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, we review 5 books. The first 4 titles are all drawn from AMS's Student Mathematical Library. This series is directed at undergraduates and high school students, but nevertheless covers much material that will be of interest both to educators and to graduate students and seasoned researchers.

1. **Primality Testing for Beginners**, by Lasse Rempe-Gillen and Rebecca Waldecker. An exposition of the AKS algorithm for primality testing, including the necessary background, starting from scratch. Reviewed by Frederic Green.

2. **The Joy of Factoring**, by Samuel Wagstaff. A book about factoring algorithms, together with much of the requisite number theoretic background. Reviewed by William Gasarch.

3. **Asymptopia**, by Joel Spencer and Laura Florescu. Asymptotics as applied to various areas of mathematics, with some of the applications to algorithms. Reviewed by William Gasarch.

4. **Ramsey Theory over the Integers (Second Edition)**, by Bruce M. Landman and Aaron Robertson. An introduction to Ramsey Theory, focusing on van der Waerden's Theorem and addressed to undergraduate math majors. Reviewed by William Gasarch.

5. **Distributed Computing Through Combinatorial Topology**, by Maurice Herlihy and Dmitry Kozlov and Sergio Rajsbaum. An intriguing study of the application of a powerful branch of mathematics to distributed computing, covering the required topological background and thus addressed to a diverse audience, ranging from undergraduates to researchers. Reviewed by Jalaj Upadhyay.

[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. *Digital Logic Design: A Rigorous Approach* by Even and Medina.
3. *Communication Networks: An Optimization, Control, and Stochastic Networks Perspective* by Srikant and Ying.
4. *CoCo: The colorful history of Tandy's Underdog Computer* by Boisy Pitre and Bill Loguidice.
5. *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. *An Episodic History of Mathematics: Mathematical Culture Through Problem Solving* by Krantz.
3. *Proof Analysis: A Contribution to Hilbert's Last Problem* by Negri and Von Plato.

Review of[2]
Primality Testing for Beginners
by Lasse Rempe-Gillen and Rebecca Waldecker
American Mathematical Society, 2014
244 pages, Softcover, $45.00 (AMS)

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

1 Background

The seminal polynomial-time algorithm for testing if a number is prime, developed in 2002 by Agrawal, Kayal and Saxena [AKS], came (one might argue) after only a few millennia of mathematical research. Ironically, in light of this long history, the AKS algorithm turned out to be nowhere near as complicated as most people expected. The mathematical prerequisites are modest, and do not go any further than quite basic college-level abstract algebra. And indeed, it was aptly characterized by F. Bornemann[3] in a 2003 Notices of the AMS exposition as a breakthrough for “Everyman.”

But who exactly is “Everyman”? Mathematicians who are not experts in number theory? Non-complexity theorists? Undergraduate math majors? Okay, how about high-school students? In “Primality Testing for Beginners,” Lasse Rempe-Gillen and Rebecca Waldecker don’t literally ask these questions, but they answer them in their introduction:

> The objective of this book is to give a complete presentation of the proof of the theorem of Agrawal, Kayal and Saxena, without requiring any prior knowledge beyond general computational skills and the ability to think logically.
>
> . . .
>
> The book is aimed at interested high school pupils and teachers, but also at undergraduate students in mathematics and computer science (to whom it should be accessible in the first year).

This is an ambitious goal! Think of all the things you’d have to do, that might not be (and, regrettably, often are not) covered in all high school educations: Axioms, definitions, theorems and lemmas, proofs (by contradiction, induction, etc.), elementary number theory (like prime factorization), polynomials, algorithms, analysis of algorithms, and on and on it goes. No matter how you slice it, that’s a lot to cover in the under 200 pages that the main text occupies.

Yet these authors do it, and succeed amazingly well. The question is, how? Let’s look at an example, starting at the very beginning. Not much is more intuitive than the counting numbers (here defined as the positive integers). The first basic and salient fact about the natural numbers is the well-ordering principle. This immediately suggests the method of descent. A perfect illustration of that method is to use it to prove the rationality of $\sqrt{2}$. So we go from counting to mathematical proof (really both induction and contradiction rolled into one) almost effortlessly. All this is dispatched with perfect elegance in the space of two pages, with strong intuition and no unnecessary formalism, yet with just the right amount of rigor. *That’s* how to

[3] [Bo]; see also [G] for more detail and, for even more, [Dtz], reviewed on these pages in 2006 (SIGACT News Vol. 37, No 1).

do it, and the only trick is to sustain that for the more advanced and subtle topics that occupy the remaining 180 or so pages of the main text.

But before saying more about the “how,” let’s look at the “what.”

2 Summary of Contents

The book is divided into two parts, “Foundations” and “The AKS Algorithm.” Part 1 consists of Chapters 1 through 4, and Part 2 is the rest.

- Chapter 1, Natural numbers and primes: Covers the most basic material, including natural numbers, proof by induction and contradiction, the binomial theorem, divisibility, prime factorization, the Euclidean algorithm and the Sieve of Eratosthenes.

- Chapter 2, Algorithms and complexity: Presents algorithms from an intuitive point of view, beginning with simple problems such as addition of binary numbers, simple algorithm analysis, the idea of computability, the halting problem, efficient computation, the classes P and NP, and probabilistic computation, both Monte Carlo (RP) and Las Vegas (ZPP). The latter are illustrated by randomized algorithms for polynomial non-identity testing and quicksort, respectively.

- Chapter 3, Foundations of number theory: This chapter provides the most crucial technical background for the algorithm. It includes modular arithmetic, Fermat’s Little Theorem, the Euler Function and the Fermat-Euler Theorem (not needed for AKS; likewise the Chinese remainder theorem, also proved in this chapter), the Fermat primality test, polynomials and modular arithmetic with polynomials.

- Chapter 4, Prime numbers and crypography: History of crypography, RSA, and the distribution of primes. Just enough of what is needed of the prime number theorem is stated and given an elementary proof. The chapter concludes with the Miller-Rabin primality test (which does use the Chinese remaindering).

- Chapter 5, The starting point: Fermat for polynomials: Generalizing Fermat’s Little Theorem to polynomials, the polynomial criterion that is the basis of the AKS algorithm, a high-level sketch of the algorithm, and the randomized Agrawal-Biswas [AB] test (which uses the same criterion, and was an important predecessor of AKS).

- Chapter 6, The theorem of Agrawal, Kayal and Saxena: The primary agenda of this chapter is to state and prove the main theorem on which the algorithm is based. It bounds the number of polynomials $P = X + a$ such that $(P(X))^n \equiv P(X^n)$ mod $(p, X^r - 1)$, for $0 \leq a \leq p - 1$, and n not a power of p and of sufficiently large order mod r. In particular, this theorem allows us to recognize if n is a non-prime-power composite. Irreducible factors of cyclotomic polynomials are used to provide a suitable bound on the order of n mod r.

- Chapter 7, The algorithm: The stage has been set to make this one of the shortest chapters in the book. First bound from above the prime r such that its order mod n is sufficiently large. This uses the weak version of the prime number theorem proved in Chapter 4. Finally, the AKS algorithm as sketched in Chapter 5 can be given in detail, and its analysis and correctness follow easily from the foregoing developments.

It must be emphasized that all topics are covered in depth, including proofs, with just the right level of detail and abstraction. All sections include diverse exercises of varying difficulty (but all quite feasible), including many that prove results used later in the text. Solutions for the latter exercises are given in the second appendix. In addition to exercises, sections also may conclude with some comments that expand on the material, provide added context (e.g., in light of Lagrange's theorem, to take an opportunity to mention group theory, which is not used in the main text), give some insight into the history, or pointers to the literature.

In addition to the appendix of problem solutions mentioned above, the first appendix contains an entertaining discussion of (mostly famous) open questions and conjectures.

3 Opinion

"Primality Testing for Beginners" will be of interest to a great many readers. It is certainly appropriate at the high school or undergraduate level. It could easily serve in a readings course or first-year seminar, or for supplementary reading in courses on algorithms or abstract algebra (to illustrate applications!). But I would also recommend it to anyone who is interested in learning about the AKS algorithm. While researchers know most of the mathematics, it's nice to have it all (and I mean all) at your fingertips.

This book does much more than "just" explain a particular important result. It shows what mathematics is really about, through the medium of explaining that particular result. And by "mathematics" I don't just mean the subject as is taught in high school or college, but also mathematical *research*. The book is always mindful of the motivation for the results that it proves, and whenever feasible points out the false starts and blind alleys that may crop up along the way. To take but one example, regarding the primality criterion near the beginning of Chapter 5:

> At first, [the theorem] seems like an incredibly strong result: we could test a number n for primality by choosing any number a coprime to n and checking the congruence. . . Unfortunately, this is, once again, impossible in practice. Indeed, we might have to compare up to n coefficients. So the effort required would be *exponential* in log n, and thus of the same order of magnitude as searching directly for a factor of n or applying the Sieve of Eratosthenes.

Thus the "what" given in the previous section is inextricably caught up in the "how." It seems the topics were chosen with great care, with two goals in mind: First and foremost, to prepare the reader for the AKS algorithm. And secondly, to give the reader sufficient mathematical background to *appreciate* the results, not just follow all the low-level details.

Along the way, the reader is introduced to a rich set of ideas, which is surely self-evident from the summary of contents given above. One learns sizable chunks of elementary number theory, algorithms and complexity from this text. I marvel at the breadth of ideas covered in so few pages. Despite the necessary pace, a reader-friendly, cogent and uncluttered style is maintained throughout. Sound pedagogy is ensured by integrating the exercises with the text, making the reader an active participant. And it is as self-contained as any mathematics book I've ever read. (Incidentally, you'd never guess from reading it that this was a translation from a German original.)

At the same time, while eminently readable by "Everyman," it probably won't always be (nor, I believe, was it meant to be) an easy read. For many beginning students, I imagine working through this book would feel akin to a short but rigorous hike in the mountains. Already at the beginning the climb is somewhat steep, although it is probably steepest in Chapter 6, where the contour lines get closer together according to the density of theorem/proof/theorem/proof. But even at that altitude, the reader encounters lucid discussions that provide some room to breath, giving insight and perspective which attenuate the required effort. And, finally, as we emerge onto the summit in Chapter 7, the view is especially rewarding.

References

[AB] M. Agrawal and S. Biswas, Primality and identity testing via Chinese remaindering. In *Journal of the ACM* **50**(4) (2003), pages 429-443.

[AKS] M. Agrawal, N. Kayal, K. Saxena, PRIMES is in P. In *Annals of Mathematics* **160**(2) (2004), pages 781-793.

[Bo] F. Bornemann, Primes is in P: A Breakthrough for "Everyman." In *Notices of the AMS* **50**(5) (2003), pages 545-552.

[Dtz] M. Dietzfelbinger, Primality testing in polynomial time: from randomized algorithms to "PRIMES is in P." Springer, 2004.

[G] A. Granville, It is easy to determine whether a given integer is prime. In *Bull. Amer. Math. Soc.* **42**(1) (2005), pages 3-38.

Review of[4]
The Joy of Factoring
by Samuel Wagstaff
Publisher: AMS
$35.00 softcover , 293 pages, Year: 2013

Review by
William Gasarch (gasarch@cs.umd.edu)
Department of Computer Science
University of Maryland, College Park, College Park, MD

1 Introduction

This is a book on algorithms for factoring. As you might expect, there is also a lot of number theory presented. What is more surprising is that there is not much in the way of analyzing algorithms. This is *not* a criticism of the book. The field in general seems not to have that much in the way of rigorous runtimes of algorithms. This is *not* a criticism of the field.

Reading the book was odd in that there was more concern for algorithms that could *actually* be coded up (many *actually* have been), that would *actually* run fast, and less concern for rigorous runtime analysis. This is unusual for computer science algorithms. Some *might* take that as a criticism of computer science research in algorithms, but I am not going to go there.

Why is factoring an area where practical algorithms are emphasized and rigorous analysis is not? I speculate that there are two reasons: (1) people really want algorithms that factor quickly (for cryptography), and (2) the mathematics needed to prove runtimes of algorithms often involves open problems in number theory.

Notation: Throughout this review N is the number we want to factor and $b = \lfloor \sqrt{N} \rfloor$.

2 Summary of Contents

The first five chapters are a blend of number theory needed for factoring algorithms, simple factoring algorithms, and factoring algorithms for numbers of a certain type. We give some examples of each:

1. (r/p) is the Legendre symbol: it is 1 when r is a nonzero square mod p, -1 when r is not a square mod p, and 0 when r divides p. There is a section on how to compute this easily. Theorems from number theory are stated but not proven.

2. Trivial Algorithm: If N is small you certainly do not want to use a fancy algorithm on it. Hence a simple fast algorithm is needed for N small. This book discusses the so-called trivial algorithm, divide n by $2, 3, \ldots, b$, in some depth. The key is that this algorithm can be sped up considerably. The first observation is that you do not need to divide by any even larger than 2. Hence you need only divide by $2, 3, 5, 7, 9, \ldots, b$. AH! – you need not divide by any multiple of 3 larger than 3. This leads to only trying numbers that are $\equiv 1, 5 \pmod{6}$. If you avoid all multiples of 2,3, and 5 then you only try numbers that are $\equiv 1, 7, 11, 13, 17, 19, 23, 29 \pmod{30}$. The fact that they are all primes is an accident which no longer holds when you avoid numbers that are a multiple of $1, 3, 5, 7$ and use mod

[4] ©2016 William Gasarch

210. One can go further and further with this but at some point the cost of making sure your numbers are in one of the congruence classes outweighs the benefits.

3. Fermat's difference of squares algorithm: For each of b^2-N, $(b+1)^2-N$, $(b+2)^2-N, \ldots$ test if it is a square and stop if it is. If $(b+i)^2-N$ is a square then $(b+i)^2-N = y^2$ so $(b+i-y)(b+i+y) = N$. Hence a factor is found (unless $b+i-y = 1$ and $b+i+y = N$). This algorithm is analyzed rigorously and ways to speed it up are given. In the worst case it works in time $O(N^{2/3})$ but if one of the factors of N is close to $\sqrt{N}$ (which is common when trying to crack RSA) then this algorithm is very fast. Also, this technique of trying to find x, y such that $x^2 - y^2$ is N (or a multiple of N) is the starting point for many other algorithms.

4. Let p be the lowest prime factor of N. We do not know p but we do know that $p \le \sqrt{N}$. Pollard's $p-1$ method begins by noting that $2^{p-1} \equiv 1 \pmod{p}$, hence $2^{p-1} - 1 \equiv 0 \pmod{N}$. Let $p_1, \ldots, p_m$ be all primes less than a parameter B. If $p-1$ has all of its factors $\le B$ then $2^{p_1^{a_1} \cdots p_m^{a_m}} - 1 \equiv 0 \pmod{N}$ where $a_i = \lfloor \log B / \log p_i \rfloor$. Hence $GCD(2^{p_1^{a_1} \cdots p_m^{a_m}} - 1, N)$ will likely yield a factor of N.

5. Let $F_1, F_2, \ldots$ be the Fibonacci numbers. If m divides n then F_m divides F_n. Hence, if you are given n and F_n, to factor it you need only factor $n = ab$ and find F_a.

Chapter 6 presents a sequence of algorithms that use continued fractions to factor. The basic idea is to find x, y, z such that $(x + by)^2 - Ny^2 = z^2$. From this one easily gets $(x + by - z)(x + by - z) = Ny^2$ so $GCD(x + by - z, N)$ is a likely factor of N. Such an x, y, z can be found by looking at convergents of continued fractions. Getting this to actually work takes many more ideas. The algorithm was first proposed in 1970. A runtime of $e^{\sqrt{2(\ln N)(\ln\ln N)}}$ was proven by Pomerance in 1982. Note that, for all ϵ, this is $\le O(N^{\epsilon})$.

Chapter 7 uses Elliptic curve methods to factor. One of them takes Pollard's $p-1$ method and instead of using the integers mod p uses a set of elliptic curves of about the right size. This increases the chance of success.

Chapter 8 is on Sieve methods- both the Quadratic Sieve and the Number Field Sieve. The latter is the method of choice for large number factorization. Both use ideas from Fermat's difference method and the Trivial method but of course use much more sophisticated ideas as well.

Chapter 9 and 10 are a collection of chapters on practical and theoretical factoring, though mostly practical. There is also a discussion of why there have not been truly new factoring algorithms since 1995.

3 Opinion

This book has lots of information and lots of pointers to more information. The field is vast and spans both practical and theoretical concerns; hence I suspect anyone who is not an active researcher in the area will find things in this book of interest. This should certainly be read by people in cryptography to get a better sense of just how vulnerable their systems might be.

While there are chapters to teach some number theory, the reader really should already know some number theory. The book could be read by bright undergraduates. Good projects could be devised by coding up some of these algorithms.

Review of[5]
Asymptopia
by Joel Spencer and Laura Florescu
Publisher: AMS
$38.00 softcover, 189 pages, Year: 2014

Review by
William Gasarch (`gasarch@cs.umd.edu`)
Department of Computer Science
University of Maryland, College Park, College Park, MD

1 Introduction

This is a book on asymptotics for undergraduates; however, most of the material is not standard so a graduate student or even a professor will find something new here.

Asymptotics is, roughly speaking, what happens to a ... formula? phenomena? that depends on n when n is large. The audience for this review (SIGACT News readers) are used to this notion for algorithm analysis. There is one chapter on that topic; however, the book is mostly about asymptotics within mathematics.

2 Summary of Contents

The first five chapters are about asymptotics of factorials, big-O notation, asymptotics of integrals and sums, and asymptotics of binomial coefficients. One could view these results as interesting in their own right or as lemmas for later applications. While the distinction between lemma and application may be a matter of taste I will point out two topics that I consider applications: (1) approximations to $\int_0^1 sin^n x dx$, and (2) random walks.

The rest of the chapters are mostly applications. This is a math book so I mean applications to other fields of mathematics. We list some of the results:

1. The number of rooted trees on $\{1, \ldots, n\}$ with root 1 is n^{n-2} (this is not asymptotic nor is it proved in this book). By contrast the number of Unicycle graphs (a graph with n vertices and n edges) is asymptotically $\sqrt{\frac{\pi}{8}} n^{n-\frac{1}{2}}$. Note that the error term is additive, not (as is often the case in computer science) multiplicative.

2. There are three asymptotic lower bounds for $R(k)$ (Ramsey of k): (1) $R(k) \ge (1+o(1))\frac{k}{e\sqrt{2}}2^{k/2}$, (2) $R(k) \ge (1+o(1))\frac{k}{e}2^{k/2}$, (3) $R(k) \ge (1+o(1))\frac{k\sqrt{2}}{e}2^{k/2}$. These results are interesting and depressing. Interesting that progress has been made, and the proofs are nice. Depressing that so little progress has been made.

3. Let $\pi(n)$ be the number of primes that are $\le n$. The prime number theorem states that $\pi(n) \sim \frac{n}{\ln n}$. This is a difficult theorem. How close can we get to it just using simple combinatorics? In this chapter they show that there are constants c_1, c_2 such that
$$(c_1 + o(1))\frac{n}{\ln n} \le \pi(n) \le (c_2 + o(1))\frac{n}{\ln n}.$$

[5] ©2016 William Gasarch

Upon seeing this my first reaction is *I bet c_1 is really small and c_2 is really large*. NO. In the proofs given $c_1 = \ln 2 \sim 0.693$ and $c_2 = 2\ln 2 \sim 1.386$. This approximation to the prime number theorem is good enough for any application in computer science.

4. If you pick three points in the unit square what is the probability that the triangle will be of size $\le \epsilon$? This will be a function of ϵ. They show that it's $\Theta(\epsilon)$.

5. There is a chapter on algorithms. This material will be familiar to most readers of this review.

6. There are two chapters on probability and there is some probability in other places. Here is one phenomenon they look at from different angles: let $X_1, X_2, \ldots$ be random variables that take on the value -1 or 1, each with probability $1/2$. Let $S_n = X_1 + \cdots + X_n$. Clearly $E(S_n) = 0$ but what is the probability that S_n will be far from 0?

3 Opinion

If n people read this review then, with high probability, $n - \ln n$ of them will find at least $\frac{2}{3} - \frac{1}{\sqrt{n}}$ of the book interesting. The proofs are readable and the results are worth knowing. One caution – some of you are used to ignoring multiplicative factors. This book is more careful about those constants so you need to get used to it. However, that is one of the benefits— it teaches you to think in a different way.

To read this book you need mathematical maturity and a basic course in combinatorics. All such people will benefit from this book since it has many results that are not that well known but perhaps should be. The triangle results above I found particularly intriguing.

Review of[6]
Ramsey Theory over the Integers (Second Edition)
by Bruce M. Landman and Aaron Robertson
Publisher: AMS
Student Mathematical Library Series Volume 73
$58.00 softcover, 380 pages, Year: 2014

Review by
William Gasarch (gasarch@cs.umd.edu)
Department of Computer Science
University of Maryland, College Park, College Park, MD

1 Introduction

Three classic theorems of Ramsey Theory are:

1. *Ramsey's Theorem:* For all r, m there exists n such that for all r-colorings of the edges of K_n there is a monochromatic clique K_m (m vertices such that all of the edges between them are colored the same). This extends to many colors and hypergraphs.

2. *Van der Warden's Theorem (henceforth VDW's Theorem:* For all r, k there exists w such that for all r-colorings of $[w] = \{1, \ldots, w\}$ there is a monochromatic arithmetic sequence of length k (henceforth a k-AP). The Gallai-Witt theorem is a generalization to more dimensions. The Hales-Jewitt theorem is a further generalization.

3. *Schur's Theorem* For all r there exists n such that for all r-colorings of $[n]$ there exists x, y, z the same colors such that $x + y = z$.

Most books on Ramsey Theory focus on both Ramsey's Theorem, VDW's Theorem, and variants of them (Schur's Theorem when generalized can be seen as a variant of VDW's Theorem). This book focuses *just* on VDW's Theorem and variants of it that *only* involve colorings of initial segments of N. There are many problems and ideas for research problems in this book that could be tackled by an undergraduate. The authors state accessibility for undergraduates and ideas for projects as explicit goals.

2 Summary of Contents

The first chapters introduce Ramsey Theory and give statements of the classic theorems above. The second chapter states and proves VDW's Theorem, and gives upper and lower bounds on some VDW numbers. The proof is complete and rigorous. This is welcome and not common. The proof of VDW's Theorem is such that it's easier to go part way and leave the rest as an exercise since it's messy to write down. By using the color-focusing method to present the theorem they obtain a complete rigorous proof. One downside: they do not present the proof of VDW's Theorem for 2 colors and 3-AP's, that uses 2-colorings of blocks-of-5 integers, which is nice to see for intuition. This proof (any version of it, any presentation of it) yields rather large upper bounds for $W(r, k)$ (not primitive recursive). Shelah had an elementary proof that yielded smaller

[6] ©2016 William Gasarch

numbers (primitive recursive) though still quite large. Gowers had a proof using advanced mathematics that yielded a bound that was *only* a finite stack of exponentials. Neither of these proofs are given. Note that the search for matching upper and lower bounds, and for an elementary proof of more reasonable upper bounds, is ongoing.

Chapters 3, 4, 5, and 6 have variants of VDW's Theorem by replacing *AP* by other types of sets of numbers:
In Chapter 3:

1. A *k-term quasi progression of diameter n* is a set of the form $\{x_1 < \cdots < x_k\}$ such that there exists d, for all i, $d \le x_{i+1} - x_i \le n + d$. This can be generalized by letting d be a function of i.

2. Let $k \ge 3$. A *k-term descending wave* is a set of the form $\{x_1 < \cdots < x_k\}$ such that, for all i, $x_i - x_{i-1} \le x_{i+1} - x_i$.

3. A *k-term semi-progression of scope m* is a set of the form $\{x_1 < \cdots < x_k\}$ such that, for all i, $x_i - x_{i-1} \in \{d, 2d, 3d, \ldots, md\}$.

4. A *k-term p_n-sequence* is a set of the form $\{x_1, \ldots, x_k\}$ such that there exists a polynomial $p(x) \in \mathsf{Z}[x]$ of degree n such that for all i, $x_{i+1} = p(x_i)$.

By VDW's Theorem, for all r, k, there is a w such that there is a k-term set of any of the above types (for the p_n sequence you would take $n = 1$). However, this would yield rather large upper bounds. In Chapter 3 they study all of the above types of sequences and get much more reasonable upper and lower bounds than are known for VDW numbers. We give one example.

Let $DW(k)$ be the least w such that for all 2-colorings of $[w]$ there is a k-term descending wave. They prove $k^2 - k + 1 \le DW(k) \le \frac{k^3}{2} - \frac{k^2}{2} + 1$. They state without proof that more is known: there is a c such that $ck^2 \le DW(k) \le \frac{k^3}{3} - \frac{4k}{3} + 3$.
Chapter 4 deals with restricting the differences of the AP:

1. A set D is *r-large* if, for all k there exists w such that for all r-colorings of $[w]$ there is a mono set with difference in D. They consider this for both finite and infinite D.

2. A special case of interest: $w'(c, k; r)$ is the least w such that for all r-colorings of $[w]$ there is a mono k-AP with difference $\ge c$. Such a w always exists by VDW's Theorem, but can we get a different proof with a better bound?

3. Let f be an increasing function from N to N. Then $w(f(x), k; r)$ is the least w such that there is a mono set $\{x_1 < x_2 < \cdots < x_k\}$ such that, for all, i $x_{i+1} - x_i = f(i)$.

A set D need not be r-large for any r. There are functions f such that $w(f(x), k; r)$ does not exist. Chapter 4 has theorems about both when these things do and do not happen. We give two examples. (1) If D is finite then D is not 2-large. (2) The Fibonacci numbers are not 4-large. (3) If $p(x) \in \mathsf{Z}[x]$ and $p(0) = 0$ then the image of p is large (this is stated but not proven).

Chapter 5 has 15 pages on sequences of the form $\{x, ax + d, bx + 2d\}$. They then look at homothetic copies of sequences. Chapter 6 deals with the differences not being equal but being congruent mod m for some m. Chapter 7 offers yet more variants on the notion of an AP.

Chapters 8 and 9 are on a different kind of variant than those of Chapters 3 through 7. Recall VDW's Theorem for $r = 2$ and $k = 4$:

There exists w such that for all 2-colorings COL of $[w]$ there exists a, d such that

$$COL(a) = COL(a+d) = COL(a+2d) = COL(a+3d).$$

We rewrite this in terms of equations.

There exists w such that for all 2-colorings COL of $[w]$ there exist distinct e_1, e_2, e_3, e_4 such that

$$COL(e_1) = COL(e_2) = COL(e_3) = COL(e_4)$$

and

$$\begin{array}{rcl} e_2 - e_1 & = & e_3 - e_2 \\ e_2 - e_1 & = & e_4 - e_3. \end{array}$$

We rewrite these equations:

$$\begin{array}{rcl} e_1 - 2e_2 + e_3 + 0e_4 & = & 0 \\ e_1 - e_2 - e_3 + e_4 & = & 0. \end{array}$$

Hence VDW's theorem for $r = 2$ and $k = 4$ can be rewritten as:

There exits w such that for all 2-colorings COL of $[w]$ there exist distinct e_1, e_2, e_3, e_4 such that

$$COL(e_1) = COL(e_2) = COL(e_3) = COL(e_4),$$

$$A\vec{e} = \vec{0},$$

where A is

$$\begin{pmatrix} 1 & -2 & 1 & 0 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

and $\vec{e} = (e_1, e_2, e_3, e_4)$.

What other matrices have this property? Schur's Theorem, which was proven before VDW's Theorem, answers this question for the single equation $x + y - z = 0$. Chapter 8 looks at variants of Schur's Theorem including counting how many monochromatic solutions there are, and generalizing to equations in more than one variable. The full generalization: Let $(a_1, \ldots, a_n)$ be a tuple of integers. Let $L(x_1, \ldots, x_n) = \sum_{i=1}^{n} a_i x_k$. Then the following are equivalent

- For all r, k there exists w such that for all r-colorings of $[w]$ there exists a monochromatic solution of $L(\vec{x}) = 0$.
- Some subset of $\{a_1, \ldots, a_n\}$ sums to 0.

Rado's theorem gives a condition C on matrices A (which we omit here but is in the book) such that the following are equivalent.

- For all r, k there exists w such that for all r-colorings of $[w]$ there exists a monochromatic solution of $A(\vec{x}) = 0$.
- A satisfies condition C.

Chapter 9 has Rado's Theorem and many variants. Chapter 10 has still more variants on VDW-type theorems.

3 Opinion

This book is excellent for what it set out to do: There are many variants of VDW's Theorem and they can form the basis of many student projects. This is not just my speculation; the first edition of this book *did* inspire many projects and many of the open problems from it have been solved. The book is well written.

From the review one might think "*Gee, there are A LOT of variants. Are they all interesting?*" This is a matter of taste. But one cautionary note is not to get overwhelmed by them: Pick A FEW that you find interesting and read about those. You may read others later but don't (as I did) read the book in a week.

The Gallai-Witt Theorem is omitted, which makes sense since this is about Ramsey Theory over *the integers*. However, just the theorem *for all 2-colorings of the lattice points in the plane there is a mono square* is on the level of undergraduates, and would have been nice. They omit the Hales-Jewitt Theorem which is a very wise decision since it is somewhat abstract and seems to be just the right cut-off point.

They do not have the polynomial VDW Theorem though they do state a corollary of it (if $p(x) \in \mathsf{Z}[x]$ and $p(0) = 0$ then the image of p is large). Here I will (1) state the full Poly VDW, (2) say why I think it should have been included, and (3) say why I might be wrong.

Polynomial VDW Theorem: For all r, for all $p_1, \ldots, p_k \in \mathsf{Z}[x]$ such that $(\forall i)[p_i(0) = 0]$, there exists W such that, for all r-colorings of $[W]$ there exists a, d such that

$$a, a + p_1(d), a + p_2(d), \ldots, a + p_k(d)$$

are all the same color.

This theorem has an elementary proof, due to Walters, that the authors know about (Walters' paper is in the bibliography). The proof uses the color-focusing method which is the same method used in the book's proof of the VDW Theorem. This theorem clearly fits into the theme of VDW on the integers. Undergraduate projects can be made out of it (I speak from experience). There is a very nice contrast between the proof of VDW's Theorem, which is an ω^2-induction, and the proof of Poly VDW, which is an ω^ω-induction.

So why might I be wrong? First off, the book is already 380 pages. By contrast, *Joy of Factoring* and *Asymptopia*, which are in the same series, are 293 and 189 pages respectively. Second, and I admit this freely, my view may be prejudiced since the elementary proof of Poly VDW is what got me into Ramsey Theory in the first place. Having said that, if the writers ever do a third edition, they should at least consider the idea.

Review of[7]
Distributed Computing Through Combinatorial Topology
by Maurice Herlihy and Dmitry Kozlov and Sergio Rajsbaum
Morgan Kauffmann/Elsevier
319 pages, Paperback $75.59 (Amazon)

Review by
Jalaj Upadhyay (jalaj@psu.edu)
Computer Science and Engineering Department
Pennsylvania State University, State College, PA

1 Introduction

The book “Distributed Computing Through Combinatorial Topology” covers the recent advances in the applications of combinatorial topology to prove various theoretical results in distributed computing. All the results presented in the book have been published in various journals and conferences in the past two decades. Each chapter in this book has a result (either impossibility result or an explicit protocol) of a specific class of tasks in a particular model of computation.

Intended Audience. This book can be either used as a textbook for a senior-level undergraduate course or a graduate course, or as a reference book for researchers interested in the area of theoretical distributed computing. The book is divided into four parts. Part I covers the fundamentals required to understand the rest of the book. Part II covers the basic results in theoretical distributed computing using combinatorial topology and its material is intended for a senior-level undergraduate course. Part III is intended to be the material for a graduate level course and covers more general results. Part IV is intended for researchers interested in this area.

Pre-requisite. The book assumes familiarity with basic discrete mathematics such as *graph theory* and *set theory*. Chapter 15 further requires a background on abstract algebra, more specifically, *finitely generated groups*, *group homomorphisms*, and *representation of finite groups*. No prior knowledge of (algebraic or combinatorial) topology is required to read this book.

2 Summary of the Contents

The book starts with a Preface by the authors that provides a brief introduction of the book. The book is then divided into four parts. The detailed overview of each of these parts is presented below.

2.1 Part I: Fundamentals

Part I of the book has four chapters and focuses on the fundamentals of combinatorial topology and distributed computing.

Chapter 1 informally discusses some of the basic models of distributed computing and gives an introduction to combinatorial topology. It also includes two classical problems in distributed computing to illustrate the connection between distributed computing and combinatorial topology at a high level. **Chapter 2**

focuses on two-process systems to give a concrete example of how techniques and concepts of combinatorial topology are used to model distributed computing. The chapter starts by formally introducing topological objects, like *simplices, simplicial complex, simplicial maps*, and *carrier maps*, and introduces models of computation in distributed computing, like the *alternating-passing model, layered read-write model*, and *layered message-passing model*. Finally, it shows how combinatorial topology is used to model computations in two-processes systems. **Chapter 3** forms the basis of the topological material covered in the entire book. Various topological structures such as *star, link*, and *join*, and various concepts such as *connectivity* and different kind of *subdivisions* are introduced. The chapter also contains the composition theorem for various types of mapping between two simplicial complexes.

2.2 Part II: Colorless Tasks

Part II of the book consists of four chapters and covers a large class of coordination problems studied in distributed computing, called *colorless tasks*, under various fault-tolerant requirements. In a colorless task, we only care about the input and output values, and not which processes are associated with which values. Although colorless tasks seem very restrictive, many tasks such as *consensus* and *set agreement* are colorless tasks.

Chapter 4 considers the simplest model of computation called *immediate snapshot* in the *shared-memory model*. Section 4.2 starts by describing how combinatorial topology can be used to model concurrent composition of protocols and is followed by defining simplicial complexes corresponding to various models of computation. **Chapter 5** introduces a stronger model called the *message-passing model*, and various adversarial models such as *wait-free adversary* and *t-faulty adversary*. The main theorem, stated as Theorem 5.5.3, characterizes when colorless tasks are computable given that a threshold number of processes may crash in the message-passing model. **Chapter 6** considers a more powerful adversarial model known as the *Byzantine model*. In the Byzantine model of computation, a faulty process can display arbitrary and malicious behaviour. Theorem 6.6.1 in this chapter provides the characterization result for computation under the Byzantine model. This part of the book ends with **Chapter 7** on the reduction techniques by giving a combinatorial framework that defines how the topology of two models should be related so that we can reduce the computation in one model to the computation in another model.

2.3 Part III: General Tasks

Part III of the book consists of four chapters and includes results for general tasks. Part III introduces topological concepts such as *manifolds, Sperner's Lemma, connectivity*, and the *nerve graph*.

Chapter 8 explores how topological objects can be used to study general tasks. General tasks and protocols are defined in Sections 8.1 and 8.2, respectively, followed by examples in Sections 8.3 and 8.4 to further illustrate the subtle differences between the framework of colorless tasks and general tasks. **Chapter 9** introduces a class of protocols called *manifold protocols* and explores a task called k-set agreement. A k-set agreement requires a distributed system to agree on at most k values. Theorem 9.3.6 in this chapter states that any manifold protocol cannot solve k-set agreement. **Chapter 10** studies k-set agreement for highly connected protocol complexes. Theorem 10.3.1 gives an impossibility result that any $k-1$ connected protocol complex cannot solve k-set agreement. This result extends the main result from Chapter 9 in the sense that there are many $k-1$ connected protocol complexes which are not manifolds. The main result in **Chapter 11** is the characterization of general tasks in the wait-free model of computation. The result is stated as Theorem 11.2.1 and the proof uses the techniques developed in the last three chapters and notions from point-set topology, such as *open covers* and *compactness*.

2.4 Part IV: Advanced Topics

Part IV of the book covers more advance concepts and results of combinatorial topology such as *shellability*, the *Nerve Lemma*, *fundamental groups*, *torsion classes*, and *Schegel diagrams*. The content of this part requires an understanding of basic concepts introduced in Chapter 8. The chapters in this part are more or less self-contained; therefore, they can be read in any order.

Chapter 12 covers the *renaming task,* in which each of the processes are given distinct names from a large domain space. The task requires the processes to choose a distinct output name from a much smaller range space. The focus of this chapter is on *adaptive* processes, where the size of the range space depends on the number of processes. Section 12.1 includes an existential proof of the upper bound on the range space and also gives an explicit protocol that matches this bound. **Chapter 13** shows an inductive way to use layering in a protocol to compute the connectivity of the protocol complexes. The chapter uses a powerful topological concept called *shellability* to show that if every single-layered complex is shellable, then connectivity is preserved under multilayer composition. The result is stated as Theorem 13.4.6. The rest of the chapter explores the application of this theorem by characterizing when a single-layer complex is shellable under different models of computation. **Chapter 14** studies simulation and reduction of general tasks under different communication models. The main theorem shows the equivalence between various communication models of shared-memory models. The main theorem of **Chapter 15**, stated and proved in Section 15.3, exhibits a connection between the *Loop Agreement Task* and the *Word Problem* for finitely-presented groups. The techniques used in this chapter are mostly algebraic in nature and the concept of *fundamental groups* is introduced. **Chapter 16** proves the result that the *standard chromatic subdivision* of a simplex is indeed a subdivision. This chapter has a flavour of discrete geometry and the results are also proven in the book on Combinatorial Topology by Kozlov [1].

3 Opinion

The book is very well-written. All the figures, examples, and illustrations serve nicely to explain various concepts. For example, Chapter 1 allows the readers, who are unfamiliar with either combinatorial topology or distributed computing, to better understand the connections explored in this book. The exercises at the ends of chapters are well thought out. I would suggest that readers take some time to solve the exercises. Personally, I would have liked the authors to mark some of slightly involved exercises. I really liked the mathematical notes in between the chapters, and I feel they would be very helpful to readers who are unfamiliar with the concepts in algebraic topology, to get a better understanding of the concepts.

The book is self-contained and I believe that mathematicians and computer scientists both would equally benefit from this book. All the results in this book are published results, and previously had different notations and terminologies. The authors have done a great job in collecting and presenting the interesting results in a consistent manner. I believe a new researcher in this area would find this book very helpful.

The book is well-organized. The mathematical sophistication increases gradually from Part II to Part IV. The authors have made sure that the relevant mathematical concepts are presented at the appropriate sections in the sense that Part I only covers the basic concepts of combinatorial topology and more advanced concepts are introduced and discussed only in the chapters where they are used.

References

[1] Dmitriĭ Nikolaevich Kozlov. *Combinatorial Algebraic Topology*, volume 21. Springer, 2008.