A New Class of Orthogonal Designs

H. Kharaghani

Department of Mathematics and Computer Science
University of Lethbridge
Lethbridge, Alberta
Canada T1K 3M4

Abstract. We give, among other results, a new method to construct for each positive integer n a class of orthogonal designs $\mathrm{OD}(4^{n+1}m; 4^n m, 4^n m, 4^n m, 4^n m)$, $m = 2^a 10^b 26^c + 4^n + 1$, a, b, c, non-negative integers.

An orthogonal design of order k and type $(s_1, s_2, \ldots s_t)$, s_i positive integers, is a $k \times k$ real matrix X, with entries from $\{0, \pm x_1, \pm x_2, \ldots, \pm x_\ell\}$ (x_i indeterminates) satisfying

$$XX^t = \left(\sum_{i=1}^{\ell} s_i x_i^2 \right) I_k,$$

where X^t denotes the transpose of X and I_k is the identity matrix of order k. If the entries of X are only ± 1, X is called an Hadamard matrix. For the matrices $A = [a_{ij}]$, B, the Kronecker product of A, B, denoted $A \times B$, is defined to be the block matrix $[a_{ij} B]$.

Let $A = \{a_1, a_2, \ldots, a_n\}$ be a sequence of commuting variables of length n. The nonperiodic auto-correlation function of the sequence A is defined by

$$N_A(j) = \begin{cases} \sum_{i=1}^{n-j} a_i a_{i+j}, & j = 1, 2, \ldots, n-1 \\ 0, & j \geq n \end{cases}.$$

Two sequences $A = \{a_1, a_2, \ldots, a_n\}$, $B = \{b_1, b_2, \ldots, b_n\}$ are called Golay sequences of length n if all the entries are ± 1 and $N_A(j) + N_B(j) = 0$ for all $j \geq 1$. Golay sequences exist for orders $2^a 10^b 26^c$, a, b, c, non-negative integers. See Turyn [6] and Geramita and Seberry [2]. Four sequences $A_i = \{a_{i1}, a_{i2}, \ldots, a_{in}\}$, $i = 1, 2, 3, 4$ with entries $\pm 1, 0$, are called T-sequences of length n if for each i precisely one $a_{ij} \neq 0$ for each j and $\sum_{i=1}^4 N_{A_i}(j) = 0$ for each integer $j \geq 1$. Four circulant $(0, 1, -1)$ matrices A_1, A_2, A_3, A_4 of order t which satisfy $A_i \star A_j = 0$ for $i \neq j$ ($\star$ denotes the Hadamard product) and $\sum_{i=1}^4 A_i A_i^t = t I_t$, are called T-matrices of order t. See [2] for details.

The matrices constructed in the next lemma are essential for our construction of orthogonal designs.

Lemma 1. *For each positive integer k, there are 4^k symmetric $(1,-1)$ matrices ${}_kC_1, {}_kC_2, \ldots, {}_kC_{4^k}$ and a symmetric Hadamard matrix ${}_kH$, all of order 4^k such that:*

(i) ${}_kC_i\,{}_kC_j = 0, i \neq j$

(ii) $\sum_{i=1}^{4^k} {}_kC_i^2 = 4^{2k} I_{4^k}$

(iii) $\{{}_kC_1, {}_kC_2, \ldots, {}_kC_{4^k}, {}_kH\}$ *is a pairwise commuting set of (symmetric) matrices.*

Proof: We use induction on k.

For $k = 1$, let

$$
{}_1C_1 = \begin{bmatrix} + & + & + & + \\ + & + & + & + \\ + & + & + & + \\ + & + & + & + \end{bmatrix}, {}_1C_2 = \begin{bmatrix} + & - & + & - \\ - & + & - & + \\ + & - & + & - \\ - & + & - & + \end{bmatrix},
$$

$$
{}_1C_3 = \begin{bmatrix} + & + & - & - \\ + & + & - & - \\ - & - & + & + \\ - & - & + & + \end{bmatrix}, {}_1C_4 = \begin{bmatrix} + & - & - & + \\ - & + & + & - \\ - & + & + & - \\ + & - & - & + \end{bmatrix}, \text{ and } {}_1H = \begin{bmatrix} + & + & + & - \\ + & + & - & + \\ + & - & + & + \\ - & + & + & + \end{bmatrix},
$$

where + means 1 and – indicates -1. It is easy to see that ${}_1C_1, {}_1C_2, {}_1C_3, {}_1C_4, {}_1H$ satisfy (i), (ii), (iii).

Suppose that for the positive integer k, there are 4^k symmetric matrices ${}_kC_1, {}_kC_2, \ldots, {}_kC_{4^k}$ and an Hadamard matrix ${}_kH$ satisfying (i), (ii), (iii).

Let ${}_{k+1}C_{ij} = {}_kC_i \times {}_1C_j$, $1 \leq i \leq 4^k$, $1 \leq j \leq 4$ and ${}_{k+1}H = {}_kH \times {}_1H$. Then ${}_{k+1}C_{ij}^t = ({}_kC_i \times {}_1C_j)^t = {}_kC_i^t \times {}_1C_j^t = {}_kC_i \times {}_1C_j = {}_{k+1}C_{ij}$ for each i, j.

Furthermore,

(i)

$$
\begin{aligned}
{}_{k+1}C_{ij}\,{}_{k+1}C_{\ell m} &= ({}_kC_i \times {}_1C_j)({}_kC_\ell \times {}_1C_m) = {}_kC_i\,{}_kC_\ell \times {}_1C_j\,{}_1C_m \\
&= \begin{cases} {}_kC_i\,{}_kC_\ell \times 0 = 0, & j \neq m \\ 0 \times {}_1C_j\,{}_1C_m = 0, & i \neq \ell \text{ (by induction hypothesis),} \end{cases}
\end{aligned}
$$

(ii)

$$
\begin{aligned}
\sum_{j=1}^{4}\sum_{i=1}^{4^k} {}_{k+1}C_{ij}^2 &= \sum_{j=1}^{4}\sum_{i=1}^{4^k} ({}_kC_i \times {}_1C_j)({}_kC_i \times {}_1C_j) = \sum_{j=1}^{4}\sum_{i=1}^{4^k} {}_kC_i^2 \times {}_1C_j^2 \\
&= \left(\sum_{i=1}^{4^k} {}_kC_i^2\right) \times \left(\sum_{j=1}^{4} {}_1C_j^2\right) \\
&= \text{(by induction hypotheses) } 4^{2k} I_{4^k} \times 4^2 I_4 = 4^{2(k+1)} I_{4^{k+1}},
\end{aligned}
$$

(iii)

$$\begin{aligned} {}_{k+1}H\ {}_{k+1}C_{ij} &= ({}_kH \times {}_1H)({}_kC_i \times {}_1C_j) = {}_kH_kC_i \times {}_1H_1C_j \\ &= \text{(by induction hypothesis) } {}_kC_i\ {}_kH \times {}_1C_j\ {}_1H \\ &= ({}_kC_i \times {}_1C_j)({}_kH \times {}_1H) = {}_{k+1}C_{ij}\ {}_{k+1}H. \end{aligned}$$

By induction the construction is complete. ∎

For simplicity we shall omit the indices on the left when we apply the above lemma.

Remark. It is obvious from the construction that for any set of matrices satisfying (i), (ii), (iii) of the lemma, the rest of the construction follows.

Two sequences $A = \{A_1, A_2, \ldots, A_n\}$, $B = \{B_1, B_2, \ldots, B_n\}$ where A_i and B_is are commuting symmetric $(1, -1)$-matrices of order m, are called block Golay sequences of length n and block size m if

(i)
$$\sum_{i=1}^{n}(A_i^2 + B_i^2) = 2nmI_m$$

(ii)
$$\begin{aligned} N_A(j) + N_B(j) &= \sum_{i=1}^{n-j}(A_iA_{i+j} + B_iB_{i+j}) \\ &= 0 \text{ for every integer } j = 1, 2, \ldots, n-1 \\ &= 0 \text{ for } j \geq n. \end{aligned}$$

As an application of Lemma 1, we have the following important theorem.

Theorem 2. *For each positive integer k, there are block Golay sequences of length $4^k + 1$ and block size 4^k.*

Proof: For positive integer k, let $H, C_1, C_2, \ldots, C_{4^k}$ be the matrices constructed in Lemma 1. Let $A = \{A_1 = H, A_2 = C_1, A_3 = C_2, \ldots, A_{4^k+1} = C_{4^k}\}$, $B = \{B_1 = -H, B_2 = C_1, B_3 = C_2, \ldots, B_{4^k+1} = C_{4^k}\}$. Then

(i)
$$\sum_{i=1}^{4^k+1}(A_i^2 + B_i^2) = 2(4^k + 1)4^k I_{4^k}, \text{ by (ii) of Lemma 1,}$$

(ii)
$$N_A(j) + N_B(j) = C_jH - C_jH = 0, \text{ by (i) of Lemma 1.}$$

The remaining properties of block Golay sequences follows from Lemma 1. ∎

For convenience for the sequence $A = \{A_1, A_2, \ldots, A_n\}$ let $A = (A_1, A_2, \ldots, A_n)$ be the corresponding circulant matrix, where as usual $(A_1, A_2, \ldots, A_n)$ is the first row of a circulant matrix.

There are many ways to use Theorem 2, as it is the case for the Golay sequences. The following is the most immediate one; see also [6, lemma 7] and [7, Corollary 16].

Corollary 3. *For each positive integer k, there is an Hadamard matrix of order* $2(4^k + l)4^k$ *which is constructible from two block circulant matrices.*

Proof: Let $A = (H, C_1, C_2, \ldots, C_{4^k})$, $B = (-H, C_1, C_2, \ldots, C_{4^k})$ be the block circulant matrices corresponding to the block Golay sequences of Theorem 2. Then the matrix

$$H = \begin{bmatrix} A & B \\ -B^t & A^t \end{bmatrix}$$

is the desired Hadamard matrix. ∎

Let A be a finite sequence of commuting variables. Let O_r denote the sequence of r zeros, $A'_{nm} = \{O_n, A, O_m\}$. Then $N_A(j) = N'_{A_{nm}}(j)$ for every integer $j \geq 1$, n, m non-negative integers; see [2, p.146]. Consequently, A, B are Golay sequences iff $N'_{A_{nm}}(j) + N'_{B_{nm}}(j) = 0$ for every $j \geq 1$ and non-negative integers n, m. The same is valid for block Golay sequences with obvious modifications.

Four block circulant commuting $(0, 1, -1)$ matrices, say A_1, A_2, A_3, A_4 of order mt and block size m which satisfy $A_i \star A_j = 0$ for $i \neq j$, $\sum_{i=1}^{4} A_i A_i^t = mtI_{mt}$ are called block T-matrices of order mt and block size m. Now we are ready for the main construction.

Theorem 4. *For each positive integer k, there are block T-matrices of order* $4^k(4^k + 1 + r)$ *and block size* 4^k *where r is the length of a Golay sequence.*

Proof: Let C, D be Golay sequences of length r. For positive integer k, let A, B be the block Golay sequences constructed in Theorem 2 and H the Hadamard matrix for order 4^k constructed in Lemma 1.

Let $A_1 = \{(\frac{C+D}{2}) \times H, O_{4^k+1}\}$, $A_2 = \{(\frac{C-D}{2}) \times H, O_{4^k+1}\}$, $A_3 = \{O_r, \frac{A+B}{2}\}$, $A_4 = \{O_r, \frac{A-B}{2}\}$, where O is the zero matrix of order 4^k. Then the circulant matrices corresponding to these sequences are the desired block T-matrices. ∎

Corollary 5. *For each positive integer n, there is an* $OD(4^{n+1}m; 4^n m, 4^n m, 4^n m, 4^n m)$, $m = r + 4^n + 1$, *r the length of a Golay sequence.*

Proof: This follows from Theorem 4 and a result of Cooper-Wallis [1], noting that the latter is valid for block T-matrices. ∎

Let $A = \{1, 1\}$, $B = \{1, -1\}$ be the Golay sequences of length 2. Let H, C_1, C_2, C_3, C_4 be the matrices of Lemma 1 for $k = 1$. Then the block circulant matrices $(H,0,0,0,0,0,0)$, $(0,H,0,0,0,0,0)$, $(0,0,0,C_1,C_2,C_3,C_4)$, $(0,0,H,0,0,0,0)$ form the block T-matrices of order 28 and block size 4.

Now, the block circulant matrices

$$(aH, bH, dH, cC_1, cC_2, cC_3, cC_4)$$
$$(-bH, aH, -cH, dC_1, dC_2, dC_3, dC_4)$$
$$(-cH, -dH, bH, aC_1, aC_2, aC_3, aC_4)$$
$$(-dH, cH, aH, -bC_1, -bC_2, -bC_3, -bC_4)$$

where a, b, c, d are commuting indeterminates, can be used in the Goethals-Seidel array to obtain an $OD(7\cdot 4^2, 7.47.4, 7.4, 7.4)$.

Remarks

a) With some obvious modifications one can define block T-sequences. It then follows that Theorem 4 can be improved to provide block T-sequences of order $4^k(4^k + 1 + r)$ and block size 4^k.

b) For positive integer k, let $H, C_1, C_2, \ldots, C_{4^k}$ be the matrices of Lemma 1. Let $C = (I_{4^k}, C_1, C_2, \ldots, C_{4^k})$, $D = (-I_{4^k}, C_1, C_2, \ldots, C_{4^k})$. Let A, B be Golay sequences of length r. Then the block circulant matrices corresponding to the sequences

$$\left\{\left(\frac{A+B}{2}\right) \times H, O_{4^{k+1}}\right\},$$
$$\left\{\left(\frac{A-B}{2}\right) \times H, O_{4^{k+1}}\right\},$$
$$\left\{O_r, \frac{C+D}{2}\right\}, \left\{O_r, \frac{C-D}{2}\right\},$$

can be used to form an $OD(4^{k+1}m; 4^k(m-1)+1, 4^k(m-1)+1, 4^k(m-1)+1, 4^k(m-1)+1)$. For $r = 2$, $k = 1$, for example, an $OD(112; 25, 25, 25, 25)$ is constructed. Similar results can also be obtained by switching H and I_{4^k}. See [5] for more possibilities of this kind.

c) Corollary 5 gives a large class of Hadamard matrices of order $4^{n+1}(r + 4^n + 1)$, where r is the length of a Golay sequence and n is a non-negative integer. For $n = 1$, there is no Hadamard matrix of new order as for this case the order is $4^2(r+5) = 8(2r+10)$ and Koukouvinos and Kounias [4] already had constructed Hadamard matrices of order $4(r + r')$ where r, r' are the lengths of Golay sequences. However, for $n \geq 2$, there are Hadamard matrices of new order. For example, the smallest known t for which there is an Hadamard matrix of order $2^t(10417)$ is 8. Our method gives an Hadamard matrix of order $2^6(10417) = 2^6(26.4.10^2 + 4^2 + 1)$.

Acknowledgement

The research is supported by NSERC grant 4972.

References

1. J. Cooper and J. Wallis, *A New Construction for Hadamard Arrays*, Bull. Austral. Math. Soc. 7 (1972), 269–277.
2. A.V. Geramita and J. Seberry, "Orthogonal Designs: Quadratic Forms and Hadamard Matraces", Marcel Dekker, New York and Basel, 1979.
3. M.J.E. Golay, *Complementary Sequences*, IRE Transactions on Information Theory IT-7 (1961), 82–87.
4. Christos Koukouvinos and Stratis Kounias, *An Infinite Class of Hadamard Matrices*, J. Austral. Math. Soc. (Series A) 46 (1989), 384–394.
5. H. Kharaghani, *Construction of Orthogonal Designs*, Ars Combinatoria 24 (1987), 149–151.
6. H. Kharaghani, *Construction of Orthogonal Designs II*, Ars Combinatoria 25 (1988), 59–64.
7. H. Kharaghani and J. Seberry, *Regular Complex Hadamard Matrices*, Congressus Numerantium 75 (1990), 187–201.
8. R.J. Turyn, *Hadamard Matrices, Baumert-Hall Units, Four-symbol Sequences, Pulse Compressions and Surface Wave Encodings*, J. Combinatorial Theory, Series A, 16 (1974), 313–333.