Foundations of logic and mathematics–Applications to computer science and cryptography by Yves Nievergelt, Birkhauser Verlag AG, Klösterberg 23, CH 4010, Basel, Switzerland, 2002, pp. 415, CHF 136.

The book is an introduction to logic and discrete mathematics. It covers a wide range of topics from Boolean algebra to sets, relations to combinatorics and decidability. In the 'application' section modular arithmetic, codes and graph theory are also discussed.

Chapter 0 (Boolean algebraic logic) deals with Boolean algebra, truth table and Karnaugh maps. Logical connectives, tautologies and synthesis of logical formulae are discussed.

The treatment in this book is different from usual books on discrete mathematics. Usually either it will be studied from 'logic' or 'switching theory' point of view. Here both directions are considered. But a few more examples using English sentences for illustrating logic concepts could have made it more interesting.

Chapter 1 (Logic and deductive reasoning) discusses propositional and predicate calculus. It introduces universal and existential quantifiers. Different proof techniques like proof by contradiction are discussed. Several deduction rules like 'modus ponens' are explained and the use of derived rules shown. Axioms and rules for predicate calculus are given and examples of proofs using them shown. The goal of this chapter seems to be in revealing the bases of mathematics and computer science, and in showing what constitutes a complete proof.

Chapter 2 (Set theory) on sets shows how to apply logic to develop set theory. The chapter gives the beginner ample practice with straightforward proofs through predicate calculus. The proofs are given in a formal manner.

Chapter 3 (Induction and arithmetic) uses set theory to introduce the concept of induction. Somehow it appears that easy things are deliberately made difficult in introducing this concept. It is then demonstrated how to derive the rules of integer and rational arithmetic, and how they apply to counting the elements of finite sets. Here the goal seems to be reveal where all the rules of arithmetic come from, starting from logic and set theory. There is a small section on use of arithmetic in finance. Somehow this section seems to be out of place for a book of this type. The difference between the first and second principles of mathematical induction is not brought out clearly.

Chapter 4 (Decidability and completeness) discusses logical independence, consistency, completeness and decidability. Sections 4.1.3 and 4.1.4 discuss two types of axiomatic systems. In Section 4.2.2, incompleteness of the implicational calculus is proved using Peirce's law. Section 4.3 discusses logics with any number of values not amenable to truth tables. Automated theorem proving is discussed in Section 4.4.

Completeness is discussed in 4.4.4. Ordinals and regularity of well-formed sets are discussed. Further issues in decidability, including Godel’s incompleteness theorem are mentioned at the end.

Part B of the book discusses some real applications making use of the theory developed in Part A. Chapter 5 (Number theory and codes) discusses elements of number theory. Modular arithmetic is discussed and use of number theory in the design of bar codes, book codes and the RSA code in public key cryptography are discussed.

In Chapter 6, elements of algebra are discussed. Basic combinatorics including permutations and combinations under different conditions is discussed. Section 6.7 discusses probability and section 6.8 ENIGMA machines. This is an interesting section dealing with enciphering of plain text and deciphering of encrypted messages and also contains a section breaking the ENIGMA ciphers.

Chapter 7 (Graph theory) deals with basics of graph theory. Fundamental concepts in graph theory are explained. Basic concepts like walks, Hamiltonian, Eulerian circuits, planar, bipartite graphs, trees, spanning trees, weighted graphs are discussed. Some applications are given at the end.

Usually books on discrete mathematics deal with topics like logic, sets, relations, etc., but a wide range of topics starting from Boolean algebra to modular arithmetic, codes and combinatorics and graph theory are covered in this book. The writing is very formal. It is really very difficult to write a book where everything is written in a very formal manner. But why one should do that is a matter may be for philosophical reflection. One could learn how to look at everything from ‘logic’ point of view and write statements in a formal manner by reading this book. A number of small exercises are given everywhere so that a new reader can learn the subject thoroughly. The book is more suited to a mathematics student rather than a computer science student as the highly formal way of writing makes it difficult for persons without such background to enjoy it. In Indian universities, this book may serve as an additional reference source for a course dealing with logic/discrete mathematics/combinatorics/codes.

Professor, Kamala Krithivasan
Department of Computer Science & Engineering,
Indian Institute of Technology,
Chennai 600 036, India.
email: kamala@shiva.iitm.ernet.in