Ovals in projective designs

Citation for published version (APA):
Assmus, E. F., & van Lint, J. H. (1979). Ovals in projective designs. *Journal of Combinatorial Theory, Series A*, *27*(3), 307-324. https://doi.org/10.1016/0097-3165(79)90019-0

DOI:
10.1016/0097-3165(79)90019-0

Document status and date:
Published: 01/01/1979

Document Version:
Publisher's PDF, also known as Version of Record (includes final page, issue and volume numbers)

70

Reprinted from JOURNAL OF COMBINATORIAL THEORY, Series A
All Rights Reserved by Academic Press, New York and London

Vol. 27, No. 3, November 1979
Printed in Belgium

Ovals in Projective Designs

E. F. ASSMUS, JR.,* AND J. H. VAN LINT†

**Lehigh University, Bethlehem, Pennsylvania 18015; and †Eindhoven Technical University, Eindhoven, The Netherlands and Bell Laboratories, Murray Hill, New Jersey*

Communicated by the Managing Editors

Received August 29, 1977

The notion of "oval" arose in the study of finite projective planes. We extend the notion to arbitrary projective designs — indeed to arbitrary designs. Most of the elementary facts admit of direct generalization and ovals appear to abound in nonclassical projective designs.

1. INTRODUCTION

Ovals have always been of interest in the theory of finite projective planes but the direct generalization of the notion to projective designs has never been considered as far as we know, presumably because, for the classical projective designs coming from points and hyperplanes of $PG_n(q)$, one never sees nontrivial collections of points no three on a block except when $n = 2$. We here consider the direct generalization to projective designs and hope to show that the notion is of considerable interest. One can define ovals for arbitrary designs and a few amusing—even interesting—facts emerge. In the interest of conciseness we relegate this further generalization to our remarks and examples.

After reviewing basic definitions in Section 2 we give the generalization and the main facts in Section 3. Section 4 is devoted to examples but also contains some theoretical results. Section 5 explains the relationships with algebraic coding theory. Finally, in Section 6, we give a somewhat more elegant description of the connection between odd-order biplanes and even-order planes which was first described in [2].

2. BASIC PRELIMINARIES

A *projective design* or a (v, k, λ)-design is a collection $\mathscr{B}$ of v k-subsets of a v-set $\mathscr{P}$ with the property that each two distinct members of $\mathscr{B}$ intersect in a set of cardinality λ. Elements of $\mathscr{P}$ are called *points*, elements of $\mathscr{B}$ *blocks* (or sometimes lines), and $k - \lambda$ is the *order* of the design. The *incidence*

0097-3165/79/060307-18$02.00/0

matrix of such a design is the v by v matrix of 0's and 1's whose columns are indexed by $\mathscr{P}$ and rows by $\mathscr{B}$ with the entry at (B, p) 1 precisely when $p \in B$. If M is this incidence matrix it follows that M^t (the transpose of M) is the incidence matrix of a projective design with the same parameters (v, k, λ), where the notions of points and blocks are interchanged. This design is called the *dual* of the original design; it may or may not be isomorphic to the original design. When $\lambda = 1$ a projective design is nothing but a projective plane and when $\lambda = 2$ we call the design a *biplane*, following Cameron. When there is a unique biplane of order m we denote it by $B(m)$. The *complement* of a projective design consists of the v-sets $\mathscr{P} - B$, where B runs through the blocks of the design. It is a projective design and if the original design has parameters (v, k, λ) the complement's parameters are $(v, v - k, (v - k)(v - k - 1)/(v - 1))$.

Now a projective design is a 2-design in the sense that each 2-subset of $\mathscr{P}$ is contained in precisely λ blocks. More generally a *t-design* or a $t - (v, k, \lambda)$-design is a collection $\mathscr{B}$ of k-subsets of a v-set with the property that each t-subset of $\mathscr{P}$ is contained in precisely λ of the elements of $\mathscr{B}$, again called *blocks*. For a 2-design, or $2 - (v, k, \lambda)$-design, Fisher's inequality shows that $|\mathscr{B}| \geqslant v$ (whenever $k < v$) and the case of equality is precisely the case of a projective design; i.e., projective designs and 2-designs with v blocks are equivalent notions. All the above notions and facts are quite elementary and the novice reader may wish to consult [8, 9, 13] for a fuller discussion.

In what follows, a *code* always means a linear code and is simply a subspace C of F^n, the vector space of n-tuples over a finite field, F. If C is of dimension l the code is referred to as an (n, l) code and n is called the *block length.* $C^\perp$, the *dual* of C, is defined to be $\{a \in F^n \mid \sum a_i c_i = 0 \text{ for all } c \in C\}$. The *weight* of an n-tuple, $a = (a_1, a_2, \ldots, a_n)$ of F^n, is simply the number of nonzero coordinates of a and the *support* of a is $\{i \mid a_i \neq 0\}$; i.e., $|\text{support}(a)| = \text{weight}(a)$. The *minimum weight* of a code C is $\text{Min}_{0 \neq c \in C}$ weight (c). Connections between codes and designs frequently arise because the collection of supports of the minimum-weight vectors of a mathematically interesting code has a good chance of being a design. There are many well-known instances of such connections. For a discussion of these connections and a fuller discussion of the notion of a code the novice reader may wish to consult [7].

3. Ovals

Consider a projective design with parameters (v, k, λ). We call a collection S of points of the design an *arc* if no three points of S lie on a block. In other words, for every block, B, of the design, $B \cap S$ has cardinality 0, 1, or 2.

Correspondingly, we call such a block an *exterior* block, *tangent* block, or *secant* block.

Now suppose S is an arc with at least one tangent, B_0 say. Let p be the single point of $S \cap B_0$. Given q in S, $q \neq p$, there are precisely λ blocks B with $S \cap B = \{p, q\}$. As q runs through $S - \{p\}$ the $\lambda(|S| - 1)$ blocks obtained are distinct. Hence $\lambda(|S| - 1) \leqslant k - 1$ since there are but $k - 1$ blocks through p other than B_0. We obtain the bound

$$|S| \leqslant \frac{k + \lambda - 1}{\lambda}.$$

If, on the other hand, there are no tangents, then choosing $p \in S$ and letting q run through $S - \{p\}$ we have that $\lambda(|S| - 1) = k$ and hence that

$$|S| = \frac{k + \lambda}{\lambda}.$$

In particular then, an arc without tangents can occur only when λ divides k and its cardinality is then determined. For such an arc S choose a point[1] p not on S and consider the k blocks through p. Suppose x of them actually meet S (in necessarily two points). Then $2x = \lambda |S|$ and therefore $k + \lambda = \lambda |S|$ is necessarily even. Since $k + \lambda \equiv k - \lambda \pmod 2$ an arc without tangents can occur only in a projective design of even ordıe (with, moreover, λ dividing k).

More can be said: Suppose $(k + \lambda - 1)/\lambda$ is an integer (and thus, for $\lambda > 1$, λ does not divide k) and we have an arc S with the maximal number of points, $(k + \lambda - 1)/\lambda$. Then, through each point p on S there must pass precisely one tangent. Assuming further that $k - \lambda$, the order of the design is odd, let p be on S and let B be the tangent through p. Suppose there is a q on B, $q \neq p$, through which there are no other tangents besides B. Then, the $k - 1$ remaining blocks through q are either secants or exterior. Suppose there are y secants. Now $\lambda - 1$ of these pass through p and hence meet S precisely once more. Hence $y - \lambda + 1$ meet $S - \{p\}$ twice and thus

$$\lambda\left(\frac{k + \lambda - 1}{\lambda} - 1\right) = \lambda - 1 + 2(y - \lambda + 1),$$

or $k - 1 = 2y - \lambda + 1$. Thus $k - \lambda = 2(y - \lambda + 1)$ is even, a contradiction. It follows that through every point not on S there pass either no tangents or at least two. Further, with p and B as above count flags of the form (q, T) where $q \in B \cap T$, $q \neq p$, $T \neq B$, and T is a tangent of S. Then $\lambda((k + \lambda - 1)/\lambda) - 1) = \sum_{i=2}^{\infty} (i - 1)\, x_i$, where x_i is the number of q's through which there pass i tangents. On the other hand $\sum_{i=2}^{\infty} x_i = k - 1$.

[1] Such a choice is possible except for the design with parameters (3, 2, 1) where the point set itself is the arc.

Hence $\sum_{i=2}^{\infty} x_i = k - 1 = \sum_{i=2}^{\infty} (i - 1) x_i$. Since all x_i are nonnegative $x_3 = x_4 = \cdots = 0$. Thus, through each $q \in B$, $q \neq p$, there pass precisely two tangents. (This proves, incidentally, that the $(k + \lambda - 1)/\lambda$ tangents form an arc meeting the bound in the dual design.) We call such a point an *exterior* point of S. Points q, $q \notin S$, through which no tangents pass are called *interior* points. Clearly the number of exterior points is $\frac{1}{2}(k - 1) \times ((k + \lambda - 1)/\lambda)$ and thus the number of interior points is easily calculated. It is $\frac{1}{2}(k - 1)((k - \lambda - 1)/\lambda)$.

The above results are generalizations of known results for $\lambda = 1$ (the case of projective planes). We summarize them in the following

THEOREM 1. *In a projective design with parameters* (v, k, λ) *with* $k > 2$, *the number of points of an arc is bounded by*

$$\frac{k + \lambda - 1}{\lambda}$$

provided either the design is of odd order or of even order with $k \not\equiv 0 \bmod \lambda$. *For a projective design of even order with* $k \equiv 0 \pmod{\lambda}$ *the bound is*

$$\frac{k + \lambda}{\lambda}.$$

In the odd-order case whenever $(k + \lambda - 1)/\lambda$ *is an integer and an arc exists meeting the bound, then through each point of the arc passes exactly one tangent and through a point not on the arc there pass either two tangents (exterior point) or none (interior point). Moreover, the tangents form an arc in the dual design.*

Our primary interest is in planes and biplanes. Here the extra condition that λ divide k in the even-order case is automatically satisfied and hence there is a natural dichotomy between even and odd orders. It is, of course, well known [8] that in a projective plane of odd order m an arc can have at most $m + 1$ points and in a projective plane of even order at most $m + 2$ points (the bounds or our theorem, the order here being $k - 1$). For biplanes (i.e., projective designs with $\lambda = 2$) we have that in a biplane of odd order $m = k - 2$ an arc can have at most

$$\frac{m + 3}{2}$$

points and for even order at most

$$\frac{m + 4}{2}$$

points.

If a projective design with parameters (v, k, λ) has an arc of cardinality at least 3, then by Theorem 1 we must have

$$3 \leqslant \frac{k+\lambda}{\lambda} = \frac{k}{\lambda} + 1.$$

Since $k/\lambda = (v-1)/(k-1)$ we have easily

PROPOSITION 1. *If a (v, k, λ)-design has an arc of cardinality at least* 3, *then*

$$2k \leqslant v + 1.$$

For a projective design of odd order with $(k + \lambda - 1)/\lambda$ an integer, an arc with $(k + \lambda - 1)/\lambda$ points will be called an *oval*; for a projective design of even order with λ dividing k, an arc with $(k + \lambda)/\lambda$ points will be called an *oval*; finally, for a projective design of even order with $\lambda > 1$ and λ dividing $k - 1$, an arc with $(k + \lambda - 1)/\lambda$ points will be called an *oval.* The term is new for designs with $\lambda > 1$ and differs from customary usage for projective planes of even order where a set of $m + 2$ points no three collinear is sometimes called a hyperoval. If D is a projective design, Oval(D) denotes the set of avals of the design.

Our next two propositions have very easy proofs (which we omit); the proofs involve only standard counting arguments.

PROPOSITION 2. *An oval in a projective design of even order* (*with λ dividing k*) *has $k(k + \lambda)/2\lambda$ secants and $(k - 2)(k - \lambda)/2\lambda$ exterior blocks* (*and, of course, no tangents*).

Remark. Taking as points the exterior blocks of such an oval and as blocks the points not on the oval, one obtains a 2-design. The parameters are

$$2 - \left(\frac{(k-2)(k-\lambda)}{2\lambda}, \frac{k-\lambda}{2}, \lambda\right).$$

Caution. For $\lambda > 1$ this 2-design may very well have repeated blocks; e.g., for (16, 6, 2)-designs the parameters are $2 - (4, 2, 2)$ and hence the design consists of the six 2-subsets of a 4-set, each 2-subset repeated.

PROPOSITION 3. *An oval in a projective design of odd order* (*with λ dividing $k - 1$*) *has $(k + \lambda - 1)/\lambda$ tangents, $(k + \lambda - 1)(k - 1)$ secants, $(k - \lambda - 1)(k - 1)/2\lambda$ exterior blocks, $(k + \lambda - 1)(k - 1)/2\lambda$ exterior points, and $(k - \lambda - 1)(k - 1)/2\lambda$ interior points. Moreover, the points of a tangent are exterior except for the point of contact, an exterior block* *contains* $(k + \lambda - 1)/2$ *exterior points and* $(k - \lambda + 1)/2$ *interior points, while a secant (besides the two points of the oval) contains* $(k + \lambda - 3)/2$ *exterior points and* $(k - \lambda - 1)/2$ *interior points.*

The theorem and propositions above are the basic counting results concerning ovals in projective designs. Next, we elaborate on the inequality of Proposition 1, settling the question of when equality occurs.

We first observe that the projective design consisting of the $(v - 1)$-subsets of a v-set has as its ovals all the 2-subsets of the point set. Its complement is the denerate projective design with $\lambda = 0$ whose only "oval" is the point set itself. Eschewing this uninteresting case we have the following consequence of Proposition 1.

PROPOSITION 4. *Suppose a projective design with parameters* (v, k, λ) *is such that both it and its complement have arcs of cardinality* 3. *Then for each design the arcs of cardinality* 3 *are the ovals and in fact the design is a Hadamard design or its complement; i.e., the parameters are either* $(4\lambda + 3, 2\lambda + 1, \lambda)$ *or* $(4\lambda - 1, 2\lambda, \lambda)$ *with* λ *even.*

Proof. Proposition 1 yields

$$v - 1 \leqslant 2k \leqslant v + 1.$$

For v odd the accounced parameters are obtained from the two equalities and the arcs of cardinality 3 are the ovals. So suppose v is even. Then $2k = v$, impossible parameters for a projective design since then $v(v - 2) = 4\lambda(v - 1)$ and hence

$$v^2 - (2 + 4\lambda)\, v + 4\lambda = 0,$$

implying that $4 + 16\lambda^2$ is a square. But then $1 + (2\lambda)^2$ would also be implying that $\lambda = 0$.

Consider such a $(4\lambda + 3, 2\lambda + 1, \lambda)$ design. Now, a "line" of a design is the intersection of all blocks containing two distinct points. In this case a line will consist merely of these two points or three points [8]. The nontrivial lines are precisely the ovals of the complementary design. Precisely we have the following

PROPOSITION 5. *The ovals of a* $(4\mu - 1, 2\mu, \mu)$*-design are precisely those lines of the complementary design whose cardinality is three.*

Proof. The complementary design has $\lambda = \mu - 1$. Consider three points and let x_i, $i = 0, 1, 2, 3$, denote the number of blocks containing i of these points. From $\sum x_i = 4\lambda + 3$, $\sum ix_i = 3(2\lambda + 1)$, and $\sum \binom{i}{2} x_i = 3\lambda$ it follows that

$$x_0 + x_3 = \lambda.$$

But for a line l of cardinality 3, $x_3 = \lambda$ and hence $x_0 = 0$. Thus l is an oval. On the other hand an oval with three points has no tangents and hence every block of the complementary design meeting it twice must contain it. Thus it is a line of the complementary design.

Thus the ovals of the complements of Hadamard designs are well-known geometric objects. These ovals will never form a 2-design except in the classical case of the complement of $PG_n(2)$, a fact easily derivable from algebraic coding theory and well known [8]. In fact, as we remarked in the Introduction, the classical projective designs consisting of points and hyperplanes of $PG_n(q)$ cannot have an arc of cardinality 3 for $n > 2$. There is this one case, however, where the complement of a classical projective design has ovals. The precise result follows easily from Proposition 1. It is

PROPOSITION 6. *If the complement of a classical projective design has an arc of cardinality* 3, *then* $q = 2$ *and the arcs of cardinality* 3 *are the ovals and consist precisely of the lines of* $PG_n(2)$.

Proof. The classical design has parameters

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

and hence the complement has $k = q^n$. Proposition 1 now implies that

$$2q^n \leqslant \frac{q^{n+1}-1}{q-1} + 1$$

or that

$$q^{n+1} \leqslant 2q^n + q - 2.$$

Hence $q \leqslant 2 + (q-2)/q^n$ or $q \leqslant 2$. Thus the parameters of the design are $(2^{n+1} - 1, 2^n, 2^{n-1})$ and the arcs of cardinality 3 are the ovals. Since every line of $PG_n(2)$ meets every hyperplane, the lines are ovals of the complementary design. On the other hand any three points of $PG_n(2)$ that meet every hyperplane (i.e., form an oval of the complementary design) must constitute a line of $PG_n(2)$.

Remark. As a final comment concerning basic general results we note that arcs can be defined more generally for an arbitrary 2-design.

Denoting the parameters by $2-(v, k, \lambda)$ define r by

$$r = \frac{\lambda(v-1)}{(k-1)}.$$

Then the order of the design is defined to be $r - \lambda$. The bounds of Theorem 1 obtain upon replacing k by r. Defining ovals in the obvious way, one can easily verify the following facts:

(a) For a Steiner triple system (i.e., a $2-(v, 3, 1)$-design) of even order (i.e., $\frac{1}{2}(v-3)$ is even) the ovals are precisely the complements of the maximal subsystems (i.e., subsystems on $(v-1)/2$ points).

(b) Given a 3-design which is a Steiner system (i.e., has parameters $3-(v, k, 1)$) contracting on a point gives a 2-design with parameters $2-(v-1, k-1, 1)$. The blocks of the 3-design not containing the point of contraction are clearly arcs. When these blocks are in fact ovals of the contraction, then in the even-order case the 3-design must be the extension of a projective plane of order 2, 4, or (possibly) 10 and in the odd-order case the 3-design must be an inversive plane of odd order.

(c) For the Desarguesian projective planes of even order q, the ovals form a 2-design. The ovals of this 2-design are the lines of the projective plane.

(d) More generally, if the ovals of an even-order 2-design with λ dividing r form a 2-design, then this 2-design is of even order with its "λ" dividing its "r" and, moreover, the blocks of the original design are among its ovals.

4. Examples

1. In the seven-point Fano plane, the projective plane of order 2, the ovals are precisely the complements of the lines and these seven ovals form the unique biplane of order 2. The ovals of this biplane are precisely the lines of the Fano plane. Thus, $\text{Oval}(PG_2(2)) = B(2)$ and $\text{Oval}\ (B(2)) = PG_2(2)$. The fact that the ovals of $B(2)$ form a 2-design is a characterization of this projective design in the following sense: Suppose a (v, k, λ)-design has $k \equiv 0 \pmod 4$, $\lambda \equiv 2 \pmod 4$, and λ divides k. Then, if its ovals form a 2-design, we have $k = 4$. That is, it must be $B(2)$. We sketch a proof.

Let C be the row space of the incidence matrix over the field with two elements. Clearly, $C \subset C^{\perp}$ and C is "doubly even" (i.e., all vectors have weight congruent to 0 modulo 4). The congruence conditions on k and λ allow one to conclude (using the theory of elementary divisors and a result of Bruck's [6, 15]) that the dimension of C is $(v-1)/2$ and hence that $C^{\perp} = C \oplus F_2(1, 1, \ldots, 1)$; i.e., C is of codimension 1 in $C^{\perp}$ and $C^{\perp}$ is obtained from C

by throwing in the all-one vector. By now almost standard arguments [1, 7] (cf. Section 3, final remark (d)) determine the minimum weights of C and $C^{\perp}$. They are $d = k$, $d^{\perp} = (k + \lambda)/\lambda$. Next suppose c and c' are minimum-weight vectors of $C^{\perp}$. They are not in C but their sum is. The weight of $c + c'$ is

$$2\left(\frac{k+\lambda}{\lambda}\right) - 2a,$$

where $a = |\text{support}(c) \cap \text{support}(c')|$. Since $2(k/\lambda + 1)$ is congruent to 2 modulo 4, a is odd. But $a > 1$ implies that the weight of $c + c'$ is less than k, an impossibility. Therefore $a = 1$. Thus, the supports of the minimal-weight vectors of $C^{\perp}$ form a 2-design in which every two blocks meet exactly once. Hence they are a projective plane of order k/λ and $v = (k/\lambda)^2 + k/\lambda + 1$. But $v = 1 + (1/\lambda)\, k(k - 1)$. It follows that $k = 4$ and we have the characterization.

2. For the unique biplane of order 1 the ovals are precisely the 2-subsets of the underlying 4-set and hence this biplane has six ovals. Although this is a trivial example we will make use of it in a nontrivial way in Section 6. In general when one has a projective design with parameters $(v, v - 1, v - 2)$, $(k + \lambda - 1)/\lambda = 2$ is an integer and the ovals are the 2-subsets of the underlying point set.

3. The three biplanes of order 4 have been extensively studied. It is quite easy to to survey the ovals via algebraic coding theory using the MacWilliams equations. Here an oval has four points. Denoting the three biplanes of order 4 by B_6, B_7, B_8 (for an explanation of the notation see [4]), we have that $|\text{Oval}(B_6)| = 60$, $|\text{Oval}(B_7)| = 28$, $|\text{Oval}(B_8)| = 12$. Since B_6 has a doubly transitive automorphism group the 60 ovals form a 2-design; the parameters are $2 - (16, 4, 3)$. This design can be broken up into the disjoint union of an affine plane of order 4 and a 2-design with parameters $2 - (16, 4, 2)$ and this latter 2-design cannot be broken up into the disjoint union of two affine plane of order 4.

4. The quadratic-residue design that yields $B(3)$, the unique biplane of order 3, i.e., an $(11, 5, 2)$-design, has ovals of cardinality 3. One sees easily that there are 55 such ovals forming a 2-design with parameters $2 - (11, 3, 3)$. In Section 6 we will make use of this result.

5. There are precisely four biplanes of order 7 [12]. The oval structure of one of these biplanes is intimately related to $PG_2(8)$. The difference set biplane has no ovals. The other three have 63 ovals (Mezzaroba and Salwach, private communication).

6. There are four known biplanes of order 9. The one related to the strongly regular graph has precisely 336 ovals. The other three have 120,

64, and 48, respectively (Mezzaroba and Salwah, private communication).

7. The remaining two known biplanes are of order 11 and are duals of each other. They hence have the same number of ovals by Theorem 1. We have not determined that number, but we know that ovals do exist.[1]

8. The (25, 9, 3)-design (number 20 of the Fisher–Yates table) has 16 ovals. (Caution: The entry in Hall's table contains an error.)

9. There are precisely five (15, 7, 3)-designs [5]. Consider the collection of 3-subsets of the point set of such a design and let y_i, $i = 0, 1, 2, 3$, be the number of 3-subsets contained in precisely i blocks. Thus y_0 is the number of ovals of the design and y_3 the number of lines. We have the following equations:

$$y_0 + y_1 + y_2 + y_3 = \binom{15}{3} = 5 \cdot 7 \cdot 13,$$

$$y_1 + 2y_2 + 3y_3 = 15 \cdot \binom{7}{3} = 5 \cdot 7 \cdot 15,$$

$$y_2 + 3y_3 = \binom{15}{2} = 7 \cdot 15.$$

Only the last equation needs explication; it is a count of flags of the form "a 3-subset contained in two blocks." One deduces immediately that

$$y_0 + y_3 = 35.$$

Bhat and Shrikhande [5] have determined y_3 for each of the five designs. Hence we can determine the number of ovals. Observe that for the classical design coming from $PG_3(2)$ the lines of the design are the lines of the geometry (whence the term and here $y_0 = 0$ as it should. Two (15, 7, 3)-designs have 7 lines and hence 28 ovals. One has 24 ovals and one 16 ovals. The one with 16 ovals has an incidence matrix that can be recorded succinctly; we do so: Let I be the 3×3 identity matrix, J the 3×3 all-one matrix, E_i the 3×3 matrix with 1's in row i and 0's elsewhere, and let F_i be the transpose of E_i. The incidence matrix is

$$\begin{pmatrix} I & E_1 & E_2 & E_3 & J \\ J - F_1 & J - I & I & I & I \\ J - F_2 & I & J - I & I & I \\ J - F_3 & I & I & J - I & I \\ 0 & J - I & J - I & J - I & I \end{pmatrix}$$

The first three points constitute an oval. The automorphism group of the

[1] *Added in proof.* There are precisely 77.

design has order 96 and the subgroup fixing the oval is Sym(3), the automorphism group being transitive on the set of 16 ovals.

10. We shall now describe the construction of a (85, 21, 5)-design, $\mathscr{D}$, with an oval L. Here $|L| = 5$. The construction will first produce a resolvable $2 - (64, 16, 5)$. We then adjoin a copy of $PG_2(4)$ as a block and to each block of a parallel class in the resolvable design, $\mathscr{R}$, we add a line of $PG_2(4)$. We shall do this in such a way that a prescribed set of five points will form the oval. Consider four copies of $AG_2(4)$ which we call A_1, A_2, A_3, A_4. These are one of the parallel classes of 16-point blocks in $\mathscr{R}$. Let Π be a $PG(2, 4)$. Choose P_i in A_i ($i = 1,..., 4$) and P_5 in Π. These five points will form the oval. Take a line l in Π not through P_5, and adjoin l to A_1,..., A_4. We now have five blocks of $\mathscr{D}$. Since each of these contains one point of L they will be tangents to the oval. Observe that the points of l are on *all* the tangents.

For the main part of our construction we need an auxiliary affine plane P of order 4 with a circle C (a set of four points, no three on a line). We observe that the five parallel classes of lines in P split the four points of C into two pairs three times and into four single points twice (i.e., if two points of C are on a line, then the other two are on a parallel line).

We now describe the construction of 16 blocks of $\mathscr{R}$, divided into four parallel classes. In each of the A_i we pick a parallel class of lines. This gives us 16 lines. We identify these 16 lines with the 16 points of P in such a way that the four lines in any A_i correspond to four points of a line in P and furthermore such that the lines containing P_1, P_2, P_3, P_4 correspond to the points of C. We saw above that this is possible. Now the structure of P immediately yields 20 blocks of 16 points divided into five parallel classes, one of which is $\{A_1, A_2, A_3, A_4\}$. In this way we have found 16 new blocks of $\mathscr{R}$. Three of the parallel classes have two blocks containing two points from $\{P_1, P_2, P_3, P_4\}$. In Π there are 15 lines different from l and not containing P_5. These lines we adjoin in an arbitrary way to the 15 parallel classes mentioned above. The remaining lines of Π are adjoined to the other parallel classes of blocks in $\mathscr{R}$. This completes the construction, and it is obvious that L is an oval. (This construction is based on a suggestion by R. M. Wilson.)

If we copy this construction replacing $PG_2(4)$ by $PG_2(3)$ and the four copies of $AG_2(4)$ by three copies of $AG_2(3)$, each with a specified point P_i ($i = 1, 2, 3$) and finally use an auxiliary $AG_2(3)$ with three points not on a line, we construct a (40, 13, 4) with a 3-arc. This design is obviously not equivalent to $PG_3(3)$. However, it does not have an oval; in fact we have not been able to find a (40, 13, 4)-design with an oval.

We have already discussed all the known biplanes and several projective designs with $\lambda \geq 3$. We conclude this section with a list, followed by comments, of the 11 parameter sets of projective designs with $\lambda \geqslant 3$ and $k \leqslant 15$ for which ovals could exist.

		v	k	λ	Oval size
Odd order					
	1	31	10	3	4
	2	19	9	4	3
	3	40	13	4	4
	4	27	13	6	3
Even order					
$\lambda \mid k$	5	25	9	3	4
	6	71	15	3	6
	7	15	8	4	3
	8	23	12	6	3
Even order					
$\lambda \mid (k-1)$	9	15	7	3	3
	10	23	11	5	3
	11	31	15	7	3

Comments. 1. Design 40 of Hall's table [9] possesses ovals. In fact, his points $0_4, 1_4, \ldots, 6_4$ contain a projective plane of order 2 whose ovals are ovals of the design. So there are at least seven.

2. All (19, 9, 4)-designs have been found. All but the classical quadratic-residue design have ovals. A proof of this assertion can be extracted from [11].

3. See the last paragraph of Example 10. This is the only set of parameters listed above for which there is some doubt concerning the existence of a design with ovals.

4. A Hadamard design. The construction of one with ovals should present little difficulty.

5. See Example 8.

6. A design with these parameters possessing an oval has been constructed by Beker and Haemers (private communication).

7. See Proposition 5 and Example 9.

8. Hadamard.

9. See Example 9.

10. Hadamard.

11. Hadamard.

5. Ovals from the Point of View of Coding Theory

The problem breaks naturally into two cases: even order and odd order. The even order case is more transparent and we treat it first.

Suppose we are given a projective design with parameters (v, k, λ) where $k - \lambda$ is even and λ divides k. Then, as we have seen, an oval is a set L of $(k + \lambda)/\lambda$ points of the design with the property that $|L \cap B|$ is either 0 or 2 for every block of the design. Clearly then an oval is a vector of weight $(k + \lambda)/\lambda$ in $C^{\perp}$ where C is the row space over F_2 of the design's incidence matrix. In fact, $C^{\perp}$'s minimal-weight vectors are the ovals; precisely we have the following

Proposition E. For a (v, k, λ)-design of even order with λ dividing k, the minimum weight of $C^{\perp}$ is at least $(k + \lambda)/\lambda$ and the vectors of weight $(k + \lambda)/\lambda$ are precisely the ovals of the design. Here C is the row space over F_2 of the design's incidence matrix.

Proof. Let v be a vector in $C^{\perp}$ and set $S = \text{support}(v) = \{p \mid v_p = 1\}$. Pick p_0 in S. Now, each of the k blocks through p_0 meets S evenly and hence in at least one other point of S. Counting flags of the form (q, B) where $q \in S$, $q \neq p_0$ with $\{p_0, q\} \subset B$, a block, yields

$$\lambda(|S| - 1) = \sum_{p_0 \in B} |B \cap (S - \{p_0\})|.$$

This yields immediately that $|S| \geqslant (k + \lambda)/\lambda$ with equality if and only if $|B \cap (S - \{p_0\})| = 1$ for each block through p_0. This proves the proposition.

Remarks. 1. For $\lambda = 1$, i.e., for projective planes of even order, this result is well known and, in fact, more is true: The minimum weight of C is k and the minimum-weight vectors are precisely the lines of the plane. For $\lambda > 1$ the minimum weight of C may or may not go down; e.g., for B_6 it is 6 and the minimum-weight vectors are the blocks, while for B_7 and B_8 the minimum weight is 4. Moreover, for B_7 and B_8 the vectors of weight 6 in C include not only the blocks of the design but others as well. For a complete discussion see [4].

2. Knowing the weight distribution of C allows one to compute, via the MacWilliams equations, the weight distribution of $C^{\perp}$ and hence the number of ovals of the design. This was the method used in many of the examples of Section 4.

Examples. 1. For $PG_2(2)$ the weight distribution of C and $C^{\perp}$ is

Weight	0	3	4	7	
No. of vectors	1	7	7	1	C
	1	0	7	0	$C^{\perp}$

2. For $PG_2(4)$ the weight distribution of C and $C^\perp$ is

Weight	0	5	6	8	9	10	12	13	14	16	21	
No. of	1	21	0	210	280	0	280	210	0	21	1	C
vectors	1	0	168	210	0	1008	280	0	360	21	0	$C^\perp$

The vectors of weight 6 are, of course, the ovals. The vectors of weight 14 are easily seen to be the complements of the projective planes of order 2 contained in $PG_2(4)$. The vectors of weight 16 are the affine planes of order 4. The vectors of weight 9 are the affine planes of order 3. These results are very easily obtained and we omit the details. The only other projective plane of even order for which the weight distribution has been obtained is $PG_2(8)$. It It was a formidable task, even with electronic computation, to obtain it —especially 20 years ago when Eugene Prange did so. We do not include it here.

3. For our final example we give the weight distribution of the modulo 2 row space of the (25, 9, 3)-design of Example 8 of Section 4. It was obtained for us by Chester Salwach via a few seconds of electronic computation. Since dim $C = 13$ and the extended code is self-dual (k and λ both being odd), C is simply the even-weight subcode of C (as in Example 1 above).

Weight	0	4	5	8	9	12	13	16	17	20	21	25
No. of vectors	1	16	36	486	961	2596	2596	961	486	36	16	1

We next discuss ovals in projective designs of odd order. Thus we give ourselves a (v, k, λ)-design with $k - \lambda$ odd and $k \equiv 1 \pmod{\lambda}$, and our ovals will be certain subsets of the points of the design of cardinality $(k + \lambda - 1)/\lambda$. Now it is well known [10] that the code C over F_q given by the row space of the design's incidence matrix is uninteresting unless the prime q divides $k - \lambda$. We want to locate the ovals in $C^\perp$ for those primes dividing $k - \lambda$. We have the following

PROPOSITION O. *Let L be an oval in a projective design of odd order with parameters (v, k, λ) and C be the row space of the design's incidence matrix over F_q where q is a prime dividing $k - \lambda$. Then the following vector v is in $C^\perp$: $v_p = 1 - \lambda$ for $p \in L$, $v_p = 1$ for p an exteriror point, and $v_p = 1 - 2\lambda$ for p an interior point.*

Proof. We must show that for every block, B, of the design $\sum_{p\in B} v_p = 0$. Now a block is either exterior, a tangent, or a secant. Since by Proposition 3 all points of a tangent are exterior points except for the point of contact, when B is a tangent $\sum_{p \in B} v_p = 1 - \lambda + (k - 1) = k - \lambda = 0$ since q divides $k - \lambda$.

Again by Proposition 3, for B an exterior block,

$$\sum_{p\in B} v_p = \frac{k+\lambda-1}{2} + (1-2\lambda)\left(\frac{k-\lambda+1}{2}\right) = (k-\lambda)(1-\lambda) = 0.$$

Finally, for B a secant, Proposition 3 yields

$$\begin{aligned}\sum_{p\in B} v_p &= 2(1-\lambda) + \frac{k+\lambda-3}{2} + (1-2\lambda)\left(\frac{k-\lambda-1}{2}\right)\\ &= (k-\lambda)(1-\lambda) = 0.\end{aligned}$$

Remark. For $\lambda = 1$, i.e., for projective planes, Proposition O was proved by Assmus and co-workers [3, 4]. In fact in this case more is true; roughly speaking Proposition 0 becomes an "if and only if." This ought to be true for $\lambda > 1$ also, at least when one works over Z, but we have not been able to prove it.

EXAMPLE. For $B(3)$, the (11, 5, 2)-design, one must take $q = 3$. C here is nothing but the ternary Golay code and $C^\perp \subset C$. There are 110 weight-9 vectors in C and 55 of them have three -1's and six 1's. These 55 vectors yield the ovals; i.e., the three coordinate positions where the -1's occur are not on a block as one easily sees from elementary facts concerning the Golay code.

6. THE PLANE–BIPLANE CONNECTION

Assmus *et al.* [2] describe four methods of producing codes from projective designs. One of these methods relates odd-order biplanes and even-order projective planes. The theorem detailing the connection has a more succinct statement in the context of ovals and we give that statement here together with the known examples.

By way of preparation, recall that given a projective plane of even order, i.e., a projective design with parameters $(m^2 + m + 1, m + 1, 1)$, m even, the modulo 2 span of its bordered incidence matrix (i.e., the design's incidence matrix bordered by a column of 1's) is a self-orthogonal code of block length $m^2 + m + 2$ and minimum weight $m + 2$. If C is this code, calling ∞ the added coordinate, we have that the vectors of weight $m + 2$ of C with a 1 at ∞ are precisely the lines of the plane (with an overall parity check added) while the vectors of weight $m + 2$ in $C^\perp$ with a 0 at ∞ are precisely the ovals of the plane. Of course, $C \subset C^\perp$ with equality whenever $m \equiv 2 \pmod 4$.

Now consider a biplane of odd order n, i.e., a projective design with parameters

$$(1 + \tfrac{1}{2}(n + 2)(n + 1), n + 2, 2),\ n \text{ odd}.$$

Let M be its incidence matrix, set $v = 1 + \frac{1}{2}(n + 2)(n + 1)$, and consider the row space modulo of the v by $2v$ matrix G where G's first v columns are those of the identity matrix I_v and the last v columns are those of M. Call this row space B. Clearly, B is self-dual $(2v, v)$ code over F_2. Incredibly, one can determine not only the minimum weight of B but its minimum-weight vectors as well. Precisely, we have the following

THEOREM 2. *If M is the incidence matrix of an odd-order biplane, M^t its transpose, then the row spaces over F_2 of $G = I_v \mid M$ and $G' = M^t \mid I_v$ are identical. This row space B is a self-dual $(2v, v)$ code over F_2 with minimum weight $n + 3$, n being the order of the biplane. Moreover, the minimum-weight vectors are, besides the rows of G and G', the characteristic functions of the sets of the form $L^d \cup L$, where L is an oval of the biplane and L^d its dual.*

Before sketching a proof we give some examples:

1. Consider the unique biplane of order 1, i.e., the (4, 3, 2) projective design consisting of the four 3-subsets of a 4-set. Its ovals are the six 2-subset of the 4-set. The (8, 4) binary code obtained is, of course, the extended Hamming code with minimum weight 4 and the minimum-weight vectors are precisely the Steiner system of type 3 — (8, 4, 1). This system is, of course, the extension of a projective plane of order 2 and could equally well be obtained as the row space of this plane's bordered incidence matrix.

2. Consider the unique biplane of order 3, i.e., the (11, 5, 2) projective design described in Example 4 of Section 4. It has 55 ovals; they are the 3-subsets of the 11-set not contained in a block. Hence B is a (22, 11) self-dual code over F_2 with 77 minimum-weight vectors, 11 each from G and G' together with the 55 of the form $L^d \cup L$, L and oval. Since B is self-orthogonal any two minimum-weight vectors have either two or no 1's in common. It follows immediately that any 3-subset of the 22-set is covered by a unique minimum-weight vector and hence these vectors form a Steiner system of type 3-(22, 6, 1), i.e., the extension of a projective plane of order 4. Observe that if C is the row space over F_2 of the bordered incidence matrix of the projective plane of order 4, then dim $C = 10$ and dim $C^\perp = 12$. $C \subset C^\perp$ and there are therefore three 11-dimensional subspaces between C and $C^\perp$. Each of them is a copy of the B produced by the theorem and these three subspaces yield the classical splitting of the 168 ovals of the plane into three groups of 56.

3. There are no biplanes of order 5 (indeed none of order congruent to 5 modulo 8). There are precisely four of order 7 [12]. Each yields a (74, 37) self-dual code over F_2 with minimum weight 10. One of these codes is related to the projective plane of order 8, the other three are not. A fuller account is in [2].

4. There are four known biplanes of order 9. No one of them yields a projective plane or order 10; they do not have enough ovals. The two known biplanes of order 11 (duals of one another) do not yield a projective plane of order 12 for the same reason. There are no other odd order biplanes known.

Since a proof of Theorem 2 has already appeared we give only a sketch here: The fact that G and G' have the same row space follows either from the fact $M^t = M^{-1}$ (modulo 2) or the fact that B is self-dual. That the minimum weight is $n + 3$ follows from the fact that the sum of fewer than $\frac{1}{2}(n + 3)$ rows of G has too high a weight on the last v coordinates. Moreover, a weight $n + 3$ vector which is not a row of G or G' must of necessity have $(n + 3)/2$ 1's both in the first v coordinates and in the last v coordinates. Now, if L is an oval of the design, the modulo 2 sum of the tangents is clearly of the form $L^d \cup L$ in veiw of Theorem 1. Moreover, given a vector of weight $n + 3$ in B which is not a row of G or G' it has one half of its 1's in the first v coordinates and one half in the last v. Denoting by L the positions in which there is a 1 in the last v coordinates for each point p of L there is at least one block B with $B \cap L = \{p\}$ and because of B's self-orthogonality these $\frac{1}{2}(n + 3)$ blocks must correspond precisely to the $\frac{1}{2}(n + 3)$ 1's in the first v coordinates with every other block meeting L either twice or not at all. That is, the vector is of the form $L^d \cup L$.

References

1. E. E. Assmus, Jr., H. F. Mattson, Jr., and M. Guza, Selforthogonal Steiner systems and projective planes, *Math. Z.* **138** (1974), 89–96.
2. E. F. Assmus, Jr., J. A. Mezzaroba, and C. J. Salwach, Planes and biplanes, *in* "Higher Combinatorics" (M. Aigner, Ed.), pp. 205–212, Reidel, Dordrecht, 1977.
3. E. F. Assmus, Jr. and H. E. Sachar, Ovals from the point of view of coding theory, *in* "Higher Combinatorics" (M. Aigner, Ed.), pp. 213–216, Reidel, Dordrecht, 1977.
4. E. F. Assmus, Jr. and C. J. Salwach, The (16, 6, 2) designs, *Internat. J. Math. Sci.* **2** (1979), 261–281.
5. V. N. Bhat and S. S. Shrikhande, Non-isomorphic solutions of some balanced incomplete block design, I, *J. Combinatorial Theory* **9** (1970), 174–191.
6. R. H. Bruck, private communication.
7. P. J. Cameron and J. H. van Lint, "Graph Theory, Coding Theory and Block Designs," London Math. Soc. Lecture Note Series 19, Cambridge Univ. Press, London/New York, 1975.
8. P. Dembowski, "Finite Geometries," Springer–Verlag, New York/Berlin, 1968.
9. M. Hall, Jr., "Combinatorial Theory," Ginn/Blaisdell, Waltham, Mass., 1967.
10. N. Hamada, On the p-rank of the incidence matrix of a balanced or partially balanced incomplete block design and its application to error-correcting codes, *Hiroshima Math. J.* **3** (1973), 153–226.
11. J. H. van Lint, H. C. A. van Tilborg, and R. Wiekema, Block designs with $v = 10$, $k = 5$, $\lambda = 4$, *J. Combinatorial Theory Ser. A* **23** (1977), 105–115.

12. J. A. MEZZAROBA AND C. J. SALWACH, The four biplanes with $k = 9$, *J. Combinatorial Theory Ser. A* **24** (1978), 141–145.
13. H. J. RYSER, "Combinatorial Mathematics," Carus Mathematical Monograph No. 14, Wiley, New York, 1963.
14. H. SACHAR, The F_p span of the incidence matrix of a finite projective plane, *Geometriae Dedicata*, in press.
15. C. J. SALWACH, "Biplanes and Projective Planes," Ph.D. dissertation, Lehigh University, Bethlehem, Pa., May 1976.

Printed by the St. Catherine Press Ltd., Tempelhof 37, Bruges, Belgium