Mathematical proofs

Lecture 3

ICOM 4075

Basic mathematical objects

A mathematical object is simply any abstract object that arises in mathematics. Some commonly found mathematical objects are:

- Numbers
- Sequences
- Relations, functions, operations

among many others

Georg Cantor (1845 – 1918) showed that all mathematical objects can be expressed as sets. His work made **sets** the basic mathematical object and **set theory** the fundamental theory of mathematics

The concept of set

Georg Cantor defined sets as:

"By set we mean any collection M into a whole of definite, distinct objects m (which are called the elements of M) of our perception or of our thoughts"

Two basic sets of numbers

We'll be mostly concerned with sets of numbers

First is the set of all **integers**, this is, the set

$$Z = \{ \ldots ,-3, -2, -1, 0, 1, 2, 3, \ldots \}$$

Another important set is the set of all **natural** numbers

$$N = \{0, 1, 2, 3, \ldots \}$$

Divisibility with integers

Definition: An integer $n \neq 0$ **divides** an integer m if there is an integer k such that $n \cdot k = m$

Examples:

- 3 divides 15 since there is k = 5 such that $5 \cdot 3 = 15$
- 3 does not divides 14 since for no integer k, $k \cdot 3 = 14$
- 3 divides -3 since there is k = -1 such that $k \cdot 3 = -3$
- Does 13 divides 8 ?

  Is there an integer k such that $k \cdot 13 = 8$? **No**!
- Does 13 divides -104 ?

  Is there an integer k such that $k \cdot 13 = 104$? **Yes**, k = -8!

Even and Odd integers

An integer is said to be **even** if it is divisible by 2. The set of all even integers is described as:

E = { …, -4, -2, 0, 2, 4, … }

An integer that is not even is said to be **odd**. Thus, the set of odd numbers is the set of all integers that are not divisible by 2. This set is described as:

O = { …, -3, -1, 1, 3, … }

Prime numbers

A natural number is said to be **prime** if it can only be divided by 1 and by itself

This is, n is prime if it satisfies the following property:

P(n): "(For all integer k and for all integer m)

If k · m = n then (k = 1 and m = n) or (k = n and m = 1)"

Examples:

- 1, 2, 3 and 5 are all prime since P(1), P(2), P(3) and P(5) are all true
- 4 is not a prime since 2·2 = 4 **(this is, P(4) is false)**
- 6 is not a prime since 2·3 = 6 and 3·2 = 6 **(thus, P(6) is also false)**

Describing sets by statements

The set of integers, natural numbers, even and odd numbers are all infinite sets. Nonetheless, they can be described by listing just a few of their elements. In each case, such list provides a clear characteristic pattern that completely defines the set

In the case of prime numbers no characteristic pattern exists. So, lists won't work

The only way to describe prime numbers is "by property". Here the property is the **logical statement** that defines prime numbers. So, the only possible description for the set of prime numbers is:

$$P = \{ x \text{ integer: } P(x) \text{ is true}\}$$

More mathematical statements

In general, a **mathematical statement** is any logical statement about **mathematical objects**

Examples:

- $2 < 223$ **is** a mathematical statement
- But, "Earth is a planet" **is not!!!**
- 342 **is not** a mathematical statement, either
- But, the property that define primes: **P(n)**, **is a mathematical statement**, as well

Mathematical proofs

Most mathematical statements are formally called **theorems, lemmas or corollaries**

A **mathematical proof** is a procedure or a sequence of mathematical arguments for proving the truth of a **mathematical implication**

Thus, given "**A implies B**": we prove **B** by

- Assuming **A** to be true, and
- Showing a true implication

Implications revisited

RECALL THAT: The **truth of an implication depends on the operational and logical rules used** to go from the hypothesis to the thesis. An implication that **uses only accepted rules**, is true

Example: If $x > 3$ then $x + 1 > 4$

Proof: (exhibits a true implication)

1. By hypothesis (is true that) $x > 3$
2. A true algebraic rule says that "adding constants to both sides of an inequality preserves the inequality"
3. Thus, by adding 1 to both sides, $x + 1 > 3 + 1 = 4$

Types of mathematical proofs

Mathematical proofs may take different forms. Among them are:

- **Direct proofs**
- **Proof by exhaustion**
- **Contrapositive**
- **Proof by contradiction**
- **If and only if proofs**
- **Proof by construction**

Next, we discuss and illustrate each of them

Direct proofs

This is the "natural approach" consisting of starting with a true hypothesis, and using true arguments to derived new facts, step by step, until the thesis is reached

So, if A and B are Boolean variables representing the hypothesis and thesis, respectively; the direct proof correspond to finding a **true implication** (arrow) for making $\mathrm{A} \Rightarrow \mathrm{B}$ true

An illustration with even numbers

Theorem: If a natural number n is even, then there is a natural number k such that $n = 2 \cdot k$

Proof:

1. Since (by hypothesis) n is even, then there is an integer k such that $n = 2 \cdot k$
2. Since n is natural (by hypothesis), n is positive
3. Since positive by negative yields negative, k must be positive
4. Thus, k is a positive integer and so, k is a natural number

Proof by exhaustion

Consists in verifying one-by-one, the truth value of each of the cases involved in the statement

- Advantage: is usually simpler than direct proofs
- Disadvantage: It works only if the number of cases is finite <u>and small</u>

Illustration: A proof by exhaustion

Theorem: If n is an integer and $2 \leq n \leq 7$, then $q = n^2 + 2$ is not divisible by 4

Proof: By exhaustion. There are only 6 cases:

n	q	Divisible by 4?
2	6	No
3	11	No
4	18	No
5	27	No
6	38	No
7	51	No

NONE IS DIVISIBLE BY 4!

The theorem is proved!!!

Limitations of exhaustion

The next extension of the previous theorem:

"If n is integer, then $n^2 + 2$ is not divisible by 4"

involves an **infinite number of cases (integers are infinite)**. So, there is no way to examine all possible cases one-by-one (there is no way we can check all of them). And a finite number of randomly chosen cases **won't prove the statement**

Proof by contradiction

A proof by contradiction proves the truth of a mathematical statement **A** as follows:

- Make of **Not A** an hypothesis
- Use a correct implication to show that **Not A** implies **B**, with **B a false mathematical statement**
- Thus, we are exactly

HERE

Not A	B	A implies B
T	T	T
T	F	F
F	T	T
F	**F**	**T**

- Conclusion: **Not A is false**. So **A** is true

An important note

The negation of A when A is itself an implication requires particular analysis

Statement: "Not (P implies Q)" is equivalent to "P and not Q"

Proof:

1. P implies Q is equivalent to Not P or Q. Therefore,
2. Not (P implies Q) is equivalent to Not(Not P or Q)
3. Not(Not P or Q) is equivalent to P and Not Q. Thus,
4. Not (P implies Q) is equivalent to P and Not Q

A proof by contradiction

Theorem: If n is even, then n + 1 is odd

Proof: By contradiction.

1. The negation is: "n is even and n + 1 is even"
2. Since n is even there is an integer k, $n = 2 \cdot k$
3. Therefore, $n + 1 = 2 \cdot k + 1$
4. Since n + 1 is also even, there is an integer t such that $2 \cdot t = 2 \cdot k + 1$
5. But then, $t = (2 \cdot k + 1) / 2 = k + ½$
6. This is a contradiction because the sum of an integer k and a fraction is not an integer

Proof by contrapositive

Uses Not B implies Not A instead of A implies B

Why? Here is an illustration:

Theorem: If x^2 is odd then x is odd

Let's try: if x^2 is odd then $x^2 = 2 \cdot k + 1$ for some natural k. So, $x = \sqrt{2 \cdot k + 1}$ ...

This is true, but, How can I prove that x is odd?

No property of the square root yields a natural next step for arguing that...

Proof by contrapositive

Let's try the contrapositive:

Theorem: If x is even, then x^2 is even

Proof:

1. if x is even, then $x = 2 \cdot k$ for some integer k
2. So, $x^2 = (2 \cdot k)(2 \cdot k) = 4 \cdot k^2$
3. Since k is integer, so is k^2
4. So, x^2 is divisible by 2, and therefore, is even

Proving and "If and Only If" statement

In general, the proof of a logical statement of the form: "**A if and only if B**" involves two proofs

1. The Proof that "A implies B", and
2. The Proof that "B implies A"

Example: Proving the statement

"x is odd if and only if $x^2 + 2x + 1$ is even" requires proving:

1. If x is odd, then $x^2 + 2x + 1$ is even; and
2. If $x^2 + 2x + 1$ is even, then x is odd

Proof of statement 1

<u>Proof</u>:

1. Since x is odd, $x = 2k + 1$ for some integer k
2. Thus, $x^2 = (2k + 1)^2 = 4k^2 + 4k + 1$
3. So, $x^2+2x+1 = 4k^2+4k+ 1+4k+2+1$
4. Or, $x^2+2x+1 = 2(2k^2+4k+ 2)$
5. Since k is an integer, so is $q = (2k^2+4k+ 2)$
6. Therefore, $x^2+2x+1 = 2q$; and thus, it is even.

Proof of statement 2

Statement is: "if x^2+2x+1 is even, then x is odd". We use the contrapositive equivalent: "If x is even then $x^2+2x+1$is odd"

<u>Proof</u>:

1. Since x is even, $x = 2k$ for some integer k
2. Thus, $x^2+2x+1=4k^2+4k+1=2(2k^2+2k)+1$
3. Since k is an integer, so is $q = 2k^2+2k$
4. So, $x^2+2x+1=2q+1$, and thus, it is odd.

To be continued

In the next lecture…