Discrete Mathematics

CMP-200

Lecture 7

Abdul Hameed

http://informationtechnology.pk/pucit

abdul.hameed@pucit.edu.pk

Mistakes in Proofs

- The most common errors are mistakes in arithmetic and basic algebra.
- Even professional mathematicians make such errors, especially when working with complicated formulae
- Whenever you use such computations you should check them as carefully as possible.

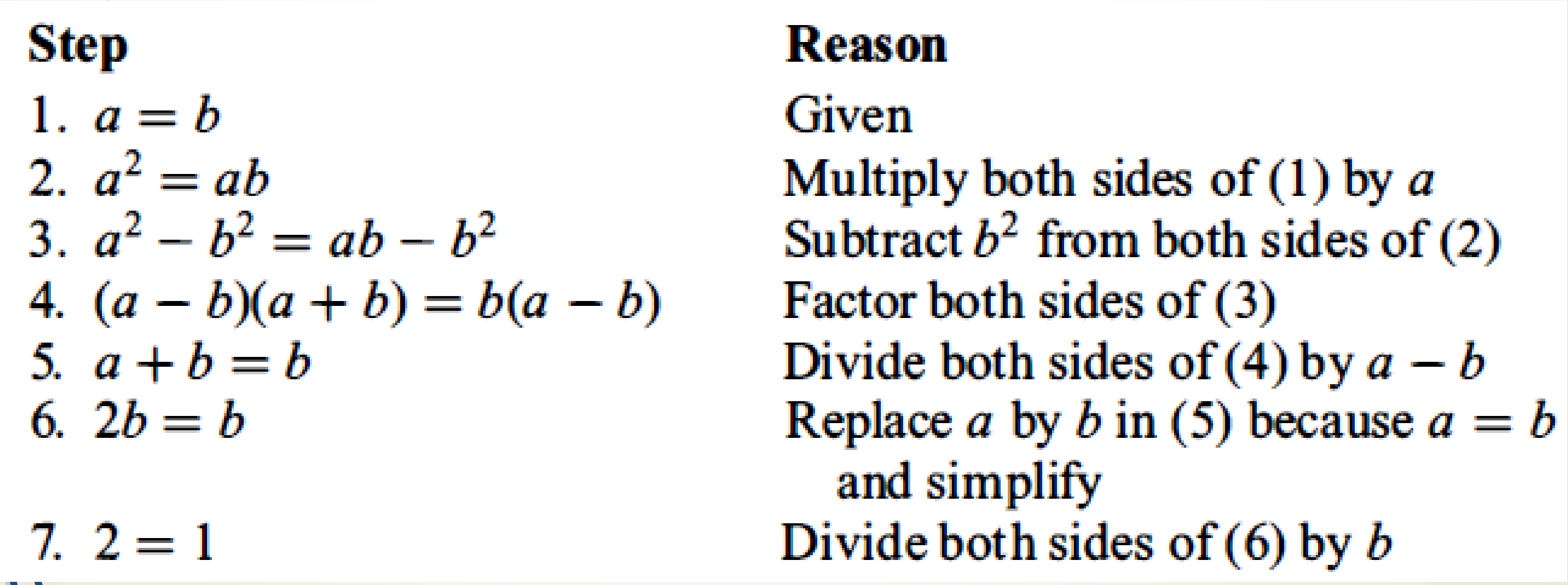
Mistakes in Proofs

- Each step of a mathematical proof needs to be correct and the conclusion needs to follow logically from the steps that precede it.

- Many mistakes result from the introduction of steps that do not logically follow from those that precede it.

Exercise

- What is wrong with this famous supposed "proof" that 1 = 2?



Step	Reason
1. $a = b$	Given
2. $a^2 = ab$	Multiply both sides of (1) by a
3. $a^2 - b^2 = ab - b^2$	Subtract b^2 from both sides of (2)
4. $(a - b)(a + b) = b(a - b)$	Factor both sides of (3)
5. $a + b = b$	Divide both sides of (4) by $a - b$
6. $2b = b$	Replace a by b in (5) because $a = b$ and simplify
7. $2 = 1$	Divide both sides of (6) by b

Solution

- Every step is valid except for one, step 5 where we divided both sides by a - b.

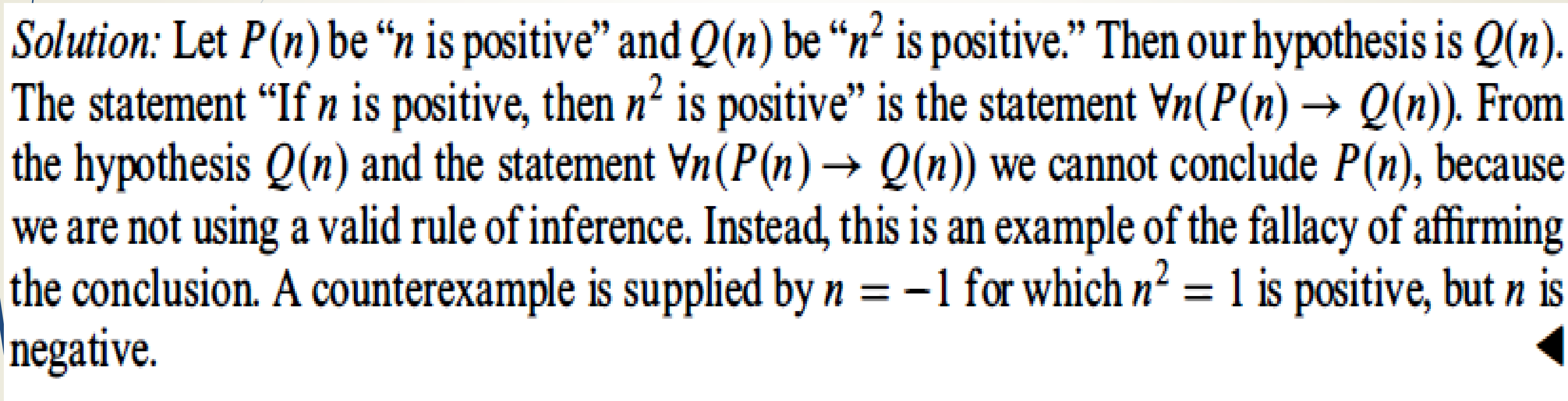
- The error is that a - b equals zero; division of both sides of an equation by the same quantity is valid as long as this quantity is not zero.

What is wrong with this "proof" ?

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

"Proof:" Suppose that n^2 is positive. Because the conditional statement "If n is positive, then n^2 is positive" is true, we can conclude that n is positive.

Solution

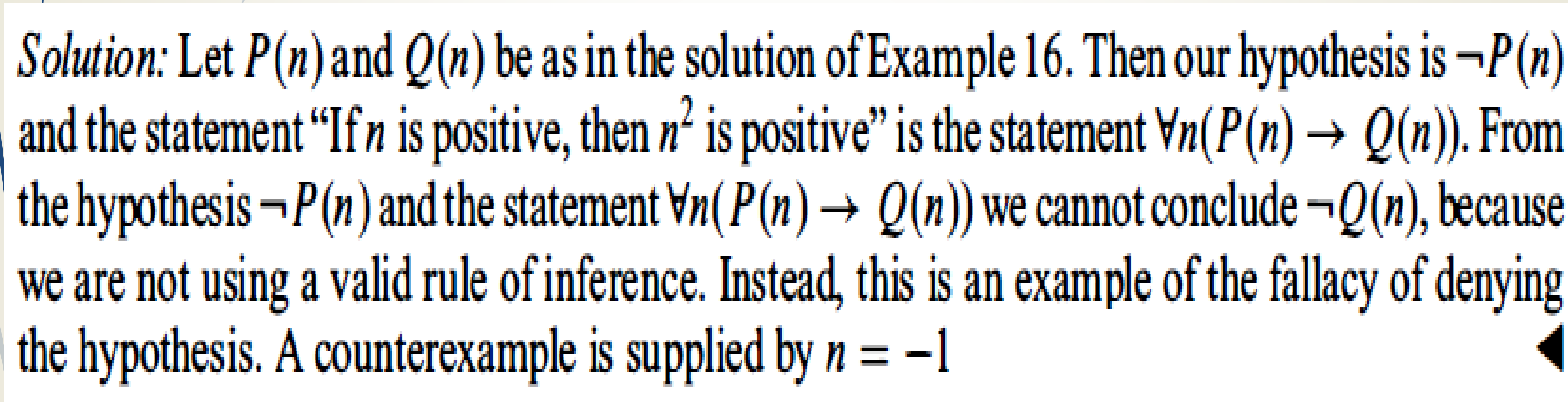


Solution: Let $P(n)$ be "n is positive" and $Q(n)$ be "n^2 is positive." Then our hypothesis is $Q(n)$. The statement "If n is positive, then n^2 is positive" is the statement $\forall n(P(n) \rightarrow Q(n))$. From the hypothesis $Q(n)$ and the statement $\forall n(P(n) \rightarrow Q(n))$ we cannot conclude $P(n)$, because we are not using a valid rule of inference. Instead, this is an example of the fallacy of affirming the conclusion. A counterexample is supplied by $n = -1$ for which $n^2 = 1$ is positive, but n is negative. ◀

What is wrong with this "proof" ? "Theorem:" If n is not positive, then n^2 is not positive.

- "Proof:" Suppose that n is not positive. Because the conditional statement "If n is positive, then n^2 is positive" is true, we can conclude that n^2 is not positive.

Solution



Solution: Let $P(n)$ and $Q(n)$ be as in the solution of Example 16. Then our hypothesis is $\neg P(n)$ and the statement "If n is positive, then n^2 is positive" is the statement $\forall n(P(n) \rightarrow Q(n))$. From the hypothesis $\neg P(n)$ and the statement $\forall n(P(n) \rightarrow Q(n))$ we cannot conclude $\neg Q(n)$, because we are not using a valid rule of inference. Instead, this is an example of the fallacy of denying the hypothesis. A counterexample is supplied by $n = -1$ ◀

Begging the question

- Many incorrect arguments are based on a fallacy called **Begging the question**. This fallacy occurs when one or more steps of a proof are based on the truth of the statement being proved.

- In other words, this fallacy arises when a statement is proved using itself, or a statement equivalent to it. That is why this fallacy is also called **circular reasoning.**

Example

- Is the following argument correct?
- It supposedly shows that n is an even integer whenever n^2 is an even integer. Suppose that n^2 is even. Then $n^2 = 2k$ for some integer k. Let $n = 2l$ for some integer l. This shows that n is even.

Solution

- This argument is incorrect. The statement "let n = 2*l* for some integer *l*" occurs in the proof. No argument has been given to show that n can be written as 2*l* for some integer *l*. This is circular reasoning because this statement is equivalent to the statement being proved, namely, "n is even." Of course, the result itself is correct; only the method of proof is wrong

Word of Caution

- Making mistakes in proofs is part of the learning process.
- When you make a mistake that someone else finds, you should carefully analyze where you went wrong and make sure that you do not make the same mistake again.
- Even professional mathematicians make mistakes in proofs.
- More than a few incorrect proofs of important results have fooled people for many years before subtle errors in them were found

Proof Methods and Strategy

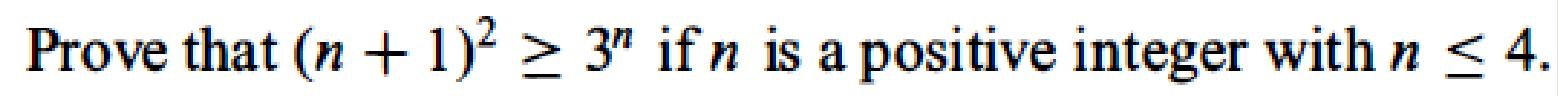
Section 1.7

Section Summary

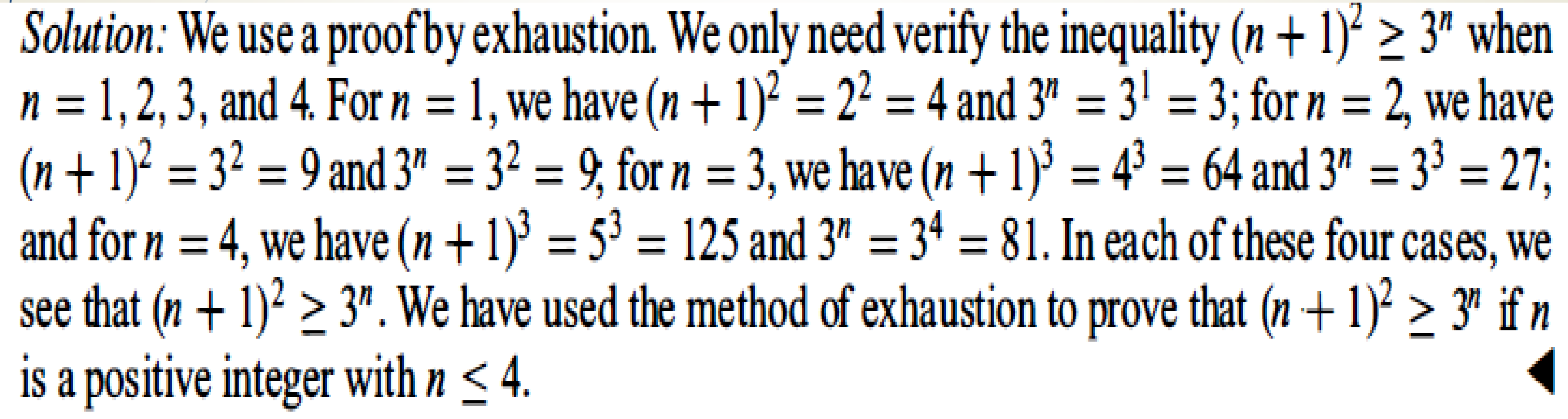
- Exhaustive proof
- Proof by Cases
- Existence Proofs
  - Constructive
  - Nonconstructive
- Disproof by Counterexample
- Nonexistence Proofs
- Uniqueness Proofs
- Proof Strategies

Example

- Some theorems can be proved by examining a relatively small number of examples. Such proofs are called exhaustive proofs, 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.



Prove that $(n+1)^2 \geq 3^n$ if n is a positive integer with $n \leq 4$.



Solution: We use a proof by exhaustion. We only need verify the inequality $(n+1)^2 \geq 3^n$ when $n = 1, 2, 3,$ and 4. For $n = 1$, we have $(n+1)^2 = 2^2 = 4$ and $3^n = 3^1 = 3$; for $n = 2$, we have $(n+1)^2 = 3^2 = 9$ and $3^n = 3^2 = 9$; for $n = 3$, we have $(n+1)^3 = 4^3 = 64$ and $3^n = 3^3 = 27$; and for $n = 4$, we have $(n+1)^3 = 5^3 = 125$ and $3^n = 3^4 = 81$. In each of these four cases, we see that $(n+1)^2 \geq 3^n$. We have used the method of exhaustion to prove that $(n+1)^2 \geq 3^n$ if n is a positive integer with $n \leq 4$. ◀

Example

- 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)

- We can prove this fact by showing that the only pair n, n + 1 of consecutive positive integers that are both perfect powers with $n < 100$ arises when $n = 8$

Example

- We can prove this fact by examining positive integers n not exceeding 100, first checking whether n is a perfect power, and if it is, checking whether n + 1 is also a perfect power.
- A quicker way to do this is simply to look at all perfect powers not exceeding 100 and checking whether the next largest integer is also a perfect power.

Example

- The squares of positive integers not exceeding 100 are 1,4,9,16,25,36,49,64,81, and 100.A quicker way to do this is simply to look at all perfect powers not exceeding 100 and checking whether the next largest integer is also a perfect power.
- The cubes of positive integers not exceeding 100 are 1,8, 27, and 64.
- The fourth powers of positive integers not exceeding 100 are 1, 16, and 81.

Example

- The fifth powers of positive integers not exceeding 100 are 1 and 32.
- The sixth powers of positive integers not exceeding 100 are 1 and 64.
- There are no powers of positive integers higher than the sixth power not exceeding 1 00, other than 1 .

Example

- Looking at this list of perfect powers not exceeding 100, we see that n = 8 is the only perfect power n for which n + 1 is also a perfect power. That is, $2^3 = 8$ and $3^2 = 9$ are the only two consecutive perfect powers not exceeding 1 00.

Proof by Cases

- To prove a conditional statement of the form:

$$(p_1 \vee p_2 \vee \ldots \vee p_n) \to q$$

- Use the tautology

$$\begin{aligned}&[(p_1 \vee p_2 \vee \ldots \vee p_n) \to q] \leftrightarrow \\ &\quad [(p_1 \to q) \wedge (p_2 \to q) \wedge \ldots \wedge (p_n \to q)]\end{aligned}$$

- Each of the implications $p_i \to q$ is a *case*.

Proof by Cases

Example: Let a @ b = max{a, b} = a if $a \geq b$, otherwise a @ b = max{a, b} = b.

Show that for all real numbers a, b, c

(a @b) @ c = a @ (b @ c)

(This means the operation @ is associative.)

Proof: Let a, b, and c be arbitrary real numbers.

Then one of the following 6 cases must hold.

1. $a \geq b \geq c$
2. $a \geq c \geq b$
3. $b \geq a \geq c$
4. $b \geq c \geq a$
5. $c \geq a \geq b$
6. $c \geq b \geq a$

Proof by Cases

Case 1: $a \geq b \geq c$

$(a @ b) = a, a @ c = a, b @ c = b$

Hence $(a @ b) @ c = a = a @ (b @ c)$

Therefore the equality holds for the first case.

A complete proof requires that the equality be shown to hold for all 6 cases. But the proofs of the remaining cases are similar. Try them.

Existence Proofs

- Proof of theorems of the form $\exists x P(x)$.
- **Constructive** existence proof:
  - Find an explicit value of *c*, for which *P(c)* is true.
  - Then $\exists x P(x)$ is true by Existential Generalization (EG).

Example: Show that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways:

Proof: 1729 is such a number since

$$1729 = 10^3 + 9^3 = 12^3 + 1^3$$

◀

Nonconstructive Existence Proofs

- In a *nonconstructive* existence proof, we assume no *c* exists which makes *P(c)* true and derive a contradiction.

Example: Show that there exist irrational numbers *x* and *y* such that x^y is rational.

Proof: We know that √2 is irrational. Consider the number $\sqrt{2}^{\sqrt{2}}$. If it is rational, we have two irrational numbers x and y with x^y rational, namely $x = \sqrt{2}$ and $y = \sqrt{2}$. But if $\sqrt{2}^{\sqrt{2}}$ is irrational, then we can let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$ so that

$$x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2}\sqrt{2})} = \sqrt{2}^{2} = 2.$$

◀

Counterexamples

- Recall $\exists x \neg P(x) \equiv \neg \forall x P(x)$
- To establish that $\neg \forall x P(x)$ is true (or $\forall x P(x)$ is false) find a *c* such that $\neg P(c)$ is true or $P(c)$ is false.
- In this case *c* is called a *counterexample* to the assertion $\forall x P(x)$.

Example: "Every positive integer is the sum of the squares of 3 integers." The integer 7 is a counterexample. So the claim is false.

Uniqueness Proofs

- Some theorems asset the existence of a unique element with a particular property, $\exists! x\, P(x)$. The two parts of a *uniqueness proof* are
  - *Existence*: We show that an element x with the property exists.
  - *Uniqueness*: We show that if $y \neq x$, then y does not have the property.

Example: Show that if a and b are real numbers and $a \neq 0$, then there is a unique real number r such that $ar + b = 0$.

Solution:

- Existence: The real number $r = -b/a$ is a solution of $ar + b = 0$ because $a(-b/a) + b = -b + b = 0$.
- Uniqueness: Suppose that s is a real number such that $as + b = 0$. Then $ar + b = as + b$, where $r = -b/a$. Subtracting b from both sides and dividing by a shows that $r = s$.

Proof Strategies for proving $p \to q$

- Choose a method.
  1. First try a direct method of proof.
  2. If this does not work, try an indirect method (e.g., try to prove the contrapositive).
- For whichever method you are trying, choose a strategy.
  1. First try *forward reasoning*. Start with the axioms and known theorems and construct a sequence of steps that end in the conclusion. Start with p and prove q, or start with $\neg q$ and prove $\neg p$.
  2. If this doesn't work, try *backward reasoning*. When trying to prove q, find a statement p that we can prove with the property $p \to q$.

Backward Reasoning

Example: Suppose that two people play a game taking turns removing, 1, 2, or 3 stones at a time from a pile that begins with 15 stones. The person who removes the last stone wins the game. Show that the first player can win the game no matter what the second player does.

Proof: Let *n* be the last step of the game.

Step n: Player$_1$ can win if the pile contains 1,2, or 3 stones.

Step n-1: Player$_2$ will have to leave such a pile if the pile that he/she is faced with has 4 stones.

Step n-2: Player$_1$ can leave 4 stones when there are 5,6, or 7 stones left at the beginning of his/her turn.

Step n-3: Player$_2$ must leave such a pile, if there are 8 stones .

Step n-4: Player$_1$ has to have a pile with 9,10, or 11 stones to ensure that there are 8 left.

Step n-5: Player$_2$ needs to be faced with 12 stones to be forced to leave 9,10, or 11.

Step n-6: Player$_1$ can leave 12 stones by removing 3 stones.

Now reasoning forward, the first player can ensure a win by removing 3 stones and leaving 12.