



Constructions for orthogonal designs using signed group orthogonal designs



Ebrahim Ghaderpour

Department of Mathematics and Statistics, University of Calgary, Calgary, AB, Canada T2N 1N4

ARTICLE INFO

Article history:

Received 3 October 2015

Received in revised form 19 August 2016

Accepted 28 August 2017

Available online 19 September 2017

Keywords:

Circulant matrix

Golay pair

Hadamard matrix

Orthogonal design

Signed group orthogonal design

ABSTRACT

Craigen introduced and studied signed group Hadamard matrices extensively and eventually provided an asymptotic existence result for Hadamard matrices. Following his lead, Ghaderpour introduced signed group orthogonal designs and showed an asymptotic existence result for orthogonal designs and consequently Hadamard matrices. In this paper, we construct some interesting families of orthogonal designs using signed group orthogonal designs to show the capability of signed group orthogonal designs in generation of different types of orthogonal designs.

© 2017 Elsevier B.V. All rights reserved.

1. Preliminaries

A *Hadamard matrix* [7,16] is a square matrix with entries from $\{\pm 1\}$ whose rows are pairwise orthogonal. An *orthogonal design* (OD) [2,7,16] of order n and type (c_1, \dots, c_k) , denoted by $OD(n; c_1, \dots, c_k)$, is a square matrix X of order n with entries from $\{0, \pm x_1, \dots, \pm x_k\}$ that satisfies

$$XX^T = \left(\sum_{j=1}^k c_j x_j^2 \right) I_n,$$

where the c_j 's are positive integers, the x_j 's are commuting variables, I_n is the identity matrix of order n , and X^T is the transpose of X . An OD with no zero entry is called a *full OD*. A Hadamard matrix can be obtained by equating all variables of a full OD to 1. The maximum number of variables in an OD of order $n = 2^a b$, b odd, is $\rho(n) = 8c + 2^d$, where $a = 4c + d$, $0 \leq d < 4$. This number is called *Radon-Hurwitz number* [7, Chapter 1].

A *complex orthogonal design* (COD) [2,6,8] of order n and type (c_1, \dots, c_k) , denoted by $COD(n; c_1, \dots, c_k)$, is a square matrix X of order n with entries from $\{0, \pm x_1, \pm ix_1, \dots, \pm x_k, \pm ix_k\}$ that satisfies

$$XX^* = \left(\sum_{j=1}^k c_j x_j^2 \right) I_n,$$

where the c_j 's are positive integers, the x_j 's are commuting variables, and $*$ is the conjugate transpose.

Two matrices A and B of the same dimension are called *disjoint* [7,10,16] if the matrix computed via entrywise multiplication of A and B is a zero matrix. Pairwise disjoint matrices such that their sum has no zero entries are called *supplementary* [2,7].

E-mail address: ebrahim.ghaderpour@ucalgary.ca.

The Kronecker product [7,10] of two matrices $A = [a_{ij}]$ and B of orders $m \times n$ and $r \times s$, respectively, denoted by $A \otimes B$, is defined by

$$A \otimes B := \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & & & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{bmatrix},$$

that is a matrix of order $mr \times ns$.

The non-periodic autocorrelation function [11] of a sequence $A = (x_1, \dots, x_n)$ of commuting square complex matrices of order m , is defined by

$$N_A(j) := \begin{cases} \sum_{i=1}^{n-j} x_{i+j}x_i^* & \text{if } j = 0, 1, 2, \dots, n-1, \\ 0 & j \geq n, \end{cases}$$

where $*$ is the conjugate transpose. A set $\{A_1, A_2, \dots, A_\ell\}$ of sequences (not necessarily in the same length) is said to have zero autocorrelation if for all $j > 0$, $\sum_{k=1}^{\ell} N_{A_k}(j) = 0$. Sequences having zero autocorrelation are called complementary [7].

A pair $(A; B)$ of $\{\pm 1\}$ -complementary sequences of length n is called a Golay pair of length n . A Golay number is a positive integer n such that there exists a Golay pair of length n . Similarly, a pair $(C; D)$ of $\{\pm 1, \pm i\}$ -complementary sequences of length m is called a complex Golay pair of length m . A complex Golay number is a positive integer m such that there exists a complex Golay pair of length m [3,4,7].

A signed group S [2,3,8] is a group with a distinguished central element of order two. We denote the unit of a signed group by 1 and the distinguished central element of order two by -1 . In every signed group, the set $\{1, -1\}$ is a normal subgroup, and the order of signed group S is the number of elements in the quotient group $S/\langle -1 \rangle$. Therefore, a signed group of order n is a group of order $2n$.

For instance, the trivial signed group $S_{\mathbb{R}} = \{1, -1\}$ is a signed group of order 1, the complex signed group $S_{\mathbb{C}} = \langle i : i^2 = -1 \rangle = \{\pm 1, \pm i\}$ is a signed group of order 2, the quaternion signed group $S_{\mathbb{Q}} = \langle j, k : j^2 = k^2 = -1, jk = -kj \rangle = \{\pm 1, \pm j, \pm k, \pm jk\}$ is a signed group of order 4, and the set of all monomial $\{0, \pm 1\}$ -matrices of order n , SP_n , forms a group of order $2^n n!$ and a signed group of order $2^{n-1} n!$. The distinguished central elements of $S_{\mathbb{R}}$, $S_{\mathbb{C}}$ and $S_{\mathbb{Q}}$ are all -1 , and the distinguished central element of SP_n is $-I_n$, where I_n is the identity matrix of order n .

A signed group S' is called a signed subgroup [2,3] of a signed group S , denoted by $S' \leq S$, if S' is a subgroup of S , and the distinguished central elements of S' and S coincide. As an example, we have $S_{\mathbb{R}} \leq S_{\mathbb{C}} \leq S_{\mathbb{Q}}$.

Let S be a signed group and $T \leq SP_n$. A remrep (real monomial representation) [2,3,5] of degree n is a map $\phi : S \rightarrow T$ such that for all $a, b \in S$, $\phi(ab) = \phi(a)\phi(b)$ and $\phi(-1) = -I_n$.

If R is a ring with unit 1_R , and S is a signed group with distinguished central element -1_S , then $R[S] := \{ \sum_{i=1}^n s_i r_i : s_i \in \varrho, r_i \in R \}$ is a signed group ring [2,3], where ϱ is a set of coset representatives of S modulo $\langle -1_S \rangle$. The set ϱ is often referred to as a transversal of $\langle -1_S \rangle$ in S . For $s \in \varrho, r \in R$, we make the identification $-sr = s(-r)$. Addition is defined termwise, and multiplication is defined by linear extension. For instance, $s_1 r_1 (s_2 r_2 + s_3 r_3) = s_1 s_2 r_1 r_2 + s_1 s_3 r_1 r_3$, where $s_i \in \varrho, r_i \in R, i \in \{1, 2, 3\}$.

In this work, we choose $R = \mathbb{R}$. If $x \in \mathbb{R}[S]$, then $x = \sum_{i=1}^n s_i r_i$, where $s_i \in \varrho, r_i \in \mathbb{R}$, and we define the conjugate of x by $\bar{x} := \sum_{i=1}^n \bar{s}_i r_i = \sum_{i=1}^n s_i^{-1} r_i$. Clearly, the conjugate is an involution that is $\bar{\bar{x}} = x$ for all $x \in \mathbb{R}[S]$, and $\overline{xy} = \bar{y}\bar{x}$ for all $x, y \in \mathbb{R}[S]$. As some examples, for any $a, b \in \mathbb{R}$, we have $\overline{a + ib} = a + \bar{i}b = a + i^{-1}b = a - ib$, where $i \in S_{\mathbb{C}}$, and $\overline{ja + jkb} = j^{-1}a + (jk)^{-1}b = -ja - jkb$, where $j, k \in S_{\mathbb{Q}}$.

A circulant matrix C [2,7,10] is a square matrix whose each row vector is rotated one element to the right with respect to the previous row vector, and we denote it by $\text{circ}(a_1, a_2, \dots, a_n)$, where (a_1, a_2, \dots, a_n) is its first row. The circulant matrix C can be written as $C = a_1 I_n + \sum_{k=1}^{n-1} a_{k+1} U^k$, where $U = \text{circ}(0, 1, 0, \dots, 0)$ (see [7, Chapter 4]). Therefore, any two circulant matrices of order n with commuting entries commute. If $C = \text{circ}(a_1, a_2, \dots, a_n)$, then $C^* = \text{circ}(\bar{a}_1, \bar{a}_n, \dots, \bar{a}_2)$, where $*$ is the conjugate transpose.

Suppose that $A = (a_1, a_2, \dots, a_n)$ is a sequence whose nonzero entries are elements of a signed group S multiplied on the right by variables x_i 's ($1 \leq i \leq n$). We use $A_{\bar{R}}$ to denote a sequence whose elements are those of A , conjugated and in reverse order [4,9] that is $A_{\bar{R}} = (\bar{a}_n, \dots, \bar{a}_2, \bar{a}_1)$.

A signed group weighing matrix (SW) [3,5] of order n and weight w over a signed group S , denoted by $SW(n, w, S)$, is a $(0, S)$ -matrix (that is a matrix whose nonzero entries are in S) W such that $WW^* = wI_n$, where $*$ is the conjugate transpose. An SW over S with a zero entry ($w = n$) is called a signed group Hadamard matrix (SH) over S [2,3], denoted by $SH(n, S)$. Note that the matrix operations for SWs and SHs are in the signed group ring $\mathbb{Z}[S]$.

Two square matrices A and B are called amicable if $AB^* = BA^*$, and they are called anti-amicable if $AB^* = -BA^*$, where $*$ is the conjugate transpose [2,7,8,16]. If the entries of A and B belong to a signed group ring, then the matrix operations are in the signed group ring as mentioned above.

2. Some non-existence results for signed group orthogonal designs

A signed group orthogonal design (SOD) of order n and type (u_1, \dots, u_k) over a signed group S , denoted by $SOD(n; u_1, \dots, u_k, S)$, is a square matrix X of order n whose nonzero entries are elements of S multiplied on the right by commuting variables x_i 's ($1 \leq i \leq k$) such that

$$XX^* = \left(\sum_{i=1}^k u_i x_i^2 \right) I_n,$$

where u_1, \dots, u_k are positive integers, and $*$ is the conjugate transpose. Note that the conjugate of entry ϵx_i ($\epsilon \in S$) is $\bar{\epsilon} x_i = \epsilon^{-1} x_i$, and the matrix operations for SODs in this work are in the signed group ring $\mathbb{R}[S]$. It is shown [8,9] that if X is an SOD over a finite signed group, then $XX^* = X^*X$. We call an SOD with no zero entries a full SOD.

Remark 2.1. In the definition of SOD in [8,9], the author says that the entries of an SOD are from $\{0, \epsilon_1 x_1, \dots, \epsilon_k x_k\}$ ($\epsilon_i \in S$). What the author means by this arrangement is that each variable may appear in the SOD with various signed group elements as coefficients. In this paper, we also use the notation $SOD(n; u_1, \dots, u_k, S)$ instead of $SOD(n; u_1, \dots, u_k)$ over a signed group S .

Example 2.1. Consider the following square matrix:

$$X = \begin{bmatrix} jkx_1 & jx_2 & kx_3 & x_3 \\ jx_2 & jkx_1 & x_3 & kx_3 \\ kx_3 & x_3 & jkx_1 & jx_2 \\ x_3 & kx_3 & jx_2 & jkx_1 \end{bmatrix},$$

where x_1, x_2 , and x_3 are commuting variables and $j, k \in S_Q$. We have

$$XX^* = X\bar{X}^T = \begin{bmatrix} jkx_1 & jx_2 & kx_3 & x_3 \\ jx_2 & jkx_1 & x_3 & kx_3 \\ kx_3 & x_3 & jkx_1 & jx_2 \\ x_3 & kx_3 & jx_2 & jkx_1 \end{bmatrix} \begin{bmatrix} \bar{j}kx_1 & \bar{j}x_2 & \bar{k}x_3 & x_3 \\ \bar{j}x_2 & \bar{j}kx_1 & x_3 & \bar{k}x_3 \\ \bar{k}x_3 & x_3 & \bar{j}kx_1 & \bar{j}x_2 \\ x_3 & \bar{k}x_3 & \bar{j}x_2 & \bar{j}kx_1 \end{bmatrix}.$$

Let $\omega_{a,b}$ be the entry of the row a and column b of matrix XX^* . We have

$$\begin{aligned} \omega_{1,1} &= (jkx_1)(\bar{j}kx_1) + (jx_2)(\bar{j}x_2) + (kx_3)(\bar{k}x_3) + (x_3)(x_3) \\ &= jk\bar{j}kx_1x_1 + j\bar{j}x_2x_2 + k\bar{k}x_3x_3 + x_3x_3 \\ &= x_1^2 + x_2^2 + 2x_3^2 \end{aligned}$$

Similarly, it can be verified that $\omega_{2,2} = \omega_{3,3} = \omega_{4,4} = x_1^2 + x_2^2 + 2x_3^2$. Moreover,

$$\begin{aligned} \omega_{1,3} &= (jkx_1)(\bar{k}x_3) + (jx_2)(x_3) + (kx_3)(\bar{j}kx_1) + (x_3)(\bar{j}x_2) \\ &= jk\bar{k}x_1x_3 + jx_2x_3 + k\bar{j}kx_3x_1 + \bar{j}x_3x_2 \\ &= jx_1x_3 + jx_2x_3 - jx_1x_3 - jx_2x_3 \quad \text{commuting variables} \\ &= j(x_1x_3 - x_1x_3) + j(x_2x_3 - x_2x_3) \\ &= 0. \end{aligned}$$

It can be verified that $\omega_{a,b} = 0$ for $1 \leq a \neq b \leq 4$. Therefore, $XX^* = (x_1^2 + x_2^2 + 2x_3^2)I_4$, and so X is $SOD(4; 1, 1, 2, S_Q)$.

Remark 2.2. Equating all variables to 1 in any SOD results in an SW. Equating all variables to 1 in any full SOD results in an SH. An SOD over the trivial signed group $S_{\mathbb{R}}$ is an OD, and an SOD over the complex signed group $S_{\mathbb{C}}$ is a COD.

The following lemma is immediate from the definition of SOD.

Lemma 2.1 ([8, Chapter 6]). *If A is an SOD over a signed group S , then permutations of the rows or columns of A do not affect the orthogonality of A , and multiplication of each row of A from the left or each column of A from the right by an element in S does not affect the orthogonality of A .*

We now show some non-existence results for SODs. The following lemma is shown in [9], and for the sake of completeness, we give a proof.

Theorem 2.1. *There does not exist any full SOD of order n over any signed group, if n is odd and $n > 1$.*

Proof. Assume that there is a full SOD of order $n > 1$ over a signed group S . Equating all variables to 1 in the SOD, one obtains a $SH(n, S) = [h_{ij}]_{i,j=1}^n$. From the second part of Lemma 2.1, one may multiply each column of the $SH(n, S)$ from the right by the inverse of corresponding entry of its first row, \bar{h}_{1j} , to get an equivalent $SH(n, S)$ with the first row all 1 (see [3,4] for the definition of equivalence). By orthogonality of the rows of the $SH(n, S)$, the number of occurrences of a given element $s \in S$ in each subsequent row must be equal to the number of occurrences of $-s$. Therefore, n has to be even. \square

Lemma 2.2. *There does not exist any $SW(6, 3, S)$.*

Proof. Assume that A is $SW(6, 3, S)$. From Lemma 2.1, one may permute the rows and columns of A to obtain a matrix of the following form:

$$A_1 = \begin{bmatrix} \star & \star & \star & 0 & 0 & 0 \\ \star & & & & & \\ \star & & & & & \\ 0 & & & & & \\ 0 & & & & & \\ 0 & & & & & \end{bmatrix},$$

where the \star 's are elements in S . Using orthogonality of the first and second rows of A_1 , only one of the entries at second row and second column or at second row and third column must be zero. Similarly, since the first and second columns of A_1 are orthogonal, one of the entries at second row and second column or at third row and second column must be zero. From the first part of Lemma 2.1, since A_1 is an SW, the following matrix must be also an SW.

$$A_2 = \begin{bmatrix} \star & \star & \star & 0 & 0 & 0 \\ \star & \star & 0 & \star & 0 & 0 \\ \star & 0 & & & & \\ 0 & \star & & & & \\ 0 & 0 & & & & \\ 0 & 0 & & & & \end{bmatrix}.$$

Now, orthogonality of the first and second rows with the third row of A_2 forces A_2 to be of the following form:

$$A_2 = \begin{bmatrix} \star & \star & \star & 0 & 0 & 0 \\ \star & \star & 0 & \star & 0 & 0 \\ \star & 0 & \star & \star & 0 & 0 \\ 0 & \star & & & & \\ 0 & 0 & & & & \\ 0 & 0 & & & & \end{bmatrix},$$

which contradicts orthogonality of the fifth and sixth columns of A_2 , so there is no $SW(6, 3, S)$. \square

Theorem 2.2. *There exists no SOD $(6; 3, 3, S)$ and no SOD $(6; 2, 2, 2, S)$.*

Proof. If there is SOD $(6; 3, 3, S)$, then equating one of its variables to 0 and the other one to 1 results in $SW(6, 3, S)$ which contradicts Lemma 2.2, so there is no SOD $(6; 3, 3, S)$.

Now suppose that B is SOD $(6; 2, 2, 2, S)$. By Lemma 2.1, if one permutes the rows and columns of B , then one of the following forms is obtained:

$$\begin{bmatrix} \epsilon_{11}a & \epsilon_{12}a & \epsilon_{13}b & \epsilon_{14}b & \epsilon_{15}c & \epsilon_{16}c \\ \epsilon_{21}a & \epsilon_{22}a & \epsilon_{23}b & \epsilon_{24}b & \epsilon_{25}c & \epsilon_{26}c \\ \epsilon_{31}b & \epsilon_{32}b & \epsilon_{33}c & \epsilon_{34}c & \epsilon_{35}a & \epsilon_{36}a \\ \epsilon_{41}b & \epsilon_{42}b & \epsilon_{43}c & \epsilon_{44}c & \epsilon_{45}a & \epsilon_{46}a \\ \epsilon_{51}c & \epsilon_{52}c & \epsilon_{53}a & \epsilon_{54}a & \epsilon_{55}b & \epsilon_{56}b \\ \epsilon_{61}c & \epsilon_{62}c & \epsilon_{63}a & \epsilon_{64}a & \epsilon_{65}b & \epsilon_{66}b \end{bmatrix} \text{ or } \begin{bmatrix} \gamma_{11}a & \gamma_{12}a & \gamma_{13}b & \gamma_{14}b & \gamma_{15}c & \gamma_{16}c \\ \gamma_{21}a & \gamma_{22}a & \gamma_{23}c & \gamma_{24}c & \gamma_{25}b & \gamma_{26}b \\ \gamma_{31}b & \gamma_{32}b & \gamma_{33}a & \gamma_{34}a & \gamma_{35}c & \gamma_{36}c \\ \gamma_{41}b & \gamma_{42}b & \gamma_{43}c & \gamma_{44}c & \gamma_{45}a & \gamma_{46}a \\ \gamma_{51}c & \gamma_{52}c & \gamma_{53}a & \gamma_{54}a & \gamma_{55}b & \gamma_{56}b \\ \gamma_{61}c & \gamma_{62}c & \gamma_{63}b & \gamma_{64}b & \gamma_{65}a & \gamma_{66}a \end{bmatrix},$$

where $\epsilon_{ij}, \gamma_{ij} \in S (1 \leq i, j \leq 6)$, and a, b, c are commuting variables.

For the left matrix, consider $\epsilon_{11} = \epsilon_{12} = 1$, so as in the proof of Theorem 2.1, orthogonality of the first row with the second and third rows forces ϵ_{21} to be $-\epsilon_{22}$ and ϵ_{31} to be $-\epsilon_{32}$. Thus, the second and third rows will not be orthogonal, which is a contradiction.

For the right matrix, consider $\gamma_{21} = \gamma_{22} = 1$, so as in the proof of Theorem 2.1, orthogonality of the second row with the third and sixth rows forces γ_{31} to be $-\gamma_{32}$ and γ_{61} to be $-\gamma_{62}$. Thus, the third and sixth rows will not be orthogonal, which is a contradiction. Hence, there is no SOD $(6; 2, 2, 2, S)$. \square

From Theorems 2.1 and 2.2, there is no SOD $(1 \cdot 3; 1, 1, 1, S)$, SOD $(2 \cdot 3; 2, 2, 2, S)$ and SOD $(3 \cdot 3; 3, 3, 3, S)$. However, it is shown [8,9] that there exists SOD $(4 \cdot 3; 4, 4, 4, S)$ and more generally for any k -tuple (u_1, \dots, u_k) of positive integers,

there exists SOD $(4u; 4u_1, \dots, 4u_k, S)$, where $u = \sum_{i=1}^k u_i$. An asymptotic existence result for full ODs is obtained in [8,9] by applying Theorem 3.3 to these full SODs, which in turn improved the asymptotic existence result for Hadamard matrices obtained by Seberry [7, Chapter 7] and Craigen [3].

3. Constructions for ODs using SODs of order 2^n

In this section, we construct SODs of order 2^n with 2^n variables over some signed groups, and by using some well-known theorems, we obtain a family of full CODs which, as we shall show, implies the existence of a family of full ODs. We use the notation $u_{(k)}$ to show u repeats k times.

Theorem 3.1 ([7, Chapter 1]). *For each positive integer m , there is a set*

$$A = \{I_m, A_1, A_2, \dots, A_{\rho(m)-1}\}$$

of pairwise disjoint anti-amicable signed permutation matrices of order m , and equivalently there is $OD(m; 1_{(\rho(m))})$, where $\rho(m)$ is the Radon-Hurwitz number.

Remark 3.1. Since the set A in Theorem 3.1 is a set of pairwise anti-amicable matrices, $A_i = -A_i^T$ for $1 \leq i \leq \rho(m) - 1$, and so $A_i^2 = -I_m$ and $A_i A_j = -A_j A_i$ for $1 \leq i \neq j \leq \rho(m) - 1$.

Theorem 3.2. *There is SOD $(2^n; 1_{(2^n)}, S)$ such that S admits a remrep of degree 2^{2^n-1} , $n > 2$.*

Proof. Let $m = 2^{2^n-1}$. It is not hard to see that $\rho(m) = 2^n$, for $n > 2$. By Theorem 3.1, there is a set $A = \{A_0, A_1, A_2, \dots, A_{2^n-1}\}$ of pairwise disjoint anti-amicable signed permutation matrices of order m , where $A_0 = I_m$. Let

$$T = \langle A_1, \dots, A_{2^n-1} \rangle. \tag{1}$$

It can be seen that T is a signed subgroup of SP_m . Thus, for each $M \in T$, $\overline{M} = M^{-1} = M^T$. Now let $B = \{B_0, B_1, \dots, B_{2^n-1}\}$ be a set of supplementary matrices obtained from all possible n -fold Kronecker products of I and P , where

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ and } P = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

It is easy to see that the matrices in the set B are pairwise amicable of order 2^n . Now we show that

$$D = \sum_{i=0}^{2^n-1} A_i x_i B_i,$$

is SOD $(2^n; 1_{(2^n)}, T)$, where the x_i 's are commuting variables. Note that the $A_i x_i$ is treated as a scalar multiplied on every entry in the B_i . We have

$$\begin{aligned} DD^* &= D\overline{D}^T = \left(\sum_{i=0}^{2^n-1} A_i x_i B_i \right) \left(\sum_{i=0}^{2^n-1} \overline{A_i} x_i B_i^T \right) \\ &= \sum_{i=0}^{2^n-1} (A_i x_i B_i) (\overline{A_i} x_i B_i^T) + \sum_{i=0}^{2^n-1} \sum_{j=i+1}^{2^n-1} \left((A_i x_i B_i) (\overline{A_j} x_j B_j^T) + (A_j x_j B_j) (\overline{A_i} x_i B_i^T) \right) \\ &= \sum_{i=0}^{2^n-1} A_i \overline{A_i} x_i^2 B_i B_i^T + \sum_{i=0}^{2^n-1} \sum_{j=i+1}^{2^n-1} (A_i \overline{A_j} x_i x_j B_i B_j^T + A_j \overline{A_i} x_j x_i B_j B_i^T) \\ &= \sum_{i=0}^{2^n-1} I_m x_i^2 I_{2^n} + \sum_{i=0}^{2^n-1} \sum_{j=i+1}^{2^n-1} (A_i \overline{A_j} x_i x_j B_i B_j^T - A_i \overline{A_j} x_j x_i B_j B_i^T) \\ &= \left(\sum_{i=0}^{2^n-1} x_i^2 \right) I_{2^n}. \end{aligned}$$

Therefore, D is SOD $(2^n; 1_{(2^n)}, T)$. One may choose the identity map π from T to T which is clearly a remrep of degree m , and so D is an SOD over T admitting the remrep π of degree m . \square

Example 3.1. We show that there is SOD $(2^3; 1_{(2^3)}, S)$ such that S admits a remrep of degree 2^3 . Let

$$\begin{aligned} B_0 &= I \otimes I \otimes I, & B_4 &= I \otimes P \otimes P, \\ B_1 &= I \otimes I \otimes P, & B_5 &= P \otimes I \otimes P, \\ B_2 &= I \otimes P \otimes I, & B_6 &= P \otimes P \otimes I, \\ B_3 &= P \otimes I \otimes I, & B_7 &= P \otimes P \otimes P. \end{aligned}$$

Let S be the signed group in (1) with $n = 3$. It can be verified that $D = \sum_{i=0}^7 A_i x_i B_i$ is the desired SOD, where the x_i 's are commuting variables. Note that S admits a remrep of degree 8 that is related to the existence of full ODs of type $(1_{(8)})$. From Theorem 3.1, for $m > 8$, there cannot exist m pairwise disjoint anti-amicable signed permutation matrices of order m .

Remark 3.2. In the proof of Theorem 3.2, noting Remark 3.1, one may let

$$S = \langle s_1, \dots, s_{2^n-1} : s_\alpha^2 = -1, s_\alpha s_\beta = -s_\beta s_\alpha, 1 \leq \alpha \neq \beta \leq 2^n - 1 \rangle, \tag{2}$$

and define a map $\phi : S \rightarrow T$ by $\phi(s_\alpha) = A_\alpha$ for $1 \leq \alpha \leq 2^n - 1$ such that multiplication is preserved [1, Section 2.3]. Therefore, $D = \sum_{i=0}^{2^n-1} s_i x_i B_i$, where $s_0 = 1_S$, is also SOD $(2^n; 1_{(2^n)}, S)$ such that S admits the remrep ϕ of degree m .

Remark 3.3. Comparing the maximum number of variables in an OD with the number of variables in the SOD constructed in Theorem 3.2, one can observe that the maximum number of variables in an SOD over a signed group depends on the type of signed group. Determination of the maximum number of variables in an SOD over different signed groups is an interesting and challenging problem.

Craigen [3] showed that if there is $SH(n, S)$ such that S admits a remrep of degree m , then there is a Hadamard matrix of order mn , where m is the order of a Hadamard matrix. Following his lead, Ghaderpour [8,9] showed the following theorem.

Theorem 3.3 ([8, Theorem 6.26]). *If there is SOD $(n; u_1, \dots, u_k, S)$ such that S admits a remrep π of degree m , then there is OD $(mn; mu_1, \dots, mu_k)$, where m is the order of a Hadamard matrix.*

Using the remrep from S_C to SP_2 defined in [8,9], we have the following corollary.

Corollary 3.1. *If there exists COD $(n; u_1, \dots, u_k)$, then there exists OD $(2n; 2u_1, \dots, 2u_k)$.*

Craigen, Holzmann and Kharaghani in [4] showed that if g_1 and g_2 are complex Golay numbers and g is an even Golay number, then gg_1g_2 is a complex Golay number. Using this fact, they showed the following theorem.

Theorem 3.4. *All numbers of the form $m = 2^{a+u}3^b5^c11^d13^e$ are complex Golay numbers, where a, b, c, d, e and u are non-negative integers such that $b + c + d + e \leq a + 2u + 1$ and $u \leq c + e$.*

Following similar techniques to [12], we show the following theorem.

Theorem 3.5. *Suppose that r is a Golay number, and $k_1, k_2, \dots, k_{2^{n-3}-1}$ are complex Golay numbers, where $n > 2$. If $m = 2\sum_{j=1}^{2^{n-3}-1} k_j + r + 1$, then there is*

$$COD \left(2^q m; 2^q, 2^q r, 2^{q+1} k_1, \dots, 2^{q+1} k_{2^{n-3}-1} \right),$$

where $q = 2^{n-1} + n - 1$.

Proof. Let n be a positive integer greater than 2. Suppose that H is a Hadamard matrix of order 2^{n-2} , $(A; B)$ is a Golay pair of length r , and $(C^{(j)}; D^{(j)})$ is a complex Golay pair of length k_j ($1 \leq j \leq 2^{n-3} - 1$). Let $m = 2\sum_{j=1}^{2^{n-3}-1} k_j + r + 1$. Consider the following two symbolic arrays:

$$\begin{aligned} E &= \left(y, x_1 C^{(1)}, \dots, x_{2^{n-3}-1} C^{(2^{n-3}-1)}, zA, x_{2^{n-3}-1} C_{\mathbb{R}}^{(2^{n-3}-1)}, \dots, x_1 C_{\mathbb{R}}^{(1)} \right), \\ F &= \left(y, x_1 D^{(1)}, \dots, x_{2^{n-3}-1} D^{(2^{n-3}-1)}, zB, x_{2^{n-3}-1} D_{\mathbb{R}}^{(2^{n-3}-1)}, \dots, x_1 D_{\mathbb{R}}^{(1)} \right), \end{aligned}$$

where the x_j 's, y and z are commuting variables. Let e be the 2^{n-2} -dimensional column vector of ones. At this point, the sequences $A, B, C^{(j)}$'s and $D^{(j)}$'s are treated as scalars, so E and F can be seen as row vectors of dimension 2^{n-2} , and so eE and eF are square matrices of order 2^{n-2} whose entries are these sequences multiplied by the variables. Let \odot denote entrywise multiplication. For each j , $1 \leq j \leq 2^{n-2}$, let E_j and F_j be the circulant matrices of order m whose first rows are the expanded j th rows of $eE \odot H$ and $eF \odot H$, respectively. In other words, the rows of $eE \odot H$ and $eF \odot H$ have a similar form as the

arrays E and F in which expanding the sequences $A, B, C^{(j)}$'s and $D^{(j)}$'s results in row vectors of dimension m . It can be verified (see [12]) that

$$\sum_{j=1}^{2^{n-2}} (E_j E_j^* + F_j F_j^*) = 2^{n-1} \left(y^2 + rz^2 + 2 \sum_{j=1}^{2^{n-3}-1} k_j x_j^2 \right) I_m. \tag{3}$$

For each $j, 1 \leq j \leq 2^{n-2}$, let

$$E'_j = \frac{1}{2}(E_j + E_j^*), \quad E''_j = \frac{i}{2}(E_j - E_j^*), \quad F'_j = \frac{1}{2}(F_j + F_j^*), \quad F''_j = \frac{i}{2}(F_j - F_j^*).$$

Note that the coefficients of elements of the E'_j 's, E''_j 's, F'_j 's and F''_j 's are in $\{0, \pm 1, \pm i\}$ because of the form of the arrays E and F . Now it can be seen that the set

$$\Omega = \left\{ E'_j - E''_j, E'_j + E''_j, F'_j - F''_j, F'_j + F''_j; \quad 1 \leq j \leq 2^{n-2} \right\}$$

consists of 2^n Hermitian circulant matrices. Moreover,

$$\begin{aligned} & \sum_{j=1}^{2^{n-2}} \left((E'_j - E''_j)(E'_j - E''_j)^* + (E'_j + E''_j)(E'_j + E''_j)^* \right. \\ & \quad \left. + (F'_j - F''_j)(F'_j - F''_j)^* + (F'_j + F''_j)(F'_j + F''_j)^* \right) \\ &= 2 \sum_{j=1}^{2^{n-2}} (E_j'^2 + E_j''^2 + F_j'^2 + F_j''^2) \\ &= \frac{1}{2} \sum_{j=1}^{2^{n-2}} \left((E_j + E_j^*)^2 - (E_j - E_j^*)^2 + (F_j + F_j^*)^2 - (F_j - F_j^*)^2 \right) \\ &= 2 \sum_{j=1}^{2^{n-2}} (E_j E_j^* + F_j F_j^*) \quad \text{from (3)} \\ &= 2^n \left(y^2 + rz^2 + 2 \sum_{j=1}^{2^{n-3}-1} k_j x_j^2 \right) I_m. \end{aligned}$$

From Theorem 3.2, there is $SOD(2^n; 1_{(2^n)}, S)$ such that S admits a remrep of degree 2^{2^n-1} . By Theorem 3.3, there is $OD(2^q; 2_{(2^n)}^{2^n-1-1})$, where $q = 2^{n-1} + n - 1$. Replacing variables in this OD by the Hermitian circulant matrices in the set Ω , one obtains the desired COD. \square

Example 3.2. Using Theorem 3.5, we show that there is

$$COD(2^{11} \cdot 31; 2^{11} \cdot 1, 2^{11} \cdot 8, 2^{11} \cdot 22).$$

Let e be the 4-dimensional column vector of all ones, $(A; B)$ be a Golay pair of length 8, and $(C; D)$ be a complex Golay pair of length 11 as follows:

$$\begin{aligned} A &= (1, 1, 1, -, 1, 1, -, 1), & B &= (1, 1, 1, -, -, -, 1, -), \\ C &= (1, i, -, 1, -, i, \bar{i}, -, i, i, 1), & D &= (1, 1, \bar{i}, \bar{i}, \bar{i}, 1, 1, i, -, 1, -). \end{aligned}$$

Let $E = (y, xC, zA, xC_{\bar{R}})$, $F = (y, xD, zB, xD_{\bar{R}})$ and

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & - & 1 & - \\ 1 & 1 & - & - \\ 1 & - & - & 1 \end{bmatrix}.$$

We have

$$eE \odot H = \begin{bmatrix} y & xC & zA & xC_{\bar{R}} \\ y & -xC & zA & -xC_{\bar{R}} \\ y & xC & -zA & -xC_{\bar{R}} \\ y & -xC & -zA & xC_{\bar{R}} \end{bmatrix} \quad \text{and} \quad eF \odot H = \begin{bmatrix} y & xD & zB & xD_{\bar{R}} \\ y & -xD & zB & -xD_{\bar{R}} \\ y & xD & -zB & -xD_{\bar{R}} \\ y & -xD & -zB & xD_{\bar{R}} \end{bmatrix}.$$

Let

$$\begin{aligned} E_1 &= \text{circ}(y, xC, zA, xC_{\bar{R}}), & F_1 &= \text{circ}(y, xD, zB, xD_{\bar{R}}), \\ E_2 &= \text{circ}(y, -xC, zA, -xC_{\bar{R}}), & F_2 &= \text{circ}(y, -xD, zB, -xD_{\bar{R}}), \\ E_3 &= \text{circ}(y, xC, -zA, -xC_{\bar{R}}), & F_3 &= \text{circ}(y, xD, -zB, -xD_{\bar{R}}), \\ E_4 &= \text{circ}(y, -xC, -zA, xC_{\bar{R}}), & F_4 &= \text{circ}(y, -xD, -zB, xD_{\bar{R}}). \end{aligned}$$

Note that the first rows of the circulant matrices above have dimension 31, and we wrote them symbolically because of space limitations. From each of the circulant matrices above, one obtains two Hermitian circulant matrices. As an example, E_3 is the circulant matrix with the following first row:

$$(y, x, \bar{i}x, \underline{x}, x, \underline{x}, \bar{i}x, \bar{i}x, \underline{x}, \bar{i}x, \bar{i}x, x, \underline{z}, \underline{z}, \underline{z}, \underline{z}, \underline{z}, \underline{z}, \underline{z}, \underline{z}, \underline{z}, \underline{x}, \bar{i}x, \bar{i}x, x, \bar{i}x, \bar{i}x, x, \underline{x}, x, \bar{i}x, \underline{x}),$$

where \underline{u} means $-u$. The following rows are the first rows of the supplementary Hermitian circulant matrices $E'_3 = \frac{1}{2}(E_3 + E_3^*)$ and $E''_3 = \frac{i}{2}(E_3 - E_3^*)$, respectively:

$$(y, 0_{(11)}, \underline{z}, 0, \underline{z}, 0, 0, \underline{z}, 0, \underline{z}, 0_{(11)}),$$

$$(0, \bar{i}x, \underline{x}, \bar{i}x, \bar{i}x, \bar{i}x, x, \bar{i}x, \underline{x}, \bar{i}x, 0, \bar{i}z, 0, \bar{i}z, \bar{i}z, 0, \bar{i}z, 0, \bar{i}x, \underline{x}, \bar{i}x, x, \underline{x}, \bar{i}x, \bar{i}x, \bar{i}x, \bar{i}x, \bar{i}x, \underline{x}, \bar{i}x).$$

Therefore, $E'_3 + E''_3$ and $E'_3 - E''_3$ are the desired two Hermitian circulant matrices obtained from E_3 . Continuing this process, one obtains 16 complementary Hermitian circulant matrices of order 31. Replacing these matrices with variables in OD $(2^{11}; 2^7_{(16)})$ obtained from [Theorems 3.2](#) and [3.3](#), one finds

$$\text{COD}(2^{11} \cdot 31; 2^{11} \cdot 1, 2^{11} \cdot 8, 2^{11} \cdot 22).$$

Remark 3.4. The method of constructing the COD above and the infinite family of CODs in [Theorem 3.5](#) is interesting because it uses (complex) Golay pairs and circulant matrices. Moreover, these CODs have no zero entries. Applying [Corollary 3.1](#) to the COD above, one obtains

$$\text{OD}(2^{12} \cdot 31; 2^{12} \cdot 1, 2^{12} \cdot 8, 2^{12} \cdot 22).$$

4. Other constructions for ODs using SODs

Suppose that $m = 2^{2^{n-1}-1}$ for some $n > 2$. By [Theorem 3.1](#), there is a set $A = \{I_m, A_1, A_2, \dots, A_{2^n-1}\}$ of pairwise disjoint anti-amicable signed permutation matrices of order m . If we let $A' = A_{2^n-3}A_{2^n-2}A_{2^n-1}$ and $T' = \langle A', A_1, \dots, A_{2^n-4} \rangle$, then clearly $T' \leq T \leq SP_m$, where T is the signed group in (1). Let

$$\begin{aligned} S' &= \langle s, s_1, \dots, s_{2^n-4} : s^2 = 1, s_\alpha^2 = -1, \\ &ss_\alpha = -s_\alpha s, s_\alpha s_\beta = -s_\beta s_\alpha, 1 \leq \alpha \neq \beta \leq 2^n - 4 \rangle. \end{aligned} \tag{4}$$

It is easy to see that $S' \leq S$, where S is the signed group in (2). We define a map $\pi : S' \rightarrow T'$ by $\pi(s) = A'$ and $\pi(s_\alpha) = A_\alpha$ for $1 \leq \alpha \leq 2^n - 4$ such that multiplication is preserved.

In the following example, we show how one can construct a full SOD over S' admitting the remrep π , which leads to a full OD.

Example 4.1. In order to construct a full SOD of type $(1, 1, 1, 9, 9, 11)$, we may first construct a full SOD of type $(1_{(8)}, 8, 8, 8)$. To do so, first let $n = 4$ in signed group S' in (4) that admits a remrep of degree 2^7 , and let

$$A = \begin{bmatrix} s_1 & 1 \\ 1 & s_1 \end{bmatrix}, \quad I_s = \begin{bmatrix} s & 0 \\ 0 & s \end{bmatrix}, \quad P_s = \begin{bmatrix} 0 & s \\ s & 0 \end{bmatrix},$$

where $s, s_1 \in S', s^2 = 1, s_1^2 = -1$ and $ss_1 = -s_1s$. It can be seen that A, I_s and P_s are pairwise amicable. Also, let

$$\begin{aligned} B_1 &= I \otimes I \otimes I_s \otimes I_s \otimes I_s, & B_9 &= P \otimes I \otimes A \otimes A \otimes A, \\ B_2 &= I \otimes I \otimes I_s \otimes I_s \otimes P_s, & B_{10} &= I \otimes P \otimes A \otimes A \otimes A, \\ B_3 &= I \otimes I \otimes I_s \otimes P_s \otimes I_s, & B_{11} &= P \otimes P \otimes A \otimes A \otimes A, \\ B_4 &= I \otimes I \otimes P_s \otimes I_s \otimes I_s, \\ B_5 &= I \otimes I \otimes I_s \otimes P_s \otimes P_s, \\ B_6 &= I \otimes I \otimes P_s \otimes I_s \otimes P_s, \\ B_7 &= I \otimes I \otimes P_s \otimes P_s \otimes I_s, \\ B_8 &= I \otimes I \otimes P_s \otimes P_s \otimes P_s, \end{aligned}$$

It can be easily verified that the B_i 's are supplementary pairwise amicable matrices. Using the relationships $s = \bar{s}$, $s_1 s = \overline{s_1 s}$, $s s_\alpha s_\beta = s_\alpha s_\beta s$, $s_1 s_\alpha s_\beta = s_\alpha s_\beta s_1$ and $s_\alpha s_\beta = -s_\beta s_\alpha$ for $2 \leq \alpha \neq \beta \leq 12$, it can be verified that $\sum_{i=1}^{11} B_i s_{i+1} x_i$ is $SOD(2^5; 1_{(8)}, 8, 8, 8, S')$ such that S' admits the remrep of degree 2^7 , where x_i 's are commuting variables. Equating variables in this SOD over S' , one obtains $SOD(2^5; 1, 1, 1, 9, 9, 11, S')$ such that S' admits the remrep of degree 2^7 . From Theorem 3.3, one also obtains

$$OD(2^7 \cdot 2^5; 2^7 \cdot 1_{(3)}, 2^7 \cdot 9_{(2)}, 2^7 \cdot 11).$$

5. Discussion

Hadamard matrices, ODs and CODs have many applications in coding theory, cryptography, signal processing, wireless networking and communications [13–15]. We observed that Hadamard matrices, ODs, CODs, SWs and SHs are specific SODs. An SOD over a signed group other than $S_{\mathbb{R}}$ or $S_{\mathbb{C}}$ may also have applications in the areas mentioned above. As we showed in Section 2, there exist types and orders in which there are no SODs of those types and orders. We also constructed some interesting families of full SODs. Using some special signed groups and extensive algebra may result in constructing other interesting families of full SODs and consequently full ODs and Hadamard matrices.

Acknowledgments

Sections 2 and 3 of this paper are a part of the author's Ph.D. thesis written under the direction of Professor Hadi Kharaghani at the University of Lethbridge. The author would like to thank Professors Hadi Kharaghani and Rob Craigen for their time and great help. The author also thank the reviewers of the journal for their time and essential comments that improved significantly the presentation of the paper.

References

- [1] O. Bogopolski, Introduction to group theory, European Math. Soc. (2008) 187.
- [2] R. Craigen, Constructions for Orthogonal Matrices (Ph.D. thesis), University of Waterloo, Canada, 1991.
- [3] R. Craigen, Signed groups, sequences, and the asymptotic existence of hadamard matrices, J. Combin. Theory Ser. A 71 (1995) 241–254.
- [4] R. Craigen, W. Holzmann, H. Kharaghani, Complex golay sequences: structure and applications, Discrete Math. 252 (2002) 73–89.
- [5] R. Craigen, H. Kharaghani, Hadamard matrices from weighing matrices via signed groups, Des. Code Cryptogr. 12 (1997) 49–58.
- [6] A.V. Geramita, J.M. Geramita, Complex orthogonal designs, J. Combin. Theory Ser. A 25 (1978) 211–225.
- [7] A.V. Geramita, J. Seberry, Orthogonal designs, lecture notes in pure and applied mathematics, in: Quadratic Forms and Hadamard Matrices, vol. 45, Marcel Dekker Inc, New York, 1979.
- [8] E. Ghaderpour, Asymptotic Existence of Orthogonal Designs (Ph.D. thesis), University of Lethbridge, Canada, 2013.
- [9] E. Ghaderpour, Signed group orthogonal designs and their applications, in: Algebraic Design Theory and Hadamard Matrices, in: Springer Proc. Math. and Stat., vol. 133, 2015, pp. 107–123.
- [10] E. Ghaderpour, Some nonexistence and asymptotic existence results for weighing matrices, Int. J. Combin. 2016 (2016) 6. <http://dx.doi.org/10.1155/2016/2162849>.
- [11] W. Holzmann, H. Kharaghani, On the amicability of orthogonal designs, J. Combin. Des. 17 (2009) 240–252.
- [12] H. Kharaghani, On the asymptotic existence of complex Williamson Hadamard matrices, Australas. J. Combin. 10 (1994) 225–230.
- [13] J. Seberry, S.A. Spence, T.A. Wysocki, A construction technique for generalized complex orthogonal designs and applications to wireless communications, Linear Algebra Appl. 405 (2005) 163–176.
- [14] J. Seberry, B.J. Wysocki, T.A. Wysocki, On some applications of Hadamard matrices, Metrika 62 (2005) 221–239.
- [15] V. Tarokh, H. Jafarkhani, A.R. Calderbank, Space-time block codes from orthogonal designs, IEEE Trans. Inform. Theory 45 (1999) 1456–1467.
- [16] W.W. Wolfe, Orthogonal Designs, Amicable Orthogonal Designs, Some Algebraic and Combinatorial Techniques (Ph.D. thesis), Queen's University, Canada, 1975.