AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **41** (2008), Pages 139–145

A series of Siamese twin designs intersecting in a BIBD and a PBD

Dean Crnković

Department of Mathematics
Faculty of Philosophy, University of Rijeka
Omladinska 14, 51000 Rijeka
Croatia
deanc@mapef.ffri.hr

Abstract

Let p and $2p-1$ be prime powers and $p \equiv 3 \pmod 4$. We describe a construction of a series of Siamese twin designs with Menon parameters $(4p^2, 2p^2-p, p^2-p)$ intersecting in a derived design with parameters $(2p^2-p, p^2-p, p^2-p-1)$, and a pairwise balanced design PBD$(2p^2-p, \{p^2, p^2-p\}, p^2-p-1)$. When p and $2p-1$ are primes, the derived design and the pairwise balanced design are cyclic. Further, these two Menon designs with parameters $(4p^2, 2p^2-p, p^2-p)$ lead to amicable regular Hadamard matrices of order $4p^2$.

1 Introduction

Let K be a subset of positive integers. A pairwise balanced design PBD(v, K, λ) is a finite incidence structure $(\mathcal{P}, \mathcal{B}, I)$, where $\mathcal{P}$ and $\mathcal{B}$ are disjoint sets and $I \subseteq \mathcal{P} \times \mathcal{B}$, with the following properties:

1. $|\mathcal{P}| = v$;

2. if an element of $\mathcal{B}$ is incident with k elements of $\mathcal{P}$, then $k \in K$;

3. every pair of distinct elements of $\mathcal{P}$ is incident with exactly λ elements of $\mathcal{B}$.

The elements of the set $\mathcal{P}$ are called points and the elements of the set $\mathcal{B}$ are called blocks. A mandatory representation design MRD(v, K, λ) is a PBD(v, K, λ) in which for each $k \in K$ there is a block incident with exactly k points.

A 2-(v, k, λ) design is a finite incidence structure $(\mathcal{P}, \mathcal{B}, I)$, where $\mathcal{P}$ and $\mathcal{B}$ are disjoint sets and $I \subseteq \mathcal{P} \times \mathcal{B}$, with the following properties:

1. $|\mathcal{P}| = v$;

2. every element of $\mathcal{B}$ is incident with exactly k elements of $\mathcal{P}$;

3. every pair of distinct elements of $\mathcal{P}$ is incident with exactly λ elements of $\mathcal{B}$.

A 2-(v,k,λ) design is a PBD(v,K,λ) with $K = \{k\}$. 2-designs are often called balanced incomplete block designs (BIBDs), or just block designs. If $|\mathcal{P}| = |\mathcal{B}| = v$ and $2 \le k \le v-2$, then a 2-(v,k,λ) design is called a symmetric design.

Let $\mathcal{D}$ be a symmetric (v,k,λ) design and let x be a block of $\mathcal{D}$. Remove x and all points that do not belong to x from other blocks. The result is a 2-$(k,\lambda,\lambda-1)$ design, a derived design of $\mathcal{D}$ with respect to the block x.

A 2-(v,k,λ) design, or a pairwise balanced design PBD(v,K,λ), with an automorphism group G is called cyclic if G contains a cycle of length v.

A Hadamard matrix of order m is an $(m \times m)$ matrix $H = (h_{i,j})$, $h_{i,j} \in \{-1,1\}$, satisfying $HH^T = H^TH = mI_m$, where I_m is an $(m \times m)$ identity matrix. A Hadamard matrix is regular if the row and column sums are constant. It is well known that the existence of a symmetric $(4u^2, 2u^2-u, u^2-u)$ design is equivalent to the existence of a regular Hadamard matrix of order $4u^2$ (see [7, Theorem 1.4, pp. 280]). Such symmetric designs are called Menon designs.

A $\{0,\pm1\}$-matrix S is called a Siamese twin design sharing the entries of I, if $S = I+K-L$, where I,K,L are non-zero $\{0,1\}$-matrices and both $I+K$ and $I+L$ are incidence matrices of symmetric designs with the same parameters. If $I+K$ and $I+L$ are incidence matrices of Menon designs, then S is called a Siamese twin Menon design.

In this article we describe a construction of a series of Siamese twin Menon designs sharing the entries of a BIBD and a PBD, using a modification of the construction introduced in [2], and further developed in [3] and [4]. To make this article self-contained, in the next section we repeat some facts about developments of Paley difference sets and Paley partial difference sets stated in [2], [3] and [4].

2 Nonzero squares in finite fields

Let p be a prime power, $p \equiv 3 \pmod 4$ and F_p be a field with p elements. Then a $(p \times p)$ matrix $D = (d_{ij})$, such that

$$d_{ij} = \begin{cases} 1, & \text{if } (i-j) \text{ is a nonzero square in } F_p, \\ 0, & \text{otherwise.} \end{cases}$$

is an incidence matrix of a symmetric $(p, \frac{p-1}{2}, \frac{p-3}{4})$ design. Such a symmetric design is called a Paley design (see [5]). Let $\overline{D}$ be an incidence matrix of a complementary symmetric design with parameters $(p, \frac{p+1}{2}, \frac{p+1}{4})$. The proof of the following lemma can be found in [3].

Lemma 1 *Let p be a prime power, $p \equiv 3 \pmod 4$. Then the matrices D and $\overline{D}$ defined as above have the following properties:*

$$D \cdot \overline{D}^T = (\overline{D} - I_p)(D + I_p)^T = \frac{p+1}{4} J_p - \frac{p+1}{4} I_p,$$

$$[\ D \mid \overline{D} - I_p\ ] \cdot [\ \overline{D} - I_p \mid D\ ]^T = \frac{p-1}{2} J_p - \frac{p-1}{2} I_p,$$

$$[\ D \mid D\ ] \cdot [\ D + I_p \mid \overline{D} - I_p\ ]^T = \frac{p-1}{2} J_p,$$

$$[\ \overline{D} \mid D\ ] \cdot [\ \overline{D} - I_p \mid \overline{D} - I_p\ ]^T = \frac{p-1}{2} J_p,$$

where J_p is the all-one matrix of dimension $(p \times p)$.

Let $\Sigma(p)$ denote the group of all permutations of F_p given by

$$x \mapsto a\sigma(x) + b,$$

where a is a nonzero square in F_p, b is any element of F_p, and σ is an automorphism of the field F_p. $\Sigma(p)$ is an automorphism group of symmetric designs with incidence matrices D, $D + I_p$, $\overline{D}$ and $\overline{D} - I_p$ (see [5, pp. 9]). If p is a prime, $\Sigma(p)$ is isomorphic to a semidirect product $Z_p : Z_{\frac{p-1}{2}}$.

Let q be a prime power, $q \equiv 1 \pmod 4$, and $C = (c_{ij})$ be a $(q \times q)$ matrix defined as follows:

$$c_{ij} = \begin{cases} 1, & \text{if } (i-j) \text{ is a nonzero square in } F_q, \\ 0, & \text{otherwise.} \end{cases}$$

C is a symmetric matrix, since -1 is a square in F_q. There are as many nonzero squares as nonsquares in F_q, so each row of C has $\frac{q-1}{2}$ elements equal 1 and $\frac{q+1}{2}$ zeros. The set of nonzero squares in F_q is a partial difference set, called a Paley partial difference set (see [1, 10.15 Example, pp. 231]). For the proof of the properties of the matrix C listed in the following lemma we refere the reader to [3].

Lemma 2 *Let q be a prime power, $q \equiv 1 \pmod 4$, and let the matrices C and $\overline{C}$ be defined as above. Then the following properties hold:*

$$C \cdot (C + I_q)^T = \overline{C} \cdot (\overline{C} - I_q)^T = \frac{q-1}{4} J_q + \frac{q-1}{4} I_q,$$

$$C \cdot (\overline{C} - I_q)^T = \frac{q-1}{4} J_q - \frac{q-1}{4} I_q,$$

$$(C + I_q) \cdot \overline{C}^T = \frac{q+3}{4} J_q - \frac{q-1}{4} I_q,$$

$$[\ C \mid C + I_q\ ] \cdot [\ C \mid C + I_q\ ]^T = \frac{q-1}{2} J_q + \frac{q+1}{2} I_q,$$

$$[\ \overline{C} \mid \overline{C} - I_q\ ] \cdot [\ \overline{C} \mid \overline{C} - I_q\ ]^T = \frac{q-1}{2} J_q + \frac{q+1}{2} I_q,$$

$$[\ C \mid C + I_q\ ] \cdot [\ \overline{C} \mid \overline{C} - I_q\ ]^T = \frac{q+1}{2} J_q - \frac{q+1}{2} I_q.$$

$\Sigma(q)$ acts as an automorphism group of incidence structures with incidence matrices C, $C + I_q$, $\overline{C}$ and $\overline{C} - I_q$. If q is a prime, $\Sigma(p)$ is isomorphic to $Z_q : Z_{\frac{q-1}{2}}$.

3 Construction of Menon Designs

For $v \in N$ we denote by j_v the all-one vector of dimension v, by 0_v the zero-vector of dimension v, and by $0_{m\times n}$ the zero-matrix of dimension $(m \times n)$.

Let p and $q = 2p-1$ be prime powers and $p \equiv 3 \pmod 4$. Further, let D, $\overline{D}$, C, and $\overline{C}$ be defined as above. Define $(4p^2 \times 4p^2)$ matrices M_1 and M_2 in the following way:

$$M_1 = \left[\begin{array}{c|c|c|c} 0 & j_{p\cdot q}^T & 0_q^T & 0_{p\cdot q}^T \\ \hline j_{p\cdot q} & \begin{array}{c} D\otimes(C+I_q) \\ + \\ (\overline{D}-I_p)\otimes\overline{C} \end{array} & j_p \otimes C & \begin{array}{c} D\otimes C \\ + \\ \overline{D}\otimes(\overline{C}-I_q) \end{array} \\ \hline 0_q & j_p^T\otimes(\overline{C}-I_q) & 0_{q\times q} & j_p^T\otimes\overline{C} \\ \hline 0_{p\cdot q} & \begin{array}{c} (D+I_p)\otimes C \\ + \\ (\overline{D}-I_p)\otimes(\overline{C}-I_q) \end{array} & j_p\otimes(C+I_q) & \begin{array}{c} (\overline{D}-I_p)\otimes(C+I_q) \\ + \\ D\otimes\overline{C} \end{array} \end{array}\right]$$

$$M_2 = \left[\begin{array}{c|c|c|c} 0 & j_{p\cdot q}^T & 0_q^T & 0_{p\cdot q}^T \\ \hline 0_{p\cdot q} & \begin{array}{c} D\otimes(C+I_q) \\ + \\ (\overline{D}-I_p)\otimes\overline{C} \end{array} & j_p \otimes \overline{C} & \begin{array}{c} D\otimes C \\ + \\ \overline{D}\otimes(\overline{C}-I_q) \end{array} \\ \hline 0_q & j_p^T\otimes(\overline{C}-I_q) & 0_{q\times q} & j_p^T\otimes\overline{C} \\ \hline j_{p\cdot q} & \begin{array}{c} (D+I_p)\otimes C \\ + \\ (\overline{D}-I_p)\otimes(\overline{C}-I_q) \end{array} & j_p\otimes(\overline{C}-I_q) & \begin{array}{c} (\overline{D}-I_p)\otimes(C+I_q) \\ + \\ D\otimes\overline{C} \end{array} \end{array}\right]$$

Let us show that M_1 and M_2 are incidence matrices of Menon designs with parameters $(4p^2, 2p^2-p, p^2-p)$. It is easy to see that $M_1 J_{4p^2} = M_2 J_{4p^2} = (2p^2-p)J_{4p^2}$. We have to prove that $M_1 M_1^T = M_2 M_2^T = (p^2-p)J_{4p^2} + p^2 I_{4p^2}$. Using properties of the matrices D, $\overline{D}$, C and $\overline{C}$ listed in Lemma 1 and Lemma 2, one computes that the product of block matrices M_1 and M_1^T, as well as the product $M_2 M_2^T$, equals:

$$\left[\begin{array}{c|c|c|c} 2p^2-p & (p^2-p)j_{pq}^T & (p^2-p)j_q^T & (p^2-p)j_{pq}^T \\ \hline (p^2-p)j_{pq} & \begin{array}{c} (p^2-p)J_{pq} \\ + \\ p^2 I_{pq} \end{array} & (p^2-p)J_{pq\times q} & (p^2-p)J_{pq\times pq} \\ \hline (p^2-p)j_q & (p^2-p)J_{q\times pq} & \begin{array}{c} (p^2-p)J_q \\ + \\ p^2 I_q \end{array} & (p^2-p)J_{q\times pq} \\ \hline (p^2-p)j_{pq} & (p^2-p)J_{pq\times pq} & (p^2-p)J_{pq\times q} & \begin{array}{c} (p^2-p)J_{pq} \\ + \\ p^2 I_{pq} \end{array} \end{array}\right]$$

where $J_{m\times n}$ is the all-one matrix of dimension $m \times n$. Thus,

$$M_1 M_1^T = M_2 M_2^T = (p^2 - p)J_{4p^2} + p^2 I_{4p^2}$$

which means that M_1 and M_2 are incidence matrices of symmetric designs with parameters $(4p^2, 2p^2 - p, p^2 - p)$. The incidence matrices M_1 and M_2 lead us to conclusion that the group $\Sigma(p) \times \Sigma(2p-1)$ acts as an automorphism group of the Menon designs, semistandardly with one fixed point (and block), one orbit of length $2p-1$, and two orbits of length $2p^2-p$. If p and $2p-1$ are primes, then $\Sigma(p)\times\Sigma(2p-1) \cong (Z_p : Z_{\frac{p-1}{2}}) \times (Z_{2p-1} : Z_{p-1})$, and the derived designs of the Menon designs with respect to the first block, i.e., the fixed block for an automorphism group $(Z_p : Z_{\frac{p-1}{2}}) \times (Z_{2p-1} : Z_{p-1})$, are cyclic.

Incidence matrices M_1 and M_2 share the entries of

$$I = \left[\begin{array}{c|c|c|c} 0 & j_{p\cdot q}^T & 0_q^T & 0_{p\cdot q}^T \\ \hline 0_{p\cdot q} & \begin{array}{c} D\otimes(C+I_q) \\ + \\ (\overline{D}-I_p)\otimes\overline{C} \end{array} & 0_{p\cdot q\times q} & \begin{array}{c} D\otimes C \\ + \\ \overline{D}\otimes(\overline{C}-I_q) \end{array} \\ \hline 0_q & j_p^T\otimes(\overline{C}-I_q) & 0_{q\times q} & j_p^T\otimes\overline{C} \\ \hline 0_{p\cdot q} & \begin{array}{c} (D+I_p)\otimes C \\ + \\ (\overline{D}-I_p)\otimes(\overline{C}-I_q) \end{array} & 0_{p\cdot q\times q} & \begin{array}{c} (\overline{D}-I_p)\otimes(C+I_q) \\ + \\ D\otimes\overline{C} \end{array} \end{array}\right]$$

Thus, the following theorem holds

Theorem 1 *Let p and $q = 2p-1$ be prime powers and $p \equiv 3 \pmod 4$. Further, let the matrices D, $\overline{D}$, C, $\overline{C}$ and I be defined as above. Then the matrix*

$$S = \left[\begin{array}{c|c|c|c} 0 & j_{p\cdot q}^T & 0_q^T & 0_{p\cdot q}^T \\ \hline j_{p\cdot q} & \begin{array}{c} D\otimes(C+I_q) \\ + \\ (\overline{D}-I_p)\otimes\overline{C} \end{array} & j_p\otimes(C-\overline{C}) & \begin{array}{c} D\otimes C \\ + \\ \overline{D}\otimes(\overline{C}-I_q) \end{array} \\ \hline 0_q & j_p^T\otimes(\overline{C}-I_q) & 0_{q\times q} & j_p^T\otimes\overline{C} \\ \hline -j_{p\cdot q} & \begin{array}{c} (D+I_p)\otimes C \\ + \\ (\overline{D}-I_p)\otimes(\overline{C}-I_q) \end{array} & j_p\otimes(C+2I_q-\overline{C}) & \begin{array}{c} (\overline{D}-I_p)\otimes(C+I_q) \\ + \\ D\otimes\overline{C} \end{array} \end{array}\right]$$

is a Siamese twin design with parameters $(4p^2, 2p^2-p, p^2-p)$ sharing the entries of I.

The matrix I can be written as

$$I = \left[\begin{array}{c|c|c|c} 0 & j_{p\cdot q}^T & 0_q^T & 0_{p\cdot q}^T \\ \hline 0_{4p^2-1} & X & 0_{(4p^2-1)\times q} & Y \end{array}\right].$$

The matrix X is the incidence matrix of a 2-$(2p^2-p, p^2-p, p^2-p-1)$ design, and Y is the incidence matrix of a pairwise balanced design $\mathrm{PBD}(2p^2-p, \{p^2, p^2-p\}, p^2-p-1)$, both having an automorphism group isomorphic to $\Sigma(p) \times \Sigma(2p-1)$. Note that X is the incidence matrix of the derived design of the Menon designs with incidence matrices M_1 and M_2, with respect to the first block. The pairwise balanced design $\mathrm{PBD}(2p^2-p, \{p^2, p^2-p\}, p^2-p-1)$ with the incidence matrix Y is a mandatory representation design $\mathrm{MRD}(2p^2-p, \{p^2, p^2-p\}, p^2-p-1)$. When p and $2p-1$ are primes, the derived design and the pairwise balanced design are cyclic.

4 Amicable Hadamard Matrices

Two square matrices M and N of order n are said to be amicable if $MN^t = NM^t$. Using the amicability property, the following theorem follows directly (see [6]):

Theorem 2 *If matrices A and B are amicable Hadamard matrices of order n, then a matrix $X = A + iB$, $i^2 = -1$, is a complex orthogonal matrix, i.e. $XX^H = 2nI_n$, where $(\cdot)^H$ is the Hermitian conjugate.*

Note that every Hadamard matrix is amicable with itself, but this is a trivial case which is certainly not interesting. In this article we construct two Menon $(4p^2, 2p^2-p, p^2-p)$ designs, when p and $2p-1$ are prime powers and $p \equiv 3 \pmod 4$, leading to amicable Hadamard matrices. In all examples that we examine, these two designs were mutually non-isomorphic.

The matrices M_1 and M_2 give rise to regular Hadamard matrices. Let us denote the Hadamard matrices corresponding to M_1 and M_2 by H_1 and H_2, respectively. For matrices M_1 and M_2 products $M_1M_2^T$ and $M_2M_1^T$ both equal:

$$\left[\begin{array}{c|c|c|c} 2p^2-p & (p^2-p)j_{p\cdot q}^T & (p^2-p)j_q^T & (p^2-p)j_{p\cdot q}^T \\ \hline (p^2-p)j_{p\cdot q} & \begin{array}{c}(p^2-p+1)J_p \otimes C \\ -(p-1)J_p \otimes I_q + p^2 I_{pq} \\ +(p^2-p-1)J_p \otimes \overline{C}\end{array} & (p^2-p)J_{p\cdot q\times q} & \begin{array}{c}(p^2-p+1)J_p \otimes J_q \\ - \\ (p-1)J_p \otimes I_q\end{array} \\ \hline (p^2-p)j_q & (p^2-p)J_{q\times p\cdot q} & (p^2-p)J_q + p^2 I_q & (p^2-p)J_{q\times p\cdot q} \\ \hline (p^2-p)j_{p\cdot q} & \begin{array}{c}(p^2-p+1)J_p \otimes J_q \\ - \\ (p-1)J_p \otimes I_q\end{array} & (p^2-p)J_{p\cdot q\times q} & \begin{array}{c}(p^2-p-1)J_p \otimes C \\ -(p+1)J_p \otimes I_q + p^2 I_{pq} \\ +(p^2-p+1)J_p \otimes \overline{C}\end{array} \end{array}\right]$$

Therefore $H_1H_2^T = H_2H_1^T$, so H_1 and H_2 are amicable Hadamard matrices. That proves the following theorem:

Theorem 3 *Let p and $2p-1$ be prime powers and $p \equiv 3 \pmod 4$. The matrices H_1 and H_2 are amicable Hadamard matrices of order $4p^2$. Further, the matrix $X = H_1 + iH_2$, $i^2 = -1$, is a complex orthogonal matrix, i.e. $XX^H = 8p^2 I_{4p^2}$, where $(\cdot)^H$ is the Hermitian conjugate.*

References

[1] T. Beth, D. Jungnickel and H. Lenz, *Design Theory*, Cambridge University Press, Cambridge, England, 1999.

[2] D. Crnković, A series of regular Hadamard matrices, *Des. Codes Cryptogr.* 39, no. 2 (2006), 247–251.

[3] D. Crnković, A series of Siamese twin designs, *Discrete Math.* (2008) (in press); doi:10.1016/j.disc.2007.12.012.

[4] D. Crnković, A series of Menon designs and 1-rotational designs, *Finite Fields Appl.* 13, no. 4 (2007), 1001–1005.

[5] E. Lander, *Symmetric Designs: An Algebraic Approach*, Cambridge University Press, Cambridge, England, 1983.

[6] J. Seberry, B. J. Wysocki and T. A. Wysocki, On some applications of Hadamard matrices, *Metrika* 62, no. 2–3 (2005), 221–239.

[7] W. D. Wallis, A. P. Street and J. S. Wallis, *Combinatorics: Room Squares, Sum-Free Sets, Hadamard matrices*, Springer-Verlag, Berlin–Heidelberg–New York, 1972.

(Received 18 May 2007)