Reed-Muller Codes And Hadamard Designs From Ovals

L. L. Carpenter and J. D. Key*
Department of Mathematical Sciences
Clemson University
Clemson SC 29634

ABSTRACT. From any projective plane Π of even order n with an oval ($(n+2)$-arc), a Hadamard 3-design on n^2 points can be defined using a well-known construction. If Π is desarguesian with $n = 2^m$ and the oval is regular (a conic plus nucleus) then it is shown that the binary code of the Hadamard 3-design contains a copy of the first-order Reed-Muller code of length 2^{2m}.

1 Introduction

Given any projective plane Π of even order n with a hyperoval ($(n+2)$-arc) $\mathcal{O}$, a Steiner 2-design with parameters $2\text{-}(\binom{n}{2}, \frac{n}{2}, 1)$ can be defined with point set the exterior lines to $\mathcal{O}$, block set the points off $\mathcal{O}$, and incidence as in Π. This is called an oval design, and we denote it by $W(\Pi, \mathcal{O})$.

Using the block graphs of oval designs, Hadamard 3-designs on n^2 points can be obtained. If $n = 2^m$, the parameters of the Hadamard design will be that of the design of points and hyperplanes of the affine geometry $AG_{2m}(F_2)$ but is only equal to this design if $m = 2$, by a result of Maschietti [8]. The binary code of the affine-geometry design is the first-order Reed-Muller code $\mathcal{R}(1, 2m)$. We give a short proof of a result of L. Carpenter that if Π is desarguesian and $\mathcal{O}$ is regular, then the binary code of the Hadamard design contains a copy of $\mathcal{R}(1, 2m)$.

*The second author acknowledges support of NSF grant GER-9450080

2 Background and Terminology

Notation and terminology will be as in Assmus and Key [2]. An incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ with point set $\mathcal{P}$ and block set $\mathcal{B}$ is a t-(v, k, λ) design if every block is incident with precisely k points and any set of t distinct points are together incident with precisely λ blocks. It follows (see [2, Chapter 1]) that $\mathcal{D}$ is 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 $n = \lambda_1 - \lambda_2$. A Steiner design is one in which $\lambda = 1$.

An oval in a projective plane of even order n is a set of $n + 2$ points that meets each line of the plane in 0 or 2 points; ovals of $n + 2$ points are generally called hyperovals in the literature. Oval designs form a class of Steiner 2-designs first described by Bose and Shrikhande in [3]. They are defined as follows: 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 with parameters 2-$(2k^2 - k, k, 1)$ and of order $n = 2k$, is easy to show: see [2, Chapter 8].

Any oval $\mathcal{O}$ in a projective plane Π 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

$$B_X = \{Y \mid Y \text{ is an exterior point and } XY \text{ is a secant to } \mathcal{O}\} \cup \{X\}. \quad (1)$$

This 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-$(n^2, \frac{1}{2}n^2, \frac{1}{4}n^2 - 1)$ Hadamard design which, since all the Hadamard designs obtained in this way are isomorphic, we may denote by $H(\Pi, \mathcal{O})$. An alternative, more general, way to construct the Hadamard designs is described in [2, Section 7.12]; another alternative is to describe the Hadamard 2-design as the block graph of the Steiner 2-design. See also Maschietti [8] for further descriptions.

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 $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ 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 of the blocks of $\mathcal{D}$. If $F = F_p$ we write also $C_p(\mathcal{D})$ or $C(\mathcal{D})$ and its dimension is referred to as the p-**rank** of $\mathcal{D}$. It is a well-known result, stated and proved in [2, Theorem 2.4.1], that the prime p must divide the order n of a 2-design for the p-ary code of the design to be of any use or interest in any characterization.

A result of Hamada and Ohmori [6] shows that the binary code of a Hadamard 3-$(2^m, 2^{m-1}, 2^{m-2} - 1)$ design has dimension at least $m + 1$ with equality if and only if the design is that of points and hyperplanes in the

affine geometry $AG_m(F_2)$, in which case the code is the $[2m, m+1, 2^{m-1}]$ first-order Reed-Muller code, $\mathcal{R}(1,m)$. A further rigidity theorem was in mind with the following question raised by Assmus and Key [2, Section 7.11, page 284]:

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

Many infinite classes of Hadamard designs have been shown to give an affirmative answer to this question (see [2]) and until very recently no counter-example had been found to negate it. However, a construction of a Hadamard 3-(64,32,15) design using the hermitian unital on 28 points has now been shown, through a computer search by G. Royle, to have a binary code that does not contain $\mathcal{R}(1,6)$: see [1]. Recently Carpenter [5] proved that the designs $H(\Pi, \mathcal{O})$ where Π is desarguesian of even order and $\mathcal{O}$ is regular do satisfy the question. The proof uses a result of Jackson [7] and an idea of Norwood [9]. We give an alternative proof here (see Theorem 2 below) .

3 The Theorem

Theorem 2. *Let* Π *be the desarguesian projective plane of order* $q = 2^m$ *where* $m \geq 2$, *and let* $\mathcal{O}$ *be a regular oval (conic plus nucleus) in* Π. *Let* $H(\Pi, \mathcal{O})$ *be the Hadamard 3-design constructed from the block graph of the oval design* $W(\Pi, \mathcal{O})$. *Then the binary code of* $H(\Pi, \mathcal{O})$ *contains a copy of the Reed-Muller code* $\mathcal{R}(1, 2m)$.

Proof: Without loss of generality we may take the conic C with equation $x^2 = yz$; then the nucleus $N = (1,0,0)$. Consider the points $P = (0,0,1)$ and $Q = (0,1,0)$ on the conic. Then $NP = [0,1,0]$ and $NQ = [0,0,1]$ (using the square brackets to denote column vectors, i.e. lines). An arbitrary exterior point on NP will be $A = (1,0,a)$ (where $a \neq 0$) and an arbitrary point on the conic, but not P, Q or N, will be $D = (1, d, d^{-1})$ where $d \neq 0$. We arrange our incidence matrix for the Hadamard 2-design $\mathcal{D}$ defined with the blocks B_X as in Equation (1) by taking successively all the points X on the secants through the nucleus N, starting with NP, say. This will produce a symmetric incidence matrix M made up of $(q+1)^2$ submatrices of size $q-1 \times q-1$. We want to examine how the parts of the rows of M in these submatrices intersect one another. Of course, down the diagonal there will be blocks of the $q-1 \times q-1$ all-ones matrix J.

With points defined as described, we have

$$AD = [1, a^{-1}d^{-2} + d^{-1}, a^{-1}]$$

$$AQ = [1, 0, a^{-1}]$$

and

$$AD \cap NQ = (1, \frac{ad^2}{1+ad}, 0)$$

$$AD \cap C = \{D, (1, \frac{d}{1+ad}, \frac{1+ad}{d})\}$$

$$AQ \cap C = \{Q, (1, a^{-1}, a)\}$$

We will show that for $a \neq b$ and $a, b \neq 0$, the sets

$$\left\{ \frac{ad^2}{1+ad} \mid d \in F^{\times}, ad \neq 1 \right\}$$

and

$$\left\{ \frac{bd^2}{1+bd} \mid d \in F^{\times}, bd \neq 1 \right\}$$

meet in $\frac{q}{4} - 1$ points.

This is equivalent to looking at the sets

$$S_a = \{ax^2 + x \mid x \in F\}$$

for all $a \neq 0$ and showing that they intersect in $\frac{q}{4}$ points. Since each is seen to be an additive subgroup of F, $+$ of order $\frac{q}{2}$ and thus a subspace of the vector space $F = V_m(F_2)$ of dimension $m-1$, each is a hyperplane and thus they meet in an $(m-2)$-dimensional space or are equal.

So we need only show that if $a \neq b$ then $S_a \neq S_b$. Suppose on the contrary that $S_a = S_b = S$; then $ax^2 + x \in S$ and $bx^2 + x \in S$ for all $x \in F$ implies that $(a+b)x^2 \in S$ for all $x \in F$, and thus $y \in S$ for all y (since $a + b \neq 0$), and thus $S = F$, a contradiction.

Since we have $PGL_2(F_q)$ fixing the conic and acting three-transitively on the points of C, what we have proved for the two secants NP and NQ will hold for any pair of secants, due to double-transitivity.

Now what we have is that each of the submatrices is either J, the all-ones $(q-1) \times (q-1)$ matrix, or it is an incidence matrix for the design of points and hyperplanes of the projective geometry $PG_{m-1}(F_2)$. Thus each section of rows of M corresponding to a secant through N will generate over F_2 a code of dimension $m+1$ that contains the all-one vector j.

We will now show that if we take any two sections, corresponding to two secants, then the binary row span of those two sections will be a $(2m+1)$-dimensional space with minimum weight $\frac{q^2}{2} - 1$ and $q^2 - 1$ vectors of this weight that form a $(q^2 - 1, \frac{q^2}{2} - 1, \frac{q^2}{4} - 1)$ design. This design must then necessarily be the design of points and hyperplanes of $PG_{2m-1}(F_2)$ Thus take a block in one section and form its binary sum with each of the blocks in the other. This means choosing a point on one secant and allowing the

points on another to range over its secant, and then picking an arbitrary third secant. By triple-transitivity, what we find for this third secant will be true for any of the other secants. Thus take three secants through N, and due to the triple-transitivity, we can take P and Q as before, and the third point $R = (1,1,1)$ on C. Now we take a general point $A = (1,0,a)$ on NP, as before, a general point $B = (1,b,0)$ on NQ, D as before, and $E = (1,e,e^{-1})$ on C. The line NR has homogeneous coordinates $[0,1,1]$, and

$$AD \cap NR = (a^{-1}d^{-2} + d^{-1} + a^{-1}, 1, 1)$$

$$BE = [b, 1, e(b+e)]$$

and

$$BE \cap NR = (b^{-1}e^2 + e + b^{-1}, 1, 1).$$

If $b = a$ then the secants from A and B will meet on NR and so the corresponding sections of the matrix will have $\frac{q}{2} - 1$ points in common. If $a \neq b$ we need to examine how the sets

$$\{a^{-1}d^{-2} + d^{-1} + a^{-1} \mid d \in F^{\times}\}$$

and

$$\{b^{-1}e^2 + e + b^{-1} \mid e \in F^{\times}\}$$

meet. This is equivalent to looking at the sets

$$\begin{aligned} S_a^* &= \{a + x(1 + ax) \mid x \in F\} \\ &= a + S_a. \end{aligned}$$

These are simply cosets of the hyperplanes S_a and intersect in $\frac{q}{4} - 1$ points. As the point B varies over NQ we will obtain all the $q - 1$ hyperplanes from the sum of the vectors, as before. Now allow A to vary over NP and by taking all these sums, along with our original two sections, we have a $(q^2-1) \times (q^2-1)$ incidence matrix of a Hadamard 2-design with dimension $(2m+1)$. The Hadamard 2-designs extend uniquely to Hadamard 3-designs, and the code of the extended design is the extended code (see [2, Theorem 7.4.1]) so the proof is now complete. □

Remarks:

(1) Norwood [9] has shown that the 2-rank of the Hadamard 3-design is $m2^{m-1} + 1$, thus confirming a conjecture in [2, Chapter 7]. His proof involves a division of the incidence matrix into subsections that give the Reed-Muller code $\mathcal{R}(1,m)$, and the use of Jackson's construction of the incidence matrix as given in [7]. Our proof is thus a geometric version of his construction.

(2) The argument works for any two secants through the nucleus, and for each choice the construction gives the Hadamard 2-design of points and

hyperplanes of $PG_{2m}(F_2)$ with at least $2(q-1)$ blocks in common with our Hadamard 2-design from the oval. The extended design, i.e. the affine design of points and hyperplanes, will thus have $4(q-1)$ blocks in common with the 3-design $H(\Pi, \mathcal{O})$ (where, as always, $q = 2^m$). The given argument does not hold for secants through a point other than the nucleus; we have used the triple-transitivity on the points of the conic in the argument. However, only one equivalence class of Hadamard matrices is obtained, and the codes from the isomorphic 3-designs are all equivalent, so the first-order Reed-Muller code will always be present.

(3) This type of proof will not work for non-regular ovals in general, since the point D on the oval will have general form $(1, x, p(x))$ where $p(x)$ will not be a quadratic for a non-regular oval. In fact we can take the same points N, P and Q to be on the oval, and the remaining points $(1, x, p(x))$ for $x \neq 0$, and compare the sections corresponding to the rows of the incidence matrix given by the points A and B on NP, as in the first part of the proof, for the section given by the secant NQ. The sets corresponding to S_a will have the form

$$\{axp(x^{-1}) + x \mid x \in F^{\times}\},$$

which will not give hyperplanes. Thus the matrix blocked in this way will not give sections of the smaller Reed-Muller code, and in fact will be quite non-homogeneous, except that it will of course still give a Hadamard matrix. Computations with Magma [4] in the case of the Lunelli-Sce-Hall non-regular oval $\mathcal{H}$ in the desarguesian plane of order 16 verified the non-uniformity of the sections of the incidence matrix constructed in this way.

That the binary code of the design arising from an oval design in the general case contains the Reed-Muller code $\mathcal{R}(1, 2m)$ is still highly plausible, but it will not be found quite as easily as in the case of the regular oval above. In fact, even if it is inside this code, the design itself might have very few blocks in common with the design $H(\Pi, \mathcal{O})$. Computationally it will be hard to locate $\mathcal{R}(1, 2m)$ inside $C_2(H(\Pi, \mathcal{O}))$ in the general case.

Acknowledgement

The second author would like to thank the Department of Computer Science and Engineering and the Center for Communication and Information Science (CCIS) at the University of Nebraska for their hospitality during the academic year 1994–95.

References

[1] E.F. Assmus, Jr. and J.D. Key. Designs and codes: an update. *Des. Codes Cryptogr.* To appear.

[2] 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).

[3] 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.

[4] John Cannon and Catherine Playoust. *An Introduction to Magma.* School of Mathematics and Statistics, University of Sydney, 1994.

[5] L.L. Carpenter. Oval designs in desarguesian projective planes. *Des. Codes Cryptogr.*, (1996), To appear.

[6] N. Hamada and H. Ohmori. On the BIB design having the minimum p-rank. *J. Combin. Theory, Ser. A*, **18** (1975), 131–140.

[7] Wen-Ai Jackson. A characterization of Hadamard designs with $SL(2, q)$ acting transitively. *Geom. Dedicata* **46** (1993), 197–206.

[8] A. Maschietti. Hyperovals and Hadamard designs. *J. Geom.*, **44** (1992), 107–116.

[9] T. Norwood. Private communication.