, , 1–22 ()

DESIGNS AND CODES: An update

E. F. ASSMUS, JR
Department of Mathematics, Lehigh University,Bethlehem PA 18015,U.S.A.

J. D. KEY*
Department of Mathematical Sciences, Clemson University, Clemson SC 29634, U.S.A.

Abstract. Since the publication in 1992 of "Designs and their Codes" significant progress has been made in the general area of codes coming from designs. This article reviews this progress and presents some of the results — including confirmation of certain conjectures made and answers to some of the questions raised in the book.

Keywords: Designs, codes, finite geometries

1. Introduction

"Designs and their Codes" [3] described the association of linear error-correcting codes with designs and collected together many of the significant known results. Recall that the linear p-ary code associated with a design $\mathcal{D}$ is equivalent to the row space over the finite field $\mathbf{F}_p$ (where p is a prime) of an incidence matrix for $\mathcal{D}$ with rows indexed by the blocks of $\mathcal{D}$ and columns indexed by the points. Various classes of designs were discussed in the book and the corresponding results concerning the codes were described and established. A second printing — with corrections but substantially unchanged — appeared in 1993; here we will review some of the classes of designs discussed in the book — updating the results — and also examine further cases not covered there. We arrange this survey into the following ten sections:

1. Introduction
2. Basic definitions and terminology
3. Projective and affine planes
4. Oval designs
5. Hadamard designs
6. Unitals
7. Steiner triple systems

* Support of NSF grant GER-9450080 acknowledged

8. Finite geometries and rigidity theorems

9. Dual structures and the "point" code of a design

10. Strongly regular graphs and their p-ranks

Notice that the survey is restricted to results related to codes associated with designs; thus there are some notable omissions concerning progress in design theory, in particular with respect to difference sets, where there have been important developments. (See [18] and [72] for a survey of recent results concerning difference sets.) We have, moreover, included nothing concerning the theory of Reed-Muller and generalized Reed-Muller codes, the subject of Chapter 5 of [3], since we have already prepared an updated version of that chapter which is available as a report [5] and will appear in *The Handbook of Coding Theory* — which is to be published by Elsevier.

2. Basic definitions and terminology

Our notation is quite standard and we refer the reader to the Glossary of [3]. We recall, however, some of the definitions we need.

An incidence structure $\mathcal{D}$ consisting of a block set $\mathcal{B}$ on a point set $\mathcal{P}$ of size v is a t-(v, k, λ) design — or t-design for short — if every block is incident with precisely k points and any set of t distinct points are together incident with precisely λ blocks. When $|\mathcal{B}| = |\mathcal{P}|$, t is at most 2 and, when $t = 2$, we refer to the *symmetric* design as a (v, k, λ) design. It follows (see [3], Chapter 1) that a t-design is also an s-design for any $s < t$; we denote the number of blocks incident with s points by λ_s. The order of a t-design, where $t \geq 2$, is $n = \lambda_1 - \lambda_2$. Because of the statistical origins of the theory, λ_1 is frequently denoted by r and λ_0 by b. We take the *incidence matrix* of an incidence structure to be the $|\mathcal{B}| \times |\mathcal{P}|$ matrix of 0s and 1s where the entry indexed by (B, x) is 1 if and only if the block B is incident with the point x.

For any field F, $F^{\mathcal{P}}$ is the vector space of functions from $\mathcal{P}$ to F with basis given by the characteristic functions of the singleton subsets of $\mathcal{P}$. If $\mathcal{D}$ is an incidence structure, the **code** $C_F(\mathcal{D})$ of $\mathcal{D}$ over F is the subspace of $F^{\mathcal{P}}$ spanned by the characteristic functions, v^B with B in $\mathcal{B}$, of the blocks of $\mathcal{D}$. Viewed concretely this code is simply the row space of an incidence matrix of the incidence structure. If $F = \mathbf{F}_p$ we write $C_p(\mathcal{D})$, or sometimes merely $C(\mathcal{D})$ if p is understood, and the dimension of $C_p(\mathcal{D})$ is referred to as the **p-rank** of $\mathcal{D}$. It is a well-known result, stated and proved in [3], Theorem 2.4.1, that the prime p must divide the order of the 2-design for the p-ary code of the design to be of any use or interest in any characterization. We wish to emphasize, however, that recent results indicate that in some cases, in particular in the case of Steiner triple systems, the column space of the incidence matrix — i.e. the code of the dual structure (see below) — is of interest for *any* prime p.

In considering the code C associated with a structure, it is necessary also to consider the orthogonal code $C^{\perp}$, where, in this update, the orthogonal is always

taken with respect to the standard inner product, namely $(u, w) = \sum_{x \in \mathcal{P}} u(x)w(x)$ for $u, w \in F^{\mathcal{P}}$. Thus

$$C^{\perp} = \{u \,|\, u \in F^{\mathcal{P}} \text{ and } (u, w) = 0 \text{ for all } w \in C\}.$$

Recall that for a design $\mathcal{D}$ and a field F, the following codes, closely related to $C_F(\mathcal{D})$, sometimes play an important role

$$C_F(\mathcal{D}) \cap C_F(\mathcal{D})^{\perp} = \mathrm{Hull}_F(\mathcal{D}) = H_F(\mathcal{D}),$$

$$C_F(\mathcal{D}) + C_F(\mathcal{D})^{\perp} = \mathrm{Hull}_F(\mathcal{D})^{\perp} = B_F(\mathcal{D}),$$

and

$$\langle v^B - v^C | B, C \in \mathcal{B} \rangle = \langle v^B - v^{B_0} | B \in \mathcal{B} \rangle = E_F(\mathcal{D}),$$

where B_0 is some fixed vector in $\mathcal{B}$. If F is $\mathbf{F}_p$, then H_p, B_p, and E_p have the obvious meaning.

Also of interest is the code of the dual structure $\mathcal{D}^t$ where, if $\mathcal{D}$ has block set $\mathcal{B}$ and point set $\mathcal{P}$, then $\mathcal{D}^t$ has block set $\mathcal{P}$ and point set $\mathcal{B}$ with a "block" x incident with a "point" B precisely when B was incident with x in $\mathcal{D}$. Concretely it is the column space of an incidence matrix for $\mathcal{D}$ which is the same as the row space of an incidence matrix for $\mathcal{D}^t$ since these matrices are transposes of one another. Even when $\mathcal{D}$ is a symmetric design the codes $C_F(\mathcal{D})$ and $C_F(\mathcal{D}^t)$ may not be isomorphic although they do, of course, have the same block length and dimension.

Recall that the weight of a vector is the number of non-zero coordinates. Clearly the code of a design will have minimum weight at most the block size k and the code of the dual structure will have minimum weight at most $\lambda_1 = r$.

3. Projective and affine planes

Finite projective planes of order n are symmetric designs with parameters $(n^2+n+1, n+1, 1)$ and finite affine planes are designs with parameters 2-$(n^2, n, 1)$, where again n is the order of the plane.

The basic general results concerning codes of planes are developed in [3], Chapter 6, and we state here the main results.

THEOREM 1 *Let Π be a projective plane of order n and let p be a prime dividing n. Set $H = \mathrm{Hull}_p(\Pi)$ and $B = H^{\perp}$. If k is the dimension of $C_p(\Pi)$, then B is an $[n^2+n+1, n^2+n+2-k, n+1]$ code and the minimum-weight vectors of B are precisely the scalar multiples of the incidence vectors of the lines of Π. Moreover, $\mathrm{Hull}_p(\Pi) = E_p(\Pi)$.*

Thus the plane can be retrieved from the minimum-weight vectors of $C_p(\Pi)$ and hence different planes must have different codes. There has been little progress in the main outstanding conjectures in this area, in particular the Hamada-Sachar conjecture (see [3], Conjecture 6.9.1):

Conjecture 1 *Every projective plane of order p^t, p a prime, has p-rank at least $\binom{p+1}{2}^t + 1$ with equality if and only if it is desarguesian.*

The Hamada-Sachar conjecture remains the most important conjecture; its truth would imply that the only planes of prime order are the desarguesian planes since, in the prime case, the p-rank of any projective plane of prime order p is $\binom{p+1}{2} + 1$.

Concerning the orthogonal code, the general result is

THEOREM 2 *If Π is a projective plane of order n and p is a prime dividing n, then the minimum weight of $C_p(\Pi)^\perp$ is at least $n + 2$. If the minimum weight is $n + 2$ then n is even, $p = 2$ and the minimum-weight vectors are all incidence vectors of ovals in Π.*

There are projective planes of even order — namely certain non-translation planes of order 16 — containing no ovals[1] (see [55]). Of course, the classical desarguesian planes always have ovals, namely those coming from conics, but for orders greater than 8 there are others and there has been progress both in producing and classifying these (see, for example, [53]). Moreover we know that the ovals generate the dual of the plane in this case: see Theorem 9 below.

The general situation for affine planes is outlined in the following theorem:

THEOREM 3 *If π is an affine plane of order n and p is a prime dividing n, then the minimum weight of $B = \mathrm{Hull}_p(\pi)^\perp$ is n and all minimum-weight vectors are constant* [2]*. Further,*

$$\mathrm{Hull}_p(\pi) = \langle v^L - v^M \mid L \text{ and } M \text{ parallel lines of } \pi \rangle.$$

We are left with the question concerning the nature of the minimum-weight vectors of $C_p(\pi)$, where π is an arbitrary affine plane. We know that the scalar multiples of the incidence vectors of the lines of π are among the minimum-weight vectors and that they are the only minimum-weight vectors when π is of prime order; moreover, when π is desarguesian these vectors are, again, the only minimum-weight vectors (see Theorem 5 below). Gordon Royle [59] has found a way to isolate the vectors of weight 9 in the ternary codes of each of the six non-desarguesian affine planes of order 9 and has determined that only the scalar multiples of the incidence vectors of lines occur. Knowledge of the Baer subplanes in each of these planes confirms this, since, by Corollary 6.4.2 of [3], page 211, any weight-9 vector in the ternary code of the plane must be the incidence vector of a line or a Baer subplane. It might thus be tempting to conjecture that the minimum-weight vectors of the code of any affine plane of order the square of a prime must be scalar multiples of the incidence vectors of the lines but we are not aware of any further evidence for this. The general case is still undecided. It is perhaps worth mentioning here that none of the weight distributions of the ternary codes of the seven affine planes of order nine has been computed. Here are the known results in the desarguesian case:

THEOREM 4 *Let p be any prime, $q = p^t$, and $\Pi = PG_2(\mathbf{F}_q)$. Then $C_p(\Pi)$ is a generalized Reed-Muller code and has dimension $\binom{p+1}{2}^t + 1$. The minimum-weight vectors of $C_p(\Pi)$ are the scalar multiples of the incidence vectors of the lines. Further,* $\mathrm{Hull}_p(\Pi)$ *has minimum weight $2q$ with the minimum-weight vectors the scalar multiples of the differences of the incidence vectors of distinct lines of Π. The minimum weight $d^\perp$ of $C_p(\Pi)^\perp$ satisfies*

$$q + p \leq d^\perp \leq 2q,$$

with equality at the lower bound if $p = 2$.

For affine planes we have

THEOREM 5 *If $\pi = AG_2(\mathbf{F}_q)$, then $C_p(\pi)$ is a generalized Reed-Muller code and has dimension $\binom{p+1}{2}^t$. The minimum weight of $C_p(\pi)$ is q, and the minimum-weight vectors of $C_p(\pi)$ are the scalar multiples of the incidence vectors of the lines of π. Further,* $\mathrm{Hull}_p(\pi)$ *has minimum weight $2q$, with the minimum-weight vectors the scalar multiples of the differences of the incidence vectors of distinct parallel lines in π. The minimum weight $d^\perp$ of $C_p(\pi)^\perp$ satisfies*

$$q + p \leq d^\perp \leq 2q,$$

with equality at the lower bound when $p = 2$.

Question 1 *If $\mathcal{D}$ is a finite projective or affine plane of order n, and p is a prime dividing n, what is the minimum weight of $Hull_p(\mathcal{D})$ and what is the nature of the minimum-weight vectors?*

We believe that the minimum weight is $2n$, but we have no idea how one might prove this. A projective plane with the property that the only minimum-weight vectors are the vectors $v^L - v^M$ where L and M are lines, was called "tame" in [3]. Desarguesian planes are tame and it is possible that only the desarguesian planes are tame, but we have no evidence for this.

The enumeration of translation planes has been pushed to order 49 by Rudi Mathon and Gordon Royle, [44]. All the 7-ranks have been computed and, curiously, all are odd. None meets the bound, namely 1135, given in Theorem 6.8.1 of [3]. We are indebted to Gordon Royle for the table of ranks, Table 1.

There have been some interesting developments in the study of the codes of desarguesian planes and we now turn to these. In a paper primarily devoted to nets, Moorhouse [47] established a basis for the affine desarguesian plane of prime order p, and hence also for the projective desarguesian planes of prime order. Dougherty [26] extended Moorhouse's results concerning nets. Notice that in the prime case the hull of the plane is equal to the orthogonal code for both the projective and affine cases.

THEOREM 6 *Let π denote the desarguesian affine plane $AG_2(\mathbf{F}_p)$ of prime order p. A basis for the code $C_p(\pi)$ can be found by taking the incidence vectors of the*

Table 1. The translation planes of order 49

7-rank	Number		7-rank	Number
785	1		919	1
855	1		921	7
897	1		925	4
899	2		927	4
901	1		929	5
905	1		931	12
907	5		933	4
911	2		935	18
913	1		937	25
915	5		939	179
917	4		941	1064

following lines: all the p lines from any one parallel class; any $p-1$ lines from any other parallel class; and so on, until a single line is chosen from one of the final two parallel classes, and no lines are chosen from the remaining class. This gives

$$p + (p-1) + (p-2) + \cdots + 1 = \frac{1}{2}p(p+1) = \binom{p+1}{2}$$

lines, whose incidence vectors form a basis for $C_p(\pi)$.

Thus we have

COROLLARY 1 *With notation as in the theorem, a basis for $C_p(\pi)^\perp$ that consists of minimum-weight vectors can be found by taking the difference of pairs of incidence vectors of lines chosen as follows: choose any one line from each of the parallel classes chosen as in the theorem; for each class take the pair consisting of the chosen line and each other line chosen for the basis. This gives*

$$(p-1) + (p-2) + \cdots + 1 + 0 = \frac{1}{2}p(p-1) = \binom{p+1}{2} - p$$

vectors that form a basis.

Since the code of the projective plane can be found by simply adding the line at infinity and its points, the following is immediate:

COROLLARY 2 *Let Π denote the desarguesian projective plane $PG_2(\mathbf{F}_p)$ of prime order p. A basis for the code $C_p(\Pi)$ can be found by taking the incidence vectors of the following lines: choose any one line L; then take all the other p lines through any one point; any $p-1$ lines from a second point on L; and so on, until a single line is chosen from one of the final two points, and no lines are chosen through the last point. This gives*

$$1 + p + (p-1) + (p-2) + \cdots + 1 = \frac{1}{2}p(p+1) + 1 = \binom{p+1}{2} + 1$$

lines, whose incidence vectors form a basis for $C_p(\Pi)$.

Further, a basis for $C_p(\Pi)^\perp$ *that consists of minimum-weight vectors can be found by taking all the differences of the incidence vectors of each line chosen as above, starting from the second line, with the first,* L. *This gives*

$$p + (p-1) + (p-2) + \cdots + 1 = \frac{1}{2}p(p+1) = \binom{p+1}{2}$$

vectors that form a basis.

Recently Blokhuis and Moorhouse [7] found a basis of minimum-weight vectors for $PG_2(\mathbf{F}_p)$ (and hence for the affine case as well), involving any conic in the plane.

THEOREM 7 *Let* Π *denote the desarguesian projective plane* $PG_2(\mathbf{F}_p)$ *of prime order* p, *and let* $\mathcal{C}$ *denote a conic in* Π. *Then a basis for the code* $C_p(\Pi)$ *can be found by taking the incidence vectors of all nonsecants to* $\mathcal{C}$, *i.e. all tangents and exterior lines.*

A basis for $C_p(\Pi)^\perp$ *can be found by taking the complements of the incidence vectors of the secants.*

The basis for $C^\perp$ given in the theorem is not in terms of minimum-weight vectors, but that can be found again quite simply by taking all the differences $v^L - v^{L_0}$, where L_0 is some chosen tangent or exterior line. Similarly it is easy to get a basis in the affine case using a conic.

This paper has more to say about generators in the general case:

THEOREM 8 *Let* Π *denote the desarguesian projective plane* $PG_2(\mathbf{F}_q)$ *of order* q, *a power of a prime* p. *If* $\mathcal{C}$ *is a conic in* Π, *then* $C_p(\Pi)$ *is spanned by the nonsecants (i.e. tangents and exterior lines) of* $\mathcal{C}$, *and* $H_p(\Pi)$ *is spanned by the complements of the secants, and also by the complements of the nonsecants.*

In the case of p odd, all arcs of $q+1$ points are conics, by a theorem of Segre [60]; however, in the case $p = 2$, there are non-regular ovals whenever $q \geq 16$. Computations with Cayley [9] by Carpenter [16] using non-regular ovals in cases up to $q = 64$ lead us to believe that Theorem 8 is true for any $(q+1)$-arc for $q = 2^m$, all m. Note in this case Pott [58] has shown that the incidence vectors of ovals span the orthogonal code, so that a basis of minimum-weight vectors could be found in this case also:

THEOREM 9 *Let* Π *be a finite projective plane of even order with an abelian group* G *acting regularly. If* Π *has ovals then the incidence vectors of the orbit of a oval under* G *span the orthogonal code* $C_2(\Pi)^\perp$.

The result of Pott answers the query posed in [3], Section 6.6, page 219. In fact, the only planes known with regular abelian groups *are* the desarguesian planes.

4. Oval designs

There is a well-known class of Steiner systems (i.e. designs with $\lambda = 1$) which, following Wertheimer [70], we will call *oval designs*. Bose and Shrikhande first described these designs in [8]. Recall that by an oval in a projective plane of even order n we mean a set of $n + 2$ points that meets each line of the plane in 0 or 2 points.

Definition. Let Π be a projective plane of order $n = 2k$ and let $\mathcal{O}$ be an oval of Π. The **oval design** $W(\Pi, \mathcal{O})$ is the incidence structure with points the lines of Π exterior to $\mathcal{O}$ and blocks the points of Π not on the oval $\mathcal{O}$; incidence is given by the incidence in Π.

That this is a Steiner system is easy to show:

PROPOSITION 1 *The incidence structure $W(\Pi, \mathcal{O})$ is a 2-$(2k^2 - k, k, 1)$ design of order $n = 2k$.*

In [3], Chapter 8 the following result concerning the 2-rank of an oval design is proved:

THEOREM 10 *Let Π be a projective plane of even order n and let $\mathcal{O}$ be an oval of Π. Let $W(\Pi, \mathcal{O})$ be the associated oval design. Then*

$$\text{rank}_2(W(\Pi, \mathcal{O})) \leq \text{rank}_2(\Pi) - (n + 1).$$

If $\Pi = PG_2(2^m)$, we have that $\text{rank}_2(W(\Pi, \mathcal{O})) \leq 3^m - 2^m$.

In the desarguesian case $\text{rank}_2(\Pi) = 3^m + 1$ which yields the last inequality above.

If Π is desarguesian with $n = 2^m$, then regular ovals (consisting of the $n + 1$ points of a conic plus its nucleus) always exist, and the adopted notation for the oval design from a regular oval is then $W(2^m)$, following [13], due to the association with Witt: see [13], Section 2.6 for an outline of the history of these designs.

In answer to a conjecture in Mackenzie [41] (see also [3], Section 8.4, page 304) Carpenter [16] has shown the following, using the result of Blokhuis and Moorhouse:

THEOREM 11 *If Π is desarguesian with $n = 2^m$, and $\mathcal{O}$ is any regular oval then*

$$\text{rank}_2(W(\Pi, \mathcal{O})) = \text{rank}(W(2^m)) = 3^m - 2^m.$$

Conjecture 2 *If Π is desarguesian with $n = 2^m$, and $\mathcal{O}$ is any oval then*

$$\text{rank}_2(W(\Pi, \mathcal{O})) = 3^m - 2^m.$$

Carpenter [16] has verified this conjecture for all the ovals in the desarguesian planes of orders less than 64 — and for some ovals in the desarguesian plane of order 64. There still does not seem to be a coding-theoretic way of distinguishing a regular oval from a sporadic oval — as there is in the case of unitals, where the hermitian unitals do distinguish themselves by being contained in the code of the containing plane: see [3], Theorem 6.7.1, page 226 — and this lends at least some meager support to the conjecture.

5. Hadamard designs

The following question was posed in [3], Section 7.11, page 284 and until very recently no counter-example had been found:

Question 2 *Does the binary code of a* 3-$(2^m, 2^{m-1}, 2^{m-2}-1)$ *design always contain a copy of the first-order Reed-Muller code,* $\mathcal{R}(1,m)$*?*

Many classes of Hadamard designs yield codes that do contain copies of the first-order Reed-Muller code and recently Carpenter [16], [17] has found this to be true for a class of designs related to regular ovals. We will discuss these classes first and then exhibit the example yielding a negative answer in the general case.

Any oval $\mathcal{O}$ in a projective plane of even order n can be used to define a Hadamard 2-design $\mathcal{E}$ in the following way: for the points of $\mathcal{E}$ take the n^2-1 exterior points to $\mathcal{O}$; for each point x of $\mathcal{E}$ define a block B_x to be the set of points

$$B_x = \{y \,|\, y \text{ is an exterior point and } xy \text{ is a secant to } \mathcal{O}\} \cup \{x\}.$$

This construction gives a 2-$(n^2-1, \frac{1}{2}n^2-1, \frac{1}{4}n^2-1)$ Hadamard design that extends uniquely to a 3-$(n^2, \frac{1}{2}n^2, \frac{1}{4}n^2-1)$ design. (A more general way to construct the Hadamard designs is described in [3], Section 7.12; alternatively this design can be described using the block graph of the Steiner 2-design. See also Maschietti [42] for further descriptions.)

L. L. Carpenter [16], [17] has now confirmed that the designs obtained from regular ovals in the desarguesian planes of even order contain copies of the first-order Reed-Muller code:

THEOREM 12 *Let* Π *be the desarguesian projective plane of order* 2^m*, where* $m \geq 1$*, and let* $\mathcal{O}$ *be a regular oval. If* $\mathcal{T}$ *is the Hadamard design constructed as described above from* $W(\Pi, \mathcal{O}) = W(2^m)$*, then* $C_2(\mathcal{T})$ *contains a copy of the first order Reed-Muller code* $\mathcal{R}(1, 2m)$*. Futhermore, sets of* $4(2^m-1)$ *blocks of* $\mathcal{T}$ *can be found that generate* $\mathcal{R}(1,2m)$ *and are thus common to* $\mathcal{T}$ *and a copy of the affine-geometry design of points and hyperplanes in* $AG_{2m}(\mathbf{F}_2)$*.*

For the first non-trivial case, i.e. $m = 2$, $C_2(\mathcal{T})$ *is* $\mathcal{R}(1,4)$, but this never occurs again for regular ovals: see [42].

A further conjecture, raised in Mackenzie [41] and quoted in [3], Section 7.12, page 292, concerns the rank of these designs:

Conjecture 3 *If* $\mathcal{T}$ *is the Hadamard design constructed by the method described above from* $W(2^m)$ *then* $\operatorname{rank}_2(\mathcal{T}) = 2^{m-1}m + 1$*.*

Tom Norwood [49] recently used a classification by Jackson [34] of Hadamard designs with $SL_2(\mathbf{F}_q)$ acting transitively to prove this conjecture.

Returning now to Question 2, the following construction has recently been shown, through computational results of Gordon Royle, to yield a counter-example: let $\mathcal{D}$ be the hermitian unital on 28 points, a 2-$(28, 4, 1)$ design. The block graph

of this design yields a Hadamard 2-design $\mathcal{E}$ with parameters 2-$(63, 32, 16)$. The complementary design $\overline{\mathcal{E}}$ extends to a Hadamard 3-(64,32,15) design, $\mathcal{T}$ with 2-rank 15. We claim that $C_2(\mathcal{T}) \not\supset \mathcal{R}(1, 6)$. The binary code $C_2(\mathcal{E})$ is an even-weight code of dimension 14, and was found to have 7497 vectors of weight 32. The search for the even-weight subcode of the punctured code in $C_2(\mathcal{E})$ was done by first collecting the 7497 vectors of weight 32 and observing that under the action of the automorphism group $P\Gamma U_3(\mathbf{F}_9)$ they fall into two orbits of length 3024, and one each of length 1008, 378 and 63 (the blocks). Searching then for six vectors that generate the even-weight subcode of $\mathcal{R}(1, 6)^*$ was computationally possible, and the search failed.

The weaker question

Question 3 *Is the binary code of a* 3-$(2^m, 2^{m-1}, 2^{m-2} - 1)$ *design always inside a copy of* $\mathcal{R}(m - 2, m)$*?*

has not been negated and may still have a positive answer.

A further question that was posed in [3], Question 7.10.1, page 282 is also still unanswered:

Question 4 *Does the binary code of a*

$$(2^{2m}, 2^{2m-1} - 2^{m-1}, 2^{2m-2} - 2^{m-1})$$

design contain the all-one vector?

We mention that all the designs of these parameters that can be constructed from any oval design in a plane of even order in the manner described in [3], Section 7.12 do contain the all-one vector.

Designs with parameters $(2^{2m}, 2^{2m-1} - 2^{m-1}, 2^{2m-2} - 2^{m-1})$ are intimately connected with bent functions (see [3], Section 7.9) and a theorem of Dillon and Schatz, [3], Theorem 7.10.4, which characterizes those designs with 2-rank $2m + 2$ *and* binary code containing the all-one vector. Recently Deirdre Smeltzer [63] has shown that if a difference set D in an elementary abelian 2-group is given by a bent function on the $2m$ variables $x_1, \ldots, x_m, y_1, \ldots, y_m$ of the form

$$\sum_{i=1}^{m} x_i y_i + h(x_1, \ldots, x_m),$$

where h is any cubic, and if C is the code over $\mathbf{F}_2$ of the development, $\mathcal{D}$, of D (see [3], Theorem 7.10.3) then $E_2(\mathcal{D})$ is *isomorphic* to the first-order Reed-Muller code $R = \mathcal{R}(1, 2m)$. It follows, of course, that the dimension of C is $2m + 2$ and that the all-one vector is in the code. Therefore the Dillon-Schatz Theorem applies, as pointed out by Dillon [24]. Thus $\mathcal{D}$ has the symmetric difference property. Dillon also showed that $\mathcal{D}$ is, in fact, isomorphic to the development of the difference set given by the quadratic bent function $q = \sum_{i=1}^{m} z_i w_i$ — which is the same as the design given by the minimum-weight vectors of $R \cup (q + R)$.

Another result concerning codes of Hadamard designs is due to T. S. Michael who shows in [46] that the incidence matrix of a $(4n-1, 2n-1, n-1)$ design from any skew Hadamard matrix has maximal p-rank, namely $2n$, when p divides n. The proof involves only elementary linear algebra. The result shows, in particular, that a Hadamard matrix cannot have a skew form unless its p-rank is $2n$ for all odd primes p dividing n (see [3], Theorems 7.4.1 and 7.4.2).

6. Unitals

A unital, or unitary design, is a Steiner 2-design with parameters 2-$(m^3+1, m+1, 1)$. Apart from one with $m = 6$ constructed by Mathon [43] and independently by Bagchi and Bagchi [6], all other known unitals have m a prime power. There are two known that have a regular cycle acting on points, one of which is the design with $m = 6$; the other has $m = 4$ and is one of the cyclic designs in [6]. Shobe [61] has examined the codes associated with these cyclic designs. The order of a unitary design is $m^2 - 1$, so the prime p over which the code is defined must have p dividing $m - 1$ or $m + 1$. In fact we know of no example where p dividing $m - 1$ and not $m + 1$ (and thus $p \neq 2$) gives a code that is not the full space. For the two classes of 2-transitive unitals this is known to be the case: see Mortimer [48]; hence in these "classical cases" one takes p dividing $m + 1$. For the cyclic unitals found in [6], the 2-$(217, 7, 1)$ design has 7-rank 214; the 2-$(65, 5, 1)$ design has 5-rank 63.

In [3] it was mentioned that more concerning the p-ary codes of the hermitian unitals on $q^3 + 1$ points, where p divides $q + 1$, was expected to be announced. A complete general theory has not been established, but Geck [29] has published some results on the Brauer characters of the unitary group, and Hiss [32] has communicated some partial results to us. Using Magma [15] we have computed the p-ranks of the hermitian unitals for all q such that $q \leq 13$, and we have found that all these codes, for p dividing $q + 1$, have dimension $b/q = (q^2 - q + 1)q$, where b is the number of blocks of the unital. This is the formula suggested originally by Andriamanalimanana [1] based on computations up to and including $q = 5$. The further computations up to $q = 13$ now lead us to formally state this as a conjecture, which is also born out by the results mentioned in [29] and [32]:

Conjecture 4 *Let $\mathcal{H}$ be the hermitian unital on $q^3 + 1$ points. If p is any prime dividing $q + 1$, then the p-rank of $\mathcal{H}$ is $(q^2 - q + 1)q$.*

Magma also leads us to the following conjecture:

Conjecture 5 *Let $\mathcal{H}$ be the hermitian unital on $q^3 + 1$ points, where q is odd. Let $C = C_2(\mathcal{H})$. Then*

$$\mathrm{Hull}_2(\mathcal{H}) = \begin{cases} C^\perp & \text{if } q \equiv 3 \pmod 4 \\ < \boldsymbol{\jmath} > & \text{if } q \equiv 1 \pmod 4 \end{cases}$$

where $\boldsymbol{\jmath}$ is the all-one vector.

Magma has verified this for $q \leq 13$. Similarly, this conjecture does not contradict indications coming from the study of the modular characters of unitary groups, as indicated in [32].

We note here also another property — possibly related to the observations above — that a search with Magma has brought out. Whenever q is odd there is the so-called Hölz design with parameters 2-$(q^3+1, q+1, q+2)$ whose blocks consist of all the blocks of the unital together with the intersections of all Baer subplanes of the ambient plane of order q^2 that meet the unital in $q+1$ points; the computations concern the binary codes of these associated Hölz designs (discovered by Hölz [33] and discussed in [3], Section 8.3). Looking at the binary codes of the Hölz designs with Magma we found, for odd q between 3 and 13, that the code is the same as that of the unital when $q \equiv 3 \pmod 4$, and larger (probably $\langle j \rangle^{\perp}$) when $q \equiv 1 \pmod 4$.

The unitals with $m = 3$, namely the 2-$(28, 4, 1)$ designs, have received a great deal of attention, partly because of the existence of two such designs having a doubly-transitive automorphism group when m is any odd power of 3 (see [3], pps. 301-302 and [2]), but also because they are small enough to examine in full. Brouwer [11] had already produced many such designs and had investigated when they could be embedded in projective planes of order nine. Gordon Royle [54] has since determined that precisely 17 of these unitals can be so embedded, one of these in two distinct planes. (There are precisely four projective planes of order nine.) As far as we know there has been no progress in characterizing the Ree unital on 28 points as the one of smallest 2-rank; its 2-rank is 19.

7. Steiner triple systems

A Steiner triple system is a 2-$(v, 3, 1)$ design. Doyen, Hubaut and Vandensavel [27] proved the following result giving a lower bound for the p-rank of any Steiner triple system, and showing that only $p = 2$ or $p = 3$ need be considered, when looking at the code.

THEOREM 13 *Let $\mathcal{D}$ be a 2-$(v, 3, 1)$ design and let p be a prime. Then*

(1) $\operatorname{rank}_p(\mathcal{D}) = v$ *if* $p \geq 5$*;*

(2)
$$\operatorname{rank}_2(\mathcal{D}) = v - d_P - 1 \geq v - \log_2(v+1),$$
with equality if and only if $\mathcal{D}$ is the design of points and lines of the projective geometry $PG_d(\mathbf{F}_2)$, where $v = 2^{d+1} - 1$;

(3)
$$\operatorname{rank}_3(\mathcal{D}) = v - d_A - 1 \geq v - \log_3(v) - 1,$$
with equality if and only if $\mathcal{D}$ is the design of points and lines of the affine geometry $AG_d(\mathbf{F}_3)$, where $v = 3^d$.

(Here d_P and d_A are the projective and affine dimensions, respectively, of $\mathcal{D}$: see Teirlinck [65].)

This theorem is in itself in the nature of a rigidity theorem, in that it characterizes the designs associated with finite geometries through the p-ranks of their incidence matrices. Since perfect linear single-error-correcting codes over any field are unique up to a monomial transformation, the binary code of the design of points and lines of a projective space over $\mathbf{F}_2$ characterizes this design. But more is true as was shown by Key and Sullivan [40] for the binary case, and by Key [37] for the ternary case. Here are the relevant results.

THEOREM 14 *Let $\mathcal{D}$ be a 2-$(v, 3, 1)$ design with $v \geq 7$. Let d satisfy $2^d - 1 \leq v < 2^{d+1} - 1$. Then $C_2(\mathcal{D})$ contains a subcode C that can be shortened (by removing $v - (2^d - 1)$ coordinate places where all the codewords of C are zero) to a code that is isomorphic to the binary Hamming code $\mathcal{H}_d$. In particular, if $v = 2^d - 1$ then $C_2(\mathcal{D}) \supseteq \mathcal{H}_d$.*

Equivalently, $C_2(\mathcal{D})$ contains a set of weight-3 vectors whose supports form the blocks of the design of points and lines of $PG_{d-1}(\mathbf{F}_2)$.

This result extends to the quadruple systems:

THEOREM 15 *If $\mathcal{E}$ is a Steiner quadruple system, i.e. a 3-$(v, 4, 1)$ design, with $2^d \leq v < 2^{d+1}$, then the binary code $C_2(\mathcal{E})$ contains a subcode that can be shortened to the Reed-Muller code, $\mathcal{R}(d-2, d)$. In particular, if $v = 2^d \geq 8$ then*

$$C_2(\mathcal{E})^\perp \subseteq \mathcal{R}(1, d) \subseteq \mathcal{R}(d-2, d) \subseteq C_2(\mathcal{E}).$$

In the ternary case we need only consider the triple systems, since, by a theorem of Dehon [19], the ternary code of a quadruple system is the entire ambient space.

THEOREM 16 *Let $\mathcal{D}$ be a 2-$(v, 3, 1)$ design with $v \geq 9$. Suppose that d is such that $3^d \leq v < 3^{d+1}$. Then $C_3(\mathcal{D})$ contains a subcode C that can be shortened (by removing $v - 3^d$ coordinate places where all the codewords of C are zero) to a code that is isomorphic to the generalized Reed-Muller code $\mathcal{R}_{\mathbf{F}_3}(2(d-1), d)$. In particular, if $v = 3^d$ and $d \geq 2$, then we always have*

$$C_3(\mathcal{D})^\perp \subseteq \mathcal{R}_{\mathbf{F}_3}(1, d) \subseteq \mathcal{R}_{\mathbf{F}_3}(2(d-1), d) \subseteq C_3(\mathcal{D}).$$

Equivalently, $C_3(\mathcal{D})$ contains a set of weight-3 vectors whose supports form the blocks of the design of points and lines of $AG_d(\mathbf{F}_3)$.

There is some interesting work in progress concerning Steiner triple systems and *non-linear* binary perfect codes. The problems being discussed go all the way back to Steiner's original paper [64]; it was clear early on (see [4]) that any perfect binary code containing the zero vector yielded an extendable Steiner triple system and that Steiner's questions were intimately related to perfect codes. Moreover, it is still widely believed that every Steiner triple system is extendable and this has been verified for the 80 systems on 15 points [23]. By the theorem of Doyen et

al. the Steiner triple systems of smallest possible rank, being classical systems, are extendable. A bit more can be said with respect to this question: using the codes of the systems and the results mentioned above, the following proposition is proved in [38], [39]:

PROPOSITION 2 *Let $\mathcal{D}$ be a Steiner triple system on $v = 2^d - 1$ (or 3^d) points and suppose that the 2-rank of $\mathcal{D}$ is $2^d - d$ (respectively, the 3-rank is $3^d - d$). Then $\mathcal{D}$ can be extended to a Steiner quadruple system. In the binary case the extension can be defined in such a way that its binary code is the extended binary code of $\mathcal{D}$.*

Thus, not only are the classical systems extendable but also those on a classical number of points with rank just above the classical rank.

A related question concerning binary perfect codes asks whether every Steiner triple system on $2^m - 1$ points can be seen as the set of weight-3 vectors of a perfect[3] binary code containing the zero vector [56]. Progress in showing this for the 80 systems on 15 points is being made. The number of inequivalent Steiner triple systems is known rather precisely in an asymptotic sense [71] and Phelps [57] has produced an asmpytotic lower bound on the number of inequivalent binary perfect codes (see also Etzion and Vardy [28]). There are more than enough perfect codes to justify the question. Of course, a given triple system may appear as the set of weight-3 vectors in many inequivalent perfect binary codes and a given perfect binary code may yield many (at most 2^{n-m} where $n = 2^m - 1$) inequivalent Steiner triple systems. Indeed, the number of perfect binary codes grows so quickly with increasing block length that it appears certain that any triple system that does appear is likely to complete to a perfect code in an enormous number of ways. One can see the phenomenon even for small lengths and mere extensions of triple systems; for example, there are two triple systems on 13 points but four quadruple systems on 14 points and each of the triple systems extends in more than one way to a quadruple system (see [45]). For the systems on 15 points this phenomenon is even more striking (see [57]).

8. Finite geometries and rigidity theorems

Hamada's conjecture from [31] still stands in a weakened form, *viz.*:

Conjecture 6 *If a design has the same parameters as a design of points and fixed-dimensional subspaces or flats of a projective or affine space over a field of characteristic p, then the p-rank of the design will be at least that of the corresponding geometric design.*

This conjectures that the designs coming from the geometry have the smallest p-rank, and this has not been shown to be false, although the examples of Tonchev [66] and of Delsarte and Goethals [30] show that it is possible for designs with the parameters of a geometric design to have the *same* p-rank as the geometric design.

The conjecture is most interesting in the hyperplane case and here it is still open in its stronger form:

Conjecture 7 *A symmetric design with parameters*

$$\left(\frac{q^{n+1}-1}{q-1}, \frac{q^n-1}{q-1}, \frac{q^{n-1}-1}{q-1}\right)$$

where $q = p^s$, p a prime, has p-rank at least

$$\binom{n+p-1}{n}^s + 1$$

with equality if and only if it is the design of points and hyperplanes of $PG_n(\mathbf{F}_q)$.

The conjecture has only been proven for $q = 2$ (see Theorem 17 below).

The symmetric design of points and hyperplanes of a projective geometry has a doubly-transitive automorphism group acting. All (v, k, λ) designs with a doubly-transitive group acting and $2k < v$ are known [36]; besides the projective designs there is another infinite class with parameters $(2^{2m}, 2^{2m-1} - 2^{m-1}, 2^{2m-2} - 2^{m-1})$ and two sporadic examples: the unique $(11, 5, 2)$ design and the so-called Higman design with parameters $(176, 50, 14)$. The designs of the second infinite class occur among the designs with the symmetric difference property; these designs have been characterized by Dillon and Schatz [25] and they have the minimum 2-rank, namely $2m+2$. In this case there is not, to our knowledge, a rigidity theorem characterizing the "best" design[4] among those with the symmetric difference property and, in fact, the binary code of a design with the symmetric difference property is a complete invariant for those designs. The Higman design probably is characterized by its 2-rank, namely 22, but proving that appears to be rather difficult. Zvonimir Janko [35] has uncovered another $(176, 50, 14)$ design that is closely related to the Higman design and it has higher 2-rank. For a short discussion of all these matters the reader may wish to consult the paper by Parker and Tonchev, [50][5]

For geometric designs it is well known that the codes, to be of interest, need to be over a prime field whose characteristic is that of the field of the geometry: see [3]. The codes of these designs are the Reed-Muller codes, $\mathcal{R}(r, m)$, in case $F = \mathbf{F}_2$, or various generalized Reed-Muller codes, as was proved mostly by the work of Delsarte et al. [20], [21], [22], [30]. These results are described in [3], Chapter 5 and in [5].

Rigidity theorems have been established: for Steiner triple systems (see Section 7) and for some classes of Hadamard designs (see Section 5). The negative answer to Question 2 described in Section 5 shows that a rigidity theorem similar to the results for Steiner triple systems (Theorems 14, 15 and 16) will not be found for Hadamard 3-$(2^m, 2^{m-1}, 2^{m-2} - 1)$ designs, although we do have the Hamada-Ohmori rigidity theorem (Corollary 7.5.1 in [3]):

THEOREM 17 *The binary code of a 3-$(2^m, 2^{m-1}, 2^{m-2} - 1)$ design has dimension at least $m + 1$ and has at least $2^{m+1} - 2$ vectors of weight 2^{m-1}. If either equality holds so does the other and this occurs if and only if the design is the design of points and hyperplanes in the affine geometry of dimension m over $\mathbf{F}_2$.*

9. Dual structures and the "point" code of a design

Bridges, Hall and Hayden in [10] gave some attention to the linear code generated by the transpose of an incidence matrix of a design, but they, like most others, thought that only those codes over fields whose characteristic divided the order of the design were of interest. It was Tonchev [68] who pointed out that these codes were of interest even when the prime did *not* divide the order of the design and, in an interesting paper, Tonchev and Weishaar [69] examined precisely these codes for all 80 Steiner triple systems on 15 points and found that the 80 binary codes of block length 35 were all different — in contrast to the usual codes of block length 15, where there are only five different codes, one for each dimension k with $11 \leq k \leq 15$. For lack of a better name we call such a code the **point code** of the design; it is merely the code of the dual incidence structure — which is only a design in the symmetric case. The point code of the design of points and lines of $PG_3(\mathbf{F}_2)$ distinguishes itself from the other 79 codes not only by its dimension but also by the fact that it is the only one of these codes that has no vectors of weight 8 or 11 (and thus none of weight 24 or 27, since $\boldsymbol{\jmath}$ is in the code); it has minimum weight 7, but there are other codes with this minimum weight. Moreover, the code is *not* contained in each of the other 79 (although it is contained in some of the 79), again in contrast to the usual codes: see Theorem 14. There are, in fact, numerous containment relations among the 80 codes, all of which were described in [69]. This was made possible computationally by the following well-known result [67], Exercise 1.1.17, page 7 — which is not normally stated in coding-theoretic terms, as below:

PROPOSITION 3 *Let $0 < \lambda < r$ and suppose given v vectors in $\mathbf{F}_2^n$, each of weight r and any two at distance $2(r-\lambda)$. Then,*

$$n \geq \frac{r^2 v}{r + \lambda(v-1)}$$

with equality if and only if the v vectors form the columns of an incidence matrix of a 2-(v,k,λ) design, where $k = \frac{r+\lambda(v-1)}{r}$.

Although the proposition is well-known its importance does not seem to have been recognized. It does, for example, show that a 2-design is the solution to an extremal problem in coding theory, a fact that went unobserved in [3].

Kevin Phelps [56] has conjectured that the binary point code of a Steiner triple system is a complete invariant; i.e. that two such point codes are isomorphic if and only if the triple systems are. Even for the 80 triple systems on 15 points the matter is rather delicate since some of the codes have the same weight distributions. In the only other case so far considered, the two triple systems on 13 points, the two binary point codes have different weight distributions; in each case they are $[26, 13]$ codes since the order of the designs is 5. Because the order of these designs is 5, rank considerations alone show that the two designs have the same codes, in the usual sense, for *every* prime p.

Of course, in general, the binary point codes of a class of designs with the same parameters cannot characterize the designs since there are symmetric designs for which this is patently false (for example, the four projective planes of order nine) and non-symmetric examples are also available. Curiously, however, the 17 embeddable unitals on 28 points [54] are so characterized [59]; we do not know what the "correct", most general conjecture might be — if, in fact, Phelps's conjecture for the triple systems is true — and the subject probably deserves further investigation. It is even theoretically possible to have a point code of one design contain the point code of another design with different parameters, but we lack an example of this. As far as we know there has been nothing substantial done with point codes except over the binary field (but see [50]).

10. Strongly regular graphs and their *p*-ranks

Although codes associated with graphs have not been extensively studied, some significant results concerning the p-rank of adjacency matrices of strongly regular graphs have recently been established: see Brouwer and van Eijl [12] and Peeters [52]. Since these concepts are closely related to certain constructions we have examined for designs, we will describe here some of the new results.[6]

Recall that a strongly regular graph Γ with parameters (v, k, λ, μ) is a regular undirected graph on v vertices with valency k, such that λ is the number of vertices adjacent to both of two adjacent vertices and μ the number of vertices adjacent to both of two non-adjacent vertices. An adjacency matrix[7] for Γ is also an incidence matrix for a quasi-symmetric 1-design (see Shrikhande and Sane [62]) on the v points with block size k. This quasi-symmetric design is a symmetric (v, k, λ) design if and only if $\lambda = \mu$.

Let Γ be a strongly regular graph with parameters (v, k, λ, μ), and let A be an adjacency matrix for Γ. It is well known (see, for example, Cameron and van Lint [14], Chapter 2) that A has three eigenvalues, namely k and two others, ρ and σ, with

$$\rho, \sigma = \frac{1}{2}(\lambda - \mu \pm \sqrt{(\lambda - \mu)^2 + 4(k - \mu)}.$$

Calling, as usual, the multiplicities f and g we have that

$$\begin{aligned} v &= f + g + 1, \\ 0 &= k + f\rho + g\sigma, \end{aligned}$$

and that $\lambda - \mu = \rho + \sigma$ and $\mu - k = \rho\sigma$. From this it follows that

$$f, g = \frac{1}{2}(v - 1 \pm \frac{(v-1)(\mu - \lambda) - 2k}{\sqrt{(\mu - \lambda)^2 + 4(k - \mu)}}),$$

respectively. We refer to the case $f = g$ as the **half** case. In the half case the parameters are $(4t + 1, 2t, t - 1, t)$, for some $t \geq 1$. The following is a consequence of results proved in [12]:

THEOREM 18 *If p is a prime and c is any integer, then the p-rank of the matrix $A+cI_v$, where A is an adjacency matrix of a strongly regular graph Γ with parameters (v,k,λ,μ), is completely determined by these parameters except possibly for the p-ranks of*

- *$A+\frac{1}{2}(p+1)I_v$ with p dividing v in the half case, and*
- *$A-\sigma I_v$ with p dividing $(\rho-\sigma)$ where ρ and σ are the eigenvalues of A other than k and are assumed to be integral,*

in which case the p-rank is upper bounded by $\min\{f+1,g+1\}$ where f and g are the multiplicities of ρ and σ.

Notice that if we have a strongly regular graph from a Steiner 2-$(v,k,1)$ design $\mathcal{D}$, then $\rho=r-1-k$, $\sigma=-k$, $f=v-1$ and $g=b-v$. Furthermore, if M is an incidence matrix for $\mathcal{D}$ and A the adjacency matrix for the block graph Γ of $\mathcal{D}$ using the same ordering of blocks, then

$$MM^t = A + kI_b,$$

and

$$\text{rank}_F(M) = \text{rank}_F(\mathcal{D}) = \text{rank}_F(A+kI_b) + \dim(\text{Hull}_F(\mathcal{D})) \tag{1}$$

over any field F.

In [52], Peeters's aim is to characterize strongly regular graphs by their parameters *and* the p-rank for one of the values of p that fall into the exclusions of the theorem (called the "relevant" p-ranks of Γ). In particular, for the half case he shows

THEOREM 19 *Let Γ be a strongly regular graph with parameters $(4t+1,2t,t-1,t)$ and adjacency matrix A. If p divides v but p^2 does not, then $A+\frac{1}{2}(p+1)I_v$ has p-rank $2t+1$.*

The block graphs of Steiner triple systems are examined by Peeters in [51]; the theorem of Doyen et al. (Theorem 13) gives the p-ranks of the Steiner 2-$(v,3,1)$ designs, and the above equality gives the rank of $A+3I_b$ where A is an adjacency matrix for the block graph. Hence when $p\geq 5$ the p-rank of $A+3I_b$ is v; if $p=2$ then from [40], Proposition 2 we know that $\text{Hull}_2(\mathcal{D})=C^\perp$ if 2 divides the order $n=(v-3)/2$ (and clearly also if not), so that equation (1) above gives the 2-rank of $A+3I_b$ as $2\times\text{rank}_2(\mathcal{D})-v$. For $p=3$, if 3 does not divide the order n then also 3 does not divide v, and so $\text{rank}_3(\mathcal{D})=v-1$ and $\text{Hull}_3(\mathcal{D})=\{0\}$, so that $A+3I_b$ has 3-rank $v-1$. If 3 divides n then the same result from [40] shows that $\text{Hull}_3(\mathcal{D})=C^\perp$, and the 3-rank of $A+3I_b$ as $2\times\text{rank}_3(\mathcal{D})-v$, except in the case where 9 does not divide v and $\mathcal{D}$ has exactly three affine hyperplanes (i.e. $d_A=1$), in which case it follows that $\text{Hull}_3(\mathcal{D})=\langle\jmath\rangle$ and that the 3-rank of $A+3I_b$ is $v-3$. (Note that there is an error in [40], Proposition 2 in the statement for $p=3$ in that it is not true that $C_3(\mathcal{D})^\perp\subseteq C_3(\mathcal{D})$ in the case where 9 does not divide v and $\mathcal{D}$ has exactly three affine hyperplanes.)

For example, the Steiner triple systems on 15 points give block graphs on 35 points and matrices $A + I_{35}$ with 2-rank in the set $\{7, 9, 11, 13, 15\}$. By way of an exercise, we used Magma to obtain the weight distribution of the code of dimension 7 spanned over $\mathbf{F}_2$ by the matrix $A + I_{35}$ for the 2-(15,3,1) design of points and lines of $PG_3(\mathbf{F}_2)$:

$$< 0, 1 >, < 15, 28 >, < 16, 35 >, < 19, 35 >, < 20, 28 >, < 35, 1 >$$

and its hull:

$$< 0, 1 >, < 16, 35 >, < 20, 28 >$$

which is the even-weight subcode in this case. The notation here is that used in Magma: the pair $< i, A_i >$ denotes A_i vectors of weight i. Similar computations could be made for the other 79 designs: we do not know if they give distinct codes or not, as in the case of the dual structures mentioned in Section 9.

We mention again that not a great deal seems to be known about the codes spanned by these matrices. Codes associated with quasi-symmetric designs have been examined by various authors: see Shrikhande and Sane [62], Chapter X for some of the available results. Even in the case of an adjacency matrix giving a symmetric design the code of the design is not well documented. Note, for example, that it was the hermitian unital on 28 points (with $k = 4$) that gave a block graph yielding a code that provided a negative answer to Question 2.

Acknowledgments

Both authors would like to thank René Peeters and John Dillon for a careful reading of an earlier draft of this article and saving us from blunders. We would also like to respectively thank INRIA and the University of Nebraska - Lincoln for their hospitality during the preparation of parts of the manuscript.

Notes

1. Ovals are also called *hyperovals* in the literature
2. A *constant* vector is a non-zero vector in which all entries are either 0 or a where a is some non-zero field element.
3. The perfect code will always be non-linear unless the system is the classical one of points and lines of $PG_{m-1}(\mathbf{F}_2)$
4. Namely the one with the doubly-transitive automorphism group.
5. In fact, the subject of this work is the construction of the Higman design via coding theory, utilizing the binary point codes of the derived or residual designs, but a discussion of all symmetric designs possessing a doubly-transitive automorphism group is included.
6. See also the last paragraph of this section for a further reference.

7. An *adjacency matrix* of a graph is a square zero-one matrix whose rows and columns are both indexed by vertices with a 1 in a given position if the respective vertices are adjacent; it is symmetric if the rows and columns are indexed in the same order and, in this case, has 0s on the diagonal. If the graph is strongly regular any row has k ones and any two distinct rows have either λ or μ ones in common.

References

1. Bruno Ratsimandefitra Andriamanalimanana. *Ovals, Unitals and Codes*. PhD thesis, Lehigh University, 1979.
2. E. F. Assmus, Jr. and J. D. Key. Arcs and ovals in the hermitian and Ree unitals. *European J. Combin.*, 10:297–308, 1989.
3. E. F. Assmus, Jr. and J. D. Key. *Designs and their Codes*. Cambridge University Press, 1992. Cambridge Tracts in Mathematics, Vol. 103 (Second printing with corrections, 1993).
4. E. F. Assmus, Jr. and H. F. Mattson, Jr. On tactical configurations and error-correcting codes. *J. Combin. Theory*, 2:243–257, 1967.
5. Edward F. Assmus, Jr. and Jennifer D. Key. Codes and finite geometries. Technical report, INRIA, 1993. Report No. 2027.
6. Sunanda Bagchi and Bhaskar Bagchi. Designs from pairs of finite fields: I. A cyclic unital $U(6)$ and other regular Steiner 2-designs. *J. Combin. Theory, Ser. A*, 52:51–61, 1989.
7. Aart Blokhuis and G. Eric Moorhouse. Some p-ranks related to orthogonal spaces. *J. Algebraic Combin.* To appear.
8. R. C. Bose and S. S. Shrikhande. On the construction of sets of mutually orthogonal latin squares and the falsity of a conjecture of Euler. *Trans. Amer. Math. Soc.*, 95:191–209, 1960.
9. W. Bosma and J. Cannon. *Handbook of Cayley Functions*. Department of Mathematics, University of Sydney, January 1993.
10. W. G. Bridges, M. Hall, Jr., and J. L. Hayden. Codes and designs. *J. Combin. Theory, Ser. A*, 31:155–174, 1981.
11. A. E. Brouwer. Some unitals on 28 points and their embeddings in projective planes of order 9. In M. Aigner and D. Jungnickel, editors, *Geometries and Groups*, pages 183–188. Springer-Verlag, 1981. Lecture Notes in Mathematics, No. 893.
12. A. E. Brouwer and C. J. van Eijl. On the p-rank of the adjacency matrices of strongly regular graphs. *J. Algebraic Combin.*, 1:329–346, 1992.
13. F. Buekenhout, A. Delandtsheer, and J. Doyen. Finite linear spaces with flag-transitive groups. *J. Combin. Theory, Ser. A*, 49:268–293, 1988.
14. P. J. Cameron and J. H. van Lint. *Designs, Graphs, Codes and their Links*. Cambridge: Cambridge University Press, 1991. London Mathematical Society Student Texts 22.
15. John Cannon and Catherine Playoust. *An Introduction to Magma*. School of Mathematics and Statistics, University of Sydney, 1994.
16. L. L. Carpenter. Oval designs in desarguesian projective planes. *Des. Codes Cryptogr.*, 1995. To appear.
17. L. L. Carpenter and J. D. Key. Reed-Muller codes and Hadamard designs from ovals. *J. Combin. Math. Combin. Comput.*, 1995. To appear.
18. James A. Davis and Jonathan Jedwab. A summary of Menon difference sets. *Congressus Numerant.*, 93:203–207, 1993.
19. Michel Dehon. Ranks of incidence matrices of t-designs $S_\lambda(t, t+1, \lambda)$. *European J. Combin.*, 1:97–100, 1980.
20. P. Delsarte, J. M. Goethals, and F. J. MacWilliams. On generalized Reed-Muller codes and their relatives. *Inform. and Control*, 16:403–442, 1970.
21. Philippe Delsarte. A geometric approach to a class of cyclic codes. *J. Combin. Theory*, 6:340–358, 1969.
22. Philippe Delsarte. On cyclic codes that are invariant under the general linear group. *IEEE Trans. Inform. Theory*, 16:760–769, 1970.

23. Immo Diener, Eberhard Schmitt, and Hans Ludwig de Vries. All 80 Steiner triple systems on 15 points are extendable. *Discrete Math.*, 55:13–19, 1985.
24. J. F. Dillon. Private communication.
25. J. F. Dillon and J. R. Schatz. Block designs with the symmetric difference property. In Robert L. Ward, editor, *Proceedings of the NSA Mathematical Sciences Meetings*, pages 159–164. The United States Government, 1987.
26. Steven Dougherty. Nets and their codes. *Des. Codes Cryptogr.*, 3:315–331, 1993.
27. Jean Doyen, Xavier Hubaut, and Monique Vandensavel. Ranks of incidence matrices of Steiner triple systems. *Math. Z.*, 163:251–259, 1978.
28. Tuvi Etzion and Alexander Vardy. Perfect binary codes: constructions, properties and enumeration. *IEEE Trans. Inform. Theory*, 40:754–763, 1994.
29. Meinolf Geck. Irreducible Brauer characters of the 3-dimensional special unitary groups in non-defining characteristic. *Comm. Algebra*, 18:563–584, 1990.
30. Jean-Marie Goethals and Philippe Delsarte. On a class of majority-logic decodable cyclic codes. *IEEE Trans. Inform. Theory*, 14:182–188, 1968.
31. N. Hamada. The geometric structure and the p-rank of an affine triple system derived from a nonassociative Moufang loop with the maximum associative center. *J. Combin. Theory, Ser. A*, 30:285–297, 1981.
32. Gerhard Hiss. Private communication.
33. G. Hölz. Construction of designs which contain a unital. *Arch. Math.*, 37:179–183, 1981.
34. Wen-Ai Jackson. A characterization of Hadamard designs with $SL(2, q)$ acting transitively. *Geom. Dedicata*, 46:197–206, 1993.
35. Zvonimir Janko. On symmetric designs with parameters $(176, 50, 14)$. Preprint.
36. William M. Kantor. Classification of 2-transitive symmetric designs. *Graphs Combin.*, 1:165–166, 1985.
37. J. D. Key. Ternary codes of Steiner triple systems. *J. Combinatorial Designs*, 2:25–30, 1994.
38. J. D. Key and F. E. Sullivan. Steiner systems from binary codes. Submitted.
39. J. D. Key and F. E. Sullivan. Steiner triple systems with many affine hyperplanes. Submitted
40. J. D. Key and F. E. Sullivan. Codes of Steiner triple and quadruple systems. *Des. Codes Cryptogr.*, 3:117–125, 1993.
41. Kirsten Mackenzie. *Codes of Designs*. PhD thesis, University of Birmingham, 1989.
42. A. Maschietti. Hyperovals and Hadamard designs. *J. Geom.*, 44:107–116, 1992.
43. R. Mathon. Constructions of cyclic Steiner 2-designs. *Ann. Discrete Math.*, 34:353–362, 1987.
44. Rudolf Mathon and Gordon F. Royle. The translation planes of order 49. *Des. Codes Cryptogr.*, 5:57–72, 1995.
45. N. S. Mendelsohn and Stephen H. Y. Hung. On the Steiner systems $S(3, 4, 14)$ and $S(4, 5, 15)$. *Utilitas Math.*, 1:5–95, 1972.
46. T. S. Michael. The p-ranks of skew Hadamard designs. *J. Combin. Theory, Ser. A*. To appear.
47. G. Eric Moorhouse. Bruck nets, codes, and characters of loops. *Des. Codes Cryptogr.*, 1:7–29, 1991.
48. Brian Mortimer. The modular permutation representations of the known doubly transitive groups. *Proc. London Math. Soc. (3)*, 41:1–20, 1980.
49. T. Norwood. Private communication.
50. Christopher Parker and Vladimir D. Tonchev. Linear codes and doubly-transitive symmetric designs. Preprint.
51. René Peeters. On the p-ranks of the block graphs of Steiner triple systems. Preprint.
52. René Peeters. Uniqueness of strongly regular graphs having minimal p-rank. Tilburg University, Department of Economics Research Memorandum, FEW 626.
53. T. Penttila and I. Pinneri. Irregular hyperovals in $PG(2, 4)$. *J. Geom.*, 51:89–100, 1994.
54. Tim Penttila and Gordon F. Royle. Sets of type (m, n) in affine and projective planes of order nine. To appear: Des. Codes Cryptogr.
55. Tim Penttila, Gordon F. Royle, and M. K. Simpson. Hyperovals in the known projective planes of order 16. In preparation.

56. K. T. Phelps. Private communication.
57. K. T. Phelps. A combinatorial construction of perfect codes. *SIAM J. Alg. Disc. Meth.*, 4:398–403, 1983.
58. Alexander Pott. On abelian difference set codes. *Des. Codes Cryptogr.*, 2:263–271, 1992.
59. Gordon F. Royle. Private communication.
60. Beniamino Segre. Ovals in a finite projective plane. *Canad. J. Math.*, 7:414–416, 1955.
61. F.D. Shobe. *On a class of Steiner systems and their codes*. PhD thesis, Clemson University, 1995. Submitted.
62. Mohan S. Shrikhande and Sharad S. Sane. *Quasi-Symmetric Designs*. Cambridge University Press, 1991. London Mathematical Society Lecture Notes Series 164.
63. Deirdre Langacher Smeltzer. *Topics in difference sets in 2-groups*. PhD thesis, University of Virginia, 1994.
64. J. Steiner. Combinatorische Aufgabe. *J. Reine Angew. Math.*, 45:181–182, 1853.
65. Luc Teirlinck. On projective and affine hyperplanes. *J. Combin. Theory, Ser. A*, 28:290–306, 1980.
66. Vladimir D. Tonchev. Quasi-symmetric 2-(31,7,7) designs and a revision of Hamada's conjecture. *J. Combin. Theory, Ser. A*, 42:104–110, 1986.
67. Vladimir D. Tonchev. *Combinatorial Configurations Designs, Codes, Graphs*. Pitman Monographs and Surveys in Pure and Applied Mathematics, No. 40. New York: Longman, 1988. Translated from the Bulgarian by Robert A. Melter.
68. Vladimir D. Tonchev. Quasi-symmetric designs, codes, quadrics, and hyperplane sections. *Geom. Dedicata*, 48:295–308, 1993.
69. Vladimir D. Tonchev and Robert S. Weishaar. Steiner triple systems of order 15 and their codes. *J. Statist. Plann. Inference*. To appear.
70. Michael A. Wertheimer. Oval designs in quadrics. *Contemp. Math.*, 111:287–297, 1990. Published by the American Mathematical Society.
71. Richard M. Wilson. Nonisomorphic Steiner triple systems. *Math. Z.*, 135:303–313, 1974.
72. M. –y. Xia. Some infinite classes of special Williamson matrices and difference sets. *J. Combin. Theory, Ser. A*, 61:230–242, 1992.