Slides

for Part IA CST 2025/26

Discrete Mathematics

<www.cl.cam.ac.uk/teaching/2526/DiscMath>

Prof Marcelo Fiore

Marcelo.Fiore@cl.cam.ac.uk

Dr Jon Sterling

js2878@cl.cam.ac.uk

What are we up to?

- Learn to read and write, and also work with, mathematical arguments.
- Doing some basic discrete mathematics.
- Getting a taste of computer science applications.

What is Discrete Mathematics ?

from *Discrete Mathematics (second edition)* by N. Biggs

Discrete Mathematics is the branch of Mathematics in which we deal with questions involving finite or countably infinite sets. In particular this means that the numbers involved are either integers, or numbers closely related to them, such as fractions or 'modular' numbers.

What is it that we do ?

In general:

Build mathematical models and apply methods to analyse problems that arise in computer science.

In particular:

Make and study mathematical constructions by means of definitions and theorems. We aim at understanding their properties and limitations.

Lecture plan

I. Proofs.

II. Numbers.

III. Sets.

IV. Regular languages and finite automata.

Proofs

Objectives

- To develop techniques for analysing and understanding mathematical statements.
- To be able to present logical arguments that establish mathematical statements in the form of clear proofs.
- To prove Fermat's Little Theorem, a basic result in the theory of numbers that has many applications in computer science.

Proofs in practice

We are interested in examining the following statement:

$\boxed{\text{The product of two odd integers is odd.}}$

This seems innocuous enough, but it is in fact full of baggage.
For instance, it presupposes that you know:

- what a statement is;
- what the integers $(\ldots, -1, 0, 1, \ldots)$ are, and that amongst them there is a class of odd ones $(\ldots, -3, -1, 1, 3, \ldots)$;
- what the product of two integers is, and that this is in turn an integer.

More precisely put, we may write:

$$\boxed{\text{If } m \text{ and } n \text{ are odd integers then so is } m \cdot n.}$$

which further presupposes that you know:

- what variables are;
- what

  $$\text{if} \ldots \text{then} \ldots$$

  statements are, and how one goes about proving them;
- that the symbol "$\cdot$" is commonly used to denote the product operation.

Even more precisely, we should write

$\boxed{\text{For all integers } m \text{ and } n, \text{ if } m \text{ and } n \text{ are odd then so is } m \cdot n.}$

which now additionally presupposes that you know:

- what

  for all . . .

  statements are, and how one goes about proving them.

Thus, in trying to understand and then prove the above statement, we are assuming quite a lot of *mathematical jargon* that one needs to learn and practice with to make it a useful, and in fact very powerful, tool.

Some mathematical jargon

Statement

A sentence that is either true or false — but not both.

Example 1

‘$e^{i\pi} + 1 = 0$’

Non-example

‘This statement is false’

Predicate

A statement whose truth depends on the value of one or more variables.

Example 2

1. ‘$e^{ix} = \cos x + i \sin x$’

2. *‘the function f is differentiable’*

Theorem

A very important true statement.

Proposition

A less important but nonetheless interesting true statement.

Lemma

A true statement used in proving other true statements.

Corollary

A true statement that is a simple deduction from a theorem or proposition.

Example 3

1. *Fermat's Last Theorem*
2. *The Pumping Lemma*

Conjecture

A statement believed to be true, but for which we have no proof.

Example 4

1. *Goldbach's Conjecture*

2. *The Riemann Hypothesis*

Proof

Logical explanation of why a statement is true; a method for establishing truth.

Logic

The study of methods and principles used to distinguish good (correct) from bad (incorrect) reasoning.

Example 5

1. *Classical predicate logic*
2. *Hoare logic*
3. *Temporal logic*

Axiom

A basic assumption about a mathematical situation.

Axioms can be considered facts that do not need to be proved (just to get us going in a subject) or they can be used in definitions.

Example 6

1. *Euclidean Geometry*
2. *Riemannian Geometry*
3. *Hyperbolic Geometry*

Definition

An explanation of the mathematical meaning of a word (or phrase).

The word (or phrase) is generally defined in terms of properties.

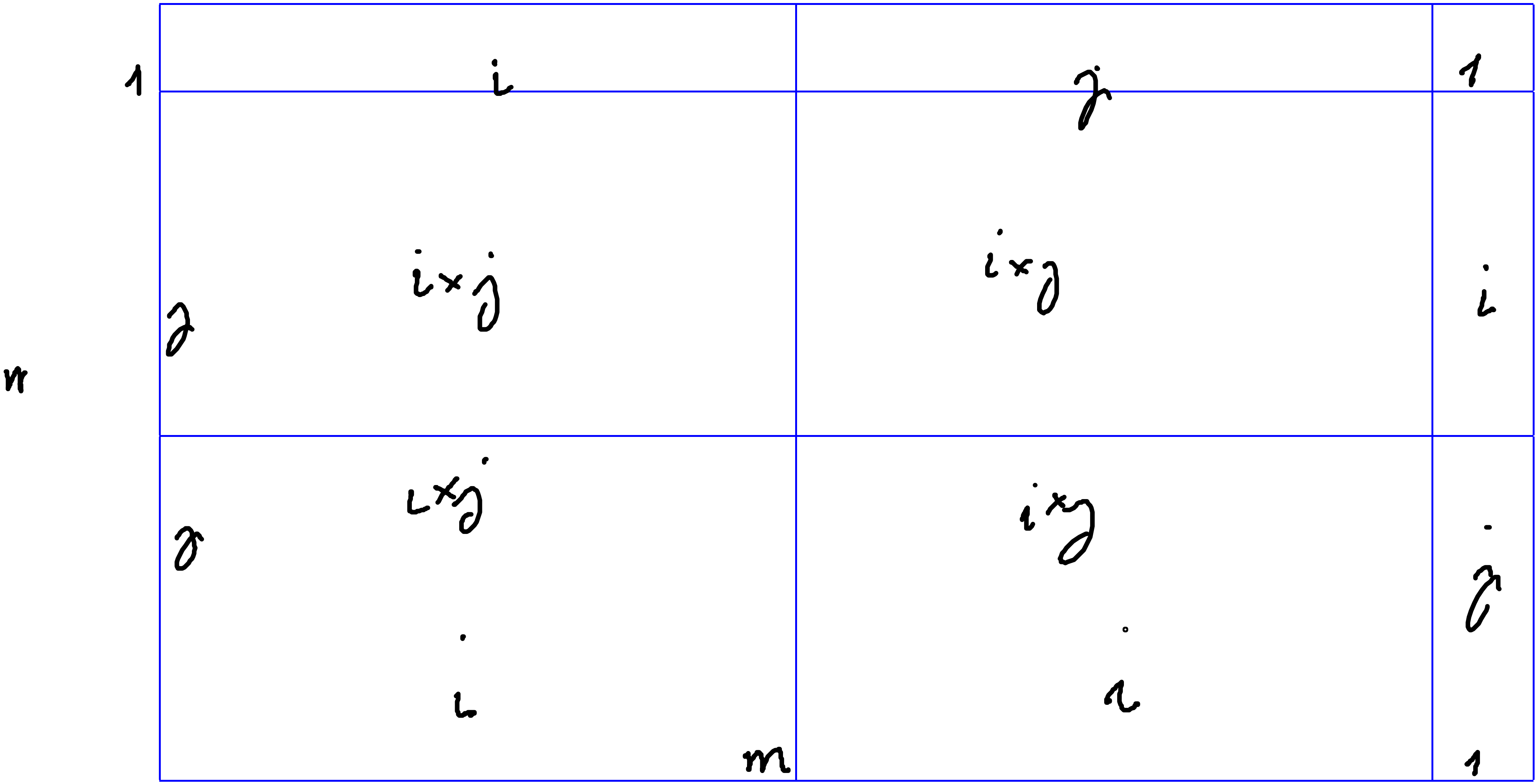
Warning: It is vitally important that you can recall definitions precisely. A common problem is not to be able to advance in some problem because the definition of a word is unknown.

Definition, theorem, intuition, proof in practice

Definition 7 *An integer is said to be odd whenever it is of the form* $2 \cdot i + 1$ *for some (necessarily unique) integer* i.

Proposition 8 *For all integers* m *and* n, *if* m *and* n *are odd then so is* $m \cdot n$.

Intuition:



PROOF OF Proposition 8:

Consider integers m and n.

They are odd, hence $m = 2i+1$ for an integer i and $n = 2j+1$ for an integer j.

Then
$$m \cdot n = (2i+1)\cdot(2j+1)$$
$$= 2(2ij + i + j) + 1$$

Since $2ij + i + j$ is an integer, $m \cdot n$ is odd.

$\boxtimes$

Simple and composite statements

A statement is *simple* (or *atomic*) when it cannot be broken into other statements, and it is *composite* when it is built by using several (simple or composite statements) connected by *logical* expressions (e.g., if...then...; ...implies ...; ...if and only if ...; ...and...; either ...or ...; it is not the case that ...; for all ...; there exists ...; etc.)

Examples:

'2 is a prime number'

'for all integers m and n, if $m \cdot n$ is even then either n or m are even'

Proof Structure

Assumptions	Goals
statements that may be used for deduction	statements to be established

Implication

Theorems can usually be written in the form

if a collection of *assumptions* holds,
then so does some *conclusion*

or, in other words,

a collection of *assumptions* **implies** some *conclusion*

or, in symbols,

a collection of *hypotheses* $\Longrightarrow$ some *conclusion*

NB Identifying precisely what the assumptions and conclusions are is the first goal in dealing with a theorem.

Implications

- How to *prove* them as goals.
- How to *use* them as assumptions.

How to prove implication goals

The main proof strategy for implication:

> To prove a goal of the form
>
> $$P \implies Q$$
>
> assume that P is true and prove Q.

NB *Assuming* is not *asserting*! Assuming a statement amounts to the same thing as adding it to your list of hypotheses.

Proof pattern:

In order to prove that

$$P \implies Q$$

1. Write: Assume P.
2. Show that Q logically follows.

Scratch work:

Before using the strategy

Assumptions	Goal
	$P \implies Q$
$\vdots$

After using the strategy

Assumptions	Goal
	Q
$\vdots$
P

Proposition 8 *If* m *and* n *are odd integers, then so is* $m \cdot n$.

PROOF:

Assume m and n are odd integers.

RTP: m.n is an odd integer.

Then $m = 2i+1$ and $n = 2j+1$ for int. i and j.

So $m \cdot n = (2i+1)(2j+1) = \cdots = 2k+1$

for $k = \cdots$ an integer and we are done. $\boxtimes$

Definition 9 *A real number is:*

- rational *if it is of the form* m/n *for a pair of integers* m *and* n*; otherwise it is* irrational*.*
- positive *if it is greater than* 0*, and* negative *if it is smaller than* 0*.*
- nonnegative *if it is greater than or equal* 0*, and* nonpositive *if it is smaller than or equal* 0*.*
- natural *if it is a nonnegative integer.*

Proposition 10 *Let* x *be a positive real number. If* $\sqrt{x}$ *is rational then so is* x*.*

PROOF:

Assume x is a positive real number.

Assume $\sqrt{x}$ is rational

<u>RTP</u>: x is rational.

Then $\sqrt{x} = p/q$ for int. p and q.

So $x = (\sqrt{x})^2 = p^2/q^2 = a/b$ with $a = p^2$ and $b = q^2$ integers.

$\boxtimes$

How to use implication assumptions

Logical Deduction by Modus Ponens

A main rule of *logical deduction* is that of *Modus Ponens*:

From the statements P and $P \implies Q$,
the statement Q follows.

or, in other words,

If P and $P \implies Q$ hold then so does Q.

or, in symbols,

$$\frac{P \qquad P \implies Q}{Q}$$

The use of implications:

To use an assumption of the form $P \implies Q$, aim at establishing P.
Once this is done, by Modus Ponens, one can conclude Q and so further assume it.

Theorem 11 *Let* P_1, P_2, *and* P_3 *be statements. If* $P_1 \implies P_2$ *and* $P_2 \implies P_3$ *then* $P_1 \implies P_3$.

PROOF:

Let P_1, P_2, P_3 be statements.

Assume: (1) $P_1 \Rightarrow P_2$ and (3) $P_2 \Rightarrow P_3$.

RTP: $P_1 \Rightarrow P_3$

Assume (2) P_1

RTP: P_3

By MP from (1) and (2), we conclude (4) P_2

By MP from (3) and (4), we have P_3 as required. ⊠

Bi-implication

Some theorems can be written in the form

$$\boxed{P \text{ is equivalent to } Q}$$

or, in other words,

$$\boxed{P \text{ implies } Q\text{, and vice versa}}$$

or

$$\boxed{Q \text{ implies } P\text{, and vice versa}}$$

or

$$\boxed{P \text{ if, and only if, } Q} \qquad \boxed{P \text{ iff } Q}$$

or, in symbols,

$$\boxed{P \iff Q}$$

Proof pattern:

In order to prove that

$$P \iff Q$$

1. Write: $(\Longrightarrow)$ and give a proof of $P \implies Q$.
2. Write: $(\Longleftarrow)$ and give a proof of $Q \implies P$.