The Book Review Column[1]

by Frederic Green
Department of Mathematics and Computer Science
Clark University
Worcester, MA 02465
email: `fgreen@clarku.edu`

In this column, six books are reviewed (across 5 reviews, one of them joint). The first five lie along what Bill Gasarch in his review aptly terms the "fractal" boundary between recreational and real mathematics, which can appeal to readers with a high school math education as well as professionals; the last, while of a technical nature, is still broad and certainly of general interest to our readers.

1. **Incredible Numbers**, by Ian Stewart. Reviewed by Frederic Green. A book about numbers and the fascinating mathematics that loves them.

2. **Mathematics Galore**, by James Tanton. Reviewed by William Gasarch. A collection of expository newsletters about mathematics, addressed to high school students with the goal of getting them interested in research, along with some of the original research itself.

3. **Math Bytes**, by Tim Chartier. Reviewed by John Tucker Bane. A fun book on the interaction between mathematics and computing.

4. **Algorithms Unplugged**, by B. Vöcking et al., Eds., and **The Power of Algorithms**, by Giorgio Ausiello and Rossella Petreschi, Eds. Joint review by Shiva Kintali. Two introductions to algorithms that can be read assuming a modest or even minimal mathematical background.

5. **Handbook of Finite Fields**, by Gary L. Mullen and Daniel Panario. Reviewed by S. V. Nagaraj. A detailed reference work on finite fields and their applications.

[1]

BOOKS THAT NEED REVIEWERS FOR THE SIGACT NEWS COLUMN

Algorithms

1. *Distributed Systems: An algorithmic approach (second edition)* by Ghosh.
2. *Tractability: Practical approach to Hard Problems* Edited by Bordeaux, Hamadi, Kohli.
3. *Recent progress in the Boolean Domain* Edited by Bernd Steinbach

Programming Languages

1. *Selected Papers on Computer Languages* by Donald Knuth.

Miscellaneous Computer Science

1. *Algebraic Geometry Modeling in Information Theory* Edited by Edgar Moro.
2. *Algebraic Coding Theory (Revised Edition, 2015)*, by Elwyn Berlekamp.
3. *Digital Logic Design: A Rigorous Approach* by Even and Medina.
4. *Communication Networks: An Optimization, Control, and Stochastic Networks Perspective* by Srikant and Ying.
5. *CoCo: The colorful history of Tandy's Underdog Computer* by Boisy Pitre and Bill Loguidice.
6. *Introduction to Reversible Computing*, by Kalyan S. Perumalla

Cryptography

1. *The Mathematics of Encryption: An Elementary Introduction,* by Margaret Cozzens and Steven J. Miller.

Miscellaneous Mathematics

1. *The Magic of Math*, by Arthur Benjamin.

Mathematics and History

1. *Professor Stewart's Casebook of Mathematical Mysteries* by Ian Stewart.
2. *The Golden Ratio and Fibonacci Numbers* by Richard Dunlap.
3. *An Episodic History of Mathematics: Mathematical Culture Through Problem Solving* by Krantz.
4. *Proof Analysis: A Contribution to Hilbert's Last Problem* by Negri and Von Plato.

Review of[2]
Incredible Numbers
by Ian Stewart
Basic Books, 2015
341 pages, Paperback, US $16.99

Review by
Frederic Green fgreen@clarku.edu
Department of Mathematics and Computer Science
Clark University, Worcester, MA

The 39 Steps (in Alfred Hitchcock's movie of that name) is an organization of spies collecting information on behalf of a certain Foreign Office of a country that goes unnamed. Mathematically, the number 39 has the distinction of being the sum of the 1st, 2nd and 3rd powers of 3, and the sum of 5 consecutive primes, such that if you take the product of the first and fifth you get 39. It also happens to be the number of chapters in Ian Stewart's new book "Incredible Numbers," which, interestingly, has no chapter numbered 39. You might think that's a consequence of starting with a Chapter 0. There is a Chapter 0 (it's the eleventh chapter in the book) but as it happens, the 39th chapter is Chapter 42.

As Stewart says, "numbers truly are incredible." And this charming, enthusiastic, and entertaining book talks about 39 of them. Chapter x is about number x, whence comes the unconventional numbering. Thus, Chapters 1 through 10 are about the numbers 1 through 10, respectively. Then we get into even more incredible territory in Chapters 0, -1, i, $1/2, \ldots$ (see below for an exhaustive list), culminating in $\aleph_0$, $\mathfrak{c}$, and, of course, 42. No doubt Chapter 39 didn't make the cut because it's not quite as interesting as the numbers that are treated; but we'll have a little more to say on the subject of "incredibility" shortly.

As the book is addressed towards a broad audience, I am sure there are SIGACT readers who already know all or at least most of what's in here. But personally, I learned quite a bit from it (some of which I find myself using in Math/CS courses!), and while in many cases I fancy it's stuff I once knew and have since forgotten, there was more material I had not and clearly should have known. And more often than not, it offered an insightful and fun perspective on what I *did* know.

While it's true that numbers are incredible, some are more incredible than others. Take e, π and i, for instance, which crop up everywhere, often where it appears they have no business being, sometimes all together (notably alongside 1 and 0 in Euler's formula). So while some of the numbers treated (e.g., $\zeta(3)$ (Apéry's constant) and γ (Euler's constant)) might seem a tad recondite for the general reader, and others (e.g., 11, 23, 26 and 56) might be something of a stretch as regards "incredibility," this is, to a large extent, beside the point. What is truly fascinating is the underlying mathematics. The chapter ordering was chosen to follow a (somewhat loose) logical, rather than numerical, progression (the latter would have been problematic due to the presence of i alone). The numbers themselves are *dramatis personæ*, characters that draw the reader into the mathematics.

The book is, not surprisingly, enumerative. It is divided into several natural sections, and the chapter numbers are already in themselves a source of amusement:

- Small Numbers: Chapters 1 through 10.
- Zero and Negative Numbers: Chapters 0 and -1.
- Complex Numbers: Chapter i.

- Rational Numbers: Chapters $\frac{1}{2}$, $\frac{22}{7}$ and $\frac{466}{885}$.
- Irrational Numbers: Chapters $\sqrt{2}$, π, φ, e, $\frac{\log 2}{\log 3}$, $\frac{\pi}{\sqrt{18}}$, $\sqrt[12]{2}$, $\zeta(3)$, and γ.
- Special Small Numbers: Chapters 11, 12, 17, 23, 26, 56, 168.
- Special Big Numbers: Chapters 26!, $43, 252, 003, 274, 489, 856, 000$, $6, 670, 903, 752, 021, 072, 936, 960$ and $2^{57,885,161} - 1$.
- Infinite Numbers: Chapters $\aleph_0$ and $\mathfrak{c}$.
- Life, the Universe, and…: Chapter 42.

Here is an enumerative description of some of the chapters n with $n \leq 10$:

- The book begins with a nice historically oriented *unnumbered* (horrors!) chapter[3] on numbers, the history of their notation, and gets as far as Frege's attempt to capture the concept in terms of classes. The verdict on Frege's definition is delivered in a chapter with a very large number!
- Chapter 1: There's more to say here than one might expect. For example I didn't know that 1 used to be regarded as prime. And in order to explain the concept of "1 as unit," it's a virtual necessity to get into the uniqueness of prime factorization.
- Chapter 2: The only even prime, and hence the oddest of them all. There are a great many concepts that come into play here: parity, the parity of a permutation (and hence permutations themselves), the binary system, and Fermat's sum of two squares theorem, to name a few. There's also the quadratic equation, and the subsequent two chapters discuss the solutions to the cubic and the quartic equations, and the sum of three- and four- squares theorems, respectively.
- Chapter 4: I liked Chapter 3, but Chapter 4 seemed to yield a richer set of topics: perfect squares, the four color theorem, quaternions, and four-dimensional (Euclidean) space!
- Chapter 5: The bad news is that there are no algebraic solutions for quintic (or higher) polynomial equations, but the good news is that we now get to meet Galois and some of his ideas. And the lack of crystals with 5-fold symmetry affords a nice opportunity to introduce the classic quasicrystals which "almost" have 5-fold symmetry.
- Chapter 7: As this is the fourth prime, and as the significance of primes has not yet been looked at, some generalities about primes are discussed here. Indeed, what could be of more practical interest in this regard than the problem of factoring a number? Here we have a nice discussion of the problem, including Fermat's (little) Theorem, the Fermat test, and even a mention of the AKS algorithm, so the phrase "polynomial time" makes a cameo appearance. A nice explanation of RSA ensues. And Brocard's problem, a new one on me: Is 7 the largest number n such that $n! + 1$ is a perfect square?
- Chapter 8: Here we meet Fibonacci numbers, Fermat's Last Theorem, and the Catalan Conjecture. Exercise for the reader: Explain why these make an appearance here.

Since the later chapters cannot be well ordered, it's interesting to point out some of the mathematics that appears in multiple chapters. These multiple appearances have the happy side effect of illustrating the unity of mathematics. For example:

[3] NB: Not included in my tally of 39.

- The Russell Paradox: Chapters 0 and $\aleph_0$. Its presence in Chapter 0 explained in part by the fact that it grew out of Frege's attempts at defining the integers, which were resolved by the von Neumann ordinal construction of the naturals from the empty set. No surprise we encounter Russell in Chapter $\aleph_0$!

- Prime Numbers: Chapters 1 and 7 (as already mentioned), Chapter $\frac{1}{2}$ (via the Riemann Hypothesis), Chapter 17 (that Gauss's construction works for Fermat primes), Chapter 168 (the symmetries of the Fano plane, leading into a discussion of finite cyclic groups); I'm sure I've missed some!

- Roots of unity: Chapters i, e, π, and 17. The first for the introduction of the idea, the last on account of Gauss' construction of the 17-gon. In Chapters e and π we meet Euler's formula $e^{i\pi} = -1$ (with an explanation).

- Fractals: Chapters $\frac{466}{885}$ and $\frac{\log 3}{\log 2}$: The former as a consequence of the intimate connection between the Towers of Hanoi and the Sierpinski Gasket (another new one on me, fun to explain in an intro CS course), and the latter by virtue of its fractal dimension.

As intimated earlier, some numbers are not quite as universally incredible as others, in particular because the underlying mathematics is not as deep or compelling, or possibly because the connection between the number and deep mathematics is tenuous. To take some examples: $\sqrt[12]{2}$ is the basis of the musical scale (in equal temperament, at any rate), and there is great interest in that alone. However (and as a music lover myself, I'm hesitant to admit this), the mathematics does not strike me as compellingly as that underlying π, for example. Chapter 26 is about cryptography, containing a lot of important and highly applicable mathematics. However, the fact that there are 26 letters in the Latin alphabet is more of a parochiality that has little to do with the underlying math. I'd also say the jury is out on how incredible 11 is, despite its connection with M-theory (the very deep, but yet-to-be-understood theory that supposedly unifies the various 10-dimensional superstring theories). This is one case where the number primarily offers a great excuse to talk about some very deep mathematics. Having said that, these are really minor quibbles. All of the chapters contain surprising and entertaining facts about mathematics, deep or otherwise.

One last minor quibble: I wish there were an index! Maybe "it's not that kind of book." But I, for one, looked for it more than once.

Is this a "popular" book? I think so. It is also therefore one of that growing genre that is not at all hesitant to set down equations such as,

$$\frac{1}{\pi} = 12\sum_{k=0}^{\infty} \frac{(-1)^k (6k)!(545,140,134k + 13,591,409)}{(3k)!(k!)^3 640,320^{3k+\frac{3}{2}}}$$

(the Chudnovsky series for approximating π), although this is probably the most daunting expression the reader will face. Equations and mathematical reasoning feature throughout, and also the occasional proof (e.g., the Pythagorean Theorem and Cantor's diagonalization). All of this is very welcome, and we may hope that the general reader will attempt to understand (or at least *appreciate*) as much as possible. Of course, those who are moderately familiar with mathematics (through a high school or elementary college course or beyond) will have no problem with this; in that case, the book can be quite inspirational. And Stewart has a special talent for conveying his own enthusiasm to the reader. I had a great time reading it.

And Chapter 42? *Pace* Douglas Adams, the author makes a good case that it's not at all a boring number. It beats 39, for sure.

Review of[4]
Mathematics Galore:
The First Five Years of the St. Marks' Institute of Mathematics
by James Tanton
Publisher: MAA
$50.00 hardcover, 268 pages, Year: 2012

Review by
William Gasarch gasarch@cs.umd.edu

1 Introduction

The author has gotten high school students into mathematics research via workshops and a newsletter that had expository math articles in it. This book is a collection of 26 of those newsletters. There are also several appendices some of which have original research done by the students.

Even though a high school student can understand the material it is interesting and sometimes surprisingly difficult. The chapters are well written and motivated.

2 Summary of Contents

I list some things I learned from the book that were both new and interesting (to me).

Chapter 1: Arctangents: Let $f_0 = 1$, $f_1 = 1$, $(\forall i \geq 2)[f_i = f_{i-1} + f_{i-2}]$, the familiar Fibonacci numbers. Then for all odd n,

$$\arctan\left(\frac{1}{f_n}\right) = \arctan\left(\frac{1}{f_{n+1}}\right) + \arctan\left(\frac{1}{f_{n+2}}\right).$$

Chapter 2: Benford's Law: Benford's law states that in many tables of numbers (e.g., log tables, IRS tax forms) more entries begin with 1 then with 2, with 2 then with 3, etc. Estimates are that 1 appears as the first digit around 30% of the time, 2 about 17% of the time. As stated above this is not rigorous. However, it is empirically true. In more well-defined settings (e.g., look at the table of powers of a number) this can be made rigorous. The author proves Benford's law in some cases.

Chapter 5: Dots and Dashes: The following is trivial: The nth square is n^2. But what about the nth *non-square*? It's not hard to work out; however, I had never thought of the question. The answer is *round*$(n+\sqrt{n})$ where *round*(x) is the rounded version of x.

Chapter 6: Factor Trees: When I teach discrete math (Honors Section) I want to show them that unique factorization over the integers is not obvious, and then that it's true (I could save time by just letting them think it's obvious). One way to show them the UF is not obvious is to show them a domain where unique factorization is not true. I often use $D = \{a + b\sqrt{6} \mid a, b \in \mathsf{Z}\}$. One can show that $2, 3, \sqrt{6}$ are all primes (defined properly) and hence $6 = \sqrt{6} \times \sqrt{6} = 2 \times 3$. So D is not a UFD. This chapter gives an easier example, though it is not an Integral Domain. Just take the even integers. A prime p is such that if $p = ab$

[4] ©2015 William Gasarch

then either $a = \pm 1$ or $b = \pm 1$. Note that $400 = 2 \times 2 \times 10 \times 10 = 2 \times 2 \times 2 \times 50$. Hence the set of even integers does not have unique factorization.

Chapter 16: Personalized Polynomials: I give a problem that is not from this chapter but is inspired by it. Let $p(x)$ be a polynomial of degree d such that $p(0), p(1), \ldots, p(d)$ are all integers. Show that, for all integers n, $p(n)$ is an integer. Hint: view $p(n)$ as a linear combination of $\binom{n}{0}$, $\binom{n}{1}, \ldots, \binom{n}{d}$.

Chapter 20: Repunits and Primes: It is well known that there is no polynomial $p(x) \in \mathsf{Z}[x]$ such that an infinite number of $p(0), p(1), p(2), \ldots$ are prime. What about if $p(x) \in \mathsf{Q}[x]$? $\mathsf{R}[x]$? $\mathsf{C}[x]$? The same holds!

Chapter 22: Tessellations: The plane can be partitioned into an infinite number of regular 3-gons, 4-gons, or 6-gons. What about 5-gons? 7-gons? In this chapter it is shown that 3, 4, 6 are the ONLY numbers n such that the plane can be partitioned into n-gons.

Appendix III-The Möbius Function: This chapter *motivated(!)* the Möbius Function and the Möbius Inversion Formula. I won't state the function or the formula, but I will state two fun problems they use to motivate it. In both the scenario is an infinite set of lockers numbered $1, 2, 3 \ldots$, and an infinite set of students numbered $1, 2, 3, \ldots$. The lockers are originally all closed. When student i walks down the hall he changes the status of lockers $i, 2i, \ldots$. (1) If the students walk down the hall in order: 1, 2, 3,... then which lockers are open at the end? (2) If you want to have only locker 1 open then which students do you send down the hall?

3 Opinion

While reading it I kept asking myself: "*Who would benefit from reading this book?*" This question is actually two questions: (1) who would understand this book, and (2) who would find things interesting and new in it. As I showed in the last section, a college professor (at least me) did find many things new and interesting. (I think "new and interesting" is equivalent to "interesting and new.")

A very bright high school student could benefit a lot from this book if he has some guidance in reading it, which I assume the original audience for this material did. A college professor will find some things new and interesting in this book.

4 Books of this Type

This is the 18th book of math essays on a variety of topics that I have reviewed. The other 17 are:

1. **Martin Gardner in the Twenty-First Century**, Edited by Michael Henle and Brian Hopkins,
2. **Selected Papers on Fun & Games**, by Donald Knuth,
3. **Six Proceedings from the Gatherings for Gardner Conference**, Edited by a variety of people,
4. **Dude, Can You Count?**, by Christian Constanda,
5. **Mathematical Treks: From Surreal Numbers to Magic Circles**, by Ivars Peterson,
6. **Professor Stewart's Cabinet of Mathematical Curiosities**, by Ian Stewart,

7. **Five Minute Mathematics**, by Ehrhard Behrends,
8. **Aha Gotcha!- Aha Insight!**, by Martin Gardner,
9. **Origami, Eleusis, and the Soma Cube**, by Martin Gardner,
10. **Hexaflexagons, Probability Paradoxes, and The Tower of Hanoi**, by Martin Gardner,
11. **Group Theory in the Bedroom and Other Mathematical Diversions**, by Brian Hayes.

There are other books that are borderline in that they were either too hard (e.g., Proceedings of the Erdős Centennial) or too focused (e.g., three books on *Games of no chance*). Having said that, the borderline between “recreational” and “real” math is a fractal.

The reviews of these books all have the same basic format: I say how well written they are, I describe some sample mathematics from the book, and I say it would be wonderful for your (1) great niece, (2) bright high school students, (3) bright undergraduates, (4) some combination of the above. This is not cynical—these books have been well written and are appropriate for some combination of (1), (2), (3).

How different are the books? I looked over all of my reviews and found, much to my surprise, that there is *very little overlap*. There is much math of interest that one can learn before it gets hard; some if it will be new and interesting to you!

Review of Math Bytes[5] of
Math Bytes
by Tim Chartier
Princeton University Press, 2014
130 pages, hardcover

Review by
John Tucker Bane
Tucker.Bane@icloud.com

1 Introduction

Math Bytes is made up of fourteen largely independent chapters and fifteen self-study problems spread throughout. The first three chapters are about math and computer science trivia with some limited real world applications. Chapters four through ten concern how a combination of math and computer science can be used to create, modify, and/or animalize images. Chapters eleven and twelve explain real world crossovers between math and computer science (for fun and profit!). Chapters thirteen and fourteen are a closing statement and a list of solutions to the self study problems posed throughout the book.

We summarize some of the chapters in more detail.

2 Summary

Chapters 4-10: Images

These chapters are (mostly) about how a computer can create and process images. Chapter 4 explains the process behind the creation of several varieties of fractals and gives step-by-step instructions on the creation of some simple ones. Instructions are given for making a fractal by hand, but use of a computer is recommended for larger or more complicated fractals. Chapter 5 explains how equations are used to create images. Chapter 6 is about finding paths in images, including mazes. Chapter 7 is about how computers deal with colors in images. Chapter 8 is about finding approximations to π by coloring a grid with M&M's. Chapter 9 is about distorting images to produce interesting effects, for example optical illusions. Chapter 10 is about forming an image out of a combination of other images.

Chapter 11: March MATHness: This chapter explains a series of statistical methods for creating "March Madness" brackets. A "March Madness" bracket is a prediction of which team will win in a series of basketball games where only the winner advances to the next round. This means that later predictions rely on earlier ones. Chartier starts with simple prediction methods, like assuming that whichever team has won the higher percentage of games in the past will win any particular game, and then compares the resulting brackets to the average human made bracket. He then introduces more sophisticated statistical methods to get better results.

3 Opinion

This book is a well written introduction to many topics in math and computer science. It didn't teach me much that I didn't already know (I am an sophmore computer science major), but it presents math and computer science topics in an accessible and fun way. Math Bytes is full of examples, pictures, and illustrations which make it very accessible and easy to understand. While I doubt this book would contain much new information for the readers of this column, it would be an excellent introductory text for less experienced students and enthusiasts.

So who should read this book? There is something in it for me, for you, and for Bill Gasarch's great niece.

Algorithms Unplugged
by B. Vöcking, H. Alt, M. Dietzfelbinger, R. Reischuk,
C. Scheideler, H. Vollmer, and D. Wagner, Eds.
2011, $40.00, Hardcover
Published by Springer
and
The Power of Algorithms
by Giorgio Ausiello and Rossella Petreschi, Eds.
2013, $40.00, Hardcover
Published by Springer

Joint Review by
Shiva Kintali

1 Introduction

Algorithms play an integral part in our daily lives. They are everywhere. They help us travel efficiently, retrieve relevant information from huge data sets, secure money transactions, recommend movies, books, videos, predict stock markets, etc. Algorithms are essentially simple extensions of our daily rational thinking process. It is very tough to think about a daily task that does not benefit from efficient algorithms. Often the algorithms that solve our daily tasks are very simple, yet their impact is tremendous.

Most of the common books on algorithms start with sorting, searching, graph algorithms and conclude with NP-completeness and perhaps some approximation and online algorithms. The breadth of algorithms cannot be covered by a single book. **Algorithms Unplugged** and **The Power of Algorithms** take a different approach compared to standard Algorithms textbooks. They are aimed at explaining several basic algorithms (written by multiple authors) in an intuitive manner with real-life examples, without compromising the details. This is how algorithms should be taught.

2 Algorithms Unplugged

This book is divided into four major parts. Each part has several chapters. Here is an overview of these parts and chapters.

Part I: The first part is about sorting and systematic search, i.e., finding things quickly. Chapter 1 introduces binary search, one of the most basic search strategies. A recursive implementation of binary search is explained using an intuitive example to find a CD in a sorted sequence of CD's. Chapter 2 explains insertion sort, one of the most intuitive comparison-based sorting algorithms and Chapter 3 explains mergesort and quicksort, two sorting algorithms based on the divide and conquer paradigm. Chapter 4 explains bitonic sorting circuits to implement a parallel sorting algorithm. Chapter 5 describes topological sorting and explains how to schedule jobs without violating any dependencies between jobs. Chapter 6 considers the string searching problem and explains the Boyer-Moore-Horspool algorithm. Chapter 7 considers the search problem in several real-world applications, and explains the depth-first search algorithm. Chapter 8 explains how to escape from a dark labyrinth using Pledge's algorithm. Chapter 9 defines strongly-connected components in directed graphs and explains how to efficiently find directed cycles. Chapter 10 introduces basic principles of search engines, introduces PageRank and explains how to find relevant pages in the World-Wide Web.

Part II: The second part deals with arithmetic problems, number theoretic, cryptographic, compression and coding algorithms. Chapter 11 presents Karatsuba's method of multiplying long integers that is much more efficient than the basic grade school method. Chapter 12 explains how to compute the greatest common divisor of two numbers using the centuries-old Euclidean algorithm. Chapter 13 explains the Sieve of Eratosthenes, a practical algorithm to compute the table of prime numbers. Chapter 14 introduces the basics of one-way functions which play a crucial role in the following chapters. Chapter 15 presents One-Time-Pad, a basic symmetric cryptographic algorithm. Chapter 16 explains Public-Key Cryptography, an asymmetric cryptographic method using different keys for encryption and decryption. Chapter 17 explains how to share a secret in such a way that all participants must meet to decode the secret. Chapter 18 presents a method to play poker by email using cryptographic methods. Chapter 19 and 20 presents fingerprinting and hashing techniques to compress large data sets so that they can be compared using only a few bits. Chapter 21 introduces the basics of coding algorithms to protect data against errors and loss.

Part III: The third part deals with strategic thinking and planning. Chapter 22 discusses broadcasting algorithms to disseminate information quickly. Chapter 23 presents algorithms to convert numbers into English words. Chapter 24 explains majority algorithms with applications and extensions. Chapter 25 explains how to generate random numbers. Chapter 26 discusses winning strategies for a matchstick game. Chapter 27 discusses algorithms to schedule sports leagues. Chapter 28 characterizes Eulerian circuits and presents algorithms to find them. Chapter 29 details how to approximately draw circles on a pixelated screen. Chapter 30 explains the Gauss-Seidel iterative method. Chapter 31 presents a dynamic programming algorithm to compute the distance between two DNA sequences.

Part IV: The final part is about optimization problems. Chapters 32, 33 and 34 describe shortest path, minimum spanning tree and maximum-flow algorithms, three basic optimization problems. Chapter 35 discusses the stable marriage problem and presents an algorithm to find a stable matching in a bipartite graph. Chapter 36 explains an algorithm to find the smallest enclosing cycle of a given set of points. Chapter 37 presents online algorithms for the Ski-Rental and Paging problems. Chapter 38 and 39 discusses the Bin-Packing and the Knapsack problems. Chapter 40 discusses the Traveling Salesman Problem, one of the most important optimization problems that challenged mathematicians and computer scientists for decades. Chapter 41 introduces the Simulated Annealing method to solve a basic tiling problem and the Traveling Salesman Problem.

At the end of every chapter there are references for further reading. Readers are highly encouraged to go through these references to get a better understanding of the corresponding concepts.

3 The Power of Algorithms

This book is divided into two major parts. Each part has several chapters. Here is an overview of these parts and chapters.

Part I: The first part is divided into three chapters. Chapter 1 gives a historical perspective of algorithms, origin of the word *algorithm*, recreational algorithms and reasoning with computers. Chapter 2 aims at explaining how to design algorithms by introducing the basics of graph theory and two algorithms techniques:

the backtracking technique and the greedy technique. Chapter 3 quickly introduces the complexity classes P and NP and the million dollar P vs. NP problem.

Part II: The second part is aimed at explaining several algorithms of daily life. Chapter 4 explains the Shortest Path problems, one of the basic optimization problems. Chapter 5 discusses the basics of Internet and Web Graphs and explains several algorithms related to Crawl, Index and Search the Internet. Chapter 6 discusses the basics of cryptographic algorithms such as RSA and digital signatures. Chapter 7 discusses biological algorithms. Chapter 8 explains networks algorithms with transmission delays. Chapter 9 discusses algorithms for auctions and games. It presents the Prisoner's Dilemma, coordination games, randomized strategies, zero-sum games, Nash's Theorem, Sperner's Lemma, Vickery-Clarke-Groves auctions, and competitive equilibria. Chapter 10 explains the power of randomness and its role in complexity theory.

At the end of every chapter there are Bibliographic Notes with several pointers for further reading.

4 Opinion

Overall I found these two books very interesting and well-written. There is a nice balance between informal introductions and formal algorithms. It was a joy for me to read these books and I recommend them to anyone (including beginners) who is curious to learn some of the basic algorithms that we use in our daily lives, in a rigorous way. I strongly encourage you to read these two books even if you have already read a bunch of other algorithms books.

There are no specific prerequisites to follow these books, except for a reasonable mathematical maturity and perhaps some familiarity with basic constructs of at least one programming language. They can be used as self-study texts by undergraduate and advanced high-school students. In terms of being used in a course, some of the topics in these books can be used in an undergraduate algorithms course. I would definitely suggest that you get them for yourself or your university/department library.

Review of[6]
Handbook of Finite Fields
by Gary L. Mullen and Daniel Panario
CRC Press, Taylor & Francis Group, 2013
Hardback

Review by
S.V.Nagaraj svnagaraj@acm.org
Chennai, India

1 Introduction

This review is about a Handbook of Finite Fields by Gary Mullen and Daniel Panario. The handbook has been published as part of the Discrete Mathematics and Its Applications series of CRC Press, Taylor and Francis Group. It contains encyclopedic information about finite fields and includes contributions by over 80 mathematicians and experts worldwide. The handbook is available in hardback (ISBN: 978-1-4398-7378-6, US $139.95) as well as ebook (ISBN: 978-1-4398-7382-3, US $139.95) formats. Discounts as well as purchasing options such as ebook rentals are also available. The handbook is a reference work rather than a textbook. The chapters of the handbook provide surveys of several topics related to finite fields. The companion website of the book http://www.crcpress.com/product/isbn/9781439873786 offers pointers to additional information such as tables and errata.

2 Summary

The handbook runs to over a thousand pages and contains seventeen chapters divided into three logical parts.

The first part is introductory and consists of two chapters that look at the history of finite fields and some basic properties of finite fields essential for the rest of the book. There is also a discussion about tables related to finite fields.

The second part on theoretical properties consists of eleven chapters. These chapters discuss topics such as irreducible polynomials; primitive polynomials; various types of bases; exponential and character sums and some of their applications; equations over finite fields; permutation polynomials; special functions over finite fields; sequences over finite fields; algorithms for factoring polynomials and computing discrete logarithms over finite fields; elliptic and hyper-elliptic curves over finite fields, and miscellaneous theoretical topics such as relations between integers and polynomials over finite fields; matrices over finite fields; computational linear algebra over finite fields; classical groups over finite fields, and Carlitz and Drinfeld modules.

The third part on applications consists of four chapters. There is discussion about combinatorial applications related to Latin squares; affine and projective planes; projective spaces; block designs; difference sets; other combinatorial structures, and Ramanujan and expander graphs. Algebraic coding theory is focussed on by looking at algebraic-geometric codes; LDPC and Gallager codes; turbo codes, raptor codes and polar codes. The chapter on cryptography studies stream and block ciphers; multivariate cryptographic systems; elliptic curve cryptography; hyper-elliptic curve cryptography; cryptosystems based on Abelian varieties,

[6] ©2015, S.V.Nagaraj

and finite field arithmetic for hardware implementations. The last chapter of the book discusses applications of finite fields in biology; quantum information theory, and engineering.

The book has an extensive bibliography containing 3084 references to the literature. The index is also helpful.

3 Opinion

The handbook lists hundreds of definitions; propositions; theorems, lemmas, corollaries, examples and remarks. However, no proofs are provided. Some problems and conjectures are also included. The reader should consult the references in the bibliography for further information. The handbook is not meant to be a textbook. Hence, substantial background in abstract algebra and discrete mathematics is required for understanding the material in the handbook.

The mostly widely cited book on finite fields is the book *Finite fields*, by Rudolf Lidl and Harald Niederreiter, Second edition, Cambridge University Press, 1997, ISBN 0-521-39231-4. That particular book contains over 2500 references and is essentially a reprint of the first edition published in 1983. Mullen and Panario were inspired by that book and focussed on advances in finite fields and their applications since 1983. Much research has been done in this area since 1983 as is evident from the huge number of papers and books published and patents issued, and from numerous applications to areas as varied as cryptography; coding theory; number theory; group theory; biology, and engineering to name a few.

Although the handbook covers numerous topics, it must be emphasized that full volumes have been written on many topics and sub-topics in the book. Mullen and Panario have aimed to provide comprehensive information in a concise reference book. However, due to space limitations certain topics that make novel use of finite fields may not have been covered in the handbook. For example, the Chor-Rivest cryptosystem is not discussed or cited. (B.Chor and R.L.Rivest, A knapsack-type public key cryptosystem based on arithmetic in finite fields, IEEE Transactions on Information Theory, Vol. 34 , No. 5, pp. 901-909, Sep. 1988). Likewise, not all information may be readily accessible through the index. For example, Burgess's bound is an important result regarding character sums. A search through the index does not help us but the bibliography tells us that this bound is discussed in pages 183 and 185 of the handbook. This illustrates that it often happens that what the reader wants is available in the book, but may not be straightforward to locate. A little perseverance from the reader will be beneficial in such instances. Very often the sought-after information may be readily available. For example, if the reader is eager to know what is known about Galois groups, the index indicates that page 20 of the book contains that information.

The handbook will be very useful for senior level students, teachers and researchers in mathematics and computer science. It will also be useful for scientists, engineers, and practitioners. The handbook is well-organized in spite of the diverse topics covered and the huge number of contributors. It is likely to become a standard reference book for the theory and applications of finite fields. The small font size employed in the handbook makes reading tables and formulae difficult. The handbook is reasonably priced despite the enormous amount of effort involved in its production. It will be a very useful addition to the libraries of academic and research institutions.