The Book Review Column[1]

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

In the last issue of SIGACT NEWS (Volume 45, No. 3) there was a review of Martin Davis's book **The Universal Computer. The road from Leibniz to Turing** that was badly typeset. This was my fault. We reprint the review, with correct typesetting, in this column.

In this column we review the following books.

1. **The Universal Computer. The road from Leibniz to Turing** by Martin Davis. Reviewed by Haim Kilov. This book has stories of the personal, social, and professional lives of Leibniz, Boole, Frege, Cantor, Gödel, and Turing, and explains some of the essentials of their thought. The mathematics is accessible to a non-expert, although some mathematical maturity, as opposed to specific knowledge, certainly helps.

2. **From Zero to Infinity** by Constance Reid. Review by John Tucker Bane. This is a classic book on fairly elementary math that was reprinted in 2006. The author tells us interesting math and history about the numbers $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, e, \aleph_0$.

3. **The LLL Algorithm** Edited by Phong Q. Nguyen and Brigitte Vallée. Review by Krishnan Narayanan. The LLL algorithm has had applications to both pure math and very applied math. This collection of articles on it highlights both.

4. **Classic Papers in Combinatorics** Edited by Ira Gessel and Gian-Carlo Rota. Review by Arya Mazumdar. This book collects together many of the classic papers in combinatorics, including those of Ramsey and Hales-Jewitt.

5. **Mathematical Treks** by Ivars Peterson. Review by John Tucker Bane. This is a compilation of thirty three articles from "Ivars Peterson's MathTrek". Each chapter is a short three to five page article about an interesting math and/or computer science topic.

6. **Six Sources of Collapse** by Charles R. Hadlock. Review by Eowyn Cenek. The author defines a "collapse" to refer loosely to "some relatively rapid process that leads to a significant reduction in quantity, quality, or level of organization." He focuses on understanding how and why things go unexpected and catastrophically wrong, and how can we manage the possibility of collapse.

7. **Visions of Infinity: The Great Mathematical Problems** by Ian Stewart. Review by Aravind Srinivasan. This book describes fourteen great mathematical problems: some solved, some yet-unsolved, and some partially solved (such as variants of the three-body problem); it does so in a good amount of detail for the lay reader. However, the mission of this book is broader: how mathematics is an interconnected whole, how solutions to problems borrow from/lead to seemingly very different mathematical areas, and how mathematics serves as a foundation for several other fields. It presents historical context and applications as well, all with a gentle sense of humor.

8. **The Satisfiability Problem: Algorithms and Analyses** by Uwe Schöning and Jacobo Torán. Review by William Gasarch. This book is about SAT on many levels-algorithms for it that work in theory, algorithms for it that work in practice, and lower bounds.

BOOKS I NEED REVIEWED FOR SIGACT NEWS COLUMN

Algorithms

1. *ReCombinatorics: The Algorithmics of Ancestral Recombination Graphs and Explicit Phylogentic Networks* by Dan Gusfeld.
2. *Algorithmics of matching under preferences* By Manlove.
3. *Pearls of Functional Algorithm Design* by Bird.
4. *Jewels of Stringology Text Algorithms* by Maxime Crochemor and Wojciech Rytter.
5. *Tractability: Practical approach to Hard Problems* Edited by Bordeaux, Hamadi, Kohli.
6. *Recent progress in the Boolean Domain* Edited by Bernd Steinbach
7. *Distributed computing through combinatorial topology* by Herlihy, Kozlov, and Rajsbaum.

Misc Computer Science

1. *Selected Papers on Computer Languages* by Donald Knuth.
2. *Introduction to the Theory of Programming Languages* by Dowek and Levy.
3. *Introduction to reversible computing* by Perumalla.
4. *Algebraic Geometry Modeling in Information Theory* Edited by Edgar Moro.
5. *Digital Logic Design: A Rigorous Approach* by Even and Medina.
6. *Communication Networks: An Optimization, Control, and Stochastic Networks Perspective* by Srikant and Ying.

Mathematics and History

1. *The Golden Ratio and Fibonacci Numbers* by Richard Dunlap.
2. *A Mathematical Orchard: Problems and Solutions* by Krusemeyer, Gilbert, Larson.
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] of
The Universal Computer. The Road from Leibniz to Turing
by Martin Davis
CRC Press, 2012, 224 pages
ISBN 978-1-4665-0519-3

Review by Haim Kilov (haimk@acm.org)

1 Introduction

This is the Turing Centenary Edition of the author's book first published in 2000. According to the additional preface to this edition, the author "tidied up some loose ends and brought a few things up to date".

This very readable "book of stories" is for a general audience. The author tells the very interesting stories of the personal, social, and professional lives of Leibniz, Boole, Frege, Cantor, Gödel, and Turing, and explains some of the essentials of their thought. The mathematics is accessible to a non-expert, although some mathematical maturity, as opposed to specific knowledge, certainly helps. Davis properly observes that the reader will come away with an "enhanced respect for the value of abstract thought".

The author is a logician and computing scientist whose professional career spans six decades.

2 Summary of Contents

The book consists of nine Chapters, excellent notes, a long reference list, and an index. The first seven Chapters are about the "seven remarkable people", with titles like "Gödel Upsets the Applecart", Chapter 8 is about making the first universal computer, and Chapter 9 is "Beyond Leibniz's Dream".

Davis reminds us that "reducing logical reasoning to formal rules is an endeavor going back to Aristotle". He emphasizes Leibniz's "wonderful idea... of an alphabet representing all fundamental concepts... and an appropriate calculational tool for manipulating these symbols", and uses the familiar symbols $\int$ for integration and d for differentiation developed by Leibniz as an important example. Those of us who value abstraction and who recall Dijkstra's distinction between two kinds of thinking – (informal) pondering and (formal) reasoning [1] – with the goal of pondering to reduce reasoning to a doable amount, will probably find Leibniz's idea not unfamiliar. Davis observes that Leibniz completed his formal education (two bachelor's, master's, and a doctorate) at the age of 21, and that his doctorate in law was on the use of logic to resolve cases thought too difficult for resolution by "the normal methods". On a more practical note, Leibniz's calculating machine was the first that could carry out the four basic operations of arithmetic.

Boole's revolutionary monograph on logic as a form of mathematics includes some of the same concepts as in Leibniz's work, although Boole was unaware of Leibniz's efforts. Davis stresses that the kind of reasoning taking place informally and implicitly in ordinary human interactions could be captured by Boole's algebra, and includes examples of doing just that. Next, Frege's "crucial insight" was that the same relations that connect propositions can be used to analyze the structure of individual propositions. While Frege's logic has been the standard logic taught to undergraduates, Davis notes that "all but simplest of deductions are almost unbearably complicated in Frege's logic". Davis also quotes from Frege's diary entry for April 22, 1924: "... I have only in the last years really learned to comprehend antisemitism. If one wants to make laws against the Jews, one must be able to specify a distinguishing mark by which one can recognize a Jew for certain. I have always seen this as a problem.", and observes that these ideas "were hardly rare in Germany after World War I". Regretfully, Peirce's general algebra of relations adopted by Peano as the basis of the modern notation of predicate calculus is not mentioned by Davis, although Peano is mentioned in passing. For an overview of this work of Peirce, see, for example, [2] heavily commented by John Sowa who stresses that "Peirce attained a level of formalization that surpassed anything achieved by Frege or Russell".

Davis provides an enjoyable treatment of Cantor's conceptual contributions (such as infinite sets coming in more than one size, the continuum hypothesis, transfinite ordinal and cardinal numbers, and the diagonal method, – but not Cantor's famous definition of a set) stressing that "Cantor was exploring a domain that had been visited by no one before him. There were no mathematical rules on which he could rely. He had to invent it all himself, relying on his intuition". Cantor's nervous breakdowns are also mentioned. Further, Hilbert's interest in and development of foundations of mathematics (starting with foundations of Euclidean geometry) is the main focus of Davis's chapter on Hilbert in which not only consistency of arithmetic and metamathematics but also Brouwer's intuitionism is treated in quite some detail.

The Chapters on Gödel and Turing are the longest in the book, and for an obvious good reason: explaining their achievements to the uninitiated – while not forgetting about the biographies as well as about political and social environments of that time – takes some effort. The author clearly succeeds in his explanations, although in my opinion somewhat overemphasizes the encoding details in both of these Chapters. For another, more abstract, treatment of Gödel's theorem, also written for and accessible to a general audience, see [3] on the very first page of which we read: "by pure deductive reasoning, *one cannot even deduce from a finite number of basic principles all true statements about integers that can be formulated in the language of high school algebra*" (Manin's italics). In this context of irreducibility of the human mind to a mechanism (recalling also Gödel's famous quote that "mind is not mechanical... mind cannot understand its own mechanism"), it would be nice to mention Hayek's "limits of explanation" [4]: no explaining agent can ever explain objects of its own kind or of its own degree of complexity, so the human brain can never fully explain its own operations in sufficient detail. While the reference to Gödel is implicit in [4], it is explicit in another Hayek's paper [5]. Nevertheless, reductionism is still alive: for example,

Davis notes that "Searle and Penrose tacitly accept the premise that ... human mind is produced by the human brain... subject to the laws of physics and chemistry".

Davis emphasizes a very important characteristic of Turing's universal machine: it showed that "the distinctness of machine, program and data is an illusion". This was understood very well, for example, by von Neumann who, as Davis notes, proposed in 1945 that the soon-to-be-built EDVAC be realized as a physical model of Turing's universal machine. (Von Neumann's work is substantially discussed by Davis, although there is no separate Chapter devoted to him. Outstanding samples of contemplation (von Neumann Universe) and action (Hiroshima) in the professional life of von Neumann are shown in [7].) Davis also observes – and includes as one of his epigraphs to his Introduction – that as late as in 1956, Howard Aiken stated: "If it should turn out that the basic logics of a machine designed for the numerical solution of differential equations coincide with the logics of a machine intended to make bills for a department store, I would regard this as the most amazing coincidence I have ever encountered." (The other epigraph is a quote from Turing's 1947 address to the London Mathematical Society about his universal machine.) And on a more practical note, Davis stresses that Turing's decoding machines built from his design during the WWII effort "worked correctly as soon as they were made". Davis also quotes both Turing's observation that programming "should be very fascinating", and his complaints about "the American tradition of solving one's difficulties by means of much equipment rather than by thought"; here again we may recall Dijkstra [6].

3 Opinion

The stories masterfully told in this book underscore the power of ideas and the "futility of predicting in advance where they will lead". While the stories draw heavily on previously published biographies and other material, the structure and presentation of the material make the book an outstanding achievement.

This book is obviously just a start. Manin's papers about Gödel [3] and Cantor [8] (the latter – for a more initiated audience), on the one hand, and Dijkstra's papers, on the other hand, may be recommended for further reading. For those who are interested in business modeling (including the so called "business rules") and in system thinking in general, Hayek's papers (such as [5]) would be an excellent starting point.

Finally, I would like to quote from Davis's Epilogue: "Too often today, those who provide scientists with the resources necessary for their lives and work, try to steer them in directions deemed most likely to provide quick results... by discouraging investigations with no obvious immediate payoff, it short-changes the future."

References

1. E.W. Dijkstra. The teaching of programming, i.e. the teaching of thinking. In: Language hierarchies and interfaces. (Eds. F.L. Bauer and K. Samelson), Lecture Notes in Computer Science, Vol. 46 (1976), pp. 1-10, Springer Verlag.

2. Existential Graphs. MS 514 by Charles Sanders Peirce, with commentary by John F. Sowa.

   jfsowa.com/peirce/ms514.htm

3. Y. Manin. Gödel's theorem. In: Y. Manin. Mathematics as Metaphor. American Mathematical Society, 2007, pp. 55-68.

4. F.A. Hayek. The sensory order. Routledge and Kegan Paul Limited, London, 1952.

5. F.A. Hayek. Rules, perception and intelligibility. Proceedings of the British Academy, XLVIII, London, 1962. [Reprinted in: F.A. Hayek. Studies in Philosophy, Politics and Economics. Simon and Schuster, NY, 1969.]

6. E.W. Dijkstra. On the fact that the Atlantic Ocean has two sides. EWD611.

   www.cs.utexas.edu/users/EWD/transcriptions/EWD06xx/EWD611.html.

7. Y. Manin. Mathematical knowledge: internal, social and cultural aspects. 2007.

   http://arxiv.org/abs/math/0703427

8. Y. Manin. Georg Cantor and his heritage. In: Y. Manin. Mathematics as Metaphor. American Mathematical Society, 2007, pp. 45-54.

Review of From Zero to Infinity[3] of
From Zero to Infinity
by Constance Reid
A K Peters, Ltd. 2006
188 pages, soft cover

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

1 Introduction

From Zero to Infinity is made up of twelve chapters about a variety of mathematical subjects. Each of the first ten chapters is about what makes one of the first ten natural numbers (including zero) special, then goes into detail on a subject related to what makes that number unique. Chapters eleven and twelve have similar form, but with regards to e and $\aleph_0$ respectively. While the mathematical topics in each chapter initially appear to have little to do with each other, by the end almost every theory explained relies on several others shown in previous chapters.

Each chapter ends in a problem for the reader to solve using the information from that chapter. These problems start out very simple, but grow more difficult as the book progresses. Answers are given upside down near the questions.

2 Summary

Chapter 1: ZERO

This chapter talks about the origin of zero as a true number rather then a place holder for a lack of value, and describes a chronological snafu caused by the lack of zero. It also speculates about why zero was not considered a real number for such a long time by so many great minds. The chapter ends with a trick question I won't spoil here.

Chapter 2: ONE

This chapter describes one as the basis from which all other number are built and waxes philosophical on the importance of one as a concept. She then uses the idea that each number is a unique number of ones as a jumping off point to talk about unique prime factorization and it's important to mathematics as a whole.

Chapter 3: TWO

This chapter talks about the importance of two as the basis of binary. It goes on to discuss what one mathematician thought were the religious implications of base two and how it forms the basis for a simple way to preform the multiplication and division of large

numbers by hand. The chapter finishes by talking about the importance of base two to digital systems and ends with several arithmetic problems in base two.

Chapter 4: THREE

In this chapter describes three as the first "typical" prime. Then there are proofs that both the prime and composite numbers are infinite using prime factorization and gives several different methods for finding prime numbers. The chapter ends with several questions concerning sums of powers of three.

Chapter 5: FOUR

This chapter describes the importance of four as the first perfect square. After a short discussion of the relation between the infinite number of natural numbers and the infinite number of squares the book goes on to discuss the Pythagorean theorem. It discusses the contributions of several famous mathematicians to our understanding of the Pythagorean theorem and the more general problem of making $a^n + b^n = c^n$.

Chapter 6: FIVE

This section talks about the properties of the number of interior angles in a set of a given number of similar pentagons which share an origin. These numbers known as the pentagonal numbers. The chapter then reveals the surprising relationship between the pentagonal numbers and the problem of finding the total number of possible partitions a given number can be split into. She then explains how partition numbers can be found using a specific generating function and closes with a limited version of a generating function for the reader to try for their own.

Chapter 7: SIX

Chapter six notes that six is the first perfect number. It also discusses the use of powerful computers to find primes and test if claimed perfect numbers are truly perfect.

Chapter 8: SEVEN

This chapter talks about the ancient Greek's mystical beliefs about the number seven. It also describes a connection between Fermat's numbers and the problem of which polygons are drawable with basic tools.

Chapter 9: EIGHT

This chapter notes that eight is the first cube and then discuses the minimum and maximum numbers of cubes and other powers known to be needed to sum to both finite and infinite ranges of integers.

Chapter 10: NINE

This chapter goes into detail about the many ways nine can be used as a short-cut to check the accuracy of arithmetic done by hand. Since this checking is all based on mod 9 the book then goes on to talk about the importance of modulo to several other problems of historical interest.

Chapter 12: EULER'S NUMBER

This chapter talks about the origin of Euler's Number and how it came to be known by that name to spite Euler's best intentions. Then this chapter transitions from Euler's Number to the importance of the natural logarithm and some of the first imaginary numbers.

Chapter 12: ALEPH ZERO

This Chapter delves into the properties of infinities and how they are classified and compared. It contains several light but interesting proofs of the classifications of the natural, rational, and decimal rational numbers as various kinds of infinity.

3 Opinion

I (an undergraduate comp sci major) personally enjoyed this book. The author clearly has a love of numbers that can prove infectious. While the proofs of some of the more complicated theorems are omitted, the proofs given are all clear and easy to understand.

I suspect that 3/4 of the readers of this column know 3/4 of the content of this book. However, it would make a perfect gift for your mathematically inclined children, niece, nephew, etc who is in, say, high school.

Review of[4]
The LLL Algorithm
Edited by Phong Q. Nguyen and Brigitte Vallée
Springer, 2009
496 pages, Hardcover

Review by
Krishnan Narayanan (nkrish2010@gmail.com)

1 Introduction

Lattices are geometric objects underlying linear Diophantine equations in the same way as vector spaces underlie linear equations. Just as every vector space has a basis (indeed lots of them), every lattice has a basis of lattice vectors (and indeed lots of them). A key difference is that, while every vector space admits a basis of orthogonal vectors, a lattice in general does not have an orthogonal basis of lattice vectors. However a lattice does have a basis close to orthogonal, which consists of reasonably short lattice vectors. Lattice basis reduction or lattice/basis reduction in short, refers to the construction of such a basis of short lattice vectors. Lattices underlie numerous problems in number theory, algebra, cryptography and combinatorial optimization and the efficient construction of a basis of reasonably short lattice vectors lies at the heart of the solution to these problems.

To begin at the beginning, a lattice can be pictured as a regular arrangement of points in space. More precisely, a lattice L is the set of integer linear combinations of n linearly independent vectors $\boldsymbol{b_1}, \boldsymbol{b_2}, \ldots \boldsymbol{b_n}$ in Euclidean space $\mathbb{R}^n$: $\mathrm{L} = \{ \boldsymbol{Bx} \,|\, \boldsymbol{x} \in \mathbb{Z}^n \}$ where matrix B has the vectors $\boldsymbol{b_1}, \boldsymbol{b_2}, \ldots \boldsymbol{b_n}$ as its columns. A more abstract but equivalent definition of a lattice is that it is a discrete subgroup of $\mathbb{R}^n$. A lattice has several bases and a lattice is conveniently described by giving any one of them. Some of the central questions about lattices are finding (the length of) a shortest vector in a lattice (there can be more than one shortest vector), finding the closest lattice vector to a given point in space, finding a short basis of the lattice, and finding short linearly independent lattice vectors. These lattice problems turned out to be NP-complete, and the best known algorithms for these problems have a running time exponential in the lattice dimension n, even for small n. The LLL algorithm is the first polynomial time algorithm for these problems though its approximation factor is exponential in the lattice dimension in the worst-case. The power of the LLL algorithm was apparent at its birth as it almost immediately led to the first polynomial time algorithms for factoring polynomials and for integer programming in fixed dimensions by its creators.

The discovery of an efficient lattice basis reduction algorithm, simply called the LLL algorithm, after its inventors Arjen Lenstra, Hendrik Lenstra and László Lovász in 1982 has

led to a major revolution in several fields such as computational number theory and algebra, combinatorial optimization and public key cryptography. More specifically in computational number theory and algebra it yielded polynomial time algorithms for simultaneous Diophantine approximation, for finding integer relations among real numbers, for checking solvability of equations by radicals and for factoring polynomials over rationals. In combinatorial optimization, it yielded an efficient algorithm for integer linear programming in fixed number of variables. Perhaps LLL's most amazing success has been in cryptography. In cryptography, it initially yielded an algorithm for cryptanalysis of Merkle-Hellman cryptosystem and several knapsack-based cryptosystems. The Coppersmith method that uses the LLL algorithm to find small roots of modular polynomials has influenced the cryptanalysis of RSA enormously. In a major breakthrough, in 1998 Ajtai showed a worst-case to average-case reduction for lattice problems and this enabled for the first time the design of cryptosystems with provable security (hard-on-average) based on worst case hardness of lattice problems. Lattice cryptography has made rapid strides in the last decade with several major advances including Gentry's seminal work on Fully Homomorphic Encryption based on ideal lattices in 2010. The LLL algorithm and its variants have been remarkably versatile in almost every application involving lattices.

This book is a compilation of survey-cum-expository articles contributed by leading experts on the occasion of the 25th anniversary of the LLL algorithm.

2 Summary

Chapter 1: The History of the LLL-Algorithm by I. Smeets

The first chapter of the book describes origins of the LLL algorithm based on the opening lectures of the three protagonists of our story - Arjen Lenstra, Hendrik Lenstra and László Lovász, and Peter van Emde Boas at the conference in Caen, France, in 2007 on the occasion of the 25th anniversary of the LLL algorithm. It is fascinating to read that a simple question about the existence of a polynomial time algorithm to determine whether a point with integer coefficients lies inside a triangle defined by three rational coordinates in the plane is the starting point of the discovery of the celebrated LLL-algorithm. Hendrik Lenstra describes how his discovery of a polynomial time algorithm for integer programming was inspired by the above question on a triangle in integer lattice and the central role of Lovász basis reduction in it. Lovász describes how his interest in applying the then new Ellipsoid algorithm to combinatorial optimization problems led to the discovery of the crucial lattice basis reduction algorithm. Arjen Lenstra describes how he used lattice basis reduction to arrive at the first polynomial time algorithm for factoring polynomials over rational numbers. The text is illustrated with historical photographs of the authors and the postcards written by them during the discovery of the LLL algorithm and they are a visual treat.

Chapter 2: Hermite's Constant and Lattice Algorithms by P. Q. Nguyen

The heart of this chapter is an insightful reconstruction of the LLL algorithm as an efficient relaxation of the proof of Hermite's theorem on Hermite's inequality. This inequality states that for any integer $d \geq 2$, the Hermite's constant γ_d satisfies $\gamma_d \leq \gamma_2^{d-1}$, where $\gamma_2 = \sqrt{4/3}$. Hermite's constant γ_d is closely related to the maximum packing density of $\mathbb{R}^d$ with spheres. The proof of the Hermite's theorem is directly translated into the first Hermite's lattice reduction algorithm stated in this chapter. As the structure of this algorithm does not match the Gaussian lattice reduction algorithm (dimension 2), a second reduction algorithm of Hermite is described. The LLL algorithm is presented essentially as a relaxed variant of Hermite's second algorithm. As another illustration of this approach, Mordell's inequality, which is a generalization of Hermite's inequality is used to derive the blockwise variant of the LLL algorithm. The lucid presentation of lattice fundamentals given in this chapter can equip the reader with the background needed to read the rest of the book.

Chapter 3: Probabilistic Analysis of Lattice Reduction Algorithms by B. Vallée and A. Vera

The focus of this chapter is a dynamical systems framework for the LLL algorithm in which a large number of two dimensional dynamical systems running in parallel are incorporated. The information collected from the running of these small dynamical systems is put together to obtain the parameters of the entire system. The two dimensional dynamical systems correspond to the Gaussian algorithm (two dimensional lattice reduction) and they operate on the sublattices of the original lattice. This chapter also provides an extensive discussion of the dynamical systems approach to the analysis of the Gaussian algorithm. A reformulation of the LLL algorithm which shows the Gaussian reduction quite explicitly is also given here. Using a variety of probabilistic models and mathematically sophisticated analysis, the behaviour of the LLL algorithm is analyzed in detail to obtain quantities such as the mean number of iterations, the mean bit complexity and the geometry of the output reduced lattice basis.

Chapter 4: Progress on LLL and Lattice Reduction by C. P. Schnorr

This chapter explores the variants of LLL in two directions. The first is the use of floating point arithmetic to perform orthogonalizations as the use of integer arithmetic in Gram-Schmidt orthogonalization (GSO) is somewhat slow and limits the use of the LLL algorithm to low dimensional lattices. The LLL algorithm with Householder orthogonalization (LLL_H) for floating point arithmetic is shown to be robust and efficient. The speedup of LLL_H for large dimensions using LLL-type segment reduction is described. Several methods that yield improved approximations of the shortest lattice vector are given. In the other direction, an extension of the LLL algorithm to indefinite quadratic forms that has applications in public key identification and signature schemes is described.

Chapter 5: Floating-Point LLL: Theoretical and Practical Aspects by D. Stehlé

The focus of this chapter is the speeding-up of the LLL algorithm by replacing the rational arithmetic used in Gram-Schmidt Orthogonalization by floating-point arithmetic. Modern applications of lattice reduction such as lattice-based cryptography, cryptanalysis of public-key cryptosystems, and univariate polynomial factorization involving lattice bases of huge (up to several hundreds) dimensions motivate the need for efficient and reliable floating-point LLL algorithms. Provable floating-point LLL algorithms guarantee termination and produce reliable output which is essential for mathematical results such as proving that there is no small linear relations among a given set of numbers. Two provable floating-point LLL algorithms - the first such algorithm by Schnorr and a later algorithm, the L^2 algorithm by Nguyen-Stehlé - are described in detail. An interesting remark states that the provable quadratic bit-complexity of the L^2 algorithm makes it a natural variant of the basic LLL algorithm. The issues arising in practical implementations of floating-point LLL algorithms in software packages such as LiDIA, Magma and NTL are described.

Chapter 6: LLL: A Tool for Effective Diophantine Approximation by G. Hanrot

Simultaneous Diophantine approximation (SDA) and the small values of linear forms along with some of their applications are the focus of this chapter. The interesting result that the LLL algorithm can be used to obtain a deterministic polynomial time algorithm for SDA at the cost of an exponential approximation factor is proved. The use of the LLL algorithm in the disproof of the famous Mertens' conjecture about the behaviour of the Möbius function is described. The small linear relations problem is stated as the dual of SDA. The LLL algorithm is used to obtain both constructive results that show small values of linear forms and negative results that show the non-existence of small relations. Some of the other results covered in this chapter are Schnorr's use of Diophantine approximation for integer factorization, the applications to Baker's method in the study of Diophantine equations, approximation of a given real number by an algebraic number, and the relation between the LLL algorithm and the ABC conjecture in number theory.

Chapter 7: Selected Applications of LLL in Number Theory by D. Simon

The focus of this chapter is the use of the LLL algorithm in solving several different linear problems and quadratic equations. Examples of linear problems are the approximation of a real number by rational numbers, finding integer relations among real numbers, and obtaining the minimal polynomial of an algebraic number. In the section on solving quadratic equations over the rationals, a variant of the LLL algorithm called the Infinite LLL for n-ary quadratic forms over integers is introduced and this formulation is used to compute the 2-Sylow subgroup in class groups with negative discriminant. By adapting the LLL algorithm to number fields, the notion of LLL reduction of ideals is presented which can compute class groups. This chapter concludes with examples that illustrate the power of LLL in settling/throwing light on conjectures such as the disproof of Mertens' conjecture and in

finding surprising relations among integers.

Chapter 8: The van Hoeij Algorithm for Factoring Polynomials by J. Klüners

This chapter describes the van Hoeij algorithm for factoring polynomials as a refinement of the classical Zassenhaus algorithm for this problem. The Zassenhaus algorithm for polynomial factorization was implemented widely in computer algebra systems and it worked well in practice although its worst-case complexity was exponential. van Hoeij showed that the combinatorial bottleneck in the Zassenhaus algorithm which made it too slow on a class of inputs can be eliminated by a simple use of the LLL algorithm in solving a specific knapsack problem involving binary weights. This new algorithm called the van Hoeij algorithm transforms the classical Zassenhaus algorithm into a truly polynomial time algorithm which also works well in practice.

Chapter 9: The LLL Algorithm and Integer Programming by K. Aardal and F. Eisenbrand

The focus of this chapter is the structural and algorithmic implications of the LLL algorithm in integer programming (IP). After giving an example to show that the branch-and-bound method for IP based on a single-variable can take exponentially many steps in the size of the input even in dimension 2, a more general branching-on-hyperplanes approach is described. This refers to enumerating parallel hyperplanes that cover all lattice points. Lenstra's IP algorithm is described as an algorithmic version of Khinchin's flatness theorem. A survey of related results such as Barvinok's polynomial time algorithm for counting integer points and a polynomial time algorithm for Hermite Normal form is given. The chapter concludes by describing a linear time algorithm for integer optimization problem in fixed dimension with fixed number of constraints.

Chapter 10: Using LLL Reduction for Solving RSA and Factorization Problems by A. May

The focus of this chapter is the Coppersmith method for finding the small roots of modular polynomials based on the LLL algorithm and its applications to the problem of inverting the RSA function and to the factorization problem. The theorems in this chapter have dual interpretation, either as cryptanalysis results or as security/hardness results. The RSA problem is introduced as the problem of inverting the RSA function on the average and its difficulty is related to the security of RSA. Several RSA related problems that can be solved by the application of the Coppersmith method are described in detail. The relaxed factorization problem is to find the factorization of given number N which is a product of two large primes in polynomial time with minimum number queries to the given oracle for the most significant bits of the larger prime factor. A solution to this problem using the Coppersmith approach is given. Using the Coppersmith approach, a deterministic reduction of factoring to computing the secret exponent of RSA is given, thereby establishing the

polynomial time equivalence of these two problems. Further applications of the Coppersmith method to the problem of finding smooth integers in an interval and in solving bivariate modular polynomial equations are given.

Chapter 11: Practical Lattice Based Cryptography: NTRUEncryt and NTRUSign by J. Hoffstein, N. Howgrave-Graham, J. Pipher, and W. Whyte

The focus of this chapter is a detailed description of NTRU, an efficient cryptosystem based on a special class of ideal lattices. A comparative overview of three lattice based cryptosystems namely, Ajtai-Dwork, GGH and NTRU shows the crucial role of efficiency in taking lattice cryptography closer to practice. The pioneering Ajtai-Dwork scheme showed for the first time the provable security of a cryptosystem based on the worst-case complexity of a lattice problem, but due to its inefficiency (large public key size, quadratic in the dimension of the input lattice) it could be broken in all cases where an implementation is practical. The GGH cryptosystem did not have the provable security property though it was more efficient than Ajtai-Dwork and it could be broken in lattice dimension 300 due to leakage of information about the secret key. The NTRU cryptosystem is the most efficient of the three (key size linear in dimension of the lattice) though it lacked a formal proof of security. (Subsequently a proof of security of NTRU-based encryption and signatures based on worst-case lattice problems was given by Stehlé-Steinfeld in 2011.) NTRU based public key cryptosystem and digital signature scheme are described here in detail along with their performance and security analysis for various choices of parameters. An interesting heuristic given here states that if the actual length of shortest lattice vector is much shorter than a quantity called the (Gaussian) probable shortest length of the lattice, then the LLL algorithm can easily locate the shortest vector. This is used to account for the success of the LLL algorithm in breaking low density knapsacks.

Chapter 12 : The Geometry of Provable Security: Some Proofs of Security in Which Lattices Make a Surprise Appearance by C. Gentry

The focus of this chapter is the role of lattice reduction in security proofs of non-lattice cryptosystems. A reduction of factoring large numbers to the problem of forging Rabin signatures in the random oracle model is given. The Coppersmith method, described in Chapter 10, plays a central role in many of the security arguments given in this chapter. It is used to obtain efficient security reductions for OAEP-enhanced Rabin and low-exponent RSA. OAEP (Optimal Enhanced Encryption Padding) is a 'padding' method for plaintext messages used in RSA to prevent malleability attacks. The interesting result that RSA-OAEP is secure for general exponents is described. The security of Rabin partial-domain-hash (Rabin-PDH) signature scheme is discussed. Hensel lifting with lattice reduction is shown to solve the hardness of RSA, Pellier and RSA-Pellier problems. The concluding section on the bit security of Diffie-Hellman problem uses lattice reduction to show the hardness of the most significant bits of the Diffie-Hellman secret.

Chapter 13: Cryptographic Functions from Worst-Case Complexity Assumptions by D. Micccianco

A distinguishing feature of lattice-based cryptographic functions is their provable security based on the worst-case hardness of lattice problems. This chapter illustrates this theme by the design of two cryptographic functions, namely Collision Resistant Hash Functions (CRHF) and Public Key Cryptosystems (PKC). An initial construction of an inefficient but provably secure CRHF is refined using a powerful analysis method which involves Gaussian distributions on lattices and specializing the construction to a particular class of lattices called ideal lattices which are lattices arising as ideals in a ring. The Gaussian perturbation techniques used in this construction are of wide applicability in lattice cryptography. The seminal Ajtai-Dwork PKC with provable security is described along with its improved security analysis using Fourier methods and a later enhancement to achieve CCA security. This chapter concludes with a discussion of concrete security issues in lattice cryptography. An interesting distinction is made between algebraic and geometric lattices in regard to the special classes of lattices used in the construction of CHRF and PKC.

Chapter 14: Inapproximability Results for Computational Problems on Lattices by S. Khot

As the best known polynomial time algorithms for basic lattice problems achieve an approximation factor which is essentially exponential in the dimension of the lattice, a natural question arises as to the largest approximation factor within which these problems can be proved to be hard to approximate. Apart from their theoretical interest, such questions are also important as they have implications to the design of provably secure cryptosystems based on the worst-case complexity assumptions about lattices. Inapproximability results establish the limitations on the provability of hardness results. Such results have the structure that if an approximation of a hard problem within a certain factor is NP-hard, then an unlikely event such as the collapse of the polynomial time hierarchy (PH) is the implication. A survey of the inapproximability of several basic lattice problems such as the shortest vector problem (SVP) and closest vector problem (CVP) is given in this chapter. For the CVP problem, a sketch of the proofs that CVP is hard to approximate to within any constant factor and also that it is hard to approximate to within almost polynomial factor unless NP is contained in quasi-polynomial time is given here. An outline of the proofs of the results that SVP is NP-hard to approximate to within a constant factor less than $\sqrt{2}$ and its subsequent improvement to inapproximability within almost polynomial factor unless NP is contained in quasi-polynomial time concludes the chapter.

Chapter 15: On the Complexity of Lattice Problems with Polynomial Approximation Factors by O. Regev

This chapter is closely related to the previous chapter. For basic computational lattice problems such as SVP, there is a huge gap between the essentially exponential approxi-

mation factor of the best known (even randomized) polynomial time algorithms and the subpolynomial factor hardness of the best known hardness results. The polynomial factor approximations lying in this gap are of crucial importance in cryptographic schemes designed for provable security as they are based on worst-case hardness assumptions of lattice problems with polynomial approximation factors. This connection was first shown by Ajtai. The results proved here show that approximating lattice problems beyond $\sqrt{n/\log n}$ is unlikely to be NP-hard. A prover efficient zero knowledge proof system described in this chapter is the basis of an interesting lattice based identification protocol. An approximation preserving reduction from SVP to CVP is given to show that all the results proved here for approximating CVP also hold for approximating SVP.

3 Opinion

The LLL algorithm embodies the power of lattice reduction on a wide range of problems in pure and applied fields from Diophantine analysis to cryptography and combinatorial optimization. As a versatile and practical algorithm, the success of the LLL algorithm attests the triumph of theory in computer science.

The LLL Algorithm book provides a broad survey of the developments in various fields of mathematics and computer science emanating from the LLL algorithm. As well-known researchers in their areas, the authors present an invaluable perspective on the topics by sharing their insights and understanding. The book is an exemplar of the unity of computer science in bringing a broad array of concepts, tools and techniques to the study of lattice problems. The many open problems and questions stated in every chapter of the book will inspire researchers to explore the LLL algorithm and its variants further. Graduate students in computer science and mathematics and researchers in theoretical computer science will find this book very useful. Finally, it is simply a pleasure to read this lovely book.

Review of[5]
Classic Papers in Combinatorics
Edited by Ira Gessel and Gian-Carlo Rota
Modern Birkhäuser Classics, 1987 (reprinted in 2009)
492 pages, SOFTCOVER

Review by
Arya Mazumdar arya@umn.edu
University of Minnesota, Minneapolis, MN 55455

1 Introduction

"We have not begun to understand the relationship between combinatorics and conceptual mathematics." –Jean Dieudonné, A Panorama of Pure Mathematics: As seen by N. Bourbaki, Academic Press, New York, 1982.

The book *Classic Papers in Combinatorics* edited by Gessel and Rota chronicles the development of combinatorics by reprinting 39 papers from the period of 1930 to 1973 – a span of 44 years. These are definitely the formative years for many branches of combinatorial theory. The papers are arranged in a completely chronological order, starting with Ramsey's paper of 1930 (Ramsey theory) and ending with Geissinger's three part paper of 1973 (Möbius functions). The authors of the papers collected in this volume are giants of the field; however this book (rightly) does not try to collect representative papers from all famous combinatorists. A more important goal perhaps is to include representative papers from all areas of combinatorics – and it might have fallen a little short of that goal.

Nonetheless, a bunch of great papers together makes it an excellent reference book. There is a two-page introduction at the start of the book, where the editors try to group the papers according to some common threads – as well as give a brief description of some of the results. This summary reads as if it were a bit hurriedly written, and I could use a longer description of papers and some justification on why these 39 papers clearly stand out among the many excellent papers published in the period. As it stands, this introduction was still quite useful to me for the purpose of browsing through the book.

It is also unclear that, given the book was first printed in 1987, why the editors stop at 1973. Is 1973 the end of the *classic* era in combinatorics by some common agreement? I can surely think of some outstanding results appearing in the seventies and eighties.

The editors also sometime put footnotes in the papers to point out errata or provide some extra relevant information. Such instances are very rare though.

2 Summary

It is clearly not a good strategy to provide summary of all thirty nine papers of the volume here - neither would that be very enlightening. I am providing many representative threads that interest computer scientists in general.

Ramsey's famous paper called "On a problem of formal logic" (Paper 1 of this collection) lays foundation of a large class of existential results that forms Ramsey theory. To quote a later paper by Erdös and Rado, also appearing in this collection (Paper 14), Ramsey's paper "discovered a remarkable extension of this (the very basis pigeon-hole) principle," and can be summarized as follows: "Let S be the set of all positive integers and suppose that all unordered pairs of distinct elements of S are distributed over two classes. Then there exists an infinite subset A of S such that all pairs of elements of A belong to the same class." Although Ramsey theory is very much a topic of textbooks now, it is intriguing to see the ideas developing in the papers by Erdös and Szekeres (Paper 3), Erdös and Rado (Paper 14) and branching out in different directions. The paper "A combinatorial problem in geometry" by Erdös and Szekeres (Paper 3) shows the existence of a number $N(n)$ for any given number n, such that any set containing at least $N(n)$ points has a subset of size n that forms a convex polygon. The graph theoretic result, that is in the core of Ramsey theory, appears in this very paper for the first time: for every large enough graph, there either exists an independent set or a clique of pretty large size.

Erdös's paper "Graph theory and probability," (Paper 19) is perhaps the pioneer of the very powerful probabilistic methods which subsequently motivated developement of many randomized algorithms. This paper starts where Erdös and Szekeres (Paper 3) lefts of. By considering the ensemble average property of all subgraphs of a complete graph, Erdös shows a *converse* result to Ramsey-type theorems: If $n \leq \ell^{1+1/2k}$, then a graph on n vertices exists that does not contain either of an independent set of size ℓ or a k-cycle.

Brooks's "On colouring the nodes of a network" (Paper 7) contains the first nontrivial result in graph-coloring. In a *coloring* of a graph we assign colors to the vertices of a graph such that no two neighbors (connected by an edge) gets the same color. Coloring a graph with a number of colors one more than the maximum degree of the graph is trivial. Brooks shows that a number of color equal to the maximum degree d is actually sufficient provided the graph does not contain a clique with d+1 vertices. The proof is algorithmic. Further results on graph coloring appear in Lovász's "A characterization of perfect graphs" (Paper 34). While it is clear that one needs a number of colors at least equal to the maximum clique size, Lovász shows the conditions under what that limit can be achieved with equality.

There is a number of papers in this volume that are celebrated among the algorithms community – and some results that almost all computer scientists are familiar with. It is nice to see Hall's marriage theorem (Paper 4), Ford and Fulkerson's network flow algorithm (Paper 15) or Edmond's algorithm for matching (Paper 26) in the original papers. I am more used to in seeing Hall's theorem in a graph theoretic formulation. In its original form, the statement involved finding a complete set of distinct representatives for a collection of sets (the graph theoretic statement follows trivially from there). Halmos and Vaughan

("The marriage problem", Paper 11) provides the standard short proof of Hall's theorem. Ford and Fulkerson's "Maximal flow through a network," (Paper 15) is the easiest read of this collection, despite its far-reaching applications. The maximum flow through a (railway) network is bottlenecked by the minimum cut (a set of links that on removal disconnects the network). The paper first provides a proof of this maxflow-mincut theorem and then turns the theorem into an efficient computational scheme for planar graphs. As an interesting observation, it was shown in the end of this paper that, by constructing a somewhat unusual *dual* graph of any planar graph, the problem of finding a minimum path can be reduced to the maximum flow problem.

Finding most of the natural graph features, such as maximum independent set, minimum vertex cover etc., are intractable computationally and many times even hard to approximate. In contrast, finding a maximum *matching* is very tractable. The algorithm to find maximum matching in polynomial time first appears in Edmond's paper "Paths, trees and flowers" (Paper 26). The philosophical question of why matching in an arbitrary nonbipartite graph tractable bothered Edmond even while writing the paper. The paper contains a rather long digression on what is efficient computability (recall, this is before Karp's or Cook's canonization). At some point Edmond says, "I am claiming, *as a mathematical result*, the existence of a *good* algorithm for finding a maximum cardinality matching in a graph." This is a truly epic paper – perhaps not so much in terms of volume (16 pages), but in terms of beauty and serenity.

This collection does a good work in chronicling the developement of the theory of matroids by including the key papers by Whitney and Tutte. Whitney's paper "Non-separable and planar graphs" (Paper 2) introduces the terminology of *rank, nullity* and *duality* for graphs, and lays foundation for studying linear dependency in combinatorial terms. Matroids are formally defined in the later paper "The abstract properties of linear dependence" (Paper 5) where we see terminologies that are quite standard today. Somewhat nonstandard nomenclature is used in Tutte's "A ring in graph theory" (Paper 9) which redefines some of Whitney's notions in terms of graph theory.

A major topic of this collection is definitely the theory of Möbius functions. In this collection more than a few, including a three-part paper by Geissinger (Papers 37, 38 and 39), deal with Möbius functions. This definitely reflect the editor's interest in the topic. Rota's "Theory of Möbius functions" (Paper 25) is really expository in terms of motivating Möbius functions for the use of enumeration. This set of papers is also the representative of algebraic combinatorics in this collection. I was unaware of Pólya's otherwise famous paper called "On picture writing" (Paper 16). This is definitely one of the most interesting papers and worthy of this collection by any measure. The editors mention in the introduction that this curious paper foreshadows the theory of incidence algebra and Rota's paper (Rota is one of the editors – hence this must be true, although Rota's paper do not cite this paper of Pólya).

Other papers of this collection include Brooks, Smith, Stone and Tutte (Paper 6), that used Kirchhoff's law of electrical circuits to solve a combinatorial problem, Kaplansky's two-page simple solution of the famous *problème des ménags* (Paper 8) and Lubell's short proof

of Sperner's lemma (Paper 28).

The few papers that we left out in the above discussion are as important in the development of combinatorics as any one above and represent works of the superstars such as de Bruijn, Dilworth, Katona, Nash-Williams and Stanley, among others.

3 Opinion

As mentioned earlier, all of the papers of this collection are excellent, and this serves as a good reference book. But who would like to have a book such as this? It is unlikely that having this book will, in any way, make life easier for a researcher – as almost all (if not all) of these papers (being very famous) are available over the internet. However a familiarity with the contents of this book might save us the time of internet searching and taking prints of a popular reference several times over the years – we may just find that reference in this collection.

A book like this therefore was somewhat more relevant in 1987 when it first came out. However, even now the *book format* perhaps give some motivation to look back at the original papers without any particular reason. I wish the editors have given some more insight into the papers, some more reasoning to include them, and perhaps share some stories behind them. The complete chronological ordering also makes little sense, as a much better idea would be to group papers that develop a particular topic together – such as papers of Ramsey theory, or papers on matroids. That way the collection would be easier to read and it would be a simpler task to find common themes and techniques out of this collection as a whole.

The editors have done a commendable job of finding a right mix of papers that divides evenly between papers that are problem-solving oriented and papers that focus on theory development. That being said this book may not be a representative of all areas of combinatorics – it is doubtful that if any one book can be. There are plenty of developments in algebraic combinatorics or additive number theory around the time frame considered here. Also the beautiful theories of combinatorial design or finite geometry are absent. Nonetheless, the chosen papers had a huge impact on combinatorics and beyond.

Some papers, such as Erdös and Szekeres (Paper 3) and Hall (Paper 4), are a bit difficult to read because of the poor typesetting. Actually, it seemed to me that every paper is reproduced as their original format and not really reprinted. Therefore there is no consistency in the print sizes of different papers.

Despite of all these, I feel glad that I have this book in my shelf – very few things beat thirty nine of the best papers of last century together under one cover.

Review of Mathematical Treks[6] of
Mathematical Treks
by Ivars Peterson
The Mathematical Association of America, 2002
170 pages, softcover, $30.00

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

1 Introduction

Mathematical Treks is a compilation of thirty three articles from "Ivars Peterson's Math-Trek". It is "the first product of a joint publishing venture between the MAA and Science News". Each chapter is a short three to five page article about an interesting math and/or computer science topic. It self describes as a book about "cool stuff" from across the world of mathematics. The structure of the articles is highly fluid, never quite the same from one to the next. But there are some common themes shared by many of the articles.

There is generally a description of the interesting problem or technique, followed by a history of who's worked on it and what progress they've made. They often end with a brief description of the best solution to a known problem or the latest areas of study in the discussed field.

What follows is a selection of the most interesting examples of each of the topics most commonly covered in this collection.

2 Summary

Chapter 1: Calculation and the Chess Master

This article brings a more human element to the battles between the chess grandmaster Kasparov and the chess computer Deep Blue. Rather then focusing on the minutia of how Deep Blue operates, it focuses on how the contests effected both Kasparov and the computer scientists behind Deep Blue. Even if you already know the story of Deep Blue, interesting anecdotes and analyses add new dimensions to the story.

Chapter 4: Computing in a Surreal Realm

This article focuses on the idea of representing some kinds of strategy games as Surreal numbers. It talks about how this kind of surreal number (recursive surreal numbers) can represent a more diverse range of values then commonly believed. This includes numbers " 'bigger' then infinity or 'smaller' then the smallest fraction." The piece's primary goal is

to call attention to the Surreal numbers as an under exposed and under explored area of number theory.

Chapter 8: Mating Games and Lizards

This article talks about similarities between various Rock, Paper, Scissors variants and the mating patterns of a very unusual species of lizard, the Uta Stansburiana. The males of this species come in three distinct variates, each with it's own mating strategy. The article then goes on to describe how these three strategies interact in a very Rock, Paper, Scissors like way, and the effect this has on the species as a whole. It concludes with a mention that a similar process has been observed in some variates of microbe.

Chapter 12: Cracking the Ball Control Myth

This article discusses attempts to dispel a commonly believed myth, that practicing Ball Control will a basket ball team more likely to win. Ball Control is the practice of rather then just trying to score as often as possible, deliberately holding onto the ball to make sure the other team can't use it. Peterson goes into detail about how different groups have used both mathematical and statistical proofs to show that practicing Ball Control does not make a basket ball team more likely to win, and in fact often has the opposite effect. It ends by musing on why this myth is so persistent in the face of all the evidence to the contrary.

Chapter 17: Computing with the EDSAC

This article talks about one of the first general purpose computing machines, the Electronic Delay Storage Automatic Calculator (EDSAC). Peterson talks about how the machine was put together, from the vacuum tubes to the teleprinter. He then talks about Maurice Wilkes, who led the effort to build the EDSAC. Peterson goes into detail as he describes Wilkes's struggle to program back when code was holes in paper tubes. This chapter reminds of that programming used to much harder for mundane reasons.

Chapter 23: Trouble with Wild-Card Poker

This article talks about the surprisingly large difference between standard Poker and it's Wild-Card variant (e.g., the 2 is wild) when the games are subjected to statistical analysis. The most interesting difference noted is that in Wild-Card Poker the best hand cannot be the lest likely, sense being the best hand makes players more likely to use a Wild-Card to construct it. The article ends with the following humorous quotation on the limits of the mathematical analysis of Poker:

"'Three assumptions have been made: that you can bluff without giving any indication, that nobody is cheating, and that the winner actually gets paid. You will not necessarily be well advised to make these assumption in practice.' Some aspects of poker are beyond the reach of mathematics."

3 Opinion

I personally liked this book. It taught me much that I didn't know (I am a sophomore computer science major). For the readers of this column this may be less true; however, I suspect (and Bill Gasarch confirms) that about half of it will be new for about half of you. Many of the chapters give pointers to more sophisticated work which may also be of interest.

So who should read this book? There is something in it for me, for you, and for Bill's great niece who just won an award for being the top math person in her second grade class.

Review of[7] of
Six Sources of Collapse
by Charles R. Hadlock
Published by MAA 2012
187 pages, hardcover

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

1 Introduction

Charles R. Hadlock defines a "collapse" to refer loosely to "some relatively rapid process that leads to a significant reduction in quantity, quality, or level of organization" in his book "Six Sources of Collapse; A Mathematician's Perspective on How Things Can Fall Apart in the Blink of an Eye". Examples of collapses include the disappearance, over a period of 30 years, of the passenger pigeon population from over four billion to zero pigeons. Enron, of course, was a collapse, as was the 1929 stock market crash or the 2005-6 housing bubble.

As a mathematician Hadlock focuses on understanding how and why things go unexpected and catastrophically wrong, and how can we manage the possibility of collapse. Specifically he focuses on six different sources; his list of sources is wide ranging but likely not conclusive.

2 Summary

The book is organized in eight chapters; the first chapter introduces the concept of a collapse, and provides a varied list of collapses lists to consider. The last chapter, written as a conclusion, discusses how to combine the six sources, or frameworks, of collapse.

The most interesting chapters are the six chapters discussing the six sources of collapse. These sources are:

- Low probability events: the probability of relatively rare events occurring is often underestimated using standard statistical methods. Unless the statistical models used to calculate probabilities are designed for calculating extreme values, the resulting probability is usually highly inaccurate.

  A second problem is the assumption of independence of variable, where collapses are due to unanticipated common cause failures.

- Group behavior: independent member of a group, interacting with one another, often result in patterns that vary widely from the patterns of behavior each individual member exhibits. In this chapter he introduces agent-based modeling, where a computer

simulates the behavior of many group members according to relatively simple rules in order to see what happens.

Interesting examples include the flight patterns of flocks of birds, the rate and pattern of infection in a population, and the way democracy might spread in a speculative world. All these examples are modeled using only a very few, simple rules, but the results are intriguing.

- Evolutionary processes: the use of game theory to capture the results of cooperating versus competing. The game playing is iterated, which leads to modeling the evolution of species and cultures.

- Instability: the study stability, instability, and oscillation. These can be captured using dynamical systems described by differential equations, whose behavior can be carefully studied. Specifically, the questions of interest are whether, from a given point, the system converges to a fixed point, diverges to infinity, or stabilizes in some orbit. But as he points out, in some systems starting at slightly different positions can lead to vastly different outcomes. Thus, even if you have an accurate model, your predicted outcome may still be wildly inaccurate if you miscalculated the starting position.

- Nonlinearity: much of calculus is based on the local linear approximation of models, and as humans we tend to assume that most changes – in the stress-strain relationships of steel used to build ships or the linear elasticity of the vertical cables supporting the Tacoma Narrows bridge – are linear. In both cases, the assumption was catastrophically wrong. In the former, the steel became brittle and during the the production of over 5000 ships during World War II, a dozen of these ships broke right in half, including while sitting in port in calm weather. In the latter case, the oscillations of the bridge were so drastic that the vertical cables actually went slack, at which point they no longer functioned as springs, Hooke's law was no longer in effect, and the vertical cables functioned as non-linear spring.

  This chapter also introduces chaos, and the butterfly that creates typhoons half way around the world.

- Networks: any time when agents are connected over a network, the health of the network can affect the ability of the agents to interact. This field, widely studied in computing science – specially graph theory – is introduced here, with particular emphasis on the network flow problems, which ask both how much information can move from one node to another in the network, as well as studying the effects if one or more connections is cut.

Each chapter includes a variety of examples, carefully chosen to illustrate the concepts he is introducing.

3 Opinion

This book is primarily written for a general audience; the author apologizes profusely and in advance whenever there is a hint of mathematical formulae in the offing. Certainly the only theorems presented are not proven but merely used. The format is that of describing concepts using specific examples. Since the book is very short, there are frequent references to cited papers, as well as suggestion to search online for specific programs. In the chapter studying group behavior, the author explicitly expects – or at least hopes that - the reader will find the software he describes online, and experiment with it. As such I actually spent more time diving down proverbial rabbit holes online; the book functioned as an interesting jumping off point, and I believe I spent more time perusing online than I did reading the book.

The illustrating concepts were themselves quite interesting and, when he is not apologizing for approaching math, the author's narration is captivating. The greatest challenge I faced was in trying to extend the concepts; the examples illustrate the concepts quite well, but it is not always clear how much of the example is necessary or sufficient to the concept. Thus, for the examples he provides, I can see how the sources of collapse might plausibly have functioned, but I do not feel comfortable considering new projects and predicting what might go wrong.

Review of[8]
Visions of Infinity: The Great Mathematical Problems
by Ian Stewart
Basic Books, 2013
340 pages, Hardcover

Review by
Aravind Srinivasan, srin@cs.umd.edu
Dept. of Computer Science and UMIACS
University of Maryland, College Park, MD 20742, USA

1 Introduction

This book describes fourteen great mathematical problems: some solved, some yet-unsolved, and some partially solved (such as variants of the three-body problem); it does so in a good amount of detail for the lay reader. However, the mission of this book is broader: how mathematics is an interconnected whole, how solutions to problems borrow from/lead to seemingly very different mathematical areas, and how mathematics serves as a foundation for several other fields. It presents historical context and applications as well, all with a gentle sense of humor.

2 Summary

This book really brings together a vast range of ideas: it must have been a real labor of love for the author to put together such a broad swath in an engaging manner. The book is really too comprehensive to review chapter-by-chapter, and so I will just give a sampling here; I will group the chapters approximately according to mathematical area.

Chapter 1 is generally on "what makes a mathematical problem great". An interesting item here is Poincaré's three-stage theory about the creative process, especially for logic-based fields such as mathematics. The three stages are perhaps obvious: preparation (where we lay the foundations and do active work), incubation (where we step away from the problem and let the subconscious do the work), and the resultant illumination. What is interesting is that as opposed to the sometimes-romanticized view of mathematics as miraculously materializing before the absent-minded genius, Poincaré was adamant about the importance of the prepatory stage. (Terence Tao has expressed a similar opinion about the inaccuracy of this romantic view.)

There are a few chapters on number theory. Chapter 2 contains a fascinating history of the Goldbach conjecture and the odd Goldbach conjecture. Apparently, work on factoring has led to some good progress on this problem – something that I was personally not aware

[8] ©2014

of – and this chapter has a useful discussion on the history of primality testing including the AKS test and factoring, and definitions of our friend P and its complement, "not-P". (P, NP, and exponential time are defined more formally in Chapter 11.) The Green-Tao theorem and the twin-prime conjecture are among the great theorems/problems discussed; the breakthrough progress of Yitang Zhang on the latter came after this book was published.

Chapter 6 is about Diophantine equations and Mordell's conjecture: Andrew Granville and Thomas Tucker describe the context of the latter as "In [1922] Mordell wrote one of the greatest papers in the history of mathematics ... Mordell asked five questions ... The most important and difficult of these questions was answered by Faltings in 1983 by inventing some of the deepest and most powerful ideas in the history of mathematics." Although I am personally skeptical of descriptions such as "one of the greatest papers" (with a full understanding of the fact that my knowledge of mathematical research is small), this gives some indication of the importance of this conjecture. There is a nice description of elliptic curves and their group operation, more of which are seen in Chapter 7. My own, possibly incomplete, understanding of the conjecture after reading this chapter, is as follows. Suppose you have a Diophantine equation which becomes an equation in two variables after allowing the variables to be rational: e.g., the Pythagorean equation becomes $x^2 + y^2 = 1$. My rough understanding about the conjecture is that if there are infinitely-many solutions, then there are only two cases: (a) there is an explicit formula, such as for the Pythagorean triples, or (b) as in the case of elliptic curves, there is a process that constructs new solutions from previous ones – which, in addition, will produce all (and only the) solutions if started off with a suitably-large, finite, set of initial solutions. (As an interesting aside, this chapter also discusses a case with only *finitely many* solutions: Mihailescu's proof in 2002 of the Catalan Conjecture, that the only integral solution to $x^m - y^n = 1$, apart from the obvious ones that use 0 and ± 1, is $3^2 - 2^3 = 1$. This work was also featured in Dick Lipton and Ken Regan's blog.)

Chapter 7 brings us to perhaps the most well-known Diophantine equation – Fermat's Last Theorem – starting with a discussion of Fermat's early years and career in the legal system; a copy of his original marginal note is included! The early history of the problem includes the proof for specific exponents. An interesting quote from this period is: "Sophie Germain, one of the great women mathematicians, divided Fermat's last theorem for a prime power p into two subcases ... Germain corresponded with Gauss, at first using a masculine pseudonym, and he was very impressed by her originality. When she revealed she was a woman, he was even more impressed, and said so. Unlike many of his contemporaries, Gauss did not assume that women were incapable of high intellectual achievement, in particular mathematical research." (The "even more impressed" may sound gratuitous, but perhaps what the author means is that Gauss was very impressed with someone who probably had to work with little encouragement owing to her gender.) This period was followed by the introduction of complex-analytic attacks on the problem, unique factorization (and the lack thereof), Kummer and Dedekind's work on ideal numbers, and the taking off of algebraic number theory. Evidence toward the proof of the theorem was mounting by the middle of the 20^{th} century. We then get a tour of elliptic curves, the Taniyama-Shimura conjecture, the

tragic events in Taniyama's life, the Langlands program, and the work of mathematicians including Frey, Serre, and Ribet. This is followed by a brief biography of Wiles, and the events leading to the proofs of Wiles and Wiles-Taylor. This chapter is a vivid telling of a major problem that led to breakthroughs in different fields. Further Diophantine equations and the Birch-Swinnerton-Dyer Conjecture are considered in Chapter 14.

The Riemann hypothesis occupies Chapter 9. Many readers of SIGACT News are perhaps familiar with the hypothesis, Miller's result that the generalized RH yields a deterministic polynomial-time algorithm for factoring, and Euler's formula that relates the zeta function to the primes: letting p_i be the i^{th} prime, this formula is that for any integer $s \geq 2$,

$$\prod_{i=1}^{\infty}(1-p_i^{-s})^{-1} = \zeta(s) \doteq \sum_{i=1}^{\infty}\frac{1}{i^s}.$$

(To see this, just observe that $(1-p^{-s})^{-1} = \sum_{j=0}^{\infty} p^{-js}$.) This was soon extended to all complex s with real part more than 1 and to a very precise formula due to Riemann. Riemann's famous conjecture, the Riemann hypothesis, is that if we consider the analytic continuation of $\zeta(s)$ to all of the complex plane excluding $s = 1$, then the only "nontrivial" zeros of $\zeta(s)$ have real part equaling $1/2$, i.e., lie on the "critical line". Riemann's above-mentioned "very precise" formula shows, in particular, that the Prime Number Theorem (that the number of primes up to x, $\pi(x)$, is asymptotic to $x/\ln x$) holds if all nontrivial zeros of the zeta function $\zeta(s)$ lie in the critical strip – the complex numbers with real part in $(0, 1)$. Proving that all the roots lie in the critical strip is how the original proof of the PNT due to Hadamard and de la Vallée Poussin went; more elementary proofs were later found by Erdős-Selberg, and by Newman. This chapter also discusses Dirichlet's result about primes in arithmetic progressions, the generalized Riemann hypothesis, and Deligne's resolution of generalizations to varieties over finite fields. Returning to the RH, it is now known that more than 10^{13} of the initial zeros of the RH lie on the critical line. Is this not overwhelming evidence? To counter this reasonable guess, this chapter discusses Littlewood's famous result that $\pi(x) - Li(x)$, where $Li(x) \doteq \int_0^x \mathrm{d}t/\ln t$ is an excellent approximation to $\pi(x)$, changes sign infinitely often – and the fact that this necessarily starts happening only for astronomically large x. The chapter closes with deep connections to mathematical physics and with an introduction to the Clay Millennium problems and the Abel Prize.

Speaking of physics, Chapter 8 discusses the three-body problem, leading to the question of whether the solar system, for instance, will remain stable; Chapter 12 is on the Navier-Stokes equation. Chapter 13 is on the *Mass Gap Hypothesis*, and as with the rest of the book, the author uses this opportunity to talk about a variety of related areas, this time from the fundamental advances in physics starting from the late 19^{th} century, quantum field theory etc.

Chapter 3 is on the long journey to the impossibility of "squaring the circle", i.e., constructing, using ruler and compass, a square with the same area as a given circle. The history is fascinating: Gauss' proof that a regular 17-gon can be constructed and how to generalize the "17", the transcendence of e, and finally the transcendence of π, leading to the proof. This chapter shows a glimpse of the wonderful interplay of geometry, algebra, and

analysis, and has a nice introduction to the complex plane for the lay reader. Chapter 10, the longest one in the book, is on the Poincaré Conjecture and Thurston's Geometrization Conjecture. It has detailed discussions on basic topology with figures, along with plenty of history. Perelman's contributions, the backdrop to them, and his reaction to his awards follow. This chapter is remarkable for its attempt to present frontier research to the lay – but motivated – reader, through a variety of pictures and details.

There are three chapters that have connections to computation. Chapter 4 is on the four-color theorem. Its history starts with Francis Guthrie, whose brother was a student of de Morgan. (Part of this early history includes a pun of Hamilton's in response to de Morgan's letter on this: 'I am unlikely to attempt your "quaternion" of colors very soon'. Readers may be aware that Hamilton invented (discovered?) the quaternions, which, however, did not achieve the heights that Hamilton had hoped for. Funnily enough, there have been reformulations of the four-color problem in the last 25 years due to Louis Kauffman, which can be viewed as assertions about the quaternions!) It then continues with Möbius, Cayley et al., and failed attempts to solve the problem. The description covers induction, minimal counterexamples, and the 6-color theorem. A good deal of attention is then given to Appel and Haken's work and its implications for mathematics, as well as the more modern work of Robertson, Sanders, Seymour, and Thomas. Chapter 5 then deals with Kepler's sphere-packing conjectures, and the cases of lattice – periodic – packings (easier) and general packings (harder). Again, several pictures that give some good insights are included. After being presented many partial results, we are led to Thomas Hales' computer-assisted proof, and Hales' current project to develop a formal (very long) computer-verified proof. Chapter 11 is on the P vs. NP problem, and includes a discussion of why NP is different from problems that require exponential time for obvious reasons. This chapter will probably be considered a good introduction to the layperson, by most SIGACT News readers.

Chapter 15 is on the Hodge Conjecture, which the author introduces, in contrast with most mathematical topics, as "defy[ing] all of these methods for making difficult abstract concepts accessible". Finally, there are two interesting chapters on what may come next (e.g., the outlook for the open problems, how and when they may be resolved), and twelve additional concrete problems for the future. The glossary, notes, index, and pointers for further reading are very comprehensive.

There is a little room for improvement in a few places, e.g., with the claim in page 213 that there are more than 300 mathematical NP-complete problems: this number can be made much bigger, of course.

3 Opinion

This book would interest any reader with curiosity about (the frontiers of) mathematics. In particular, readers with relatively less mathematical training, but with enthusiasm in putting in the effort to read the book, as well as its glossary and copious notes, would find the effort worthwhile. The typical SIGACT News reader will probably find the book quite interesting. Indeed, Ian Stewart's enthusiasm for mathematical exposition is apparent from the range of

books he has written.

Why can't this book be replaced by separate study of each of the problems introduced in, say, Wikipedia? This book gives an integrated look at the problems discussed, with detailed discussion of history, personalities, and above all, mathematical links. This makes the book valuable in my opinion, to a general readership interested in mathematics.

Review of[9]
The Satisfiability Problem: Algorithms and Analyses
by Uwe Schöning and Jacobo Torán
Lehmanns, 2013
180 pages, Softcover, $29.00

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

1 Introduction

As the readers of this column already know, SAT is an NP-complete problem. Indeed, SAT is *the first* NP-complete problem. Doing research on the difficulty of SAT comes in several flavors:

1. Lets build SAT solvers that work well, though perhaps we do not know why they work well. They will use shortcuts and heuristics.

2. Lets devise SAT algorithms that we can prove work well, perhaps an algorithm for 3-SAT that works in c^n steps where $c < 2$. These may be inspired by, or inspire, the algorithms used for real SAT-solvers.

3. Lets try to prove that SAT is hard. For example, that there are poly sized formulas with exponentially long resolution proofs.

This book is mostly concerned with item 2- algorithms for SAT that you can actually analyze. However, there is one chapter on resolution lower bounds and one chapter on using methods of Physics to solve SAT. There are also some sections on real world SAT solvers.

At the University of Maryland we currently do not teach SAT algorithms in the algorithms course. This wonderful book may change that as it lays out clearly some simple (and some complicated) algorithms for 3-SAT (and k-SAT) that take time c^n for $c < 2$. Students already learn about approximation algorithms and FPT algorithms to get around NP-completeness; however exponential-but-not-too-bad should also be taught.

2 Summary

Chapter 1 introduces the problem and defines terms that will be used later. It also contains some interesting tidbits that the reader might not know: Tsetin's method for $SAT \leq 3\text{-}SAT$ (note that the right hand side is SAT not CNF-SAT), using the Local Lovasz Lemma to prove a formula is satisfiable, and Craig Interpolants.

[9] ©2014, William Gasarch

Chapter 2 gives a self-contained (including definition) account of resolution theorem proving and the classic theorem that any resolution proof to show that NOT(PHP_n) (negation of the Pigeonhole Principle) requires exponential size. They present a variant of a proof by Buss and Pitassi. This is a wise choice as it is a pedagogical improvement on the original proof of Haken.

Chapter 3 gives algorithms for easy cases of SAT such as 2-SAT. This is important since, in more complicated algorithms, if a subcase is 2-SAT or some other easy instance, you need to use these algorithms.

Chapter 4 gives the classic DPLL (Davis-Putnam-Logemann-Loveland) algorithm. This is a very general algorithm on which one can try many heuristics. We present it here:
DPLL(F) (F is a set of clauses. The goal is to determine if there is an assignment that satisfies all of them)

1. If $\emptyset \in F$ then return NO. (The empty clause cannot be satisfied.)
2. If $F = \emptyset$ then return YES. (There are no clauses that need satisfying.)
3. If there is a unit clause $\{u\}$ (so u is the only literal in the clause) then return $DPLL(F\{u = 1\})$. This is because u must be set to true to make that clause true.
4. If there is a pure literal (a literal u where $\neg u$ never appears) u then return $DPLL(F\{u = 1\})$. This is because there is no reason not to set u to true since it can only help.
5. Cleverly choose some variable x. If $DPLL(F\{x = 0\}$ returns TRUE then return 1, else return $DPLL(F\{x = 1\}$.

That last line leaves lots of room for innovation. There are many algorithms that use this framework, or variants where you choose several variables. This chapter goes through many such variants including the best algorithm for k-SAT, the Paturi-Pudlak-Zane algorithm which solves k-SAT in $O^*(2^{n(1-1/k)})$ (O^* means we ignore polynomial factors.)

Chapter 5 discusses local search algorithms. In such algorithms there is a measure of how close a partial assignment is to satisfying the formula and you make local progress increasing that measure. One algorithm uses a covering code of $\{0,1\}^n$. For this one a randomized approach is best.

Chapter 6 discusses more algorithms without a unifying theme. Of particular interest are (1) Stalmarck's algorithm since it is used in industrial applications, and (2) SAT algorithms for OBBD's (Oblivious Binary Decision Diagrams) since they are also more real world than (say) 3-SAT.

Chapter 7 discusses work that connects Physics to SAT algorithms and Chapter 8 discusses Heavy Tails and some randomized algorithms. Neither chapter has theorems as they are dealing with heuristic methods. Chapter 9 is a final discussion which also includes some comments are real world SAT solvers.

There are many appendices that serve to make the book self contained.

3 Opinion

This is a great book that fills a gap in the literature. There has been much progress on SAT algorithms of varying levels of difficulties. It is good to have it all in one place. The book is well written and covers what you want to know.