1 Summary of the review

In its third edition, *Discrete Mathematics*, is a mature textbook providing an introduction to those aspects of university level mathematics needed by computer science majors. For the most part, it provides an excellent pedagogical treatment of its subject matter, along with numerous worked exercises. The newly introduced chapter on public key cryptography is exemplary in this respect. *Discrete Mathematics* is also suitable as a reference book; however, the treatment of most topics is probably too basic to be of immediate use to the practicing professional.

2 Summary of the book

This is the third edition of *Discrete Mathematics*, though you might not recognize the title because the first two editions went under the name: *Discrete Mathematics for New Technology*. While one can debate which, if either, of these two titles more adequately describes the contents, the main intent of this book is to present a concise introduction to the core mathematical knowledge required of those seeking a computer science degree in the UK. The casual reader will rapidly confirm that *Discrete Mathematics* is indeed aimed mainly at undergraduate students, however, according to the authors, practicing scientists will also find this book valuable as a reference tool, a claim which is not without merit, but it is not the book’s main purpose.

In under 900 pages, *Discrete Mathematics* manages to cover the following topics: *Mathematical Logic, Set Theory, Relations, Functions, Matrix Algebra, Systems of Linear Equations, Algebraic Structures, Number Theory, Boolean Algebra* and *Graph Theory*. As the authors themselves note, the choice of topics is largely driven by curricula considerations at UK universities; however, most professionals around the world would probably agree that these topics covered belong to the set of essential mathematical concepts with which any computer scientists should have at least a nodding acquaintance.

Earlier readers criticized the first edition for not having enough exercises given its pretense of being a textbook. Those critics will be pleased to know that this defect has been amply rectified. There are now copious exercises from every chapter for the instructor to select from and more than 100 pages of hints and answers to get the student started. Even if the instructor is not using this book as the primary reference in his or her lectures, it would be worthwhile keeping a copy as a secondary reference due to the high quality of the worked exercises. In addition to the exercises there are numerous worked examples in each chapter demonstrating how to use each new theorem in problem solving, or as a basis for proving additional theorems. Whereby in the latter case, the principals of mathematical proof discussed in Chapter 2 play a prominent role.

Members of IACR will be particularly interested in Chapter 9, *Introduction to Number Theory*, which is making its first appearance in the third edition, though the title is somewhat misleading. Undeniably, it does provide a nice introduction to number theory, but only insofar as it is necessary to explain public
key cryptography systems. Those aspects of Number Theory not required to understand public key cryptography are neglected. Starting from the concept of integer division, working up to group theory in modular arithmetic, the complete machinery necessary to understand RSA encryption is developed. For the student or interested layman, this chapter represents a fascinating and accessible journey through pure mathematics, cumulating with one of the key technologies behind modern day Internet commerce. If this chapter does not convince the student of the practical importance of pure mathematics, then there is probably not much that will.

Other sections of exceptional pedagogical excellence include chapters 11, Graph Theory and 12, Applications of Graph Theory. The sections on sorting and searching in particular are amplified with copious, detailed diagrams to support the discussions as the authors delve in the subtleties of these very important algorithms.

There is more than enough material in this book for a one semester course at the Freshman level; hence, some material has to be skipped. One obvious candidate for skipping is Chapter 7, Systems of Linear Equations, which is by far the weakest chapter in the entire book. The material in this chapter properly belongs to a course on Numerical Analysis, not Discrete Mathematics, as there is very seldom a need in the real world to apply Gaussian elimination on a system of equations with discrete coefficients yielding discrete values in the results. In the real world, the coefficients are, well, real values and the trick is not just to get the answer, but to know what errors were made in arriving at the answer. Additionally, I suspect the material in chapter 6, Matrix Algebra, is included as a refresher for the student, or in order to make the book self-contained, since the level of treatment is such as would normally would be covered in high school.

The index and table of contents are both well organized, lending support to the author’s claim that the book is suitable as a reference. Additionally, as an aid to those who are not reading the book linearly, located immediately before the first chapter is a very complete table of all symbols, including section numbers where the symbols first appear.

3 What is the book like (style)?

The book is typeset in the typical University level textbook style, with a clean, crisp font, ample white space and, where necessary, black and white illustrations to support the discourse. A few obligatory cartoons (again in black and white) are also scattered throughout the book, seemingly as a nod to en vogue teaching methods, though they are not in the quantity or quality to hold the interest of today’s multi-media saturated youth.

As a teaching aid, important theorems and definitions are set apart from the main text by way of enclosure inside rectangular boxes. The worked examples are also set apart from the main text by a single horizontal line; the exercises for the student are set apart by a double horizontal line. Being similar it is easy to confuse the two. Here one could have wished for a bit more visual offset. Another nick-pick: the section title appears at the top right of every odd-numbered page, but not the section number. This is particularly unfortunate because the table of symbols list the section number of first appearance, not the section name, making it difficult to look the symbols up directly without referring back to the table of contents.

The writing style, sentence structure and vocabulary are appropriate for the University level audience without being overly dense or pretentious. Evidently, the authors are experienced educators striving for a rigorous, yet readable book whose main purpose is to educate the reader using a maximum of relevant information with a minimum of extraneousness.

This being the third edition, most of the errors have, as would be expected, already been exorcised; except of course those in the newly introduced chapter 9. Here there are quite a few typos, most of which the astute reader will easily spot.
Would you recommend this book?

As a text book for students entering computer science, *Discrete Mathematics* is highly recommended because of its exceptional pedagogical qualities. Furthermore, any student who uses this book in their course work would be well advised to hang on to it for future reference. Likewise, those entering the field of computer science after having earned a degree in another field, will find this book useful as an introduction to mathematical concepts not normally covered in the curriculum of other sciences. (E.g., Typed Set Theory, Logic Networks, Functional analysis as it applies to Relational Databases as well as the above mentioned material on the Applications of Graph Theory.)

Professionals already working in the field will find most of the material herein too basic, because all of the topics treated here are treated in more depth in other books aimed at the specialist audience. Nevertheless, if one needs to enter a new area, but lacks (or has forgotten) the necessary mathematical prerequisites, then *Discrete Mathematics* will provide a more coherent introduction than the typical Wikipedia article.

*The reviewer is an analyst and researcher with Inversik Laboratories in Germany.*