + 2 is odd, then n is odd.*
Solution:

Ex. 4(84):

Prove that if $n = ab$, where a and b are positive integers, then $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Solution:

VACUOUS AND TRIVIAL PROOFS:

- We can quickly prove that a conditional statement $p \rightarrow q$ *is true when we know that p is false, because* $p \rightarrow q$ *must be true when p is false.*
- Consequently, if we can show that *p is false, then we have a proof, called a* ***vacuous proof, of*** the conditional statement $p \rightarrow q$.
- *Vacuous proofs are often used to establish special cases of* theorems that state that a conditional statement is true for all positive integers

Ex. 5(84):

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.

Solution:

✓ We can also quickly prove a conditional statement $p \rightarrow q$ *if we know that the conclusion q is true. By showing that q is true, it follows that* $p \rightarrow q$ *must also be true. A proof of* $p \rightarrow q$ that uses the fact that *q is true is called a trivial proof. Trivial proofs are often important when* special cases of theorems are proved

Ex. 6(85):

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.

Solution:

Definition: The real number *r is rational if there exist integers p and q with q = 0 such that r = p/q.*
A real number that is not rational is called *irrational.*

Ex. 7(85): Prove that the sum of two rational numbers is rational. (Note that if we include the implicit quantifiers here, the theorem we want to prove is "For every real number *r and every real* number *s, if r and s are rational numbers, then r + s is rational.)*
Solution:

Ex. 8(85):

Prove that if n is an integer and n^2 is odd, then n is odd.

Solution:

Proofs by Contradiction

• Because the statement *$r \wedge \neg r$ is a contradiction whenever r is a proposition, we can prove* that *p is true if we can show that $\neg p \rightarrow (r \wedge \neg r)$ is true for some proposition r. Proofs of this* type are called **proofs by contradiction.**

• Because a proof by contradiction does not prove a result directly, it is another type of indirect proof.

• Suppose we want to prove that a statement *p is true. Furthermore, suppose that we can find* a contradiction *q such that $\neg p \rightarrow q$ is true. Because q is false, but $\neg p \rightarrow q$ is true, we can* conclude that *$\neg p$ is false, which means that p is true.*

Ex. 9(86): Show that at least four of any 22 days must fall on the same day of the week.
Solution:

Ex. 10(86):Prove that $\sqrt{2}$ is irrational by giving a proof by contradiction.
Solution:

Note that,

• Proof by contradiction can be used to prove conditional statements. In such proofs, we first assume the negation of the conclusion. We then use the premises of the theorem and the negation of the conclusion to arrive at a contradiction. (Both of the statements $p \rightarrow q$ and $(p \wedge \neg q) \rightarrow F$ are logically equivalance)

• Note that we can rewrite a proof by contraposition of a conditional statement as a proof by contradiction. In a proof of *p → q by contraposition, we assume that ¬q is true. We then* show that *¬p must also be true. To rewrite a proof by contraposition of p → q as a proof by* contradiction, we suppose that both *p and ¬q are true. Then, we use the steps from the proof* of *¬q → ¬p to show that ¬p is true. This leads to the contradiction p ∧¬p, completing the* proof. Example 11 illustrates how a proof by contraposition of a conditional statement can be rewritten as a proof by contradiction.

Ex. 11(87): Give a proof by contradiction of the theorem "If $3n + 2$ *is odd, then n is odd.*"
Solution:

• Note also that, we can also prove by contradiction that *p → q is true by assuming that p and ¬q are true, and showing that q must be also be true. This implies that ¬q and q are both* true, a contradiction. This observation tells us that we can turn a direct proof into a proof by contradiction.

PROOFS OF EQUIVALENCE

To prove a theorem that is a biconditional statement, that is, a statement of the form *p ↔ q, we show that p → q and q → p are both true. The validity of* this approach is based on the tautology

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

Ex. 12(87): Prove the theorem "If n is an integer, then n is odd if and only if n^2 is odd."

Solution:

Ex. 13(87): 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.

Solution:

COUNTER EXAMPLES

If we want to show that a statement of the form $\forall x P(x)$ *is false, we need only find a counterexample, that is, an example x for which P(x)* is false. When presented with a statement of the form $\forall x P(x)$*, which we believe to be false or* which has resisted all proof attempts, we look for a counterexample.

Ex. 14(88): Show that the statement "Every positive integer is the sum of the squares of two integers" is false.
Solution:

Ex. 15(88): What is wrong with this famous supposed "proof" that 1 = 2?
Solution:

Ex. 16(88): What is wrong with this "proof?"

"Theorem:" If n^2 is positive, then n is positive.

Solution:

Proof Methods and Strategy

In the previous chapter, we provided many methods and related examples. Now, we will present other familiar proof methods. Moreover, we will discuss the strategy behind the constructive(construction the argument step by step) proof.

Exhaustive Proof and Proof by Cases:

• Sometimes we cannot prove a theorem using a single argument that holds for all possible cases. We now introduce a method that can be used to prove a theorem, by considering different cases seperately.

• This method is based on a rule of inference that we will now introduce. To prove a conditional statement of the form $(p_1 \vee p_2 \vee \cdots \vee p_n) \rightarrow q$ the tautology

$$[(p_1 \vee p_2 \vee \cdots \vee p_n) \rightarrow q] \leftrightarrow [(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \cdots \wedge (p_n \rightarrow q)]$$

can be used as a rule of inference.

• This shows that the original conditional statement with a hypothesis made up of a disjunction of the propositions $p_1, p_2, \ldots, p_n$ *can be proved by* proving each of the *n conditional statements* $p_i \rightarrow q$, $i = 1, 2, \ldots, n$, *individually. Such an* argument is called a proof by cases.

Exhaustive(kapsamlı, ayrıntılı) Proof: Some theorems can be proved by examining a relatively small number of examples. Such proofs are called exhaustive proofs, or proofs by exhaustion because these proofs proceed by exhausting all possibilities. An exhaustive proof is a special type of proof by cases where each case involves checking a single example.

Ex. 1(93): Prove that $(n+1)^3 \geq 3^n$ if n is a positive integer with $n \leq 4$.
Solution:

Ex. 2(93): Prove that the only consecutive positive integers not exceeding 100 that are perfect powers are 8 and 9. (An integer is a perfect power if it equals n^a, *where a is an integer greater than 1.)*
Solution:

Note that, People can carry out exhaustive proofs when it is necessary to check only a relatively small number of instances of a statement. Computers do not complain when they are asked to check a much larger number of instances of a statement, but they still have limitations. Note that not even a computer can check all instances when it is impossible to list all instances to check.

PROOF BY CASES: A proof by cases must cover all possible cases that arise in a theorem. We illustrate proof by cases with a couple of examples. In each example, you should check that all possible cases are covered.

Ex. 3(93): Prove that if n is an integer, then $n^2 \geq n$.

Solution:

Ex. 4(94):
Use a proof by cases to show that $|xy| = |x||y|$, where x and y are real numbers. (Recall that $|a|$, the absolute value of a, equals a when $a \geq 0$ and equals $-a$ when $a \leq 0$.)

Solution:

LEVERAGING PROOF BY CASES: In particular, when it is not possible to consider all cases of a proof at the same time, a proof by cases should be considered. Generally, look for a proof by cases when there is no obvious way to begin a proof, but when extra information in each case helps move the proof forward.

Ex. 5(94): Formulate a conjecture about the final decimal digit of the square of an integer and prove your result.
Solution:

Ex. 6(95):
Show that there are no solutions in integers x and y of $x^2 + 3y^2 = 8$.

Solution:

WITHOUT LOSS OF GENERALITY:
•In general, when the phrase "without loss of generality" is used in a proof (often abbreviated as WLOG), we assert that by proving one case of a theorem, no additional argument is required to prove other specified cases.

•In the proof in Example 4, we dismissed case *(iii),*where *x < 0 and y ≥ 0, because it is the same as case (ii), where x ≥ 0 and y < 0, with the* roles of *x and y reversed. To shorten the proof, we could have proved cases (ii) and (iii) together* by assuming, without loss of generality, that *x ≥ 0 and y < 0. Implicit in this statement is that* we can complete the case with *x < 0 and y ≥ 0 using the same argument as we used for the* case with *x ≥ 0 and y < 0, but with the obvious changes.*

•incorrect use of WLOG can lead to unfortunate errors.

Ex. 7(95): Show that if *x and y are integers and both xy and x + y are even, then both x and y are even.*
Solution:

Common Error with Exhaustive Proof and Proof by Cases: The problem of proving a theorem is analogous to showing that a computer program always produces the output desired. No matter how many input values are tested, unless all input values are tested, we cannot conclude that the program always produces the correct output.

Ex. 8(96): Is it true that every positive integer is the sum of 18 fourth powers of integers?
Solution:

Existence Proofs

A proof of a proposition of the form ∃xP(x) is called an **existence proof.** There are several ways to prove a theorem of this type. Sometimes an existence proof of ∃xP(x) can be given by finding an element a, called a **witness,** such that P(a) is true. This type of existence proof is called **constructive.** It is also possible to give an existence proof that is **nonconstructive;** that is, we do not find an element a such that P(a) is true, but rather prove that ∃xP(x) is true in some other way. One common method of giving a nonconstructive existence proof is to use proof by contradiction and show that the negation of the existential quantification implies a contradiction

Ex. 10(96): A Constructive Existence Proof Show that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways.
Solution:

Ex. 11(96): A Nonconstructive Existence Proof Show that there exist irrational numbers *x and y such* that *x^y is rational*.
Solution:

Uniqueness Proofs:
Some theorems assert the existence of a unique element with a particular property.
These theorems assert that there is exactly one element with this property.
To prove a statement of this type we need to show that an element with this property exists and that no other element has this property.
The two parts of a uniqueness proof are the "Existence" and "Uniqueness". Existence needs to show that an element x with the desired property exists. Besides that, uniqueness is to show that if y = x, then y does not have the desired property. Namely, if we can show that if x and y both have the desired property, then x = y.

Ex. 13(100): Show that if *a and b are real numbers and a = 0, then there is a unique real number r such that ar + b = 0.*
Solution:

Proof Strategies:

• When you are confronted with a statement to prove, you should first replace terms by their definitions and then carefully analyze what the hypotheses and the conclusion mean.

• After doing so, you can attempt to prove the result using one of the available methods of proof.

• Generally, if the statement is a conditional statement, you should first try a direct proof; if this fails, you can try an indirect proof. If neither of these approaches works, you might try a proof by contradiction.

FORWARD REASONING: To begin a direct proof of a conditional statement, you start with the premises. Using these premises, together with axioms and known theorems, you can construct a proof using a sequence of steps that leads to the conclusion. This type of reasoning, called *forward reasoning, is the most common type of reasoning used to prove relatively simple* results. Similarly, with indirect reasoning you can start with the negation of the conclusion and, using a sequence of steps, obtain the negation of the premises.

BACKWARD REASONING: Unfortunately, forward reasoning is often difficult to use to prove more complicated results, because the reasoning needed to reach the desired conclusion may be far from obvious. In such cases it may be helpful to use *backward reasoning. To reason backward to prove a statement q,* we find a statement *p that we can prove with the property that p → q.*

Ex. 14(100):

Given two positive real numbers x and y, their **arithmetic mean** is $(x + y)/2$ and their **geometric mean** is $\sqrt{xy}$. When we compare the arithmetic and geometric means of pairs of distinct positive real numbers, we find that the arithmetic mean is always greater than the geometric mean. [For example, when $x = 4$ and $y = 6$, we have $5 = (4 + 6)/2 > \sqrt{4 \cdot 6} = \sqrt{24}$.] Can we prove that this inequality is always true?

Solution:

Look for Counterexample: When confronted with a conjecture, you might first try to prove this conjecture, and if your attempts are unsuccessful, you might try to find a counterexample, first by looking at the simplest, smallest examples. If you cannot find a counterexample, you might again try to prove the statement.

Ex. 17(102): is the statement "Every positive integer is the sum of the squares of three integers" true or false?

Solution: