Part IA — Discrete Mathematics

Lectures by xxx
Latex by Z.Yan

Michaelmas 2016

* **Proof [5 lectures]**
Proofs in practice and mathematical jargon. Mathematical statements: implication, bi-implication, universal quantification, conjunction, existential quantification, disjunction, negation. Logical deduction: proof strategies and patterns, scratch work, logical equivalences. Proof by contradiction. Divisibility and congruences. Fermats Little Theorem.

* **Numbers [5 lectures]**
Number systems: natural numbers, integers, rationals, modular integers. The Division Theorem and Algorithm. Modular arithmetic. Sets: membership and comprehension. The greatest common divisor, and Euclids Algorithm and Theorem.The Extended Euclids Algorithm and multiplicative inverses in modular arithmetic. The Diffie-Hellman cryptographic method. Mathematical induction: Binomial Theorem, Pascals Triangle, Fundamental Theorem of Arithmetic, Euclids innity of primes.

* **Sets [7 lectures]**
Extensionality Axiom: subsets and supersets. Separation Principle: Russells Paradox, the empty set. Powerset Axiom: the powerset Boolean algebra, Venn and Hasse diagrams. Pairing Axiom: singletons, ordered pairs, products. Union axiom: big unions, big intersections, disjoint unions. Relations: composition, matrices, directed graphs, preorders and partial orders. Partial and (total) functions. Bijections: sections and retractions. Equivalence relations and set partitions. Calculus of bijections: characteristic (or indicator) functions. Finite cardinality and counting. Infinity axiom. Surjections. Enumerable and countable sets. Axiom of choice. Injections. Images: direct and inverse images. Replacement Axiom: set-indexed constructions. Set cardinality: Cantor-Schoeder-Bernstein Theorem, unbounded cardinality, diagonalisation, fixed-points. Foundation Axiom.

* **Formal languages and automata [7 lectures]**
Introduction to inductive definitions using rules and proof by rule induction. Abstract syntax trees. Regular expressions and their algebra. Finite automata and regular languages: Kleenes theorem and the Pumping Lemma.

Contents

1 Proofs **3**
1.1 Proofs in practice . . . 3
1.2 Mathematical jargon . . . 3
1.3 Mathematical statements . . . 5
1.4 Logical deduction . . . 5
1.5 Proof by contradiction . . . 5
1.6 Divisibility and congruences . . . 5
1.7 Fermats Little Theorem . . . 5

2 Numbers **6**

3 Sets **7**

4 Regular languages and finite automata **8**

1 Proofs

. : implication, bi-implication, universal quantication, conjunction, existential quantication, disjunction, negation. : proof strategies and patterns, scratch work, logical equivalences. . . .

1.1 Proofs in practice

We are interested in examining the following statement:

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

More precisely put, we may write:

Statement. If m and n are odd integers then so is $m \cdot n$.

which further presupposes that you know:

- what variables are;
- what

  $$if...then...$$

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

Even more precisely, we should write

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

- 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.

1.2 Mathematical jargon

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

Example (1)**.**

$$e^{i\pi} + 1 = 0$$

Example (Wrong)**.** This statement is false.

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

Example (2)**.**

(i)

$$e^{ix} = \cos x + i \sin x$$

(ii) 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)**.**

(i) **Fermat's Last Theorem** If x,y,z and n are integers satisfying

$$x^n + y^n = z^n$$

then either $n \leq 2$ or $xyz = 0$.

(ii) **The Pumping Lemma** Let $\mathcal{L}$ be a regular language. then there is a positive integer p such that any word $w \in \mathcal{L}$ of length exceeding p can expressed as $w = xyz$, $|y| > 0, |xy| \leq p$, such that, for all $i > 0$, xy^iz is also a word of $\mathcal{L}$.

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

Example (4)**.**

(i) Goldbach's Conjecture
(ii) 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)**.**

(i) Classical predicate logic
(ii) Hoare logic
(iii) Temporal logic

Axiom A basic assumption about a mathematical situation.
Axioms cam 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)**.**

(i) Euclidean Geometry
(ii) Riemannian Geometry
(iii) Hyperbolic Geometry

Definition A explanation of the mathematical meaning of a word (or phase).
The word (or phase) 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 (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 off then so is $m \cdot n$.

Proof. Let m and n be arbitrary odd integers. Thus, $m = 2 \cdot i + 1$ and $n = 2 \cdot j + 1$ for some integers i and j. Hence, we have that $m \cdot n = 2 \cdot k + 1$ for $k = 2 \cdot i \cdot j + i + j$, showing that $m \cdot n$ is indeed odd. □

Warning. Though the scratch work contains the idea behind the given proof, it is not a proper proof.

Definition (Mathematical proof)**.** A mathematical proof is a sequence of logical deductions from axioms and previously proved statements that concludes with the proposition in the question. The axioms-and-proof approach is called the axiomatic method.

1.3 Mathematical statements

1.4 Logical deduction

1.5 Proof by contradiction

1.6 Divisibility and congruences

1.7 Fermats Little Theorem

2 Numbers

3 Sets

4 Regular languages and finite automata