Ovals in the Designs $W(2^m)$

J.D. Key and K. Mackenzie

Department of Mathematical Sciences,
Clemson University,
Clemson, SC 29634, U.S.A.

Abstract. Using the permutation action of the group $PSL_2(2^m)$ on its dihedral subgroups of order $2(2^m + 1)$ for the description of the class of designs $W(2^m)$ derived from regular ovals in the desarguesian projective plane of order 2^m, we construct a 2-design of ovals for $W(2^m)$ for $m \geq 3$, and thus determine certain properties of the binary codes of these classes of designs.

1. Introduction

The class of designs that we consider were given originally through a general construction of Bose and Shrikhande [4], and involves a finite projective plane Π of even order n with an oval $\mathcal{O}$, i.e. an $(n+2)$-arc (also called a hyperoval in the literature). Define an incidence structure, which we denote by $W(\Pi, \mathcal{O})$, as follows: the point set $\mathcal{P}$ is the set of cardinality $\frac{1}{2}n(n-1)$ consisting of the exterior lines of $\mathcal{O}$, i.e. the lines of Π that do not meet $\mathcal{O}$; the block set $\mathcal{B}$ is the set of points of Π not on $\mathcal{O}$; incidence is defined as in Π. Then, if $n \geq 2$, $W(\Pi, \mathcal{O})$ is a 2-$(\frac{1}{2}n(n-1), \frac{1}{2}n, 1)$ design, with $b = |\mathcal{B}| = n^2 - 1$, $r = n + 1$ and order $r - 1 = n$.

In particular, for $n = 2^m$, $m \geq 2$, $W(\Pi, \mathcal{O})$ is a $2-(2^{m-1}(2^m-1), 2^{m-1}, 1)$ design, with $b = 2^{2m}-1$, $r = 2^m+1$, and order $n = 2^m$. For $\Pi = PG_2(n)$, with $n = 2^m$, and $\mathcal{O}$ a regular oval (i.e. a conic together with its nucleus), we write $W(\Pi, \mathcal{O}) = W(n)$, following Buekenhout et al. [5], since all regular ovals are equivalent. Wertheimer [9, Prop. 5.2] and [10] found these designs in a new way amongst a general class of elliptic quadric designs. For our purposes we need yet another construction, which we take from Kantor [7,Lemma 6.3] but see also Camina [6].

Let $G = PSL_2(n)$, where $n = 2^m \geq 4$, and let H be a subgroup of G that is dihedral, of order $2(n+1)$. Now let G act in the usual way on the set of right cosets of H, which we will denote by Ω. Since G is simple, the representation is faithful, and we have $|\Omega| = (n+1)n(n-1)/2(n+1) = \frac{1}{2}n(n-1)$. For any point α of Ω, $|G_\alpha| = |H| = 2(n+1)$. The involutions of G fix exactly 2^{m-1} points of Ω (see [7, p. 508]), and we take these sets of points as the blocks of the design. Thus a point α is on a block t if and only if t fixes α, i.e. t is in G_α. Since each G_α is dihedral of order $2(n+1)$, it contains $n+1$ involutions, so every point α is on $r = n+1$ blocks. The number b of blocks is the number of involutions in G, i.e. $(n+1)(n-1) = n^2 - 1$. Since all involutions are conjugate, the number of points per block is a constant, k, where k is given by $bk = vr$, since we at least have a 1-design. Thus $k = \frac{1}{2}n$. To show that we have a 2-design, notice first that if α and β are two distinct points of Ω, then $|G_\alpha \cap G_\beta| \leq 2$, so there is at most one involution fixing α and β, i.e. there is at most one block through α and β. Now, counting points on blocks through α, we have α on $n+1$ blocks, each with $\frac{1}{2}n-1$ points other than α, and no point on more than one block through α. This gives the number of points on a block with α as $(n+1)(\frac{1}{2}n-1) = v-1$. Thus we have a 2-design with $\lambda = 1$.

For $n = 8$, only the desarguesian plane exists, and all ovals are regular. The design $W(8)$ is then the familiar smallest Ree unital, with parameters 2-(28, 4, 1), and a doubly transitive automorphism group, $P\Gamma L_2(8)$. For $n > 8$, the automorphism group of $W(n)$ is only $1\frac{1}{2}$-transitive: see [5].

2. Ovals for $W(n)$, $n \geq 8$

For a 2-(v, k, λ) design $\mathcal{D}$ of even order $n = r - \lambda$, where r is the number of blocks through a point, an oval is an arc of maximal size, viz $(r+\lambda)/\lambda$: see [1] for discussion on this. There it was shown that if $\mathcal{D}$ has ovals, and if some of these ovals form a 2-design, then the binary code C of $\mathcal{D}$ has minimum weight equal to k, the block size of $\mathcal{D}$. (By the code of a design $\mathcal{D}$ over a prime field $\mathbf{F}_p$ we mean the subspace of $\mathbf{F}_p^v$ spanned by the characteristic functions on the blocks of $\mathcal{D}$: see [1], for example.)

We show now how to find a set of ovals for $W(n)$, for $n \geq 8$, and then how these ovals form the blocks of a 2-design. Notice that the size of an oval for $W(n)$ is $n+2$ (since $\lambda = 1$, and $r = n+1$), which is the same as the size of an oval in the plane. Essentially, of course, we are simply looking for a particular class of ovals in the dual plane of Π.

First some notation: for a particular α in Ω let T denote the set of involutions (equivalently, blocks) in G_α. So $|T| = n+1$. Further, since $|G_{\alpha,\beta}| = 2$ for $\alpha \neq \beta$, each orbit of G_α on $\Omega - \{\alpha\}$ has length $n+1$. We denote these $\frac{1}{2}n-1$ orbits by $\mathcal{O}_i(\alpha)$, for $1 \leq i \leq \frac{1}{2}n-1$. We will show that $\{\alpha\} \cup \mathcal{O}_i(\alpha)$ is an oval for $W(n)$ for each i and every α, when $n \geq 8$.

Proposition 1. *For every block ℓ with α not on ℓ, there is a unique involution t in T such that $\ell^t = \ell$.*

Proof: The number of blocks ℓ with $\alpha \notin \ell$ is $(n^2-1)-(n+1) = 2(\frac{1}{2}n-1)(n+1)$. Each t in T fixes $\frac{1}{2}n$ points and has $\frac{1}{2}[\frac{1}{2}n(n-1) - \frac{1}{2}n] = \frac{1}{2}n(\frac{1}{2}n-1)$ transpositions. If a block ℓ is fixed by t, and $\alpha \notin \ell$ then no point of ℓ can be fixed by t, so each t fixes $\frac{1}{2}n(\frac{1}{2}n-1)/\frac{1}{4}n$ blocks other than its pointwise-fixed block, i.e. each t fixes $n-2$ blocks that do not contain α.

Now $|G_{\alpha,\ell}| = 1$ or 2, so at most one involution in T can fix any given block. Now count the members of the set $S = \{(\ell, t) \mid t \in T, \alpha \notin \ell, \ell^t = \ell\}$ in two ways:

involutions first gives $|S| = (n+1)(n+2)$; blocks first gives $|S| = \sum_{\ell \not\ni \alpha} x_\ell$, where x_ℓ is the number of involutions in T that fix ℓ, i.e. $x_\ell = 0$ or 1. Since there are $(n-2)(n+1)$ such blocks ℓ, we must have $x_\ell = 1$ for all $\ell \not\ni \alpha$, proving the assertion.

Proposition 2. *If β and γ are two points in $\mathcal{O}_i(\alpha)$, then α, β, γ are not together on a block of $W(n)$.*

Proof: Since β and γ are together in an orbit of G_α there is an element $g \in G_\alpha$ such that $\gamma^g = \beta$. Suppose α, β, γ are together on a block. Then there exists $t \in T$ such that t fixes α, β and γ. Then $t^g \in T$ and also fixes α and β, so $t = t^g$. But since H is dihedral of order $2(n+1)$, with $n = 2^m$, $C_H(t)$, for any involution, is $\langle t \rangle$. Thus g cannot centralize t, and we have a contradiction.

Proposition 3. *For each i, $1 \leq i \leq \frac{1}{2}n - 1$, and each $\alpha \in \Omega$, $\{\alpha\} \cup \mathcal{O}_i(\alpha)$ is an oval for $W(n)$, $n \geq 8$.*

Proof: For any fixed α and i, let us write $\Delta = \{a\} \cup \mathcal{O}_i(\alpha)$. First notice that $|\Delta| = n+2$, which is the correct size for an oval for $W(n)$.

Let $\mathcal{B} \in \mathcal{O}_i(\alpha)$. There are $n+1$ blocks through β, one of which passes through α. The other n do not pass through α, and hence, by Proposition 1, there is an involution $t \in T$ for each of these n blocks that fixes the block. Since t is in T, and $\mathcal{O}_i(\alpha)$ is fixed by T, $\beta^t \in \mathcal{O}_i(\alpha)$, and hence each of these n blocks must meet $\mathcal{O}_i(\alpha)$ again. But there are exactly n other points on $\mathcal{O}_i(\alpha)$ and each is certainly on a block with β. Thus the blocks are all distinct, and so $\mathcal{O}_i(\alpha)$ is an $(n+1)$-arc. By Proposition 2, Δ is an oval.

We now show that, with the set of ovals as constucted in Proposition 3 as blocks, a new design can be defined on the point set Ω. We need another observation:

Proposition 4. *The design $W(n)$ is resolvable, and the fixed blocks of any involution form a parallel class of blocks.*

Proof: A Sylow 2-subgroup of G is elementary abelian of order n, and thus contains $n-1$ involutions. Since Sylow 2-subgroups of G intersect trivially, the involutions are partitioned in this way. Each involution t fixes $n-1$ blocks, and these form a parallel class, these being the blocks that correspond to the involutions in the Sylow 2-subgroup that contains t.

Theorem. *With notation as defined above, and $n \geq 8$, the incidence structure $D(n)$ with point set Ω and block set $\mathcal{B} = \{\{\alpha\} \cup \mathcal{O}_i(\alpha) \mid 1 \leq i \leq \frac{1}{2}n - 1, \alpha \in \Omega\}$, is a 2-$(\frac{1}{2}n(n-1), n+2, n+2)$ design.*

Proof: Clearly the structure is a 1-design, with $b = |\mathcal{B}| = \frac{1}{2}n(n-1)(\frac{1}{2}n - 1)$, $k = n+2$, and $r = (\frac{1}{2}n - 1) + (\frac{1}{2}n(n-1) - 1) = \frac{1}{2}n^2 - 2$.

Let β and γ be any two points. Then certainly there is a block $\{B\} \cup \mathcal{O}(\beta)$ with $\gamma \in \mathcal{O}(\beta)$ and a block $\{\gamma\} \cup \mathcal{O}(\gamma)$ with $\beta \in \mathcal{O}(\gamma)$ where $\mathcal{O}(\beta)$ and

$\mathcal{O}(\gamma)$ are orbits of G_β and G_γ respectively. These blocks cannot be the same: for suppose $\{\beta\} \cup \mathcal{O}(\beta) = \{\gamma\} \cup \mathcal{O}(\gamma) = \Delta$. Then G_Δ is 2-transitive on Δ, so that $(n+2)(n+1)$ divides the order of G, which is not possible.

Now β and γ will be in an orbit together for some G_α if and only if there is a $t \in T$ for which (β, γ) is a transposition. Let ℓ be the block of $W(n)$ through β and γ. Then G_ℓ is a Sylow 2-subgroup of G, elementary abelian of order n, and every involution in G_ℓ fixes a unique block pointwise. So there are $n-1$ parallel blocks corresponding to these involutions, ℓ being one of them, and ℓ is fixed by $n-2$ involutions other than the one that fixes it pointwise. Also, G_ℓ is transitive on the points of ℓ, since $|\ell| = \frac{1}{2}n$, and for any $\beta \in \ell$, $|G_{\beta,\ell}| = 2$, so $|\beta^{G}\ell| = \frac{1}{2}|G_\ell| = \frac{1}{2}n = |\ell|$. Thus every transposition (β, γ) occurs, and there are $n-2$ involutions available, and $\frac{1}{2}n-1$ transpositions, so each transposition occurs twice, with different blocks fixed pointwise. So there are two blocks, which are parallel, giving $2(\frac{1}{2}n)$ points for which β and γ are in the same orbit, i.e. giving n new blocks. Thus the total number of blocks through both β and γ is $n+2$, giving $\lambda = n+2$, and showing that $D(n)$ is a 2-design.

Corollary. *Each of the binary codes $C_2(W(n))$ and $C_2(D(n))$, for $n \geq 8$, has minimum weight equal to its block size, i.e. $\frac{1}{2}n$ for $W(n)$ and $n+2$ for $D(n)$.*

Proof: The result of Assmus [1] states that if an even order design $\mathcal{D}$ has a 2-design of ovals, then $\mathcal{D}$ has minimum weight equal to its block size. Clearly $D(n)$ is such a design for $\mathcal{D} = W(n)$, proving the first assertion. Also the blocks of $W(n)$ form a 2-design of ovals for $D(n)$, so the second assertion follows also.

3. Remarks

(1). Wertheimer [9, Theorem 4.8] and [10] constructed the 2-designs of ovals for $W(n)$ for $n \geq 8$ in the general context of designs arising from quadrics.

(2). For $n = 8$, the design $W(8)$ is the smallest Ree unital, which is well known to have ovals. In [2] the larger Ree unitals were examined for the existence of ovals, and, although none were found, a construction analogous to the one we have given here yielded arcs of size $3q+1$ for the Ree unital of block size $q+1$, where $q = 3^{2m+1}$.

(3). No 2-design of ovals seems to be known for the designs $W(\Pi, \mathcal{O})$ in general. Computations using Cayley in the desarguesian plane $\Pi = PG_2(16)$ with $\mathcal{O} = \mathcal{H}$ a Hall oval did yield the following fact: if $K = PGL_3(16)$, then evidently $K_\mathcal{H}$, which has order 36, is an automorphism group of the design $W = W(\Pi, \mathcal{H})$, and, acting on the points $\mathcal{P}$ of W, it turns out that $K_\mathcal{H}$ has two orbits of length 18, and that each of these orbits is an oval for W. In fact, many other ovals then appeared from a random look at the codewords of length 18 in the orthogonal code. It was not clear how a 2-design could be extracted from these. Comparing the designs W and $W(16)$, that they are non-isomorphic follows from the nature of their automorphism groups, but is also demonstrated by the properties of their binary codes: for although the codes $C(W)$ and $C(W(16))$ have the same dimension, viz 65 (see [8]), the hulls of the two designs are vastly different, being of dimension 1 and 33 respectively. (The hull is given by $C \cap C^{\perp}$: see [3] for a general discussion of this code for a design.)

(4). Computations (using Cayley) with $n = 8, 16$ and 32 yielded that the binary code $C(W(n))$, where $n = 2^m$, has dimension $3^m - 2^m$ for each of these cases. It was conjectured by E.F. Assmus (see [8, Chapter 3]) that this is always the dimension of this code; in [8] it is shown to be an upper bound for the dimension. It was also found computationally that the code $C(D(n))$ is the full orthogonal to the code of $W(n)$ in each of these cases, and that the dimension of the hull was given by $3^m - 2^m(1 + \frac{1}{2}m)$. It is not known if either of these properties is generally satisfied.

(5). In [8], again through computational results, ovals for some of the translation planes of order 16 were found, and the corresponding designs constructed.

References

1. E.F. Assmus, Jr, *The binary code arising from a 2-design with a nice collection of ovals*, IEEE **29** (1983), 367–369.
2. E.F. Assmus, Jr and J.D. Key, *Arcs and ovals in the hermitian and Ree unitals*, European Journal of Combinatorics **10** (1989), 297–308.
3. E.F. Assmus, Jr and J.D. Key, *Affine and projective planes*, Discrete Math., Special Coding Theory Issue **83** (1990), 161–187.
4. 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** (1960), 191–209.
5. F. Buekenhout, A. Delandtsheer and J. Doyen, *Finite linear spaces with flag-transitive groups*, J. Combin. Theory A **49** (1988), 268–293.
6. A.R. Camina, *Groups acting flag-transitively on designs*, Arch. Math. **32** (1979), 424–430.
7. W.M. Kantor, *Plane geometries associated with certain 2-transitive groups*, J. Algebra **37** (1975), 489–521.
8. K. Mackenzie, *Codes and Designs*. Ph.D. (University of Birmingham), 1989.
9. M.A. Wertheimer, *Designs in Quadrics*. Ph.D. (University of Pennsylvania), 1986.
10. M.A. Wertheimer, *Oval designs in quadrics*, Contemporary Mathematics **111** (1990), 287–297.