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. **Understanding Cryptography: A Textbook for Students and Practitioners** by Christof Paar and Jan Pelzl. Review by Subhayan Roy Moulick. Apart from the traditional topics expected in an undergraduate level textbook, the book has entire chapters devoted to the discussion of DES and AES cryptosystems. There is also a brief introductory chapter on Elliptic Curve Cryptography.

2. **The Erdős Distance Problem** by Julia Garibaldi, Alex Iosevich, Steven Senger. Review by William Gasarch. The Erdős Distance Problem is the following: given n points in the plane how many distinct distances are there guaranteed to be? We denote this function by $h(n)$. In 1945 Erdős posed this problem and showed $h(n) = \Omega(n^{1/2})$. There has been steady progress on this problem, increasing the lower bound on h. This book presents proofs of most of the results. To do this they go through much mathematics of interest.

3. **Clustering in Bioinformatics and Drug Design** by John D. MacCuish and Norah E. MacCuish. Review by Mohsen Mahmoudi Aznaveh. Drug design can now be done with *lots* of data. How to use this data? This book is about how to do feature extraction, classification, and other operations on data using computational methods.

4. **The Block Cipher Companion** by Lars R. Knudsen and Matthew J.B. Robshaw. Review by Jonathan Katz. Block ciphers serve as fundamental building blocks for much of modern cryptography. This book is, to the reviewer's knowledge, the first book to focus on modern block ciphers. The book is quite thorough, covering block-cipher design principles and cryptanalytic techniques, discussing applications of block ciphers, and providing detailed descriptions of several prominent block ciphers (including DES and AES).

5. **Networked Life: 20 Questions and Answers** by Mung Chiang. Review by Jonathan Katz. This is a rather focused book about Network. How focused? As the title says it asks and answers 20 questions. The math needed for these questions is developed as needed.

6. **Graph Structure and Monadic Second-Order Logic: A Language-Theoretic Approach** by Bruno Courcelle and Joost Engelfriet. Review by Michaël Cadilhac. This book is built around three axes: specification of graphs akin to context-free grammars, efficient model-checking on graphs, and logical description of graphs.

7. **Basic Phylogenetic Combinatorics** by Andreas Dress, Katharina T. Huber. Review by Kipper Fletez-Brant. Phylogenetics is the science of relationships between organisms, as measured by some characteristic, such as gene, genome, RNA or protein sequence. This can be used to tell how close together two organisms are. This may sound like biology, but there is lots of math.

8. **Analytic Combinatorics in Several Variables** by Robin Pemantle and Mark Wilson. Review by Miklós Bóna. Generating functions (in one variable) are a common topic in undergraduate courses in combinatorics. By contrast, generating functions in many variables is very recent topic that began in about the 1990s. This is the first book on the subject. It is not a textbook, but rather a collection of research results of the last 15 years.

9. **The Tower of Hanoi - Myths and Maths** by Andreas M. Hinz, Sandi Klavžar, Uroš Milutinović, Ciril Petr. Review by László Kozma. Most people (including the reviewer and the book column editor) remember the Tower of Hanoi puzzle as something quite simple, interesting mainly as a textbook example of recursion, and as an example of a problem where powers of two appear naturally. In reality, as the book demonstrates, the Tower of Hanoi has a very rich mathematical structure, and as soon as we tweak the parameters we surprisingly quickly find ourselves in the realm of open problems. (The proper name for the problem is *the Tower of Hanoi* not *the Towers of Hanoi*.)

BOOKS I NEED REVIEWED FOR SIGACT NEWS COLUMN

Algorithms

1. *Algorithmics of matching under preferences* By Manlove.
2. *Pearls of Functional Algorithm Design* by Bird.
3. *Jewels of Stringology Text Algorithms* by Maxime Crochemor and Wojciech Rytter.
4. *Tractability: Practical approach to Hard Problems* Edited by Bordeaux, Hamadi, Kohli.

Probability and Combinatorics

1. *Digital Dice: Computational Solutions to Practical Probability Problems* by Paul Nahin.

Misc Computer Science

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

Misc

1. *The Golden Ratio and Fibonacci Numbers* by Richard Dunlap.
2. *A Mathematical Orchard: Problems and Solutions* by Krusemeyer, Gilbert, Larson.
3. *Mathematics Galore! The first five years of the St. Marks Institue of Mathematics* by Tanton.
4. *The king of infinite space: Euclid and his elements* by David Berlinski.
5. *From Zero to Infinity: What makes Numbers Interesting* by Constance Reid.
6. *CoCo: The Colorful history of Tandy's Underdog Computer* by Pitre and Loguidice.
7. *Mathematics Everywhere* Edited by Aigner and Behrends.
8. *An Episodic History of Mathematics: Mathematical Culture Through Problem Solving* by Krantz.
9. *The Logician and the Engineer* by Nahin.
10. *Proof Analysis: A Contribution to Hilbert's Last Problem* by Negri and Von Plato.

Review of[2]
Understanding Cryptography: A Textbook for Students and Practitioners
by Christof Paar and Jan Pelzl
Springer, 2010
372 pages, Hardcover, $40.00

Review by Subhayan Roy Moulick (subhayan@acm.org)

1 Introduction

Cryptography, or more generally cryptology, deals with the study of secrets. The most common form of cryptography is seen as establishing secure communications and verifying authentication. However, modern cryptography is not limited to just establishing secure communication channels, but extends to understanding hard computational problems, to designing secure hardware infrastructure. In short, it lies in the intersection of engineering, computer science and mathematics.

Understanding Cryptography: A textbook for students and Practitioners is an undergraduate level (text)book covering foundational topics in cryptography. Apart from the traditional topics expected in an undergraduate level textbook, in symmetric key and asymmetric key cryptography, hash functions and key establishment, the book has entire chapters devoted to the discussion of DES and AES cryptosystems. Also keeping in par with the latest developments, it gives a brief introductory chapter on Elliptic Curve Cryptography.

Each chapter begins by stating the goals and motivation of the chapter. It then introduces the broad topic and goes on to talk about the definitions. Every chapter contains a significant portion, discussing implementation and security features and possible flaws and attacks. Finally, with a summary, further references and (fun) exercise problems conclude the chapter.

The book assumes no prior background in cryptography or advanced mathematics and is targeted towards undergraduate classes and beginning graduate classes. The main focus of the book has been on practical cryptography and the authors often omit aspects related to theoretical foundations in cryptography. However, the math requirement is minimal, and the chapters give necessary and sufficient mathematical understanding required to continue with the materials. The math here is discussed in the the chapters, and not through an appendix.

While there are many textbooks written in the area, this book takes a different approach and tries to emphasize the practical aspects. The book has a rather ”lecture notes” type tone and typography, that makes it easy to follow. The book is very much approachable and while this book can be easily used to introduce cryptography to engineers, it may not suffice mathematicians.

Also, the accompanying classroom-based lecture videos (available in English and German), recited by one of the authors of the book, Prof. Christof Paar, can be found on the book's website. These lecture videos are closely based on the book and are accessible to anyone with internet access (and not just the buyers of the book).

2 Contents

Understanding Cryptography consists of 13 chapters. *Chapter 1* introduces the reader to the classical world of cryptography and reason why classical cryptography is not secure.

Symmetric Key cryptography is covered in Chapters 2-5. Chapter 2 (Stream Ciphers) starts out by defining stream ciphers. It then discusses about Pseudorandom Generators and goes on to talk about two important constructions of Pseudorandom Generators - LFSR and Trivium. Chapter 3 talks about the DES (Feistel Cipher) and presents a nice overview of the construction, security and implementation details. The next chapter, Chapter 4, talks about AES. It starts with a brief introduction to concepts in Galois Fields. It then gives the internal structure of the current AES (Rijndael), and ends with a brief discussion on the implementation details. Chapter 5 discusses different modes of operation with block ciphers and concludes with a brief exploration of encryption techniques used in practice.

Public Key Cryptography is introduced through chapters 6-8. Chapter 6 gives an overview of public key cryptography and gives a self contained manual on number theory concepts that is used in the later chapters. Chapter 7 studies the RSA cryptosystem while talking about practical aspects of implementing and attacking the system. Chapter 8 introduces Public Key Cryptosystems that are based on the discrete log problem and includes discussions on Diffie Hellman key exchange and encryption using Elgamal scheme.

Elliptic Curve Cryptosystems are given in chapter 9. The chapter gives a good introduction to elliptic curves and gives a brief tutorial on realizing the discrete log problem with elliptic curves and using it for DH key exchange. Unlike the earlier chapters, this chapter mainly tries to motivate ECC, and lacks many technical details. However, this is a good starting point to study elliptic curve cryptography.

Digital Signatures Hash Functions and MACs are discussed through chapters 10-12. Chapter 10, is on Digital Signatures and starts out by motivating the problem. It then presents the ideas behind digital signatures using RSA, Elgamal and Elliptic Curve Digital signature scheme (ECDSA). It also gives the standardized Digital Signature Algorithm (DSA) and the desirable key sizes. Chapter 11, discusses the motivation and security requirements of Hash Functions and gives a high level overview of the MD4 hash function family and a more detailed overview of the computation and implementation of the SHA1 hash function. Chapter 12 briefly talks about Message Authentication Codes - on principles and constructions from Hash Functions and Block Ciphers.

Key Establishment, in chapter 13 gives a quick overview of key establishments using symmetric key and public key Techniques. It also gives several protocols and attacks, in practice, that the parties exchanging keys often incur.

3 Additional Learning Materials

Classroom based video lectures taught by one of the authors of the textbook, Dr. Paar, can be found on the book's website. These lectures are available both in German and English (and are accessible to everyone, and not just to the ones who purchased the book!). I followed the English version, and will be commenting on the same.

One of the nicest things about the lectures were how well synchronized they were with the book. While they were not a session of reading straight out of the book, the lectures were mostly discussions based on the chapters from the book. For a first course in cryptography, these lecture videos were well paced and very lucid and easy to follow. Dr. Paar also has an excellent way of teaching and I enjoyed his recitations and his occasional *"everybody wake up"* and *"okay go back to sleep now"* notifications before and after important parts of the day's discussion.

I strongly felt the video lectures (without or without the book) can be used as an excellent source for a self study course for anyone who wants to understand cryptography.

4 Opinion

The book left a good impression with me. Although often, while reading, I craved for more formal definitions and mathematical rigor in the content, I cannot complain much about it, given the authors did admit their goals of introducing practical cryptography.

The book is very much self-contained and anyone with *some* background in science or engineering can follow the book. Also the chapters are not exactly dependent on each other and one can jump between the chapters without a lot of difficulty. I felt the authors with their precise English definitions and diagrams tried to deliver the essential ideas of security. The authors did not solely rely on definitions, but often, after introducing the fundamentals, went on to talk about the constructions to explain what's really happening *under the hood*.

The book, as stated earlier, can be used as a self study book. It may be worthwhile to note that the while this book will perhaps not take a student to a level of competence to follow papers from top conferences in crypto, it will however develop a sound foundation in crypto and security. On mastering the content, the reader will have a fairly good knowledge on implementation of protocols and be able to reason about side channels and other common pitfalls in cryptography.

To sum it up, this textbook gives an amalgamated perspective of an engineer and cryptographer to a reader. While most textbooks in this area try to introduce the reader to the subject matter with formal arguments, and emphasize on the math behind them, I found this textbook tied to convey the major ideas and talk *about* them. I would recommend the textbook (and the wonderful video lectures) to anyone who is looking for a (self study) book for a first course in cryptography and has little or no math background.

Review of

The Erdős Distance Problem [3]

by Julia Garibaldi, Alex Iosevich, Steven Senger

Publisher: American Math Society

$24.00 Paperback, 2010, 150 pages

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

1 Introduction

(All of the papers mentioned in this review are available at www.cs.umd.edu/~gasarch/erdos_dist/erdos_dist.html)

The following problem was posed by Erdős in 1946: Given n points in the plane how many distinct distances are there guaranteed to be? We denote this $h(n)$. Erdős showed that $\Omega(\sqrt{n}) \leq h(n) \leq O(\frac{n}{\sqrt{\log n}})$. The lower bound could be on a High School Math competition. The upper bound is from the $\sqrt{n} \times \sqrt{n}$ grid and requires some number theory to prove. Moser and Chung and this book attribute to Erdős the conjecture that $(\forall \epsilon)[h_n \geq n^{1-\epsilon}]$. This conjecture is not in Erdős's paper; however, it is likely he gave it in lectures.

There has been considerable progress on this problem over the years. Some of the progress has come from geometry and some from pure combinatorics. This book gives proofs of many improvements to the bound on $h(n)$. This book also has material on other metrics, the problem in d-dimensional space, and the problem over finite fields.

Has the problem been solved? The last result on the Erdős Distance Problem in this book is $h(n) \geq n^{\frac{48-14e}{55-16e}}$ which is approximately $n^{0.864137}$. The book then goes on to show why the methods used to obtain that result cannot be extended. Right before the book went to press Katz and Guth showed $h(n) \geq \Omega(\frac{n}{\log n})$, which solved the conjecture (though note that we still have the gap $\Omega(\frac{n}{\log n}) \leq h(n) \leq O(\frac{n}{\sqrt{\log n}})$). This should makes this book *more interesting* to people in TCS. In TCS we have proven results like "such-and-such technique won't suffice to crack P vs NP" and take this as evidence that P vs NP is hard. For the Erdős distance problem they also proved that "such and such techniques won't suffice" but they *cracked the problem anyway!* To be fair, P vs NP seems much harder than the Erdős Distance Problem; however, it still makes one pause. More to the point, having an example of a barrier result, and then how it was overcome, is interesting. Hence I recommend the reader read this book *and* then go read the Katz-Guth paper.

Moreover, the mathematics in this book is often of independent interest. For example, the Szemerédi-Trotter theorem on incidences in the plane and the crossing lemma for graphs are proven and used in this book; however they have many other applications.

[3] William Gasarch ©2014

2 Summary of Contents

The first two chapters introduce the problem, give Erdős's proof that $h(n) \geq \Omega(\sqrt{n})$, and Moser's proof that $h(n) \geq \Omega(n^{2/3})$. These proofs are both geometric. The third chapter proves the Cauchy-Schwartz inequality and gives some applications.

The fourth chapter proves the following two theorems that is uses as Lemmas.

1. The Crossing Lemma for graphs: If a graph has n vertices and $e \geq 4n$ edges then the number of crossings is at least $\Omega(\frac{e^3}{n^2})$.

2. The Crossing Lemma for multi-graphs: If a multigraph has multiplicity $\leq m$, n vertices and $e \geq 5mn$ edges then the number of crossings is at least $\Omega(\frac{e^3}{mn^2})$.

3. The Szemerédi-Trotter theorem on incidences in the plane: For an set of P points and L lines in the plane the number of incidences of points on lines is at most $O(P + L + (LP)^{2/3})$.

These are both used in the fifth chapter to obtain better lower bounds on $h(n)$. Just using the crossing lemma for multigraphs you can obtain $h(n) \geq \Omega(n^{2/3})$ approximately $\Omega(n^{0.67})$. which, alas, we already have. But if you also use the Szemerédi-Trotter theorem then one can obtain $\Omega(n^{0.8})$. This is a result of Székely. This is a very nice proof since you translate the problem to one in pure combinatorics and then solve it there with the crossing lemma.

The sixth chapter proves $h(n) \geq \Omega(n^{6/7})$ (note that $6/7$ is approximately 0.8574). This is a careful argument involving taking, for each point p, THREE points that p_1, p_2, p_3 such that $|p - p_1| = |p - p_2| = |p - p_3|$. The seventh chapter extends the argument to FIVE points. More than that, this chapter casts the $n^{6/7}$ argument in a new light (same proof, different way of looking at it) so that one sees how you could *try* to generalize it. The better results depend on theorems from pure combinatorics. Here is the key combinatorial question they tackle: Given k find a small α_k such that the following holds: for all an $M \times k$ matrices of distinct elements, if S is the set of pairwise distinct sums of entries of A in the same row, then $M \leq O(S^{\alpha_k})$. Gabor Tardos obtained, for $k = 5$, $\alpha = 11/4$ which yields $h(n) \geq \Omega(n^{44/51})$ (approximately $n^{0.8627}$, using sets of FIVE points. Katz and Tardos later obtained $k = 5$, $\alpha = 19/7$ which yields $h(n) \geq \Omega(n^{19/22})$ (approximately $n^{0.8636}$. The best result using these techniques (and higher values of k), also due to Katz and Tardos, is $h(n) \geq n^{(48-14e}55 - 16e$ which is approximately $n^{0.864137}$ (the proof of this is not presented). The book then gives a proof by Imre Ruzsa that, using these techniques, this result is optimal.

The seventh chapter is about information theory. What does information theory have to do with the Erdős distance problem? Using information theory one can obtain results like the ones above about matrices.

3 Opinion

Hypothetically anyone could read this book. Virtually all of the math that you need is in it. But of course there is the issue of *Mathematical Maturity*. A good Junior Math major should be able to read and understand most of the book, though some parts will be tough going. The authors leave

many of the results for the exercises. This makes the book harder to read but this does force you to be involved.

Is the Erdős distance problem a good problem? Yes. Hilbert said that a good math problem *should be difficult in order to entice us, yet not completely inaccessible lest it mock our efforts*. The interesting mathematics that has been applied to it, and come out of, make it enticing. The steady progress shows that the problem does not Mock our efforts some do (Collatz Conjecture-I'm talking about you!)

Is this the book to read on the problem? The sarcastic (and unfair) answer is *yes, because its the only one*. However, in absolute terms this is a good book on the problem and will take the reader through much math of interest.

Review of[4] of
Clustering in Bioinformatics and Drug Design
by John D. MacCuish and Norah E. MacCuish
CRC Press, Taylor and Francis Group, 2011
244 pages, Hardcover, $75.00, Kindle $75.00

Review by Mohsen Mahmoudi Aznaveh (mahmoudi.mohsen@gmail.com)

1 Introduction

Classification plays an important role in drug discovery. Biology experts classify molecules based on their own experience. As the amount of data increases this will no longer work. Nowadays there is a huge amount of data in biology. Feature extraction and classification are the first steps to design or discover new drugs. Computational methods are one of the powerful techniques both for these problems. This book is about classification techniques which are used for drug discovery and design.

2 Chapter 1

Chapter 1 begins with the history of quantitative methods used in drug discovery. Clustering and classification use different tools; using the right features, or amalgamating the important features, can lead us to a good classification.

Machine learning has two types of problems which appear in bioinformatic: supervised learning and unsupervised learning. Supervised learning exploit labeled data and introduce clusters which can be used in further prognostication. Unsupervised learning is the method of using unlabeled data to classify the data into different clusters which show their relevance and also can be used for regression problems.

This chapter also depicts a brief statement about drug discovery and its process and discusses fundamental computational complexity classes and parallel algorithms.

3 Chapter 2

Chapter 2 is about different data structures and criteria using in bioinformatics. The chapter categorize them into four basic data types: 1)binary data, 2)ordinal(count) data 3) continuous data and 4) categorical data.

Binary data is a set of standards approved by chemists or biologists and are widely used. WLN, SMILES and InChI are some examples of this type. WLN or Wiswesser Line Notation contains an ASCII string with a defined standard that manifest a certain molecule. SMILES, also uses

ASCII characters. For instance, a caffeine string is c12c(n(c(n(c1=O)C)ncn2c. Each standard developed for some certain use. The free software OpenBabel can be used for converting chemical file formats. Obviously a one type must have enough information to be converted into a certain format.

Count data are common in many fields. They are discrete and have their own standards in computers. Continuous data is also one of the other common data types in many fields. Note that precision is one of the important factors in this type when represented in computer. Categorical data are the data which has certain amount of types. There are also Mixed data types which is a combined form of different types. Comparison is one of the main reason of measuring. Some different measuring criterion is exemplified in this chapter. Tanimoto or Jaccard, Baroni-Urbain coefficient, Hamann measure and some other binary measures has been exemplified in the book. There are some common measures for other types that the book mentioned briefly.

4 Chapter 3

Chapter 3 is about two main clustering algorithms: partitional and hierarchical. This techniques that use unsupervised learning methods are explained with pseudo code. Some side aspects have also been covered in this chapter like Overlap in clusters, Fuzzy clustering and Hybrids. Hierarchical models is made based on a top-down or bottom-up tree design. Clusters can be made by cutting the tree. Partitional approach is using multi level partitioning and making new subset. The famous algorithm K-means methods are categorized as partitional algorithm and its pseudo code is also given.

5 Chapter 4

Chapter 4 is about different partitional algorithms. The main algorithm is K-means which is shown with different assumptions. K-means is an iterative algorithm which tries to find K different clusters in the data (in which K is predefined). Each iteration entails two phases: centroid movement and cluster determination. These two phases are done respectively. K random points are generated in N-dimensional space, where N is number of features. K points with their Voronoi diagram specify K clusters in the space. Each cluster centroid is moved based on points in their cluster. This process is done iteratively till the centroids do not need any location displacement.

This method may have some drawback for certain use. So there are many assumptions to improve this algorithm. K-Medoid and K-Modes are two examples in this chapter.

6 Chapter 5-7

Chapter 5 is about cluster sampling algorithms. Data collation and management lead us to have huge amount of data in this field. So, sampling seems a necessary process for some applications.

Chapter 6 is about hierarchical algorithms, which is a more incisive explanation in this part. Chapter 7 covers hybrid algorithms which exploit both partitional and hierarchical algorithms. Divisive hierarchical K-means and Exclusion region hierarchical are two examples. Then, Biclustering as a feature selection algorithm came at the end of 7th chapter.

7 Chapter 8-11

Chapter 8 titled Asymmetry and about the asymmetric relation in bioinformatic problems and how to address them. Asymmetric relation can make the algorithms much more complex.

Chapter 9 is about ambiguities might happen in computational biology ecosystem. Precision, data duplication and chemical notations may make some ambiguities that must considered carefully.

Chapter 10 is about clustering validation. Some numerical measures are in this part, plus graphical intuition.

The last chapter is about parallel algorithms. In this chapter some of the algorithms mentioned earlier is shown and the way they could be parallelized is also debated.

8 Opinion

The titles of each chapter are well chosen but the book seems to be a little bit incoherent. The subject is one of the most compelling subjects today and the lack of such a book is perceptible. Early chapters are well written, though still hard to follow. The main problem is that, throughout the book, the descriptions of the problems are hard to follow. For someone who already knows machine learning and some computational biology this is not an issue; however, to a beginner, this is an impediment to reading.

If someone already has the background this is a good book. However, for these people, the author should state the open problems. There are many of them since this is a relatively new field.

Review of
The Block Cipher Companion
by Lars R. Knudsen and Matthew J.B. Robshaw
Springer, 2011, Hardcover, $50.00, 214 pages

Review by Jonathan Katz
Dept. of Computer Science, University of Maryland

1 Overview

Block ciphers serve as fundamental building blocks for much of modern cryptography. They are used extensively in practice for (symmetric-key) encryption, and to a lesser extent for message authentication. Specially designed block ciphers can also be used to construct hash functions, as has indeed been done for, e.g., the SHA family of hash functions. Block ciphers can be used for pseudorandom number generation, as part of challenge/response protocols for entity authentication, and for defining a random-looking mapping between elements. In short, they are both incredibly useful and truly ubiquitous.

Several specific block ciphers are also among the most well-known cryptographic primitives. The block cipher DES (the Data Encryption Standard) was perhaps the first modern cryptographic algorithm—it predates RSA—and is certainly one of the earliest to be standardized. Developed in the late '70s, DES served as a cryptographic workhorse for over 20 years and is still used today in the strengthened form of triple-DES. The Advanced Encryption Standard (AES), the modern replacement for DES, was designed by public competition in the late '90s and is in widespread use today. DES and AES are among the most heavily analyzed cryptographic algorithms we have.

At the most basic level, a block cipher F is an efficiently computable, keyed permutation. That is, F is a function $F : \{0,1\}^n \times \{0,1\}^\ell \to \{0,1\}^\ell$ where the first input serves as a key, and we let $F_k(x)$ denote $F(k,x)$. The fact that F is a permutation means that for every key k the function $F_k : \{0,1\}^\ell \to \{0,1\}^\ell$ is a bijection; moreover, F_k^{-1} should be efficiently computable (given k). From a theoretical cryptographer's point of view, the main security property of a block cipher is that it that should be indistinguishable from a random permutation. A formal definition is somewhat involved, but informally we imagine an attacker interacting with a "black box" that either computes $F_k(\cdot)$ for an unknown, random key k, or that computes $f(\cdot)$ for a permutation chosen uniformly from the set of permutations on $\{0,1\}^\ell$. The block cipher F is *secure* if no efficient attacker can distinguish between these two possibilities with probability significantly better than random guessing. (The book under review—which takes a practical perspective—leaves this notion of security informal and does not focus on it too much. In practice, block ciphers are often required to satisfy even stronger security properties.)

The Block Cipher Companion is, to my knowledge, the first book to focus on modern block ciphers. The book is quite thorough, covering block-cipher design principles and cryptanalytic techniques, discussing applications of block ciphers, and providing detailed descriptions of several prominent block ciphers (including DES and AES). The contents of the book are discussed in more detail in the section that follows.

2 Contents

The book opens with a brief introductory chapter discussing cryptography at a high level, and introducing the notion of block ciphers. Different attack models are also presented. The formal definition above, where an attacker has "black-box" access to $F_k(\cdot)$, corresponds to what is called a *chosen-plaintext attack*. (As a side note, this terminology is accurate but unfortunate since block ciphers are not encryption schemes and can be used for things other than encryption. But it is impossible to fight terminology once it becomes standard.) One could also consider weaker *known-plaintext attacks*, where the attacker is given pairs $(x, F_k(x))$ with the x's outside the attacker's control, or stronger *chosen-ciphertext attacks*, where the attacker also has black-box access to $F_k^{-1}(\cdot)$. I found particularly interesting the footnote showing how chosen-plaintext attacks were actually used by the British during World War II.

Chapter 2 describes DES and triple-DES in full detail. Most of the chapter is not particularly interesting unless one happens to be specifically interested in byte-level details of DES, though there is a brief section on *Feistel networks*, a design template for ciphers in general, as well as a discussion of design principles for certain components of DES. The block cipher AES is featured in a similar level of detail in Chapter 3. One nice feature of the book, especially important in these chapters, is that it tabulates the best known attacks against the ciphers, along with relevant references to the literature. This makes the book a great starting point for anyone interesting in studying DES/AES.

Chapter 4 focuses on applications of block ciphers to encryption, message authentication, and hashing. While I can understand why the authors included this chapter, I have to say that I found it disappointing since this material is already available, in greater depth, in any good textbook on cryptography.

Chapter 5 begins a sequence of chapters dealing with basic block-cipher cryptanalysis. The first of these chapters covers "brute-force" attacks that can perform better than a trivial exhaustive key-search attack. Covered here are Hellman's time/space tradeoff, which shows how to use preprocessing (and a significant amount of memory) to improve the time complexity of a key-recovery attack once an attacker is given access to a cipher. The chapter also includes a description of the classic meet-in-the-middle attack which can be used to attack composed ciphers (such as triple-DES).

The following two chapters were the highlight of the book for me. In clear prose and several worked out examples, the authors provide a near-perfect explanation of the basic elements of differential and linear cryptanalysis. These methods, developed in the late-'80s and early-'90s, led to the first successful attacks against DES, and have become a standard part of the cryptanalyst's toolbox ever since. Chapter 8 concludes the main technical portion of the book with some more advanced details related to differential and linear cryptanalysis, along with a brief discussion of design principles intended to counter such attacks.

The book concludes in Chapter 9 with a discussion of ciphers besides DES and AES. These include the other finalists of the AES competition, all of which were judged to be secure at the conclusion of the competition, along with some prominent historical examples (some of which have been broken) such as FEAL and IDEA.

At the end of each chapter, the authors include a fairly detailed guide to the research literature for readers interested in learning more about some particular topic.

3 Recommendation

The Block Cipher Companion is a highly readable account of block ciphers. I found the book an absolute joy to read, and it was evident that a lot of care had been taken by the authors in their selection of topics and care in the presentation. Judged as a whole, the book is simply fantastic!

On the negative side, I have already noted above that I would have omitted Chapter 4, though it is not a big deal either way. Perhaps more critical is the organization of the topics. Personally, I might have organized them differently; I found it a bit strange, for example, that bit-level descriptions of DES and AES preceded any broader discussion of block-cipher design principles.

A bit closer to my own area of interest, I would have liked to see in the book a bit more of an appreciation, and coverage of, the complexity-theoretic perspective of block ciphers. (I say this even as I fully understand that the intention of the book is to serve as a practical guide and *not* another complexity-theoretic treatment.) As two examples that stuck out to me: I missed seeing any formal discussion of the notion of pseudorandom functions and strong pseudorandom functions, and I felt that the Luby-Rackoff proofs of security for 3- and 4-round Feistel networks should have been given more prominence. Perhaps the authors felt that these topics are already covered elsewhere. (Full disclosure: these topics are treated in my textbook *Introduction to Modern Cryptography*.)

Notwithstanding the minor quibbles above, I highly recommend this text to anyone looking to learn more about the subject. It could easily be used to teach a graduate-level seminar, or even as part of a graduate class on cryptography more broadly. It would also serve well as a text for self-study by graduate students and researchers.

Review of
Networked Life: 20 Questions and Answers
by Mung Chiang
Cambridge University Press, 2012
Hardcover $40.00, Kindle $21.00, 503 pages

Review by Jonathan Katz
Dept. of Computer Science, University of Maryland

1 Overview

Everyone—or at least anyone who uses the Internet—is impacted daily by networking technologies, whether through their use by companies such as Google, Netflix, or Facebook or in the Internet backbone itself. Scratching the surface of these technologies just a little bit, one finds great ideas from theoretical computer science underlying many of them. These applications thus provide a great "hook" by which to interest students in the field of computer science in general, or theoretical computer science in particular.

Networked Life uses these technologies that we are all familiar with to motivate the material it covers. As a textbook, it is unusual in several respects. First, it is organized around *questions*—20, to be exact—rather by "answers." That is to say, each of the book's 20 chapters focuses on a question that any curious person might raise (e.g., "How does traffic get through the Internet?"), and develops the necessary background and mathematics needed to address that question. As a consequence, material on, say, game theory is not developed in one place but is instead spread across several chapters throughout the book. The book is also written in a conversational style; moreover, each chapter is divided into sections containing a short answer to the relevant question, a longer answer, and then advanced material. Whether this works or not depends on the reader and (for this reader, at least) on the question being addressed as well.

The following provides a taste of some of the questions addressed in thus book, with additional comments in parentheses about what technical material each one corresponds to:

- How does a distributed system of wireless transmitters/receivers agree on a set of power levels that will allow them all to communicate without too much interference? (Linear algebra; game theory and linear programming are introduced as well though not really used.)
- How do auctions work? (Game theory, algorithmic mechanism design.)
- How are webpages ranked? (The Pagerank algorithm, linear algebra.)
- How do recommendation systems work? (Convex optimization, machine learning.)
- How are user ratings aggregated? (Statistical estimation, AdaBoost.)
- How do voting systems work? (Voting theory, Arrow's impossibility result, game theory.)

- How do networks influence technology adoption? (Feedback, synchronization, network-influence models, network centrality measures.)
- How are networks formed, and what effects does this have? Generative graph models, the "small-world" phenomenon, scale-free networks.)
- How are services priced, and how should they be priced? (Game theory, microeconomics.)
- How are packets routed through the Internet? (Networking, routing protocols, shortest-path algorithms, congestion control.)
- Is network allocation fair? (Game theory, axiomatic fairness measures.)

2 Examples

To give a better sense of what the book is like, I discuss two representative chapters in detail.

2.1 Chapter 1: What Makes CDMA Work?

The central question addressed here is how a distributed collection of wireless transmitters and receivers can adjust their power levels so that they can each communicate effectively without too much interference. The "short answer" that leads off the chapter discusses the general setup of cellular networks and then mentions FDMA, TDMA, and CDMA with (what I found to be) insufficient explanation. Strangely, these topics are then dropped in the "long answer" and "advanced material." Instead, the chapter transitions into a discussion of the distributed power control (DPC) algorithm, which allows transmitters to iteratively adjust their transmission power so that they each achieve a desired Signal-to-Interference Ratio (SIR), when possible. The algorithm itself is explained in detail in the "long answer" section, where the problem is also recast as a linear-programming problem as well as one of finding a game-theoretic equilibrium. This is followed by a fully worked out example, which was helpful. Finally, the "advanced material" provides a short proof of convergence for the DPC algorithm.

While I found the chapter enjoyable to read, I also found several aspects of it puzzling. The main question left in my mind is how the desired SIR levels are set by each transmitter; it would seem to me that each transmitter would prefer as high an SIR as possible? Of course, this would require using more power, but since no cost for using power (or, for that matter, utility for achieving a given SIR) was defined, it is difficult to say whether this would be a net win. I also found the repeated linear-programming formulation and game-theoretic motivation somewhat out-of-place, though I guess these were put here primarily to set the stage for later chapters. Finally, I wish the FDMA, TDMA, and CDMA approaches were fleshed out more fully.

I was also left a bit confused about the prerequisites for this book (which were never specified in the preface). Although not strictly necessary to follow the chapter, the material seems to

assume some knowledge of physical-layer terms like channel gain and interference that an average computer-science student might not have. The advanced section uses the term "eigenvalue" without comment, as if every undergraduate majoring in a technical field would be familiar with it.

2.2 Chapter 9: Are There Really Six Degrees of Separation?

This chapter takes up the question of why networks have short average distances between nodes, and how such paths can be found efficiently. The "short answer" section describes Milgram's famous experiment from 1967, and then introduces the idea of the *clustering coefficient* of a graph. (Roughly, this is a measure of the fraction of times two nodes who have an edge to a common node also have an edge between themselves.) The "long answer" introduces the Erdös-Renyi random-graph model as well as the Watts-Strogatz model which, with its mix of short-range and long-range links, more successfully captures real-world social networks. It also briefly touches on Kleinberg's work proposing another model along with a (local) algorithm that could be used to find short paths within that model. The "advanced material" calculates some properties of the Watts-Strogatz model, and also considers a generalized model

Again, the material covered here was fascinating but there were a few holes. There was no discussion of how well real-world networks match any of the models that were introduced. Also, Kleinberg's model and others include a notion of "dimension" that is fine for rings and meshes, but works less well when talking about a social network; this disparity was never addressed.

3 Recommendation

This book is aimed at juniors or seniors in electrical engineering or computer science, but is structured so that it could be enjoyed by a bright first-year undergraduate or someone with a mathematical bent but no prior training in those fields. The book does a fantastic job of motivating the material and presenting it in a compelling way; it also strikes an incredible balance between theory and applications. I would heartily recommend it to anyone who is already intrigued by the 20 questions in the book, or as a gift to inspire someone to become interested in those questions.

Although the book has been used successfully as a textbook in an undergraduate class at Princeton, as well as in an on-line course, I question whether I could teach a class based on it. My sense is that the book would have to be supplemented with a lot of external resources. It may work best as a supplemental text of its own in courses on Networking, Algorithms, or Game Theory.

Review of[5]
Graph Structure and Monadic Second-Order Logic
A Language-Theoretic Approach
by Bruno Courcelle and Joost Engelfriet
Cambridge University Press, 2012
728 pages, hardcover, $160.00

Review by
Michaël Cadilhac michael@cadilhac.name
Wilhelm-Schickard-Institut für Informatik, Universität Tübingen

1 Introduction

This book is built around three axes: specification of graphs akin to context-free grammars, efficient model-checking on graphs, and logical description of graphs. The study is motivated by two classes of "context-free" sets of graphs: the HR (Hyperedge Replacement) and VR (Vertex Replacement) equational sets. Those sets are linked to two important complexity measures on graphs which are used to devise fixed-parameter tractable algorithms for monadic second-order (MSO) model-checking. The book focuses on the interplay between algorithmics, algebra, and logic on graphs, and does so in a very detailed, precise, and exhaustive way. Statistically speaking, there is roughly one theorem (or proposition, etc.) and 9 cross-references per page. The book contains no exercises but an extensive list of open problems.

2 Summary

One great didactic value of the book is its first chapter, which constitutes an extended survey (2^6 pages) of the book's matter. This chapter helps a lot in making the book pleasant to read. It lays down the structure of the following 600 pages in a very accessible, illustrated, and clear way, hence making both skimming and exhaustive reading of the remainder of the book more natural. This chapter has a similar content to a survey written by Courcelle in 1997.

Chapter 2 presents the two graph algebras that will be the main focus of the book. Both are motivated by a generalization of context-free grammars to graphs, with different generalizations of concatenation on words. These are (1) the *HR graph algebra*, consisting of injectively and partially labeled graphs, built from trivial graphs by identifying nodes with the same labels, and (2) the *VR graph algebra*, consisting of labeled simple graphs, built from trivial graphs by adding edges between nodes with given labels. As equational ("context-free") sets, HR graphs correspond in a precise sense to bounded tree-width graphs, and, as a more artificial yet still natural counterpart, VR graphs correspond to a measure called *bounded clique-width*. It is still open whether this

[5] ©2014, Michaël Cadilhac

measure has an independent combinatorial characterization. Those two width measures will lead to fixed-parameter tractable algorithms for MSO problems on graphs.

Chapter 3 deals with many-sorted algebras in a more general context. Their equational and recognizable ("regular") sets are studied, hence laying the ground for the study of such sets for the HR and VR graph algebras. Within this general framework, terms and automata on terms (tree automata) are introduced. The classical result that context-free languages are preserved under intersection with regular languages carries through in this setting.

Chapter 4 studies the {equational, recognizable} sets of graphs of the {HR, VR} algebras. Decidability results are presented, and the links between HR-equationality and tree-width on the one hand, and VR-equationality and clique-width on the other hand are made precise. Some equivalents of the Myhill-Nerode theorem for the recognizable sets are shown. Connecting HR and VR, it is shown that HR-equational sets of simple graphs are VR-equational, and that the converse holds for sparse graphs (a similar result holds for recognizable sets, but in the opposite direction).

Chapter 5 introduces MSO logic, and shows a variant of Büchi's theorem on the equivalence of MSO and recognizable. More precisely, MSO-definable sets of graphs are VR-recognizable, and if quantification on the set of edges is allowed, they are HR-recognizable. This in turn implies the decidability of MSO satisfiability for the set of graphs of tree-width and clique-width at most k, for each k. The chapter is placed in a more general framework.

Chapter 6 develops fixed-parameter tractable model-checking algorithms, with tree- and clique-width as parameters, for graph properties specified by MSO formulas. Of particular interest are alternative proofs of previous important theorems, leading to a better algorithmic understanding of the results.

Chapter 7, a very important chapter, focuses on MSO transductions, i.e., graph transformations specified by MSO formulas. One of the main results in this line is that a set of graphs is VR-equational iff it is the image of the set of trees under an MSO transduction; a similar characterization exists for HR-equational sets, thus emphasizing the strong links between the two formalisms. Some consequences on the decidability of MSO satisfiability and on the logical characterization of recognizability are given.

Chapter 8 considers MSO transductions of terms (trees) and words. In particular, implementations of such transductions with finite-state transducers are presented (relying on two-way transducers for words, and compositions of tree-walking transducers — and other devices — for terms). This leads to automata-theoretic characterizations of the VR-equational sets of terms and words.

Chapter 9 is about more general relational structures, and strives to generalize the preceding results, in particular algorithmic results, to that setting — some of them being already presented in previous chapters for the algebra of all relational structures. Considering the incidence graphs of relational structures, the results about graphs of bounded tree-width and MSO are generalized. Going further, a new complexity measure generalizing clique-width is introduced, leading to important open questions.

The book is concluded with an opening on the future, including an extensive list of open problems.

3 Opinion

This book is an impressive work, in that it is precise yet didactic, and extensive yet focused.

The prospective reader should have a good understanding of formal language theory, some knowledge on tree automata, and a ground basis of logic. I believe this is a necessary *and sufficient* basis to be interested in this book. Anyone to which the title sounds interesting could (should) read Chapter 1 (the overview) and the Conclusion. This gives a broad picture of the field and the results of the past (and next) 25 years.

The writing style is, to say the least, precise. This implies a huge number of cross-references which are not always easy to follow. In such cases, completeness has been preferred to succinctness, making this book a great reference. However, when cross-references become too numerous, the authors do not hesitate to repeat succinctly a definition, helping the flow of reading. Most chapters are filled with (precisely delimited) digressions, which may open the view of the reader and contain possible new directions.

Review of [6]
Basic Phylogenetic Combinatorics
by Andreas Dress, Katharina T. Huber,
Jacobus Koolen, Vincent Moulton, Andreas Spillner
Cambridge University Press, 2012
260 pages, Hardcover-$62.00, Kindle-$44.00

Review by Kipper Fletez-Brant (cfletez1@jhmi.edu)
McKusick-Nathans Institute for Genetic Medicine
Johns Hopkins School of Medicine
Baltimore, MD, USA

1 Introduction

Phylogenetics is the science of relationships between organisms, as measured by some characteristic, such as gene, genome, RNA or protein sequence (the authors of the present work abstract slightly and refer to the concept of an Operational Taxonomic Unit, or OTU). A frequent object of study in phylogenetics is to ascertain the nature and order of the evolution of a group of OTUs, such as a set of animal species - which species are closely related, and which diverged in evolution less recently? Additionally, phylogenetic analysis can have more practical applications and has been used in the study of viruses and other pathogens as well.

Generally the OTU or characteristic of interest in a phylogenetic analysis is sequence based: gene and genome sequences, composed of nucleotides, are represented as strings over the alphabet {A, C, G, T}, (or similar for RNA) and protein sequences, composed of amino acids, as strings over all English letters except {B, J, O, U, X, Z}. In such a phylogenetic analysis, the question of similarity is specified to be about similarity of sequence and the series of changes needed to get from one sequence to another. This is a difficult problem, because methods for phylogenetics must account for different factors, including site-specific (individual nucleotide or amino acid position) and general mutation rates.

The end product of a phylogenetic analysis is a *phylogeny*. Yang and Rannala [1] define a phylogeny as a 'model of genealogical history', which is a tree 'in which the lengths of the branches are unknown parameters' that 'represent the persistence of a ... lineage through time'. These trees have the interpretation that interior nodes represent points of evolutionary divergence and leaf nodes represent OTUs.

In *Basic Phylogenetic Combinatorics*, the authors focus on the encodings of phylogenetic trees, and the relationships between these encodings. Specifically, they describe the nature of phylogenies represented as metrics, and then as two other types, split systems and quartet systems. Metrics are some measure of relationship between two OTUs while, roughly, split systems are systems of binary splits of OTUs, and quartet systems are systems of partitioned sets of four OTUs. Additionally, the authors address the twin issues of finding an X-tree given an encoding, and given an

encoding, moving to a different one; these are referred to as the 'decoding' and 'recoding' problems. Finally, the authors address the issues of rooted trees and finding a 'correct' encoding, given a poor one.

2 Summary

The first major portion of this book introduces the major notions to be used throughout, and I will give a little more attention to communicate basic concepts. There is some review of basic set theory. They also define splits, which are bipartitions of some set and will be a major instrument for the development of phylogenetic objects, quartets, which are bipartitions of sets of four elements; both of these terms are defined in the context of set systems.

Importantly, they give their formal version of a phylogenetic tree, which is an X-tree. An X-tree is generally defined is a tuple T = (V, E, ϕ) with a vertex set V, an edge set E and a mapping ϕ : X (the OTUs) $\rightarrow$ V such that the image of X in V is the union of all vertices of degree 1 and 2; a phylogenetic tree is specifically the case in which ϕ maps the OTUs to the set of vertices of degree 1. Finally, they address which split or quartet systems, or metrics, are X-tree encodings: metrics satisfying the '4-point condition', which states that the sum of distances between 2 sets of 2 points is $\leq$ the greater of the two other possible combinations of the 4 points, while for split systems the answer is that those systems of splits of which a union of subset of splits will given X are actually an encoding. The case of quartet system is more involved, and will generally be glossed over in the remainder of this review.

The book moves on to discuss how an encoding such as a metric can be used to derive a phylogenetic relationship (an X-tree). This is the 'decoding' problem, and, on a practical level, this is the challenge posed by phylogenetics: some data is given, such as values from a metric, and relationships must be inferred. In the case of a split system, a clever use of the Buneman graph, which allows for the various splits in a system to be represented, provides the necessary connection between the given encoding and the desired X-tree. Given a metric, the needed bridge is found in the tight span of that metric, while for quartet systems, the answer is in the satisfaction of a definition of the size of the system, which will define the X-tree.

Logically, a next step would be to ask about moving between encodings, and this is what the authors do; this is the 'recoding' problem. The authors show an equivalence between a metric and a split system's weighting specifically when that weighting coincides with the values assigned by the metric. Split systems are shown to have a fundamental relationship to quartet systems, while metrics are related to quartet systems by observing relationships between paths in a quartet system and the 4-point condition.

The final segment of the book addresses some more practice-based questions. First, the notion of rooted trees are addressed - in the context of phylogenetics, the root would be some inferred common ancestor for all of the OTUs under consideration. Because a rooted tree has a definite orientation, the concepts explored in the previous sections of the book require some modification - we move from splits, quartets and metrics to clusters, triplets and maps. Finally, the book addresses problems that arise in actual analysis: often data is incomplete or not entirely accurate, and may

lead to an incorrect encoding of an X-tree, which is to say, an incorrect set of relationships between OTUs. The authors close the book by addressing ways (and software) to resolve this problem.

3 Opinion

Overall, I enjoyed learning in detail about the study of phylogenetic trees, as the authors find or highlight many interesting facts about the encodings of relationships of OTUs (X-trees). Not previously familiar with the rich combinatorics literature assembled and presented in this work, I learned a great deal about the ways in which a phylogeny can be considered, and more about the relatedness of these encodings. In particular, having full proofs for each proposition made understanding the claims much easier, although more familiar readers can readily skim for just the results and fill in details where needed. On a purely operational level, I appreciated the extensiveness of the per-chapter symbol list at the end of the book, as little of their specific notation was ignored.

The issue of inference of evolutionary history, or the 'decoding' problem, is attacked from multiple different angles, and as per [1], many of the solutions are statistical in nature, although neighbor-joining is a popular approach. This work and the combinatorics approach is an interesting addition to the phylogenetics literature, as it opens additional avenues for research, both for the mathematician and the biologist. In this connection, I should note that the authors make a point of citing not only their mathematical papers, but also their biological findings, highlighting the fact that their work is not only interesting, but broadly applicable as well.

There is an interestingly composed (to me, at least) audience for which this book is recommended. On the theoretical side of things, mathematicians with in an interest in combinatorics may find this work of interest, as the authors demonstrate that phylogenetics-as-combinatorics can be its own field of study. On the other, more practice-based side of things, I would also recommend this book to phylogenetic researchers, although I would warn that they must have a strong appetite for mathematical analysis, as this book is scant on explanations of formulae. Regardless of which audience you fall into, this work casts several different lights on the intersection of two branches of science.

References

[1] Ziheng Yang and Bruce Rannala, Molecular phylogenetics: principles and practices. *Nature Reviews Genetics* 13 (2012), 303-314.

Review of[7]
Analytic Combinatorics in Several Variables
by Robin Pemantle and Mark Wilson
Cambridge Univ Press, 2013
392 pages, Hardcover, $63.00

Review by Miklós Bóna

1 Introduction

The use univariate generating functions in combinatorial enumeration is a classic topic. In contrast, as the authors explain in the preface, analytic combinatorics in several variables was in its infancy as recently as in the 1990s. It is therefore not surprising that this book is not a textbook, but a collection of research results of the last 15 years. It is certainly a very high-level book, even for the Cambridge Series in Advanced Mathematics, where it is published.

Part I, Combinatorial Enumeration, can be viewed as a very high-level introduction to the rest of the book in that it mostly (but not exclusively) deals with univariate generating functions. Readers who have carefully read the books of *Enumerative Combinatorics, Volume 2* by Richard Stanley and *Analytic Combinatorics* by Philippe Flajolet and Robert Sedgewick will find the chapter easier to read than others, but not easy.

The authors cover three particularly frequent classes of generating functions. These are, in increasing order of containment, rational functions, algebraic power series, and differentiable finite power series. The latter turn out to be precisely the power series whose coefficients satisfy a linear recurrence relation with polynomial coefficients, such as

$$a_{n+2}(n^2+1) + a_{n+1}(2n+3) - a_n(3n-2) = 0. \tag{1}$$

The notion of polynomial recurrences, and hence, that of differentiable finite power series can be extended to several variables, just as the notion of algebraic power series and rational functions.

The concept of *diagonals* is an interesting way to turn a multivariate series into a univariate one. For simplicity, we give the definition for a bivariate power series. Let

$$F(x,y) = \sum_{r,s} a_{r,s} x^r y^s,$$

then

$$\mathrm{diag}F(z) = \sum_{n\geq 0} a_{n,n} z^n.$$

An interesting example of this is the case when $a_{r,s} = r + \binom{s}{r}$. The reader is invited to verify that $\mathrm{diag}F(z) = (1-4z)^{-1/2}$.

[7] ©2014

It is then proved that if $F(x, y)$ is a rational power series in two variables, then its diagonal is algebraic. Another interesting theorem is that the diagonal of a d-finite power series is d-finite.

Part II, Mathematical Background, is just what its title says. It does not contain much combinatorics, but it is a collection of Analytic and Algebraic tools that will be used later. An example of these is the Saddle Point Method, which is a method to estimate the growth rate of coefficients of power series that is especially useful for power series that do not have singular points. In its simplest form, it states that if $G(z)$ is a power series that is not a polynomial that is analytic at 0, has non-negative coefficients, is convergent in a circle of radius R, and satisfies $G(R^-) = \infty$, then

$$[z^n]G(z) \leq \frac{G(\alpha)}{\alpha^n},$$

where α is the unique root of the equation

$$\alpha \frac{G'(\alpha)}{G(\alpha)} = n + 1.$$

The authors devote two full chapters to a series of stronger and stronger versions of this result.

An example for an algebraic tool is the theory of Gröbner bases. Consider the polynomial ring $Q[\mathbf{z}]$, where $\mathbf{z} = (z_1 z_2 \cdots z_d)$. A *monomial order* on this ring is a relation $>$ on the set $z^{\mathbf{r}}$ of monomials that is a total ordering, a well ordering, and in which $\mathbf{z}^\alpha > \mathbf{z}^\beta$ implies $\mathbf{z}^{\alpha+\gamma} > \mathbf{z}^{\beta+\gamma}$. In a monomial order, $LT(f)$ denotes the leading term of f with respect to that monomial order. Finally, for an ideal I of $Q[\mathbf{z}]$, a *Gröbner basis* is a basis $\{g_1, g_2, \cdots, g_k\}$ so that for any nonzero $f \in I$, it holds that $LT(f)$ is divisible by $LT(g_i)$ for some i. The authors show a few examples for the use of these bases in computations with algebraic numbers.

On the whole, it is a viable reading strategy to skip all of Part 2, and to return to it when needed in order to understand some later chapters.

Part III, Multivariate Enumeration, is the heart of the book. The general goal is to compute the coefficients of multivariate power series using the Cauchy coefficient formula

$$a_r = \left(\frac{1}{2\pi i}\right)^d \int_T \mathbf{z}^{-\mathbf{r}-\mathbf{1}} F(z)\, dz,$$

where $F(\mathbf{z})$ is a function in d variables. The authors explain how to choose the contour T of integration so that information about the integral could be gained by studying the behavior at the integrand at *one* point, which is called the *critical point*. A chapter is devoted to each of three kinds of critical points, namely *smooth points*, *multiple points*, and *cone points*. Among the discussed methods, there will be some that the reader may have encountered before in the one-variable case, such as computation of residues. On the other hand, this reviewer never met the method of *surgery* before, even though it predates residue computations. This method, which really involves chopping a Cauchy integral into two pieces, is illustrated by several examples, and its advantages and drawbacks are explained, and compared to those of the residue computation method.

The part ends with a chapter on worked-out examples of an increasing level of difficulty, which illustrate the methods of the preceding chapters. For a reader who gets stuck in one of the difficult chapters on methods, it is probably a good idea to jump ahead to this chapter for some motivation.

The last part of the book consists of three Appendices, on Integration of Manifolds, Morse Theory, and Stratification and Stratified Morse Theory. Each chapter ends with a short list of exercises with no solutions. Software and other supporting materials can be downloaded from the authors' website.

The book is not easy to read. Various units often start with a general version of a theorem, and at that early point, the reader may not be ready for that level of generality. It could have been better to start these sections and chapter with an example, before any theoretical introduction. If a reader gets discouraged by getting stuck early in a chapter, perhaps a good strategy is to go to Chapter 12 (Worked Examples), find an example that is close to the topic at hand, and then go back to the theory.

It should be clear from all the above that there is no other book on the market that comes remotely close to this one. The authors laid the foundation for the *systematic* study of Analytic Combinatorics in Several Variables. For the readers, there is a lot of work to do.

Review of[8]
The Tower of Hanoi - Myths and Maths
by Andreas M. Hinz, Sandi Klavžar, Uroš Milutinović, Ciril Petr
Birkhäuser, 2013
335 pages, Hardcover, $42.00

Review by László Kozma, kozma@cs.uni-saarland.de
Saarland University, Saarbrücken, Germany

1 Introduction

The book revolves around the classical puzzle, the Tower(s) of Hanoi, apparently invented and first published in 1883 by the French mathematician Édouard Lucas (sometimes called the Martin Gardner of the 19th century). Lucas also came up with a fanciful legend around the game which might have contributed to its popularity. Probably everyone with a passing interest in recreational mathematics or some exposure to computer science will have already encountered the basic variant of the problem: there are three pegs and n discs of different sizes with holes in the middle. Originally the discs are stacked on top of each other from largest to smallest on the first peg. The goal is to transfer all discs onto the third peg with as few moves as possible. A valid move consists of taking the top disc from one of the pegs and placing it on another peg, with the rule that no disc can be placed on top of a smaller disc.

Perhaps most people (including this reviewer) remember the puzzle as something quite simple, interesting mainly as a textbook example of recursion, and as an example of a problem where powers of two appear naturally. In reality, as the book demonstrates, the Tower of Hanoi has a very rich mathematical structure, and as soon as we tweak the parameters we surprisingly quickly find ourselves in the realm of open problems.

2 Summary

The first chapter (Chapter 0) tells the history of the Tower of Hanoi puzzle, and a closely related puzzle called Chinese Rings. It is also mentioned that the puzzle has been used as a psychological test of sorts to measure the problem solving ability of subjects. The rest of the chapter is devoted to mathematical preliminaries and selected topics including binomial coefficients, the Sierpiński triangle, equivalence classes, Stern-Brocot trees, basic graph theory (the usual suspects from the bridges of Königsberg to the 4-color-theorem), group actions and Burnside Lemma. What connects these topics is mostly that they will be used later in the analysis of the game, but we also see interesting connections right away, such as the fact that plotting Pascal's triangle modulo 2 yields the Sierpiński triangle.

[8]

Chapter 1 concerns the Chinese Rings puzzle. This puzzle is interesting here mostly because the description of its solution involves the Gros sequence $(1, 2, 1, 3, 1, 2, 1, 4, 1, 2, 1, 3, 1, 2, 1, 5, \dots)$ which appears in many places in mathematics. The sequence indicates (among other things) which bit to flip during the construction of binary reflected Gray codes. As seen later, it is also closely related to the Tower of Hanoi.

Chapter 2 is perhaps the most important part of the book, as it describes its main subject, the Tower of Hanoi puzzle with 3 pegs. The basic variant is the *perfect to perfect* puzzle described above. For this task there is an optimal solution of length $2^n - 1$, in which in step i we move disc a_i, where a is the Gros sequence mentioned above. An actual algorithm for obtaining the sequence of moves is easily formulated. Writing it in recursive and non-recursive ways gives different perspectives on the structure of the optimal solution.

In the *regular to perfect* puzzle, the starting state is arbitrary (as long as no disc is above a smaller disc), and the goal is to move into the same target state as before. It is shown that from any regular state there is a unique shortest path to the perfect state, and an algorithm is given for finding this path.

Next, the graph of all regular states is considered (edges correspond to moves between states). This graph, called the Hanoi graph H_3^n resembles, quite remarkably, a discrete version of the Sierpiński triangle. Many different properties of H_3^n are explored, including connectivity, hamiltonicity, perfect codes, chromatic number, number of matchings, or more importantly for the problem at hand, properties related to shortest paths and distances. The H_3^n graph is understood well enough to obtain an efficient algorithm for the *regular to regular* puzzle and to answer structural questions related to the number of optimal solutions (there are at most two) or the average length of an optimal solution (it tends to a 466/885 fraction of the diameter $2^n - 1$). Another interesting property is that every regular state of the puzzle is identifiable by two distances (to two of the perfect states).

Chapter 3 considers the relaxation of the puzzle to irregular initial states (but still only regular moves are allowed) - now the Hanoi graph is augmented with many new states and edges become directed. The structure of this (di)graph is also relatively well understood, allowing an algorithm for the *irregular to perfect* puzzle. For the general *irregular to regular* puzzle no algorithm seems to be known, although some properties of the shortest paths are given. The last category of puzzles, *irregular to irregular* is not always solvable and it is not discussed.

Chapter 4 concerns Sierpiński graphs, a generalization of the H_3^n graph of the Tower of Hanoi states. The graph S_3^n is a relabeling of H_3^n, and it is naturally extended to S_p^n. The structure of the graphs S_p^n is relatively well understood for $p > 3$ too, but unfortunately, these *do not* correspond directly to H_p^n, the graph of Hanoi states with p pegs. Again, many properties of these graphs are explored, such as the crossing number of S_p^n (for $p \geq 4$ and $n \geq 3$ the graph is not planar). Not all of these properties are relevant to the Hanoi puzzle.

Chapter 5 is perhaps the most interesting, as it introduces the Tower of Hanoi with more than 3 pegs. As the problem is difficult enough, mostly the *perfect to perfect* case is discussed. With 4 pegs, a natural approach is the following: move the top part of the tower of size m onto an idle peg, then transfer the remaining $n - m$ discs to the target as if there were only 3 pegs, then transfer the tower of size m on top of the target (again, using all 4 pegs). The length of this solution is given by

$f(n) = 2f(m) + 2^{n-m} - 1$. For given n the optimal value of m can be (and has been) found. Thus, the lengths $f(n)$ of the paths obtained by the above algorithm can be expressed in closed form (and are called Frame-Stewart numbers). The main open problem is whether the above algorithm is optimal. Numerical evidence has not disproved it so far, and a number of conjectures are given, which together would imply the optimality of the algorithm. A generalization of this approach is also conjectured to be optimal for $p > 4$ pegs. While the exact optimum is elusive, a lower bound of Szegedy shows that the algorithm is essentially optimal asymptotically (albeit up to a constant factor in the exponent). In the remainder of the chapter the graph H_n^p is explored - it is remarkable that quite little is understood about its structure.

Chapter 6 presents variants of the puzzle. Some of these involve discs with different colors, others place additional restrictions on the allowed moves, or relax some of the restrictions (for example, by allowing a larger disc to be placed above a smaller disc if their difference is not too large). Some of these variants exhibit interesting mathematical structure and algorithms are presented for their solution. The Tower of London puzzle presented in Chapter 7 also fits into this category, it is treated in slightly more detail because of its interesting structure, and because apparently its variants are often used in problem solving tests. Chapter 8 presents yet another class of variants, the oriented Tower of Hanoi puzzles, where movement of discs is allowed only between certain directed pairs of pegs. The solvability of such puzzles is characterized depending on the underlying digraph and the length of the solution is analyzed.

Finally, in Chapter 9 the open questions of the book are collected, among which the most interesting are the weak and strong Frame-Stewart conjecture, that posit the optimality of the presented algorithm for the Tower of Hanoi with 4, respectively p pegs.

3 Opinion

In my opinion, the book could serve two main categories of readers (with possible overlap between the two of course). The first are those interested in the Tower of Hanoi and its variants, trying to better understand the game or to attempt some of the research questions left open. The second are those looking for a book about interesting mathematics, random mathematical "gems", accessible theorems and proofs about an entertaining topic.

For the first category of readers the book is indispensable. It comprehensively collects the facts known about the puzzle and corrects many mathematical myths, statements which were assumed without proof (sometimes even in print), and were found to be false. The authors know the literature of the problem intimately (there are 352 bibliography items), so anyone seriously interested in the problem would benefit from consulting the book.

For the interested layperson, the book is accessible and mostly self-contained, the topic is engaging and the enthusiasm of the authors is contagious. The exercises are well-chosen and complement the text nicely, and solutions are given in the end, so the book can be followed through quite easily. Thus, I would warmly recommend the book for anyone interested, or as a gift for say, a mathematically-inclined high school student or undergraduate - with a number of small remarks and minor criticisms.

As the book tries to be a comprehensive account of the puzzle, not all the statements are equally important or interesting. A bit of care is needed to avoid being lost in the details. Some of the notational formalism is necessary to present *all* the results, but could have been simplified slightly if only *some* of the results were included. In some places the notation could be difficult to parse for the above-mentioned hypothetical high schoolers (even when the underlying ideas are relatively simple). Once the Hanoi and Sierpiński graphs are defined there are an infinite number of questions we can ask about them - perhaps the book would have been more focused if only those that take us closer to understanding the game would have been included (one can skip through sections at will, of course).

The introduction covers topics that are later needed - here the level of difficulty is somewhat uneven, and in some cases the explanations could have been slightly clearer: the definition of planar graphs and the discussion of duality is somewhat confusing, and the definition of the graph of a map as the dual of its dual is a bit unintuitive.

The historical asides and anecdotes are interesting and sometimes funny. The authors express their annoyance on three different occasions at Mandelbrot's choice of the term Sierpiński's "gasket". I found the strong words amusing, but have to admit that didn't entirely understand why exactly the authors disliked the term.

Overall, despite its minor shortcomings, I think the book fulfills its intended purpose, the authors give an authoritative and comprehensive overview of an interesting (if somewhat narrow) topic, they strike a good balance between intuitive explanations and formal clarity. The book invites further thinking and research and both the historical and the mathematical parts (the latter making up the majority of the book) are enjoyable to read.