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 quantication, conjunction, existential quantication, 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 Dife-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. Innity 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, xed-points. Foundation Axiom.

* **Formal languages and automata [7 lectures]**
  Introduction to inductive denitions 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

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

1.1 Proofs in practice and mathematical jargon

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.

1.2 Mathematical statements

1.3 Logical deduction

1.4 Proof by contradiction

1.5 Divisibility and congruences

1.6 Fermats Little Theorem

2 Numbers

3 Sets

4 Regular languages and finite automata