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

After this column I am resigning as SIGACT News Book Review Editor. I've been editing this column for 17 years which is longer than anyone should have a job of this type.

I have enjoyed editing this column and reviewing books. I have enjoyed getting to know publishers and authors and reviewers. I have enjoyed getting books in the mail that I *want* to read. I have not enjoyed giving those books to others who really *will* read them.

I want to thank all authors-of-books, authors-of-reviews, publishers, and readers-of-this-column. The first three mentioned were crucial to *getting* this column published. The fourth mentioned are *why* we get this column published.

Fred Green will be taking over starting with the next issue. If you want to review any of the books in the *Books we want reviewed* list then email both him

`fgreen@black.clarku.edu`
and me
`gasarch@cs.umd.edu`.

In this column we review the following books.

1. **Digital Signatures** by Jonathan Katz. Reviewed by Subhayan Roy Moulick. Digital signatures are used for a computer or person to verify who they are. This book looks at signatures that are based on hardness assumptions from number theory.

2. **A Walk Through Combinatorics** by Miklós Bóna. Review by Bill Gasarch. This is a textbook on combinatorics that has very broad coverage and many excellent problems.

3. **A Wealth of Numbers: An Anthology of 500 Years of Popular Mathematics writing** by Benjamin Wardhaugh. Review by Omar Shehab. When you say *Popular Mathematics Writing* you might think of Martin Gardner or Ian Stewart. If you know a bit of history you might think of Sam Lloyd. How far back does popularization of mathematics go? This looks at such articles, why they were written, what they contained, going back *several centuries*. The oldest article is from 1491.

4. **A Guide to Experimental Algorithms** by Catherine McGeoch. Review by Shoshana Marcus. Often when I read about an algorithm I wonder *I wonder if they coded it up?* or *I wonder how well that would do in practice?*. Designing experiments to answer these questions is difficult. There are many pitfalls to avoid. If you want to know how to do it right then **Read This Book!**

5. **Fundamentals of Parameterized Complexity (second edition)**. by Rodney Downey and Michael Fellows. Review by Rajesh Chitnis. Given a graph G and a number k, does V have a vertex cover of size k? This problem is NP-complete. What if you fix k? For example. Given a graph G does it have a vertex cover of size 17? You could solve this in roughly n^{17} steps. But it turns out you can do *much*

[1] © William Gasarch, 2015.

better. I think the current record is $n + (1.34)^{17}$. More generally the algorithm for VC with fixed k has a time analysis where the k does not go into the exponent but instead into the additive constant. Even if it went into the multiplicative constant that would be good. A problem is *fixed parameter tractable* if it has this property- fix the parameter and the time analysis does not put that parameter into the exponent. This is an important and on-going field of algorithms. This is not a second edition of their prior book on the subject (from 1998) but a brand new book.

6. **The King of Infinite Space: Euclid and his Elements** by David Berlinski. Review by Eownyn Cenek. Since very little is really known about Euclid any book about him has to be speculative. That's fine so long as the speculations are interesting. In this book, they are.

BOOKS THAT NEED REVIEWED FOR THE SIGACT NEWS COLUMN

Algorithms

1. *ReCombinatorics: The algorithmics of ancestral recombination graphs and phylogenic networks* by Gusfield.
2. *Distributed Systems: An algorithmic approach (second edition)* by Ghosh.
3. *Algorithmics of matching under preferences* by Manlove.
4. *Tractability: Practical approach to Hard Problems* Edited by Bordeaux, Hamadi, Kohli.
5. *Recent progress in the Boolean Domain* Edited by Bernd Steinbach
6. *Distributed computing through combinatorial topology* by Herlihy, Kozlov, and Rajsbaum.

Programming Languages

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

Misc Computer Science

1. *Introduction to reversible computing* by Perumalla.
2. *Algebraic Geometry Modeling in Information Theory* Edited by Edgar Moro.
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.

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. *Mathematics Galore! The first five years of the St. Marks Institute of Mathematics* by Tanton.
4. *Mathematics Everywhere* Edited by Aigner and Behrends.
5. *An Episodic History of Mathematics: Mathematical Culture Through Problem Solving* by Krantz.
6. *Proof Analysis: A Contribution to Hilbert's Last Problem* by Negri and Von Plato.

Review of[2]
Digital Signatures
by Jonathan Katz
Springer, 2010, 192 pages
Hardcover, \$95.00, Softcover \$105.00

Review by Subhayan Roy Moulick subhayan@acm.org

1 Introduction

Digital Signatures are one of the most prominent applications of (public key) cryptography. They ensure integrity and authenticity in digital communications (in public channels). One of the most commonly used applications of digital signatures are for issuing digital certificates, particularly in the internet. When a web browser visits a (secure) website, it looks for a digital certificate, which verifies the identity of the website. A digital certificate is granted by a trusted third party, called a ”certificate authority”. It is (mainly) because of digital signatures, that one can hope to have secure e-commerce like services over the internet and protocols like the https to work effectively. Digital Signatures are also used in Electronic Smart Cards, software vendors to authenticate their distributions. (The book talks a bit more about this!).

While digital signatures have several other important applications, they are also very interesting to study mathematically. Digital signatures are a form of asymmetric (public) key cryptography. Asymmetric Key Cryptography, requires two different (sets of) keys, a Public Key, known to all, and a corresponding Private key (which is chosen such that it satisfies some mathematical 'bindings' with the Public Key) which is a secret, (often) known only to the associated user.

At a high level, a digital signature scheme consists on three algorithms, $(Gen, Sign, Verify)$. The Gen is a generator function that sets up the parameters and assigns keys. The $Sign$ algorithm, on input a message, m and a secret key, K_{sk} and produces a signature, σ, that can be (universally) verified with a public key, K_{pk}, (usually) without any further interactions with the signer, using the $Verify$ algorithm.

An ideal digital signature scheme is expected to be unforgeable, i.e no one without the K_{sk} should be able to produce a valid σ (under the signer's name) and non-repudiation (of origin), which says after a signer has signed a message, the signer should not be able to deny his signature on the message.

Digital Signatures were initially introduced back in 1970s, when Diffie and Hellman conjectured the existence of such schemes. The later works of Rivest, Shamir, Adelman; Lamport, Rabin and others proved their existence. Goldwasser, Micali and Rivest later studied their security and gave concrete definitions of their security.

2 Summary

It may be noted, at this point, the book only covers Generic Constructions and Standard Constructions based on Number Theoretic Assumptions, and shies away from non-number theoretic constructions involving lattices or code based schemes. This, however, in no means, makes the book any less valuable.

Also, not all chapters in the book are independent, and it may not be ideal to jump between the chapters. Discussions in the i^{th} chapter may follow from results from the earlier chapters

[2] ©2015, Subhayan Roy Moulick

The first part, consists of two chapters, and is (literally) ”Setting the Stage”. The first chapter quickly reminds the reader the nitty-gritty formalisms and the properties of digital signature and talks about notions (and formal definitions) of their security. It then goes on to draw relations between the notions of security. It also gives two important constructions that ’amplify’ the security of weaker schemes and proves how one can achieve CMA-secure (i.e secure against Chosen Message Attack) schemes using a RMA-secure (i.e secure against Random Message Attack) scheme and KMA secure (i.e secure against Known Message Attack) scheme respectively. Finally it concludes by recalling Bellare and Shoup’s construction for achieving strong Unforgettability from standard schemes.

Chapter 2 talks about the Cryptographic Hardness Assumptions (used in the book). Apart from discussions about standard assumptions of One-way Functions and One-way Permutations, (double enhanced) Trapdoor Permutations, there’s also a good discussion about Clawfree (Trapdoor) Permutation. Specific Assumptions discussed here are the factoring problem (and quadratic residue problem), RSA Assumption and Discrete Log Assumption. The chapter concludes with a thorough study of Hash Functions, constructions of collisions resistant (from clawfree permutations) and universal one way hash functions, and their applications in digital signatures schemes - by way of increasing the message length and reducing the public key length

Part II is where things become interesting. It surveys Digital Signature Schemes whose security rely on the Standard Model.

Chapter 3 talks mostly about One Time Signatures. It formally discusses Lamport’s One Time Signature Scheme and shows how to achieve strong Unforgettability. It then introduces the notion of Stateful and Stateless signature schemes, and exemplifies two important generic (stateful) constructions for Chain Based and Tree Based Signatures, and talks about their security and efficiency, in terms of the number of messages being signed. Finally concludes the section with a clever modification to convert the previous stateful Tree based scheme to a stateless signature scheme. The last section shows how to construct a CMA-secure signature scheme from any one-way function.

Chapter 4 discusses Signature Schemes based on the RSA assumption and Strong RSA Assumption. Following a, quick, necessary and sufficient introduction to the technical preliminaries, it describes the Dwork-Naor Scheme and Cramer-Damgard Scheme, which is a modification of the Dwork-Naor and improves on the drawback of large public keys in DN Scheme. Finally Hohenberger-Water’s scheme is introduced which is *short* as well as a stateless signature scheme from the RSA assumption. This is followed by a discussion on schemes based on Strong RSA Assumption.Following a description of construction of a KMA secure scheme, it discusses the Cramer-Shoup Scheme and the Fischlin Scheme. It then presents the Gennaro-Halevi-Rabin Scheme. The GHR Scheme discussed here has been made surprisingly easy to analyze due to a simple assumption.

Chapter 5 gives a brief overview of constructions based on Bilinear Maps. The use of Bilinear Maps in cryptography has become prominent only in the last decade, and is extremely popular in constructions of certificate-free schemes (such as identity based schemes, certificateless crypto, etc). The chapter gives a very high level introduction to Bilinear Maps and then describes the full version of Boneh-Boyen Scheme and the Waters Scheme. However in the Waters Scheme, the security analysis is given for the signature scheme only not for IBE, as in the original paper (This is apt to the context of the book).

Part III broadly talks about Signature Schemes in the Random Oracle Model. Random Oracles in cryptography are modeled after ”ideal” hash functions that map a fixed-length string (from the input space) to a (truly) random string (from the output space). Chapter 6 is dedicated to the Random Oracle Model and also probes its validity and soundness, and talks about the negative results and how security of schemes proved in the random oracles is relevant in practice.

Chapter 7 discusses Signature Schemes related to Full Domain Hash (FDH). A Full Domain Hash is a provable secure scheme in the Random Oracle Model, that follows a hash-and-sign paradigm. Following the a construction based on trapdoor permutations, it also shows an approach using Bilinear Maps, given by Boneh-Lynn-Shacham. (BLS-Scheme was one of the most important papers that got attention to Bilinear Maps). It concludes the chapter with discussions on a probabilistic variant of FDH (PFDH), first using a random salt as a part of the signature and then a (deterministic) variant without the random salt.

Chapter 8 gives an overview of Signature Schemes derived from Identification Schemes. With an introduction to Identification schemes and the notion and criteria for passive security for such schemes - Honest-verifier zero Knowledge (HVZK) and Special Soundness., the chapter describes the Fiat Shamir Transforms. Following ideas of protocols that are HVZK and satisfy special soundness, and a construction of OTS from canonical Identification scheme the chapter concludes with demonstrations of Secure Identification Schemes, namely, Goldwasser-Micali-Rackoff Identification Scheme, Fiat Shamir Identification Scheme, Guillou-Quisquater Scheme(RSA) Assumption), Micali/Ong-Schnoor (Blum Integers are hard to factor), Schnorr (Discrete Log Problem).

3 Opinion

I was really impressed by the scope and flow of the book. The book talks about the constructions of digital signatures and drives it home. Each chapter is rigorous and complete in its own right, yet there is a level of simplicity and elegance maintained throughout the book that makes it very readable.

One of the many things I really appreciate about this book is, unlike other graduate level books, the author is polite enough to actually give informal proof sketches before actually diving into the formalisms. It can be seen how well the author tried to keep the discussions complete, yet keeping the material accessible to someone who has had only an introductory course in cryptography, while maintaining necessary formalism, that one would expect in a advanced monograph. Also the references at the end of the chapter are very up to date and one can find necessary pointers to dig deeper into the topics of interest.

As the author says in the preface, ”this book has been written with a beginning graduate student in mind: a student who is potentially interested in doing research in the field of cryptography, and who has taken an introductory course on the subject, but is not sure where to turn next”, and I think the book exceeds expectations in that context. The book does a admirable job in its attempt to give a survey of digital signatures. The breadth and completeness of topics covered is praiseworthy. A reader who assimilates the material would have a commendable proficiency in the area, and can possibly find further research directions.

The book is essentially a ”Greatest Hits Collection” of Digital Signatures, and I would highly recommend it to graduate students and early stage researchers interested in cryptography and Digital Signatures, who have taken a first course in cryptography.

Review of[3]
A Walk Through Combinatorics
by Miklós Bóna
World Science Publishing, 2011
550 pages, Softcover, $55.00, Paperback

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

1 Introduction

Combinatorics is both the easiest and hardest branch of mathematics. What? It's the easiest since you do not need that much background to begin learning it and even doing research in it. This makes it a popular topic for high school math competitions and high school math projects. It's the hardest since either there are fewer tools to help you or they are extremely hard (e.g., Szemeredi's regularity lemma). In summary, its easy since you don't need hard tools, its hard since there are no hard tools, except ones that are really hard.

There is much one can learn in combinatorics before ever using hard tools. How much? This book is 550 pages and could be read by a *very* good high school student. That does not mean its an easy read. But it does mean that any reader of my column can read this book cover to cover and learn much that she does not already know.

This book is intended for a year-long undergraduate course in combinatorics. It covers all of the basic results one would expect and a selection of advanced topics as well. There are *many* very good problems in it. I went through the problem sections intending to mark the problems that were interesting that I might use in my class or on a math competition. I ended up making almost all of them. I repeat- the problems in this book are, as the kids say, **awesome**.

2 Summary

There are four sections called (I) Basic Methods (2 chapters), (II) Enumeration methods (6 chapters), (III) Graph Theory (4 chapters), (IV) Horizons (8 chapters).

The *Basic Methods* section truly are basic: the the Pigeonhole principle and induction. The chapter content is standard though done well. There are many problems, some quite clever.

The *Enumerative Combinatorics* section has the usual: permutations, combinations, binomial theorem (including for non-integer exponents), partitions, cycles in permutations (is that usual?), the law of inclusion and exclusion, ordinary generating functions, and exponential generating functions. Most textbooks in combinatorics have only a subset of these topics. There were a few theorems I had never seen before, and again many very good exercise on all levels. Here is an example of a theorem that was new to me:

Theorem 6.9 Let $a_1, \ldots, a_n$ be nonnegative integers so that $\sum_{i=1}^{n} ia_i = n$. Then the number of permutations with a_i cycles of length i where $i \in [n]$ is

$$\frac{n!}{a_1!a_2! \cdots a_n! 1^{a_1} 2^{a_2} \cdots n^{a_n}}.$$

The *Graph Theory* section has information on the standard topics: matchings, coloring, and planarity. They are covered well and Again, done well and lots of exercises.

The *Horizons* section comprises 44% of the book. There are many topics here, some standard and some not. We present the topics and one item in each.

- *Ramsey Theory* In addition to the usual Ramsey Theorem they have the following Ramseyish theorem: Let T be a triangle with angles 30-60-90. For all 2-colorings of the plane there exists a triangle congruent to T where all the vertices are the same color.
- *Subsequence Conditions on Permutations* The number of permutations that do not have a 132 pattern (that is, no $\cdots a \cdots b \cdots c \cdots$ where $a < c < b$ is the Catalan number $\binom{2n}{n}/(n+1)$.
- *Prob Method* If G is a graph with n vertices and m edges then G has a bipartite subgraph with at least $m/2$ edges.
- *Partial orders and lattices* Dilworth's theorem: A partial order has width w iff it can be covered with w chains.
- *Block designs and error correcting codes* One way to motivate block designs is via competitions: If need to set up a competition between n runners, but only k can use the track at any one time, how can you do this fairly (this needs to be defined) so that the first, second, etc best can be determined. Error Correcting codes are well known to my readers. This chapter talks about both and the connections between them.
- *Counting unlabeled structures* If you have four colors and want to color the edges of a hexagon, how many ways can you do that, noting that (say) $RRBGWG$ is equivalent to any of its cyclic rotations. It turns out to be 700. Why 700? Read the chapter to find out how to solve this and many related problems. Group theory is used to keep track of symmetries.
- *Combinatorial algorithms* and *P vs NP*. Both of these chapters give a brisk introduction to the subjects. There will be nothing new for the readers of this column.

3 Opinion

This is a rather comprehensive book on combinatorics. For all combinations of topics in combinatorics that you want to cover, they are in this book. Exposition is clear, coverage is massive, and the problems are plentiful and excellent.

Review of[4]
A Wealth of Numbers : An Anthology of 500 Years of Popular Mathematics Writing
by Benjamin Wardhaugh
Princeton University Press, 2012
370 pages, Hardcover-$40.00, Kindle-$37.00

Review by Omar Shehab shehab1@umbc.edu

1 Introduction

This book presents a representative collection of popular mathematics publications in the history of English language. The author has his own choices of categories under each of which he mentions important publications starting from the epoch to date. He also elucidates why the publication was considered representative by describing the culture and time when the publication took place and created impacts. To the amusement of the readers, he occasionally also brings in the perspective of different other categories while discussing a representative publication under a particular category. This three hundred and seventy pages long journey is one which takes you to your cultural past of the popular intellectual practices, taken place over last five hundred years, which shaped what you see around and read today. It helps you to connect the scene of an old lady seating right next to you in the bus solving Sudoku to the social and cultural evolution popular mathematics underwent throughout these centuries.

2 Summary

Wardhaugh has chosen eleven themes for the book. For each theme, there is a rich chapter, in general, starting somewhere around the sixteenth century. Then, it gradually mentions at least one important publication from each subsequent century to today. The author also shows how the ideas and presentations evolved from generations to generations while keeping the passion for recreational mathematics same as it originally was. The themes are - Mathematical Games, Arithmetic and Algebra, Problems and Puzzles, Geometry and Trigonometry, Popularization of Mathematics, Mathematical Instruments, History of Mathematics, Practical Mathematics, Pedagogy of Mathematics, Philosophy of Mathematics, and Mathematics in Fiction. We dedicate a section for each them in the rest of this review.

2.1 Mathematical Tricks, Mathematical Games

This chapter reviews seven publications published in between 1564 and 2004. The first publication is *The Wellspring of Sciences* by Humfrey Baker from 1564. This had been a very successful arithmetic primer and one of the very first books on recreational arithmetic printed in England. The second publication, *Mathematical Recreations* by Henry van Etten, published in French a century later also contains trick problems along with standard arithmetic. It even discussed the, then recently invented, telescopes by Galileo Galilei. The next publication was an extract from the works of William Leybourne published in 1667. Being a surveyor, he discussed several problems interesting to landowners and surveyors. Almost half a century later, another book was published with a really long title covering everything from arithmetic to pyrotechnics. I think that Wardhaugh kept it in the list because of the diversity of its contents. He then discusses two more publications of later centuries both focusing on the use of arithmetic for winning combinatorial challenges. The last mention is not a book but the NRICH website, `nrich.maths.org`. This website is a popular place of free and open exchange of mathematics learning materials both for teachers and student up to secondary level. It is based in both the University of Cambridge's Faculty of Education and the Centre for Mathematical Sciences.

2.2 From Arithmetic to Algebra

This chapter reviews ten publications published in between 1543 and 1931. As the abstraction in mathematics had been a growing practice, algebraic techniques for solving arithmetic problems were also becoming more commonplace. At the same time improvement in algebraic notations was also making it stronger. Here is an example from the previous chapter which is in rather descriptive form.

> **..., if a man casts three dice, you may know the score of each of them**
>
> Ask him to double the score of one die, add 5, and then multiply by 5. Next, add the score of one of the other dice, and append to the result the score of the last die. Then ask him what number he has. Subtract 250, and there will remain 3 digits, which tell you the points of the three dice.

On the other hand in the current chapter, the example of adding numbers suggests to write them one under other and then draw a line and keep adding columnwise. It is mentioned as follows.

> MASTER: ... I must write those two numbers, one over another, writing the greatest number highest, so that the first figure of the one be under the first figure of the other, and the second under the second, and so forth in order. When you have so done, draw under them a straight line: then will they stand thus: ...

The first two publications, by Robert Recorde and Thomas Masterson respectively, from 1543 and 1592 introduces mechanized rules for addition, subtraction, multiplication and division. The next two publications, by John Tapp and Edward Hatton respectively, discusses general and decimal fractions. We are talking about the time line of 1621 to 1695 when the merchants and engineers were increasingly using fractions in abstract form. A 1771 publication in this chapter also mentions the now obsolete *rule of three* of arithmetic which is a shorthand of cross-multiplication between two fractions. The next publication from 1792 presents the same rule in verses so that young learners could memorize. In later centuries people started getting more insights about algebra. Joseph Fenn, in one of the very first English book of analysis, published in 1775, discussed how problems are expressed in terms of algebraic equations and how to solve the first degree ones. The rest of the publications are from later years and obviously about how to solve systems of even more involved equations.

2.3 Problems, Puzzles, and Challenges

Compare to arithmetic and algebra, purely recreational and abstract mathematical problems had a late entrance in English literature. Wardhaugh has chosen six publications ranging from 1798 to 1989 for this chapter. By 1798, the English speakers were already familiar with algebra and geometry hence the problems of the oldest publication by Charles Hutton, a long running series for female math enthusiasts is not much of a surprise. Careful readers might ask about the significance of publishing popular mathematics books in as early as eighteenth century. Does it mean that, back then women had higher social status then today in the society? I am not sure what to make of it. Throughout the book I have found titles like - ”The Ladies Diary” (1798), ”The Girl’s Own Book” (1835), ”The Boy’s Own Magazine” (1855), ”The Young Gentleman’s Trigonometry, Mechanicks, and Opticks” (1714), ”Sir Isaac Newton’s philosophy explained for the use of the ladies” (1739), ”Higher Mathematics for Women” (1912), etc. I am not sure what conclusion I should arrive at. The next two publications are from 1835 and 1855 written for juvenile readers covering a wide range of problems. By then, the problems were always in abstract nature using standard algebraic or geometric notations. The extracts of the rest of the publications contain pretty much the same forms and difficulties of the problems solved by the school children these days.

2.4 Geometry and Trigonometry

Being about topics older than abstract mathematical problems, this chapter takes us back to 1500s again. The first publication is by Robert Recorde who was also mentioned previously in the first chapter. His definitions of basic concepts of geometry remind us of *Elements* by Euclid. The 1650 publication of Thomas Rudd and the 1705 publication by Edmund Scarburgh present different sections from the *Elements* to the English readers. In later centuries, geometry in English literature saw the spin off of trigonometry as a new branch. The notations and definitions were yet to take the form of modern trigonometry in the publications of 1700s though. A publication from 1854 shows how the field had been growing over time in terms of complexity. The last publication from 1956 by Alan Clive Gardner written for seamen presents the notations and definitions of trigonometry as they are today in the textbooks.

2.5 The Worlds of Mathematical Popularization

Popular mathematics had it’s first stride in early eighteenth century when the then new Newtonian science was needed to be explained to amateurs. Even before that, as mentioned by the author, there were regular sections in newspapers where readers used to send mathematical problems to get answered to by mathematicians. The Athenian Mercury published from 1691 to 1697 is one such example. The chapter also mentions one of the first presentation of Newtonian mechanics for amateur readers by Francesco Algarotti in 1739. Then we take a giant leap to more than one century later and there we are with the nineteenth century classic by W. W. Rouse Ball which came out in 1892. Now we are about to see the second stride of the popularization of mathematics which started in twentieth century and still continuing. The chapter mentions seven publications from this phase which clearly indicates that the interest of in popular mathematics is now at it’s all time high.

2.6 Mathematical Instruments and How to Use Them

The first publication in this chapter by Martín Cortés in 1561 discusses how to make navigation cards for seafarers. Another publication from the same century teaches us how to make a sundial with minute details. Then the chapter moves on and discusses, due to John Napier, how to compute faster with number rods as documented by Seth Partridge in 1648. In those days mathematics was yet to spun off from philosophy let alone physics or astronomy. So, manuals of telescopes from 1800s are considered as publications on mathematical instruments. Three more publications were mentioned, one from the nineteenth century by J. F. Heather, which mentioned how to make scales to measure distances by navigators, two from twentieth century, a book on making astronomical tools by Roy Worvill and a book on doing astronomical calculation on personal computer by Peter Duffet-Smith.

2.7 Mathematicians Past

History of mathematics has always been an important section of mathematics literature. Voltaire's *Letters Concerning the English Nation*, dated 1733, was one of the early enlightening classics in English language. Three of the letters discussed Newtonian, more specifically, the genesis of calculus. The celebrated dictionary of mathematics by Charles Hutton published in 1796 recorded history of mathematical concepts, one of the early examples of its kind. Two nineteenth century publication was mentioned where the life of early mathematicians and their contributions were discussed in equal important. The rest of the chapter contains six twentieth century publications discussing mathematicians of different ages starting from ancient Pythagoras to last century's Ramanujan. Back in those days women were always kept away from professions which were intellectually demanding. Despite this segregation, many female mathematicians were able to make fundamental contributions because of their geniuses. One such mathematician, Emmy Noether, was featured in one of the nineteenth century publications.

2.8 Mathematicians at Work

Popular mathematical writings on practical uses are sometimes trade and tool specific. So, some of the publications may seem uninteresting to the readers who are uninitiated. The first literature by Leonard Digges, published in 1579, is a manual on how to distributed and form the army battalions in a limited area camp ground. The second mention was from almost a century later by William Hunt. It was on gauging volumes of vessels containing liquids subject to taxation. Five more articles were mentioned from eighteenth, nineteenth and twentieth centuries discussing different trades, namely, sailing, engines, metallurgy, plumbing, hydraulics, automobiles, printing etc.

2.9 Thoughts on Teaching and Learning Mathematics

The pedagogical evolution of mathematics has it's very rich history. The first publication in this chapter is a 1590 advertisement of a semi-boarding school which used to teach arithmetic, *Arithmetic vulgar* as they had said, to *children and servants*. Later, the professor and priest Isaac Barrow, in his 1660 introduction to Euclid's book, discusses how the newly introduced algebraic notations makes teaching mathematics much easier. Euler's letters to the German princess Anhalt-Dessau, sent twice each week from 1760 to 1762, discussed applied mathematics which were always, interestingly, in the language of geometry instead of algebra. Two of the later century literatures were focused on enabling the mothers with better pedagogical tools to teach their children. Among other publications, one of the obvious choices was *The Game of Logic* by Lewis Carroll published in 1887 who was otherwise famous for *Alice's Adventures in Wonderland.*

2.10 Reflections on Mathematics and Its Place in the World

Since mathematics (more accurate it's early branches like geometry, arithmetic, algebra etc.) had started spin off as a noticeably different sub-discipline of philosophy, interested parties have always wondered where is it's place in the consolidated body of human knowledge. Initially, the importance of mathematics was judged by it's ability to solve practical problems. The publications from 1481, 1570, 1664, 1705, 1710, 1798, 1825 and 1834, as mentioned in this chapter, are witnesses to that. An interesting extract dated 1870 due to J.

J. Sylvester was also mentioned which complained about the too much abstractness in the mathematical problems practiced by the learners of those days. Since twentieth century, the place of mathematics in the human body of knowledge has started to be judged by it's internal complexity and philosophical aspects. Publications by Keyser, Feynman and Hammond, mentioned in this chapter, are evidences of this newly formed approach.

2.11 Fiction and Humor

As goes the title, this is the most hilarious chapter of the book. The first mention was by Margaret Cavendish, published in 1666, who was the only woman to attend a meeting of the Royal Society in the seventeenth century. She created a fantasy world in her book poking fun at different groups of mathematicians. The second publication, by Eliza Heywood, is a utopian fiction published in 1727, interestingly, takes, a stand against mathematics comparing it with sorcery. In John Kirkby's 1745 desert island novel, the protagonist Automathes was trapped with some food and, you would love to know, few mathematical tools he over the time teaches himself an idiosyncratic form of mathematics. Isn't that creative? The rest of the publications contain a number of poetry about mathematics and a few very interesting illustrations. This is the last chapter of the book you would want to miss.

3 Opinion

Benjamin Wardhaugh has been very successful in communicating how popular mathematics writing in English has evolved in last five hundred years through this book. The book tracks how popular take on mathematics has changed from the perspective of both practical and recreational. The tools and pedagogy have also faced the test of time and transformed accordingly. Being a scholar of the history of mathematics, the author was very lucid about justifying his picks. It was also interesting to see how he cross-connected literatures from different themes but same century to show how the culture of popular mathematics writing has influenced the century when it was written. Are you an English speaker? Ever wondered how mathematics was popularized in your society? Go and read this book!

Review of[5] of
A Guide to Experimental Algorithmics
by Catherine C. McGeoch
Cambridge University Press, 2012
261 pages, Softcover$45.00, Hardcover-$100.00

Review by Shoshana Marcus shoshana.marcus@kbcc.cuny.edu

1 Introduction

The foundational work in the field of algorithm design and analysis has been with a theoretical approach, designing in pseudo code and analyzing the algorithm's asymptotic bounds. Conducting experiments can help researchers gain insight into the practical efficiency of an algorithm. Insights from laboratory experiments can be more precise and realistic than pure theoretical analysis provides, and also more general than field experiments can produce. Experimental algorithmics combines the coding and measurement tools of the empiricist with the abstraction-based approach of the theoretician.

The experimental approach to analyzing an algorithm complements the other approaches to understanding algorithmic performance. Yet, it does not replace them. The field of experimental algorithmics is intended to bridge the gap between theory and practice in the design of algorithms. Often, theoretical advances in computer science are not as useful as purported to be. Similarly, it is often the case that an algorithm does not seem optimally efficient from a theoretical standpoint, yet it is useful in practice. The burgeoning field of experimental algorithmics provides a common ground for theoreticians and practitioners to exchange insights and discoveries about algorithm and program performance.

Computational experiments on algorithms can supplement theoretical analysis by showing which algorithms, implementations, and speed-up methods are best suited for specific problems, not just in theory but also in practice. This book guides the reader through the process of designing experiments to analyze algorithms, from deciding what properties to measure and what inputs to test to understanding how to analyze the data gathered. This book draws on ideas from the fields of algorithm design and analysis, computer systems, and statistics and data analysis.

This book's wide-ranging discussion includes a tutorial on system clocks and CPU timers, a survey of strategies for tuning algorithms and data structures, a cookbook of methods for generating random combinatorial inputs, and a demonstration of variance reduction techniques. The book is sprinkled with extensive case studies and examples that show how to properly apply these concepts. Its audience is intended to include anyone who is already equipped with some understanding of data structures and algorithms. Thus, any prerequisite understanding of computer architecture and data analysis are covered in the text.

Experimental algorithmics is intended to stimulate research in algorithms based upon implementation and experimentation. It seeks to encourage the testing, evaluation and reuse of complex theoretical algorithms and data structures. It aims to distribute programs that implement state-of-the-art algorithms, along with testbeds, throughout the research community and to provide a repository of useful programs and packages to both researchers and practitioners. Until focus was placed on experimental algorithmics, repositories were not readily available, and most researchers were faced with programming their own versions of well-known algorithms and data structures.

[5] ©2015, Shoshana Marcus

Many published algorithms and data structures have never been implemented and are at risk of remaining purely in the theoretical arena. To bring such algorithms and data structures into the practical realm often requires considerable sophistication in application. Thus, researchers need to be encouraged to turn their talents in that direction by engaging in experimental algorithmics. This book seeks to achieve this goal by teaching theoreticians how to experiment effectively.

The author is an authoritative expert in the field of experimental algorithmics. Catherine McGeoch is one of the founding members of this emerging subfield of the algorithms community. She is a past Editor in Chief of the ACM Journal of Experimental Algorithmics. She was co-organizer of the first DIMACS Implementation Challenge. She was also co-organizer of the first ALENEX (Algorithm Engineering and Experimentation) workshop, which is held each year together with SODA (Symposium on Discrete Algorithms), the premiere American conference on the design and analysis of algorithms.

2 Summary

This book begins by guiding the reader to the considerations that allow one to properly apply the principles of experimental design to algorithmic problems. Not only must academic experiments be reproducible and efficient but they must also be newsworthy and demonstrate knowledge that was not previously known. The preliminary first stage in an experimental study, the pilot study, along with the existing literature, complement the carefully designed workhorse study to produce novel and valid results. Experimental design should be based on problem-specific knowledge as well as common sense.

Time is the performance metric of primary interest in most algorithmic experiments. Thus, the third chapter presents different definitions of time performance and surveys tools and techniques for measuring it. The text guides the user through the criteria to consider in choosing a utility to measure time performance. For example, one needs to determine when it is preferable to measure CPU time or real time, for how long a process should run to give meaningful results, and when it is worthwhile to use compiler-based performance indicators. Quality of solutions is the other essential metric that must be considered when evaluating an approximation algorithm. The chapter concludes by describing how best to evaluate the bounds of inexact solutions along with case studies that depict the different possibilities.

Chapter 4 addresses an essential concern of experimental algorithmics: how to speed up the implementation of an algorithm. This is explored at both the level of algorithm tuning, replacing data structures with more efficient counterparts, and of code tuning, improving the low-level code in the program. The developer must focus on reducing the number of instructions and on reducing the time spent running these instructions. The designer must weigh the benefits of code tuning against the difficulty of maintaining more complicated code. Some of the techniques that the text demonstrates through case studies are branch and bound, propagation, preprocessing, pruning and memoization. Ultimately, the time space trade-off must be kept in perspective of the ultimate goals of the experiment.

In Chapter 5, the focus shifts from the application program to the test program. In experimental algorithmics, the experimenter must often design his tools. First and foremost, one should take advantage of experimental resources that are already available in his workplace and research community. Although essential parts of the program usually need to be written from scratch, instance testbeds, instance generators, and tools for program measurement and data analysis can often be procured and reused. The book describes several excellent repositories that are available on the Internet, ranging from efficient implementations of data structures to datasets and input files. The test environment must support correct, efficient and well-documented experiments. This chapter also includes a survey of techniques for constructing input sets that are demonstrably random according to a variety of distributions.

An experiment fails by being inconclusive. Chapter 6 discusses technique that exploit the laboratory setting to adjust test programs and maximize their effectiveness. The objective is that the researcher selects test data sets that are easy to analyze by reducing variance in their output. Employing variance reduction techniques when generating test data results in more successful analyses and stronger conclusions. By reducing computation time, simulation shortcuts generate larger data sets which naturally yield reduced variance in the program output.

Data alone, in their raw form, have no value or meaning. When organized and interpreted, data become useful information. The ultimate goal of data analysis is to obtain knowledge and further understanding. Chapter 7 presents techniques for data analysis that address the questions most commonly asked about algorithms. The chapter describes which scenarios these techniques are suitable for. The text focuses on one and two dimensional relationships among data. Location and dispersion of data are inseparable from one another. It is crucial to verify that data are normally distributed before applying the rules of the normal distribution. Applying logarithmic or power transformations can impose symmetry in a skewed data sample. One should consider symmetry, outliers, skew, kurtosis, and data censoring when deciding how to summarize a data sample. Different graphs give different views of relationships in data. The experimenter is encouraged to try many alternative views of the same data to learn the full story. Similarly, the trend in residuals should guide the search for a better model for specific data.

3 Opinion

This book aptly begins by saying, “This book is written for anyone - student, researcher, or practitioner - who wants to carry out computational experiments on algorithms.” This book is very well-written and accessible to anyone who has some background in the design of algorithms and in writing computer programs. This text achieves its primary goal of introducing the reader to the developing field of experimental algorithmics. Each chapter concludes with a set of problems for the reader to think about. This enables a newcomer to the field of experimental algorithmics to concretize the ideas developed in this text. The companion website, AlgLab (www.cs.amherst.edu/alglab), contains downloadable tools for use in experimental projects. Furthermore, the website guides the reader to supplementary material so that he can explore the emerging field of experimental algorithmics at greater depth. This resource serves to make the book’s content even more accessible, particularly to a novice in the field. The experimental study of combinatorial algorithms is a rapidly growing research area. This book successfully highlights the role of applied algorithms research both in the design and in the evaluation of algorithms and data structures.

Review of[6]
Fundamentals of Parameterized Complexity
by Rodney G. Downey and Michael R. Fellows
Springer, 2013
763 pages, 35 Chapters, Hardcover, $77.00

Review by Rajesh Chitnis `rajeshchitnis@gmail.com`

1 Introduction

Most interesting optimization problems on graphs are NP-hard, which means that (unless P=NP) there is no polynomial time algorithm that solves all the instances of such a problem exactly. However as noted by Garey and Johnson [3], hardness results such as NP-hardness should merely *constitute the beginning* of research. The traditional way to combat the intractability is to design approximation algorithms or randomized algorithms which run in polynomial time. These methods have their own shortcomings: we either get an approximate solution or lose the guarantee that the output is always correct. All problems in NP have trivial *exponential time* algorithms which just search and verify all the witnesses. Any algorithm which beats the brute-force algorithm can be thought of as making a *clever search* in the big space of all candidate solutions.

expressing it as a function of only the input size n, one

Parameterized Complexity is essentially a two-dimensional analogue of P vs NP. Unlike classical complexity, we define a parameter which is a non-negative integer often denoted by k and perform a refined multivariate analysis of the running time by expressing it as a function of both the input size n and the parameter k, instead of expressing it as solely as a function of n. The goal is to design algorithms that work efficiently if the parameters of the input instance are small, even if the size of the input is large. More precisely, a NP-hard problem is said to be fixed-parameter tractable (FPT) with respect to parameter k if the problem can be solved in time $f(k) \cdot n^{O(1)}$ where f is a computable function and n is the input size. A straightforward generalization is to define more than one parameter.

Parameterized complexity allows us to completely determine the effect of a parameter on the complexity of a certain problem. In particular, if one can design an FPT algorithm for a problem with respect to a parameter k then this means that instances of the problem where k is small are easier to handle than others. This theory of multivariate analysis has found applications to problems in varied areas such as social networks, streaming algorithms, game theory, coding theory, machine learning, etc. Since the first book on this area by Downey and Fellows [1] there have been two other books viz. by Flum and Grohe [2] and by Niedermeier [4] which appeared in 2006. Since then there was no book to cover the new developments in the field of parameterized complexity and this book fulfills exactly this void.

2 Summary

Part I gives a brief introduction to classical and parameterized complexity. Chapter 1 reviews some basic notions from classical complexity. Chapter 2 defines fixed-parameter tractability (FPT) along with the three variations of strongly uniform, uniform and non-uniform fixed-parameter tractability.

[6] ©2015, Rajesh Chitnis

Part II surveys some basic techniques to design FPT algorithms. Chapter 3 introduces bounded depth search trees, which is probably the most intuitive technique used in FPT algorithms. This chapter starts with the simple example of Vertex Cover before proceeding onto more complicated problems such as Feedback Vertex Set. Chapter 4 introduces the concept of polynomial time preprocessing which is formalized by the framework of kernelization. Since the publication of the book by Downey and Fellows in 1999, kernelization has become a fast growing research area in its own right. A few basic tools for obtaining kernels are introduced in Chapter 4, while more advanced concepts like Turing kernelization appear in Chapter 5. Chapter 6 introduces two important techniques: iterative compression and measure-and-conquer. Iterative compression was discovered by Reed, Smith and Vetta in 2002 to show that the Odd Cycle Transversal problem is FPT, and has been used since then as a very useful important step in showing the fixed-parameter tractability of several fundamental problems such as Directed Feedback Vertex Set, Undirected Multicut, etc. Measure-and-conquer is a very effective method to speed up branching algorithms by considering non-standard "measures". Chapter 7 describes the technique of greedy localization (branching along with a nondeterministic guess at each step) and also some methods based on mathematical induction. It also describes the famous result of Lenstra and Kannan that Integer Programming is FPT parameterized by the number of variables. Chapter 8 describes what is probably the most famous randomized technique for designing FPT algorithms: the technique of color coding introduced by Alon, Yuster and Zwick. Informally, this technique consists of random coloring followed by dynamic programming. The chapter ends with two advanced topics: the first is the approach of Koutis speeding up the dynamic programming by instead using algebraic techniques, and the second is the technique of randomized divide-and-color (also known as chromatic coding) due to Alon, Lokshtanov and Saurabh. Chapter 9 provides the first connection between parameterized complexity and classical complexity by relating FPT with known complexity classes like MAX SNP.

Part III deals with exploiting the structure or "width" of graphs to design algorithms. Chapter 10 defines treewidth, and shows how it is useful via dynamic programming on graphs of bounded treewidth. The algorithms for finding treewidth described in Chapter 10 are unpractical, and Chapter 11 gives some heuristics which can be used in practice to find "approximate" tree-decompositions. Chapter 12 deals with automata and treewidth: most of the material is standard except for Chapters 12.6 and 12.7. Chapter 13 presents the hammer that is Courcelle's theorem: informally, any property of graphs that can be described by a formula in monadic second order logic is FPT parameterized by the combined parameter (treewidth of the graph)+(size of the formula). Chapter 14 discusses local treewidth, and also applications of width metrics to structures beyond graphs! Chapter 15 shows how a simple idea like depth first search (DFS) can be used to prove deep results like the Plehn-Voigt Theorem: If the treewidth of H is t, then we can check if H is a subgraph of G in time $f(|H|) \cdot |G|^t$. Finally, Chapter 16 introduces width measures different from treewidth such as cliquewidth, branchwidth, rankwidth, etc. and how one can do dynamic programming over these decompositions.

Part IV consists of the so-called "exotic" meta-techniques: these are very general frameworks which are very involved, but help to resolve the fixed-parameter tractability of a large class of problems. In preparation for the Graph Minor theorem (in Chapter 18), Chapter 17 introduces the basics of well-quasi orderings,its connections with automata and graphs of bounded treewidth. This chapter also contains the proof of Kruskal's theorem: trees are well-quasi ordered under the relation of taking a minor. This was the first major step towards proving the Graph Minor theorem. Chapter 18 gives a very high-level overview of the proof of Graph Minor theorem. First only forests are excluded as a minor, and then more general graphs are excluded. Chapter 19 shows how to invoke the Graph Minor theorem to demonstrate the fixed-parameter tractability of certain problems. Two important concepts from this chapter are protrusions and the "irrelevant vertex" technique.

Part V deals with the hardness part of parameterized complexity. Chapter 20 introduces the concept of parameterized reductions, which forms the basis of all the lower bounds derived later on. Chapter 21 defines the class W[1], and gives the parameterized analogue of Cook's theorem: the two problems of Weighted n-Satisfiability (for $n \geq 2$) and Short Turing Machine Acceptance are W[1]-complete. These two problems are the fundamental problems from which one can reduce to show the W[1]-completeness of other problems with one such example being a reduction to the Clique problem. Chapter 22 describes some other W[1]-hard problems such as Perfect Code and VC Dimension. Chapter 23 introduces the so-called W-hierarchy which is the containment relation between the different complexity classes in parameterized complexity. Using the Normalization Theorem (which can be viewed as an analogue of Cook's Theorem), the W and W* hierarchies are characterized leading to easier proofs of membership and hardness. Chapter 24 contains proofs of the Collapse theorems for monotone and antimonotone problems. Formally, it shows that Monotone W[2t+1]=W[2t] and Antimonotone W[2t+2]=W[2t+1]. Chapter 25 show how to prove membership and hardness results for the classes W[P] and W[SAT], which contain W[t] for every t. Chapter 26 deviates from measuring time to measuring space: the AW-classes are introduced, which are the parameterized analogues space complexity classes such as PSPACE etc. Chapter 27 covers one of the few unconditional results known in this area: FPT is a strict subset of XP. Chapter 28 discusses the hypothesis that the W-hierarchy is proper, in particular the hypothesis that W[1]$\neq$W[2].

Part VI discusses techniques for showing lower bounds for running time of FPT algorithms and size of kernels. Chapter 29 describes lower bounds based on hypotheses such as ETH and SETH, and also how to design subexponential algorithms using the theory of bidimensionality. Chapter 30 shows how to prove lower bounds on kernels using techniques like the OR-compositions and also gives a sketch of the recent proof of the AND-conjecture due to Drucker.

Part VII discusses two slightly offbeat topics: parameterized approximation and parameterized counting. Chapter 31 considers the combination of the two seemingly unrelated areas of parameterized complexity and approximation algorithms. After giving the FPT approximation results for pathwidth and treewidth, almost all of the known positive and negative results in this relatively new area are mentioned. Chapter 32 introduces the counting analogs of the classes in the W-hierarchy. Randomized parameterized reductions and their consequences are also considered.

Part VIII offers four lists of open problems, each with its own special significance to the field of parameterized complexity. Some basic prerequisites are described in Part IX (Appendices) to bring all readers onto the same page.

3 Opinion

This book supersedes the original book by Downey and Fellows [1], and gives a complete overview of all the (recent) progress in the field since then. It can be read by graduate students who have some background in computational complexity. Parts I and II give a reasonably complete picture of the development in algorithmic techniques in the parameterized world since the first book was published by Downey and Fellows in 1999. This material coupled with some other chapters (picked as per personal choice, say Chapters 10,21-22,31) can be taught as a graduate level course.

I strongly recommend *Fundamentals of Parameterized Complexity* for all researchers in theoretical computer science. For researchers who are already working in parameterized complexity, you will still find many things that you should know but probably did not - for example, I was not at all familiar with material from Chapters 9, 14-16,26,32. For researchers who are not working in parameterized complexity, this book can serve as a good introduction to the field. Parts I-IV will heavily strengthen the toolkit of researchers working in algorithms, while Chapters V-VI would be of interest to researchers working on lower bounds. It is my belief that this book is now the definitive text on parameterized complexity, both for the breadth and depth of material covered and also for including the latest developments in the field (as recently as 2012).

4 Known Corrections

The authors keep a list of corrections here:

`http://homepages.ecs.vuw.ac.nz/~downey/errors.pdf`

References

[1] R. G. Downey and M. R. Fellows. *Parameterized Complexity*. Springer-Verlag, 1999. 530 pp.

[2] J. Flum and M. Grohe. *Parameterized Complexity Theory*. Springer-Verlag, 2006. 493 pp.

[3] M. R. Garey and D. S. Johnson. *Computers and Intractability: A Guide to the Theory of NP-completeness*. W. H. Freeman and Co., San Francisco, Calif., 1979.

[4] R. Niedermeier. *Invitation to Fixed-Parameter Algorithms*. Oxford University Press, 2006. 312 pp.

Review of[7]
The King of Infinite Space: Euclid and his Elements
by David Berlinski
Basic Books, 2013
172 pages, Hardcover-$18.00, Paperback-$11.00, Kindle-$10.00

Review by Eowyn Cenek eowyn.cenek@eagles.usm.edu

1 Summary

Very little is known of Euclid, beyond his writing, and especially his *Elements*, and hence any traditional biography of Euclid must be short. Hence David Berlinski focuses on Euclid's Elements, and proposes insight into the mind and thoughts of Euclid. In the process, he discusses the way in which the Euclidean model – axiom, proposition, and most importantly proof – has endured for over two millennia. In the discussion he brings forth connections between Euclid and more modern mathematicians, ranging from Newton and Descartes to Hardy, Hilbert and Poincare.

To appreciate this book, it is perhaps best to picture one sitting in a french cafe, a glass of wine at hand, as one listens to the discourse of a learned man. Sometimes on point, sometimes more discursive, the story ranges over the full span of history, touching on both the early days of Plato and Euclid and the modern days of twentieth century mathematics.

The book is written for mathematicians rather than computer scientists; some things the mathematician Berlinski finds hard to imagine – the moving of abstract angles – the computer scientist finds all too simple. still, the book is a short, eloquent call to the study of Euclid's Elements as a geometry textbook still worthy of note today.

2 Opinion

Personally, I enjoyed the book as a pleasant companion to pick up during odd moments. It is not a traditional math book, nor does it rely on heavy mental lifting from the reader. Instead, the reader is invited to enjoy the eloquence and follow along in the stream, but the few proofs included are fully explained. Of most benefit was the ability to follow a mathematician's train of thought as he in turns attempt to persuade us of the value of both the old book itself and the style of mathematics, in which definitions are carefully defined, axioms are stated clearly, and propositions are proven using logic, which the book embodies.

This is not a book that will explain the proofs in Euclid's Elements, but it may entice the reader into digging up a copy and working through the propositions as a useful practice of logic.

[7] ©2015, Eowyn Cenek