CS 2305: Discrete Mathematics for Computing I

Lecture 12

- KP Bhat

Mistakes in Proofs

- There are many errors made in constructing mathematical proofs. Some of the common errors are:
  - performing a disallowed mathematical operation (e.g. division by 0)
  - given $p \rightarrow q$ is true and q is true implying the conclusion that p is true (**fallacy of affirming the conclusion**)
  - given $p \rightarrow q$ is true and p is false implying the conclusion that q is false (**fallacy of denying the hypothesis**)
  - basing one or more steps of the proof on the truth of the statement being proved, or a statement equivalent to it (**begging the question** or **circular reasoning**)

What is wrong with this?

"Proof" that *1 = 2*

Step	**Reason**
1. $a = b$	Premise
2. $a^2 = a \times b$	Multiply both sides of (1) by a
3. $a^2 - b^2 = a \times b - b^2$	Subtract b^2 from both sides of (2)
4. $(a-b)(a+b) = b(a-b)$	Algebra on (3)
5. $a + b = b$	Divide both sides by $a - b$
6. $2b = b$	Replace a by b in (5) because $a = b$
7. $2 = 1$	Divide both sides of (6) by b

Solution: Step 5. a - b = 0 by the premise and division by 0 is undefined.

Looking Ahead

If direct methods of proof do not work

- We may need a clever use of a proof by contraposition.
- Or a proof by contradiction.
- In the next section, we will see strategies that can be used when straightforward approaches do not work.
- In Chapter 5, we will see mathematical induction and related techniques.
- In Chapter 6, we will see combinatorial proofs

Self Study: Mistakes in Proof

- Section 1.7, Example 17
- Section 1.7, Example 18
- Section 1.7, Example 19

Proof Methods and Strategy

Section 1.8

Proof by Exhaustion

- Used in situations where theorems can be proved by examining a relatively small number of examples

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

  Solution:

  Case n = 1: $(1 + 1)^3 = 2^3 = 8$, which is $\geq 3^1$ i.e. 3

  Case n = 2: $(2 + 1)^3 = 3^3 = 27$, which is $\geq 3^2$ i.e. 9

  Case n = 3: $(3 + 1)^3 = 4^3 = 64$, which is $\geq 3^3$ i.e. 27

  Case n = 4: $(4 + 1)^3 = 5^3 = 125$, which is $\geq 3^4$ i.e. 81

  QED

Self Study: Proof by Exhaustion

- Section 1.8, Example 2

Proof by Cases 1

- Used in situations where:
  - the proof needs to consider different cases and the theorem can be proved for each different case separately
  - the number of cases to consider often makes proof by exhaustion impractical

Proof by Cases 2

To prove a conditional statement of the form:

$$\left(p_1 \vee p_2 \vee \ldots \vee p_n\right) \rightarrow q$$

Use the tautology

$$\left[\left(p_1 \vee p_2 \vee \ldots \vee p_n\right) \rightarrow q\right] \leftrightarrow$$

$$\left[\left(p_1 \rightarrow q\right) \wedge \left(p_2 \rightarrow q\right) \wedge \ldots \wedge \left(p_n \rightarrow q\right)\right]$$

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

$(p_1 \vee p_2) \rightarrow q$	
$\neg(p_1 \vee p_2) \vee q$	Logical Equivalence
$(\neg p_1 \wedge \neg p_2) \vee q$	De Morgan's Law
$q \vee (\neg p_1 \wedge \neg p_2)$	Commutative Law
$(q \vee \neg p_1) \wedge (q \vee \neg p_2)$	Distributive Law
$(\neg p_1 \vee q) \wedge (\neg p_2 \vee q)$	Commutative Law
$(p_1 \rightarrow q) \wedge (p_2 \rightarrow q)$	Logical Equivalence

Proof by Cases 3

Example 1: Prove that if *n* is an integer, then $n^2 \geq n$.
Solution:
Case 1 (n = 0): $0^2 = 0$, so $n^2 \geq n$ holds

Case 2 ($n \geq 1$): Multiply both sides by n
$n * n \geq 1 * n$ or $n^2 \geq n$

Case 3 ($n \leq -1$): We know that $n^2 \geq 0$
n is a –ve number and n^2 is a +ve number
$\therefore n^2 \geq n$

Since the inequality $n^2 \geq n$ holds in all three cases, we can conclude that if n is an integer, then $n^2 \geq n$.

QED

Proof by Cases 4

Example 2: Prove that the final decimal digit of a perfect square is 0, 1, 4, 5, 6, or 9

Solution:

We first note that the final digit of the perfect square of a number depends upon the final digit of the number alone.

To focus on the final digit alone, we express the number in the "quotient & modulo" form i.e. 10a + b, where a is the quotient and b is the modulus of division by 10. Clearly b, the final digit of n, is 0, 1, 2, 3, 4, 5, 6, 7, 8, or 9

Now $n^2 = (10a + b)^2 = 100a^2 + 20ab + b^2$

$n^2 = 10(10a^2 + 2ab) + b^2$

Although the RHS is not strictly in "quotient & modulo" form (since for $b > 3$ b^2 overflows the units place), the final digit of n^2 is the same as the final digit of b^2

To see how many possible cases there are for the final digit of b^2 we notice that

$(10-b)^2 = 100 - 20b + b^2 = 10(10 – 2b) + b^2$

Again the RHS is not strictly in "quotient & modulo" form but we can see that the final digit of b^2 is the same as the final digit of $(10-b)^2$

Continued on next slide →

Proof by Cases 5

Solution (Cont'd):

Since the final digit of b^2 is the same as the final digit of $(10-b)^2$, we can lump all {b, 10-b} pairs in the same category, as their squares yield the same final digit.

So we need to consider the following cases:

Case 1 (final digit b is 1 or 10-1 i.e. 9): In this case b^2 ends with 1 so n^2 ends with 1
Case 2 (final digit b is 2 or 10-2 i.e. 8): In this case b^2 ends with 4 so n^2 ends with 4
Case 3 (final digit b is 3 or 10-3 i.e. 7): In this case b^2 ends with 9 so n^2 ends with 9
Case 4 (final digit b is 4 or 10-4 i.e. 6): In this case b^2 ends with 6 so n^2 ends with 6
Case 5 (final digit b is 5 or 10-5 i.e. 5): In this case b^2 ends with 5 so n^2 ends with 5
Case 6 (final digit b is 0): In this case b^2 ends with 0 so n^2 ends with 0

Because we have considered all six cases, we can conclude that the final decimal digit of n^2, where n is an integer, is either 0, 1, 2, 4, 5, 6, or 9.

QED

Without Loss of Generality (1)

- The phrase “Without Loss of Generality” (WLOG) is used in proofs with cases to assert that by proving one case of a theorem, no additional argument is required to prove other specified cases
  - other cases follow by making straightforward changes to the argument

Without Loss of Generality (2)

Example: Prove by contraposition that if *x* and *y* are integers and both *x·y and x+y* are even, then both *x* and *y* are even.

Proof:

We are required to prove that:

(EVEN(x*y) ∧ EVEN (x+y)) → (EVEN(x) ∧ EVEN (y))

The contrapositive of this claim is:

¬(EVEN(x) ∧ EVEN (y)) → ¬(EVEN(x*y) ∧ EVEN (x+y))

By De Morgan's Law (ODD(x) ∨ ODD (y)) → (ODD(x*y) ∨ ODD (x+y))

The premise requires that between x and y one or both are odd. **Without loss of generality**, assume that *x* is odd. Then $x = 2m + 1$ for some integer *m*.

We need to consider two cases here.

Case 1: *y* is even. Then $y = 2n$ for some integer *n*, so
$x + y = (2m + 1) + 2n = 2(m + n) + 1$ is odd.
[No need to evaluate x*y case since x+y is already odd]

Case 2: *y* is odd. Then $y = 2n + 1$ for some integer *n*, so
$x \cdot y = (2m + 1)(2n + 1) = 2(2m \cdot n + m + n) + 1$ is odd.
[No need to evaluate x+y case since x*y is already odd]

p

QED

Existence Proofs 1

- A proof of a proposition of the form $\exists x P(x)$ is called an existence proof
- Existence proofs come in two flavors:
  - Constructive: Finding an element a, called a witness, such that P(a) is true
  - Nonconstructive: Proving that $\exists x P(x)$ is true without finding the witness element e.g. by using proof by contradiction to show that the negation of the existential quantification implies a contradiction

Existence Proofs 2

Srinivasa Ramanujan

(1887-1920)

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

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

https://www.youtube.com/watch?v=LzjaDKVC4iY

QED

Note: This is an example of a constructive existence proof since we have found a witness element

Godfrey Harold Hardy

(1877-1947)

Existence Proofs 3

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

Proof:

We know that $\sqrt{2}$ is irrational. Let us consider the number $\sqrt{2}^{\sqrt{2}}$. There are two possibilities to consider.

Possibility 1: $\sqrt{2}^{\sqrt{2}}$ is rational

In this case $x = y = \sqrt{2}$ and x^y is rational

Possibility 2: $\sqrt{2}^{\sqrt{2}}$ is irrational

In this case let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$. Therefore $x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^2 = 2$, a rational number

QED

Note: This is an example of a nonconstructive existence proof. We don't know which of the two cases $\sqrt{2}^{\sqrt{2}}$ or $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}}$ has the desired property, but we have proved that one of them does!

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 $as + b = 0$.

$ar + b = as + b$

ar = as (subtracting b from both sides)

r = s (dividing both sides by $a \neq 0$)

QED

Counterexamples

Recall that $\exists x \neg P(x) \equiv \neg \forall x P(x)$

To establish that $\forall x P(x)$ is false

find a *c* such that *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."

Solution: The integer 7 is a counterexample. So the claim is false.

QED

Proof Strategies for proving $p \rightarrow q$

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*

Continued on next slide →

Backward Reasoning (1)

- In Backward Reasoning we first assume that the conclusion is true. We then try to derive some "secondary conclusion". Next we try to establish the veracity of the "secondary conclusion" through independent means. If we are able to do that, the "secondary conclusion" will become the starting point for our proof.

Continued on next slide →

Backward Reasoning (2)

Example: Prove that for any two distinct positive real numbers x and y, their arithmetic mean [i.e. $(x + y)/2$] is greater than their geometric mean [i.e. $\sqrt{(xy)}$]

Solution

We start by using backward reasoning to establish the **starting point** of our proof

Let us assume the conclusion is true

$(x + y)/2 > \sqrt{(xy)}$	
$(x + y)^2/4 > xy$	[Squaring both sides]
$(x + y)^2 > 4xy$	[Transposing]
$x^2 + 2xy + y^2 > 4xy$	[Expanding the $(x + y)^2$ formula]
$x^2 - 2xy + y^2 > 0$	[Subtracting 4xy from both sides]
$(x - y)^2 > 0$	[Using the $(x - y)^2$ formula]

Now that we have our secondary conclusion, let us see if we can prove it.

$(x - y)^2 > 0$ is indeed true for distinct positive real numbers since the square of any real number, whether +ve or –ve, is always +ve.

So $(x - y)^2 > 0$ will be the starting point for our formal proof

Continued on next slide →

Backward Reasoning (3)

Solution (Cont'd)

Now we move to our formal proof

Formal proof

$(x - y)^2 > 0$

$x^2 - 2xy + y^2 > 0$

$x^2 + 2xy + y^2 > 4xy$

$(x + y)^2 > 4xy$

$(x + y)^2/4 > xy$

$(x + y)/2 > \sqrt{(xy)}$