The Book Review Column[1]
by Frederic Green

Department of Mathematics and Computer Science
Clark University
Worcester, MA 01610
email: fgreen@clarku.edu

In this column, we review these three books:

1. **Essential Discrete Mathematics for Computer Science**, by Harry Lewis and Rachel Zax. Review by Bill Gasarch.
2. **Applied Number Theory**, by Harald Niederreiter and Arne Winterhof. Review by Song Y Yan.
3. **Market Design: A Linear Programming Approach to Auctions and Matching**, by Martin Bichler. Review by S.V. Nagaraj.

In these days of social distancing, what better way to pass the time than to settle down with a good book? Please contact me to write a review; choose from among the books listed on the next pages. Or choose one of your own. The latter is actually preferable in the current circumstances, as I can then ask the publisher to forward it directly to you.

BOOKS THAT NEED REVIEWERS FOR THE SIGACT NEWS COLUMN

Computability, Complexity, Logic

1. *The Foundations of Computability Theory,* by Borut Robič
2. *Applied Logic for Computer Scientists: Computational Deduction and Formal Proofs*, by Mauricio Ayala-Rincón and Flávio L.C. de Moura.
3. *Descriptive Complexity, Canonisation, and Definable Graph Structure Theory*, by Martin Grohe.
4. *Kernelization: Theory of Parameterized Preprocessing,* by Fedor V. Fomin, Daniel Lokshtanov, Saket Saurabh, and Meirav Zehavi.

Miscellaneous Computer Science

1. *Elements of Causal Inference: Foundations and Learning Algorithms*, by Jonas Peters, Dominik Janzing, and Bernhard Schölkopf.
2. *Elements of Parallel Computing*, by Eric Aubanel
3. *CoCo: The colorful history of Tandy's Underdog Computer* by Boisy Pitre and Bill Loguidice
4. *Introduction to Reversible Computing*, by Kalyan S. Perumalla
5. *A Short Course in Computational Geometry and Topology*, by Herbert Edelsbrunner
6. *Partially Observed Markov Decision Processes,* by Vikram Krishnamurthy
7. *Statistical Modeling and Machine Learning for Molecular Biology*, by Alan Moses
8. *The Problem With Software: Why Smart Engineers Write Bad Code,* by Adam Barr.
9. *Language, Cognition, and Computational Models,* Theirry Poibeau and Aline Villavicencio, eds.
10. *Computational Bayesian Statistics, An Introduction,* by M. Antónia Amaral Turkman, Carlos Daniel Paulino, and Peter Müller.
11. *Variational Bayesian Learning Theory,* by Shinichi Nakajima, Kazuho Watanabe, and Masashi Sugiyama.

Cryptography and Security

1. *Cryptography in Constant Parallel Time,* by Benny Appelbaum
2. *A Cryptography Primer: Secrets and Promises*, by Philip N. Klein

Combinatorics and Graph Theory

1. *Finite Geometry and Combinatorial Applications*, by Simeon Ball
2. *Introduction to Random Graphs*, by Alan Frieze and Michał Karoński
3. *Erdős –Ko–Rado Theorems: Algebraic Approaches*, by Christopher Godsil and Karen Meagher
4. *Combinatorics, Words and Symbolic Dynamics,* Edited by Valérie Berthé and Michel Rigo

Miscellaneous Mathematics

1. *Introduction to Probability*, by David F. Anderson, Timo Seppäläinen, and Benedek Valkó.

Review of[2]
Essential Discrete Mathematics for Computer Science
By Harry Lewis and Rachel Zax
Published by Princeton University Press, 2019
408 Pages, $75 on Princeton Site, Hardcover or $45 on Amazon Kindle

Review by
William Gasarch (gasarch@cs.umd.edu)

Disclaimer: One of the authors of the book, Harry Lewis, was my Ph.D. thesis advisor.

1 Introduction

At various times representatives from book publishers come to my office and ask what kind of book do I want to see. I often say

I want to see a cheap Discrete Math textbooks that leaves out some of the topics that nobody covers such as algorithms, finite automata, Bayes Theorem (more on that later).

Why do I say this? Because Discrete Math (henceforth DM) books (and in fact many textbooks) are expensive. In preparing this review I looked at DM textbooks on Amazon to see if my complaint is still true.

Here is what I found (I also include what the first chapter is for reasons we will see later.) The prices on Amazon for e-books or paper are often cheaper but may be counterfeits supplied to Amazon by third parties.

1. Discrete Mathematics by Chartrand and Zhang. $122.95 for the hardcover. First chapter is on logic.
2. Discrete Mathematics and its Applications by Kenneth Rosen. $185.02 for the paperback. First chapter is on logic.
3. Discrete Mathematics: An Open Introduction by Oscar Levine. $14 for the paperback. First chapter on Logic, Sets, Functions.
4. Discrete Mathematics by Richard Johnsonbaugh. $126.65 hardcover, $64 paperback. First chapter on Sets and Logic.
5. Discrete Mathematics by Susanna Epp. $145.95 hardcover. First chapter is on logic.

Most of the books are expensive, though some were not.

Caveat: Some of the books were available for rent at a cheaper price, but even the cheaper price seemed expensive.

Harry Lewis and Rachel Zax have written a book that is cheaply priced and, oddly enough, still has some of those chapters that I can't imagine many teachers getting to. This is not a complaint.

2 Format

Many discrete math books have (say) 5 parts (e.g, *Techniques of Proof*)), and each part has (say) 4 chapters (e.g., *(1) Direct Proof, (2) Proof by contradiction, (3) Disproof by Counterexample, (4) Proof by Induction*). This book does not have any parts, 31 short chapters. The chapters' lengths, and the fact that they are not part of a set of X chapters, makes the book more flexible and easier to read than other books.

3 The Book Does Not Begin With Logic!

Which of the following statements is interesting?

- If P is true and $P \to Q$ then Q is true.
- One can build an n-bit ADDER out of AND, OR, and NOT gates.
- $\sqrt{2}$ is irrational.
- $\prod_{i=1}^{n}(1+\frac{1}{i}) = n+1$. (Disclaimer: I might find this more interesting than you do since I didn't know it before I reviewed this book.)

This is of course a matter of opinion, so there is no right answer. **I am lying (hmmm, a paradox?)**. Of course the first one is not interesting and the rest are. The first one is about the *form* of a proof but does not have interesting content.

As noted above when I listed DM textbooks and their prices, most begin with logic. The book under review begins with a chapter on the Pigeonhole principle. They give *interesting* applications of it. They then do a chapter on basic proof techniques which includes the proof that $\sqrt{2}$ is irrational. Chapters 3 and 4 are on induction and strong induction, with many interesting examples. Hence the students *begin* with theorems of interest.

4 But There Have to Be Some Boring Parts

Chapter 5 is on sets, Chapter 6 is on Relations and Functions, Chapter 9 is on Prop Logic, Chapter 10 is on Normal Forms, Chapter 12 is on Quantification Logic. These chapters are mostly definitions. It is a challenge for any DM textbook to make these topics interesting. This book does the next best thing: the chapters are short.

5 And of Course Lots of DM IS Interesting

Chapter 7 is on uncountable sets. This was right after the chapter on functions, which makes sense.

Chapter 11 is on how to use AND, OR and NOT gates to build a computer (or at least and ADDER). This was just after the chapter on normal forms, which makes sense.

Chapters 22 and 23 are on combinatorics. Chapters 26-29 are on probability. It is a bit odd that the Pigeonhole principle (Chapter 1), Combinatorics (22 and 23) and Probability (26-29) are scattered in the book. However, since pigeonhole is there to whet their appetites, perhaps it is best to not then go whole-hog into combinatorics. As for the gap between combinatorics and probability, the chapters between are on Series and Recurrences, which makes sense. **I am lying again**—I don't see why that makes sense at all. I checked to see if series or recurrences are in the section on probability—they are not. This is odd, but it is not a problem since a teacher can pick and choose as they see fit.

Chapter 30 is on Mod Arithmetic. I am surprised it is so late in the book since I usually use it to show numbers are irrational.

6 Why are These Chapters in a DM Textbook?

- Chapters 13, 14, 16, 17, 18 are on Graph Theory and Graph Algorithms.
- Chapter 15 is on States and Invariants which is about modeling programs as graphs and looking for invariants. It reminds me of proving-programs-correct, but it does not quite get there.
- Chapters 19, 20 are on Finite Automata and Regular Languages.
- Chapter 21 is on Order Notation.
- Chapters 26-29 are on Probability, including Bayes Theorem.
- Chapter 31 is on RSA.

These are all topics that I did not cover *when I first taught the DM in 1990*. And I think I am not alone in this point of view for that time frame. I have since incorporated O-notation into the section on quantifiers, Bayes theorem (inspired by an early version of this book) into my section on probability, and RSA in my section on Number Theory, though only in the honors sections. RSA may well migrate to the standard sections at some point.

My original complaint to the publishers that they should *get rid of the material that nobody covers* is incorrect. (1) Who knows what the future may bring?, and (2) Page count is not the end-all and be-all of book pricing.

7 Opinion

The book is well written, has lots of exercises, and has all the topics (and more) that a teacher would want to cover. This is also true of other books I have used (Rosen's book and Epp's book).

So why is this book different from other books:

- The ordering of the chapters allows students to see interesting material early on.
- The book is well paced—the boring parts are shorter than in other books, and the interesting parts get to their point, make it, and shut up. Other books talk too much.
- The 31 chapters are somewhat independent making it easier for a teacher to pick-and-choose.
- The price for the hardcover edition is low. I expect that if there is a softcover version the price will be amazingly low.

Given all of the above, I highly recommend this book.

Review of[3]
Applied Number Theory
Harald Niederreiter and Arne Winterhof
Springer, 2015
442 pages, Hardcover, $44.99 on Springer Site

Reviewed by
Song Y Yan (songyuanyan2560@hotmail.com)

1 Introduction

Number theory (or the theory of numbers [1]) starts from *elementary* (not necessarily simple and easy, and in fact, it is often very hard) number theory and grows up with *analytic* number theory (including additive and multiplicative number theory), *algebraic* number theory, *geometric* number theory (including arithmetic algebraic geometry), *combinatorial* number theory, *computational* number theory (including algorithmic number theory), to name just a few. Applied number theory, on the other hand, is involved in the application of various branches of number theory to a wide range of areas including, e.g., physics, chemistry, biology, graphics, arts, music, and particularly computing and digital communications [2]. Number theory was once viewed as the purest of the pure mathematics, with little application to other areas. However, with the advent of modern computers and digital communications, number theory becomes increasingly important and applicable to many areas ranging from natural sciences, engineering to social sciences.

2 Summary of Contents

Although number theory is applicable to many areas in sciences and engineering, it is very hard to write a book to include all such applications. Rather, most of the books in the applications of number theory concentrate only on certain selected areas; this book is no exception. In fact, the book concentrates on the applications of number theory to four important areas: cryptography, coding theory, quasi-Monte Carlo methods, and pseudorandom number generation. It consists of six chapters. The first chapter presents some basic concepts and results in elementary number theory and abstract algebra (particularly Abelian groups and finite fields), that are useful in the rest of the book. Chapters 2 to 5 form the main body of the book. More specifically, Chapter 2 discusses various standard cryptographic schemes and systems, such as the secret-key cryptographic systems DES and AES, and the public-key cryptographic systems RSA and El-Gamal. Digital signatures, secret-sharing, elliptic curves, and primality testing are also mentioned in this chapter to a certain extent. Various coding schemes including linear codes and cyclic codes are introduced in Chapter 3. Chapter 4 gives an account of various quasi-Monte Carlo methods, whereas Chapter 5 gives an acount of various methods for generating random numbers in a similar way as Knuth did in his famous book [3]. The last chapter of the book discusses some other applications of number theory in, e.g., checking digits, packing sets, and quantum computing. Between 26 to 58 exercises are given at end of each chapter. There are 206 bibliographic items at the end of the book for further references.

3 Evaluation and Opinion

Two loosely related groups of topics of applications of number theory are discussed in this book: coding and cryptography, and probability and statistics. The first group of topics are standard and discussed extensive in many books, whereas the second groups of topics, particularly the variants of the quasi Monte Carlo method are less popular. The Monte Carlo method was first studied and used by Stan Ulam and John von Neumann in the 1940s. It is a statistical technique that has been successfully applied to a vast number of scientific problems and it is based on random numbers. On the other hand, the quasi Monte Carlo method tries to use the deterministic low discrepancy sequences or other similar sequences, lattices and nets generated by, e.g., numerical integrations to replace the random number sequences used in the Monte Carlo method. Number theory has an important application in producing the deterministic low discrepancy sequences ([4] and [5]) and the like. The book should be useful for researchers in number theory as a reference for applications of number theory in coding, cryptography and random computation. To adopt it as a text, one may want to supplement the first chapter with some additional information about probability, statistics, numerical integration and random computation, beyond the basic concepts of number theory and abstract algebra in that chapter. Some motivations and ideas of the quasi Monte Carlo method would also be useful. Overall, it is a good book in applied number theory and I can strongly recommend it.

4 References

[1] G. H. Hardy and E. Wright, Introduction to the Theory of Numbers, 6th Edition, Oxford University Press., 2010.

[2] M. Schroeder, Number Theory in Science and Communication, 5th Edition, Springer, 2009.

[3] D. E. Knuth, The Art of Computer Programming, Volume 2, Seminumerical Algorithms, Third Edition, Addison-Wesley, 1997.

[4] L. K. Hua and Y. Wang, Applications of Number Theory to Numerical Analysis, Springer, 1981.

[5] K. T. Fang and Y. Wang, Number-Theoretic Methods in Statistics, Chapman & Hall/CRC, 1993.

Review of[4]
Market Design: A Linear Programming Approach to Auctions and Matching
Martin Bichler
Cambridge University Press, 2018
294 pages, Hardback, $64.99 on CUP Site

Review by
S.V. Nagaraj (svnagaraj@acm.org)
VIT, Chennai Campus, India

1 Introduction

Nowadays, supply has to be matched with demand for various types of goods and services. For designing real-world markets, the study of market design becomes essential, which is the focus of this book. The book comprises four parts and consists of twelve chapters. A brief introductory chapter provides an outline of the book. The first part focuses on microeconomic fundamentals. The second part is on multi-object auction design. The third part looks at approximation and matching markets. The fourth part has appendices on linear optimization, and algorithms and complexity At the end of the book, there are references to the literature and a helpful index. Many chapters include questions for comprehension and problems for practice. The book is intended to be a textbook for a single semester course on market design. The prerequisites for the book include familiarity with linear programming, integer linear programming, rudimentary calculus and probability theory. The intended audience comprises students with backgrounds in computer science, information systems, mathematics, and management science. The book is available in hardcover and eBook formats. The ISBN/price are 9781107173187 / US $ 64.99 and 9781316805350 / US $ 52 for the hardback and eBook respectively.

2 Summary

The book comprises four parts and consists of twelve chapters.

Chapter 1 [Introduction] brings out the connections between market design and mechanism design and also between market design and mathematical optimization. This chapter includes an outline of the book which provides the readers an insight into the chapters that follow.

The first part of the book is on microeconomic fundamentals. It consists of three chapters.

Chapter 2 [Game-Theoretical Basics] introduces basic game-theoretical concepts and notions relevant to market design, which alone are the key focus of this chapter. Here the reader is introduced to normal-form games, extensive-form games, and Bayesian games along with solution concepts. The author briefly touches upon games and human behavior.

Chapter 3 [Mechanism Design] provides familiarity with the concept of social choice, utility functions,

mechanism design theory, and quasi-linear mechanism design. Market design problems may be considered as games where participants should be given incentives to reveal their preferences for objects in a truthful manner. Unfortunately, simple truthful mechanisms for general preferences are often infeasible. Hence, it becomes necessary to restrict preferences to independent and private valuations and quasi-linear utility functions, where agents maximize payoff and monetary transfers are permitted. In this chapter, we come across the celebrated Vickrey-Clarke-Groves (VCG) mechanism and the Myerson-Satterthwaite theorem. The VCG mechanism provides a general solution for designing truthful mechanisms in a quasi-linear setting. Non-quasi-linear mechanism design is also looked at briefly. The chapter also discusses robust mechanism design, algorithmic mechanism design, and dynamic mechanism design.

Chapter 4 [Single-Object Auctions] looks at different types of auction formats. An auction format describes an economic mechanism which determines the rules governing when and how a deal is closed. The auction formats discussed in this chapter include ascending auctions, first-price sealed-bid and second-price sealed-bid auctions, and descending (or Dutch) auctions. The reader is introduced to the revenue equivalence theorem, which is a key result in single-object auction theory. Other topics discussed in this chapter include risk-averse bidders, interdependent values, asymmetry of bidders, and uncertainty about the number of bidders, collusion among bidders, optimal auction design, and some experimental results.

The second part of the book focuses on multi-object design. This part comprises five chapters.

Chapter 5 [An Overview of Multi-Object Auctions] introduces multi-unit auctions (for homogeneous objects) and multi-item auctions (for heterogeneous objects). For these two types of auctions, sealed-bid and open auction formats are discussed. Open auctions include those that are continuous or organized iteratively in rounds. They can be ascending or descending but always reveal some information about competitors through the process. Multi-item auctions are also described in this chapter. Such auctions are widely used by industry for procurement, in the public sector and in logistics. The author briefly discusses online and dynamic auction designs.

Chapter 6 [The Simultaneous Multi-Round Auction Format] concentrates on a simple and widely used format known as simultaneous multi-round auction. This format offers a nice manner to introduce some problems that arise in multi-item auctions. These problems lead to the development of combinatorial auctions, which allow bidders to express all types of preferences including complements and substitutes. Thus they can be looked at as the most general type of multi-object auctions. The focus of this chapter is on rules, tactics, and strategic situations.

Chapter 7 [Sealed-Bid Multi-Object Auctions] introduces sealed-bid combinatorial auctions. It focuses on generic bid languages, the winner determination problem, payment rules, equilibrium bidding strategies, domain-specific compact bid languages, combinatorial double auctions, and empirical results. It is mentioned that the VCG mechanism may not be practical, although it leads to dominant-strategy equilibria in combinatorial auctions with payoff-maximizing bidders. There are also other reasons why the VCG mechanism may be impractical. Hence, alternative payment rules and domain-specific bid languages to address these issues are illustrated in this chapter.

Chapter 8 [Open Multi-Object Auctions] looks at open and iterative combinatorial auctions. In these types of auctions, the bidders will be able to outbid each other in a manner similar to that of English auctions. The

chapter discusses primal-dual auctions for assignment markets, greedy auctions and matroids, models of open combinatorial auctions, open combinatorial auction formats, and empirical results with markets large as well as small. In assignment markets, each bidder wants to win at most one out of several items. For these auctions, ascending auctions with dominant strategies are applicable.

Chapter 9 [The Combinatorial Clock Auction Formats] discusses the auction process and efficiency of the single-stage combinatorial clock auction format very briefly. For the two-stage combinatorial clock auction format, the auction process and the activity rules are highlighted. Experimental results are also described. These auction formats have been used for the sale of spectrum by many governments. The difficulties and problems associated with these auction formats are mentioned by the author.

The third part of the book is on approximation and matching markets. This part consists of three chapters.

Chapter 10 [Approximation Mechanisms] focuses on deterministic and randomized approximation mechanisms. The allocation problem of many real-world market design problems can be described as a combinatorial optimization problem. The VCG mechanism provides dominant strategies only if the allocation problem can be solved exactly. This is often infeasible for many real-world problems. Hence, the only recourse is approximation mechanisms. They solve the allocation problem in polynomial time within a certain approximation ratio.

Chapter 11 [Matching Markets] provides an overview of matching problems, one-sided matching, two-sided matching, one-sided matching with complementarities, and applications and empirical results.

Chapter 12 [Outlook] is very brief. It discusses challenges in market design and the road ahead.

The fourth part of the book comprises brief appendices on linear optimization, and algorithms and complexity.

3 Opinion

The book includes some basics from game theory and focuses on auctions and matching. It takes a mathematical programming approach to market design. The author Martin Bichler has made many contributions to market design, auctions, electronic commerce, and related disciplines. Thus he is uniquely placed in authoring this book. Bichler has published two other books related to market mechanisms: The Future of e-Markets: Multidimensional Market Mechanisms, 2001, Cambridge University Press, ISBN 9780521003834 and Handbook of Spectrum Auction Design, 2017, Cambridge University Press, ISBN 9781107135345. These books are also relevant and worth reading. The design of spectrum auctions involves the application of game theory and auction theory. Various auction formats have been invented for dealing with basic questions about efficiently selling multiple objects to a group of buyers. Some of these are discussed in this book. In addition to scholarly work, Bichler has also done consultancy for various organizations. He is known for his work on design of auctions for advertising, industrial procurement, logistics, fishery access rights, and spectrum sales agreements. Bichler has also been involved in the development of several software packages, which have been or are being used by industries. This book by Bichler is very readable and suitable for various types of courses such as those for advanced undergraduate and entry level graduate students. It will

serve its intended purpose as a textbook for students with backgrounds in computer science, information systems, mathematics, and management science, apart from other disciplines such as economics and operations research. The questions for comprehension and problems for practice at the ends of chapters will aid this. In addition to students for whom the book is intended, I feel it will also be useful for other categories of readers such as bidders, consultants, market designers, regulators, professionals, and researchers.