The Book Review Column[1]

by William Gasarch
Department of Computer Science
University of Maryland at College Park
College Park, MD, 20742
email: gasarch@cs.umd.edu

In this column we review the following books.

1. **From Zero to Infinity: What Makes Numbers Interesting** by Constance Reid. Review by Vaishak Belle. The book is an informal (non-technical) introduction to the lore of natural numbers. It benefits a general audience, and those with an inclination for an appreciation of general mathematical lore in particular. Advanced readers may also be challenged.

2. **Mathematics for the Analysis of Algorithms** by Daniel H. Greene and Donald E. Knuth. Review by Mladen Miksa. To determine how fast an algorithm runs you may need to do some hard math. This classic book presents a diverse set of mathematical paradigms used for solving these problems.

3. **Algebraic Cryptanalysis** by Gregory V. Bard. Review by Joseph Fitzsimons. This book is about the branch of cryptanalysis which is tied to areas of computational complexity and finite-field algebra. The book focuses on attacks which can be constructed when given matching pairs of plain-text (unencrypted messages) and their corresponding cipher-text (the corresponding encrypted messages).

4. **Algebraic Function Fields and Codes** by Henning Stichtenoth. Reviewed by Swastik Kopparty. This book gives a rigorous, systematic and thorough treatment of the theory of algebraic function fields and its applications in coding theory. Algebraic function fields are natural objects that arise in the study of algebraic curves and exponential sums over finite fields, and have found widespread applications in the areas of coding theory and pseudorandomness.

5. **Those Fascinating Numbers** by Jean-Marie De Konick. Review by William Gasarch. When I wrote the review the book was selling on amazon for $37.80. The book tells me that 378 is the smallest number which is not a cube but which can be written as the sum of the cubes of its prime factors. If you like this sort of thing you will like this book.

6. **Pólya Urn Models** by Hosam Mahmoud. Review by Stephen Stanhope. If an Urn has 99 red balls, 810 white balls, and 80 blue balls then what is the probability that a white ball is taken. This is easy. But what happens if you pick without replacement and ask asymptotic questions? Many interesting questions can be asked and answered in this model.

7. **Not always buried deep: a second course in elementary number theory** by Paul Pollack. Reviewed by S. C. Coutinho. In a first course in number theory you learn things like *a prime p is the sum of 2 squares iff the $p \equiv 1 \pmod 4$* and you hear mentioned harder theorems like *an infinite arithmetic progression $a, a+d, a+2d, \ldots$ (where $gcd(a,d) = 1$) has an infinite number of primes*. This book is for that second course where you actually prove these theorems.

8. **Pioneering Women in American Mathematics: The Pre-1940 PhD's** by Judy Green and Jeanne LaDuke. Review by Sorelle A. Friedler. This is a comprehensive examination of the lives of all 228 women who earned PhDs in mathematics before 1940 who were US-born or earned their PhDs in the US.

9. **A Guide to Elementary Number Theory** by Underwood Dudley. Reviewed by Song Yan. This is not quite a text on number theory. It is, as the title says, a guide. It is 39 chapters of varying lenghts each devoted to a single question about numbers.

10. **Mathematical Tools for Data Mining: Set Theory, Partial Orders, Combinatorics** by Dan A. Simovici and Chabane Djeraba. Reviewed by Pauli Miettinen. A sutdent, or even a researcher, in Data Mining may find that they need to know some math that they do not know. This book intends to fill that gap.

BOOKS I NEED REVIEWED FOR SIGACT NEWS COLUMN
Algorithms and Related Topics

1. *Combinatorial Pattern Matching Algorithms in Computational Biology Using Perl and R* by Valiente.

2. *Triangulations: Structure for Algorithms and Applications* by De Loera, Rambau, Santos.

3. *Proofs and Algorithms* by Gilles Dowek.

4. *Flows in Networks* by Ford and Fulkerson. (the classic reprinted!)

5. *Fast Algorithms for Signal Processing* by Blahut.

6. *Bioinspired Computation in Combinatorial Optimization* by Neumann and Witt.

7. *Modern Computer Arithmetic* by Brent and Zimmermann.

Cryptography, Coding Theory, Security

1. *Locally Decodable Codes and Private Information Retrieval* by Yekhanin.

2. *The Cryptoclub: Using Mathematics to Make and Break Secret Codes* by Beissinger and Pless (for middle school students).

3. *Mathematical Ciphers: From Ceaser to RSA* by Anne Young. (For a non-majors course.)

4. *Adaptive Cryptographic Access Control* by Kayem, Akl, and Martin.

5. *Preserving Privacy in data outsourcing* by Sara Foresti.

6. *Cryptanalysis of RSA and its variants* by Hinek.

7. *Algorithmic Cryptanalysis* by Joux.

Math

1. *Polynomia and Related Realms* by Dan Kalman.

2. *Mathematica: A problem centered approach* by Hazrat.
3. *Mathematics Everywhere* Edited by Aigner and Behrends.
4. *Mathematical Omnibus: Thirty Lectures on Classic Mathematics* by Fuchs and Tabachnikov.
5. *Probability Theory: An Analytic View* by Stroock.
6. *The Dots and Boxes Game: Sophisticated Child's play* By Berlekamp.
7. *New Mathematical Diversions* by Martin Gardner.
8. *The Magic Numbers of the Professor* by O'Shea and Dudley.
9. *Kurt Godel: Essays for his Centennial* by

Misc-Comp Sci

1. *Quantum computing: A gentle introduction* by Rieffel and Polak.
2. *Foundations of XML Processing: The Tree-Automata Approach* by Haruo Hosoya.
3. *Introduction to Computational Proteomics* by Yona.
4. *Introduction to the Theory of Programming Languages* by Dowek and Levy.
5. *Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics* by Platzer.
6. *Digital Nets and Sequences: Discrepancy theory and Quasi-Monte Carlo Integration* by Josef Dick and Friedrich Pillichshammer.
7. *Approximation and Computation: In Honors of Gradimir Milovanovic* Edited by Gautchi, Mastoianni, Rassias.
8. *Clustering in Bioinformatics and Drug Discovery* by MacCuish and MacCuish.
9. *Drawing Programs: The theory and Practice of Schematic Functional Programming* by Addis and Addis.

History of Math

1. *History of Mathematics: Highways and Byways* by Amy Dahan-Dalmedico and Jeanne Peilfer.
2. *An Episodic History of Mathematics: Mathematical Culture through Problem Solving* by Steven Krantz.

Review of
From Zero to Infinity: What Makes Numbers Interesting
by Constance Reid
A K Peters, Ltd. 2006
208 pages, Softcover, $19.95 as a book, $9.95 in Kindle

Review by
Vaishak Belle; belle@cs.rwth-aachen.de
Blondelstr. 28, 52062 Aachen, Germany

1 Introduction

The book is an informal (non-technical) introduction to the lore of natural numbers. It benefits a general audience, and those with an inclination for an appreciation of general mathematical lore in particular. Advanced readers are invited to tackle puzzles at the end of each chapter.

2 Summary

It would be difficult for anyone to be more profoundly interested in anything than I am in the theory of primes. - G. H. Hardy (see book).

From Zero to Infinity by Constance Reid has been inspiring the mathematically keen for over 50 years now. Written in informal style, the book offers an introduction to the beauty of natural numbers. It is organized into 12 chapters, with a chapter each for the first ten natural numbers. A special chapter is dedicated to the Euler identity, and another one to Aleph-0. Tracing the discovery of the numbers, the chapters expand upon features and facts, all of which tells us why these numbers are interesting. While perhaps many of such facts can be found in elementary undergraduate texts, it nonetheless attempts a holistic picture describing relations between prime, composite, perfect, rational and irrational numbers.

As the author explains in the preface, the book has a story. The advent of computers enabled the discovery of a new set of *perfect numbers*, which started the chapters. While it may be hard to imagine how a whole chapter could be written about the most common of numbers, the author does so in a very satisfactory manner. The chapters usually end with some notes, open problems and hints about these problems. The reader is often encouraged to tackle them, and not all are that elementary!

The discovery of "0" is perhaps well known. It is also known that it serves as an important identity. The chapter introduces the modern *positional notation*, and goes to explain why this number is so important. Chapter "1" serves to form the foundation of natural numbers, via addition, and also enables discussions about factorization. Chapter "2" not surprisingly speaks of the binary notation, its significance and introduces a novice reader to binary addition and multiplication. Chapter "3" talks about primes and chapter "4" talks about squares. In there, the readers gets a first feeling with notions of infinity. In particular, the author helps us to reason about what it means to say that a set is infinite: *A set is infinite when it can be placed in one-to-one correspondence with a part of itself.* Also discussed in this chapter is the Pythagorean Theorem and Fermat's Last Problem.

Chapter "5" takes us through Euler generating functions. The motivation for this function lies in the theory of partitions. For instances, in how many ways can you define the number 5 as the sum of one, two, three, four or five numbers? It is easy to verify that there are 7 possibilities. Partitioning the number 6 leads

to 11 possibilities, and continuing this further shows that there is no apparent relation between the number and the cardinality of its partitions. Euler's function sheds light on this theory. Chapter "6" takes us through how large primes can be found, and why people think this search is important. This can be understood as follows. The number 6 is a perfect number, that is the sum of all its divisors except itself $(3, 2, 1)$. So how many perfect numbers are there? Euclid claimed that all numbers of the form $2^{n-1} \times (2^n - 1)$ are perfect, but provided $2^n - 1$ is prime. The search for perfect numbers inevitably lead to the search for primes. Chapter "7" talks about Fermat primes, and chapter "8" introduces Waring's suggestion. What this states is that every (natural) number can expressed as the sum of 4 squares, 9 cubes, 19 biquadrates and so on. Of course, the number 8 brings to mind cubes, and so Waring's claim can be seen as an extension to two dual questions about numbers: how can cubes be represented as other natural numbers, and how can natural numbers be represented as the product or sum of cubes? Mainly, what is the maximal number of cubes one needs to represent in terms of a sum any given natural number? Finally, chapter "9" returns to the theme of notations.

The chapter on the Euler identity is well explained. It offers a clean introduction to the natural logarithm, explaining what sort of conceptual breakthrough came about with its discovery. Also discussed are the imaginary numbers. Coming to the last chapter, this is arguably the most difficult theme to present in a simple language, and this is where the author does well. Discussing the controversy that Cantor's discovery created in the mathematical circles, the author goes on to explain the diagonalization argument among other things. All is all, a very accurate summarization of the theory of the infinite is given. I believe readers will certainly be compelled to obtain copies of her other books, such as the one on David Hilbert.

It is interesting to note that Constance Reid has no formal education is mathematics, and yet her books could not be any more lucid.

3 Opinion

The book is well written, uses an informal languages, and serves as a great introduction to the theory of numbers, known facts about them and the history of this discovery.

Review of
Mathematics for the Analysis of Algorithms [2]
Authors: Daniel H. Greene and Donald E. Knuth
Publisher: Birkhauser, 2008, ISBN: 978-0-8176-4728-5
132 pages, Softcover, $40

Reviewer: Mladen Miksa (`mladen.miksa@fer.hr`)

1 Overview

When designing an algorithm it is important to know how well it will perform at a given task. In order to answer that question, we define mathematical equations that describe the relation between performance and input. Most of the time we are interested in the explicit form of that relation, but finding such a form can be a difficult task. *Mathematics for the Analysis of Algorithms* by Daniel H. Greene and Donald E. Knuth presents a diverse set of mathematical paradigms used for solving those equations.

2 Summary of Contents

The book consists of four thematically separated chapters covering: binomial identities, recurrence relations, operator methods and asymptotic analysis. The last third of the book contains exams given at Stanford and their solutions, providing additional examples for presented topics. It consists of three midterm and three final exams along with one additional problem.

This summary gives a short description of the chapters and is not intended as a comprehensive list of everything described in the book.

2.1 Chapter 1: Binomial Identities

This chapter is relatively short and to the point. It starts with a summary of useful identities and then proceeds to the description of "meta" concepts used in classifying binomial identities (e.g. inverse relations), ending with another list of identities, this time involving harmonic numbers. Some ideas for proving the identities are explained, but the reader is mostly referred to other sources for additional information on the subject.

2.2 Chapter 2: Recurrence Relations

Methods for solving recurrence relations are described in this chapter. They are divided into two major categories: linear and nonlinear relations.

The part describing linear relations presents additional subdivisions of types of relations, starting with easier ones and progressing to those more challenging. It describes finite and full history relations with solving techniques varying from trying trial solutions to the repertoire approach.

The division of nonlinear relations is not as detailed as that of their linear counterparts, owing to the fact that the methods for solving them are less systematic, as mentioned in the book. Relations covered in this part include relations with maximum or minimum functions, and relations with hidden or approximate linear recurrences.

2.3 Chapter 3: Operator Methods

Another relatively short chapter presents operator methods and their use in the analysis of algorithms. Through various examples it demonstrates the use of operators in removing recurrence from equations. The removals are achieved using a variety of tricks, all of them relying on moving through the recurrence using a self-replicating process (e.g. eigenoperator).

One other key concept used in this chapter is *induction at the other end*, a form of induction where new elements are added to the beginning of the sequence, rather than the end.

2.4 Chapter 4: Asymptotic Analysis

A lot of times the solutions to the recurrences can not be expressed in a closed form, so effort is instead turned to finding an asymptotic solution. This chapter covers techniques used in finding those solutions and is divided into three parts: basic concepts, the use of Stieltjes integration and recovering asymptotic solutions from generating functions. The emphasis is on as thorough approximations of the exact solution as possible, trying to find the approximation with the smallest error term.

The basic concepts starts with briefly describing O-notation, moving its way through several other topics and ending with Tauberian theorems. The part on the use of Stieltjes integration gives its definition and relation to asymptotics with additional attention given to Euler's summation formula. The last part uses generating functions to recover asymptotics and covers Darboux's method for functions with singularities, and the saddle point method for functions without them.

Each of three parts is followed with an example which uses the techniques described in it. The first two examples that are presented come from factorization and number theory, while the last example is a proof of the central limit theorem.

3 Opinion

Mathematics for the Analysis of Algorithms covers a variety of topics in a relatively small amount of pages. Despite its briefness, most of the topics are clearly and fully explained using detailed examples for better understanding. As such, the book is suitable for use as a study material, as well as a good reference guide.

The focus of the book is placed on advanced techniques described in chapters three and four, and the later parts of chapter two. Those chapters are mostly driven by detailed examples which give a clear presentation of the use of techniques described in each of them. Following the emphasis, the first few chapters are explained less thoroughly with no or just brief examples presented.

Familiarity with the basic concepts in combinatorics and complex analysis is assumed in the book. Some of them are explained, but only briefly and in passing to more advanced methods. On some occasions it may require more than just the basics and additional knowledge could help, but nothing too difficult that can not be easily looked up from other sources.

The book presents mathematics used in the analysis of algorithms; it does not describe them any more than it is necessary for the analysis. The intention of it is to be an addition to other books on algorithms, namely *The Art of Computer Programming* series by Donald E. Knuth which is referenced a lot. Even without the other books it can still provide an interesting read, although it can sometimes present problems with the understanding of the material, depending on the reader's prior knowledge of the properties of mentioned algorithms. More can certainly be gained from it if used with other references, and that is what the author of this review would recommend.

Many summations in the chapter on binomial identities and some of recurrences in the second chapter can now be automatically solved using available mathematical software. That makes those parts less relevant for the analysis of algorithms, but the focus of those chapters is more on the basic ideas (rather than detailed methods) and they are relatively short containing some insights that could still provide an enjoyable read.

The reviewer recommends this book to anyone interested in advanced theory of algorithms and the mathematics behind it, either as an exposition to the topic or as reference material in future work.

Review of[3]
Algebraic Cryptanalysis
by Gregory V. Bard
Published by Springer, 2009
356 pages, Hardcover

Review by
Joseph Fitzsimons (joe.fitzsimons@gmail.com)
Merton College, Merton Street, Oxford OX1 4JD, UK

> "Few false ideas have more firmly gripped the minds of so many intelligent men than the one that, if they just tried, they could invent a cipher that no one could break."
> — David Kahn, *The Code Breakers*.

1 Introduction

Throughout its history, computer science has been inextricably linked with code-breaking. Charles Babbage, a pioneer in the field of mechanical computation in the mid-19^{th} century and inventor of the first Turing-complete mechanical computer, is credited with breaking the Autokey and Vigenère ciphers. Turing himself spent the years of World War Two working in the Government Code and Cypher School at Bletchley Park, where he contributed to the breaking of the Enigma and Lorenz ciphers. It should come as no surprised then that cryptography and cryptanalysis, the making and breaking of ciphers, are still closely tied to the study of computational complexity. *Algebraic Cryptanalysis* focuses on a particular form of cryptanalysis which is particularly closely tied to areas of computational complexity and finite-field algebra. The book focuses on attacks which can be constructed when given matching pairs of plain-text (unencrypted messages) and their corresponding cipher-text (the corresponding encrypted messages). These are by no means the most general attacks, but do have the advantage of allowing the relationship between these pairs to be expressed as a system of polynomial equations which include the encryption key as variables. Thus a number of constraints exist, which if sufficiently many pairs are used can be simultaneously satisfied only by the correct encryption key. The goal of this book is to show how such constraints can be generated given the specification of a cipher, and to demonstrate how such constraint problems can be solved, either via computer algebra techniques or by translating to instances of the conjugate normal form satisfiability problem.

2 Summary

The book is arranged into three parts, each consisting of a number of chapters. Part I covers the topic of converting a cipher into a system of polynomial equations over a finite field; Part II covers various aspects of the algebra of finite fields and complexity theory; finally Part III covers algorithmic methods for solving systems of equations as generated in Part I. The division between parts is relatively clear, although the chapters within each part often cover quite disparate topics. As such it makes sense to cover the contents of each chapter separately, with the exception of Chapter 1, which merely outlines the structure of the book.

[3]

2.1 Part I: Cryptanalysis

Part I of the book focuses on generating systems of simultaneous equations from the description of a cipher. Much of this section is based on the author's own work on the Keeloq cipher, which is used as an example throughout the early chapters. As a result, it is helpful to print a copy of the authors PhD thesis[4] which covers much of the material used in the book and which can be used as a reference while working through Part I.

2.1.1 Chapter 2: The Block Cipher Keeloq and Algebraic Attacks

In this chapter the reader is first introduced to the Keeloq cipher. The reader is then taken step by step through the process of generating a system of polynomial equations from the specifications of Keeloq. The chapter concludes with a discussion of the failure of attempts to directly solve the equations generated in this way.

2.1.2 Chapter 3: The Fixed-Point Attack

This chapter describes an attack on Keeloq taken from the authors PhD thesis. The attack works by exploiting the structure of Keeloq to express it in a particular form, such that at its heart there is a new function $f(x)$ which is iterated eight times. The attack proceeds by trying to identify fixed points of $f(x)$, and then using a pair of such fixed points to provide the constraints used to generate a system of polynomials which is then solved algorithmically.

2.1.3 Chapter 4: Iterated Permutations

Chapter 4 is quite long, and has two distinct parts. The first half of the chapter forms a general introduction to the field of analytic combinatorics, while the second half of the chapter examines attacks arising when a particular operation is applied recursively a large number of times within a cipher.

2.1.4 Chapter 5: Stream Ciphers

This part of the book concludes with a discussion of stream ciphers. In a stream cipher the plain-text is encrypted by combining with a pseudo-random bit stream in such a way that the cipher-text generated by a given piece of plain-text depends on the current state of the encrypting device. The main focus of this chapter is simply on generating systems of polynomials from the initial description of the cipher. In particular the author highlights the Bivium, Trivium and QUAD ciphers.

2.2 Part II: Linear Systems Mod 2

Part II of the book contains chapters on a variety of topics, for the most part related to the complexity of linear algebra over $\mathbb{GF}(2)$. For those unfamiliar with it, $\mathbb{GF}(2)$ is the Galois Field of 2 elements. The field's addition and multiplication operations correspond to bitwise XOR and AND respectively, and so $\mathbb{GF}(2)$ provides a convenient representation for systems described in terms of Boolean operations.

[4] Currently available at http://www-users.math.umd.edu/∼bardg/

2.2.1 Chapter 6: Some Basic Facts about Linear Algebra over $\mathbb{GF}(2)$

This chapter acts as an introduction to linear algebra over $\mathbb{GF}(2)$. It is clearly aimed at the reader familiar with linear algebra over $\mathbb{R}$ or $\mathbb{C}$, and simply highlights important differences between $\mathbb{GF}(2)$ and the more familiar cases.

2.2.2 Chapter 7: The Complexity of $\mathbb{GF}(2)$-Matrix Operations

In this chapter the author introduces a new complexity measure for matrix operations on $\mathbb{GF}(2)$. The reason for this is that, traditionally, counting floating point operations has served as a proxy for time complexity when analysing operations on real or complex matrices, significantly simplifying calculations. For operations over $\mathbb{GF}(2)$, however, there is no need for floating point operations, and so another proxy is desirable. The scheme the author introduces is simply to count memory operations. The scheme is outlined and the limitations discussed.

2.2.3 Chapter 8: On the Exponent of Certain Matrix Operations

Chapter 8 collects a number of theorems proving that many important matrix operations have equivalent computational complexity to matrix multiplication. These include matrix inversion and squaring, as well as LUP-factorization and inversion of triangular matrices. This is particularly useful, as using these results such operations can be constructed directly from matrix multiplication. A number of algorithms are known for matrix multiplication, and so there is a choice available. One might expect that the best choice is simply to choose the option with the smallest asymptotic scaling. This is however not the case as in practice the cross-over can occur at extremely large matrix sizes and so the choice is either between algorithms of cubic complexity, Strassen's algorithm or the Method of Four Russians described in the Chapter 9.

2.2.4 Chapter 9: The Method of Four Russians

This chapter introduces a method of matrix multiplication known as the Method of Four Russians (M4RM), and makes use of it to create an algorithm for matrix inversion, which the author calls the Method of Four Russians for Inversion (M4RI). Both algorithms run in time $O(n/\log(n))$, and so do not out-perform Strassen's algorithms. However, the author proposes these be used as the fall-back algorithm in Strassen's algorithm, since it works by recursively dividing up matrices into smaller matrices until a threshold size is reached. These small matrices are then naively multiplied, and so by using M4RM and M4RI a constant speed-up can be achieved.

2.2.5 Chapter 10: The Quadratic Sieve

Chapter 10 stands out from the rest of the book. It introduces the RSA cryptosystem and focuses on two distinct algorithms for integer factorization, namely the linear and quadratic sieves. With its number theoretic underpinnings, RSA differs greatly from the block and stream ciphers discussed earlier in the book and so a number of results are imported from number theory in order to construct these algorithms.

2.3 Part III: Polynomial Systems and Satisfiability

The final part of the book focuses on methods for algorithmically solving systems of polynomial equations as generated earlier in Part I. Initially the focus is on computer algebra techniques, though the focus rapidly

changes to SAT-solvers with which the final three chapters are concerned.

2.3.1 Chapter 11: Strategies for Polynomial Systems

This chapter begins Part III with a look at techniques used to make systems of polynomial equations over finite fields more amenable to the computational approaches used later in the book. In particular the author introduces techniques for reducing the degree of polynomials encountered, as well as discussing the utility of guessing the value of particular variables and the consequences for running time of solvers of having over-defined variables.

2.3.2 Chapter 12: Algorithms for Solving Polynomial Systems

Chapter 12 introduces an number of algorithms for solving systems of equations. By necessity, these algorithms have poor worst case run times, as solving such problems is known to be NP-complete. The most widely studied class of such algorithms, those based on finding Gröbner bases, is only mentioned in passing and it is suggested that the reader use the implementations built into already existing computer algebra systems. Instead the main focus is on algorithms based on linearisation of the polynomials, which appear to be a more practical choice for cryptanalysis problems.

2.3.3 Chapter 13: Converting MQ to CNF-SAT

The focus of this chapter is on converting $\mathbb{GF}(2)$ systems into instances of the conjugate normal form satisfiability problem (CNF-SAT). CNF-SAT has been studied in great detail in its own right, and a number of good heuristic algorithms exist. The reader is walked through the conversion, which is then followed by a discussion of running times.

2.3.4 Chapter 14: How do SAT-Solvers Operate?

Chapter 14 provides a detailed introduction to the world of SAT-solvers. SAT-solvers are often used as a black box, but this chapter provides an interesting look under the hood of such algorithms. A number of different approaches to SAT are introduced and the algorithms underlying some prominent solvers are examined, with a view to fostering some understanding of what constitute easy and difficult instances.

2.3.5 Chapter 15: Applying SAT-Solvers to Extension Fields of Low Degree

Chapter 15 closes off the main text with a discussion of how to use SAT-solvers in conjunction with systems over $\mathbb{GF}(2^k)$ for low k, by converting them to $\mathbb{GF}(2)$ systems. For many cryptosystems this is a more natural form than working directly with a Boolean representation, and so this is a fitting way in which to conclude the book.

2.4 Appendices

Algebraic Cryptanalysis also contains a total of five appendices, which vary widely in their utility. Appendix A contains a discussion of the security of block ciphers with extremely small block sizes. This is an important inclusion, as the security of a cipher does not only depend on the difficulty of solving the relevant constraint satisfiability problems, but also on the practicality of other attacks, such as frequency analysis,

which become important at small block sizes. Appendix B contains explicit formulae for field multiplication laws for $\mathbb{GF}(4)$, $\mathbb{GF}(8)$, $\mathbb{GF}(16)$, $\mathbb{GF}(32)$ and $\mathbb{GF}(64)$. Appendix C extends the approaches taken in the book to tackle the task of graph colouring, in which vertices on a graph have to be assigned one of c different colours in such a way that no two neighbouring vertices have the same colour. The general forms of both the constraint satisfiability problems discussed in the main text and the graph colouring problem are NP-complete, and so the author reasons that the approaches outlined in the main text can be translated to problems outside of cryptanalysis which are expressible as graph colouring problems. Indeed this appendix concludes with a number of example applications. Appendix D contains a review of fast algorithms for the manipulation of sparse matrices. This makes a useful reference for anyone wishing to implement the cryptanalysis techniques discussed in the main text. The book concludes with Appendix E which contains three quotes from Robert Recorde which the author considers inspirational, and are apparently the compromise he has come to between continuing the tradition of starting each chapter with a quote[5] and the difficulty imposed by having an insufficient supply of suitable quotations. Finally, *Algebraic Cryptanalysis* also contains a detailed bibliography, which the author has been careful to cite from throughout the text.

3 Opinion

This book aims to appeal to graduate students moving into the area of algebraic cryptanalysis, as well as to researchers from other areas of cryptography and computer algebra. The book is well written in a discursive style that makes it quite accessible, and so I believe that *Algebraic Cryptanalysis* will be a welcome addition to the bookshelves of anyone with an intrest in code-breaking. There is however one small caveat: This book is clearly not intended to be a definitive guide to the subject, and tends to focus on general principles illustrated with specific examples. There is little discussion of the different kinds of cryptanlytic attacks frequently encountered or of techniques such as linear and differential cryptanalysis which have become common-place. Unusually for a book of this type, there is also no discussion of attacks on historical ciphers. One additional concern is that the complexity measure introduced in Chapter 7 seems to conflate space and time in a way that will potentially cause trouble in the context of time-memory tradeoffs common in cryptanalysis, and so should be taken with a grain of salt. With this in mind, however, *Algebraic Cryptanalysis* would make an excellent second book for anyone with an interest in the area. The discussion of algorithms goes far beyond what is normally encountered in such books, which together with the wealth of examples taken from real cryptosystems and the in-depth coverage of SAT-solvers and finite-field algebra provides an excellent way to deepen the readers existing knowledge.

[5] As mentioned on page 6 of *Algebraic Cryptanalysis*.

Review of
Algebraic Function Fields and Codes [6]
Author: Henning Stichtenoth
Publisher: Springer, 2009
ISBN: 978-3-540-76877-7, $59.95
Graduate Texts in Mathematics, 254

Reviewer: Swastik Kopparty (swastik@mit.edu)

1 Overview

The book being reviewed, "Algebraic Function Fields and Codes" by Henning Stichtenoth, gives a rigorous, systematic and thorough treatment of the theory of algebraic function fields and its applications in coding theory. Algebraic function fields are natural objects that arise in the study of algebraic curves and exponential sums over finite fields, and have found widespread applications in the areas of coding theory and pseudorandomness.

This is the second edition of a book that is already one of the standard references in the area of algebraic-geometry codes. The new edition features a new chapter on curves with many rational points, as well as a large number of exercises at the end of every chapter. The new chapter is a particularly welcome addition, since the book now contains an explicit construction and complete analysis of excellent error-correcting codes that beat random codes (which is one of the most celebrated applications of the theory of algebraic function fields to coding theory and theoretical computer science).

Below we will give a short introduction to algebraic function fields and a brief description of one of their major applications in coding theory We will then proceed to discuss the contents of this book.

1.1 Algebraic function fields

The abstract algebraic theory of function fields was first studied by Dedekind, Kronecker and Weber in the 1880s, when they noticed many formal similarities between the theory of number fields and the theory of algebraic functions on complex algebraic curves. Since then, it has seen much activity and developed into a flourishing theory in the hands of E. Artin, F. K. Schmidt, H. Hasse, A. Weil, C. Chevalley and others.

Formally, an algebraic function field over a base field $\mathbb{F}$ is a field of transcendence degree 1 over $\mathbb{F}$. In practice, the notion of an algebraic function field arises naturally as a generalization of the field of rational functions $\mathbb{F}(X)$ over a field $\mathbb{F}$:

$$\mathbb{F}(X) = \left\{ \frac{f(X)}{g(X)} \;\middle|\; f(X), g(X) \text{ polynomials with coefficients in } \mathbb{F}, \text{ and } g(X) \neq 0 \right\}.$$

An *algebraic function field* is simply a finite algebraic extension field of $\mathbb{F}(X)$, and the elements of this field are called algebraic functions. For example, the field

$$\mathbb{L} = \mathbb{F}(X)[Y]/\langle Y^2 - X^3 + 2X + 1 \rangle$$

is an algebraic function field. The rational function field $\mathbb{F}(X)$ is naturally viewed as the field of rational functions on a *line*. Analogously, an algebraic function field arises as the field of rational functions on a

one-dimensional algebraic curve. For example, the field $\mathbb{L}$ is the field of rational functions on the curve in $\mathbb{F}^2$ defined by $Y^2 = X^3 - 2X - 1$.

The theory of algebraic function fields sets up a rich and beautiful theory of polynomials and rational functions on every algebraic curve. It enables us to formulate and answer questions such as: How many roots can a "low-degree algebraic function" have? What is the dimension of the space of "low-degree algebraic functions"? The theory then allows us to go back and answer basic questions (that make no mention of the algebraic function field) about algebraic curves themselves: how many points in $\mathbb{F}^2$ lie on a given algebraic curve? For instance, if $\mathbb{F}$ is a finite field with q elements, it turns out that the number of solutions to $Y^2 = X^3 + 2X + 1$ in $\mathbb{F}^2$ lies in the interval $[q - 2\sqrt{q}, q + 2\sqrt{q}]$, which is a *highly* non-trivial fact derived from the theory of the algebraic function field $\mathbb{L}$.

We now highlight two of the results coming from the theory of algebraic function fields (and proved in this book) that have been especially impactful in coding theory and theoretical computer science. The first is the Hasse-Weil theorem on the number of solutions to polynomial equations over finite fields, which plays an important role in pseudorandomness, coding theory and cryptography. The second result is the Ihara-Tsfasman-Vladut-Zink Theorem on the existence of curves with many rational points and low genus, which plays an important role in the construction of excellent error-correcting codes. In the next subsection, we briefly describe this second application.

1.2 Algebraic-geometry codes

One of the outstanding problems in the theory of error-correcting codes is to determine the size of the largest set C of n-letter strings over a q-ary alphabet, such that every pair of elements in C differs in at least δn coordinates. A large set C with this property (an "error-correcting code") can be used to protect data against error as follows: a unique codeword in C is associated to each q-ary string of length $\log_q |C|$. Any given q-ary string of length $\log_q |C|$ is represented using its associated codeword; now even if a $\delta/2$ fraction of the coordinates of this representation get corrupted, the uncorrupted codeword (and hence the original data) is still uniquely determined.

The tradeoff here is between the efficiency of the encoding, measured by the rate $R = \frac{\log_q |C|}{n}$, and the relative distance δ of the code. One is interested in determining the best tradeoff between rate and relative distance for arbitrarily long codes, i.e., as $n \to \infty$.

In the 1950s, several different constructions of codes were proposed that all achieved the best-known tradeoff between rate and distance (meeting the so-called Gilbert-Varshamov bound). For a long time, many believed that these codes had the optimal tradeoff between the rate R and distance δ, but a proof was elusive. Another concern was that all these constructions were not explicit: some of these constructions were randomized, while others were inefficient (membership in C took time $\exp(n)$ to decide). The quest for explicit codes at least as good as random codes was also stuck for a long time.

And then in the 1980s, algebraic-geometry codes announced themselves with a bang: there are *explicit* codes which achieve a *better* tradeoff between rate and relative distance than the random code!

We begin by describing a classical code, the Reed-Solomon code, associated with the simplest algebraic function field $\mathbb{F}(X)$. Generalizing this to more general algebraic function fields yields algebraic-geometry codes. The Reed-Solomon code over $\mathbb{F}_q$ is given by the following data: (1) a collection of "evaluation points" $\alpha_1, \ldots, \alpha_n$ in $\mathbb{F}_q$, and (2) a degree bound m. The codewords are indexed by polynomials of degree at most m; the codeword corresponding to the polynomial $p(X)$ is the vector $(p(\alpha_1), p(\alpha_2), \ldots, p(\alpha_n))$. This code clearly has rate = $(m + 1)/n$, and has relative distance $(n - m)/n$, since two polynomials of degree $\leq m$ can agree on at most m points (or else their difference, which is also of degree at most m,

would have more than m roots).

However, the Reed-Solomon code has a basic limitation: because of the need to pick n distinct points from $\mathbb{F}_q$, we must have $n \leq q$. In particular, this construction does not[7] directly give codes of arbitrarily long length for a fixed q.

In the late 1970s, Goppa suggested an elegant way of getting longer codes by generalizing this construction to arbitrary one-dimensional algebraic curves in place of the line. These lead to algebraic-geometry codes. Then in the early 1980s, Tsfasman-Vladut-Zink showed that by specializing this construction to a certain remarkable family of algebraic curves (a family independently studied by Ihara), one can get excellent error-correcting codes beating the Gilbert-Varshamov bound.

An algebraic-geometry code over an algebraic curve C is given by the following data: (1) a collection of evaluation points $P_1, \ldots, P_n$ on C, and (2) a degree bound m. The codewords of this code are indexed by "algebraic functions of degree at most m" on C. The rate of this code can be calculated by understanding the dimension of the space of algebraic functions of degree at most m. The relative distance of this code can be calculated by understanding the number of roots that an algebraic function of degree at most m can have. Finally, one wants to choose the curve C so that the above calculations lead to excellent codes.

The basis for all this, and much much more, is provided by the theory of algebraic function fields. We now describe the contents of the book.

2 Summary of Contents

Chapter 1 gives an introduction to algebraic function fields over a base field $\mathbb{F}$ and proves some basic results about them. The chapter begins by defining valuation rings and places of an algebraic function field. The places of an algebraic function field correspond to the points of the underlying algebraic curve; the *rational* places correspond to the $\mathbb{F}$-points of that curve. Thus, from an algebraic function field one can recover the points of an algebraic curve, and one can speak of evaluating the algebraic functions at points (places) of the algebraic curve. The important notions of vanishing-order and degree of an algebraic function are introduced. This leads us into the definition of a Riemann-Roch space (which is the analogue of the space of low-degree univariate polynomials in $\mathbb{F}(X)$). We then see a proof of the fundamental Riemann-Roch theorem, which calculates the dimension of Riemann-Roch spaces. In the process, we get introduced to the *genus* of a function field, which quantifies how different the function field is from the rational function field $\mathbb{F}(X)$. We also get introduced to *adeles* and *Weil differentials*, both of which are elegant algebraic constructs which capture the local-to-global phenomena in the underlying algebraic curve, and are of fundamental importance to the rest of this book.

Chapter 2 deals with coding theory. It begins by introducing error-correcting codes. We then get introduced to two general constructions of algebraic-geometry codes from an algebraic function field. Using the Riemann-Roch theorem, the rate and relative distance of these codes is calculated, and we see that the important parameters that govern the performance of these algebraic-geometry codes are the genus and the number of rational places of the function field. The chapter ends with an in-depth treatment of algebraic geometry codes based on the rational function field (a.k.a. Reed-Solomon codes).

Chapters 3 develops some technical machinery which is useful for function fields. The basic setting for this chapter is the following: we have a algebraic function field, $\mathbb{L}_1$, and a finite algebraic extension field of it. $\mathbb{L}_2$; how can we deduce properties of $\mathbb{L}_2$ from the properties of $\mathbb{L}_1$? We get introduced to important

[7] Nevertheless, the family of Reed-Solomon codes with $q = n$ (i.e., over a non-constant sized alphabet) does play an important role in coding theory, and even help in constructing codes over a constant sized alphabet.

notions such as ramification, the splitting of places and the "different", and important theorems such as the Hurwitz Genus Formula and Dedekind's Different Theorem. Additionally, important examples of function field extensions, such as Kummer extensions and Artin-Schrier extensions, are discussed and examined in detail. There are also detailed subsections on Galois extensions, inseparable extensions, compositums of extensions, Hilbert's theory of higher ramification groups and Castelnuovo's and Riemann's upper bounds on the genus of a function field.

Chapter 4 takes a step back and revisits the notion of a Weil differential, and relates it to the more familiar notion of differential form. Along the way we study completions at a place, which allows one to expand out algebraic functions as power-series.

Chapter 5 starts discussing algebraic function fields over a finite field $\mathbb{F}_q$. This chapter starts by defining the *zeta function* of a function field over a finite field, which is a power series that encodes the number of $\mathbb{F}_{q^m}$-points on the underlying algebraic curve, for all $m \geq 1$. It is then proved that this zeta function is actually a rational function, and it satisfies a functional equation. The next goal of this chapter is to prove the fundamental Hasse-Weil theorem, which is an analogue of the Riemann hypothesis (for the Riemann zeta function; which is as yet unproven) for the zeta function of a function field over a finite field. The beautiful proof of this theorem due to Bombieri (building on earlier proofs of Stepanov and Schmidt) is given here.

Chapter 6 performs a detailed study of some important examples of function fields, including elliptic function fields, hyperelliptic function fields and Hermitian function fields.

Chapter 7 (which is new to this edition of this book) studies the asymptotic relationship between the number of rational places and the genus of a function field. We first see the Drinfeld-Vladut upper bound on their asymptotic ratio. The rest of the chapter establishes the Ihara-Tsfasman-Vladut-Zink theorem, that the Drinfeld-Vladut bound is tight. Here the remarkably elegant proof of this theorem due to Garcia and Stichtenoth (the author) is given, which gives an explicit construction of a tower of Artin-Schrier extensions of function fields with many rational places relative to their genera.

Chapter 8 revisits the topic of algebraic-geometry codes. Most significantly, this chapter proves the Tsfasman-Vladut-Zink theorem on the existence of algebraic-geometry codes with better tradeoff between rate and distance than the Gilbert-Varshamov bound. This is proved by combining the generalities on algebraic-geometry codes from Chapter 2 with the remarkable function fields of the Ihara-Tsfasman-Vladut-Zink theorem from Chapter 7. The chapter ends with a description of the Skorobogatov-Vladut decoding algorithm for algebraic-geometry codes, which decodes them upto nearly half their (designed) minimum distance.

Finally, Chapter 9 studies subfield subcodes and trace codes, which include the Bose-Chaudhuri-Hocquenghem (BCH) codes and the dual-BCH codes. The minimum distance and dimension of these codes is then estimated; the Hasse-Weil bound from Chapter 5 turns out to play a crucial role in this.

The first appendix covers the basics of field theory. The second appendix provides a dictionary between the language of algebraic function fields and the more geometric language of algebraic curves.

3 Opinion

This book gives a thorough and self-contained introduction to the theory of algebraic function fields and algebraic-geometry codes. The purely algebraic approach taken in this book allows it to take off with minimal prerequisites in algebra, and proceed to give complete proofs of all the fundamental results of the area. The thorough treatment of the Tsfasman-Vladut-Zink theorem is an especially appealing aspect of this book. All this, combined with the fact that algebraic techniques and results from the theory of algebraic

function fields are playing an ever-increasingly important role in theoretical computer science and coding theory, makes this book highly-recommended for the bookshelf of every theoretical computer scientist with an algebraic leaning[8].

I must now add a pinch of salt. First and foremost, this book is not for the faint of heart. The main topic of this book is *the theory of algebraic function fields*, and even the application-oriented reader will have to learn *the theory of algebraic function fields*. In particular, there are no "shortcuts" or "guided tours" in this book for the coding theorist seeking to understand the analysis of codes meeting the Tsfasman-Vladut-Zink bound, or the pseudorandomizer seeking to learn a proof of the Hasse-Weil theorem. The book has been written in a traditional mathematical style, with definitions and lemmas coming first, and reasons and theorems later. The typical theoretical computer science reader will perhaps find this style a bit foreign, and will have to be highly motivated about the final fruits in order to make it through the book cheerfully. That being said, the investment of time and effort for one who does makes it through will be very rewarding, both intellectually and technically.

There are many approaches to studying algebraic function fields: purely algebraic [Sch76, Mor91], approaches emphasising geometric aspects [Har77, HKT08, TV91], or by analogy with the theory of number fields [Ros02, Wei67]. Each of these approaches has their own advantages; the different points of view enrich and inform each other. Admittedly, the more geometric treatments of the theory of algebraic curves and algebraic geometry codes in the literature either require a certain degree of expertise in algebraic geometry, or else omit proofs of some fundamental theorems. On the other hand, with the geometry comes intuition, and awareness of the geometric approach can nicely complement the rigorous-but-sometimes-dry algebraic approach to the subject.

For one seeking a thorough introduction to algebraic geometry codes, or for one seeking to add some powerful viewpoints and techniques to their pseudorandomness toolkit, this book would serve the purpose well. There are many well-chosen exercises at the end of each chapter. This book would also be an excellent supplementary text for a course on algebraic coding theory.

Overall, I like the book very much, and I am sure that this book will become very influential and a standard reference in the years to come.

References

[Har77] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[HKT08] J. W. P. Hirschfeld, G. Korchmáros, and F. Torres. *Algebraic curves over a finite field*. Princeton Series in Applied Mathematics. Princeton University Press, Princeton, NJ, 2008.

[Mor91] Carlos Moreno. *Algebraic curves over finite fields*, volume 97 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 1991.

[Ros02] Michael Rosen. *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

[Sch76] W. Schmidt. Equations over finite fields. In *Lecture Notes in Mathematics*, pages 53–6. Springer Verlag, 1976.

[8] or even a leaning of transcendence degree 1!

[TV91] M. A. Tsfasman and S. G. Vlăduţ. *Algebraic-geometric codes*, volume 58 of *Mathematics and its Applications (Soviet Series)*. Kluwer Academic Publishers Group, Dordrecht, 1991. Translated from the Russian by the authors.

[Wei67] André Weil. *Basic number theory*. Die Grundlehren der mathematischen Wissenschaften, Band 144. Springer-Verlag New York, Inc., New York, 1967.

Review of[9] of
Those Fascinating Numbers
by Jean-Marie De Konick
Published by the AMS, 2009
426 pages, Softcover, $42.00 on amazon, $39.00 for AMS members at AMS[10]
Review by
William Gasarch gasarch@cs.umd.edu

1 Introduction

This is a very odd book. I had a back and forth argument with myself on whether I liked it or not. The book is a list of numbers and the properties of them. There are references which are helpful to learn more. I can imagine someone reading some property and getting interested in that property. I can also imagine someone saying *all of these properties? Who cares!* Indeed, some of the properties I don't care about.

In most cases I was not interested in the number but I was interested in the property. Here is an example: The number 1167 is the largest number that cannot be written as the sum of 5 composite numbers. I do not care about 1167. However, I do care about the theorem: for almost all n, n can be written as the sum of 5 composite numbers.

2 A Random Sample of the Book

I looked at every square-numbered page and picked out some numbers from that page to discuss. I pick those that are either interesting or to make some point about what the author finds interesting. I also tried to pick concepts that the readers of this review do not know.

1. 3 is the prime number that appears the most often as the second largest prime factor of an integer. Later in the book he has the prime that appears most often as the third, fourth, etc (I am not sure what the last one is.) Now that I know the concept I want to read up on it. It seems like a deep question. A reference is given so I could start there.

2. 11 is the smallest prime p such that $3^{p-1} \equiv 1 \pmod{p^2}$. Why do we care about 3^{p-1}?

3. 12 is the smallest psuedo-perfect number. A number is psuedo-perfect if it it is the sum of *some of* its proper divisors. Now that I know this concept I want to read up on it. However, I am not sure if this is a deep question or if much is known, though a reference is given.

[9] ©2011, William Gasarch

[10] The book has no entry for 426. For 42 we find that it is the least number such that the sum of the squares of its divisors is a perfect square. For 39 we find that its the smallest number n such that $2^n - 7$ is prime.

4. 24 is the only $n \geq 2$ such that $1^2 + \cdots + n^2$ is a perfect square. This could be the basis of a good programming assignment

5. 43 is the fourth prime p such that $19^{p-1} \equiv 1 \pmod{p^2}$. This is an example of what is wrong with some of the entries in the book. The first such number might be interesting. But the fourth? And why do I care about $19^{p-1} \pmod{p^2}$? This needs more context. It might be supplied in the reference.

6. 44. This one needs some notation. Let $\omega(m)$ be the number of distinct prime factors of m. 44 is the smallest number n such that

$$S_n = \sum_{m \leq n, \omega(m)=2} \frac{1}{m} > 1.$$

   This makes me wonder if the sequence $S_1, S_2, \ldots$ diverges.

7. 77 is the largest number which cannot be written as the sum of positive integers whose sum of reciprocals is equal to 1. Note that

   - $78 = 2 + 6 + 8 + 10 + 12 + 40$
   - $\frac{1}{2} + \frac{1}{6} + \frac{1}{8} + \frac{1}{10} + \frac{1}{12} + \frac{1}{40} = 1$

   This is interesting: for almost all all n, n can be written as the sum of numbers whose reciprocals sum to 1.

8. 111 is the smallest insolite number. A number is insolite if its decimal representation has no 0's and the number is divisible by both the sum and the product of the squares of its digits. This concept is tied to base 10 and hence is not that interesting.

9. 164 is the fifth solution of $\phi(n) = \phi(n+1)$ where $\phi(n)$ is the number of numbers $m \leq n$ that are co-prime to n. This is a typical entry of the book: Let F be a function like $\phi(n)$ or $\sigma(n)$ (the sum of the divisors of a number) or $\sigma^2(n)$ (the sum of the squares of the divisors of n). Let $k, m \in N$. This book may have the kth number n such that $F(n) = F(n+m)$. These entries draw attention to the function F but get repetitive.

10. 167 is the seventh numbers n such that $n! + 2^n - 1$ is prime. This could be the basis of a good programming assignment

11. 251 is the smallest number which can be written as the sum of three cubes in two distinct ways: $251 = 1^3 + 5^3 + 5^3 = 2^3 + 3^3 + 6^3$. Ramanujan would think this was interesting. And he was a far better mathematician than I, so I defer to him.

12. 255 is the number of Carmichael numbers that are $< 10^8$. A number n is a Carmichael number if it is composite but satisfies all the equations $b^{n-1} \equiv 1 \pmod{n}$ for b relatively prime to n. The concept is very interesting since some of the randomized polynomial time algorithms for Primality fail on Carmichael numbers. This is an odd entry in that they are using 255 to count some other type of number. There are a few other entries like this: the number of numbers of type X that are $< y$. That does not seem to be in the spirit of the book for two reasons: (1) they use the number to count something else, and (2) they have an arbitrary upper bound. Even so, this introduces you to a new concept.

13. 384 is the least number n such that $n2^n - 1$ is prime. This could be the basis of a good programming assignment

14. 671. This one needs notation. Let $f(x) = x/2$ if x is even, $3x + 1$ if x is odd. A number n is self-contained if there exists a k such that n divides $f^k(n)$ (f iterated k times). 671 is the third self-contained number. This could link to the Collatz Conjecture[11] but the author does not mention this.

15. 1215. The smallest number n such that both n and $n + 1$ are divisible by a fifth power. Are there an infinite number of such? The book does not say. This could be the basis of a good programming assignment. It may also lead to some mathematics of interest.

16. 2295. The fifth positive solution x of the Diophantine equation $x^3 + 999 = y^3$. The entry refers to the entry for 251. In the entry for 251 we find that there are only a finite number of solutions and they are all listed, along with a reference. This sounds interesting.

17. 5906. The smallest number which can be written as the sum of two fourth powers of *rationals* but not the sum of two fourth powers of *naturals*. This number lives up to the title of the book. This is fascinating in that I never knew there were any such numbers.

18. 70841. The largest prime p such that $\pi(p) \leq \frac{p}{\ln p} + \frac{p}{\ln^2 p} + \frac{2p}{\ln^3 p}$. These are the first three terms in the asymptotic expansion of $Li(p)$ where $Li(x) = \int_0^x \frac{dt}{lg(t)}$. By the prime number theorem $Li(p)$ is a very good estimate for $\pi(p)$. The prime number theorem is very interesting; however, it is not clear how this factoid relates to it. No references were given for more information on this topic.

19. 366439. The 21st prime number p_k such that $p_1 \cdots p_k + 1$ is prime. The concept is interesting since it relates to Euclid's proof that the primes are infinite.

20. 4,729,494. The number appearing in the famous *cattle problem* of Archimedes, namely in the Fermat-Pell equation $x^2 - 4729494y^2 = 1$. I urge the reader to look up *cattle problem*. This is interesting historically, though not mathematically. That is absolutely fine!

21. 173,706,136. The 19th dihedral perfect number. A number n is *dihedral perfect number* if $\sigma(n) + \tau(n) = 2n$ where $\sigma(n)$ is the sum of the divisors of n (including 1 and n) and $\tau(n)$ is the number of divisors of n. I care about the concept. But why the 19th?

22. 250,330,350,875. Possibly the only number whose index of composition is > 2.2 and which can be written as the sum of 2 co-primes numbers whose index of composition is ≥ 6. What is an *index of composition*? The entry does not tell me nor give a reference to another number. The books index points to the number 629693, but that did not help. I went online to find out but could not.

23. From pages 400-406 almost all of the numbers are either Mersenne primes, even perfect numbers, Fermat Numbers, properties that depend on base 10, or empirical properties (e.g., the largest known number such that . . .).

24. Page 407 has the Skewes numbers which are interesting for their relation to the prime number theorem, and Goodstein sequences which are interesting because they lead to large numbers.

[11] for all n there exists a k such that $f^k(x) = 1$

3 Opinion

Should you buy this book? On the one hand this book introduces some interesting concepts in number theory. On the other hand, some of the concepts are not that interesting and some of the references are missing. My final verdict: if you are interested in concepts about numbers then this book is good to browse through. Whether that means you buy it new, used, off a grant, have your department buy it for their library, or sneak a peek at it during an AMS meeting is up to you.

This book would make more sense as a website with pointers to the relevant definitions and (if available) papers. There already is such a website which is not connected to the book:

http://www2.stetson.edu/ efriedma/numbers.html.

(Other websites of interest are

http://www.nathanieljohnston.com/2009/06/11630-is-the-first-uninteresting-number/

and

http://primes.utm.edu/curios/page.php?short=11.)

There is some information on the website that is not in the book (95 is the number of planar partitions of 10) but there is a lot more in the book that is not on the website.

The author asks for suggestions for improvements. Here is one: make the book into a website.

Review[12] of
Pólya Urn Models
Author of Book: Hosam Mahmoud
2009, CRC Press, Hardcover, 312 pages
$80.00
Review by Stephen Stanhope sstanhop@bsd.uchicago.edu

1 Introduction

Consider an urn containing a number of colored balls. Suppose that you are assigned the task of repeatedly reaching blindly into it, picking out a ball, replacing it, and then depending on the color of that ball adding a specified number of new colored balls into the urn. Such an urn and associated sampling-replacement scheme is referred to as a "Pólya urn," and given this description a number of mathematical questions can be asked: What is the long-term proportion of balls expected to be allocated to one color? After a given number of samples are drawn, what is the distribution of the number of balls of a particular color? How do the answers to these questions change as the rules for the urn are generalized - for example, what if conditional on drawing a ball of a particular color a random rather than specified set of balls of various colors are readded to the urn, or what if rather than drawing only one ball at a time, multiple balls are drawn? More applied researchers might utilize these mathematical results to attempt to model a variety of physical systems, and in so doing create new demands for both further generalizations of the Pólya Urn and mathematical technique for analyzing the behavior of these urns.

In Pólya Urn Models (2009), Hosam Mahmoud provides both an overview of the mathematical tools used to study Pólya urns and examples of their application to multiple problems in computer science and the biosciences. The primary requirement for the book is a familiarity with probability and stochastic processes, although additional background in differential equations and combinatorics is useful. There is substantial

citation of the results presented in the text, and the pacing of the book makes it useful for either self study or as a reference for applied work.

2 Summary

The book is comprised of 10 chapters. The first two provide background material. Of the remaining eight, six are related to mathematical tool development and two to applications. Each chapter is concluded with several questions, and solutions to all questions are provided in the text. For each chapter, I will briefly restate a problem and the suggested approach for solving it in order to provide some flavor for the types of questions asked.

Chapter 1: Urn Models and Rudiments of Discrete Probability (16 questions)

Chapter 1 covers basic definitions, probability axioms, stochastic processes and exchangability. Examples of discrete distributions relevant to urn models are provided. Poisson processes and Markov chains are discussed.

Sample question, #1.4

An urn contains five white balls and three blue balls. Three balls are taken out (one at a time) and each draw is at random and without replacement. What is the probability that (a) all three balls are white; (b) two balls are white and one is blue; (c) that the first two balls in the sample are white and the last is blue? (The distribution of total number of white balls drawn is hypergeometric, which solves parts a and b. Part c can be solved by conditioning or by exchangability.)

Chapter 2: Some Classical Urn Problems (8 questions)

This chapter continues building background material by providing descriptions of several classical (i.e. non-Pólya) urn problems. Occupancy problems (n balls are placed into m urns, what is the probability that no urn will be empty?) and coupon collecting (one of n distinct coupons is randomly received upon visiting a store. How many visits are required to obtain a complete set?) are briefly described, as is Banach's matchbook problem (a smoker has two pockets each containing n matches, and randomly pulls matches from one or the other. Upon first emptying a pocket, how many matches remain in the other?). Ballot problems and the Gambler's Ruin are described in more detail. The first of these supposes that $m > n$ votes are respectively cast for two candidates in an election, and is concerned with calculating the probability that the first candidate is ahead throughout the vote. The second asks, for two gamblers who repeatedly wager \$1 on the toss of a (weighted) coin, what is the probability that one or the other gambler will go bankrupt? Mahmoud's treatments of these questions use recurrence relations in manners similar to suggested in other texts and are explained clearly.

Sample question, #2.6

In an n-coupon collecting problem, what is the expected waiting time to collect all coupon types? (Mahmoud suggests stating the waiting time as a sum of geometric-distributed random variables.)

Chapter 3: Pólya Urn Models (7 questions)

Chapter 3 introduces the main topic of the text. The preface for the chapter describes how a sampling-replacement scheme for a urn can be represented through a matrix with rows and column indexing the balls drawn and reintroduced respectively. Such a matrix is referred to as a "schema." A discussion of the tenability of an urn scheme is provided, with particular focus on two color problems with deterministic schema entries and single ball draws. That focus continues by analyzing a number of two color Pólya urn problems. In increasing order of generality the Pólya-Eggenberger (in which a draw of a ball reintroduces a number of same colored balls into the urn), Friedman (in which a draw of a ball reintroduces a number of balls of each color into the urn, with symmetry dependent on the color of the drawn ball) and Bagchi-Pal urns (draws of balls of a given color reintroduce a number of balls of each color into the urn, with no symmetry such as used by the Friedman urn) are examined. The chapter concludes by describing the Ehrenfest urn, which can be regarded as a special case of Friedman's urn that holds the total number of balls constant, and is of particular interest because of its use as a model for the exchange of gas molecules across two chambers.

Sample question, #3.3

A Pólya-Eggenberger scheme with the ball replacement matrix $diag(2)$ starts with four white balls and three blue balls. (a) Given the first draw is blue, what is the probability that the second draw is white? (b) Show that irrespective of the draw number, the probability of picking a blue ball is 3/7. (c) Show that the probability that two consecutive drawings are the same color is 13/21. (Mahmoud suggests that b and c be approached by using exchangeability.)

Chapters 4 and 5: Poissonization (6 questions) and The Depoissonization Heuristic (4 questions)

Chapters 4 and 5 are focused on developing mathematical tools for analyzing urn models. As in Chapter 3 their main focus is two color problems with deterministic schema entries, although the author provides some suggestions and extensions for multicolor deterministic schemes and two color schemes with random entries.

Chapter 4 deals with poissonization - that is, the embedding of the discrete time urn in continuous time. The author begins by describing the embedding, which uses a Poisson process to approximate the number of draws of each ball initially contained in the urn that are obtained in a given time interval. Two results are obtained that pertain to the dynamics of the total number of balls of each color. The first shows that the moment generating function for the joint process satisfies a first order partial differential equation, and the second manipulates this partial differential equation to yield a formula for the expected number of balls of each color at a particular time. The chapter then applies these results to the monochromatic Pólya urn, Pólya-Eggenberger urn, and Ehrenfest urn. In each of these cases, the moment generating function is used to obtain convergence properties.

In Chapter 5, the reverse operation of depoissonization is discussed with a focus on problems with invertible schemas. As preparation, Mahmoud shows that the (random) time of the n^{th} draw has convergence in probability. Through an intricate series of steps, he then demonstrates how that asymptotic property can be manipulated to obtain a relationship between the expected number of balls of each color after n draws as a function of the schema and n. The chapter concludes by providing example calculations for several cases, including a Friedman urn and two instances of Bagchi-Pal urns.

Sample question, #4.2

Suppose a poissonized Ehrenfest process starts with two white balls and one blue. What is the probability distribution of the number of white balls at time t? What are the mean and variance exactly and asymptotically? (As noted in the text, the moment generating function for the number of white and blue balls satisfies a first order partial differential equation. The probability distribution is obtained by solving this pde and appropriately using the definition of the moment generating function. After doing so, moments can be calculated in a variety of ways. Note that Mahmoud describes a two-ball version of this problem in the chapter, and provides a number of references to his own work on the subject for interested readers.)

Sample question, #5.1

Apply the depoissonization heuristic to derive the average number of balls in a Pólya-Eggenberger dichromatic urn scheme growing in discrete time after n draws, where s balls of the same color are added after each draw. (This is solved by recognizing that the schema is symmetric and invertible and then directly applying results derived in the chapter.)

Chapter 6: Urn Schemes with Random Replacement (3 questions)

Chapter 6 expands upon previous results to consider urns with random replacement - that is, conditional on a ball of a particular color being drawn, a random number of balls of each color are reintroduced into the urn. The chapter begins by extending deterministic schemas defined in Chapter 3 for describing sampling-replacement schemes to those with random entries. Such matrices are referred to as a generators, and under appropriate restrictions (e.g. tenability) "extended urn schemes." Convergence properties of two color deterministic extended urn schemes (where the deterministic entries of the matrix are regarded as degenerate random variables) are derived, which lead to results on the asymptotic normality of the number of balls of a given color after n draws. The results obtained for deterministic extended urn schemes are then developed to obtain analogous properties of extended urn schemes with random entries.

Sample question, #6.1

An extended Pólya urn scheme of white and blue balls progresses by sampling a ball at random and adding balls according to a given fixed schema. After n draws, let $\tilde{W}_n$ be the number of times a white ball has been sampled. Derive a weak law for $\tilde{W}_n/n$. (After n draws, the number of white balls can be expressed as a function of n and $\tilde{W}_n$. This relationship is inverted, and a weak law for $\tilde{W}_n$ is obtained from the weak laws on the number of white balls.)

Sample question, #6.2

A Pólya urn scheme on white and blue balls grows in discrete time by adding X and Y balls of each color respectively irrespective of what color ball is drawn, where X and Y are Bernoulli(p) distributed. a) Determine the exact distribution of the number of white balls after n draws. b) Find a central limit representation for the number of white balls. (These questions can be addressed through properties of sums of Bernoulli random variables.)

Chapter 7: Analytic Urns (4 questions)

The goal of Chapter 7 is to provide an alternative method for analyzing Pólya urns based on the enumeration of histories that lead to a particular state, rather than the probabilistic methods used in most of the text. As previously, the focus is on two color problems with deterministic schema. The proposed technique is based on extracting the coefficients of generating functions expressed as a summation over exponentiated terms. Mahmoud shows that a generating function for urn histories can be derived by solving a system of differential equations related to the scheme and initial condition, and that coefficients of terms of that function are directly related to the probability of obtaining a particular result after n draws. A simplified version of the approach is used to obtain formulas for the exact and asymptotic number of possible histories after n draws. More detailed examples are demonstrated by reanalyzing the Pólya-Eggenberger, Friedman, Ehrenfest, and Coupon Collector's urns.

Sample question, #7.3

Suppose that white and blue balls are sampled one at a time without replacement from an urn. Let W_n and B_n be the number of white and blue balls in the urn after n draws. Using the analytic urn method, show that $\{W_n, B_n\}$ are jointly hypergeometrically distributed. (This problem involves solving a pair of differential equations to obtain the form of the generator function, as suggested by Mahmoud. After the generator function is obtained, it is expressed as binomial series, and the coefficients can be extracted and used as described in the chapter to obtain the distribution of $\{W_n, B_n\}$. Although the distribution is hypergeometric by definition, it is useful and interesting to rederive the result with the techniques described in the chapter.)

Chapter 8: Applications of Pólya Urns in Informatics (5 questions)

Chapter 8 covers applications of Pólya urn models to a wide variety of search trees - binary, balanced, m-ary, 2-3, paged binary, bucket quad and bucket k-d. Recursive trees are also discussed in some detail. In each case, the structure of the tree is presented followed by a description of how growth of the tree can be modeled by a Pólya urn, and moments or asymptotic properties of its number of leaves, internal nodes or total nodes are derived. The chapter provide a broad overview of results, and provides citations that make it useful as a source for further study in the original research papers.

Sample question, #8.5

A binary pyramid (a recursive tree with at most 2 outdegrees per node) grows in real time t. New nodes appear at interarrival times that are independent and exponential(1) distributed. When a new node appears, it chooses as parent an unsaturated node in the pyramid at random. What is the average number of leaves in the pyramid at time t? (In the discussion of binary pyramid trees it is shown that their growth dynamics can be represented by a those of a two color urn, with white balls representing leaves and blue balls unsaturated nodes. Mahmoud suggests poissonization of the urn, which is natural given that nodes arrive at continuous time, and application of the results in Chapter 4 yield a solution to the problem directly.)

Chapter 9: Urn Schemes in Bioscience (3 questions)

Chapter 9 describes the application of Pólya urn models to questions and problems in the biosciences. As in Chapter 8 the focus is on providing a wide array of results with appropriately heavy citations. Most of

the chapter is concerned with models of population genetics and evolution. Basic Wright-Fisher models are discussed with extensions to gene miscopying and mutation, as are Hoppe's urn scheme and Ewens' formula for modeling speciation, and models of competitive exclusion and niches. In the discussion of these models, moments and asymptotic behaviors are derived for the composition of the population, the number of species and the size of each species. Lyapunov's and Lindeberg's central limit theorems are provided in the process of developing these results. In the area of epidemiology Kriz' urn scheme for contagion is described, and applications of "play the winner" schemes to clinical trials are discussed. Finally, an application of urn schemes to the structure of phylogenetic trees is provided. The text notes that such trees are related to binary trees studies in Chapter 8.

Sample question, #9.3

In a phylogenetic tree following the edge-splitting model, what proportion of nodes are leaves, what proportion of leaves are not in cherries, and what proportion of nodes are internal? (In the discussion of phylogenetic trees in the text, it is shown that the structure of the tree can be represented by a 3-color Pólya urn with colors representing different types of edges and draws representing an edge split. The number of nodes in the tree can be expressed as a function of edge split operations, and then following the chapter's discussion of phylogenetic trees asymptotic relationships between numbers of edges and edge splits can be derived. Relationships between edges, total number of leaves and leaves of different types can then be used to solve the problem.)

Chapter 10: Urns Evolving by Multiple Drawing (7 questions)

Chapter 10 expands upon the results obtained in previous chapters to study the case of urns in which multiple balls (rather than one) are drawn at a time. The focus of the chapter is on two color urns with deterministic schema. It begins by describing how such problems can be structured and analyzed, and obtains a result for the equilibrium behavior of such urns. General results are obtained for the mean and variance of the number of balls of a particular color after n multi-draws, which lead to related asymptotic properties. A martingale transformation is introduced, and asymptotic properties of that process lead to asymptotic convergence in the distribution of the nonmartingalized process. To provide an example, the results are applied to the problem of modeling the number of outputs in an evolving random circuit.

Sample question, #10.1

Consider an urn starting with 1 white and 2 blue balls. Pairs of balls are drawn. If two white balls are drawn two white and 1 blue ball is added; if two blue balls are drawn 3 blue balls are added; else 1 white and 2 blue balls are added. Show that the mean number of white balls after n draws of ball pairs is approximately $n^{2/3}\Gamma(5/3)^{-1}$ as n. (After using the applicable results the mean number of white balls is shown to be a ratio of two gamma functions of n. Mahmoud suggests using Sterling's approximation to the gamma function to show that this ratio is approximately equal to $n^{2/3}$. Alternatively, it seems that the ratio can be expressed as the expectation of a function of a gamma-distributed random variable that can be approximated with a Taylor's expansion.)

3 Opinion

In his bibliographic notes, Mahmoud suggests that he was inspired by Urn Models and Their Applications by Johnson and Kotz (published in 1977) and An Introduction to Probability Theory and Applications by Feller (published in 1968). The actual bibliography for Pólya Urn Models spans 177 separate publications, the earliest of which is The Doctrine of Chances written in 1712 by Abraham De Moivre. I mention this to provide context for my first opinion regarding the book - it is very broad and overall a reasonably challenging text.

Having said that, Pólya Urn Models is also extremely enjoyable and engaging. I found sitting down with it in a quiet room and working through Mahmoud's arguments and problems to be very rewarding. The book has a good balance of analytic tool building and application, its pacing is fast without skipping the majority of details necessary to understand and use the material, and the problems Mahmoud poses help add to the reader's understanding. I think that the book is particularly nice in its presentation of probability-based methods for analyzing urn models (Chapters 3-5) and applications of Pólya Urns to problems in biology (Chapter 9), although this probably reflects on my own interests and background. Mahmoud's description of the analytic method (Chapter 7) was intriguing, as were the parallels Mahmoud drew between phylogenetic trees in Chapter 9 and other tree structures considered in Chapter 8. Somewhat related to this comment, because of Mahmoud's meticulous use of citation the book is an excellent choice for self study or as a background text for researchers.

To be fair, I can think of two small issues with the book. The first is that answers to all the questions asked in the book are provided in an appendix. This might be a problem for the classroom use of the book, although it is a real benefit to other readers. The second is that the ordering of presentation seemed at times to jump ahead or back. For example, as I read the book it seemed as if Chapter 10 might have been better placed before the applications chapters, and likewise the description of the poissonization of schemes with random entries in Chapter 4 with the other material on schemas with random entries in Chapter 6. Although it is easy enough to reorder some of the material after reading the text once, at first reading these transitions seem somewhat abrupt.

These are however very minor points, and the book is quite pleasant. In his bibliographic notes, the author cites Sheldon Ross' books as inspiration. Pólya Urn Models will most definitely have a continued place on my bookshelf near these texts, and I plan on reading and consulting it further in the future.

‘

Review[13] of
Not always buried deep: a second course in elementary number theory
Author of book: Paul Pollack
Publisher: American Mathematical Society, 2009, 303 pp.
ISBN NUMBER: 978-8218-4880-7, PRICE: $62.00

Reviewer: S. C. Coutinho (collier@impa.br)

1 Overview

The definition of prime number is at least as old as Euclid, who states in Book 7 of his *Elements* that

> a prime number is one which is measured [we would say, divisible] by the unit alone.

The remainder of Book 7 contains many results that are still a part of a first course in number theory, including the algorithm that we use to compute the greatest common divisor of two integers (Proposition 2). Actually, a result of another book of the *Elements* has been chosen over and over as a paradigm of what a beautiful and simple proof in mathematics should be. It is Proposition 20 of Book 9, which Euclid states as follows:

> The (set of all) prime numbers is more numerous than any assigned multitude of prime numbers;

or, as we would say today: *there are infinitely many prime numbers*. Further testimony to the Greek fascination with prime numbers can be found in the work Erathostenes, who lived in Ptolemaic Alexandria a little later than Euclid. He seems to have been the first to propose a systematic method for finding prime numbers. In the words of Nichomachus of Gerasa (c. 100 C. E.):

> The method for obtaining these [i.e. the prime numbers] is called by Erathostenes a sieve, since we take the odd numbers mixed together and indiscriminate, and out of them by this method, as though by some instrument or sieve, we separate the prime and indecomposable by themselves, and the secondary and composite by themselves.

Prime numbers were not the only aspect of number theory that fascinated the Ancient Greeks. An even earlier trend which gets mixed up with the study of primes was apparently initiated by the Pythagoreans, for whom some numbers had mystical properties. For example, they considered an integer n to be *perfect* if its proper divisors added up to n. These numbers are also discussed in *The Elements*. In Proposition 36 of Book 9 Euclid shows that if $2^p - 1$ is prime, then $2^{p-1}(2^p - 1)$ is a perfect number. That all even perfect numbers are of this form was eventually proved by Euler.

Another famous number theoretic result, unrelated to primes, that appears in the *Elements* is the construction of Pythagorean triples given in Proposition 29 of Book 10. In modern parlance, this proposition describes a formula that enables one to generate all triples of positive integers (x, y, z) that satisfy $x^2 + y^2 = z^2$. This result, which probably antedates Euclid, marks the beginning of what we now call *diophantine analysis*, after the last hellenistic mathematician to make substantial contributions to number theory, Diophantus of Alexandria. Actually, his *Arithmetica* is a collection of rules for finding rational solutions of indeterminate equations, of which the Pytaghorean one is a simple example.

After the collapse of Hellenistic civilization, number theory remained more or less dormant until the 16th century, when it found a new champion in Pierre de Fermat. One of Fermat's source was Diophantus's *Arithmetica*, in a margin of which he made the famous note concerning the integer solutions of the equation $x^n + y^n = z^n$. Given that, it is not surprising that many of Fermat's results are concerned, in one way or another, with indeterminate equations; his contributions to the theory of prime numbers were rather few. That would only change in the 18th century, after Goldbach succeeded in interesting Euler in the work of Fermat. Among other things, Euler gave a new proof of the infinity of primes, based on the divergence of the harmonic series, which would bear good fruit in the next century.

The 19th century was a great time for number theory. It opened with Gauss's *Disquisitiones arithmeticae*, which contains the first complete proof that every integer greater than one can be uniquely factored in prime numbers, and where modular arithmetic is formally introduced for the first time. It was also in this century that the study of prime numbers came of age. Both Gauss, and his contemporary Legendre, proposed an asymptotic formula for counting prime numbers. More precisely, they conjectured, based on numerical evidence, that if $\pi(x)$ denotes the number of positive primes less than or equal to x, then

$$\lim_{x\to\infty} \frac{\pi(x)\log(x)}{x} = 1; \tag{1}$$

a result that became known as the *Prime Number Theorem*. The breakthrough that would eventually lead to the proof of this theorem came from Dirichlet. In a paper published in 1837 he proved another conjecture of Legendre, according to which

> there are infinitely many primes in an arithmetic progression whose first term is coprime with the ratio.

In order to do this, he systematically used analytic methods (L-series), thus showing the power of continuous methods in the study of integers, the domain of the discrete par excellence.

The first major contribution to the proof of the Prime Number Theorem came from Chebyshev. In papers published in 1851 and 1852 he showed, among other things, that if the limit in (1) existed then it had to be equal to one. The final push to the proof of the Prime Number Theorem was prompted by a paper Riemann contributed to the Berliner Akademie in 1859. In it he introduced the ζ function, defined on a complex number s by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s};$$

and proved some of its elementary properties. He also stated a number of results without proof, among them an explicit formula from which the Prime Number Theorem would follow directly.

Unfortunately Riemann did not live long enough to prove any of these results, and some of them, like the explicit formula mentioned above and the famous *Riemann hypothesis* concerning the zeroes of the ζ function, remain unproved to this day. Luckily it turned out that the formula was not really necessary for a proof of the Prime Number Theorem. Indeed, two independent proofs were published in 1896, by Hadamard and de la Vallé Poussin, both of which made heavy use of the complex analytic methods introduced by Riemann.

If anything, number theory has been keeping the momentum it had acquired by the end of the 19th century. Among the many results proved in the 20th century and with which this book is concerned, we should mention:

- Hilbert's proof of Waring's statement that for every power k there exists a finite integer $g(k)$ such that every positive integer is the sum of at most $g(k)$ kth-powers (1909);
- Brun's sieve and its application to Goldbach's conjecture (1915);
- the elementary (in the sense of not using complex analysis) proof of the Prime Number Theorem by Erdös and Selberg (1949).

To end with a more recent result which is not discussed in this book, Ben J. Green and Terence Tao proved in 2004 that the sequence of primes contains arbitrarily long arithmetic progressions. Amazingly, the longest of these progressions that we know explicitly has only 24 primes.

2 Summary of Contents

The book under review is intended as a second course in elementary number theory, with an emphasis on analytic methods. Actually the book is mostly about prime numbers, with four of the eight chapters having the word prime in their titles. Chapter one, perhaps the most charming of the whole book, is the first of two that are entitled *Elementary prime number theory*. It is mainly a collection of proofs that there are infinitely many primes. These range for Euclid's simple argument to what the author calls "sledgehammers", proofs that use very high powered theorems indeed. The chapter ends with three sections on prime producing formulae.

Entitled *cyclotomy*, Chapter 2 is the most algebraic in the whole book. It contains Gauss's characterization of the polygons that can be constructed by straight edge and compass and applications of cyclotomic extensions to reciprocity laws, both quadratic and cubic. With chapter 3 we are back in the realm of prime numbers. Although not as elementary as chapter 1 (with which it shares its title), this chapter contains several basic results that are required in the proof of the Prime Number Theorem given in chapter 7. As a corollary, we have Chebyshev's proof of *Bertrand's postulate*:

> for all sufficiently large x there is always a prime between x and $2x$.

The next chapter is one of my favourites: it contains a beautiful proof of Dirichlet's Theorem on arithmetic progressions, mentioned above. Chapter 5, which is concerned with Hilbert's proof of the *Waring Problem* is the shortest of the whole book. Sieve methods are discussed in chapter 6, which begins with Legendre's improvement of the sieve of Erathostenes and proceeds to Brun's sieve and its application to *Goldbach's Conjecture*.

The book reaches its climax in chapter 7, which is totally devoted to a version of Selberg's elementary proof of the Prime Number Theorem. The ingenuity required is breathtaking. If you enjoy slick analytic arguments, you will certainly like this chapter. Finally, chapter 8 reaches back to the dawn of mathematics, for it is concerned with perfect numbers, the very same that the Pythagoreans defined thousands of years ago. Given that Euclid had already characterized *even* perfect numbers, the focus here is on *odd* perfect numbers. Surprisingly no odd perfect numbers are known and Pollack gives a heuristic argument, due to Pomerance, that such numbers probably do not exist. This chapter also contains results on other numbers with properties that would have delighted the Pythagoreans, like abundant numbers, amicable numbers and sociable numbers.

3 Opinion

Let me begin by saying that this is one of the best mathematics books that I have read recently. It is beautifully written and very well organised, the kind of book that is well within the reach of an undergraduate student, even one with little complex analysis. Indeed, a good knowledge of the analysis of real functions of one variable is probably enough for reading most of the book. Chapter one is a case apart, it is so elementary and so interesting that it should be read by anyone interested in mathematics. The other chapters are far more demanding and have to be studied carefully if one is to profit by them. However, I know of no better place to learn about Dirichlet's Theorem on arithmetic progressions or Selberg's proof of the Prime Number Theorem. And if there are two results of analytic number theory that deserve to be known to every mathematician, these are certainly they.

Since no book is perfect, there are a number of minor points that may be improved in future editions. For instance, given the technical nature of the subject matter, it is not to be expected that readers will remember previously proved results without an explicit reference. Unfortunately, the author often does not cite such results, which makes the reading a little harder than necessary. A few more brackets in some of the more complicated equations would also have helped the reader. I should also add that I have my doubts about the author's statement that

> [t]he proof [of Selberg's fundamental formula] [...] can be understood by a talented high-school student (p. 215).

But these are very minor points on an otherwise excellent book. I only wish more well-organised, clear and passionate books like this were written. Mathematics would benefit very much from it!

Review of [14]

Pioneering Women in American Mathematics: The Pre-1940 PhD's
by Judy Green and Jeanne LaDuke
345 pages, $63.00, hardcover, 2009, AMS

Review by Sorelle A. Friedler (sorelle@google.com)

1 Introduction

Pioneering Women in American Mathematics: The Pre-1940 PhD's is a comprehensive examination of the lives of all 228 women who earned PhDs in mathematics before 1940 who were US-born or earned their PhDs in the US. The first eight chapters of the book examine the themes of these women's lives with regards to family background and childhood education, undergraduate and graduate education, and career and professional opportunities and contributions. The rest of the book contains short biographies (approximately one page each) of each of the 228 women.[15] The authors focus mainly on the large set of facts they collected, much of it from first-hand data or interviews. The information is extensive, and though some themes and summaries are suggested, mostly the data is left to speak for itself.

[14]

[15] Longer biographies and more extensive references can be found on the AMS site: http://www.ams.org/bookpages/hmath-34.

2 Summary

A surprising statement sets the tone for the book; "More than 14 percent of the PhD's awarded in mathematics during the first four decades of the twentieth century went to women, a proportion not achieved again until the early 1980s."[16] The authors continue by exploring the reasons why the percentage was not higher, and begin explanation of the drop in percentage, through careful examination of the lives of the women who earned PhDs in those years. These women represented a geographically, educationally, and economically (but not racially) diverse snapshot of the United States population of the time. In addition to the plethora of facts, we are given some insight into the perseverance and spirit of these women through anecdotes about particular women.

The first woman to earn her PhD in mathematics was Christine Ladd-Franklin. She passed her dissertation defense in 1882 at Johns Hopkins University and the mathematics department agreed that she had earned a PhD. The awarding of her PhD was blocked by the university trustees because she was a woman.

> In 1926, at the fiftieth anniversary of the founding of Johns Hopkins, Ladd was offered an honorary degree as a result of her work in physiological optics. She insisted, instead, that it be the PhD she had earned forty-four years earlier or none.[17]

They agreed, and so 44 years after earning it, Ladd was awarded her PhD.

After presenting this story and giving some broad information to set the scene, the book begins by examining trends in the women's early education and family backgrounds. The authors found that there were no common trends in the early education and family backgrounds of women who earned PhDs. The women came from around the country, in numbers somewhat dependent on the availability of undergraduate education for women in their state (e.g., Southern states produced proportionally less PhDs, North Eastern states produced proportionally more). Similarly, while one might hypothesize that many of the women's parents also had advanced degrees, only a few parents did. The women's pre-college schooling was made up of about 70% public secondary schooling, with the remaining attending private schools or studying with tutors. Unfortunately, the authors do not discuss if this was true for the broader population of the time as well. Anecdotally, parents and high school teachers were described as important in leading to strong interests in mathematics.

Women's colleges were critical to producing women with PhDs in mathematics before 1940. Among the ten schools that led in providing college educations to women who later earned PhDs, eight were women's colleges. Similarly, it is anecdotally reported that classes taught by women or supportive male faculty were very influential to the women's decisions to continue their education. Nola Anderson Haynes (PhD, University of Missouri, 1929) describes the influence a supportive chairman had on her decision to pursue a PhD as follows:

> One day... the chairman of the department asked, "Miss Anderson, what are you going to do next year?" I said, "I guess go out and get a job in a junior college," thinking I could very easily, of course. And he said, "Would you be interested in going on towards a PhD if you got a fellowship?" Well, that was an easy thing; ... I didn't have to think about getting a job, so I accepted it and went on and got my PhD.[18]

[16] Page 1.

[17] Page 5

[18] Page 60, as quoted from Smithsonian meeting tapes recorded August 31, 1981 at a luncheon for pre-World War II female American mathematics PhDs.

The authors note that while most other prominent women's colleges were among the leaders in producing future PhDs, Barnard and Radcliffe were not. "Perhaps it is noteworthy that at both Barnard and Radcliffe the undergraduate classes were taught by the male faculty of the associated men's universities."[19]

The graduate education of these 228 women included many firsts, and not just firsts for women. For example, six women were the first of any sex to be awarded a PhD in mathematics at their university.[20] Many universities were willing to admit women as graduate students long before they were willing to admit female undergraduates.

> The definiteness of aims, the increased earnestness and the more mature character which belong to the greater age of graduate students, may entirely or largely remove difficulties which are found in the way of men and women mingling in the undergraduate department. The Faculty of Yale University knows very well that to admit women to its graduate school is quite unlike opening the doors of Yale College to girls of the age of eighteen.[21]

But the most important factor in the graduate education of these women was their advisor; the eight advisors who directed the most dissertations of women in the study advised two-thirds of all women who earned PhDs at the schools in which they taught, and were the main reason why those schools were leaders in educating women at the PhD level in mathematics.[22] The University of Chicago, the leading producer of female mathematics PhDs during this period, had two advisors, L. E. Dickson and G. A. Bliss, who together advised 65% of the 46 Chicago women PhDs or 13% of the total 228 women considered in this book.[23]

After earning their PhDs, 90% of the women were employed within one year (even though many graduated during the Depression). Most of these were jobs in academia, either in teaching, research, or other associated positions. Of these, two-thirds had previous relationships with their employer, as employees or students. Half of the women's first teaching jobs were at women's colleges, most of which employed only single women. Marriage was a large factor in the employment of the women in this study, and the work patterns for women differed based on marital status.

Of the women who were married, 36% were unemployed during the time that they were married. A main cause of this unemployment was the existence of anti-nepotism laws which disproportionally affected women. 65% of these married women were married to other PhDs, and it was only them, not their husbands, who lost or were refused jobs. After World War II, the rise in undergraduate students due to the GI Bill meant that many of these women who were previously denied employment were offered jobs.

In contrast, 96% of the women studied who were single were employed, despite the Depression. Many of them were employed at women's colleges, and were promoted to full professor by the time they had retired. There were also some women who earned PhDs in this time period who were nuns. Generally, these women were encouraged by their church to pursue a PhD to satisfy the teaching needs of their order's colleges. These women had the advantage of having a guaranteed job after graduation. They frequently served in positions of administrative authority within their university or religious order.

While women's colleges and religious orders served as positive employers in terms of the promotion and advancement of their female employees, women teaching at co-ed schools often remained at the instructor level throughout their careers. At the University of Chicago, despite graduating many female PhDs, there have only been two women promoted to associate or full professor from its founding in 1892 until the writing

[19] Page 28.
[20] Page 55.
[21] Page 8, as quoted from *The College Woman* (New York: Baker and Taylor, 1894), 130-131.
[22] Page 46.
[23] Pages 44-45.

of this book in 2009.[24] Despite the professional set-backs some of these women experienced, one expressed satisfaction with her choice in earning a PhD in mathematics in a 1926 professional survey, saying:

> The freedom from monotony in the work in mathematics, the vision and grasp of fields of knowledge that may be interpreted through mathematics, the ideals of thought and of thinking, and the ability to interpret in conduct, relief from the turmoil of a crowded life, all these make the Ph.D. more valuable than any professional advantage to be derived from it.[25]

In addition to academic employment, about two dozen women chose industry, military, or other non-academic careers. One of the most notable of these women was Grace Murray Hopper. She graduated from Vassar College in 1928 and from Yale with a PhD in mathematics in 1934. In 1941 she was an assistant professor at Vassar when she took a leave of absence to join WAVES, a female branch of the US Naval Reserve. From that time forward she had an ongoing involvement with the military, though she was not always on active duty. She also worked at Harvard, the University of Pennsylvania, George Washington University, and many computer companies. During her career she wrote code for the Mark I computer and worked on the UNIVAC and developed its first compiler. She is best known for developing the first English-language programming language, FLOW-MATIC, and for her work as one of the leading developers on its successor, COBOL. When she was forced to retire from the navy in 1986, she had reached the rank of rear admiral (lower half).[26]

Hopper's contributions, though non-academic, could be considered to be the most influential produced by the women in this book. Many research and other professional contributions were made by the women. As a group, these women published almost 400 papers. With 14 papers presented at the meetings of the AMS between 1914 and 1930, Olive C. Hazlett was among the top 10% of all math researchers of the time.[27] Many women also contributed professionally through math education publications and professional organizations and, of course, through the students they taught.

In the final chapter before the bibliographic entries, the authors suggest possible reasons for the decline of women as a percentage of mathematics PhD earners after 1939. The main reason suggested is a demographic one - after World War II, the GI Bill provided the means by which many more men could enter college and graduate school. The number of male students increased dramatically, thus decreasing the percentage of women to about 5 percent in the 1950s. For example, the University of Chicago, one of the leading graduate schools for women in mathematics in the 1930s, graduated a total of 88 students in the 1930s, 24 of whom were women, and a total of 102 students in the 1950s, only 3 of whom were women.[28] While there were circumstances specific to the University of Chicago that contributed to the precipitous decline (most notably, the retirement of some professors especially supportive to women students), the trend was nationwide. "By the 1950s the number and percent of women earning PhD's in mathematics were so low that women in mathematics were effectively invisible."[29]

[24] Page 88. It appears from the university's website that this is still the case.
[25] Page 96, as quoted from Hutchinson, *Women and the Ph.D.*, page 101.
[26] Pages 205-206.
[27] Pages 98-99.
[28] Page 116.
[29] Page 118.

3 Opinion

Pioneering Women in American Mathematics presents an extensive history of the 228 American women who earned PhDs in mathematics before 1940. While the book does summarize the data collected in its introductory chapters, its purposeful lack of broad thematic description results in a dry, though important, collection of the facts. The first such comprehensive investigation into the lives of these 228 women, perhaps the book will serve as the foundation for future understanding of the trends and anomalies in these women's lives. It would be especially interesting to see more instances in which the experiences and lives of these women are compared proportionally to equivalent experiences of all mathematics PhDs from the time.

The main takeaway message, if trying to use this history to understand how to support women PhDs in mathematics and computer science today, is the import of teachers and advisors. As mentioned earlier, supportive undergraduate faculty were influential in these women's decisions to pursue a PhD, and two professors were single-handedly responsible for supervising the dissertations of 13% of these women. Though the number of students has increased, professors today should not underestimate the impact they can have on the total number of female PhDs simply by supporting the efforts of the ones who arrive in their department.

For readers interested in research on women in mathematics, this book is a fundamental source. For the average reader, I recommend skimming the first eight chapters and using the bibliographic entries and embedded tables as an important reference. If you are interested in the specific history of your university, the book contains an extensive index.

Review[30] of
A Guide to Elementary Number Theory
Author of book: Underwood Dudley
Publisher: MAA, 2009, 141 pages, hardcover
$50.00
Reviewed by Song Yan `syan@math.harvard.edu`

1 Introduction

Number theory, in mathematics, is the study of the properties of integers. It used to be the purist of the pure branch of mathematics. With the advent of modern computers and digital communications, it is now also a very applied subject of mathematics, with applications particularly in cryptography and Internet security. A traditional introductory book in elementary number theory such as [1] would include theories of divisibility, congruences, continued fractions, arithmetic functions and Diophantine equations, whereas a modern introductory book such as [2] would also include some materials in the theory of elliptic curves (the revised sixth edition of [1] also included a chapter on elliptic curves at the end of the book), and some applications of number theory to e.g., coding and/or cryptography.

2 Overview

As the author claimed, this is not a textbook in elementary number theory, it is written for someone who wants to know e.g., which integers are the sum of two squares, or someone who once knew but has forgotten. However, the author did write a text in elementary number theory 42 years ago [3].

The book consists of 39 distinct chapters (or better call sections), of various pages lengths from 1 to 7. It covers almost all the basic concepts, ideas and results in elementary number theory. Roughly speaking, the theory of congruences is discussed in e.g., chapters 4, 5, 6, 16, 17, 18 and 19, the theory for arithmetic functions is introduced in e.g., chapters 7, 8, 9, 10, 11, 12, 13, 14, 29 and 39, whereas Diophantine equations and sum of squares are presented in e.g., chapters 3, 21, 22, 23, 24, 25, 26. There are also chapters devoted to the famous unsolved problems of Riemann's hypothesis and the ABC conjecture, as well as many other unsolved problems related to the distribution of prime numbers and the additive properties of integers such as the twin prime conjecture, the odd perfect number conjecture, the Mersenne prime conjecture and the Goldbach conjecture.

3 Opinion

This is one of the books in the MAA Guides series, others include A Guide to Complex variables, Real Variable, and Topology, etc. Since this is a small book, the book review must be short. What we would like to say is that this is a very nice book for anyone interested in number theory. However, if you want to know more about number theory, you can read this book first, make yourself familiar with the basic concepts and ideas of number theory, then read Baker's marvelous introductory book [4], or Hardy's authoritative and comprehensive book [1].

References

[1] G. H. Hardy and E. M. Wright, *An introduction to the Theory of Numbers*, Fifth Edition, Oxford University Press, 1979.

[2] J. H. Silverman, *A Friendly Introduction the Number Theory*, Third Edition, Pearson/Prentice-Hall, 2006.

[3] U. Dudley, *Elementary Number Theory*, Second Edition, Freeman, 1978.

[4] A. Baker, *A Concise Introduction to the Theory of Numbers*, Cambridge University Press, 1984.

Review of
Mathematical Tools for Data Mining:
Set Theory, Partial Orders, Combinatorics[31]
by Dan A. Simovici and Chabane Djeraba
Springer-Verlag London, 2008
ISBN: 978-1-84800-200-5
$129, 616 pages, Hardcover

Reviewer: Pauli Miettinen

1 Overview

Data mining is a field of computer science developing methods for finding things from data sets that you did not know to exists or even look for. While the field is relatively new, it has already produced a huge number of methods. Students and researchers alike can easily spend all their time on learning just the methods, without ever understanding the mathematics behind them. And as the authors note (p. v) "many students of data mining are handicapped in their research by the lack of a formal, systematic education in its mathematics." And, I must add, as today's students are tomorrow's researchers, this handicap is not limited to students.

To cure the handicap, the authors provide a formal, systematic treatise of mathematics behind data mining. But the task is immense: data miners do not limit themselves to any particular subfield of modern mathematics, but freely use any methods they happen to know and find suitable to the task at hand. The mathematics behind, say, frequent itemset mining, dimensionality reduction, and probabilistic mixture models are so different that covering them fully takes easily at least three volumes. The authors of this book have apparently reached the same conclusion. This book, as its subtitle reveals, covers what the authors call the set-theoretic foundations of data mining. The authors say (p. v) that they are planning two more volumes, covering linear algebra and probability theory.

The book is a math book, not a data mining book. Some data mining topics are discussed, but mostly to provide a superficial case study of the mathematics covered. So if you buy this book to learn data mining, you will be disappointed.

2 Summary of Contents

The book is divided into five parts, Set Theory, Partial Orders, Metric Spaces, Combinatorics, and Appendices. Each part is divided into chapters and each chapter (except those in Appendices) ends with a set of exercises and short bibliographical comments.

2.1 Set Theory

The back cover claims the book to be self-contained—and it very much is. The first part, Set Theory, starts with basic properties of relations and a definition of a function as a special type of relation. It also gives the basics of sets, sequences, and their functions, including power sets, partitions, countable and uncountable sets, and even the axiom of choice. As an application the authors give the very basics of relational data

bases, but in the spirit of this book, assuming nothing from the reader that is not yet covered, the authors cannot even discuss the relational algebra yielding a very superficial image of the topic.

The second chapter is about algebras with an emphasis on basics of linear algebra and matrices. Third and final chapter of this section covers graphs, trees, and hypergraphs. It contains topics such as heaps, minimum spanning trees, flows, and matchings. All in all, any student with basic information of mathematics and computer science should be able to skip this part, except for some notations used through the book.

2.2 Partial Orders

Partial orders, partially ordered sets (posets), and lattices are important concepts in data mining, and they are used extensively in connection with frequent itemset mining and related tasks. First chapter of this part presents the basic definitions and results about posets focusing on two important ones: the poset of real numbers and the poset of partitions of a finite set. Chains, antichains, poset products, and Möbius functions are also presented.

The second chapter is about lattices, covering topics such as complete lattices and Galois connection. The chapter continues with Boolean algebras and Boolean functions and ends with a case study application called Logical Data Analysis.

The topic of the next chapter in this part is a surprising one: topologies and measures. After all, at least I do not see any particularly strong connection between posets and point-set topologies or measures. Nor would I consider them even nearly as important tools for data miners as, for example, lattices are. But they will be needed later in the book, justifying the chapter. The topics covered are standard: open and closed sets, closures, dense sets, countable unions and intersections, compactness, continuous functions and others. For measures, the topics include σ-fields, measurable sets, outer measures, and, of course, measures, the Lebesgue measure being an important example.

Next the authors present the first application deserving its own chapter: frequent item sets and association rules. The authors present Apriori and Levelwise algorithms for finding frequent item sets and association rules, and show the connections of these tasks to lattices and posets.

The next chapter is entitled "Applications to Databases and Data Mining"—though the previous chapter was already an "application chapter." The main content of this chapter is not an application but a tool: the concept of entropy. The authors avoid the information-theoretic interpretation of entropy (as that would require much more background to keep the book self-contained) by defining it as a function over partitions of a finite set. And instead of restricting themselves to the usual Shannon entropy, the authors study a generalized version of entropy required to have certain reasonable monotonicity properties and "nice" behavior under addition and multiplication of partitions. The authors show that both the Shannon entropy and the Gini index are special cases of this generalized entropy.

The final chapter of this part is about rough sets, and the associated idea of approximating sets with (in some sense simpler) partitions. An example application in classification is given.

2.3 Metric Spaces

Clustering and nearest neighbor searches are two prominent data mining questions where metrics (or, more generally, dissimilarity measures) play a central role. In the first chapter of this section, authors define three dissimilarity measures, metrics, ultrametrics, and treemetrics, and give examples of them. A natural focus is on metrics, in particular for $\mathbb{R}^n$ and for set systems. The chapter ends with applications to k-nearest-neighbor and range queries.

The next chapter is about topologies and measures in metric spaces, covering the basics of the topic, including completeness and Cauchy sequences. The chapter ends with a short introduction to embedding of metric spaces. This chapter's main purpose, however, is to introduce necessary background for the next chapter.

The third chapter of this section is about the dimensions of metric spaces. This topic is motivated by the notorious "curse of dimensionality." The chapter focuses on various methods to define the "true" dimensionality of data, such as the inductive dimensions of topological spaces or the covering dimension for set systems. But notice that it does not discuss dimensionality reduction methods or any other related topics stemming from linear algebra.

The main application of this part's results is clustering, the topic of the fourth chapter. This chapter contains algorithms for both hierarchical and partition-based (like k-means) clustering, with various link functions for the former. It also covers Kleinberg's impossibility theorem, and ends with a short introduction to evaluating cluster quality.

2.4 Combinatorics

The last part before appendices contains additional topics from combinatorics, such as the inclusion-exclusion principle and Ramsey's theorem. It is also here the Sperner's theorem is presented. Nevertheless, the main topic of this part is the Vapnik–Chervonenkis dimension with its applications.

3 Style

The book follows a classical concise mathematics style: the body text contains definitions followed by lemmas, theorems, and corollaries, and their proofs. Every now and again an example appears. But virtually no motivation is given for theorems (except of type "this theorem generalizes the previous one"), the rationale behind the definitions must be deduced from their usage, and the connections between different theorems and concepts mentioned are those appearing in the proofs.

The self-contained nature of this book allows the authors to build on earlier material without repeating it. Sometimes that makes the text hard to follow as the reader can hardly remember notation introduced some 300 pages earlier. Adding to the confusion, the text has more than enough typographical errors. Most of the time they are easy to ignore and are irritating at worst, but sometimes they are in critical parts of theorems, proofs, or equations.

All this makes the book laborious to read. The style of books like this is always a compromise, and as the book already has over 600 pages, one can easily see why the authors did not select a more verbose style. But while the choice of the style is understandable, the lack of copy-editing is not. In addition to the errors, there are other aspects that create an unfinished impression, such as recurrent theorems and definitions that can have different names (Cauchy's inequality is first proved on page 67 and again on page 379 under the name "The Cauchy Inequality") or even be contradictory ("the product of 0 with either $+\infty$ or $-\infty$ is undefined" (p. 4) versus "$x \cdot \infty = 0$ if $x = 0$" (p. 139)).

4 Opinion

The authors mentioned the students' lack of formal education in mathematics as a motivation of the book. It is also "intended as a reference for the working data miner" (p. v). Does it fulfil these roles, and who else

could benefit from it?

As mentioned above, this is not a data mining book, and will not serve you well if you want to learn data mining techniques. The applications in this book tell you only the very basics, and will probably leave you wondering where do you need all the math covered.

Yet, you can read the book without knowing any data mining. If you need a concise presentation on some of the book's topics, then you could consider this book. Of course, if it is only one or two parts of the book you are interested in, a specialized book might be a better choice. And remember that these tools are not the tools to analyze an algorithm's time complexity; they are the tools needed to understand and develop the algorithms.

What about the students, then? The authors consider a "typical three-semester sequence in calculus" sufficient for "making the best use" of the book (p. vi). Not even that is needed, thanks to the self-contained form. But a student should know his data mining, and should have a strong mathematical intuition to avoid the book turning to a dull list of theorems and to see the connections where they are not mentioned and to understand the rationale behind the definitions. Alternatively, he should have a good teacher.

Teachers and researchers alike can benefit from this book as it provides a comprehensive reference. There are some drawbacks, though. The first is the number of typographical errors that require you to be rather careful when consulting this book. The second is the index. The book has one, but if you want to use this as a reference, it should have much more keywords. The third is a by-product of the big size and self-contained nature of this book. Using the book as a reference can be hard if in order to understand a theorem in, say, page 400, you need to find the notation and definitions buried somewhere in the preceding 399 pages. The pointers to previous material are very few in this book.

These drawbacks can be irritating, but compared to the the alternative—having half a dozen specialized books on the various topics—easy to ignore. Hence, in my opinion, this book is a useful reference for researchers and teachers. I am looking forward to the remaining parts of the planned trilogy—not least because they will increase the usability of this book even further.