Some New Bush-Type Hadamard Matrices of Order 100 and Infinite Classes of Symmetric Designs

Dean Crnković ¹
Department of Mathematics
Faculty of Philosophy
Omladinska 14, 51000 Rijeka, Croatia

and

Dieter Held Fachbereich Mathematik Johannes Gutenberg-Universität 55099 Mainz, Germany

Abstract

There are at least 52432 symmetric (100, 45, 20) designs on which $Frob_{10} \times Z_2$ acts as an automorphism group. All these designs correspond to Bush-type Hadamard matrices of order 100, and each leads to an infinite class of twin designs with parameters

$$v = 100(81^m + 81^{m-1} + \dots + 81 + 1), \ k = 45(81)^m, \ \lambda = 20(81)^m,$$

and an infinite class of Siamese twin designs with parameters

$$v = 100(121^m + 121^{m-1} + \dots + 121 + 1), \ k = 55(121)^m, \ \lambda = 30(121)^m,$$

where m is an arbitrary positive integer. One of the constructed designs is isomorphic to that used by Z. Janko, H. Kharaghani and V. D. Tonchev [4].

¹Supported by a DAAD grant

1 Introduction and Preliminaries

A symmetric (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. $|\mathcal{P}| = |\mathcal{B}| = v$;
- 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} .

The elements of the set \mathcal{P} are called points and the elements of the set \mathcal{B} are called blocks.

Given two designs $\mathcal{D}_1 = (\mathcal{P}_1, \mathcal{B}_1, I_1)$ and $\mathcal{D}_2 = (\mathcal{P}_2, \mathcal{B}_2, I_2)$, an isomorphism from \mathcal{D}_1 onto \mathcal{D}_2 is a bijection which maps points onto points and blocks onto blocks preserving the incidence relation. An isomorphism from a symmetric design \mathcal{D} onto itself is called an automorphism of \mathcal{D} . The set of all automorphisms of the design \mathcal{D} forms a group; it is called the full automorphism group of \mathcal{D} and denoted by $Aut\mathcal{D}$.

Let $\mathcal{D} = (\mathcal{P}, \mathcal{B}, I)$ be a symmetric (v, k, λ) design and $G \leq Aut\mathcal{D}$. The group action of G produces the same number of point and block orbits (see [9, Theorem 3.3, p. 79]). We denote that number by t, the point orbits by $\mathcal{P}_1, \ldots, \mathcal{P}_t$, the block orbits by $\mathcal{B}_1, \ldots, \mathcal{B}_t$, and put $|\mathcal{P}_r| = \omega_r$ and $|\mathcal{B}_i| = \Omega_i$. We shall denote the points of the orbit \mathcal{P}_r by $r_0, \ldots, r_{\omega_r-1}$, (i.e. $\mathcal{P}_r = \{r_0, \ldots, r_{\omega_r-1}\}$). Further, we denote by γ_{ir} the number of points of \mathcal{P}_r which are incident with a representative of the block orbit \mathcal{B}_i . The numbers γ_{ir} are independent of the choice of the representative of the block orbit \mathcal{B}_i . For those numbers the following equalities hold (see [5]):

$$\sum_{r=1}^{t} \gamma_{ir} = k, \qquad (1)$$

$$\sum_{r=1}^{t} \frac{\Omega_{j}}{\omega_{r}} \gamma_{ir} \gamma_{jr} = \lambda \Omega_{j} + \delta_{ij} \cdot (k - \lambda).$$
 (2)

Definition 1 Let (\mathcal{D}) be a symmetric (v, k, λ) design and $G \leq Aut \mathcal{D}$. Further, let $\mathcal{P}_1, \ldots, \mathcal{P}_t$ be the point orbits and $\mathcal{B}_1, \ldots, \mathcal{B}_t$ the block orbits with respect to G, and let $\omega_1, \ldots, \omega_t$ and $\Omega_1, \ldots, \Omega_t$ be the respective orbit lengths. We call $(\mathcal{P}_1, \ldots, \mathcal{P}_t)$ and $(\mathcal{B}_1, \ldots, \mathcal{B}_t)$ the orbit distributions, and $(\omega_1, \ldots, \omega_t)$ and $(\Omega_1, \ldots, \Omega_t)$ the orbit size distributions for the design and the group G. A $(t \times t)$ -matrix (γ_{ir}) with entries satisfying conditions (1) and (2) is called an orbit structure for the parameters (v, k, λ) and orbit distributions $(\mathcal{P}_1, \ldots, \mathcal{P}_t)$ and $(\mathcal{B}_1, \ldots, \mathcal{B}_t)$.

The first step – when constructing designs for given parameters and orbit distributions – is to find all compatible orbit structures (γ_{ir}) . The next step, called indexing, consists in determining exactly which points from the point orbit \mathcal{P}_r are incident with a chosen representative of the block orbit \mathcal{B}_i for each number γ_{ir} . Because of the large number of possibilities, it is often necessary to involve a computer in both steps of the construction.

Definition 2 The set of those indices of points of the orbit \mathcal{P}_r which are incident with a fixed representative of the block orbit \mathcal{B}_i is called the index set for the position (i, r) of the orbit structure and the given representative.

It is well known that the existence of a symmetric design with parameters $(4u^2, 2u^2-u, u^2-u)$ is equivalent to the existence of a regular Hadamard matrix of order $4u^2$ (see [15, Theorem 1.4 p. 280]). Thus, symmetric designs with parameters (100,45,20) have been known to exist for a long time. However, this fact did not impede combinatorialists from constructing new designs with that parameter triple (see [11], [14]).

A Hadamard matrix of order m is an $(m \times m)$ -matrix $H = (h_{i,j})$, $h_{i,j} \in \{-1,1\}$, satisfying $HH^T = H^TH = mI$, where I is the unit matrix. A Bush-type Hadamard matrix of order $4n^2$ is a Hadamard matrix with the additional property of being a block matrix $H = [H_{i,j}]$ with blocks of size $2n \times 2n$, such that $H_{i,i} = J_{2n}$ and $H_{i,j}J_{2n} = J_{2n}H_{i,j} = 0$, $i \neq j$, $1 \leq i \leq 2n$, $1 \leq j \leq 2n$, where J_{2n} is the all-ones $(2n \times 2n)$ -matrix.

H. Kharaghani [8] showed that a Bush-type Hadamard matrix of order $4n^2$ with 2n-1 or 2n+1 a prime power can be used to construct infinite classes of symmetric designs. Z. Janko, H. Kharaghani and V. D. Tonchev [4] have constructed a Bush-type Hadamard matrix of order 100 using a symmetric (100, 45, 20) design admitting an automorphism group isomorphic to $Frob_{10} \times Z_{10}$ acting in 20 orbits of length 5 on points and blocks.

For a $\{0,\pm 1\}$ -matrix K let $K=K^+-K^-$, where K^+ and K^- are $\{0,1\}$ -matrices and $K=K^++K^-$ is a $\{0,1\}$ -matrix. A $\{0,\pm 1\}$ -matrix

D is called a twin design if both D^+ and D^- are incidence matrices of symmetric designs with the same parameters. A $\{0,\pm 1\}$ -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.

Definition 3 Let G be a group written multiplicatively. A balanced generalized weighing matrix $BGW(v,k,\lambda)$ over G is a $(v \times v)$ -matrix $W = (g_{ij})$ with entries from $\overline{G} = G \cup \{0\}$ such that each row of W contains exactly k nonzero entries, and for every $a,b \in \{1,\ldots,v\}$, $a \neq b$, the multiset $\{g_{ai}g_{bi}^{-1}| 1 \leq i \leq v, g_{ai} \neq 0, g_{bi} \neq 0\}$ contains exactly $\frac{1}{|G|}$ copies of each element of G.

2 Symmetric (100, 45, 20) Designs

Lemma 1 The following matrix, denoted by OS, is an orbit structure for the parameter triple (100, 45, 20) and orbit distributions resulting in an orbit size distribution $(5, \ldots, 5)$ for blocks and points:

Proof. Use equations (1) and (2). \Box

Theorem 1 Up to isomorphism there are exactly four symmetric (100, 45, 20) designs admitting an automorphism group G isomorphic to $Frob_{10} \times Z_5$ which operates in such a way that $Frob_{10}$ acts in 20 orbits of length 5 on points and blocks and induces the orbit structure OS from Lemma 1. Further, a generator of Z_5 acts as the permutation

$$(1, 3, 5, 7, 9)(2, 4, 6, 8, 10)(11, 13, 15, 17, 19)(12, 14, 16, 18, 20)$$

on the 20 point and block orbits of the group $Frob_{10}$. The full automorphism groups of these four designs are all isomorphic to $Frob_{10} \times Z_{10}$. The designs are not self-dual.

Sketch of proof. The designs have been constructed by the method described in [1] and [3]. We denote the points by $1_i, \ldots, 20_i, i = 0, 1, 2, 3, 4$ and put $G = \langle \rho, \sigma, \tau \rangle$ where the generators for G are permutations defined as follows:

$$\rho = (I_0, I_1, I_2, I_3, I_4), I = 1, 2, \dots, 20,
\sigma = (K_0)(K_1, K_4)(K_2, K_3), K = 1, 2, \dots, 20,
\tau = (1_i, 3_i, 5_i, 7_i, 9_i) (2_i, 4_i, 6_i, 8_i, 10_i) (11_i, 13_i, 15_i, 17_i, 19_i)
(12_i, 14_i, 16_i, 18_i, 20_i), i = 0, 1, 2, 3, 4.$$

To eliminate isomorphic structures during the indexing process we have used the permutation which – on each $\langle \rho \rangle$ -orbit – acts as $x \mapsto 2x \pmod{5}$, and those automorphisms of our orbit structure OS which commute with τ .

As representatives for the block orbits we chose blocks fixed by $\langle \sigma \rangle$. Therefore, the index sets – numbered from 0 to 6 – which could occur in the designs are among the following:

$$0 = \emptyset$$
, $1 = \{0\}$, $2 = \{1,4\}$, $3 = \{2,3\}$, $4 = \{0,1,4\}$, $5 = \{0,2,3\}$, $6 = \{1,2,3,4\}$.

The indexing process of our orbit structure OS led to four designs, denoted by $\mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3$ and \mathcal{D}_4 . Using a computer program by V. Krčadinac (see [7], [10]) we get that $(\mathcal{D}_1, \mathcal{D}_3)$ and $(\mathcal{D}_2, \mathcal{D}_4)$ are pairs of mutually dual designs. We write down base blocks for the designs \mathcal{D}_1 and \mathcal{D}_2 in terms of the index sets defined above:

 \mathcal{D}_1 $B_1:00244352242442161653$ $B_2:00423425424224616135$ $B_{11}:24531616420053253453$ $B_{12}:42356161240035524335$ \mathcal{D}_2 $B_1:00244352242442161653$ $B_2:00423425424224616135$ $B_{11}:35421616530042253442$

We have determined the automorphism groups of the constructed designs using GAP [2] and a program by V. D. Tonchev [13].

 $B_{12}: 53246161350024524324$

Theorem 2 There are at least 52432 pairwise nonisomorphic symmetric (100, 45, 20) designs admitting an automorphism group H isomorphic to $Frob_{10} \times Z_2$.

Sketch of proof. The designs are obtained from the orbit structure OS together with the assumed group H. We put $H = \langle \rho, \sigma, \tau \rangle$, where the generators of H are permutations defined as follows:

$$\rho = (I_0, I_1, I_2, I_3, I_4), I = 1, 2, \dots, 20,
\sigma = (K_0)(K_1, K_4)(K_2, K_3), K = 1, 2, \dots, 20,
\tau = (1_i, 2_i)(3_i, 4_i)(5_i, 6_i)(7_i, 8_i)(9_i, 10_i)(11_i, 12_i)(13_i, 14_i)(15_i, 16_i) (17_i, 18_i)
(19_i, 20_i), i = 0, 1, 2, 3, 4.$$

We have constructed 104864 designs. Among them there are 52432 designs with mutually different statistics of intersections of any three blocks. All constructed designs except the designs described in Theorem 1 have $Frob_{10} \times Z_2$ as full automorphism group.

3 Bush-Type Hadamard Matrices of Order 100 and Classes of Symmetric Designs

Replacing each zero by 1 and each one by -1 in the incidence matrix of each symmetric (100, 45, 20) design from Theorem 2 results in a Bush-type

Hadamard matrix of order 100. Some of these Hadamard matrices might be equivalent.

Let $U=circ(0,1,0,\ldots,0)$ be the circulant matrix of order 10 and $N=diag(-1,1,1,\ldots,1)$ be the diagonal matrix of order 10. Let E=UN and $G_{20}=\{E^i\otimes I_{10}|i=1,2,\ldots,20\}$, where $E^i\otimes I_{10}$ is a Kronecker product, and I_{10} is the unit matrix of order 10. Then E is a signed permutation matrix of order 10, G_{20} is a cyclic group of order 20, and $\Sigma_{g\in G_{20}}$ g=0.

The q-ary simplex code $S_d(q)$ of length $(q^d - 1)/(q - 1)$, where $d \ge 2$ and q is a prime power, is a linear code over GF(q) with a generator matrix having as columns representatives of all distinct one-dimensional subspaces of the d-dimensional vector space $GF(q)^d$. The code $S_d(q)$ is the dual of the unique linear perfect single-error-correcting code of length $(q^d - 1)/(q - 1)$ over GF(q). We use the following theorem of Jungnickel and Tonchev [6]:

Theorem 3 Any $(q^d-1)/(q-1) \times (q^d-1)/(q-1)$ matrix M with rows a set of representatives of the $(q^d-1)/(q-1)$ distinct one-dimensional subspaces of $S_d(q)$ is a balanced generalized weighing matrix with parameters

$$v = \frac{q^d - 1}{q - 1}, \quad k = q^d - 1, \quad \lambda = q^{d - 1} - q^{d - 2}$$

over the multiplicative group $GF(q)^*$.

Corollary 1 There exists a balanced generalized weighing matrix $BGW(q^m + q^{m-1} + ... + q + 1, q^m, q^m - q^{m-1})$ over the group G_{20} for each positive integer m and $q \in \{81, 121\}$.

Proof. This is a direct consequence of Theorem 3, because 81 and 121 are prime powers and 20 divides 80 and 120. □

Each Bush-type Hadamard matrix of order 100 leads to infinite classes of twin and Siamese twin designs.

Theorem 4 Let m be a positive integer, H any Bush-type Hadamard matrix of order 100, and $M = H - I_{10} \otimes J_{10}$. Further, let $W = [w_{ij}]$ be the balanced generalized weighing matrix $BGW(81^m + 81^{m-1} + \ldots + 81 + 1, 81^m, 81^m - 81^{m-1})$ from Corollary 1. Then, the matrix $D = [Mw_{ij}]$ is a twin design with parameters

(1)
$$v = 100(81^m + 81^{m-1} + \dots + 81 + 1), k = 45(81)^m, \lambda = 20(81)^m.$$

Proof. We follow the proof by H. Kharaghani ([8, Theorem 8, p. 8]). Let $P = J_{100} - I_{10} \otimes J_{10}$. For a matrix $w_{ij} = [a_{kl}]$ denote by $|w_{ij}|$ the matrix $||a_{kl}||$. The matrices

$$D^{+} = \frac{1}{2}[P|w_{ij}| + Mw_{ij}]$$
 and $D^{-} = \frac{1}{2}[P|w_{ij}| - Mw_{ij}]$

are symmetric designs with parameters (1).

To prove that D^+ is a symmetric (v, k, λ) design we have to prove that $D^+D^{+t} = \lambda J + (k-\lambda)I$.

For
$$k \neq l$$
,

$$\sum_{j=1}^{(81^m + \dots + 81 + 1)} M w_{kj} (M w_{jl})^t = \sum_{j=1}^{(81^m + \dots + 81 + 1)} M (w_{kj} w_{lj}^t) M^t = M(\frac{81^m - 81^{m-1}}{20} \sum_{g \in G_{20}} g) M^t = 0.$$

For
$$k = l$$
,

$$\sum_{j=1}^{(81^m + \dots + 81 + 1)} M w_{kj} (M w_{jk})^t = 81^m M M^t.$$

Therefore, $[Mw_{ij}][Mw_{ij}]^t = 81^m (I_{81^m + ... + 81 + 1} \otimes MM^t)$. Also, for every $i, j, k, l, (P|w_{ij}|)(Mw_{kl})^t = (Mw_{kl})(P|w_{ij}|)^t = 0$.

Thus, we have, $4D^+D^{+t} = [P|w_{ij}|][P|w_{ij}|]^t + [Mw_{ij}][Mw_{ij}]^t = [P|w_{ij}][P|w_{ij}]^t + 81^m(I_{81^m + ... + 81 + 1} \otimes MM^t).$

For
$$k \neq l$$
,

$$\sum_{j=1}^{(81^m + \dots + 81 + 1)} P|w_{kj}|(P|w_{jl}|)^t = \sum_{j=1}^{(81^m + \dots + 81 + 1)} P|w_{kj}||w_{lj}|^t P^t = \frac{81^m - 81^{m-1}}{10} P(J_{10} \otimes I_{10}) P^t = 80(81)^m J_{100}.$$

For
$$k = l$$
,

$$\sum_{j=1}^{(81^m + \dots + 81 + 1)} P|w_{kj}|(P|w_{jk}|)^t + \sum_{j=1}^{(81^m + \dots + 81 + 1)} Mw_{kj}(Mw_{jk})^t = 81^m (PP^t + MM^t) = 81^m (100I_{100} + 80J_{100}).$$

Therefore, D^+ is a symmetric design with parameters (1). In a similar way one can prove that D^- is also a symmetric design with parameters (1).

Theorem 5 Let m be a positive integer, H any Bush-type Hadamard matrix of order 100, and $M = H - I_{10} \otimes J_{10}$. Further, let $W = [w_{ij}]$ be the balanced generalized weighing matrix $BGW(121^m + 121^{m-1} + \ldots + 121 + 1, 121^m, 121^m - 121^{m-1})$ from the above corollary. Then, the matrices

$$\frac{1}{2}[((J_{10}+I_{10})\otimes J_{10})|w_{ij}|+Mw_{ij}] \quad and \quad \frac{1}{2}[((J_{10}+I_{10})\otimes J_{10})|w_{ij}|-Mw_{ij}]$$

are symmetric designs with parameters

$$v = 100(121^m + 121^{m-1} + \dots + 121 + 1), \ k = 55(121)^m, \ \lambda = 30(121)^m.$$

sharing the entries of $I = [(I_{10} \otimes J_{10})|w_{ij}|].$

Proof. Similar to the proof of Theorem 4.

References

- [1] D. Crnković, Symmetric (70,24,8) designs having $Frob_{21} \times Z_2$ as an automorphism group, Glasnik Matematički Vol. 34(54) (1999), 109–121.
- [2] GAP, Lehrstuhl D für Mathematik, RWTH Aachen.
- [3] Z. Janko, Coset Enumeration in Groups and Constructions of Symmetric Designs, Combinatorics '90 (1992), 275-277.
- [4] Z. Janko, H. Kharaghani, V. D. Tonchev, Bush-Type Hadamard Matrices and Symmetric Designs, J. Combin Designs 9: 72-78, 2001.
- [5] Z. Janko, Tran van Trung, Construction of a new symmetric block design for (78,22,6) with the help of tactical decomposition, J. of Comb. Theory, Series A 40 (1985), 451-455.
- [6] D. Jungnickel, V. Tonchev, Perfect Codes and Balanced Weighing Matrices, Finite Fields and their Applications 5 (1999), 294-300.
- [7] V. Krčadinac, Steiner 2-designs $S(k, 2k^2 2k + 1)$, MSc thesis, University of Zagreb (1999).
- [8] H. Kharaghani, On the twin designs with the Ionin-type parameters, The Electronic Journal of Combinatorics 7 (2000), #R1.
- [9] E. Lander, Symmetric Designs: An Algebraic Approach, Cambridge University Press (1983).
- [10] B.D. McKay, Nauty Users Guide (version 1.5) Technical Report TR-CS-90-02, Department of Computer Science, Australian National University, 1990.
- [11] M.-O. Pavčević, Symmetric Designs of Menon Series Admitting an Action of Frobenius Groups, Glasnik Matematički Vol. 31(51) (1996), 209-223.

- [12] V. D. Tonchev, Codes, in "The CRC Handbook of Combinatorial Design" (C. J. Colbourn and J. H. Dinitz, Eds.), CRC Press, Boca Raton, 1996.
- [13] V. D. Tonchev, MTU, private communication via Z. Janko of Universität Heidelberg.
- [14] T. Vučičić, New Symmetric Designs and Nonabelian Difference Sets with Parameters (100,45,20), J. Combin. Designs 8 (2000), 291-299.
- [15] 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).