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. **A Concise Introduction to Data Compression** by David Salomon. This book covers different aspects of data communications with a main focus on source coding, more commonly known as data compression. We can view source coding as lossless compression, where the goal is to find a bijective function that when fed a bitstream, also known as a message, outputs a shorter bitstream.

2. **Parallel Algorithms** by Henri Casanova, Arnaud Legrand, and Yves Robert. This book provides the reader with an advanced introduction into the principles of Parallel computing. The book is targeted at advanced readers – graduate students and post-graduate researchers with a strong computational background – and represents a good resource both in support of a graduate course in parallel algorithms, and for self-guided learning.

3. **Polynomia And Related Realms** by Dan Kalman. This book is about polynomials. Topics include Horners rule, root finding (e.g., the cubic equation) and max-min problems. There is also some history in the book so you'll know where the ideas come from. The MAA awarded this book a Beckenback Prize at the January meetings. Details are posted at http://maa.org/news/jmm2012awards/beckenbach.html

4. **Biscuits of Number Theory** Edited by Arthur T. Benjamin and Ezra Brown. The authors themselves give the best description of the book: *an assortment of articles and notes on number theory, where each item is not too big, easily digested, and makes you feel all warm and fuzzy when you're through.*

5. **Combinatorial Geometry and Its Algorithmic Applications: The Alcalá Lectures** by János Pach and Micha Sharir. Combinatorial Geometry is the study of points, lines, and planes. This material often has algorithmic applications; however, unlike Computational Geometry, this is not the original motivation. This book explores the aspects of combinatorial geometry that have applications to algorithms.

6. **Handbook of Large-Scale Random Networks** Edited by : Bela Bollobás, Robert Kozma and Desző Miklós. Networks can often be modeled as a random graph. The research here is truly interdisciplinary. This handbook is an outcome of a U.S.-Hungarian workshop on complex networks held at the Rényi Istitute in Budapest in 2006. According to its editors, its purpose is to *provide a significant update and extension beyond the materials presented in the "Handbook of Graphs and Networks", published in 2003 by Wiley.*

7. **Algorithms and Theory of Computation Handbook** Edited by : Mikhail J. Atallah and Marina Blanton. This is a pair of volumes that cover many topics of interest to TCS research. Volume I is mostly algorithms and Volume II has some real applications.

8. **Primality testing and integer factorization in public key cryptography** by Song Y. Yan. This book covers number theory, some of which is quite advanced, and how it interacts with modern cryptography.

9. **Process Algebra: Equational Theories of Communicating Processes** by J. C. M. Baeten, T. Basten, and M. A. Reniers. Process algebra is a method for specifying and verifying distributed and parallel systems that uses logic and universal algebra. This book deals mostly with using Process Algebras for communicating processes.

10. **Insider Threats in Cyber Security** Edited by Probst, Hunker, Gollman, and Bishop. This book seeks to educate the reader about the various aspects of insider threat and attempt to define/explain the problem (e.g., types of insiders, the nature of the problem and types of misuse), and ways in which end users and businesses can seek to mitigate some of these risks. Other topics include fraud detection and insider threat mitigation technologies. Several challenges from both practitioner and research perspectives are discussed.

BOOKS I NEED REVIEWED FOR SIGACT NEWS COLUMN

1. *The Art of Computer Programming Volume 4A: Combinatorial Algorithms* by Donald Knuth.
2. *Combinatorial Optimization: Theory and Algorithms (Fifth Edition)* By Korte and Vygen.
3. *Integrated Methods for Optimization (second edition)* by John Hooke
4. *A Guide to Experimental Algorithms* by Catherine McGeoch.
5. *Bioinformatics for Biologists* Edited by Pavel Pevzner and Ron Shamir.
6. *Computability and Complexity Theory (2nd Edition)* by Homer and Selman.
7. *Information Theory and Best Practices in the IT industry* by Sanjay Mohapatra.
8. *Security and Game Theory: Algorithms, Deployed Systems, Lessons Learned* by Milind Tambe.
9. *Algebraic Shift Register Sequences* by Mark Goresky and Andrew Klapper.
10. *A Survey of Data Leakage Detection and Prevention Solutions* by Asaf Shabtai, Yuval Elovici, and Lior Rokach.
11. *Bayesian Reasoning and Machine Learning* by David Barber.
12. *Software Abstractions: Logic, Language, and Analysis* by Daniel Jackson.
13. *In pursuit of the Unknown: 17 Equations that changed the world* by Ian Stewart.
14. *Enumerative Combinatorics Volume 1 (Second Edition)* By Richard Stanley.
15. *Applications of Combinatorial Matrix Theory to Laplacian matrices of Graphs* by Jason Molitierno.
16. *Proof Analysis: A Contribution to Hilbert's Last Problem* by Negri and Von Plato.
17. *The shape of inner space* by Shing-Tung Yau and Steve Nadis.

Review [2] of
A Concise Introduction to Data Compression
Author: Professor David Salomon (emeritus)
Publisher: Springer-Verlag, 2008
978-1-84800-0710-1, 39.95 USD
Part of the Undergraduate Topics in Computer Science

Reviewer: Ville Hautamäki (vishv@i2r.a-star.edu.sg)

1 Overview

Prof. David Salomon is known for many excellent books covering different aspects of data communications. One of his main focuses is source coding, more commonly known as data compression. This book aims to bring the wealth of knowledge from his previous books to a one- or two-semester undergraduate course.

We can view source coding as lossless compression, where the goal is to find a bijective function that, when fed a bitstream, outputs a shorter bitstream. Efficiency of the source coding can be measured by the length of the output bitstream. the lower limit of the efficiency is the entropy of the message.

Lossy compression is achieved by performing quantization on the message/signal and then using source coding to generate the final compressed bitstream. Some mathematical transformations are typically performed in advance to reveal some structure in the message. The best known example of this is *discrete cosine transformation* (DCT) performed on subimages in JPEG image compression standard. The first DCT coefficients are more important than the last coefficients; therefore, the first one's should be quantized less than the last ones.

2 Summary of Contents

The book is divided into two parts:

1. **Basic concepts (Chapters 1,2,3,4:** These chapters cover source coding and arithmetic coding.

2. **Advanced Concepts:** This is a miscellaneous collection of topics.

I would have preferred that the book be organized book in such a way that the first part deals with source coding and the second part deals with how source coding theory is applied to different signal types. In that organization, video compression could have been easily added as a short chapter after image compression.

Chapter 1 deals with the basics of compression. He first introduces basic concepts of entropy and redundancy and then continuing to variable length coding. Few elementary variable length coding methods are introduced. The final part of the chapter introduces the lossy compression in the form of scalar quantization and vector quantization.

Chapter 2 is all about Huffman coding. It starts with the basics of static (or semi-adaptive) Huffman coding, where symbol probabilities are known in advance and then moves to adaptive coding. This chapter rightly discusses different aspects, and details, of the Huffman coding, as it is a powerful method and yes is easy to explain.

In Chapter 3 a larger context is taken into account. Previous chapters were about coding each symbol of the input *independent* of the other symbols. As such, an implicit assumption was that the source is zeroth order Markov. When considering files user wants to compress, this is not the case; typically, there exists considerable dependency between adjacent symbols. Chapter 3 explains dictionary methods that attempt to utilize this fact. A Dictionary of symbol sequences seen so far is formed, and when same sequence is seen again the index is transmitted to the decoder. Dictionary methods, starting with LZ77 and the well known LZW, are explained with considerable detail in this Chapter.

Chapter 4 explains all the important arithmetic coding. I would have liked to seen a comparison of arithmetic coding and Huffman codings. It would have been nice if QM/MQ-coding would have been explained at least shortly.

Chapter 5 introduces some basic image compression techniques, building first to JPEG image compression and then finally to Wavelet based techniques. Fingerprint compression system used by the FBI, namely WSQ, is introduced here as an example. Some high-level information about the new standard compression method JPEG2000, that uses wavelet transforms, could have been included in the end of the Chapter 5.

Chapter 6 is about audio compression. It also gives a good explanation of predictive coding. The main part of the Chapter starts first with a short tour of the human auditory system and then goes to explain *linear prediction* (LP). Later, μ-Law, A-law and shortened audio compression methods are explained.

Chapter 7 deals with the miscellaneous methods such as Burrows-Wheeler universal compression method and the SCSU unicode compression method.

3 Style

I have always enjoyed reading Prof. Salomon's books, a large part of the enjoyment comes from the his judicious use of quotations to spice up the text. This book is consistent with that style. In the present book, multiple explanations and examples are used to clarify and expose different and important concepts, such as entropy and variable length coding.

The book also includes a numerous program code snippets. These programs are clearly written and so should be easily understood by students.

4 Opinion

The book is excellent and fills the stated goal. When I am going to teach data compression again, I will most definitely use A Concise Introduction to Data Compression as a textbook for the class.

Review [3] of
Parallel Algorithms
Author: Henri Casanova, Arnaud Legrand, and Yves Robert
Publisher: Chapman and Hall/CRC, 2008
ISBN 978-1584889458, $ 79.95
Chapman & Hall/CRC Numerical Analysis & Scientific Computation Series

Reviewer: Mihai Pop

1 Overview

Parallel computation is hot... again. Articles in the popular press now often refer to "cloud computing", "multicores", or "GPUs" – buzzwords referencing recent parallel architectures. While yesterday's parallel computers were mainly found in large computing centers, their modern counterparts are significantly more ubiquitous: most middle to high-end desktop computers contain multiple processors, each with two or more cores, and their graphics cards have hundreds of Graphical Processing Units (GPUs). Furthermore, many of us have joined widely distributed computing grids such as SETI@home or Folding@home – lending spare CPU cycles to efforts aimed at finding extraterrestrial life, or figuring out the complex shapes into which proteins fold. Access to even higher computational power is also becoming increasingly easy – most academic departments and research labs maintain large computer clusters, while Amazon's Electric Compute Cloud (EC2) service allows anybody with an internet connection to rent computational resources tailored to their needs (in terms of numbers and features of interconnected processors).

While the hardware underlying parallel computers has changed significantly in recent years, the fundamental principles underlying the way in which these computers are programmed have remained largely the same. The book "Parallel Algorithms" by Casanova, Legrand, and Robert provides the reader with an advanced introduction into these principles. The book is targeted at advanced readers – graduate students and post-graduate researchers with a strong computational background – and represents a good resource both in support of a graduate course in parallel algorithms, and for self-guided learning.

2 Summary of Contents

The book is organized into three broad sections – Models, Algorithms, and Scheduling – each covering several key results in the respective areas of parallel computation. These are described in more detail below.

2.1 Computational models

The discussion of computational models begins with the theoretical PRAM model (shared memory machine with unlimited memory and processors, and negligible communication costs). This first chapter introduces parallel prefix computation and sorting algorithms, as well as the issues arising from handling concurrent accesses to a same memory cell, i.e. the three versions of the

[3]

PRAM model: CREW (concurrent read exclusive write), CRCW (concurrent read concurrent write), EREW (exclusive read exclusive write).

The second chapter covers sorting networks – ways to organize a collection of simple processors (comparators) that can be used to sort numbers without the need to adaptively reconfigure the network connections (the processors perform the same set of comparisons and route the data in the same way regardless of the sequence of numbers provided as an input). The authors describe several classical designs for sorting networks and analyze their performance in terms of number of comparators and time needed to perform the computation. In addition, they introduce and prove the 0-1 principle: the idea that in order to prove that a network correctly sorts arbitrary number sequences it is necessary and sufficient to verify that the network can sort a sequence of just 0s and 1s.

The third chapter focuses on more realistic models of parallel architectures that take into account communication costs. Discussed in this chapter are different topologies used to interconnect multiple processors and models that allow researchers to analyze the performance of algorithms executing on these network topologies, taking into account both the computational characteristics of the processors and the bandwidth, latency, and multiplexing abilities of the interconnection network. In addition, the authors describe how certain communication procedures such as routing and broadcast operations can be performed efficiently under certain assumptions about the topology of the underlying network. Also discussed are distributed hash tables in the context of peer-to-peer computing.

2.2 Algorithms

This section focuses primarily on parallel matrix algorithms, including matrix multiplication, LU factorization, and stencil operations (operations that update a cell in a matrix using information from the adjacent cells). While these seem to be a restricted set of problems, matrix algorithms are central to many other problems including graph algorithms, operations research, and dynamic programming approaches (e.g., many string matching problems can be phrased as stencil operations).

The first two chapters in this section focus on the effect of the underlying network topology on the design and performance of matrix algorithms – chapter 4 discusses ring topologies, and chapter 5 focuses on grids. The latter chapter also discusses some of the trade-offs between ring and grid topologies and indicate that (at least for matrix operations) 2-D (grid) data distributions lead to lower communication costs than 1-D (ring) data distributions. This chapter also describes three classic algorithms for matrix multiplication – Cannon, Fox, and Snyder – and discusses the trade-offs between the three approaches. The chapter ends with a discussion of 2-D block-cyclic data distribution – an approach for organizing data blocks on a grid.

Chapter 6 introduces the issues arising from heterogeneous platforms (not all processors have the same computation speeds). Primarily the discussion is focused on load balancing – the task of allocating each processor a sub-problem commensurate with the processors' computational abilities. The authors show that this problem can be efficiently solved for one-dimensional architectures, however the problem becomes NP-hard in a two-dimensional setting, both in the general case, and if the data are organized in a column-wise fashion. For the latter case they describe an approximation partitioning algorithm and prove a lower bound on its performance (in terms of communication costs) with respect to the optimal partitioning.

2.3 Scheduling

The third section is focused on task graph scheduling algorithms – the task of assigning tasks to a heterogeneous set of processors such that the execution time is minimized while observing all data dependencies between individual tasks.

Chapter 7 provides an introduction to the task graph concept and the scheduling problem. Scheduling is first discussed in the context of negligible communication costs. The authors show that in this case the scheduling problem is easy if the number of processors is unbounded and describe a polynomial time algorithm for this problem. They also show that the problem becomes NP hard if the number of processors is limited, leading to a discussion of heuristic scheduling algorithms. The chapter ends with a discussion of the complexity introduced when taking into account communication costs – in this context the scheduling problem is NP hard even if the number of processors is unlimited. The authors prove this fact and describe how scheduling heuristics discussed in the "no communication" setting can be extended to take into account communication cots.

Chapter 8 focuses on several advanced scheduling topics, including divisible load applications (where the scheduling algorithm is allowed to schedule partial tasks), throughput (rather than total running time) optimization and scheduling of scientific workflows. The latter problem corresponds to the situation where large data-sets must be processed by a series of analysis programs operating in a pipelined fashion. The chapter (and the book) ends with a discussion of loop nest scheduling – a problem that arises in the context of automated parallelization of programs at compile time.

3 Style

The cover of "Parallel Algorithms" advertises a "rigorous yet accessible treatment" of concepts related to parallel computation, and the book delivers on this promise. The text is overall easy to follow, technical concepts being introduced at a high level and accompanied by numerous examples. At the same time, the authors do not sacrifice rigor for the sake of simplicity of presentation: the algorithms described in the book are presented in pseudo-code, their performance is rigorously evaluated, and all the necessary theorems and proofs are provided. In addition, a significant fraction of the text is focused on a discussion of the computational complexity of parallel algorithms under different assumptions about the physical organization and characteristics of the underlying parallel architecture.

Each chapter ends with a few sections outlining advanced topics that are beyond the scope of the book. These are not presented in as much detail, however provide the reader with the basic background and with pointers to the relevant literature. The text throughout the book is well referenced, and the chapters conclude with detailed bibliographical notes.

3.1 Exercises

The exercises accompanying every chapter are well chosen to complement the text. In many cases, the exercises require the reader to "re-discover" results or algorithms not presented in the book, which I find a wonderful way to both reinforcing already described concepts and providing the reader with additional material. Solutions are provided for most exercises – which is great for self-guided learning, but makes the exercises less useful in a classroom setting.

4 Opinion

What this book is: Great starting point for learning basic concepts in parallel computation.
What this book is not: A resource for learning to write parallel programs.

Overall the book is well written and easy to follow and provides a good introduction to several advanced topics in parallel algorithms. It is important to stress that this is just an introduction, rather than a collection of recent results in the field. References are provided throughout the book that allow the interested reader to delve deeper in the topics being discussed. Also, while this is largely an introductory text, it is targeted at an advanced audience with a strong background in algorithms, i.e. it would not be suitable as a textbook for an undergraduate course.

Finally, the prospective reader should be aware that the title "Parallel Algorithms" is perhaps a bit misleading as the book is more focused on low-level algorithmic topics than on parallel algorithms for solving high-level problems. As an example, there is no discussion of parallel graph algorithms – a highly relevant research area given the large graph data-sets generated by many research fields like physics, social network analysis, economics, or biology. The main focus is at a systems level rather than on applications of parallel architectures.

Review of[4] of
Polynomia And Related Realms
by Dan Kalman
The Mathematical Association of America, December 15, 2008
300 pages, HARDCOVER

Review by
Akash Kumar akashkum@yahoo-inc.com
1031 Clyde Avenue, Apt 1004, Santa Clara, 95054, CA

1 Introduction

Dan Kalman is a Lester R. Ford Award winner for his expository writing and though this statement might indicate some bias, I think its only natural as he has done a wonderful job in writing this book. The text is divided into 3 major portions. In the first part, the author discusses many aspects of polynomials in a single variable which one does not typically encounter in his school. In fact, as stated in the preface, the readers author has in mind are usually the teachers and/or "anyone who has a long history of applying mathematics, including scientists, engineers and analysts." The second part of the text explores maximization and minimization of an *objective function* given some *constraint*. And finally, in the third part, we see some "tourist spots" in the "calculsian republic" which I had never encountered before – at least not expressed in a way this masterly.

The treatment of the topic is detailed and many times there are pauses, reflections and ruminations of some ideas. The author is guiding the reader all the way through difficult topics with his narrative communicating serious ideas in an elegant fashion. He has also included suitable historical context in many places which help you appreciate an idea better and in context. The text also contains many useful pedagogical instructions which detail how the author prefers to present a topic. Sometimes this includes the common mistakes that students might make and suggests that the teachers warn students against these potential pitfalls. In the sections to follow, I will describe (rather ashamedly) one place where I was also mistaken.

2 Summary

This is a section wise summary of the chapters in this book. Though I tried a little, I could not make the summary totally objective. There are clear signs of bias for which I apologize.

Chapter 1

In this chapter, the author walks the reader through many properties and aspects of polynomial equation in a single variable. In this regard, the author describes Horner's rule, its connection with synthetic division and base change rules. The most fascinating aspect of this chapter, I think undoubtedly, is the section on Lill's paper folding method of *solving polynomial equations* – or as the author cautions, Lill's method of *visualizing the roots geometrically*. The method consists in writing down the polynomial $p(x)$ in standard form and tracing the polygonal path corresponding to the

[4]©2012, Akash Kumar

polynomial. If the equation has got real roots, then you can obtain a Lill path using which the root can be obtained and the proof follows by an application of the Horner's rule. Then Kalman also goes on to investigate what happens visually when $p(x)$ does not have any real root and therefore $|p(x)|$ achieves a max value. In this case, the second Lill path won't "close". There is also some more information about different proofs that can be worked out visually using the Lill's method and thus exhibit its charm. I share author's enthusiasm in that the method deserves to be a *l'ill* more well known.

Chapter 2

This chapter develops a solution to the cubic (not Cardano's which is what most popular books give) by defining what the author calls the *curly root* function $Cr(x)$ which is the inverse of the function $f(x) = \frac{x^3}{1-x}$. This allows obtaining the roots r of a "depressed" cubics (i.e., cubics with x^2 coefficient made 0 and it is possible to "depress" every cubic) like $x^3+ax+b = 0$ as $r = -\frac{b}{a} \cdot Cr(\frac{a^3}{b^2})$. Next, author discusses Newton's method and describes the effects that different seed values can lead to. The section is light on technical details most of which are intuitively described and to an extent hand-waved and author also points this out. This is followed by a discussion on Lagrange Interpolation and what the author calls *palindromials* which are the so called reverse polynomials. Reverse of a polynomial $p(x)$ is given as $Rev(p(x)) = x^n p(1/x)$ whence it follows that whenever $r \neq 0$ is a root of $p(x) = 0$, $1/r$ is a root of $Rev(p(x)) = 0$. Methods are developed in this chapter reduce the problem of solving a palindromic polynomial equation to solving a polynomial equation of roughly half the degree. These methods generalize to all palindromials. Lastly, this chapter explains the content of *Marden's* theorem. It was for his masterly exposition of an elementary proof of this theorem that Kalman won the Lester R. Ford Award. The theorem describes where the roots of the quadratic $p'(z)$ – the derivative of a complex cubic polynomial $p(z)$ with non-collinear roots z_1, z_2, z_3 lie. They are given by the focii of the unique ellipse inscribed inside the triangle formed by the roots of the cubic which is tangent to its sides at their midpoints. The proof can be found on the book's website which again is a very helpful resource. Its not yet totally updated and currently some appendices are missing.

Chapter 3

This is a very interesting chapter. The chapter investigates the idea of symmetry historically and discusses the work of Galois and Klein. This is followed by elementary symmetric functions which is followed by *the fundamental theorem of symmetric polynomials* and finally the author brings down the curtain with a discussion of Newton's identities. In a little more detail, the chapter starts out by pointing out that the coefficients of a polynomial are symmetric functions of the negatives of the roots. Soon, we find ourselves following the author's exposition into the fundamental theorem which states that any symmetric polynomial can be expressed in terms of elementary symmetric polynomials. Finally, the author derives the Newton's identities in a very clear way by using reverse polynomials and Horner evaluation of a polynomial. The chapter is followed (like other chapters) by sources for further reading. One reference, that I find particularly interesting (and have been looking for) is Doron Zeilberger's paper which contains a combinatorial proof for Newton's identities. There was one typo in this chapter on page 50. The author states in the last sentence of 2^{nd} last paragraph that

> if a polynomial has all real roots, and if the coefficient of the second highest power of x

is negative, then there has to be at least one "negative" root.

The negative in quotes should be positive.

Chapter 4

The chapter begins with a discussion of what it means for a root of a polynomial to exist when the root in question is irrational or complex. For an equation (say an arbitrary polynomial of degree at least 5 with integer coefficients) with an irrational root r, usually we can only get better and better approximations to r without actually finding r itself. Then does it make sense to say that equation does have a solution? The author mentions that ideas of continuity can be invoked and the existence of irrational roots can be dealt with rigorously. For complex solutions also, the author appeals to modern understanding of mathematics and states that it is the distilled thought product of many a mathematical lifetime. Then assuming that the reader accepts complex numbers as legitimate, author states the fundamental theorem of algebra. Before giving out this theorem, he investigates the *rational roots theorem* which states that for a polynomial $p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$ with integer coefficients with a rational root r/s in lowest terms, we have (i) $r|a_0$. (ii) $s|a_n$. The author then considers a corollary to it which motivates why *algebraic integers* are called such. If the polynomial $p(x)$ in the above theorem is monic, then any rational roots are actually integers, thus motivating the name. Next, author goes on to describe Cardano's solution to the cubic by considering the depressed cubic. This is followed with Ferrari's solution to the quartic. This is followed with a bunch of interesting methods to solve the cubic and the quartics including one matrix algebra method which is explored in an article by Dan Kalman in the *American Mathematical Monthly* titled "Polynomial equations and circulant matrices." Finally, there is a brief discussion of Galois theory for unsolvability of quintics and beyond by radicals, but it still leaves much to be desired. I feel a "popular exposition" on Galois Theory is still missing.

Chapter 5

This chapter kicks off the second part of the text which is on finding maximum/minimum attained by a objective function $f(x, y)$ subject to some constraint $g(x, y) = 0$, both continuously differentiable. Kalman uses the two variable case only for instructional clarity noting that these methods can be readily extended to the case of n variables. He begins by noting that for the points $(x*, y*)$ where the objective function attains a local minima/maxima wrt to the constraints, we must have $\nabla \mathbf{f}(\mathbf{x}*, \mathbf{y}*) = \lambda \cdot \nabla \mathbf{g}(\mathbf{x}*, \mathbf{y}*)$ (assuming $\nabla g \neq 0$) for some $\lambda \in \mathbb{R}$. Next he goes on to give several geometric proofs, some really charming, for this fact. These proofs are unconventional in the sense that the only proof I knew was by invoking the Lagrange Multiplier theorem and I fell prey to the misconception that Kalman points out is common with this technique. As he points out, the technique is right but not for the reason that someone like me might intuitively expect. More on this a little later. Kalman begins the constrained maximization with a slurry of methods ranging from the idea that at the extremum point $(x*, y*)$, the constraint curve g and some level set of f will be tangent. (A level set is a collection of points of the domain at which the function attains a fixed value). The tangency condition implies that the gradients at this point to ∇f and ∇g will be parallel. Then he proves this fact over and over again by parametrizing the constraint curve, by using ideas from implicit function theory (basically, here the author uses the constraint curve g to express $y = y(x)$ and then asserts the existence of some function $\phi(x, y(x))$ such that $g \circ \phi$ is identically 0). Then the claim that the gradients are parallel at points of extrema follows by invoking the chain rule (as we noted above the functions are assumed continuously differentiable). There is then a proof by directional derivatives and finally we come to a proof that I liked the most.

The method is due to *Carathéodory* and Kalman calls it Cartheodory's Multiplier rule or the *CMT*. Kalman notes that this method can be applied to the case of n variables and $n-1$ constraints in its full generality but again for instructional clarity, he considers the 2–variable case. This method defines a mapping $\phi\colon \mathbb{R}^{\not\vDash} \to \mathbb{R}^{\not\vDash}$ as $\phi(x,y) = (f(x,y), g(x,y))$ and plots it on the uv axis with $u = f(x,y)$ and $v = g(x,y)$. He observes that points satisfying the constraint will fall on the u–axis. And maximizing f subject to this condition means that the point falls on boundary of the range of ϕ as far to the right as possible. We know that ϕ maps the neighborhood of a point (x,y) to the neighborhood of the point $\phi(x,y)$. But this is not true of the point maximizing f and so the matrix of partial derivatives is singular and has parallel row vectors which again implies the theorem. The author notes that this means that the set of equations we need to look at is the following

$$\frac{\partial f}{\partial x} = \lambda \frac{\partial g}{\partial x},\ \frac{\partial f}{\partial y} = \lambda \frac{\partial g}{\partial y} \text{ and } g(x,y) = 0$$

In the method of Lagrange multipliers,we begin by writing $F = f + \lambda g$. And then the equations that we need to follow by considering in turn $\frac{\partial F}{\partial x}$, $\frac{\partial F}{\partial y}$ and $\frac{\partial F}{\partial \lambda}$ and equating each to 0. This is however not justified. We cannot expect that unconstrained maxima of F has anything to do with constrained maxima of f. They are just not related. Then Kalman goes on to give one geometric justification for why this technique works. The discussion is not totally rigorous but I think it can be done with some effort.

Chapter 6

This chapter begins by looking at some different optimization problems. The author invokes Lagrange multipliers to solve the well known recreational problem of minimizing distance traveled $f(x,y)$, in the plane, from a point A to another point B the quickest when we are constrained to pay a visit to a line L. He observes that the level curve for the objective function of minimum value of f subject to visiting L gives rise to an ellipse as we force $AP + PB$ to stay constant. Then he launches into the study of ellipses with rotated axes and presents an attempt to find the angle of rotation using Lagrange multipliers. Next, he introduces the reader to envelope by giving an unusual but intuitive definition that an envelope of a family of curves F with a member curve C_a given by $F(x,y,a) = 0$ is the boundary of the family F. Under suitable assumptions, this boundary is obtained by eliminating a from $F(x,y,a) = 0$ and $\frac{\partial F}{\partial a} = 0$. As a clincher, he solves the $AM - GM$ problem in full and introduces the reader to the notion of iso-perimetric duality again by using Lagrangian Multipliers.

Chapter 7

This chapter is about the famous ladder problem in standard calculus texts. The problem asks the reader to find the *longest* ladder that can be carried through an L–shaped region without getting stuck. The standard trick is to instead look for the *shortest* ladder which gets stuck. The advantage is that this makes using the geometry a little easy and helps in "dealing with the equation of the ladder". The author asks if there is a more direct approach and though he admits that it is no substitute for the standard approach, he still offers it as it makes for an interesting discussion in the classroom. I totally agree with this view and more so after looking at his solution which makes use of the envelope of a family of ladders of continuously increasing size (all the way from ladder of length 0). These ladders are navigated through the corner by first overlapping with the x–axis and then their tip resting on the vertical wall is gently raised. The author looks at the space swept by

the family of these ladders and invokes the envelope algorithm to find the boundary curve solving the problem. Then to spice it up, he considers moving a cot around a corner which he again solves using envelopes.

Chapter 8
This chapter begins by another maximization problem. The goal is to find a point on an ellipse which maximizes the angle between the radius vector and the normal at that point. After solving this problem using Lagrangian Multipliers, Kalman also considers the generalization where we have a n dimensional ellipsoid.

Chapter 9
This chapter marks the beginning of the final part of the book. The author looks at *exponential linear equations* which have the form $a^x = mx + b$. In order to solve this equation the author introduces a new function called *glog* as the inverse of the function $y = e^x/x$. He mentions that this idea is similar in spirit to solve cubic in the 2^{nd} chapter of the text where he introduced the aforementioned function $Cr(x)$. In fact, upon some reflection, we can see in author's footsteps that in order to solve a certain class of equations (say $x^2 = b$ or $s(x) = b$ assuming $s(x) = x^2$), we can instead focus on equations in a subclass that can be solved by inverting a particular function (i.e., we can define $a = \sqrt{b}$ *iff* $b = a^2$) which amounts to defining $\sqrt{x}$ as the inverse of $y = x^2$. However, so far all that has been achieved is little more than window dressing. This requires identifying the properties of the new inverse function defined and in our case this means identifying the properties of *glog* which can be studied by looking at the intersection of the exponential curve $y = a^x$ with the line $y = mx + b$. And as the author shows, *glog* or *generalized logarithm* has some nice additive properties using which exponential linear equations can be solved. Author does remark that this also leaves open the possibility that our approach might be an overkill. For example, we know that the function $Cr(x)$ helps in solving cubics. But, if we had no idea about solving the cubics in general then Abel's Theorem could have been true for cubics onward for all we knew. But cubics do admit a solution by radicals which means that we need not define a new inverse function to solve them. Similarly, there is a possibility that exponential linear equations can be solved without defining *glog*. Kalman remarks that the work of Bronstein et al. has settled this question in the negative.

Chapter 10
In this chapter Kalman revisits asymptotes. He gives the traditional definition of an envelope of a family of curves as the curve which is tangent at each of its points to some member of the family. Then under some suitable assumptions, Kalman shows that the envelope algorithm described above follows from the traditional definition. He closes the discussion on envelopes by saying a few words on how his boundary definition of envelope relates to the traditional definition. Next he takes up a lively discussion on asymptotes. The asymptotes he considers are motivated from the consideration of the sketch of curves $f(x) = x^3$ and $g(x) = x^3 - x$. He notes that in some sense, the curve f "looks" asymptotic to g. In order to make this intuition precise, he tries defining asymptotes in a new fashion. After making the reader realize that defining the asymptotes is a somewhat subtle topic, he defines what he calls *horizontal asymptotes* and notes that the distance $d(a)$ between f and g along the line $y = a$. It can be seen $d(y) \to 0$ as $y \to \infty$. Then he gives the condition for two polynomials f and g to be horizontally asymptotic which says that f and g are horizontally asymptotic iff they $deg(f) = deg(g) = n$ and the coefficients of x^n and x^{n-1} are the same for both

the polynomials.

Chapter 11, 12
Chapter 11 is wonderful in that author using some ideas from Descartes' work; mainly the fact that tangency implies some polynomial has got a double root at some $x = x_0$, goes on to derive differentiation rules for quite a few functions. The work is quite masterly and easily followable. Trigonometric functions have not been totally amenable to differentiation using this approach, but polynomials, exponentials have been "captured" by this method. Finally, in the last chapter Kalman discusses the power of Calculus and remarks that some properties like continuity and differentiability that are shared by the broad class of elementary functions is almost like a miracle. It is so commonplace that we sometimes do not recognize this fact. Then he also brings up a second miracle of Calculus which is that it is accurate model for natural phenomena in the limiting case of discrete approximation and not only this, but it also simplifies the equations involved in the discrete cases.

3 Opinion

My background is in theoretical computer science and software engineering. For me, the best part of the text was that even with this background, it was highly accessible. If you have done a course in analysis (or even a course in first year calculus), you will be able to follow most of the ideas. That said, *there are* ideas in this book which are usually not presented elsewhere so even if you have a decent mathematical background, you will find something spicy for your taste here. There are a few typos, but for the most part, the presentation of the material and the author's narrative totally outruns it. The book also lists quite a decent number of references which the reader is invited to investigate if he is interested. The pedagogical instructions and the suggestion that author makes when a teacher is presenting a topic makes the text all the more lively and the material even more understandable. I will give the text full score. It was really a wonderful mathematical excursion into Polynomia and related realms.

Review[5] of

Biscuits of Number Theory

Editors of book: Arthur T. Benjamin and Ezra Brown

Dolciani Mathematical Expositions #34

Published by MAA, 2009

Review by Jeffrey Shallit[6]

Art Benjamin and Ezra Brown, editors of *Biscuits of Number Theory*, describe this book as follows: "an assortment of articles and notes on number theory, where each item is not too big, easily digested, and makes you feel all warm and fuzzy when you're through."

Benjamin teaches at Harvey Mudd College, and was named "America's best math whiz" by *Reader's Digest* in May 2005. He's also a professional magician who has appeared on many TV shows and National Public Radio. Brown teaches mathematics at Virginia Tech, and according to his web page, likes to bake his students actual biscuits.

Biscuits of Number Theory consists of 40 short articles copied from journals such as *Math Horizons*, *Mathematics Magazine*, *Mathematics Teacher*, and the *American Mathematical Monthly*. And when I say "copied", I mean it: some of the articles appear in exactly the same font as their original source — which means that typographically, the book feels a bit disorganized. Whether copied or not, errors from the original works seem to be faithfully preserved: read 257 for 251 on page 85, and replace U by $\bigcup$ on page 223 (twice).

The authors represented include some of the best expositors of elementary number theory: Peter Borwein, Stan Wagon, Carl Pomerance, Ivan Niven, Edward Burger, Ross Honsberger, and Martin Gardner, just to name a few. The articles are classified into seven different parts: arithmetic, primes, irrationality and continued fractions, sums of squares and polygonal numbers, Fibonacci numbers, number-theoretic functions, and elliptic curves and Fermat's last theorem.

Many of the chapters will be accessible to high school students or even bright junior high students. For example, chapter 3, entitled "Reducing the Sum of Two Fractions", explores the following simple question: sometimes when we add two fractions by putting them both over the same denominator l (the least common multiple of the two denominators), the resulting fraction is in lowest terms, and sometimes it isn't. For example, $\frac{4}{21} + \frac{7}{15} = \frac{69}{105}$ is not in lowest terms, but $\frac{7}{10} + \frac{11}{12}$ is. Can we characterize those pairs of denominators according to their behavior upon addition? Harris Shultz and Ray Shiflett show the answer is yes, and depends on the exponents of the prime factors dividing the denominators.

Some of the chapters are truly excellent. I particularly liked Henry Cohn's article, "A short proof of the simple continued fraction of e". Here Cohn shows how to derive the expansion

$$e = [2, 1, 2, 1, 1, 4, 1, 1, 6, \ldots, 1, 1, 2n, \ldots]$$

using nothing more than some simple integrals and the product rule for derivatives.

Other chapters will likely be very mysterious even for beginning graduate students. Furstenberg's topological proof of the infinitude of the primes (Chapter 8) will likely be incomprehensible for many students, as will the last article, about Fermat's last theorem. But that doesn't matter; it's *good* when a book has *some* content above the level of the typical reader, because this will

[6]School of Computer Science, University of Waterloo, Waterloo, ON N2L 3G1, Canada.

intrigue some readers sufficiently that they'll feel the need to learn the required material. The challenge is to have the right amount, and my feeling is that this book has a good balance of material.

This book wouldn't make a good textbook, but could certainly be used as a supplement to an introductory undergraduate (or even high school) course on number theory.

Review[7] of

Combinatorial Geometry and Its Algorithmic Applications: The Alcalá Lectures
Author: János Pach and Micha Sharir
Publisher: American Mathematical Society, 2009
Mathematical Surveys and Monographs, Volume 152

Reviewer: Sergio Cabello

1 Overview

Elementary geometric structures, like points, lines, and planes give rise to a large number of fascinating combinatorial problems. Several of these problems naturally appear in the study of algorithms handling geometric data, and thus are motivated by algorithmic applications. Others are just intriguing: easy to state, but apparently hard to solve. Each of the nine chapters of this book constitutes a survey of some area of combinatorial geometry.

2 Summary of Contents

Chapter 1 is dedicated to combinatorial problems concerning points and the set of lines passing through at least two of them. The chapter starts with a historic perspective on Sylvester's problem: is it true that for any finite set of points in the plane, not all on a line, there exists a line that contains precisely two of them? Different extensions of this problem are then considered, namely how many such lines through precisely two points exist, how many different directions are determined by those lines, as well as versions where the points have two colors. A part of the chapter is dedicated to an extension of the problem studying the set of directions determined in 3-space.

Chapter 2 is dedicated to arrangements of surfaces and hypersurfaces, and it spans about 30% of the book. The arrangement of a set of geometric objects is the decomposition of the space into cells, where each cell is a maximal connected subset of points contained in the intersection of some subset of the objects. Although one has to read the definition a few times to understand it, it pays off: it is a fundamental structure used in most papers in computational geometry. The chapter starts with some motivating examples, followed by formal definitions and assumptions used in the study of arrangements. An arrangement has several important substructures: single cells, zones, levels, etc. A section of the chapter is devoted to each of these substructures. The chapter then describes computational aspects of constructing, storing, and manipulating arrangements and its substructures. The chapter concludes as it started, listing several applications, which well could be considered motivation.

Chapter 3 is dedicated to Davenport-Schinzel sequences and their relation to arrangements of curves in the plane. A Davenport-Schinzel sequence is a sequence of numbers from $\{1, \dots n\}$ with certain forbidden patterns. The maximum length of a Davenport-Schinzel sequence, as a function of n, is near-linear. However, precise upper and lower bounds *need* the inverse Ackermann function $\alpha(n)$, which is an an extremely-slowly increasing function. It holds $\alpha(n) \leq 4$ for any n smaller than a tower of 65536 2s. The chapter describes and provides proofs for several upper and lower bounds on this maximum length. This maximum length is a fundamental tool to study the

combinatorial complexity of arrangements of curves in the plane, where it provides tight bounds for several combinatorial problems. The chapter describes this relation in detail.

Chapter 4 is dedicated to incidences: given a set of n points and m lines in the plane, how many point-line pairs, such that the point lies on the line, can there be? The answer is $O(n+m+n^{2/3}m^{2/3})$, and the chapter provides two different proofs of this fact. One proof is based on a partition of the plane into suitable parts, while the other is based on crossing numbers of graphs. The chapter also discusses the related problems obtained by considering other geometric objects, like circles, instead of lines, as well as generalizations of the problem to 3-space. These problems have a tight relation with problems concerning inter-point distances for finite point sets. Finally, applications of these bounds in other problems of combinatorial geometry are discussed.

Chapter 5 is dedicated to crossing numbers of graphs. The chapter starts considering two classical problems: the brick factory problem and Conway's thrackle conjecture. Afterwards, different definitions of crossing numbers are introduced, and known relations between them are stated. Then, there is a discussion on the structure of graphs drawn with straight-line segments with several or few crossings per edge. The chapter finishes showing the relation between the bisection width and the crossing number of graphs, and providing a proof of the crossing lemma.

Chapter 6 is dedicated to patterns in point sets. A pattern A is in B if a suitable transformation (translation, congruence, homothety, or affine transformation) transforms A into a subset of B. The scenario is different for each type of transformation. All these cases are considered, and in each of them, both combinatorial aspects, mainly extremal, and algorithmic aspects are described. The chapter finishes describing more 'flexible' patterns, like for example triangles with unit area spanned by the point set.

Chapter 7 is dedicated to lines in 3-space. It starts describing parameterizations of lines in 3-space, with emphasis in Plücker coordinates. The use of Plücker coordinates is then shown with a couple of problems: deciding if a line is above n given lines, and deciding if each red line is above each blue line in a given set of red and blue lines. The discussion then moves to the problem of cutting a given set of lines in 3-space so that the above-below relation among the resulting segments can be extended to a total order. This problem is essentially not well understood. Next, visibility problems among objects in 3d are considered, followed by a discussion on problems concerning transversals: is there a line stabbing n given objects? are there many combinatorially distinct stabbing lines? The chapter finishes with a list of open problems.

Chapter 8 is dedicated to two problems concerning colorings of geometric objects to obtain a certain property. The first problem is as follows: given a family of geometric objects (disks, unit disks, squares) that cover each point of the plane at least k times, is it possible to color each object red or blue, so that each monochromatic subfamily covers the whole plane? The answer depends on the geometric objects and the value of k. The second problem is known as conflict-free coloring: given a set of points P in the plane, assign a color to each point such that for any disk D there is a color that is assigned to precisely one point of $D \cap P$. Several natural extensions of this problem as well as the dual problem of coloring disks are discussed.

Chapter 9 is dedicated to problems concerning motion of coins in the plane. One wants to move from an original configuration to a target configuration. At each given step, one coin can be moved an arbitrary distance but without colliding with other coins. How many steps are needed in the worst-case? Similar problems when the 'ambient space' is a graph are also discussed

3 Opinion

The book is based on a series of lectures for graduate students and people with interest in combinatorial and computational geometry. Each chapter is essentially an independent survey of a small area of combinatorial geometry. The only dependency is that Chapter 7 requires several concepts explained in Chapter 2. In each chapter, several results are described, but only a sample of the most interesting and illustrating proofs is given. The reader obtains a comprehensive view of the results in the area, but only a high-level view of the techniques that are employed.

The book is suitable for people with interest in combinatorial or computational geometry. Some of the chapters treat classical topics, while other chapters consider newer trends. In my opinion, the book is not suitable as a basic textbook. Instead, the book is a valuable resource for people wishing to broaden their knowledge of geometric tools. It also provides a perfect starting point for doing research in the area, especially because it lists several open problems. The book provides a nice historical perspective and includes a number of anecdotes that make the reading smoother.

Review [8] of

Handbook of Large-Scale Random Networks
Edited by : Bela Bollobás, Robert Kozma and Desző Miklós
Publisher: Springer Verlag,2009
ISBN 1217-4696, List price: 199$
Bolyai Society Mathematical Studies vol. 18

Reviewer: Gabriel Istrate, gabrielistrate@acm.org

1 Overview

Random graph models (or *networks*, in the parlance of natural sciences) have become a (fashionable) hotbed of truly interdisciplinary research this millennium, with no shortage of good textbooks written from a multitude of perspectives

[Dur06, LC06, PSV07, BBV08, VR07], collections of fundamental texts [NBW06], popular science accounts [Bar03, Wat04, Buc03], a handbook [BS03], and significant research and media attention.

The volume is an outcome of a U.S.-Hungarian workshop on complex networks held at the Rényi Istitute in Budapest in 2006. According to its editors, its purpose is to "provide a significant update and extension beyond the materials presented in the "Handbook of Graphs and Networks", published in 2003 by Wiley".

2 Summary of Contents

The book under review is composed of twelve chapters. The perspective is interdisciplinary: Chapters 1,2, 4 are written from a mathematical perspective. Chapters 3,5 and 9 come from the Statistical Physics literature. Chapters 6,7,8 deal with properties of biological networks. Finally, applications to other areas, mainly inference and data mining are presented in the last three chapters of the book.

Chapter 1, "Random Graphs and Branching Processes" by B. Bollobás and O. Riordan surveys some basic models of inhomogeneous random graphs. The focus of the presentation is on properties of such models that can be obtained using the branching process approach. The presentation starts with a short outlook of some classical models, such as the Erdős-Rényi random graphs and random graphs with a fixed degree sequence and then proceeds to several inhomogeneous models, a central one being due to Bollobás, Janson and Riordan. The presentation covers the phase transition (with a historical perspective), local behavior and the giant component, as well as global properties such as diameter and the k-core. The chapter concludes with a critical discussion concerning the appropriateness of graph models in applications. The approach relies on considering a metric quantifying similarity of two graphs. Examples of such metrics considered in this chapter include edit distance, subgraph distance and a cut metric due to Borgs et al.

Chapter 2, due to P. Ballister, B. Bollobás and A. Sarkar, is titled "Percolation, connectivity, coverage and Colouring of Random Geometric Graphs". It surveys structural properties of several

classes of geometric models, such as the Gilbert disc model, the k-nearest neighbor model, and two random tessellation models, namely random Voronoi and random Johnson-Mehl percolation.

In Chapter 4, "Random Tree Growth With Branching Processes - A Survey", A. Rudas and B. Tóth rigorously investigate a random tree growth model that generalizes the preferential attachment model of Barabási-Albert. The model first arose in the Statistical physics literature through the work of Krapivsky and Redner. Both local and global results (in terms of the underlying structure of the resulting graph are presented.

Physicists' perspective is present in Chapters 3, "Scaling Properties of Complex Networks and Spanning Trees" (R. Cohen and S. Havlin), Chapter 5 "Reaction-Diffusion Processes in Scale-Free Networks" (M. Catanzaro, M. Boguña and R. Pastor-Santorras) and Chapter 9, "k-Clique Percolation and Clustering" (G. Palla, D. Ábel, I. Farkas, P. Pollner, I. Derényi and T. Vicsek).

Cohen and Havlin investigate the interconnectedness of three properties of networks: the fractal structure of the percolation cluster at the phase transition, the structure of distribution of shortest paths distances between vertices and properties of the minimum spanning tree. The emphasis is on scaling and critical exponents.

Catanzaro et al. present the structure of reaction-diffusion processes (models of disease propagation, such as the well-known *SIR models*, are a prime application), using a combination of analytical techniques (at the level of rigor usual for the Statistical Physics literature) and experiments.

The chapter by Vicsek et al. summarizes recent results on the *clique percolation problem*, a generalization of the edge percolation problem, and similar models for directed and weighted random graphs (models considered in this chapter are variants of the classical Erdős-Rényi random graph). The conclusion is that the phase transition has a continuous and highly nontrivial nature. Some applications are presented in the closing of the article to the problem of community detection. The results in this section have an experimental nature.

Biological applications of random graph models are presented in the book in Chapter 6, "Towards understanding the Structure and Function of Cellular Interaction Networks" (J, Thakar, C. Christensen and R. Albert), and two chapters on *cortical networks*. The first of them is Chapter 7, "Scale-Free Cortical Planar Networks" (W. Freeman and R. Kozma). The second of them (Chapter 8), due to T. Nepusz, L. Négyessy, G. Tusnády and F. Bazsó deals with a particular instance of the problem of reconstructing cortical networks.

Freeman and Kozma discuss structural properties of quantitative brain dynamics and the requirements imposed on random graph models. The emphasis is not so much centered on formal models (though this chapter is complemented by a mathematical appendix due to Bollobás and Riordan), but on modeling. In particular random graph theory is suggested as a complement to the ordinary differential equation methods employed in the literature.

Whereas the previously discussed chapter was focused on modeling issues, the chapter due to Nepusz et al. has a more experimental approach, discussing fitting real network with a particular model of networks called *preference model*. Two methods are employed: a greedy approach and a Markov chain Monte Carlo method (which experimentally seems to be display rapid mixing). Engineering and performance issues of the approach are discussed.

The last three chapters of the book are "The Inverse Problem of Evolving Networks - With Applications to Social Nets" (G. Csárdi, K. Strandburg, J. Tobochnik and P. Érdi), ", "Learning and Representation: From Comprehensive Sampling to the 'Symbol Learning Problem'" (A. Lőrincz) and "Telephone Call Network Data Mining: A Survey With Experiments" (M. Kurucz, L. Lukács, D. Siklósi, A. Benczúr K. Csalogány and A. Lukács).

Csárdi et al. study the problem of learning evolving network models. Two approaches are used: a frequentist and a maximum likelihood method. Presented applications deal with the dynamics of scientific collaboration networks (in this case the *cond-mat* section of arxiv.org), and the U.S. patent system (using a "forest fire" model of Leskovec et al.).

Lőrincz studies a particular approach in neurocognitive modeling. The contribution argues that inherent constraints (from the theory of reinforcement learning) give rise to a particular learning task called *the symbol learning problem*. The author of this review found this chapter to be somewhat more difficult to summarize in relation with the main perspective of the book, though connections with extremal graph theory and graph algorithmics are discussed in the conclusion.

Finally, Kurucz et al. present datasets, methods and algorithm used for a data mining study of telephone call networks arising from logs of Hungarian telephone companies. Structural graph properties are shown to impact the quality of clustering/mining methods (among them clique percolation and spectral clustering).

3 Style

Although titled "Handbook", the fact that the volume grew out of a conference shows in its nature: while some of the chapters have a true handbook-like feel, other chapters look somewhat more like research papers. Also in my opinion the progress in the area since 2003 goes significantly beyond the scope of this book.

4 Opinion

The previous remark is not intended to mean that the book is not worth consulting. In fact, as someone interested in the interdisciplinary dialog between theoretical computer science, statistical physics, biology and the social sciences under the banner of Complex Systems, I quite enjoyed reading the book. The choice of topics and presentations is illustrative of the type of work taking place in this area; many of the authors are top researchers working in this area. Several chapters (particularly the more mathematical ones) are likely to be useful to the theoretical computer scientist interested in random structures and algorithms, but most of the chapters were reasonably interesting to me.

To conclude, this is a book that belongs to the bookshelves of any respectable university library. Does it belong to individual book collections as well? The answer may vary due to a list price I found rather high, but inexpensive buying options are available at the moment of writing this review on the Internet.

References

[Bar03] A.L. Barabási. *Linked: How Everything is Connected to Everything Else, and What it Means for Business and Everyday Life*. Plume, 2003.

[BBV08] A. Barrat, M. Barthélemy, and A. Vespignani. *Dynamical Processes on Complex Networks*. Cambridge University Press, 2008.

[BS03] S. Bornholdt and H.G. Schuster, editors. *Handbook of Graphs and Networks: From the Genome to the Internet*. Wiley, 2003.

[Buc03] M. Buchanan. *Nexus: Small Worlds and the Groundbreaking Theory of Networks*. W. W. Norton & Company, 2003.

[Dur06] R. Durrett. *Random Graph Dynamics*. Cambridge University Press, 2006.

[LC06] L. Lu and F. Chung. *Complex Graphs and Networks*. American Mathematical Society, 2006.

[NBW06] M. Newman, A.L. Barabási, and D. Watts, editors. *The Structure and Dynamics of Networks*. Princeton University Press, 2006.

[PSV07] R. Pastor-Santorras and A. Vespigniani. *Evolution and Structure of the Internet: A Statistical Physics approach*. Cambridge University Press, 2007.

[VR07] F. Vega-Redondo. *Complex Social Networks*. Cambridge University Press, 2007.

[Wat04] D. Watts. *Six Degrees: The Science of a Connected Age*. W. W. Norton & Company, 2004.

Review[9] of
Algorithms and Theory of Computation Handbook
Edited by : Mikhail J. Atallah and Marina Blanton
Publisher: Chapman & Hall / CRC Press, 2010
ISBN: 978-1-58488-822-2, Price: $157.63
Two Volumes: *General Concepts and Techniques* **(Vol. I)**
and *Special Topics and Techniques* **(Vol. II)**

Reviewer: Nick Papanikolaou, HP Labs (np1@hp.com)

1 Overview

This pair of volumes is an extensive compendium of survey articles on issues of current importance in theoretical CS research. Without a shadow of a doubt it is a much needed resource for any theory researcher, as well as serving as a detailed introduction to the field for non-specialists. The first volume covers algorithms and algorithmic techniques, aspects of data structures, complexity theory, formal languages and computability, in addition to having a handful of chapters on related but more specialized topics, such as learning theory, coding theory, parallel and distributed computing. This volume in itself is a treasure of material in core computer science and can serve as a replacement for more specialized texts when only a good foundation is required. The articles are written by experts in the field and are eminently readable.

There is a couple of very useful chapters on searching and sorting algorithms, which can be used as a complement and gentle introduction to Knuth's seminal tome [1] on the subject. But to have, in the very same volume, an equally accessible introduction to convex optimization, and another on simulated annealing, makes for a rich and enjoyable afternoon read. In fact, you may find yourself wondering many times whether you could change research topic or theme, as this volume is rather inspiring!

While there is still emphasis on algorithms and algorithmic approaches, Volume II has a broader remit and introduces several application areas, including AI and robotics, cryptography, voting and auction schemes, privacy and databases, computational biology, grid and DNA computing. What a feast! The coverage of cryptography, cryptanalysis and security protocols is particularly extensive, which makes this a useful reference for security research. The chapter on privacy and anonymity is particularly relevant and a very timely review of k-anonymity techniques. In the wake of Narayanan and Shmatikov's recent award-winning results on the de-anonymisation of the Netflix prize database [2], this material is particularly interesting and should serve as a foundation for further research on anonymity and anonymisation methods.

It is not possible to review this pair of volumes in the usual manner, due to their length and the sheer breadth of material. I will provide the table of contents for both volumes in Section 2, however, for readers of this review to get an inkling of the variety therein. Then I will give and justify my opinion of this text, concluding with references.

[9]

Comparison with *Handbook of Theoretical Computer Science*

It is interesting to make a comparison with the already established *Handbook of Theoretical Computer Science* [3, 4], edited by Leeuwen. Leeuwen's book is also extensive, and is similarly divided into one volume on Algorithms and Complexity [3] and another on Formal Models and Semantics [4].

First one should point out that Leeuwen's book is older, and is not designed to be as broad an introduction as this one is. So the contributions in the former tend to be not just survey articles, but often also focused research articles which also give general background on the topics of interest. There is some degree of overlap, especially with regard to complexity theory, but Leeuwen's volumes do not introduce algorithmics in a textbook manner. Some of the chapters have very similar coverage to those in this handbook (under review), although this handbook is more up-to-date. VLSI theory is covered in both, data structures, cryptography and graph algorithms also.

The fundamental difference between the *Handbook of Theoretical Computer Science* by Leeuwen and the handbook under review is one of style. While the former has detailed chapters on a selection of topics, the latter has more extensive and systematic coverage of algorithms arising across the spectrum of computer science research.

The next section shows the contents of the two volumes. In Section 3 I round off this review with a personal view.

2 Tables of Contents

2.1 Volume I: General Concepts and Techniques

Preface ..... **ix**

Editors ..... **xi**

Contributors ..... **xiii**

1 Algorithm Design and Analysis Techniques
Edward M. Reingold 1-1

2 Searching
Ricardo Baeza-Yates and Patricio V. Poblete ... 2-1

3 Sorting and Order Statistics
Vladimir Estivill-Castro 3-1

4 Basic Data Structures
Roberto Tamassia and Bryan Cantrill 4-1

5 Topics in Data Structures
Giuseppe F. Italiano and Rajeev Raman 5-1

6 Multidimensional Data Structures for Spatial Applications
Hanan Samet 6-1

7 Basic Graph Algorithms
Samir Khuller and Balaji Raghavachari 7-1

8 Advanced Combinatorial Algorithms
Samir Khuller and Balaji Raghavachari 8-1

9 Dynamic Graph Algorithms
Camil Demetrescu, David Eppstein, Zvi Galil, and Giuseppe F. Italiano 9-1

10 External-Memory Algorithms and Data Structures
Lars Arge and Norbert Zeh 10-1

11 Average Case Analysis of Algorithms
Wojciech Szpankowski 11-1

12 Randomized Algorithms
Rajeev Motwani and Prabhakar Raghavan 12-1

13 Pattern Matching in Strings
Maxime Crochemore and Christophe Hancart . 13-1

14 Text Data Compression Algorithms
Maxime Crochemore and Thierry Lecroq 14-1

15 General Pattern Matching
Alberto Apostolico 15-1

16 Computational Number Theory
Samuel S. Wagstaff, Jr 16-1

17 Algebraic and Numerical Algorithms
Ioannis Z. Emiris, Victor Y. Pan, and Elias P. Tsigaridas 17-1

18 Applications of FFT and Structured Matrices
Ioannis Z. Emiris and Victor Y. Pan 18-1

19 Basic Notions in Computational Complex-

ity
Tao Jiang, Ming Li, and Bala Ravikumar 19-1
20 Formal Grammars and Languages
Tao Jiang, Ming Li, Bala Ravikumar, and Kenneth W. Regan 20-1
21 Computability
Tao Jiang, Ming Li, Bala Ravikumar, and Kenneth W. Regan 21-1
22 Complexity Classes
Eric Allender, Michael C. Loui, and Kenneth W. Regan 22-1
23 Reducibility and Completeness
Eric Allender, Michael C. Loui, and Kenneth W. Regan 23-1
24 Other Complexity Classes and Measures
Eric Allender, Michael C. Loui, and Kenneth W. Regan 24-1
25 Parameterized Algorithms
Rodney G. Downey and Catherine McCartin .. 25-1
26 Computational Learning Theory
Sally A. Goldman 26-1
27 Algorithmic Coding Theory
Atri Rudra 27-1
28 Parallel Computation: Models and Complexity Issues
Raymond Greenlaw and H. James Hoover 28-1
29 Distributed Computing: A Glimmer of a Theory
Eli Gafni 29-1
30 Linear Programming
Vijay Chandru and M.R. Rao 30-1
31 Integer Programming
Vijay Chandru and M.R. Rao 31-1
32 Convex Optimization
Florian Jarre and Stephen A. Vavasis 32-1
33 Simulated Annealing Techniques
Albert Y. Zomaya and Rick Kazman 33-1
34 Approximation Algorithms for NP-Hard Optimization Problems
Philip N. Klein and Neal E. Young 34-1

2.2 Volume II: Special Topics and Techniques

Preface ix

Editors xi

Contributors xiii

1 Computational Geometry I
D.T. Lee 1-1
2 Computational Geometry II
D.T. Lee 2-1
3 Computational Topology
Afra Zomorodian 3-1
4 Robot Algorithms
Konstantinos Tsianos, Dan Halperin, Lydia Kavraki, and Jean-Claude Latombe 4-1
5 Vision and Image Processing Algorithms
Concettina Guerra 5-1
6 Graph Drawing Algorithms
Peter Eades, Carsten Gutwenger, Seok-Hee Hong, and Petra Mutzel 6-1
7 Algorithmics in Intensity-Modulated Radiation Therapy
Danny Z. Chen and Chao Wang 7-1
8 VLSI Layout Algorithms
Andrea S. LaPaugh 8-1
9 Cryptographic Foundations
Yvo Desmedt 9-1
10 Encryption Schemes
Yvo Desmedt 10-1
11 Cryptanalysis
Samuel S. Wagstaff, Jr 11-1
12 Crypto Topics and Applications I
Jennifer Seberry, Chris Charnes, Josef Pieprzyk, and Rei Safavi-Naini 12-1
13 Crypto Topics and Applications II
Jennifer Seberry, Chris Charnes, Josef Pieprzyk, and Rei Safavi-Naini 13-1
14 Secure Multiparty Computation
Keith B. Frikken 14-1
15 Voting Schemes
Berry Schoenmakers 15-1
16 Auction Protocols
Vincent Conitzer 16-1
17 Pseudorandom Sequences and Stream Ciphers
Andrew Klapper 17-1
18 Theory of Privacy and Anonymity
Valentina Ciriani, Sabrina De Capitani di Vimercati, Sara Foresti, and Pierangela Samarati 18-1
19 Database Theory: Query Languages
Nicole Schweikardt, Thomas Schwentick, and Luc Segoufin 19-1
20 Scheduling Algorithms
David Karger, Cliff Stein, and Joel Wein 20-1

21 Computational Game Theory: An Introduction
Paul G. Spirakis and Panagiota N. Panagopoulou 21-1
22 Artificial Intelligence Search Algorithms
Richard E. Korf 22-1
23 Algorithmic Aspects of Natural Language Processing
Mark-Jan Nederhof and Giorgio Satta 23-1
24 Algorithmic Techniques for Regular Networks of Processors
Russ Miller and Quentin F. Stout 24-1
25 Parallel Algorithms
Guy E. Blelloch and Bruce M. Maggs 25-1
26 Self-Stabilizing Algorithms
Séastien Tixeuil 26-1
27 Theory of Communication Networks
Gopal Pandurangan and Maleq Khan 27-1
28 Network Algorithmics
George Varghese 28-1
29 Algorithmic Issues in Grid Computing
Yves Robert and Frédéric Vivien 29-1
30 Uncheatable Grid Computing
Wenliang Du, Mummoorthy Murugesan, and Jing Jia 30-1
31 DNA Computing: A Research Snapshot
Lila Kari and Kalpana Mahalingam 31-1
32 Computational Systems Biology
T.M. Murali and Srinivas Aluru 32-1
33 Pricing Algorithms for Financial Derivatives
Ruppa K. Thulasiram and Parimala Thulasiraman 33-1

3 Opinion

I think this handbook is an essential resource for any computer science researcher, whether theorist or practitioner. It comes at a price, but the introductory coverage of such a wide range of topics is likely to be useful throughout one's career in computer science. For the moment, it is also a practical way of getting into some of the "hot" areas of the field, and I found the chapters on DNA computing and computational systems biology very welcoming.

One omission from this handbook which I believe could be addressed in a future edition would be a chapter on quantum algorithms. The rapid growth of this field cannot be ignored, and its impact on computing cannot be underestimated as we get closer and closer to transcribing bits on the atomic scale. The efficiency of quantum algorithms, namely the massive parallelism which is... unparalleled by their classical counterparts, makes for an exciting and attractive research proposition. Inclusion of a chapter on this material in a handbook such as this one would make the field more accessible to a wider audience.

All in all, I highly recommend this pair of volumes for inclusion in your bookshelf.

References

[1] Donald E. Knuth. *The Art of Computer Programming*, volume 3: Sorting and Searching. Addison-Wesley Professional, 2nd edition, 1998.

[2] Arvind Narayanan and Vitaly Shmatikov. Robust de-anonymization of large sparse datasets. In *Proceedings of 29th IEEE Symposium on Security and Privacy, Oakland, CA*, pages 111—125, May 2008.

[3] Jan van Leeuwen, editor. *Handbook of Theoretical Computer Science*, volume A: Algorithms and Complexity. MIT Press, 1994.

[4] Jan van Leeuwen, editor. *Handbook of Theoretical Computer Science*, volume B: Formal Models and Semantics. MIT Press, 1994.

Review of [10]

Primality testing and integer factorization in public key cryptography
Author: Song Y. Yan
Publisher: Springer, 2009, 371 pp.
ISBN NUMBER: 978-0-387-77267-7, PRICE: U$ 119.00

Reviewer: S. C. Coutinho (collier@impa.br)

1 Overview

Although public key cryptography was discovered in the 1970s, it did not percolate through the mathematical community until much later. I first encountered it at an Open Day at the University of Leeds in the early 1980s. One of the lecturers had programmed RSA in a computer–which, in those days, meant a mainframe–and one could play with encrypting and decrypting messages. The security, he explained, depended on the difficulty of factoring large numbers. At that time I could never have imagined that ten years later I would be not only regularly teaching CS students about the workings of RSA, but actually using it to buy books over the web.

Public key cryptography, and the RSA system in particular, had some interesting side effects in mathematics. Take, for example, the following statement from §329 of Gauss's *Disquisitiones Arithmeticae*:

> The problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic. (...) Further, the dignity of the science itself seems to require that every possible means be explored for the solution of a problem so elegant and so celebrated.

Ironically it was the Disquisitiones itself, with its treasure of new ideas, that pushed these problems out of the mainstream in number theory for most of the 19th century. Although these problems did not cease to be studied, they passed mostly into the hands of people like Edouard Lucas, who spent his whole life as a teacher of Lycées.

Then came the 1950s. With machines becoming capable of performing computations faster and in greater bulk than people, it would not take long before new algorithms for primality and factorization were developed and implemented. Dick Lehmer and his wife Emma became famous for using ENIAC in the weekends to solve sieve problems. But the real revolution in the area would only come in the 1970s, with the invention of RSA public key cryptography. The first paper to describe this cryptosystem was published by Ron Rivest, Adi Shamir, and Leonard Adleman in 1978. But a description of the method, based on a preprint, had already appeared in 1977 in Martin Gardner's *Mathematical Games* column in Scientific American. This article included a challenge proposed by Rivest, Shamir and Adleman: an RSA encoded message whose public key was a 129-digit integer. To break the message one would have to factor this number into its two prime factors. Rivest estimated that using the methods available at the time, it would take a computer 40 quadrillion years to factor such a large number.

What Rivest could not have guessed was that the cryptosystem he had helped to invent, and the increasing power of computers, would bring back primality testing and integer factorization into

the mainstream of number theory. New and more powerful factorization algorithms were developed and by the 1990s the world wide web had put so many computers online that it became possible to use hundreds of them as a distributed network to factor the 129-digit number and discover that the message said "The Magic Words are Squeamish Ossifrage". Since then the field has kept expanding, and now include two remarkable polynomial time algorithms among its pearls: Peter Shor's quantum factorization algorithm (1994) and the primality test discovered by Manindra Agrawal, Neeraj Kayal, and Nitin Saxena (2002).

Nowadays, the applications of number theory to cryptography go way beyond the factorization and primality problems, to include, among others, the discrete logarithm problem for both finite fields and elliptic curves. Indeed, computational number theory and cryptography are so closely intertwined these days that it is sometimes difficult to know where one ends and the other begins.

2 Summary of Contents

The book under review has four chapters, of which only the last one deals directly with cryptography. The other three are concerned with number theory. Actually, chapter one is something of a miscellany. It opens with a section that is meant to give the reader a taste of some of the more characteristic problems of number theory. This is followed by a summary of the definitions and main results on rings and fields that are used later on in the book. The other sections lead the reader from divisibility properties to elliptic curves including, on the way, such classical topics as arithmetic functions, quadratic congruences and primitive roots. All this in 120 pages!

Although the theme of chapter two is primality testing and prime generation, its first section discusses the cost of algorithms for computing with integers and curves, with the usual emphasis on fast exponentiation. The next section deals with Riemann's ζ-function, Dirichlet's L-function and their relation to primes. Only then do we move to primality tests, not only the classic ones named after Lucas, Pocklington, and Rabin, but also the elliptic curve test and AKS. The latter is based on the polynomial time primality algorithm proposed by Agrawal, Kayal, and Saxena in 2002, which has already been mentioned in the overview. There is also a section on primality tests for special numbers, the best known of which is the Lucas-Lehmer test for Mersenne numbers so successfully used by GIMPS, the *Great Internet Mersenne Prime Search*.

Having learned how to prove the primality of a number for use in ones favorite cryptosystem, we turn in chapter three to algorithms that could be used to break such cyphers. In other words, algorithms for factorization and the computation of discrete logarithms. All the major factorization algorithms are presented, including those based on elliptic curves, continued fractions and the quadratic and number field sieves. There is also a short discussion of Shor's quantum factorization algorithm. The second major topic in this chapter is the *discrete logarithm problem*, that can be formulated for a (multiplicative) cyclic group G as follows:

> Given a generator g of G and any $h \in G$, find a positive integer k such that $h = g^k$.

The number k is known as the *discrete logarithm* of h to basis g. It turns out that in some groups this problem is difficult to solve, among them, the group $\mathbb{Z}_p^*$ of integers invertible module a prime number p and the group of points of an elliptic curve over a finite field. Several algorithms that solve this problem are discussed. Some of these can be applied to any cyclic group, among them Shanks's baby-step/giant step and the Silver-Pohlig-Hellman algorithm. However, the best algorithms work

only in special groups; for $\mathbb{Z}_p^*$ two algorithms are given: Gordon's NFS and the index calculus algorithm. On an elliptic curve, where the discrete logarithm problem seems to be specially hard to solve, one proposal discussed in this book is the *xedni* algorithm of J. Silverman.

The last chapter is the only one that is directly concerned with cryptography. A short introduction to public key cryptography is followed by a detailed discussion of RSA, including questions of security and cryptanalysis. Two other factorization based cryptosystems are presented, Rabin and Goldwasser-Micali. Next come the Diffie-Hellman key exchange protocol, El-Gamal and Massey-Omura encryption, all three of which are based on the difficulty of solving the discrete logarithm problem. The implementation of these algorithms for elliptic curve groups is discussed in some detail. The last three sections of chapter four deal with zero-knowledge techniques, deniable authentication and what has come to be known as post-quantum cryptography; that is, cryptosystems for which no fast quantum algorithm is known.

Each chapter ends with a number of notes on the topics discussed, including suggestions for further reading. The book also contains exercises of varying degrees of difficult, from solving a given system of linear congruences (Problem 1.6.1 on p. 84) to proving or disproving the Riemann Hypothesis (Problem 1.1.1 on p. 11). The bibliography, containing more than 270 items, is very complete and fairly up to date.

3 Opinion

This is the second edition of a book originally published in 2004. The book has been updated and now includes new topics such as the Atkin-Morain elliptic curve test and a brief discussion of Shor's quantum factorization algorithm. The coverage of topics is fairly complete, with all the important algorithms described in some detail. I used it as a reference in preparing lectures for an advanced cryptography course for undergraduates, and it proved to be a wonderful source for a general description of the algorithms. Although the book will be a valuable addition to any good reference library on cryptography and number theory, it has to be used with some caution.

To begin with, it is difficult to determine what its intended readership might be. Although the author felt it necessary to give a formal definition of even and odd numbers (Definition 1.3.2 on p. 24), the whole theory of finite fields is summed up in only 14 lines (p. 18). The discussion of elliptic curves in section 1.9 (p. 113) is very incomplete, and in the description of the number field sieve on p. 243 a factorization in terms of products of prime ideals is performed, without any further reference, even though this topic is not mentioned elsewhere in the book.

The book has also been very poorly copy-edited: it is peppered with misprints. At times the author's opinion seems to be at odds with the evaluation of most mathematicians. Indeed, to say that "[w]hether or not there is an odd perfect number is one of the most important unsolved problems in all of mathematics" seems a bit of an exaggeration.

Summing up, I think that the book will be most useful as a quick reference in the area of primality testing, factorization and their applications to cryptography. It contains descriptions of all the main algorithms, together with explanations of the key ideas behind them. The many misprints make the book harder to use; a corrected reprint would be most welcome.

Review [11] of

Process Algebra: Equational Theories of Communicating Processes
Author: J. C. M. Baeten, T. Basten, and M. A. Reniers
Publisher: Cambridge, 2010
ISBN 978-0-521-82049-3, $83.99, 460pp.
Cambridge Tracts in Theoretical Computer Science, 50

Reviewer: Wesley Calvert (wcalvert@siu.edu)

1 Overview

Process algebra is a rather loose collection of contexts for specifying and verifying distributed and parallel systems. These contexts are based on logic and universal algebra. In short, "processes" are elements of a first-order structure (an algebra) whose language includes such functions as choice, the application of actions, communication between processes, and several others, depending on the context.

The origins of the field, narrowly construed, came in the late 1970's with papers of Milner [5, 6] and Hoare [3], and were attempts to describe the semantics of parallel computation. The systems presented by Milner and Hoare (called CCS — the Calculus of Communicating Systems — and CSP — Communicating Sequential Processes, respectively) were rather different, and other systems have since been proposed. There is some central body of features that all systems seek to capture, and all are closely related.

A typical feature of choice (+) and action application (.) captured by process algebra systems is non-distributivity. If a is an action and x and y are processes — that is, the application of a to one of x and y — is different in an important way from $a.x + a.y$ in when the choice is made. In the latter case, one has committed to a particular side of the choice before executing action a, and in the former case, the choice is delayed.

2 Summary of Contents

The book under review is in the school of the Algebra of Communicating Processes (ACP), a system (to be compared with CCS and CSP) proposed in the early 1980s by Bergstra and Klop [2], and has much in common with its predecessor, [1]. Much is made in both the forewords (by Hoare, Milner, and Bergstra) and the preface of the unification of the various systems in the present book; the preface even claims that it is a successor to the earlier textbooks [7, 4] on other systems. However, one sees only the faintest sketches of this played out in the book, and never systematically. To find an explicit definition of CCS or CSP — or even of ACP — one must go elsewhere.

What one does have here is a detailed and careful exposition of how one narrow family of systems works. The first chapter is mainly bibliographical, but the next two chapters give clear explanations of universal algebra (including conservativity and term rewriting) and transition systems (including bisimulation equivalence), respectively. The first is used throughout the book as a system of syntax, the second as semantics.

The next four chapters form the technical core of the book, developing a large family of theories for processes. A very basic theory is introduced first, and then various enrichments are proposed, including facilities for handling projection, iteration, recursion in various forms, sequential composition, abstraction, and encapsulation, as well as parallel composition with and without communication. Each theory is meticulously compared to those it extends. Elimination and conservativity theorems are proved where possible, and refuted where they are not possible. In the end, we have a system strong enough to specify the Alternating-Bit Protocol for communication — a laborious process, but one which is carried out in some (although not full) detail here as perhaps the central example of the book.

The remaining three chapters describe how to extend the theories to account for timing of several kinds, for process-data interaction, for priority systems, and for probabilistic behavior. A final chapter explores alternate semantic contexts.

3 The Successes of the Book

Perhaps the book's greatest strength will be as a text. It seems an unfortunate situation in the literature that so many different systems are used, often without intentional connection to one another that the usefulness of this book as a reference is limited by its exclusive focus on the ACP family of systems — and at that on the most recent relatives in the family.

As a text, however, the book has considerable strength. The background absolutely necessary of the student is minimal — mostly just some sufficient combination of mathematical maturity and determination. Even the background necessary for the student to comfortably learn from this book is not so much. A student with a background in any two of predicate logic, automata theory, and modern algebra should find the book pleasant reading. The practical meaning of each of the seemingly non-terminating list of axioms is clearly explained, often with catchy and enlightening examples.

There are minor drawbacks. The transparently useful examples are few and difficult — perhaps a feature of the subject. For a long initial segment of the text, the theory of natural number arithmetic seems the primary motivating example. While the reviewer (a mathematical logician by training) appreciated this, students in computer science might not. Moreover, the very number of systems described is daunting. The reviewer took to drawing a score-card in the back cover to track which systems extended which, but even this got exhausting after the first ten systems or so — less than halfway through the book. However, both of these drawbacks can be corrected by a judicious instructor, and the quality of the prose makes this minor effort worthwhile.

References

[1] J. C. M. Baeten and W. P. Weijland, *Process Algebra*, Cambridge Tracts in Theoretical Computer Science no. 18, Cambridge University Press, 1990.

[2] J. A. Bergstra and J. W. Klop, *Fixed Point Semantics in Process Algebra*, Technical Report IW 208, Mathematical Centre, Amsterdam, 1982.

[3] C. A. R. Hoare, "Communicating Sequential Processes," *Communications of the ACM*, 21 (1978) 666–677.

[4] C. A. R. Hoare, *Communicating Sequential Processes*, Prentice-Hall, 1985.

[5] R. Milner, "An Approach to the Semantics of Parallel Programs", in *Convegno di Informatica Teoretica, Proceedings*, Instituto de Elaborazione della Informazione, Pisa, 1973, pages 285–301.

[6] R. Milner, "Processes: A Mathematical Model of Computing Agents," in *Logic Colloquium '73*, North-Holland, 1975, pages 157–174.

[7] R. Milner, *A Calculus of Communicating Systems*, LNCS 92, Springer, 1980.

Review of[12] **of**
Insider Threats in Cyber Security
Edited by Probst, Hunker, Gollman, Bishop
Published by Springer 2010
247 pages

Review by
Kim-Kwang Raymond Choo raymond.choo@fulbrightmail.org

1 Introduction

In our increasingly interconnected world, threats to national security can come from unexpected sources and directions – and this is what one may label as a 360-degree challenge. Cyber attacks are no longer a matter of if but of when, and they are enduring. In recent years, cyber exploitation and malicious activities have grown more sophisticated, more targeted, and more serious (Choo 2011). The Australian Government's Defense Signals Directorate, for example, reported that an average of 700 cyber incidents targeting Defense networks were detected in 2010 – an increase of 250% from 2009 (AAP 2010). More recently in 2011, the parliamentary computers of at least ten Australian Federal ministers including the Prime Minister, Foreign Minister and Defense Minister were reportedly compromised (Benson 2011). The 2010 report to US Congress by the US-China Economic and Security Review Commission also indicated that the number of reported incidents of malicious cyber activity targeting US Department of Defense's system has been on the increase since 2000

Malicious cyber activities can have serious effects on the present and/or future of defensive or offensive effectiveness of a country's national and cyber security. As critical information systems are increasingly dependent on software and are connected to the internet, insider threats will also be of ongoing concern. Threats from insiders can be broadly categorized into two categories:

1. Attacks on behalf of or controlled by an outsider (e.g., zombie computers controlled by bot malware)

2. Self-motivated insider attacks. For example, corrupt insiders could deliberately introduce vulnerabilities during the coding of in-house software that is used to manage sensitive government, military or corporate networks or deliberately introduce vulnerabilities into corporate network. This could allow both state and non-state sponsored actors to exploit the vulnerabilities and surreptitiously enter systems, gain control, and launch online attacks via and against compromised systems (Choo, Smith & McCusker 2007).

Information could also be leaked by insiders – employees and vendors. Recent examples include the high profile incident involving a former US Intelligence Analyst allegedly leaking classified information to Wikileaks (Poulsen & Zetter 2010). A 2009 McAfee study also suggested that data thefts by insiders tend to have a far greater financial impact given the higher level of data access and hence poses a great financial risk to corporations and Government agencies (McAfee 2009).

In order to mitigate cyber criminal risks and make informed decisions about cyber security, it is essential to have a clear understanding of the threat landscape. The importance of looking

ahead to future offending in the online environment was highlighted by Smith, Grabosky and Urbas (2004: 156) who, only eight years ago, noted that crime in cyber space was prone to rapid change and those who fail to anticipate the future are in for a rude shock when it arrives. This edited book provides a timely summary of recent research and development results in this area of insider-related cyber security issues, which, hopefully, will enable the reader to incorporate insider threats into his/her business decision making processes, and identify avenues for risk reduction.

2 Summary

The first three chapters set out to educate the reader about the various aspects of insider threat and attempt to define/explain the problem (e.g., types of insiders, the nature of the problem and types of misuse), and ways in which end users and businesses can seek to mitigate some of these risks. It is refreshing to read about criminology theories being mentioned in this book : Social Bond Theory, Social Learning Theory and Situational Crime Prevention. The latter, as explained in Chapter 3 Insider Threat and Information Security Management, is based on the hypothesis that to commit a crime, an individual requires both motive and opportunity. This is somewhat similar to the Routine Activity Theory which proposes that crime occurs when a suitable target is in the presence of a motivated offender and is without a capable guardian (Cohen & Felson 1979, also see Choo 2011). The theory assumes criminals are rational and appropriately resourced actors that operate in the context of high-value, attractive targets protected by weak guardians (Felson 1998; Yar 2005). In cyber crime, an assumption is that cyber criminals are (1) financially motivated that seek out (2) opportunities provided by cyber space such as anonymity and no geographical limitations, acquire the necessary resources for cyber crime by (inter alia) using delinquent IT professionals and (3) targeting weakly protected systems/networks and exploiting situations where law enforcement agencies are being hampered by jurisdictional, legislative and evidentiary issues, particularly in cross-border cyber criminal cases. The latter also include situations where insider access and knowledge of an organization's vulnerabilities may provide the insiders (including contractors and vendors who are given authorized insider access) the ability and opportunity to bypass physical and technical security measures designed to prevent unauthorized access and carry out malicious activity, if they are properly motivated. Motivations include theft or modification of information for financial gain (such as selling stolen data) and for business advantage (e.g., obtaining information for a new job or starting their own business).

The remaining seven chapters provide general overview of existing fraud detection and insider threat mitigation technologies, outline several challenges from both practitioner and research perspectives, and put forward broad recommendations for future research.

3 Opinion

Overall, this book is an important work for academics, policy makers, and practitioners as it is a step toward a better understanding of the recent research and trends in insider threats, albeit that the contributions are uneven in depth and breadth and some cover familiar ground. I also like the fact that most of the chapters can be read as a stand-alone chapter and readers interested only in specific aspects of insider threats and mitigation strategies can read the respective chapter(s). However, I am somewhat disappointed that the risk of Hardware Trojans is not covered in any breadth or

depth. It is a known fact that state and non-state sponsored actors can exploit commercial joint venture and offshore outsourcing relationships by corrupting insiders to introduce vulnerabilities during the coding of in-house software used in our critical infrastructure systems, or introduce vulnerabilities onto hardware such as IC chips that can be exploited when these hardware are deployed in systems (see Jin & Makris 2010).

References:

1. Australian Associated Press (AAP) 2010. Military Faces Huge Cyber Espionage threat. News.com.au 9 October. http://www.news.com.au/technology/military-faces-huge-cyber-espionage-threat/story-e6frfrnr-1225936268254

2. Benson S 2011. China Spies Suspected of Hacking Julia Gillard's Emails. News.com.au 29 March. http://www.news.com.au/technology/federal-ministers-emails-suspected-of-being-hacked/story-e6frfrnr-1226029713668

3. Choo KKR, Smith RG & McCusker R 2007. Future Directions in Technology-Enabled Crime : 2007-09. Research and Public Policy Series no 78. Canberra: Australian Institute of Criminology. http://www.aic.gov.au/publications/current%20series/rpp/61-80/rpp78.aspx

4. Choo K-K R 2011. The Cyber Threat Landscape: Challenges and Future Research Directions. *Computers & Security* 30 (8): 719–731

5. Cohen LE & Felson M 1979. Social change and crime rate trends: A routine activity approach. American sociological review 44(4): 588608

6. Felson M 1998. Crime and everyday life. New York: Pine Forge Press.

7. Jin Y & Makris Y 2010. Hardware Trojans in Wireless Cryptographic ICs. IEEE Design & Test of Computers January/February issue: 2635

8. McAfee 2009. Unsecured economies: protecting vital information. Santa Clara CA: McAfee

9. Poulsen K & Zetter K 2010. U.S. Intelligence Analyst Arrested in Wikileaks Video Probe. Wired.com 6 June. http://www.wired.com/threatlevel/2010/06/leak/

10. Smith RG, Grabosky P & Urbas G 2004. Cyber criminals on trial. Cambridge: Cambridge University Press Yar M 2005. The novelty of cybercrime: An assessment in light of routine activity theory. European journal of criminology 2(4): 407427