

BOOK REVIEW

Designs and their codes, by E. F. Assmus, Jr., and J. D. Key. Cambridge University Press, London and New York, 1992, x + 352 pp., \$69.95. ISBN 0-521-41361-3

The announcement several years back of the nonexistence of a projective plane of order ten brought both elation and a lingering sense of disappointment to the mathematics community. The disappointment was due in part to the “proof” being supplied by a computer. But perhaps more significant was the prevailing opinion that much of what was accomplished in solving this problem applied only to the plane of order ten. In effect, outside of some programming advances, we failed to “learn anything”. However, one can argue very much to the contrary that the projective plane of order ten served as a catalyst to the community that coding theory can play a very significant role in the study of combinatorial designs. Indeed, much of what is contained in *Designs and their codes* speaks to the tremendous influence the plane of order ten has subsequently had on the analysis and classification of designs in a much broader context than projective planes. As the recent book of van Lint and Wilson [7] testifies, coding theory is finding a place in the mainstream of combinatorics. This new book by Assmus and Key is a welcome addition to a very exciting and relatively new application of an established discipline to combinatorics.

To bring the story into focus, we briefly recount the influence of coding theory on the resolution of the plane of order ten. Put simply, a projective plane of order ten is a collection of 111 subsets of size eleven from the set $\{1, 2, \dots, 111\}$ with the special property that any two subsets have precisely one element in common. Generally, a projective plane of order n is a collection of $n^2 + n + 1$ subsets (called *lines*) of size $n + 1$ from a set of *points* $\{v_1, v_2, \dots, v_{n^2+n+1}\}$ with the special property that any two subsets have precisely one element in common.

Construction of a projective plane of order n is immediate (but often not unique) when n is a power of a prime: take as the $(n^2 + n + 1)$ -set of points the one-dimensional subspaces of $V = GF(n) \times GF(n) \times GF(n)$. Take for lines the two-dimensional subspaces of V , i.e., the *hyperplanes*. A quick check shows that each line has $n + 1$ points and that the intersection of any two lines (hyperplanes) is a point (one-dimensional subspace). Moreover, there are precisely $(n^3 - 1)/(n - 1) = n^2 + n + 1$ lines.

This construction implies the existence of projective planes of orders 2, 3, 4, 5, 7, 8, and 9. The case $n = 6$ is ruled out by the famous Bruck-Ryser-Chowla theorem which asserts that for $n \equiv 2 \pmod{4}$ a necessary condition for the existence of a projective plane of order n is that n be the sum of two squares. This leaves $n = 10$ the first instance where *existence* would be nontrivial.

Associated with any projective plane of order n is its incidence matrix A : a square matrix of size $n^2 + n + 1$ with rows indexed by the lines, columns indexed by the points, and entry (i, j) of the matrix set to 1 if point v_j is on line i , and 0 if otherwise. The definition of a projective plane implies that

$$AA^t = nI + J = \begin{bmatrix} n+1 & 1 & \cdots & 1 \\ 1 & n+1 & & \vdots \\ \vdots & & \ddots & 1 \\ 1 & \cdots & 1 & n+1 \end{bmatrix}$$

where I is the identity matrix of size $n^2 + n + 1$ and J is the matrix of all ones of the same size. It follows that the all-one vector is an eigenvector of AA^t with eigenvalue $(n+1)^2$ and that there are $n^2 + n$ eigenvectors $(1, -1, 0, \dots, 0)$, $(0, 1, -1, 0, \dots)$, \dots with eigenvalue n . In particular, this implies that $|A| = (n+1)n^{(n^2+n)/2}$.

In 1970 Professor Assmus suggested at a meeting in Oberwolfach that one consider the $GF(2)$ vector subspace of $V = [GF(2)]^{111}$ generated by the rows of the incidence matrix of a projective plane of order ten. Since the study of subspaces of finite vector spaces is within the realm of coding theory, it was hoped (quite correctly) that the theorems and techniques of coding theory might shed significant new light on the structure of a plane or even prove that it could not exist. In particular, Assmus described interesting constraints that would have to hold on the *weight enumerator* of the code associated with the plane.

A code C is any subset of S^n where S is an arbitrary finite set. An individual element $\mathbf{c} \in C$ is called a *codeword*. When $S = \{0, 1\}$, the code is said to be *binary*; when $S = \{0, 1, 2\}$, the code is *ternary*; etc. Together with a code comes a distance function, commonly referred to as the Hamming distance, which is defined as the number of coordinate positions in which two codewords differ:

$$d(\mathbf{x}, \mathbf{y}) = |\{i : x_i \neq y_i, 0 \leq i \leq n\}|.$$

When $S = GF(q)$ and C is a k -dimensional vector subspace of S^n , the code is said to be a q -ary $[n, k]$ linear code. This means, in particular, that sums of codewords are codewords and the zero vector $\mathbf{0} = (0, 0, \dots, 0)$ is also a codeword. When $\mathbf{0} \in C$, as it is for linear codes, the weight of a codeword is defined by

$$w(\mathbf{x}) = d(\mathbf{x}, \mathbf{0});$$

that is, the weight of a codeword is the number of its nonzero components.

Since a linear code is finite, one can at least theoretically define A_j to be the number of codewords of weight precisely j in the code. The *weight enumerator* of an $[n, k]$ code C is the polynomial

$$W_C(X, Y) = \sum_{j=0}^n A_j X^j Y^{n-j}.$$

Even though it is usually impossible to compute the weight enumerator for an arbitrary code of large dimension (the codes for the planes of order 2, 3, and 4 are known; for orders 5 and 7 they are not known), in fact, Assmus and Mattson [1] showed that the weight enumerator for the plane of order ten would be completely determined by A_{12} , A_{15} , and A_{16} .

In showing this, they used what is probably the most striking and useful theorem in coding theory. This, of course, is the theorem of MacWilliams:

Theorem (MacWilliams). *Let C be an $[n, k]$ code over $GF(q)$. Denote by C^\perp the $[n, n - k]$ linear code of vectors perpendicular to C , i.e.,*

$$C^\perp = \left\{ v \mid (v \cdot w) = \sum_{i=1}^n v_i w_i = 0, \forall w \in C \right\}.$$

Then the weight enumerators for C and C^\perp are related by

$$W_C(X, Y) = \sum_{j=0}^n A_j X^j Y^{n-j},$$

$$W_{C^\perp}(X, Y) = \frac{1}{|C|} W_C(Y - X, Y + (q - 1)X).$$

In the case of a projective plane of order ten, the p -ary code, p a prime, generated by the rows of the incidence matrix for the plane would be all of $[GF(p)]^{111}$ when p is not 2, 5, or 11. When $p = 11$, it would have co-rank 1. When $p = 2$ or 5, the dimension of the code would be precisely 56. Moreover, for these primes $C^\perp \subset C$. (These details are part of the lovely and more general Theorem 4.6.2.) What is more striking still is that if one were to append a column of all ones to the incidence matrix of the plane of order ten, the dimension of the binary code C thus generated would remain the same; but now $C^\perp = C$, and all the codewords would have weights divisible by four (a *doubly even* code).

Using this information, MacWilliams, Sloane, and Thompson [9] provided the first significant cutdown in the amount of work necessary to affect an exhaustive search for the plane. They were able to show that any line of the plane would necessarily intersect any even-weighted codeword in an even number of points. This simple fact led the way to showing that $A_{15} = 0$ and that an exhaustive search was possible. In 1983 it was announced that $A_{12} = 0$ and soon after that $A_{16} = 0$. At this point the full weight enumerator was known. The rest of the story involved hypothesizing starting configurations and using the computer to show they could not be extended to a full plane. The interested reader should consult the marvelous summary article by Lam [4], who affectionately recounts the full story from the perspective of someone intimately involved in its resolution.

Designs and their codes is an advanced-level text suitable for both investigating and teaching the evolving connections between combinatorial designs and the codes they generate. The book is organized into two parts. The first five chapters are introductory: two devoted to design theory, two devoted to coding theory, and one devoted to the geometry of vector spaces. The final three chapters focus on applications of coding theory to various classes of designs. Exercises are scattered throughout the text, but unfortunately solutions and hints are rarely given. Whereas the introductory chapters can be skipped by the expert or the reader who is only interested in a specific application covered in a later chapter, there is much gold to be mined in the early sections.

Chapter 1 provides an introduction to designs. There the fundamental object, a $t = (v, k, \lambda)$ design, is defined through incidence relations but is equivalent to a collection of k -subsets (called *blocks*) of a v -set (called *points*) with the property that every t -subset is contained in precisely λ blocks. The automorphism group of a design is defined to be the largest group of permutations on the points which

induces a permutation on the blocks. One important result of this section is the statement and proof of Block's theorem which implies that any subgroup of the automorphism group of a t -design has at least as many block orbits as point orbits.

Chapter 2 gives a brief historical introduction to error-correcting codes and quickly moves on to their algebraic properties. Several of the standard codes associated with designs are defined and examined. For any one design the focus throughout the book is on four related codes: $C, C^\perp, C \cap C^\perp = \text{Hull}(C)$, and $\text{Hull}(C)^\perp$ where C is generated from the row space of an incidence matrix for the design over an appropriate finite field. Klemm's Theorem (Theorem 2.4.2) is presented and proved—this theorem gives bounds on the dimensions of the codes associated with any 2-design.

Together, Chapters 2 and 5 present most of the standard linear codes that appear in the theory. Hamming, maximum distance separable (MDS), quadratic residue (QR), BCH, and general cyclic codes are covered in Chapter 2. Chapter 5, under the heading "Geometric Codes", covers the Reed-Muller and generalized Reed-Muller codes. These later codes arise in the analysis of designs coming from finite geometries. The presentation in this chapter is rather novel and provides a new perspective to these important codes. The downside is that the notation is cumbersome and difficult to follow if care is not taken to read the entire chapter. This extends to the definitions, as the following illustrates:

Definition 5.6.1. The *nonprimitive generalized Reed-Muller code* $\mathcal{R}_{F_q}^b(\nu, m)^*$ of order ν , where $0 \leq \nu < m(q-1)$ and b divides $q^m - 1$, is the code of length $n = (q^m - 1)/b$ and dimension

$$|\{j \mid 0 \leq j \leq q^m - 1, b \text{ divides } j, w_q(j) \leq \nu\}|$$

given as the set of vectors

$$\{(q(1), q(\omega), \dots, q(\omega^{n-1})) \mid q(X) \in \mathcal{Q}_{\nu/b}\}.$$

Chapter 4, "Symmetric Designs", concerns $t - (v, k, \lambda)$ designs for which the number of blocks equals the number of points. It is immediately deduced that $t \geq 3$ implies the design is trivial (i.e., $k = v - 1$). When $t = 2$, the possible parameter sets are known and given in Theorem 4.2.1. Surprisingly, whereas for $\lambda = 1$ there are an infinite number of known symmetric designs (i.e., projective planes), only a finite number of biplanes ($\lambda = 2$) have so far been constructed.

When a $2 - (v, k, \lambda)$ design has an automorphism group G of order v acting transitively on the points and blocks, we say any block forms a *difference set* in G . The theory of difference sets has a beautiful and distinguished history and is a very active area of current research in design theory. Since the focus of this book is on the coding theoretic aspects of symmetric designs, much of the material regarding difference sets is relegated to concluding remarks that provide references. However, difference sets reappear in the chapter on Hadamard designs.

The final three chapters examine planes, Hadamard designs, and Steiner systems, respectively. Here is where the material becomes very contemporary and most interesting. A sophisticated knowledge of classical groups and finite geometry above and beyond that given in the introductory chapters proves indispensable.

Chapter 6 examines codes from planes. Here the situation is reversed from what one normally expects: usually the dimension of a code is easily found, but the

codewords of minimum nonzero weight are not known. However, for a projective plane of order n the minimum nonzero weight of the code over $GF(p)$ for any prime $p \mid n$ is $n + 1$, and the codewords of this weight are precisely the scalar multiples of the lines of the plane. The actual dimension of the code is generally not known. The Hamada-Sachar conjecture (Conjecture 6.9.1) is a partial attempt to characterize planes coordinatized by finite fields (Desarguesian planes) by the ranks of their codes. It asserts that every projective plane of order p^s , p a prime, has p -rank at least $\binom{p+1}{2}^s + 1$ with equality if and only if it is Desarguesian. This conjecture is examined carefully, and partial results are proved. In addition, the chapter contains a thorough treatment of translation planes and a special section on Hermitian unitals which characterizes these objects through the codes of planes of order q^2 .

The goal of Chapter 7, "Hadamard Designs", is to provide a framework for the organization of these classical designs using a coding theoretical approach. A Hadamard 2-design of order n is a $2 - (4n - 1, 2n - 1, n - 1)$ symmetric design. Amongst all symmetric $2 - (v, k, \lambda)$ designs of order $n = k - \lambda$, they have the minimal value for v (projective planes have the maximum value). Combinatorially, all values of n are possible, and, indeed, it is conjectured that all values of n give rise to Hadamard designs. Hadamard designs give rise to Hadamard matrices in a natural way (a Hadamard matrix of size $4n$ is a $4n \times 4n$ matrix, each of whose entries is ± 1 and whose rows are orthogonal) and vice versa. Theorem 7.10.4 is a particularly beautiful and characteristic result, relating the codes of a Hadamard 3-design (parameters $3 - (4n, 2n, n - 1)$) with difference sets, bent functions, and the first-order Reed-Muller code.

Chapter 8 concludes the book with a discussion of Steiner systems: $t - (v, k, \lambda)$ designs with $\lambda = 1$, $t \geq 2$. These designs have roots in recreational problems dating to the previous century. Somewhat surprising for such a venerable problem, no examples are known for $t \geq 6$, only a finite number are known for $t = 4, 5$, while infinite classes are known for $t = 2, 3$. Unfortunately (as the authors point out) coding theory seems to play little role for the cases $t \geq 6$. The emphasis throughout this chapter is on $t = 2$ and 3, although one section is reserved for the famous Mathieu (or Witt) designs $4 - (23, 7, 1)$ and $5 - (24, 6, 1)$ arising as they do from the binary Golay code \mathcal{G}_{23} and its extension \mathcal{G}_{24} . The chapter concludes with sections on unitary designs (unitals) and oval designs coming from projective planes. Bounds are given for the dimensions of the codes, and group-theoretic constructions are given for the designs themselves.

Designs and their codes is a truly fascinating and useful book. It belongs on the shelves of all those who wish to be current on the state of design theory and who are seeking interesting problems in the field to pursue. References are meticulously maintained throughout, and there are useful symbol and subject indices. The strongest criticism, alluded to above, may be in the difficulty of understanding the statement of a particular theorem in the abstract or following the thread of one topic throughout the book. Notation, often not limited to the current section, is relied on very heavily, and it can be frustrating to gather together all the definitions necessary to bring a theorem to life. Fortunately each chapter has a lively introduction which includes a summary of the most important points to be covered, and special remarks are highlighted throughout the text. All in all, this is a book that rewards concentrated effort in kind.

REFERENCES

1. E. F. Assmus, Jr. and H. F. Mattson, Jr., *On the possibility of a projective plane of order 10*, Algebraic Theory of Codes II, Air Force Cambridge Research Laboratories Report AFCRL-71-0013, Sylvania Electronic Systems, Needham Heights, MA, 1970.
2. Th. Beth, D. Jungnickel, and H. Lenz, *Design theory*, Bibliographisches Institut Wissenschaftsverlag, Mannheim, Wien, Zürich, 1985.
3. D. R. Hughes and F. C. Piper, *Design theory*, Cambridge Univ. Press, Cambridge, 1985.
4. C. W. H. Lam, *The search for a finite projective plane of order 10*, Amer. Math. Monthly **98** (1991), 305–318.
5. C. W. H. Lam, L. Thiel, S. Swiercz, and J. McKay, *The nonexistence of ovals in a projective plane of order 10*, Discrete Math. **45** (1983), 319–321.
6. J. H. van Lint, *Introduction to coding theory*, Graduate Texts in Math., vol. 86, Springer-Verlag, New York, 1982.
7. J. H. van Lint and R. M. Wilson, *A course in combinatorics*, Cambridge Univ. Press, Cambridge, 1992.
8. F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland, Amsterdam, 1983.
9. F. J. MacWilliams, N. J. A. Sloane, and J. G. Thompson, *On the existence of a projective plane of order 10*, J. Combin. Theory Ser. A **14** (1973), 66–78.

M. A. WERTHEIMER
CENTER FOR COMMUNICATIONS RESEARCH