# Discrete Mathematics II

12 lectures for Part IA CST 2012/13

Marcelo Fiore

Course web page:

http://www.cl.cam.ac.uk/teaching/1213/DiscMathII/

# Motivations

- Circuits in hardware $\leadsto$ Boolean algebra
- Datatypes in programming languages $\leadsto$ recursive datatypes
- Formal languages in compilers $\leadsto$ Regular languages.
- Relations in databases $\leadsto$ The algebra of relations
- Graphs in algorithms $\leadsto$ networks, dags, ... trees ...
- Counting in discrete probability $\leadsto$ bijective correspondence.
- Proof in program correctness
- Type systems

  inductive definitions.
- Computability $\leadsto$ countability.

# Discrete Mathematics I

- Propositional logic.
- Predicate logic.
- Proof.
- Set theory.
- Induction.

formal proof

mathematical argument

# Chapter 1

**Reading list:**

1.1 Logical notation

1.2 Patterns of proof

1.3 Mathematical induction

- The principle of mathematical induction
- Definition by mathematical induction
- Tower of Hanoi

**Suggested exercises:** 1.5, 1.7.

# Logical Notation

- $P \land Q$ , $P \,\&\, Q$ , P and Q — conjuction
- $P \lor Q$ , P or Q — disjunction
- $P \Rightarrow Q$ , P implies Q , if P then Q — implication
- $P \Leftrightarrow Q$ , P iff Q — biimplication
- $\neg P$ , P does not hold — negation

Introduce quantifiers

universal quantification

existential quantification

- $\forall x.\, P(x)$ , for all $x$, $P(x)$ , $\forall x_1, \ldots, x_n.\, P(x_1, \ldots, x_n)$;

- $\exists x.\, P(x)$ , there exists $x$ such that $P(x)$ , $\exists x_1, \ldots, x_n.\, P(x_1, \ldots, x_n)$

- $\exists! x.\, P(x)$ , there exists a unique $x$ such that $P(x)$

unique

## Definitions

$\mathbb{N}$ – The set of natural numbers

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

$\mathbb{N}_0$ – The set of natural numbers with zero

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

# Principle of Mathematical Induction

To show a property $P(k)$ for all $k$ ranging over the natural numbers, that is

to prove $\boxed{\forall k \in \mathbb{N}_0.\, P(k)}$

by the *principle of mathematical induction* we proceed as follows:

1. We show the property for $0$; that is

   we prove $\boxed{P(0)}$

2. We show that if the property holds for an arbitrary number then it will also hold for its successor; that is

   we prove $\boxed{\forall n \in \mathbb{N}_0.\, P(n) \Rightarrow P(n+1)}$

$$\sum_{i=0}^{k} i = 0+1+2+\cdots+k$$

**Example:**

$$P(k) =_{\text{def}} \left[ \sum_{i=0}^{k} i = \frac{k(k+1)}{2} \right]$$

Show $\forall n \in \mathbb{N}_0 .\ P(n)$

that is $\forall n \in \mathbb{N}_0 .\ \sum_{i=0}^{n} i = n(n+1)/2$

By induction, we need show

BASE CASE

(1) $P(0) =_{\text{def}} \sum_{i=0}^{0} i \stackrel{?}{=} 0(0+1)/2$

Both are $0$ so the equality holds

INDUCTION STEP

(2) $\forall n \in \mathbb{N} .\ P(n) \Rightarrow P(n+1)$

Assume $P(n)$ holds for some arbitrary $n$

Show $P(n+1)$, that is

$$\sum_{i=0}^{n+1} i \stackrel{?}{=} (n+1)(n+1+1)/2$$

$$\sum_{i=0}^{n+1} i = \left(\sum_{i=0}^{n} i\right) + (n+1)$$

$$= n(n+1)/2 + (n+1) \quad \text{by induction hypothesis}$$

$$= (n+1)(n+2)/2$$

$\boxed{X}$

In particular

$$\sum_{i=0}^{n+1} i = \sum_{i=0}^{n} i + (n+1) = (n+1)(n+2)/2$$

IS NOT A PROOF.

# Definition by Mathematical Induction

PRIMITIVE RECURSION

To define a function $f$ ranging over the natural numbers; that is,

to define values $\boxed{f(k) \text{ for all } k \in \mathbb{N}_0}$

one may

- define the value $f(0)$ of the function $f$ at $0$; that is,

  set $\boxed{f(0) = b}$

- define the value for $f(n+1)$ in terms of the values $n$ and $f(n)$; that is

  set $\boxed{f(n+1) = h\big(n, f(n)\big)}$

**Example:** Tower of Hanoi

recurrence relation

$$T(n) =_{\text{def}} \begin{cases} \cancel{T(n-1)}\ 0 & \text{, if } n = 0 \\ 2T(n-1)+1 & \text{, if } n \in \mathbb{N} \end{cases}$$

a function from numbers to numbers

Actually $T(n) = 2^n - 1 \quad \forall n \in \mathbb{N}_0$.

EXERCISE Show it by induction.

# Chapter 2

**Reading list:**

2.1 Sets

2.2 Set laws

**Suggested exercises:** 2.2, 2.8

# Sets

- *Sets* and *classes* are unordered collections.

without repetition

**Examples:** $\emptyset$, $\mathbb{N}$, $\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$.

The empty set

integers

$\{\ldots, -2, -1, 0, 1, 2, \ldots\}$

$\mathbb{N}$ $\mathbb{N}_0$ $\mathbb{Z}$ $\mathbb{Q}$ $\mathbb{R}$

- Comprehension:

$$\{x \mid P(x)\}\ , \quad \{x \in X \mid P(x)\}$$

$a \in \{x \mid P(x)\}$

iff $P(a)$ holds

$\boxed{?}$ What properties should be allowed for this to define a set?