

New quasi-symmetric designs constructed
using mutually orthogonal Latin squares and
Hadamard matrices

Carl Bracken, Gary McGuire

Department of Mathematics, National University of Ireland,
Maynooth, Co. Kildare, Ireland

Harold Ward

Department of Mathematics, University of Virginia,
Charlottesville, VA 22904, USA

July 7, 2006

Abstract

Using Hadamard matrices and mutually orthogonal Latin squares, we construct two new quasi-symmetric designs, with parameters $2 - (66, 30, 29)$ and $2 - (78, 36, 30)$. These are the first examples of quasi-symmetric designs with these parameters. The parameters belong to the families $2 - (2u^2 - u, u^2 - u, u^2 - u - 1)$ and $2 - (2u^2 + u, u^2, u^2 - u)$ which are related to Hadamard parameters. The designs correspond to new codes meeting the Grey-Rankin bound.

Keywords: binary code; Grey-Rankin bound; Hadamard matrix; mutually orthogonal Latin squares; quasi-symmetric design

1 Introduction

A design is said to be *quasi-symmetric* if there are only two possible intersection sizes for any two blocks. In this note we construct two quasi-symmetric designs, one with parameters $2 - (66, 30, 29)$ and block intersection sizes 12 and 15, and the other with parameters $2 - (78, 36, 30)$ and block intersection sizes 15 and 18. These are the first examples of quasi-symmetric designs with these parameters (the $2 - (66, 30, 29)$ design removes the question mark for item 69 of Table 37.22 in [4]).

In fact we will prove more general results, but the only application that we have of our results is to construct the above two designs. This is due to the difficulty of obtaining good numbers of mutually orthogonal Latin squares (MOLS). Our results are the following.

Theorem 1 *Let u be an even positive integer. Suppose there exists a $2u \times 2u$ Hadamard matrix, and $u-2$ mutually orthogonal $2u \times 2u$ Latin squares. Then there exists a quasi-symmetric $2 - (2u^2 - u, u^2 - u, u^2 - u - 1)$ design with block intersection sizes $u(u-1)/2$ and $u(u-2)/2$.*

In the case $u = 6$, it is known that a 12×12 Hadamard matrix exists and it is also known [2] that four MOLS of size 12 exist. It then follows from Theorem 1 that the $2 - (66, 30, 29)$ design exists.

The paper [2] actually shows that there are *five* MOLS of size 12, so that the $2 - (78, 36, 30)$ design exists by our next theorem.

Theorem 2 *Let u be an even positive integer. Suppose there exists a $2u \times 2u$ Hadamard matrix, and $u-1$ mutually orthogonal $2u \times 2u$ Latin squares. Then there exists a quasi-symmetric $2 - (2u^2 + u, u^2, u^2 - u)$ design with block intersection sizes $u(u-1)/2$ and $u^2/2$.*

It might appear from the hypotheses that Theorem 1 is a special case of Theorem 2, but we do not have a direct proof of Theorem 1 as a corollary of Theorem 2.

We point out that the parameters in Theorem 1 and Theorem 2 are the derived and residual parameters (respectively) of a $(4u^2, 2u^2 - u, u^2 - u)$ Hadamard design. There are of course many designs with these parameters, but until [1], *quasi-symmetric* designs with these parameters have been constructed only in the case that u is a power of 2. There are many papers on this case; see [5] for a survey. The first examples when u is not a power of 2 are constructed in Bracken [1] – they exist whenever there exists a $u \times u$ Hadamard matrix, and thus $u \equiv 0 \pmod{4}$ necessarily. Our examples are the first with $u \equiv 2 \pmod{4}$.

Designs with our parameters correspond to codes that meet the Grey-Rankin bound, as discussed in Section 2. In fact, the proofs of our theorems will construct the codes, and from that we deduce the existence of the designs.

2 Preliminaries on Codes

We recall that an (n, M, d) code over an alphabet A is a set of M members of A^n with the property that any two members of the set differ in at least d places. A binary code, for which A is the two-element field, is *self-complementary* if the binary complement of any codeword is also a codeword. We denote the binary complement of a vector x by \bar{x} . The *Grey-Rankin bound* states that

$$M \leq \frac{8d(n-d)}{n - (n-2d)^2}$$

for any (n, M, d) binary self-complementary code, provided the right-hand side is positive.

We will use the second part of the following theorem from McGuire [3].

Theorem 3 *Suppose n and d satisfy $n - \sqrt{n} < 2d < n$. Then:*

1. *If n is odd, there exists a self-complementary code meeting the Grey-Rankin bound if and only if there exists a Hadamard matrix of size $n + 1$.*
2. *If n is even, there exists a self-complementary code meeting the Grey-Rankin bound if and only if there exists a quasi-symmetric $2 - (n, d, \lambda)$ design with block intersection sizes $d/2$ and $(3d - n)/2$, where $\lambda = d(d - 1)/(n - (n - 2d)^2)$.*

Therefore, by Theorem 3, to prove Theorem 1 it will suffice to prove the existence of a binary self-complementary $(2u^2 - u, 8u^2, u^2 - u)$ code. Similarly, to prove Theorem 2 it will suffice to prove the existence of a binary self-complementary $(2u^2 + u, 8u^2, u^2)$ code.

3 Preliminaries on Latin Squares

A *Latin square* of size n is an $n \times n$ array with the property that each of n chosen symbols occurs exactly once in each row and column. We will take the n symbols to be the numbers $0, 1, 2, \dots, n - 1$, and we will also use these numbers to index the rows and columns. For a Latin square L , the entry in row i and column j will be denoted L_{ij} . Two Latin squares $L^{(1)}$ and $L^{(2)}$ of size n are said to be *orthogonal* if the n^2 ordered pairs $(L_{ij}^{(1)}, L_{ij}^{(2)})$ are distinct. The Latin squares $L^{(1)}, L^{(2)}, \dots, L^{(r)}$ are said to be *mutually orthogonal* if each two of them are orthogonal; they then form a set of *mutually orthogonal Latin squares (MOLS)*.

The existence of r MOLS of size n is equivalent to the existence of an $(r + 2, n^2, r + 1)$ code over the alphabet of n symbols. The codewords are the vectors of the form $(i, j, L_{ij}^{(1)}, L_{ij}^{(2)}, \dots, L_{ij}^{(r)})$ for each value of i and j .

4 The Construction

4.1 Proof of Theorem 1

We now begin the proof of Theorem 1. As we said, it will suffice to prove the existence of a binary self-complementary $(2u^2 - u, 8u^2, u^2 - u)$ code.

Let H be a $2u \times 2u$ normalized Hadamard matrix, one with the entries in the first row and the first column all $+1$'s. Let M be the $2u \times (2u - 1)$ matrix obtained from H by deleting the left column, and changing $+1$ to 0 and -1 to 1 throughout. We index the rows of M with the numbers $0, 1, \dots, 2u - 1$, so that row 0 consists of all zeros. Note that any two rows of M differ in exactly u places.

Now suppose we have $u - 2$ MOLS of size $2u$. Let D be the $(u, 4u^2, u - 1)$ code over the alphabet $\{0, 1, \dots, 2u - 1\}$, arising from these MOLS, as at the end of Section 3. Next, in each codeword in D we replace the symbol i by the entire row i of M . We will denote this replacement by ϕ , i.e., if r_i denotes the i -th row of M then

$$\phi : \{0, 1, \dots, 2u - 1\} \longrightarrow \{r_0, r_1, \dots, r_{2u-1}\}$$

is defined by $\phi(i) = r_i$. Extend ϕ to vectors componentwise. This replacement yields a binary code $\phi(D)$ of length $u(2u - 1)$ with $4u^2$ codewords. Add the binary complements of these codewords, and call the resulting code C .

Theorem 4 *Let C be the code constructed above. Then C is a binary $(2u^2 - u, 8u^2, u^2 - u)$ self-complementary code.*

Proof: It remains to prove that any two codewords in C have Hamming distance at least $u^2 - u$. In the code D of length u , any two codewords differ in at least $u - 1$ places. Also, any two rows of M differ in exactly u places. It follows that any two elements of $\phi(D)$ differ in at least $(u - 1)u$ places. (In fact, they differ in either $(u - 1)u$ or $u \cdot u = u^2$ places.) The same argument will

apply to two complements of elements of $\phi(D)$, since for Hamming distances $d(x, y) = d(\bar{x}, \bar{y})$. Finally, if $x, y \in \phi(D)$ we note that $d(\bar{x}, y) + d(x, y) = (2u^2 - u)$, so $d(\bar{x}, y)$ will take the two values $(2u^2 - u) - (u - 1)u = u^2$ and $(2u^2 - u) - u^2 = u(u - 1)$. This completes the proof.

4.2 Proof of Theorem 2

The proof of Theorem 2. is similar to that of Theorem 1, and we continue the same notation. Once again, we prove the existence of a binary self-complementary $(2u^2 + u, 8u^2, u^2)$ code, and we use the same matrix M .

Starting with $u - 1$ MOOLS of size $2u$, let D be the $(u + 1, 4u^2, u)$ code over the alphabet $\{0, 1, \dots, 2u - 1\}$ arising from these MOOLS. We will again denote by ϕ the replacement of the symbol i in a codeword of D by row i of M . The resulting binary code $\phi(D)$, of length $(u + 1)(2u - 1) = 2u^2 + u - 1$, has $4u^2$ codewords. Add a 0 to the end of each of the codewords of $\phi(D)$ to obtain a code D' of length $(u + 1)(2u - 1) + 1 = 2u^2 + u$ also with $4u^2$ codewords. Then augment D' by the binary complements of the codewords, and call the resulting code C .

Theorem 5 *Let C be the code constructed above. Then C is a binary $(2u^2 + u, 8u^2, u^2)$ self-complementary code.*

Proof: This time we need to show that any two codewords in C have Hamming distance at least u^2 . Any two codewords differ in at least u places in the code D of length $u + 1$. Moreover, any two rows of M differ in exactly u places. It follows that any two elements of D' differ in at least u^2 places; they actually differ in either u^2 or $(u + 1)u$ places. The same holds for any two complements of elements of D' .

If $x, y \in D'$, then $d(\bar{x}, y) + d(x, y) = (2u^2 + u)$, and $d(\bar{x}, y)$ will take the two values $(2u^2 + u) - u^2 = u(u + 1)$ and $(2u^2 + u) - u(u + 1) = u^2$. Thus the theorem is proved.

Remarks

1. The blocks of the quasi-symmetric designs are obtained by taking the codewords of the appropriate weight in the code.
2. The construction applied with $u - 3$ or u MOLS of size $2u$ (the numbers below and above those we have used) does not yield a code with only two distances.

References

- [1] C. Bracken, Designs, codes, spin models and the Walsh transform, Ph.D. Thesis, National University of Ireland, Maynooth (2004).
- [2] A. L. Dulmage, D. Johnson, N. S. Mendelsohn, Orthomorphisms of groups and orthogonal Latin squares, *Canad. J. Math.*, Vol.13 (1960)pp. 356–372.
- [3] G. McGuire, Quasi-symmetric designs and codes meeting the Grey-Rankin bound, *J. Combin. Theory Ser. A*, Vol. 78, No. 2 (1997)pp. 280–291.
- [4] M. S. Shrikhande, Quasi-Symmetric Designs, *The CRC Handbook of Combinatorial Designs*, C. J. Colbourn and J. H. Dinitz, Eds., CRC Press, Boca Raton (1996)pp. 430–434.
- [5] V. D. Tonchev, Codes, *The CRC Handbook of Combinatorial Designs*, C. J. Colbourn and J. H. Dinitz, Eds., CRC Press, Boca Raton (1996)pp. 517–543.