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. **Combinatorial Designs: Constructions and Analysis** by Douglas R. Stinson. Review by Gregory Taylor. A combinatorial design is a set of sets of (say) $\{1, \ldots, n\}$ that have various properties, such as that no two of them have a large intersection. For what parameters do such designs exist? This is an interesting question that touches on many branches of math for both origin and application.

2. **Combinatorics of Permutations** by Miklós Bóna. Review by Gregory Taylor. Usually permutations are viewed as a tool in combinatorics. In this book they are considered as objects worthy of study in and of themselves.

3. **Enumerative Combinatorics** by Charalambos A. Charalambides. Review by Sergey Kitaev, 2008. Enumerative combinatorics is a branch of combinatorics concerned with counting objects satisfying certain criteria. This is a far reaching and deep question.

4. **Geometric Algebra for Computer Science** by L. Dorst, D. Fontijne, and S. Mann. Review by B. Fasy and D. Millman. How can we view Geometry in terms that a computer can understand and deal with? This book helps answer that question.

5. **Privacy on the Line: The Politics of Wiretapping and Encryption** by Whitfield Diffie and Susan Landau. Review by Richard Jankowski. What is the status of your privacy given current technology and law? Read this book and find out!

Books I want Reviewed

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

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

Books on Algorithms and Data Structures

1. *Algorithms on Strings* by Crochemore, Hancart, and Lecroq.

2. *Algorithms for Statistical Signal Processing* by Proakis, Rader, Ling, Nikias, Moonen, Proudler.

3. *Nonlinear Integer Programming* by Li and Sun.

4. *Binary Quadratic Forms: An Algorithmic Approach* by Buchmann and Vollmer.

5. *Curve and Surface Reconstruction: Algorithms with Mathematical Analysis* by Dey

Books on Cryptography and Nothing else

1. *An Introductino to Mathematical Crytography* by Hoffstein, Pipher, and Silverman.
2. *Concurrent Zero-Knowledge* by Alon Rosen.
3. *Introduction to cryptography: Principles and Applications* by Delfs and Knebl.

Books on Coding Theory, Security, and Crypto++

1. *Protecting Information: From Classical Error Correction to Quantum Cryptography* by Loepp and Wootters.
2. *Codes: An Introduction to Information Communication and Cryptography*
3. *Coding for Data and Computer Communications* by David Salomon.
4. *Formal Correctness of Security Protcols* by Bella
5. *Coding for Data and Computer Communications* by David Salomon.
6. *Block Error-Correcting Codes: A Computational Primer* by Xambo-Descamps.

Combinatorics Books

1. *A Course on the Web Graph* by Bona.
2. *A Course in Enumeration* by Aigner.
3. *Algorithmic Combinatorics on Partial Words* by Blanchet-Sadri.

Logic and Verification Books

1. *Software Abstractions: Logic, Language, and Analysis* by Jackson.
2. *Formal Models of Communicating Systems: Languages, Automata, and Monadic Second-Order Logic* by Benedikt Bollig.
3. *Modelling Distributed Systems* by Fokkink.

Misc Books

1. *Quantum Computing for Computer Scientists* by Yanofsky and Mannucci.
2. *Advanced Data Structures* by Peter Brass.
3. *Introduction to Information Retrieval* by Manning, Raghavan, and Schutze.
4. *Higher Arithmetic: An algorithmic introduction to Number Theory*
5. *A Conscise introduction to Data Compression* by Salomon.

6. *Putting Auction Theory to Work* by Paul Milgrom.

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

Review of [2]

Combinatorial Designs: Constructions and Analysis
Author of Book: Douglas R. Stinson
Springer-Verlag, New York, 2004, 300 pages

Review by R. Gregory Taylor

1 Introduction

The origins of combinatorial design theory lie within recreational mathematics. With the work of Fisher and Yates in the 1930s it began to take on the character of a serious academic subject with deep connections to linear algebra, group theory, and number theory; there are applications to statistical experimentation, tournament scheduling, mathematical biology, algorithm design and analysis, and cryptography. The basic notion is that of a *design*, whereby one intends a pair $(X, \mathcal{A})$ with X any set of elements (or *points*) and $\mathcal{A}$ any multiset of nonempty subsets of X (termed *blocks*). (If $\mathcal{A}$ is a set, then $(X, \mathcal{A})$ is *simple*.) The focus of design theory is so-called BIBDs (Balanced Incomplete Block Designs) and the identification of necessary and sufficient conditions on v, k, and λ such that (v, k, λ)-BIBDs exist. (Steiner triple systems of order v are $(v, 3, 1)$-BIBDs.)

The book under review has eleven chapters. Equivalence results, which anchor each of them, take the form "there exists a ... if and only if there exists a __" but almost invariably have constructive proofs showing that, given a ..., we can construct a __, and vice versa.

2 Summary of Contents

Chapter 1: Introduction to Balanced Incomplete Block Designs. With $v > k \geq 2$ and λ positive integers, a (v, k, λ)-*balanced incomplete block design* (or (v, k, λ)-BIBD) is a design $(X, \mathcal{A})$ such that (1) $|X| = v$, (2) each block contains exactly k points, and (3) every pair of distinct points is contained in exactly λ blocks. (By $v > k$ each block is incomplete, and Property 3 makes for balance.) Every point within any (v, k, λ)-BIBD $(X, \mathcal{A})$ figures in exactly $r =: \frac{\lambda(v-1)}{k-1}$ blocks, and $b =:$ the number of blocks in $\mathcal{A}$ including multiplicities $= \frac{vr}{k}$ in turn. Since r and b must be integers, no $(8, 3, 1)$-BIBD, for example, can exist. In the case of any $(22, 8, 4)$-BIBD we have $r = 12$ and $b = 33$, but it is currently unknown whether such a BIBD exists.

Very elementary BIBDs have nice graphical representations. More generally, BIBD $(X, \mathcal{A})$ is represented by a so-called *incidence matrix*—a $v \times b$ Boolean matrix M whose (i, j)-entry is 1 just in case the i^{th} point of X is in the j^{th} block of $\mathcal{A}$. In Theorem 1.13 the author presents necessary and sufficient conditions for a $v \times b$ Boolean matrix to be the incidence matrix of a (v, k, λ)-BIBD. Design isomorphism is characterized in terms of incidence matrices, which in turn yields the notion of the automorphism group of a BIBD. In Section 1.4.1 the author describes a method for determining whether a BIBD having specified automorphism group exists. Two methods ("sum construction" and "block complementation") for constructing new BIBDs from given BIBDs

are illustrated. Fisher's Inequality (Theorem 1.33) provides another necessary condition for the existence of a (v, k, λ)-BIBD, namely, $b \geq v$. (It follows that no $(16, 6, 1)$-BIBD exists.) Finally, $b \geq v$ holds in any *nontrivial regular pairwise balanced design* (PBD) as well, whereby the size of blocks is now permitted to vary and at least one block must be incomplete.

Chapter 2: Symmetric BIBDs. A BIBD $(X, \mathcal{A})$ is termed *symmetric* if $v = b$. Since the intersection of any two distinct blocks of a symmetric (v, k, λ)-BIBD has cardinaliy λ, symmetric BIBDs can be used to construct new BIBDs, as illustrated in Example 2.8. Necessary conditions for the existence of symmetric (v, k, λ)-BIBDs are provided by Bruck–Ryser–Chowla Theorems 2.16 and 2.17. By the former, if v is even, then $k - \lambda$ must be a perfect square, from which it follows that no $(22, 7, 2)$-BIBD exists. By the latter, if v is odd, then a certain diophantine equation in three variables with coefficients in v, k, and λ has a nontrivial solution, from which it follows that no (symmetric) $(43, 7, 1)$-BIBD exists (Example 2.20). Open questions with respect to the existence of symmetric BIBDs abound, and, in this regard, no real advance has occurred in half a century.

Chapter 3: Difference Sets and Automorphisms of Designs. The usefulness of a *difference set in an abelian group* for construction of a symmetric BIBD can be illustrated by the author's Example 3.2. First, $D = \{0, 1, 6, 8, 18\}$ is a $(21, 5, 1)$-difference set in $(\mathbb{Z}_{21}, +)$ since D contains 5 elements of $\mathbb{Z}_{21}$ and since the multiset of all possible differences (modulo 21) of distinct elements of D contains each nonzero element of $\mathbb{Z}_{21}$ exactly 1 time. Each such difference set can be used to construct a symmetric $(21, 5, 1)$-BIBD $(X, \mathcal{A})$ as follows: we let X be $\mathbb{Z}_{21}$ and let $\mathcal{A}$ be the set that results from "translating" D by each element of $\mathbb{Z}_{21}$. (Thus, the blocks of $\mathcal{A}$ are D itself as well as $\{1, 2, 7, 9, 19\}, \ldots, \{20, 0, 5, 7, 17\}$.) Theorem 3.8 asserts that this construction is always possible. and Theorem 3.16 amounts to a converse in the special case whereby given symmetric BIBD $(X, \mathcal{A})$ has a certain sort of automorphism. Much of the remainder of this chapter describes alternative means of obtaining difference sets: the method of quadratic (alternatively quartic) residues (§3.2), a method due to J. A. Singer (§3.3), and the method of mulipliers (§3.4). In two final sections the notion of a difference set is generalized to that of a *difference family for a group*, difference families are shown to yield symmetric BIBDs (Theorem 3.46), and a method of constructing such families, due to R. M. Wilson, is presented.

Chapter 4: Hadamard Matrices and Designs. Recall that a Hadamard matrix of order n is an $n \times n$ matrix all of whose entries are either 1 or -1 and such that $HH^T = nI_n$. It turns out that there is a close link between the existence of Hadamard matrices of a given order and the existence of BIBDs. In particular, any Hadamard matrix of order $4m$ with $m > 1$ is easily transformed into the incidence matrix of a symmetric $(4m-1, 2m-1, m-1)$-BIBD (Theorems 4.5). Consequently, construction techniques for Hadamard matrices are of interest, and most of the remainder of Chapter 4 describes such techniques: the method of so-called *conference matrices* (§4.3), the recursive *Kronecker product construction* (§4.4), and a method due to J. Williamson (§4.5). In §4.8 so-called *bent functions* ("maximally nonlinear" Boolean functions) are the topic. They are related to Hadamard matrices in Theorem 4.42 and proved equivalent to certain difference sets in Theorem 4.44.

Chapter 5: Resolvable BIBDs. A BIBD $(X, \mathcal{A})$ is said to be *resolvable* if $\mathcal{A}$ can be partitioned into parts, each of which consists of a mutually disjoint collection of blocks whose union is X. Bose's Inequality (Theorem 5.14) asserts that a (v, k, λ)-BIBD is resolvable only if $b \geq v + r - 1$.

Chapter 6: Latin Squares. A *Latin square of order* n is an $n \times n$ array L each cell of which is occupied by some member of a set X with $|X| = n$ and such that each row and each column of L is a permutation of X. Where $\circ$ is a binary operation on a finite set X with $|X| = n$, then $(X, \circ)$

is a quasigroup if and only if its operation table is a Latin square of order n. (The designation "quasigroup" means that X is closed under $\circ$ and that $\circ$ satisfies left and right cancellation laws.) Thus quasigroups provide a convenient means of discussing Latin squares. Steiner triple systems of order v (STS(v)s) are the topic in §6.2, where the reader is reminded that there exists an STS(v) if and only if $v \equiv 1, 3 \pmod 6$ with $v \geq 7$ (Theorem 6.17). The proof of one direction here takes the form of two constructions, due to R. C. Bose and T. Skolem, respectively, based on symmetric (half-)idempotent quasigroups.

Section 6.3 is an investigation of *orthogonal Latin squares*. (Two Latin squares of order n over X are orthogonal is their component wise amalgamation contains every member of Cartesian product $X \times X$.) Orthogonal Latin squares of orders 1, 3, 4, 5, 7, and 8 exist, whereas there are none of orders 2 or 6. This led Euler to conjecture that no orthogonal Latin squares of order n exist if $n \equiv 2 \pmod 4$. A refutation of Euler's conjecture for all $n \neq 2, 6$ was published in 1960 by Bose, S. S. Shrikhande, and E. T. Parker, and a newer proof of their result, based on R. M. Wilson's construction of mutually orthogonal Latin squares, is presented in §6.8. In §6.5 an equivalent formulation of the mutually orthogonality concept called *orthogonal arrays* is introduced.

Chapter 7: Pairwise Balanced Designs I: Designs wih Specified Block Sizes. A (v, K, λ)-PBD is a set system $(X, \mathcal{A})$ satisfying (1) $|X| = v$, (2) $|A| \in K$ for every block $A \in \mathcal{A}$, and (3) every pair of distinct points is contained in exactly λ blocks. (Here $v \geq 2$, $\lambda \geq 1$, and K is any set of natural numbers each of which is at least 2.) Clearly, any (v, k, λ)-BIBD is a $(v, \{k\}, \lambda)$-PBD, and, conversely, if $k < v$, then any $(v, \{k\}, \lambda)$-PBD is a (v, k, λ)-BIBD. The emphasis in this chapter is on constructions (first half of book's subtitle) as well as necessary conditions for the existence of $(v, K, 1)$-PBDs. In contrast, the focus of **Chapter 8: Pairwise Balanced Designs II: Minimal Designs** is analysis (second half); specifically, the author takes up the problem of determining the minimum number of blocks in a PBD such that maximum block size has been specified or such that the size of a particular block has been specified. The so-called Stanton–Kalbfleisch Bound is an example of the latter and states that any $(v, \{2, \ldots, v-1\}, 1)$-PBD having a block with k points satisfies $b \geq 1 + \frac{k^2(v-k)}{v-1}$ (Theorem 8.1). A strengthening of this lower bound, published in 1982 by the author himself, is presented in Theorem 8.7.

Chapter 9: t-Designs and t-wise Balanced Designs. The t-design concept is a generalization of the notion of (v, k, λ)-BIBD: every set of t distinct points is contained in exactly λ blocks. Repeated blocks are permitted, although one is most interested in the more difficult task of constructing *simple* t-designs that have none. The proof of Theorem 9.10 gives an easy construction for a 1-(v, k, λ)-design provided $v\lambda \equiv 0 \bmod k$. Since 2-designs are the BIBDs of Chapters 1 through 5, that leaves t-designs with $t \geq 3$, and §9.2 presents construction techniques for 3-designs based on Hadamard matrices and resolvable BIBDs. Final section §9.3 generalizes the notion of a PBD to that of *t-wise balanced design*.

Chapter 10: Orthogonal Arrays and Codes. A very general notion of orthogonal array is defined, and it is shown that such arrays are easily constructed from Hadamard matrices of order $4m$ as well as from any finite field $\mathbb{F}_q$. The elements of coding theory are introduced in §10.2 and, in subsequent sections, codes are related to orthogonal arrays and BIBDs in two ways (Theorems 10.21 and 10.25).

Chapter 11: Applications of Combinatorial Designs. In this final chapter the author considers four applications of design theory: authentication codes, threshold schemes, group testing algorithms, and two-point sampling. It is shown in Theorems 11.2 and 11.5, respectively, that authentication codes and threshold schemes, both from cryptography, can be constructed from

orthogonal arrays. In §11.3 BIBDs are used to construct *nonadaptive group testing algorithms* of a sort that might be used to test a large number of blood samples, in combination, for a rare disease, where each test is expensive. (A negative result indicates that none of the combined samples is positive.) In §11.4 orthogonal arrays are used to construct yes-biased Monte Carlo algorithms, specifically, for finding a sequence of pseudo-random sample points that can then be tested deterministically.

3 Opinion

The author's stated goal is a textbook account of design theory that emphasizes results from the middle decades of the last century. There are a dozen or so exercises—all of at least moderate difficulty, it seems—at the end of each chapter. The book is very well written and well organized. We identified very few typographical errors, all trivial in character. This text should serve as a rich source of interesting research projects for advanced undergraduates. One minor criticism concerns the author's presentation of a certain "geometric theme" (our term). In Definition 2.9 a *projective plane of order n* is defined to be any $(n^2 + n + 1, n + 1, 1)$-BIBD with $n \geq 2$, and it is shown (Theorem 2.10) that projective planes of order q exist for every prime power exceeding 1. A certain related design is then described as an *affine plane of order n*, and affine planes of arbitrary prime power order $q \geq 2$ are shown to exist (Theorem 2.13). Both notions are generalized, essentially by increasing exponent 2, to that of projective and affine *geometries*. However, the author does not explain why talk of planes and geometries is appropriate. Given that "senior undergraduate or beginning graduate level" students are the intended audience, some mention of axiomatic treatments of finite geometries would have been useful. (Incidentally, the author mentions the existence of a projective plane of nonprime power order as an important open question in the field.)

A more substantial criticism of this excellent book is the following: whereas the central organizational concept is that of a design, there are long excursions into topics whose links to designs are not going to be apparent to many readers. For example, Chapter 10 is largely an exploration of coding theory—23 out of 26 pages. While interesting in its own right, it would have been useful to see how this material bears on design theory. The link appears to be the following. Theorem 4.5 concerns symmetric BIBDs and Hadamard matrices; Theorem 10.2 concerns Hadamard matrices and orthogonal arrays. Putting them together yields an equivalence between symmetric BIBDs and orthogonal arrays. Now it is on to coding theory with an emphasis on the use of codes to construct orthogonal arrays, which, by the aforementioned equivalence and some more theory, means that codes are being used to construct symmetric BIBDs. This is never spelled out, however. (Exercises 10.7 and 10.9 suggest rather direct links between codes and BIBDs, however.) Similarly, the notion of *resilient function* introduced in §10.6 is directly related only to codes and orthogonal arrays, the link to designs being left to the reader.

Review of[3]
Combinatorics of Permutations
Author of book: Miklós Bóna
Publisher: Chapman & Hall/CRC
2004, 383 pages

Review by R. Gregory Taylor

[3]

1 Introduction

Any permutation of ordered n-element set $[n] =: \{1, \ldots, n\}$ may be regarded as introducing a (possibly null) measure of disorder to that set. For example, the natural order of [7] is maximally disturbed by permutation 7654321, where the occurrence of j in position i with $1 \leq i, j \leq 7$ indicates that position i, formerly filled by element i, is now filled by element j. In contrast, identity permutation 1234567 preserves the pre-ordained order. Somewhere between these two extremes we find the likes of $p = 2156743$, which representation figures as second line in the familiar two-line representation

$$\begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 5 & 6 & 7 & 4 & 3 \end{array}$$

of p. The latter suggests the more standard conception of 7-permutations as function members of symmetric group S_7 ("p maps 1 to 2, 2 to 1, ..., and 7 to 3."). By identifying "closed orbits" within the above example one obtains a cycle representation (12)(357)(46) of p. It is natural to ask whether one-line representations and cycle representations can be related in interesting ways. The answer is yes, and, as a preliminary, let us represent p *canonically* as (21)(64)(735) by placing the largest member of each cycle on the left and afterward arranging the cycles in ascending order using leftmost members. (We may assume disjoint cycles.) One useful link between the two representation schemes is then the following: the "parentheses-dropping" mapping that takes canonical (21)(64)(735) to one-line representation 2164735 happens to be a bijection of S_7 onto itself. Author M. Bóna makes this result, for general n, his Transition Lemma 3.39 and uses it to prove that the total number of cycles in all n-permutations equals the number of $(n+1)$-permutations having exactly two cycles (Theorem 3.45).

2 Summary of Contents

Chapter 1 (*In One Line and Close. Permutations As Linear Orders. Runs.*) of the book under review introduces three important notions arising out of the linear-order conception of permutations and investigates the close links between them.

1. First, there is the concept of *Eulerian number* $A(n, k)$ with $k \leq n$ and $n \geq 1$, defined as the number of n-permutations having $k - 1$ descents—equivalently, k ascending runs. (The 7-permutation $p = 3412576$ has two descents—positions 2 and 6—and three ascending runs.)

2. Second, *Stirling number of the second kind* $S(n, k)$ is the number of partitions of $[n]$ into k parts or *blocks*.

3. One writes $G(n, k)$ for the number of n-permutations having k *alternating runs* or changes in direction.

In Theorem 1.17 and Corollary 1.18, it is shown that (1) and (2) are closely related. For any $n \geq 1$, the sequence $\{A(n, k)\}_{1 \leq k \leq n}$ is proved to be *log-concave* in the sense that $A(n, k-1) \cdot A(n, k+1) \leq A(n, k)^2$ for all $1 < k < n$ (Theorem 1.26). As elsewhere, the author makes a point of presenting a fully combinatorial proof of this result, due to himself and R. Ehrenborg, while also showing that it follows from an analytical result stating that, for $n \geq 1$, all roots of

polynomial $\sum_{k=1}^{n} A(n,k)x^k$ are real (Theorem 1.33). Chapter 1 closes with a sketch of H. Wilf's proof that polynomial $\sum_{k=1}^{n} G(n,k)x^k$ has real roots only (Theorem 1.41) from which it follows that sequence $\{G(n,k)\}_{1\leq k\leq n}$ is log-concave. (Log-concavity implies unimodality, the increase-then-decrease property possessed by any row of Pascal's triangle and so important in combinatorics.)

Chapter 2 (*In One Line and Anywhere. Permutations As Linear Orders. Inversions*) introduces two more permutation statistics.

4. One uses $b(n,k)$ with $n \geq 1$ and $1 \leq k \leq \binom{n}{2}$ to denote the number of n-permutations having k *inversions*, where an inversion of permutation p is a pair (p_i, p_j) such that $i < j$ with $p_i > p_j$.

5. The *major index* of permutation p is defined to be the sum of the descents of p (see (1)).

After recursive formulæ for $b(n,k)$ are identified (Lemma 2.5 for $n \geq k$ and Exercise 28 for $n < k$), search for an explicit formula leads through the theory of integer partitions and pentagonal numbers. The inversion concept is used to give a definition of the determinant of a matrix (Theorem 2.19) that is then applied so as to yield a sufficient condition for G's having a perfect matching, where G is a bipartite graph whose two collections of vertices are of equal size. Ultimately, generalizations of binomial coefficients known as Gaussian coefficients (or polynomials) are used in Theorems 2.27 and 2.28 to describe generating functions for sequences $b_1, b_2, \ldots$, where b_i is the number of permutations, of some given multiset, having i inversions, respectively, having major index i.

In Chapter 3 (*In Many Circles. Permutations As Products of Cycles.*), n-permutations are reconceived as function members of the symmetric group S_n, and canonical cycle notation is presented as described above. Two ways of associating an n-permutation p with bistochastic Boolean matrices A_p, respectively, B_p of order n are described. Parity notions are introduced, and it is shown that p is *even* (read: the number of its inversions is even) just in case $\det(A_p) = \det(B_p) = 1$. This result is then used to characterize the alternating group A_n as well as geometric transformations of a regular hexagon. Two new concepts are central to this chapter.

6. The number of n-permutations having k cycles is denoted $c(n,k)$, and we speak of *signless Stirling numbers*.

7. *Stirling numbers of the first kind* are defined by $s(n,k) =: (-1)^{n-k}c(n,k)$.

Stirling numbers of the first and second kind are related in Theorem 3.30: lower triangular order-$\aleph_0$ matrices s with $s_{i,j} = s(i,j)$ and S with $S_{i,j} = S(i,j)$ satisfy $sS = Ss = I$. Given $n \geq 0$ fixed, a recursive formula for $c(n,k)$ is presented in Lemma 3.19, and in Theorem 3.10 it is shown that the terms of sequence $\{c(n,k)\}_{0\leq k\leq n}$ are the coefficients of polynomial $x(x+1)\ldots(x+n-1)$. Similarly, the terms of $\{s(n,k)\}_{0\leq k\leq n}$ are the coefficients of $x(x-1)\ldots(x-n+1)$ (Corollary 3.29), and a recursive formula for $s(n,k)$ is presented in Lemma 3.36. Finally, Chapter 3 ends with a proof of a closed formula (Schlömilch's formula) for $s(n,k)$. Along the way, probability plays a role when it is shown (Lemma 3.26) that the average number of cycles in a randomly chosen n-permutation p is $\sum_{i=1}^{n} \frac{1}{i}$ and that, for n sufficiently large, p fixes no element of $[n]$ whatever with probability greater than $\frac{1}{3}$.

Chapter 4 (*In Any Way But This. Pattern Avoidance. The Basics.*) presents the notion of pattern avoidance. Thus the permutation-qua-linear-order 3451267 of [7] avoids pattern 321 in that it contains no decreasing subsequence of length 3, whereas it contains pattern 2134 in the guise of

subsequence 4267 (likewise 5167). To begin, $S_n(q)$ is defined as the number of n-permutations that avoid pattern q, and it is shown that, where q is any length-3 pattern, $S_n(q) = \frac{\binom{2n}{n}}{n+1}$, which is the n^{th} Catalan number. Since no such results are known for patterns of length exceeding 4, the remainder of the chapter is given over to two long-time conjectures, both recently proved. First, the Stanley–Wilf Conjecture from 1980 states that, for any pattern q, there exists a constant c_q with $S_n(q) \leq c_q^n$ for all $n \geq 1$, which says in effect that $S_n(q) \ll n!$ eventually. The Füredi-Hajnal Conjecture is a similar claim concerning Boolean matrices. M. Klazar's argument that Füredi–Hajnal implies Stanley–Wilf is presented, followed by the proof of Füredi–Hajnal due to A. Marcus and G. Tardos. (Their celebrated paper appeared only in 2004, and Klazar's proof dates from 2000.)

Whereas Chapter 4 focuses on the size of the several $S_n(q)$, Chapter 5 (*In This Way. But Nicely. Pattern Avoidance. Followup.*) shows that, for at least some patterns q, the sequence $\{S_n(q)\}_{1\leq n}$ is well behaved. Here good behavior means being *polynomially-recursive* (or *P-recursive*), where a sequence $\{a_n\}$ of complex numbers is P-recursive provided that there exist $P_0, \ldots, P_k \in \mathbb{Q}[n]$ with $P_k \neq 0$ such that

$$P_k(n+k) \cdot a_{n+k} + P_{k-1}(n+k-1) \cdot a_{n+k-1} + \ldots + P_0(n) \cdot a_n = 0$$

for all $n \in \mathbb{N}$. (Incidentally, the sequence $\{n!\}_{0\leq n}$ is P-recursive by virtue of $(n+1)! - (n+1)n! = 0$, as is the sequence of Catalan numbers [since $(n+2)C_{n+1} - (4n+2)C_n = 0$].) In the course of this chapter, it is shown that $\{S_n(1342)\}_{0\leq n}$ and $\{S_n(132)\}_{0\leq n}$ are P-recursive sequences. With regard to the latter, what the author in fact establishes is stronger, namely, that $\{S_{n,r}(132)\}_{0\leq n}$ is a P-recursive sequence for arbitrary r fixed, where $\{S_{n,r}(q)\}$ is the number of length-n permutations containing precisely r copies of pattern q. Later, the author takes up the question, Given n, how many copies of pattern q can be "packed into" some length-n permutation or other? This leads to a notion of the *packing density* $g(q)$ of pattern q, defined as a certain limit, and $g(132)$ is shown to be 0.464.

Chapter 6 (*Mean and Insensitive. Random Permutations.*) turns to the probabilistic viewpoint: for instance, if an n-permutation qua linear order is chosen at random, how many ascending runs will it have? (The answer turns out to be $\frac{n+1}{2}$ (Example 6.24).) Or, conceived functionally, how many 2-cycles will it have? (Answer: $\frac{1}{2}$ (Example 6.27).) Finally, the length of the longest increasing subsequence of a randomly selected n-permutation is at least $\sqrt{n}$ (Corollary 6.38). (Note again that 'increasing subsequence' is a more general notion that 'ascending run.') Probability theory is developed in the course of proving several classical results concerning Standard Young Tableaux (SYTs), which play a big role in Chapter 7. Much of the chapter is devoted to a probabilistic proof of the Frobenius formula stating that the number of pairs of SYTs on n boxes having the same Ferrers shape is none other than $n!$.

In Chapter 7 (*Permutations vs. Everything Else. Algebraic Combinatorics of Permutations.*), the author provides an overview of the combinatorial connections between permutations and other sorts of objects (such as SYTs and simplicial complexes). The Robinson–Schensted–Knuth (*risk*) correspondence between n-permutations and pairs of n-box SYTs having the same shape is described and shown to be a bijection (Theorem 7.1), which amounts to an alternative, nonprobabilistic proof of the Frobenius formula. Along the way, the author uses SYTs to prove that, for any fixed $1 \leq k \leq n$, the sequence $\{S_n(12\ldots k)\}_{1\leq n}$ is P-recursive, thus providing a link to Chapter 5. It is noted that this is the only known result establishing P-recursiveness for an infinite number of patterns. A theme of this chapter is that natural properties of permutations correspond to natural properties of SYTs. In that spirit it is shown that, where $\text{risk}(\pi) = \langle P, Q \rangle$, then any descent

within permutation-qua-linear-order π corresponds to a descent, appropriately defined, within SYT Q (Theorem 7.15). Section 7.2 describes two ways in which a partial order may be imposed on S_n, namely, by using either the *Bruhat order*, based on inversions, or the *weak Bruhat order*, based on transpositions (adjacent out-of-order entries). The number of maximal chains in the latter poset is then shown to coincide with the number of so-called *balanced tableaux* having a certain Ferrers shape. Finally, given a Ferrers shape, the number of balanced tableaux having that shape is the same as the number of SYTs having that shape (Theorem 7.29).

In final Chapter 8 (*Get Them All. Algorithms and Permutations*), programmable algorithms for generating all n-permutations, alternatively, all 231-avoiding permutations are described in detail. Next, n-permutation p is classified as *stack-sortable* if, using a single stack in a rather circumscribed manner, one can transform p into identity permutation $12\ldots n$. It is then shown that a permutation is stack-sortable just in case it avoids pattern 231, which means that many n-permutations are not stack-sortable. Some of these are *two-stack-sortable*—sorting, using the mentioned stack, and afterward sorting the result produces $12\ldots n$. That all n-permutations are $(n-1)$-stack-sortable ($n-1$ passes) is left as an exercise. An alternative, nondeterministic use of a stack due to D. Knuth is described and the resulting classification of n-permutations is then related to stack-sortability (Proposition 8.31). Knuth's notions of *deque-obtainability* and *deque-sortability* round out the chapter. (A double-ended queue has the capabilities of both a stack and a queue.)

3 Opinion

The book is intended as a graduate textbook and will surely succeed in giving its readers an overview of our current knowledge of permutations, formulæ for enumerating them, and algorithms for generating them, possibly with restrictions. The author's conjecture-driven approach in Chapters 4 and 5 is especially good and even rather exciting, and the reader thereby obtains a clear sense of how the field has developed as well as how much remains to be done. We found the author's explanations very clear, and there is an abundance of useful examples and helpful figures. Each chapter of the text is following by several dozen exercises, some quite challenging, and solutions to odd-numbered exercises appear in the back of the book. There is a rich bibliography for those seeking more information or full proofs of cited results. Finally, the book was a joy to read; it is *remarkably* well written in an English to meet any standard. We recognized very few typographical errors.

We feel compelled to find some fault with this excellent book, and here it is. We could see no difference between the author's 'propositions' and his 'theorems'—both numerous; both sorts of statements may or may not be followed by proofs, for instance. Some, but not all, 'examples' have proofs and are immediately followed by corollaries. The typography, although generally very good, does not support this; the label 'Example' is given in a rather small font followed by a 'PROOF,' and the body of an example is nonitalic, utterly unlike other statements accompanied by demonstrations. The proofs of some theorems are continued after the statements and proofs of needed lemmas with no helpful demarcations ("Continuation of proof of Theorem ..."). Finally, at least one lemma (3.34) has a corollary with no theorem or proposition in sight; the status of Lemma 3.36 is also unclear. Lemma 1.16 on page 12 giving a closed formula for Stirling numbers of the second kind is important enough to figure in the proof of capstone Theorem 3.71 (Schlömilch's formula) on page 114. This nonstandard approach to chapter organization may impede some readers' comprehending the structure of the author's highly purposeful discussion.

Review of [4]
Enumerative Combinatorics
Author of Book: Charalambos A. Charalambides
Publisher: Chapman & Hall/CRC
ISBN L-58488-290-5, Hard Cover, 609 pages
Reviewer: Sergey Kitaev
Mathematics Institute, Reykjavík University, Reykjavík, Iceland, sergey@ru.is

1 Introduction

Combinatorics is a branch of mathematics concerning the study of discrete (and usually finite) objects. *Enumerative combinatorics* is a branch of combinatorics concerned with counting objects satisfying certain criteria. An example of a problem in enumerative combinatorics is the following question: "In how many different ways can you place 8 rooks on a chessboard so that none can take another?" The answer to this question is given by 8!=40320. The earliest books about combinatorics are from India, dating from around 300 BC, but combinatorics came to Europe in the 13th century through two mathematicians, Leonardo Fibonacci and Jordanus de Nemore. Nowadays combinatorial methods are used widely not only in other areas of mathematics, but also in many other fields of science, in particular in theoretical computer science, in physics and in biology. The book being reviewed here provides a systematic coverage of the main notions of enumerative combinatorics and it is designed to serve as a textbook for introductory or intermediate level enumerative combinatorics courses usually given to advanced undergraduate or first year graduate students in mathematics, computer science, combinatorics, or mathematical statistics. This book may be of interest to those interested in operations research, physical and social sciences.

2 Summary of contents

In Chapters 1–4 three basic combinatorial principles are discussed: those of addition and multiplication, as well as inclusion-exclusion. Along with these principles, the notions of recurrence relation and discrete probability are introduced. The symbols of summation and product are presented and some of their properties are discussed. Permutations, combinations, partitions of a finite set, integer solutions of a linear equation, and enumeration of lattice paths are considered. Also, Vandermonde's factorial formula, Newton's binomial formula, the multinomial formula, and Stirling's approximation formula are presented.

Chapter 5 deals with enumeration of permutations with fixed points and a related problem of enumeration of permutations with successions. The famous problem of coincidences is examined in the same chapter.

Chapter 6 is devoted to a thorough presentation of generating functions.

Chapter 7 deals with basic methods of solving linear recurrence relations.

In Chapter 8, one has an extensive treatment of the Stirling numbers of the first and second kind, which are the coefficients of the expansion of factorials into powers and of powers into factorials, respectively. In addition, the coefficients of the expansion of generating factorials into usual factorials are examined in the chapter.

[4]

Chapter 9 deals with enumeration of distributions (of balls into urns) and occupancy (of urns by balls).

A few elementary aspects of the combinatorial theory of partitions of integers are discussed in Chapter 10. In particular, a number of classical q-identities are included in the chapter.

Chapter 11 deals with the partition polynomials in n variables. The coefficient of the general term of these polynomials is the number of partitions of a finite set of n elements in specified numbers of subsets of the same cardinality and the summation is extended over all partitions of n. The inverse of a power series by using the potential polynomials is presented in the same chapter.

Chapter 12 is devoted to enumeration problems emerging from the representation of a permutation as a product of cycles.

The problem of counting the number of equivalence classes of a finite set under a group of its permutations is the subject of Chapter 13.

Finally, Chapter 14 considers the Eulerian and the Carlitz numbers. These numbers are used to express the number of permutations with a given number of ascending runs and the number of permutations with repetitions with a given number of non-descending runs.

3 Opinion

Overall, this is a well-written book. In particular, I like the vast amount of exercises ranging in difficulty from very easy to quite hard, as well as the remarks following most of the definitions and theorems where a particular concept or result presented is discussed and extensions or generalizations of it are pointed out. Also, I like the brief bibliographic notes, mainly of historical interest, at the end of each chapter.

A neutral comment is that in many examples illustrating different concepts an accent is made on discrete probability type problems, which is not so surprising taking into account the background of the author.

My negative comments are as follows. The book contains a number of misprints: Roughly the first third of the book has at least 25 misprints, which is probably not that bad. It would not hurt to include in textbook of this kind, for example, by means of examples/excercises, some enumerative aspects of graph theory. A good candidate to be included in a book like this one is Cayley's formula giving the number of labeled trees. This formula is a good illustration of approaches to enumeration, and it can also be a nice example of using the Lagrange inversion formula considered in the book. In any case, my main negative comment is on the way in which some important concepts, in particular, famous number sequences, are introduced. As an example, I would like to discuss the *Stirling numbers of the second kind*. The first time the reader sees the notation $S(n, k)$ for these numbers is in problem 43 on page 96, but it says only in problem 44 on page 97 that $S(n, k)$ is in fact called the Stirling numbers of the second kind. Further, these numbers appear on page 150 in a different form where the notation is kept but the name for the numbers is emphasized as if they were just being introduced. On page 165, we meet these numbers again emphasized and in a slightly different form without any mention that the reader has already met these numbers. On page 202, in example 6.5, the numbers are introduced again as if for the first time. In addition, in the chapter devoted to these numbers, one meets yet another definition of them (keeping the same notation) on page 278, but no explicit link is made, at least not right away, to the other definition(s) of the numbers throughout the book (the first one of which is the most typical one in introductory combinatorics courses). I believe that it would be nicer if the Stirling numbers of the

second kind were introduced once somewhere in the beginning, to avoid possible confusion with equivalent definitions/properties of these numbers. Similar comments can be made about some other objects in the book.

In any case, I believe that this is a nice book, though not the easiest one to read among introductory books in combinatorics because of many rather advanced, but interesting topics included in the second half of the book. This book indeed should be suitable for first year graduate students or advanced undergraduates.

Review[5] of
Geometric Algebra for Computer Science
Authors: L. Dorst, D. Fontijne, and S. Mann
Morgan Kaufmann Publishers, 2007
626 pages, Hardcover

Review by
Brittany Terese Fasy brittany@cs.duke.edu
and David Millman dave@cs.unc.edu

1 Introduction

This book provides an in-depth introduction to the area of geometric algebra (GA). Objects in geometry, e.g. lines, planes, circles, spheres and tangents, have mathematical descriptions involving the coordinates of these objects. (These primitive geometric objects are represented by blades in GA). Heavily relying on linear algebra to perform operations such as rotations and projections, geometric algorithms are notoriously difficult to program. GA, however, uses the geometric objects as the basic elements of computation. The underlying linear algebra is abstracted so that the operations act directly on the geometric objects. This book defines geometric algebra to the novice as well as explains an implementation of GA.

2 Summary

The preface provides the history of geometric algebra. It briefly describes the connection of Clifford and Grassman Algebras to GA. Then, the first chapter of the book motivates why the reader should want to use geometric algebra, and provides an outline of how the book will proceed.

The first chapter also acknowledges the fact that the notation and terminology used in the book is similar, yet notably different, from linear algebra terminology. Since their notation deviates from traditional linear algebra, acknowledging the similarities and differences helps the reader to realize that s/he must be familiar with the definitions that appear in the first few chapters in order to understand the concepts presented throughout this book. Although this creates more work initially from the reader, the choice of their terminology and notation is deliberate and defended. For example, a linear transformation acting on a vector x is denoted $f[x]$ as opposed to $f(x)$ to emphasize the linearity of the operation.

Part I develops the concepts and ideas used by Parts II and III by giving the necessary background for anyone interested in geometric algebra. This part begins with familiar concepts of linear algebra (vectors and dot products) and redefines them in GA terminology. It starts by introducing operators such as outer product, scalar product and contraction, while weaving in the introduction of geometric elements such as k-vectors, k-blades, oriented areas and oriented volumes. Each new element is given a clear geometric interpretation; for example, taking the outer product of k vectors forms a k-blade. This k-blade represents an oriented area or volume; whereas, vectors represent space.

Using the geometric tools and concepts developed, the book further explains how to compute standard geometric operations, such as projections, using the initial set of primitives. Towards the end of the first part the geometric product is introduced tying together many of the operations already explained. Standard operations are reconsidered, generalized and simplified through application of the geometric product. It should be noted that these methods are always done geometrically so in the projection example, a projection matrix is never explicitly computed but instead constructed from the primitives. In addition, Part 1 introduces the meet (union) and join (intersection) operations, rotations through rotors, and the concept of a versor. Although the reader may be familiar with some of these topics, it is important for even the expert to familiarize him/herself with the subject matter of Part I in order to understand the subsequent sections.

There are three models of geometries that this book focuses on: the vector space model, the homogeneous model, and the conformal model. In the vector space model, there are two basic units: the point and the direction vector. This model allows for the operations of rotations and reflections. In the homogeneous model, the operation of translation is introduced. Finally, the conformal model allows for all angle-preserving transformations, such as the spherical inversion, using a 5D model to represent 3D Euclidean geometry.

Part I of this book used the vector space model to illustrate concepts. Part II explains in detail all three models, as well as presents many applications of the models and dual representations, including a comparison of how all three models treat reflections. The remainder of the section focuses on the conformal model, and provides many examples, including how to compute voronoi diagrams and how to smoothly interpolate motions.

Part III uses GA to implement a ray tracer. This section of the book begins by offering alternative implementation approaches, explaining the strengths and weaknesses of each. For example, using a matrix algebra representation would be wasteful as many of the matrices created will be sparse. Then, implementations of operations is detailed using the conformal model of Euclidean geometry. Chapter 22 considers efficiency issues, aiming to have a set of GA primitives that is at least comparable to those based in linear algebra. Chapter 23 ties everything together to complete the ray tracer.

In addition to the main text, this book has a large appendix that goes through the derivations which the authors feel are be too distracting to put within the chapters. Furthermore, there is a website *www.geometricalgebra.net* that provides a library of code. GA Sandbox provides a C++ implementation of the examples given in the textbook, providing the necessary framework to start using GA techniques while programming. GA Viewer is an interactive environment that can be used to generate and interact with geometric figures. Every example that appears in the book is also provided online. The examples provided allow for a programmer to quickly become comfortable working with the code.

On the website, the authors also provide a page on the relationship between quaternions and

geometric algebra. This page was added after the authors discovered that those who were purchasing their book were also interested in quaternions, demonstrating the level of commitment that they have for their audience.

3 Opinion

Assuming only previous knowledge in linear algebra and calculus, the authors intended this book to be for professionals and graduate students in computer graphics, gaming, and geometric modeling. Experience in graphics is not assumed, but would probably be helpful. In addition to those prerequisites stipulated by the authors, we believe that familiarity with object oriented programming is also necessary.

This book is well-suited for self-study, as long as the reader is willing to start from the beginning. Since the terminology and notation may not be familiar to the reader, it is difficult to jump to a chapter in the middle of the book without understanding what precedes that chapter. That being said, they use this novel-like style in order to help the reader develop an intuition for the methods of GA.

There are a few minor deficiencies that are worth noting in this review. The examples given in the first chapter of the book are overwhelming to someone who is unfamiliar with GA. They present concepts that are detailed later in the book, but cannot fully explain the examples they do provide. To some, the usefulness of GA can be buried under the plethora of new notations and concepts. Second, it is difficult to use this book as a reference unless you have read it in its entirety, since concepts are explained and built up rather than concisely stated. Finally, there are some inconsistencies in the formatting of the chapters. Some chapters end with a full summary of the chapter (e.g. chapter four), and some do not (e.g. chapter six). Other chapters have definitions italicized and separated from the text as in chapter seven, but most chapters do not do this.

Despite the criticisms discussed above, this book was very carefully organized and well-written. It is full of examples, geometric interpretations of theoretical results, and applications of the theory. Below, we list the key strengths of this book:

- The online resources are invaluable to someone new to geometric algebra.
- The authors were upfront about the organization of the book. The introduction to each chapter explained how it fit into the overall framework of their methodology.
- Each section concludes with drills (when appropriate), structural exercises, and programming exercises. The drills and structural exercises aim at developing an intuition for GA. Furthermore, the exercises and the examples demonstrate how to implement GA by providing real applications of the theory. For example, chapter five has an exercise on floating point issues and visualizing Julia Fractals is an exercise in chapter seven.
- The authors provide motivation for using GA. They explain why one should abstract the geometric ideas from the underlying linear algebra as well as explain decisions that they made in their implementation. For example, crystallography and camera calibration are used as motivating examples in chapter ten.
- The book focuses on important topics for their implementation, as well as introduces a breadth of GA tools and techniques. For example, they spend a great deal of time explaining the outer

product and the contraction operations since they are integral to the geometric techniques in Part II. On the other hand, the definitions of the operations of revision and grade involution were described more concisely since a more thorough description was not necessary.

- In general, the authors tend to put the derivations in the appendix or refer the reader to another source, but demonstrate briefly with an example or a diagram. However, topics that are too abstract to understand by an example or a diagram alone, such as the transforming dual representation in chapter 4, are derived within the text itself.

- The authors are very aware of the common misconceptions that arise when studying GA. For example, they are aware that the quaternions are commonly used in graphics, but very few who implement the quaternions understand how or why. In chapter seven, a short by very clear geometric interpretation of unit quaternions is given as it is a specific use of rotors in $\mathbb{R}^3$. In addition, homogeneous coordinate is well illustrated in chapter 11. The treatment of these two topics alone is so well articulated that a novice and an expert alike can appreciate the eloquence.

In summary, *Geometric Algebra for Computer Science* provides a thorough introduction to GA. It explains the primitives of GA, builds intuition for working with geometric objects as opposed to points and lines, defines basic operations on these objects, generalizes until operators can even act on other operators, and constructs an implementation of the theory. This book is an excellent resource for learning and motivating your learning of the subject. The authors have provided all of the resources necessary for a graduate student or a professional to begin learning and using the techniques of geometric algebra.

Review of[6]
Privacy on the Line: The Politics of Wiretapping and Encryption
Authors of Books: by Whitfield Diffie and Susan Landau
The MIT Press; 2nd Edition 2007 400 pp., $27.95, Hardcover

Review by
Richard Jankowski rjankowski@acm.org

1 Introduction

You would be hard-pressed to find two more authoritative experts on the field of cryptography and privacy than Whit Diffie and Susan Landau. In their important and timely book, *Privacy on the Line*, they explore the history and politics surrounding wiretapping and encryption and the associated impact on personal privacy.

This book engages the reader on several levels - first it's a well-written book that will keep the reader interested with the numerous espionage and law enforcement stories. Second, you can finish the book and see how politics have shaped our society, both from a technological and right to privacy point of view.

[6]

2 Summary

Chapter 1 is an introductory chapter detailing the impact that technology of communications has on today's society. The issue of wiretapping and its associated abuses is discussed, and the effect encryption has on keeping communications secure.

Chapter 2 is a complete layman's introduction to the basics on cryptography. You're probably not going to find a more readable introductory overview of cryptography anywhere. The authors cover topics such as the various cryptosystems, the strengths and weaknesses of encryption and, and the effect encryption has on business processes. The authors stay completely non-technical in this chapter, while still offering a great overview of the subject.

Chapter 3 discusses cryptography's effect on public policy in an engaging chapter starting with the mechanization of cryptosystems in World War II to modern day concerns. The authors cover how we got to where we are with modern-day cryptography, and the politics and issues surrounding DES.

Chapter 4, entitled "National Security," is a complete overview of the intelligence field. The authors outline the various forms of intelligence, and cover topics such as information warfare and counterintelligence. A clear association is drawn between communications and information assets and their importance to the intelligence community.

While the previous chapter was a overview of the intelligence community, Chapter 5 covers the law enforcement community. Topics such as police wiretaps and electronic surveillance are discussed as well as the effects of the US PATRIOT act.

Chapter 6 is an introduction to privacy as a right. The authors discuss privacy as it affected early American colonists, subsequent litigation of privacy issues, through the erosion of personal privacy affecting citizens today. One of the most poignant statements of the book come from this chapter where the authors argue about the importance of privacy to a democratic society.

Chapter 7 covers wiretapping and the legal and political implications of the use of wiretaps.

Chapter 8 covers the topic of communications in the 1990s. The issue of wiretapping this technology is explored with many historical examples covering civilian and diplomatic targets.

Chapter 9 covers the evolution of encryption in the 1990s, with coverage of Philip Zimmermann's Pretty Good Privacy application and the politics and issues surrounding the proposed key-escrow system within the Clipper Chip.

Chapter 10 covers the modern impact cryptography had on society since the late 1990's. The authors start with the process of the government's selection of the Advanced Encryption Standard and discuss some of the negative impacts of cryptography, such as the use of steganography and watermarking in digital rights management systems.

Chapter 11 discusses the topics affecting privacy today, from the expansion of intelligence after the September 11 attacks, to the PATRIOT act and the response to terrorism.

Chapter 12 is a conclusion to the book where the authors discuss the overall political landscape and argue that by failing to ensure that our current computer and communications infrastructures are not adequately secured, we will further erode what little privacy we have left.

3 Opinion

Privacy on the Line is a lucid book that explores the topic of personal privacy. The writing is captivating, taking the reader from one story to the next in a seamless transition that illustrate the

historical and political undertones of the world in which we live. The authors cover the technology background in a very readable way, making this book approachable by someone with no technical background. The authors are experts in their field, passionate about the encroachment of an individual's right to privacy, and are able to communicate their message in a very effective manner.

I would not hesitate recommending this book to anyone who is interested in privacy or security topics.

@inproceedings{Stinson2003CombinatorialDC, title={Combinatorial designs: constructions and analysis}, author={Douglas R. Stinson}, booktitle={SIGA}, year={2003} }. Douglas R. Stinson. Published in SIGA 2003. Mathematics, Computer Science. Introduction to BIBDs.- Symmetric BIBDs.- Difference sets and automorphisms.- Hadamard matrices and designs.- Resolvable BIBDs.- Steiner triple systems.- Mutually orthogonal Latin squares.- Pairwise balanced designs.- t-designs.- Orthogonal arrays and codes.- Index. View on ACM. Finding books BookSee | BookSee - Download books for free. Find books.Â Combinatorial designs. Constructions and analysis. Douglas R. Stinson. 17.20 Mb. #22. Cryptography: Theory and Practice, Third Edition (Discrete Mathematics and Its Applications). Douglas R. Stinson. 22.75 Mb. Combinatorial Designs book. Read reviews from worldâ€™s largest community for readers. Created to teach students many of the most important techniques used...Â Combinatorial Designs: by Douglas R Stinson. Other editions. Want to Read savingâ€¦ Error rating book. Refresh and try again. Rate this book. Clear rating.Â In these settings, the student will master various construction techniques, both classic and modern, and will be well-prepared to construct a vast array of combinatorial designs. Design theory offers a progressive approach to the subject, with carefully ordered results. It begins with simple constructions that gradually increase in complexity. Each design has a construction that contains new ideas or that reinforces and builds upon similar ideas previously introduced.