The Book Review Column[1]

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

In this column we review the following books.

1. **Blown to Bits: Your Life, Liberty, and Happiness after the Digital Explosion** by Hal Abelson, Ken Ledeen, and Harry Lewis. Review by Bill Gasarch. You've all heard vague stories about record companies suing 12 years olds for downloading music (if not then download from You-Tube Weird Al's classic song *Don't Download this Song*). Whats really going on? How are technological changes affecting our lives? To find out read this book. Or at least my review of this book.

2. **Solving polynomial equation systems II: Macaulay's paradigm and Gröbner technology** by Teo Mora. Review by S. C. Coutinho. Solving polynomial equations is a classic (read: old) field of math. However, it has been reborn with the advent of computers. This book guides you through both the classic theory and the modern computational viewpoint. Grobner basis are prominent.

3. **How To Prove It: A Structured Approach** by Daniel J. Velleman. Review by Brent Smith. This is a guide for students who have had calculus (though its not needed) on how to prove things. The usual topics are there: induction, relations, functions, etc. Note that at $30.00 its considerably cheaper than your usual Discrete Math book.

4. **Practical Optimization: Algorithms and Engineering Applications** by Andreas Antoniou and Wu–Sheng Lu. Review by Brian Borchers. This is a rather practical book on optimization that tells students how to optimize and has lots of examples. The target is EE students.

5. **Rock, Paper, Scissors: Game Theory for Everyday Life** by Len Fisher. Review by William Gasarch. This is a book on Game Theory for the layperson. There are more examples, more real world ways around the problems raised, and less mathematics than in a usual Game Theory book.

We are looking for reviewers of the following books

Books I want Reviewed

If you want a FREE copy of one of these books in exchange for a review, then email me at gasarchcs.umd.edu

Reviews need to be in LaTeX, LaTeX2e, or Plaintext.

Books on Algorithms and Data Structures

1. *The Algorithms Design Manual* by Skiena.
2. *Algorithms on Strings* by Crochemore, Hancart, and Lecroq.
3. *Algorithms for Statistical Signal Processing* by Proakis, Rader, Ling, Nikias, Moonen, Proudler.
4. *Nonlinear Integer Programming* by Li and Sun.
5. *Binary Quadratic Forms: An Algorithmic Approach* by Buchmann and Vollmer.
6. *Geometric Folding Algorithms: Linkages, Origami, Polyhedra* by Demaine and O'Rourke
7. *Algorithmic Number Theory: Lattices, Number Fields, Curves, Cryptography* by Buhler and Stevenhagen.
8. *Time Dependent Scheduling* by Gawiejnowicz.
9. *The Burrows-Wheeler Transform: Data Compression, Suffix Arrays, and Pattern Matching* by Adjeroh, Bell, Mukherjee.

Books on Cryptography, Coding Theory

1. *Concurrent Zero-Knowledge* by Alon Rosen.
2. *Introduction to cryptography: Principles and Applications* by Delfs and Knebl.
3. *Primality Testing and Integer Factorization in Public-Key Cryptography* by Yan
4. *Secure Key Establishment* by Choo.
5. *Codes: An Introduction to Information Communication and Cryptography*
6. *Algebraic Function Fields and Codes* by Stichtenoth.
7. *Coding for Data and Computer Communications* by David Salomon.
8. *Block Error-Correcting Codes: A Computational Primer* by Xambo-Descamps.

Books on Theory of Computation

1. *A Second Course in Formal Languages and Automata Theory* by Shalitt.
2. *A Conscise Introduction to Languages and Machines* by Parkes

3. *The Calculus of Computation: Decision Procedures with Applications to Verification* by Bradley and Manna.

4. *The Annotated Turing: A Guided Tour through Alan Turing's Historic Paper on Computability and the Turing Machine* by Perzold.

5. *Computability of the Julia Sets* by Braverman and Yampolsky.

Misc Books

1. *A Course in Enumeration* by Aigner.

2. *Difference Equations: From Rabbits to Chaos* by Cull, Flahive, and Robson.

3. *Random Graphs* by Bollobas.

4. *Mathematical Tools for Data Mining* by Simovici and Djeraba.

5. *The Modern Algebra of Information Retrieval* by Dominich.

6. *A Concise introduction to Data Compression* by Salomon.

Review of

Blown to Bits: Your Life, Liberty, and Happiness after the Digital Explosion[2]

Author: Hal Abelson, Ken Ledeen, and Harry Lewis

Publisher: Addison Wesley, 2008

$25.95, 366 pages, Softcover

Reviewer: William Gasarch (gasarch@cs.umd.edu)

1 Disclosure

Harry Lewis, one of the authors of the book under review, was my adviser.

2 Overview

The Music industry has the following valid complaint:

People who download music illegally are ripping off the artists! That's an outrage! That's our job!

The book under review is about the changes to society caused by the electronic age. My impression is that they started out wanting to do an intelligent and unbiased view, and that they

[2] © William Gasarch, 2009

succeeded. However business look immoral and the government looks incompetent. As Stephan Colbert might say *The truth has an anti-business agenda*.

The book is not just about business and government. Its about virtually all aspects of the electronic age. Much of what the book says is obvious *once you see it written down* but not obvious before that point. This is quite valuable. Will this book become out of date as technology changes? There are two answers: (1) NO, and (2) HELL NO- they have a blog associated to the book that has updated material: www.bitbooks.com.

Note that the website associated to the book also has an errata sheet.

3 Summary of Contents

3.1 Chapter 1: Digital Explosion—Why is it happening and what is at Stake?

The first chapter drives home the point that the world really has changed. It states 7 Koans about the modern world which are obvious once they are stated, but worth stating. I give one example:

Koan 5: More of the same can be a whole new thing.

This means that even though computers, to some extent, do what we used to do only faster, this is still very new. Compare looking up information in a library to on a computer. Same activity, yet very very different.

The first chapter also emphasizes that technology is not good or bad, its how you use it. Again, this is obvious but needs to be stated. This book is not an anti-technology tract by any means. But it is a sequence of true cautionary tales.

3.2 Chapter 2: Naked in the Sunlight—Privacy Lost, Privacy Abandoned

Twenty years ago the biggest threat to privacy was the government. Phone taping, cameras everywhere, etc. While this is still a problem (e.g., intercepting emails) two unexpected things happened: (1) people give up their privacy too easily, and in the process may give up yours, and (2) little brother is watching. Not big brother, little brother.

Who is little brother? Its you! And me! And anyone who has a cell phone camera or Internet connection. It seems that anyone can look up and find out anything. The notion of *sealed records* is now a joke. This works both ways— people can find out things about government and companies.

This chapter describes how we got here: not by some nefarious plan but by the slow erosion of privacy laws, the fast evolution of technology, and people's willingness to trade information about themselves for convenience. This chapter does not say what we can do about it. Its not clear we can do anything about it.

3.3 Chapter 3: Ghosts in the Machine—Secrets and Surprised of Electronic Documents

When I email a pdf file or word document I am emailing more information than I think. Material I blocked out, material from earlier versions, may well be hidden there. And if someone wanted to they can find that information. This could be a problem for national security and privacy.

There is so much hidden in what we send that we may not realize how much we are giving away. This happened in a more concrete setting recently. In the blog associated to the book I read the following:

... the McCain-Palin campaign was much less clued in on how to use the technologies [than the Obama-Biden campaign]. And the evidence for this continues to accumulate after the campaign is over. The campaign auctioned its Blackberry phones without wiping the memory clean— so those who bought them bought phone numbers of donors, lobbyists, and journalists too. Apparently they were not amused when the purchaser called them up.

3.4 Chapter 4: Needles in the Haystack—Google and other Brokers in the Bit Bazaar

Searching the web is a complicated phenomenon. It has changed everything. And there are still issues to work out with it. For the user this is great— we can actually find anything we want. In fact, we are spoiled! I was disappointed I could not find a translation into English of Hilbert's article *Uber die irreduzibilitat ganzer reationaler funktionen mit ganzahigen keffizienten* from *J. Reine Angew. Math* which appeared in 1892, volume 110, pages 104-129. I couldn't even find a copy in German! I had to go to a non-digital *library* and use a *photocopy machine* (if you don't know what these terms mean then ask your grandfather).

But there are issues. Some sites have advertisers pay to be ranked higher (goto.com). Google does not do this which is part of its popularity. However, google's own pagerank system may (unintentionally) discriminate. There have been lawsuits about this (KinderStart v. Google). There have also been lawsuits in the other direction— suing because Google copies their index (Field v. Google). Google has also blacklisted companies that try to game the system. Its a constant game of cat-and-mouse.

More troublesome is that if you search for something then somewhere somehow there is a record of it. This may come back to haunt you.

3.5 Chapter 5: Secret Bits—How Codes become Unbreakable

The good news: with modern crypto we can have privacy. The bad news: few people use it, and there are ways around it. This chapter details all of this, plus a discussion of the Clipper Chip Controversy. It was good to see the whole story told.

3.6 Chapter 6: Balance Toppled—Who Owns the Bits?

Now that everything is online and we have perfect copies (Koan 2: Perfection is Normal) books, journal articles, music, movies, information, is all free. Neither Business, government, nor the legal system has adjusted to this yet.

You've probably all heard stories about 12-year olds being prosecuted for downloading music. Its worse than you think. The music companies have not only gone after people who have downloaded music. They have also gone after people who are involved in a secondary way, and even some who have not connection to downloading whatsoever.

While companies have acted terribly (and perhaps counter productively as their claims to be 'protecting the artists rights' seem more and more spurious) the law has been mixed. The legal system is not designed to handle fast changing technologies.

Do the music companies have a legitimate complaint? And what can they or the law do that is fair to all parties concerned. The book *Wikinomics* would say that they need to find a new business

model. Services like itunes may be a step in the right direction; however, it may be too little too late.

This chapter details this entire story accurately. The story goes back further than most people think: there were lawsuits about VCR's that foreshadow lawsuits about Napster and other services (I wonder if painters sued photographers who took pictures of their paintings and sold them). Even though the book is written factually (unbiased), the companies look awful and the Government looks incompetent.

3.7 Chapter 7: You Can't Say That on the Internet: Guarding the Frontiers of Digital Expression

The title of the chapter makes you think of censorship. However, the issue of this chapter is far more complicated. Lets say an adult male uses FACEBOOK to arrange a meeting with an underage female for immoral purposes. Should FACEBOOK be liable? Who is responsible?

This chapter gives a nice history of what has happened here, Much like the last chapter, some of the laws being debated here have been looked at before in other contexts. It is good to know those contexts.

3.8 Chapter 8: Bits in the Air—Old Metaphors, New Technologies, and Free Speech

At one time the radio spectrum needed the government to referee it so that stations would not interfere with each other. This is no longer true. Yet our laws still operate as though it is true and entrenched interests are resistant to change. This chapter tells that story. And more.

4 Opinion

The one word that describes this book is *intelligent*. For every issue they give history, context, relevancy, and current status. If this ends up making certain people or organizations look bad, that's fine.

Who should read this book? People who technology affects should read this book. Who should not read this book: $\emptyset$.

The book is available for download at www.bitsbooks.com. I asked Harry Lewis what their business model was. He says that printing it out is more expensive than buying it, and the fact that its online will create buzz. That's an alternative business model that may work.

Review[3] of

Solving polynomial equation systems II: Macaulay's paradigm and Gröbner technology

Author of Book: Teo Mora

Cambridge University Press (2005), 759 pages

ISBN 0–521–81156–2, Price $150.00 new[4]

Review by S. C. Coutinho collier@impa.br[5]

1 Introduction to the area

One of the most important areas of algebra for most of the 19th century was the theory of algebraic invariants. Take a group acting on a polynomial ring with n variables over a field. The polynomials that are fixed points for this action form another ring, called its *ring of invariants*. The best known example is given by the symmetric group on n symbols acting on the ring of polynomials by permuting the n variables $x_1, \ldots, x_n$. In this case, a polynomial is fixed by the action if it remains unchanged under any permutation of its variables. In other words, the fixed points are the *symmetric polynomials*. Moreover, it is known at least since the 17th century that every symmetric polynomial can be written in terms of a finite set of so-called *elementary symmetric polynomials*. For $n = 3$, this set consists of only three polynomials,

$$x_1 + x_2 + x_3, \quad x_1x_2 + x_1x_3 + x_2x_3, \quad \text{and} \quad x_1x_2x_3.$$

In the terminology of 19th century invariant theory, such a set was called a "finite basis" of the ring of invariants.

In 1868, Paul Gordan proved that the ring of invariants (of a linear group) always has a "finite basis" when $n = 2$. This led to the *base problem*, which consisted in extending Gordan's result to $n > 2$, and became one of the key problems in invariant theory at the time. Despite a number of advances, some by Gordan himself, the problem remained unsolved, even for $n = 3$, for the next twenty years.

The turning point came in 1888 when David Hilbert proved the basis theorem in full generality. As it often happens in such cases, Hilbert's proof represented a complete break with the previous methods of invariant theory. Indeed, up till then, to prove the existence of a finite basis mathematicians would describe a method that could be used to compute it. Not so Hilbert; his proof was purely existential, and could not be turned into an algorithm for computing the required basis. The impact was immediate, and led Gordan to declare "This is not mathematics; it is theology".

Hilbert's proof of the basis problem shifted the emphasis from constructive to existential methods, and pushed algebra in the direction of greater abstraction, a trend that lasted for most of the 20th century. Some mathematicians even made a conscious effort to avoid constructive arguments in their proofs. Thus, we read in a footnote of André Weil's influential *Foundations of algebraic geometry* (published in 1946) that this book would "finally eliminate ... the last traces of elimination theory" – elimination theory being one of the oldest constructive methods in algebraic geometry. However, as so often happens, the tide would eventually turn. This time what tipped the balance was a machine, the computer.

[3]

[4] amazon.com lists it used at around $30.00

[5] Address: Departamento de Ciência da Computação, Instituto de Matemática, Universidade Federal do Rio de Janeiro, P.O. Box 68530, 21945-970 Rio de Janeiro, RJ, Brazil

At this point we must take a break from the history to introduce some definitions. Let A be the polynomial ring in the variables $x_1, \ldots, x_n$, with coefficients in a field K. Assuming that $x_1 < \cdots < x_s$ we may order the monomials in these n variables lexicographically. This allows us to define the *leading monomial* of a given polynomial f as the largest monomial that appears in f with nonzero coefficient.

Now, the ideal I, generated by the polynomials $g_1, \ldots, g_s \in A$ is the set of all polynomials of the form $f_1 g_1 + \cdots + f_s g_s$, where $f_1, \ldots, f_s \in A$. Using the concepts introduced in the last paragraph, we may define $\mathbf{T}(I)$, the ideal generated by the leading monomials of *all* the polynomials in I. Since $\mathbf{T}(I)$ is generated by monomials one would expect it to be more amenable to calculations than I itself: but what is $\mathbf{T}(I)$ good for? It turns out that this new ideal retains many of the properties of I. For example, we may use it to determine the dimension of the residue class ring A/I and to compute its Hilbert function, which explains why this technique is so useful in commutative algebra and algebraic geometry.

So far, so good; but how do we compute $\mathbf{T}(I)$? After all, I is an infinite set, so the definition we gave above is in fact an infinite process. One's first thought might be that the leading monomials of the gs (the generators of I) should generate the whole of $\mathbf{T}(I)$. Unfortunately, that is not always true. The reason for that is easy to explain. When we consider leading monomials, we disregard all smaller terms. However, it may be possible to cancel the leading monomials of two different gs, thereby creating a new element of I whose leading monomial belongs to $\mathbf{T}(I)$, but that cannot be written in term of the leading monomials of the gs.

Let us resume the history at the moment Bruno Buchberger entered the scene. In his PhD thesis, written in 1965, he showed that every ideal I of A admits a set of generators whose leading coefficients are enough to generate all of $\mathbf{T}(I)$. He called such a set a *Gröbner basis*, after his thesis supervisor W. Gröbner. Moreover, Buchberger introduced an algorithm that allows one to compute a Gröbner basis for any given ideal of I. The key idea is the use of the so-called *S-polynomials*, which give the most economical way of cancelling the leading terms between two given polynomials of I.

Although Buchberger's method is a true algorithm, it is too complicated to do by hand for all, but the simplest examples. So, it is not really surprising to find that by 1970, when Buchberger published his thesis, he had already programmed the algorithm (in a ZUSE Z23V computer). From then on, the ideas introduced by Buchberger have snowballed, especially after the introduction of the personal computer. Indeed, the method of Gröbner basis, and its manifold applications, are now part of most general computer algebra systems, including AXIOM, MAXIMA, MAPLE and MATHEMATICA, to mention only the better known general purpose systems.

The main application of Buchberger's algorithm is in the solution of nonlinear polynomial systems. For example, let $g_1, \ldots, g_s \in A$, and assume that we want to solve the nonlinear system

$$S: \quad g_1 = \cdots = g_s = 0,$$

in $\mathbb{C}^n$. Since the solution set is the same, for any two polynomial systems that generate the same ideal of A, we may replace S by a system G, whose polynomials form a Gröbner basis of I–the ideal generated by the gs. Now, if S has a finite number of solutions in $\mathbb{C}^n$, then the first n polynomials of the Gröbner basis of I (with respect to the lexicographical order) are in "echelon" form. More precisely, the first polynomial contains only the variable x_1, the second polynomial is of the form $x_2^m - h(x_1, x_2)$, for a polynomial h of degree smaller than m in x_2, and so on. Such a system may be solved very easily: all we need to do is compute roots of one variable polynomials at each step.

2 Review of the book

The book under review gives a systematic account of the method introduced by Buchberger – the Gröbner technology of the subtitle – including a large number of later developments, some of which are based on results discovered long before 1965. These earlier results are related to *Macaulay's paradigm*, which Mora defines to be the reduction of "computational problems for ideals to the corresponding combinatorial problems over monomials". By the way, Francis Macaulay (1862-1937) was a teacher of mathematics at St Paul's School (London), and although he became a Fellow of the Royal Society in 1928, he never held a university position.

Although this book is the second of a trilogy (of which part III has still not been published), it is mostly self-contained, and readers with some experience in the area will have no difficulty reading it even if they do not have access to the first volume [1]. This also explains why the book begins in chapter 20 of part three. The elementary theory of Gröbner bases is developed in the seven chapters of this first part, which include the definition of Gröbner bases and Buchberger's algorithm (chapter 22), the computation of the Hilbert function of an ideal (chapter 23), besides several improvements and generalizations of the basic algorithm.

A key theme of part four is the study of the linear equations that must be satisfied by the coefficients of a polynomial if it is to belong to a given ideal. This leads one to work with the vector space of linear functionals over a polynomial ring; which explains why this part is simply called "duality". Actually, part four begins with a number of basic results on noetherian rings (chapter 27) and includes (chapter 29) a description of the FGLM algorithm (named after Faugère, Gianni, Lazard, and Mora) that allows one to compute the Gröbner basis under the lexicographical order (which is very useful in many applications, but is slow to compute) directly from a Gröbner basis under a degree order (which can be done very much faster), when the residue ring is finite dimensional. Finally, part V takes us to dimensions greater than zero, and includes an algorithm for the primary decomposition of an ideal (chapter 35).

One question that we have not touched yet concerns the complexity of the Buchberger algorithm. Let I be an ideal of a polynomial ring in n variables over a field, and let γ be the largest degree of a polynomial in a given Gröbner basis G of I. It is easy to show (p. 107) that all polynomials that appear in the computation of G have degree smaller than γ^{4n}. This may not look so bad, but remember that it assumes that the basis G has already been computed, which is clearly unsatisfactory. What we really want is a bound in terms of the maximal degree δ of the polynomials of the generating set of I that was used in computing G. For that, it is enough to find an upper bound for γ. The evaluation of this bound is discussed in chapter 35, where it is shown that (under some extra hypotheses)

$$\gamma \leq (\delta + 1)^{(n-d)2^d},$$

where d is the dimension of I. In other words, the only 'general' bound known for γ is a double-exponential. Despite that, computers are fast enough nowadays to make these algorithms very useful in many applications.

3 Opinion

To be honest, this does not by any means do justice to this long and carefully crafted book. Just to give an example concerning the most elementary topics, it takes almost 100 pages to get to the

Buchberger algorithm. Before that, we are led through the relation between ideals and varieties (affine and projective), Hilbert's Nullstellensatz, Hilbert's function, and proofs of the base theorem by Hilbert and Gordan (chapter 20). Next (chapter 21) comes a study of Gaussian reduction for, as the author points out, Gröbner bases can be described "as a finite model of an infinite linear Gauss-reduction basis of an ideal viewed as a vectorspace" (p. 46). Moreover, this is used to link Gröbner bases to the duality that is described in part IV. Finally, we come to the definition of Gröbner bases, at the very beginning of chapter 22. The Buchberger algorithm itself will only be introduced 24 pages further on.

As one might expect, these characteristics also mean that this is not the best starting place for a beginner who wants to learn about Gröbner bases. For that, it would be preferable to use a book that goes straight to the point, and that also includes at least some of the applications of the theory, both inside and outside algebra. Although such applications are legion, ranging from automatic proof of theorems to robotics, only those related to commutative algebra and algebraic geometry are mentioned in this book. However, if you are already conversant with the basics of Gröbner technology, I can think of no better place where you can learn the full details of the algorithms, their generalizations, and the first applications to commutative algebra.

I have to admit that I fell in love with this book at first sight; for it is not just extremely well organized, it is also written in a style that is a joy to read. Unlike many mathematics books, which seem to be written by an omniscient author that is forever hiding his real persona, Mora shows up every so often to tell us what he thinks. Among the many side comments, I will repeat here one of my favourites, just to give you an idea of what I mean. The context is a criterion used to stop Buchberger's algorithm. Having established on p. 78 what it means for a polynomial to have a *Gröbner representation* with respect to a certain Gröbner basis, Mora defines on p. 96 a *weak Gröbner representation* of an S-polynomial, which is a key ingredient of Buchberger's algorithm. On the difference between the two representations, he has this to say (p. 96):

> The reader should keep in mind that *true* weak Gröbner representations do not exist: they are just a fiction; as with unicorns, I cannot provide a single example of a weak Gröbner representation that is not itself a Gröbner representation.

Of course, like all things human, this book has its share of minor flaws. Take the index, for instance: it is only two pages long, against the 759 pages of the book itself. This is difficult to understand. After all the book is published as part of the *Encyclopedia of Mathematics and its Applications*; so it is meant to be a reference book. Moreover, the lack of a proper index will certainly make the book less useful as a quick source of reference, which is really a pity. Luckily, the table of contents is quite detailed, and make up somewhat for the lack of a proper index.

To sum up, this is a wonderful book, beautifully written and produced, that should be in every mathematical library. Actually, if you are a serious user of Gröbner bases you will probably wish to have your own copy of the book, which, I bet, will soon be very well thumbed.

References

[1] Teo Mora, *Solving Polynomial Equation Systems I: The Kronecker-Duval Philosophy*, Encyclopedia of Mathematics and its Applications (No. 88), Cambridge University Press, Cambridge (2003).

Review of [6]

How To Prove It: A Structured Approach, Second Edition
Author of Book: Daniel J. Velleman
Cambridge University Press, 2006, 383 pages
$30.00 new, $20.00 used (on amazon.com)
Review written by Brent Smith

1 Introduction

This book is intended for use by undergraduate students transitioning from computational mathematics like calculus and differential equations to advanced proof-based mathematics. It first presents set theory, propositional logic, and predicate logic as foundational material to prepare the student for writing proofs. The heart of the book is the proof strategies, presented in chapter 3. The remainder of the book uses these proof strategies to prove theorems from discrete mathematics topics like functions, relations, and recursion.

How To Prove It is a well-written introduction to proving theorems in discrete mathematics. The writing is smooth and flows along nicely. There are many examples, and many problems have complete solutions in the back, making this a good book for students in a formal class and for the self-learner who is simply interested in learning about mathematics. At 384 pages (including the appendixes and index) this is a book that can be completed in a reasonable amount of time. With a list price of $29.99 for the paperback version, this is a book that is affordable for the average undergraduate student or for the overworked and underpaid programmer.

Velleman argues that writing proofs is similar to structured programming. In structured programming the programmer combines abstract building blocks like functions, if-statements and while-loops, both sequentially and through nesting to form the final product - "a program that works correctly." In the same way, proofs can be constructed by combining, through sequencing and nesting, basic building blocks like the "suppose-until" structure and the "for arbitrary x prove" structure. The ultimate goal of this book is to "teach students how to design and write mathematical proofs by spelling out the underlying principles involved in the construction of proofs."

2 Chapter by chapter summary

Chapter 1 is a basic introduction to propositional logic and sets. The goal is to start building the framework to teach and practice writing proofs starting in Chapter 3. Chapter 1 includes all the necessary topics - statements, well-formed formulas, truth tables, equivalences, contradictions, tautologies, conditionals, bi-conditionals, sets, and operations on sets. Lots of examples and exercises with answers guide the reader through the material.

Chapter 2 presents the basics of predicate logic, adding quantifiers ("there exists" and "for all") to the framework begun in Chapter 1. Some additional material on sets is also included.

Chapter 3 is the heart of the book and the longest chapter. This is where the proof strategies are presented. The chapter begins with a justification for why mathematicians insist on proofs, saying that "[Mathematicians] are generally not convinced that an answer is correct unless you can prove it." While discussing the process of proof writing, Velleman continues to guide the reader

[6]

gently into the world of proof writing by connecting it to familiar examples such as working a jigsaw puzzle.

Now we come to the strategies themselves. Strategy I states "To prove a conclusion of the form $P \rightarrow Q$, assume P is true, and then prove Q". This is followed by two examples. The first is worked out in detail including a "scratch work" section that demonstrates some of the beginning thought processes like how to split the statement into "givens" and "goals". The second example is a tighter finished proof, followed by a detailed explanation.

The chapter continues with the remaining proof strategies, each followed by examples. There are also several sets of exercises within this chapter, each with solved problems. All the proof techniques are summarized at the back of the book.

Chapters 4, 5, 6, and 7 continue to present discrete mathematics concepts, while guiding the student in using the proof strategies of chapter 3.

Chapter 4 covers relations, including closures, equivalences, and ordering.

Chapter 5 covers functions, including one-to-one, onto, and inverse functions. At the end of this chapter is a "research project in which you will discover for yourself the answers to basic mathematical questions about images and inverse images". This is an extended example and exercise intended to give the student a chance to "put your proof-writing skills to work in answering mathematical questions."

Chapter 6 covers mathematical induction, recursion, and strong induction. While section 1 only provides typical proof by induction examples, section 2 is quite longer and provides several more interesting examples of "the wide range of uses of induction."

Chapter 7 is a short chapter and focuses on methods of comparing sizes of different sets. The proofs here in this last chapter are presented without much explanation. The reader is expected to be able to follow the proofs with less hand-holding at this stage in the book. The chapter concludes with a discussion and proof of the Cantor-Schroder-Bernstein Theorem.

Appendix 1 contains solutions to many of the exercises in the book. These are full-fledged solutions rather than the simple, terse (and often useless) "hints" that are found in some mathematics books.

Appendix 2 describes "Proof Designer", a Java applet that can be used to help design proofs. Although the book stands alone without the software, it could be a good motivator and help for students.

The "Suggestions for Further Reading" section is a short list of other books that may be of interest to the motivated student or self-learner. These include books on set theory, logic and discrete mathematics.

The "Summary of Proof Techniques" section outlines the proof techniques discussed in chapter 3 and explains how to use each technique in the Proof Designer software.

Finally, there is a very short index.

3 Conclusion

The author may want to consider further integrating Proof Designer into the remainder of the text (for example: adding exercises and solutions with Proof Designer in mind). At the same time, I think it is good that the book stands alone without Proof Designer, and I hope it continues to do so in the future.

This is a good book, and an exceptionally good mathematics book. Thorough and clear explanations, examples, and (especially) exercises with complete solutions all contribute to make this an excellent choice for teaching yourself, or a class, about writing proofs. I highly recommend it to students as a supplement to their course textbook, and to self-learners.

Review[7] of
Practical Optimization: Algorithms and Engineering Applications
Author of book: Andreas Antoniou and Wu–Sheng Lu
Springer Verlag, 2007, 669 pages
Reviewed by Brian Borchers

The author of an introductory textbook on optimization is faced with the difficult challenge of introducing a subject that is inherently interdisciplinary both in its theoretical basis and its applications. Optimization makes use of theory from mathematical analysis, numerical analysis, and computer science, and it has applications in areas as diverse as engineering design, statistics, finance, and public policy analysis. Students taking courses in optimization often come from wildly disparate backgrounds in mathematics, computer science, engineering, or business. Introductory textbooks typically focus on some combination of the mathematical theory of optimization, algorithms for various classes of optimization problems, or optimization modeling and applications. Although a more theoretical approach may be appropriate for an audience of mathematics students, most successful textbooks on optimization have focused primarily on algorithms, with examples drawn from various areas of application.

The subtitle, "Algorithms and Engineering Applications" aptly describes the approach of this book. Antoniou and Lu have written an introductory textbook on optimization that provides broad coverage of algorithmic techniques of optimization as well as applications of these techniques to problems in electrical engineering. The book is targeted at an audience of electrical engineering graduate students who can be expected to have a mathematical background that includes vector calculus and linear algebra but little or no analysis. Many examples are used to illustrate important mathematical concepts. The authors are not afraid to state definitions and theorems, but they feel no obligation to provide proofs of all of the theorems. The applications presented in the book motivate the development of the algorithms and provide material for exercises. This is a very good way to introduce this audience to optimization. However, this specialized approach might not be appropriate for other audiences.

The authors first consider unconstrained optimization problems of the form

$$\min f(x)$$

where x is a vector of real variables.

If the function $f(x)$ is convex, then any local minimum point is also a global minimum. However, if $f(x)$ is nonconvex, then the function may have many local minima that are not globally optimal. The methods discussed in this book can be used to find local minima of convex or nonconvex optimization problems. Antoniou and Lu do not discuss methods for the global optimization of nonconvex problems. Another important issue is the differentiability of the objective function $f(x)$. Many methods use the gradient or Hessian of $f(x)$. These methods are obviously not applicable

[7] © Brian Borchers, 2009

to problems in which $f(x)$ is nondifferentiable. Antoniou and Lu do not discuss methods for nondifferentiable optimization.

The presentation of methods for smooth unconstrained optimization problems includes traditional material on methods for one dimensional optimization, steepest descent, the method of conjugate gradients, Newton's method, and quasi-Newton methods. Antoniou and Lu also include a chapter on minimax problems. This is a topic not typically discussed in introductory optimization textbooks but it has important applications in digital filter design. A separate chapter on applications of unconstrained optimization includes sections on pattern matching, inverse kinematics for robotic manipulators, and the design of digital filters.

The second half of the book covers constrained optimization problems of the form

$$\begin{array}{lll} \min & f(x) & \\ & g(x) & \leq \quad 0 \\ & h(x) & = \quad b. \end{array}$$

The most specialized but still widely applicable class of constrained convex optimization problems are ones in which f, g, and h are linear functions. These linear programming (LP) problems can be solved either by the simplex method or interior point methods. LP can be generalized to convex quadratic programming (CQP) in which f is a convex quadratic function while g and h are still linear. Second order cone programming (SOCP) problems are a new and interesting class of problems that further generalize CQP by adding inequality constraints of the form

$$x_1 \geq \sqrt{x_2^2 + \ldots + x_n^2}.$$

The authors show how convex quadratic programming problems can be rewritten using SOCP constraints and demonstrate that the feasible region of an SOCP problem is convex. Semidefinite programming (SDP) problems involve symmetric matrix variables that are constrained to be positive semidefinite matrices. The authors demonstrate that SDP problems are convex and that SOCP problems can be rewritten in SDP form. Of course there are also general convex programming (CP) problems in which the only restrictions are that the feasible region and objective function f are convex.

The connection between these problem classes is that

$$\text{LP} \subset \text{CQP} \subset \text{SOCP} \subset \text{SDP} \subset \text{CP}.$$

Although the simplex method for linear programming cannot easily be extended to any of the other problem classes, polynomial time interior point methods for LP can be extended to CQP, SOCP, and SDP problems. The authors present Kelly's cutting plane algorithm as an approach to the solution of CP problems. The cutting plane approach is very general, but can be very slow in practice. SOCP and SDP problems are important because they are more general than LP while still being efficiently solvable.

After a chapter on the theory of constrained optimization, the authors discuss methods for all of the above classes of constrained convex optimization problems. The coverage of second order cone programming and semidefinite programming is unusual for an introductory textbook in optimization, but these topics are becoming very important in electrical engineering applications. The authors also include a chapter on sequential quadratic programming and interior point methods for general constrained nonlinear optimization problems. The final chapter is on applications of

constrained optimization to the design of digital filters, optimal control, robotics, and multiuser detection in wireless networks.

Although students who have read this book might be able to implement some of the methods discussed here, they should generally make use of more sophisticated and robust software packages. A surprising weakness of the book is the lack of any discussion of available software implementations of the various algorithms.

This textbook is appropriate for its intended audience of graduate students in electrical engineering, but it would not be appropriate for more general audiences. Readers looking for a broad introduction to optimization with more theory but without the electrical engineering applications and without the coverage of SOCP and SDP might be better off with a mainstream textbook such as Nocedal and Wright [2]. Readers looking for a more specialized text that discusses convex optimization, SOCP, SDP, and applications would be well served by the textbook of Boyd and Vandenberghe [1].

References

[1] S.P. Boyd and L. Vandenberghe. *Convex Optimization*. Cambridge University Press, 2004.

[2] J. Nocedal and S.J. Wright. *Numerical Optimization*. Springer Verlag, second edition, 2006.

Review of

Rock, Paper, Scissors: Game Theory for Everyday Life[8]

Author of book: Len Fisher

Publisher: Basic Books, 2008

$12.00, Softcover

Reviewer: William Gasarch `gasarch@cs.umd.edu`

1 Overview

This is a book on Game Theory for the layperson, though it covers some material outside of Game Theory as well. The aim of the book is to understand the real world through the lens of game theory and even try to see what we can do to make the world a better place. The book has lots of examples but not much mathematics. This is appropriate for their target audience: laypeople who want to know some game theory as it relates to the real world.

2 Summary of Contents

This book views game theory as trying to solve the following human problem:

If we all act in our own self interest than we are collectively worse off. How can we get around that.

[8] William Gasarch©2009

Chapters 1 (Trapped in the Matrix), 3 (Seven Deadly Dilemmas), and 4 (Rock, Paper, Scissors) describe some classical game theory scenarios. We describe one from chapter 3:
Stag Hunt: Cooperation between members of a group gives them a good chance of success (say, hunting a Stag) where an individual can defect and get a certain reward (say, a Hare). The payoff matrix is as follows. Ronald (R) is playing the row, Carolyn (C) is playing the column.

	Chase Hare	Hunt Stag
Chase Hare	R-2, C-2	R-5, C-0
Hunt Stag	R-0, C-5	R-8, C-8

Clearly both Ronald and Carolyn are better off if they both hunt the Stag. But the fear that the other one will chase the Hare will drive both of them to chase the Hare. The book gives many many examples of all of these scenarios and more.

Chapters 5 (Let's Get Together), 6 (Trust), 7 (Tit for Tat), and 8 (Changing the Game) are about ways around this problem. That is, how can we get groups of people to cooperate for the greater good. The book does not discuss this mathematically. Instead the book discusses social pressures, contracts, negotiations, and other real-world scenarios. Chapter 8 has a solution using Quantum Computing; however, it really just uses the ability to communicate. It has been simulated by classical computers (hence one wonders if the quantum is really needed) and seems to work.

Chapter 3 (I Cut and You Choose) is on cake cutting— actually resource allocation. The title comes from what a parent should do with two children that want to split a cake: one cuts, and the other chooses. This topic is usually not in a Game Theory book; however it seems to fit into this book nicely.

3 Style

The author gives many many examples. Some of them are quite personal. This is fine but at times I feel like I am reading his personal diary. The author intentionally keeps math and details out of the book but are in extensive end notes. These notes are excellent and they reassured me that the author knows the material very well.

The book claims that Game Theory can be applied to understand and solve some of the worlds problems. I would absolutely agree about understanding them. Even though it was written before the economic collapse it provides some insights on it. As for solving them, I am more skeptical. However, he makes a good argument for it.

The author Len Fischer has a blog which contains other applications of Game Theory to the real world including the recent ecomonic collapse. The blog is at `www.lenfischerscience.com`. He also has an article in the Washington Post about the Bernie Madoff's pyramid scheme at `http://www.washingtonpost.com/wp-dyn/content/article/2008/12/19/AR2008121902977.html`.

4 Opinion

If someone does not know that much math and wants to learn some Game Theory then this is an excellent book. If you know some, but not alot, of game theory, then this will be a quick read and you will learn some nuggets. If you know lots of game theory then buy it anyway as it will provide you with more examples, and you can give it to your math-inclined niece.