Block Golay Sequences with Applications

H. Kharaghani

University of Lethbridge

Abstract

Golay sequences have been used extensively for constructing base sequences, Yang numbers, T-sequences, Hadamard matrices, SBIBDs and Hadamard matrices with maximum possible sums.

The possibility of obtaining new Golay sequences is diminishing and only non-existence results are appearing nowadays.

We introduce block Golay sequences. It turns out that every existing result on Golay sequences could be extended to block Golay sequences. The abundance of such sequences and their applications will be presented.

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 $(1,-1)$-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.

The sequence $A = \{A_1, A_2, \ldots, A_n\}$, where A_is are $(1,-1)$-matrices of order m, is called a Block Barker sequence of length n and block size m if:

(i) $A_i A_j^t = A_j A_i^t$ for all i, j;

(ii) $\sum_{i=1}^{n} A_i A_i^t = nmI_m$;

(iii) $$N_A(j) = \begin{cases} \sum_{i=1}^{n-j} A_i A_{i+j}^t = 0 \ \text{for} & j = 1, 2, \ldots, n-1, \\ 0 & j \geq n. \end{cases}$$

Australasian Journal of Combinatorics 6(1992), pp.293-303

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

$$\begin{array}{lrcl}
\text{(i)} & A_iB_j^t & = & B_jA_i^t \text{ ; for all } i, j; \\
\text{(ii)} & \sum_{i=1}^{n} (A_iA_i^t + B_iB_i^t) & = & 2nmI_m; \\
\text{(iii)} & N_A(j) + N_B(j) & = & \sum_{i=1}^{n-j} A_iA_{i+j}^t + \sum_{i=1}^{n-j} B_iB_{i+j}^t = 0 \\
 & & & \text{for } j = 1, 2, \ldots, n-1, \\
 & & = & 0 \text{ for } j \geq n.
\end{array}$$

Lemma 1: Let $X = \{A, B\}$ be two Barker sequences of lengths n, ℓ respectively, and block size m. Then $Z = (A, B)$, $Y = (A, -B)$, is a block Golay sequence of length $n + \ell$ and block size m.

Proof:
Note that $(N_X + N_Y)(j) = 2N_A(j) + 2N_B(j) = 0$ for all $j \geq 1$. The rest is straightforward. □

Lemma 2:

(i) If there is a block Golay sequence of length n and block size m, then there is a block Golay sequence of length rn and block size m, where r is the length of a Golay sequence.

(ii) If there are block Golay sequences of lengths n, ℓ and block size m, k respectively, then there are block Golay sequences of length $n^a\ell^b$ and block size m^ak^b where a, b are non-negative integers.

Proof:

(i) Let A, B be block Golay sequences of length n and block size m and C, D Golay sequences of length r. Using an idea of Turyn, the following are the required block Golay sequences:

$$\begin{array}{c}
A \times \frac{1}{2}(C + D) \quad + \quad B \times \frac{1}{2}(C - D) \\
A \times \frac{1}{2}(C^* - D^*) \quad - \quad B \times \frac{1}{2}(C^* + D^*),
\end{array}$$

where X^* is the sequence whose elements are the reverse of those in X. The proof that the nonperiodic auto-correlation function is zero is similar to that of Turyn and the rest is straightforward.

(ii) Assume C, D is a block Golay sequence of length ℓ and block size k in the proof of part (i). □

We let $-$ stand for -1 and $+$ for 1.

Lemma 3: Let $\eta = \begin{pmatrix} + & + & + & - \\ + & + & - & + \\ + & - & + & + \\ - & + & + & + \end{pmatrix}$, $\alpha_1 = \begin{pmatrix} + & + & + & + \\ + & + & + & + \\ + & + & + & + \\ + & + & + & + \end{pmatrix}$,

$$\alpha_2 = \begin{pmatrix} + & + & - & - \\ + & + & - & - \\ - & - & + & + \\ - & - & + & + \end{pmatrix}, \alpha_3 = \begin{pmatrix} + & - & + & - \\ - & + & - & + \\ + & - & + & - \\ - & + & - & + \end{pmatrix}, \alpha_4 = \begin{pmatrix} + & - & - & + \\ - & + & + & - \\ - & + & + & - \\ + & - & - & + \end{pmatrix}.$$

Then

$$\alpha_i\alpha_j^t = \alpha_j\alpha_i^t = 0,\ i \neq j, \eta\eta^t = 4I_4\,, \sum_{i=1}^{4} \alpha_i\alpha_i^t = 16I_4 \text{ and } \eta\alpha_i^t = \alpha_i\eta^t,\ 1 \le i \le 4.$$

Proof:
Trivial. See also [2]. □

Lemma 4: For each positive integer k, there are $2^{2k-1}(1,-1)$-matrices, say, ${}_kC_1$, ${}_kC_2$, $\ldots$, ${}_kC_{2^{2k-1}}$ and an Hadamard matrix ${}_kH$, all of order 4^k, such that:

(i) $\quad {}_kC_i\, {}_kC_j^t = {}_kC_j\, {}_kC_i^t = 0,\ i \neq j;$

(ii) $\quad \sum_{i=1}^{2^{2k-1}} {}_kC_i\, {}_kC_i^t = 2^{4k-1} I_{2^{2k}};$

(iii) $\quad {}_kC_i\, {}_kH^t = {}_kH\, {}_kC_i^t,\ 1 \le i \le 2^{2k-1}.$

Proof: We use induction on k.

For $k = 1$, let

$${}_1C_1 = \begin{bmatrix} + & + & + & + \\ + & + & + & + \\ + & + & - & - \\ + & + & - & - \end{bmatrix}, \quad {}_1C_2 = \begin{bmatrix} + & - & + & - \\ - & + & - & + \\ + & - & - & + \\ - & + & + & - \end{bmatrix}, \quad {}_1H = \begin{bmatrix} + & + & + & - \\ + & + & - & + \\ - & + & + & + \\ + & - & + & + \end{bmatrix}.$$

It is easy to see that ${}_1C_1$, ${}_1C_2$, ${}_1H$ satisfy (i), (ii), (iii) above.

Suppose that for the positive integer k, there are $2^{2k-1}(1,-1)$-matrices, say, ${}_kC_1$, ${}_kC_2$, $\dots$, ${}_kC_{2^{2k-1}}$ and an Hadamard matrix ${}_kH$, all of order 4^k satisfying (i), (ii), (iii) above. Let α_i, η be the matrices of Lemma 3 and consider any enumeration ${}_{k+1}C_1$, ${}_{k+1}C_2, \dots$, ${}_{k+1}C_{2^{2k+1}}$ of the matrices ${}_kC_i \times \alpha_j$, $1 \le i \le 2^{2k-1}$, $1 \le j \le 4$.

Let ${}_{k+1}H = {}_kH \times \eta$. Then:

(i) $({}_kC_i \times \alpha_j)({}_kC^t_{i'} \times \alpha^t_{j'}) ={}_k C_i\, {}_kC^t_{i'} \times \alpha_j\alpha^t_{j'} = 0 = ({}_kC_{i'} \times \alpha_{j'})({}_kC^t_i \times \alpha^t_j), (i,j) \neq (i',j');$

(ii)

$$\begin{aligned}
\sum_{i=1}^{2^{2k+1}} {}_{k+1}C_i\, {}_{k+1}C^t_i &= \sum_{i=1}^{2^{2k-1}} \sum_{j=1}^{4} ({}_kC_i \times \alpha_j)({}_kC^t_i \times \alpha^t_j) \\
&= \sum_{i=1}^{2^{2k-1}} \sum_{j=1}^{4} ({}_kC_i\, {}_kC^t_i \times \alpha_j\alpha^t_j) \\
&= \left(\sum_{i=1}^{2^{2k-1}} {}_kC_i\, {}_kC^t_i\right) \times \left(\sum_{j=1}^{4} \alpha_j\alpha^t_j\right) \\
&= (2^{4k-1} I_{2^{2k}}) \times (4I_4) \\
&\qquad \text{by induction hypothesis and Lemma 3.} \\
&= 2^{4k+1} I_{2^{2k+2}};
\end{aligned}$$

(iii)

$$\begin{aligned}
{}_{k+1}H\, {}_{k+1}C^t_i &= ({}_kH \times \eta)({}_kC^t_{i'} \times \alpha^t_j) \\
&= {}_kH\, {}_kC^t_{i'} \times \eta\alpha^t_j \\
&= {}_kC_{i'}\, {}_kH^t \times \alpha_j\eta^t \\
&\qquad \text{by induction hypothesis and Lemma 3} \\
&= ({}_kC_{i'} \times \alpha_j)({}_kH^t \times \eta^t) =_{k+1} C_i\, {}_{k+1}H^t.
\end{aligned}$$

By induction the construction is complete. □

Lemma 5: [Kharaghani [2]] For each positive integer k, there are 4^k symmetric $(1,-1)$-matrices ${}_kC_1$, ${}_kC_2, \dots, {}_kC_{4^k}$ and a symmetric matrix ${}_kH$, all of order 4^k, such that:

(i) $\quad {}_kC_kC_j = 0, i \neq j;$

(ii) $\quad \displaystyle\sum_{i=1}^{4^k} {}_kC^2 = 4^{2k} I_{4^k};$

(iii) $\quad {}_kC_i\,{}_kH = {}_kH_kC_i, 1 \leq i \leq 4^k.$

Proof:
Start with matrices of Lemma 3 and follow the proof of Lemma 4. See [2]. □

For simplicity we shall omit the indices on the left when we apply Lemma 4 or 5.

Theorem 6:
(i) For each positive integer k, there are block Golay sequences of length $2^{2k-1}+1$ and block size 4^k.

(ii) For each positive integer k, there are block Golay sequences of length 4^k+1 and block size 4^k.

Proof:
(i) For positive integer k, let $H, C_1, C_2, \ldots, C_{2^{2k-1}}$ be the matrices constructed in Lemma 4. Let $A = \{H\}$, $B = \{C_1, C_2, \ldots, C_{2^{2k-1}}\}$. Then A, B are two block Barker sequences satisfying the condition of Lemma 1. Thus $Z = (A, B)$, $Y = (-A, B)$ is a block Golay sequence of length $2^{2k+1}+1$ and block size 4^k.

(ii) For positive integer k, let $H, C_1, C_2, \ldots, C_{4^k}$ be the matrices constructed in Lemma 5. The rest follows are in part (i). □

Table 1 is drawn from Theorem 6 and Lemma 2.

Length	Block Size
3	4
5	4
9	4^2
15	4^2
17	4^2
25	4^2
27	4^3
33	4^3
45	4^3

Table 1: Block Golay Sequence of Odd Length

Lemma 7: Let $X = \{A, B\}$, $Y = \{E, D\}$ be block Golay sequences of length n, m respectively and block size k such that $FG^t = GF^t$ for all entries G, F of A, B, E, D. Let $X_1 = (A, E)$, $X_2 = (A, -E)$, $X_3 = (B, D)$, $X_4 = (B, -D)$. Then $N_{X_1} + N_{X_2} + N_{X_3} + N_{X_4} = 0$. Consequently, if X, Y, Z, W are block circulant matrices whose first rows are entries of X_1, X_2, X_3, X_4 respectively, then $XX^t + YY^t + ZZ^t + WW^t = 4(n+m)kI_{(n+m)k}$.

Proof:
Note that $(N_{X_1} + N_{X_2} + N_{X_3} + N_{X_4})(j) = 2(N_A + N_B + N_E + N_D)(j) = 0$ for all $j \geq 1$. The rest follows from properties of block Golay sequences. □

Example 8: Let H, C_1, C_2 be matrices of Lemma 4 for $k = 1$. Let

$$\begin{aligned} A &= \{A_1 = H, A_2 = C_1, A_3 = C_2\}, \\ B &= \{B_1 = H, B_2 = C_1, B_3 = C_2\}, \\ E &= \{E_1 = H, E_2 = H\}, \\ D &= \{D_1 = H, D_2 = H\}. \end{aligned}$$

Then

$$\begin{aligned} X &= (H, C_1, C_2, H, H), \\ Y &= (H, C_1, C_2, -H, -H), \\ Z &= (-H, C_1, C_2, H, -H), \\ W &= (-H, C_1, C_2, -H, H). \end{aligned}$$

Let $A = [a_{ij}A_{ij}], B = [b_{ij}B_{ij}]$ be to block circulant matrices. Let $A_t = [a_{ji}A_{ji}], B_t = [b_{ji}B_{ji}]$ and assume that $A_{ij}B_{k\ell}^t = B_{k\ell}A_{ij}^t$ for all i, j, k, ℓ. Then $A(B_t)^t = B(A_t)^t$.

Theorem 9: The existence of block Golay sequences of lengths n, m and block size k of Lemma 7 implies the existence of an Hadamard matrix of order $4(n+m)k$.

Proof:
Let X, Y, Z, W be the matrices in Lemma 7. Let R be the back identity matrix. Then

$$H = \begin{bmatrix} X & YR & ZR & WR \\ -YR & X & -W_tR & Z_tR \\ -ZR & W_tR & X & -Y_tR \\ -WR & -Z_tR & Y_tR & X \end{bmatrix}$$

is an Hadamard matrix of order $4(n+m)k$. □

Remark

Let C, D be a Golay sequence of length r. Then $C \times H$, $D \times H$ (H is the Hadamard matrix in the proof of Theorem 6) is a block Golay sequence of length r and block size 4^k. Thus the existence of Hadamard matrices of order $4^{\alpha k+1}\left[r+(2^{2k-1}+1)^{\alpha}r'\right]$ and $4^{\alpha k+1}\left[r+(4^k+1)^{\alpha}r'\right]$ follows from Theorem 9 and Lemma 2, where r' is the length of a Golay sequence and α is a non-negative integer. As an application of Theorem 9, we have the following.

Some New Hadamard Matrices of order $2^t p$

p	t	t'
479	12	16
491	13	15
659	7	17
1499	12	18
2063	6	8

t' is given in Seberry and Yamada [3].

Let S, P be $(1,-1)$-matrices of order m. (S, P) is called an orthogonal pair of order m (see Craigen [1]) if:

(i) $SP^t = PS^t = 0;$

(ii) $SS^t + PP^t = 2mI_m.$

Let (S,P), (M,N) be two orthogonal pairs of order m, n respectively.
Let ${}_1H = \frac{1}{2}(S+P)\times M + \frac{1}{2}(S-P)\times N$, $A_1 = S\times M$, $A_2 = P\times M$, $A_3 = S\times N$, $A_4 = P \times N$.
Then ${}_1H_1H^t = mnI_{mn}$,
$A_iA_j^t = A_jA_i^t = 0,\ i \neq j,\ \sum_{i=1}^{4} A_iA_i^t = (SS^t+PP^t)\times(MM^t+NN^t) = 4mnI_{mn}$
and ${}_1HA_i^t = A_i\,{}_1H^t$, $1 \le i \le 4$.

Noting that Lemma 5 depends entirely on Lemma 3, the above observation allows us to get the following extension of Lemma 5.
The reader has noted that in Lemma 3, the property of $\eta\alpha_i^t = \alpha_i\eta^t$, $1 \le i \le 4$, follows because of block circulancy of the matrices η, α_i, $1 \le i \le 4$. The fact that the block circulancy can be replaced, as above, is quite interesting.

Theorem 10: Let (S,P), (M,N) be two orthogonal pairs of order m,n respectively. Then for each positive integer k, there are $4^k(1,-1)$-matrices, say, ${}_kC_1,\ {}_kC_2,\ldots,{}_kC_{4^k}$ and an Hadamard matrix ${}_kH$, all of order $(mn)^k$, such that:

(i) $${}_kC_i\ {}_kC_j^t = {}_kC_j\ {}_kC_i^t = 0,\quad i \neq j;$$

(ii) $$\sum_{k=1}^{4^k} {}_kC_i\ {}_kC_i^t = 4^k(mn)^k I_{(mn)^k};$$

(iii) $${}_kC_i\ {}_kH^t = {}_kH_kC_i^t,\quad 1 \leq i \leq 4^k.$$

To see that Theorem 10 is an extension of Lemma 5, let $M = S = \begin{pmatrix} + & + \\ + & + \end{pmatrix}$, $P = N = \begin{pmatrix} + & - \\ - & + \end{pmatrix}$.

Remark:
There are other ways of extending Lemma 5, besides the above method.

Starting with orthogonal pairs (S,P), (M,N), we can construct ${}_1H, A_1, A_2, A_3, A_4$ as before. Next consider $M_1 = S \times_1 H$, $N_1 = P \times_1 H$, $C_i = S \times A_i$, $C_{i+4} = P \times A_i$, $1 \leq i \leq 4$. Then (M_1, N_1) is an orthogonal pair and $C_i M_1^t = M_1 C_i^t$, $C_i N_1^t = N_1 C_i^t$, $1 \leq i \leq 8$.

Now consider, ${}_2H = \frac{1}{2}(S+P) \times M_1 + \frac{1}{2}(S-P) \times N_1$, ${}_2C_i = S \times C_i$, ${}_2C_{i+8} = P \times C_i$, $1 \leq i \leq 8$. The next steps are obvious now.

Let (S,P) be an orthogonal pair of order m. Let

$${}_1H = \begin{pmatrix} S & P \\ -P & S \end{pmatrix},\ {}_1C_1 = \begin{pmatrix} S & S \\ S & -S \end{pmatrix},\ {}_1C_2 = \begin{pmatrix} P & P \\ P & -P \end{pmatrix}.$$

Then ${}_1H_1H^t = 2mI_{2m}$, ${}_1C_i\ {}_1C_2^t ={}_1 C_2\ {}_1C_1^t = 0$, ${}_1C_1\ {}_1C_1^t +_1 C_2\ {}_1C_2^t = 4mI_{2m}$ and ${}_1H_1C_i^t ={}_1 C_i\ {}_1H^t$, $i = 1,2$. Consequently, we have the following extension of Lemma 4.

Theorem 11: Let (S,P) be an orthogonal pair of order m. Then, for each positive integer k, there are $2^{2k+1}(1,-1)$-matrices, say, ${}_kC_1,\ {}_kC_2,\ldots,{}_kC_{2^{2k-1}}$ and an Hadamard matrix ${}_kH$, all of order $2^{2k-1}m$, such that:

(i) $${}_kC_i\ {}_kC_j^t = {}_kC_j\ {}_kC_i^t = 0,\quad i \neq j;$$

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

(iii) $\quad {}_kC_i\,{}_kH^t = {}_kH_k C_i^t, \;\; 1 \le i \le 2^{2k-1}.$

Note that if we let $S = \begin{pmatrix} + & + \\ + & + \end{pmatrix}$, $P = \begin{pmatrix} + & - \\ - & + \end{pmatrix}$, then we get Lemma 4.

Corollary 12:

(i) If there is an orthogonal pair of order m, then for each positive integer k there are block Golay sequences of length $2^{2k-1}+1$ and block size $2^{2k-1}m$.

(ii) If there are two orthogonal pairs of order m, n, then for each positive integer k, there are block Golay sequences of length 4^k+1 and block size $(mn)^k$.

Proof:

(i) This follows from Theorem 10. (See proof of Theorem 6(i).)

(ii) This follows from Theorem 11. (See proof of Theorem 6(ii).) □

Theorem 13:

(i) If there is an orthogonal pair of order m, then for each positive integer k, there is an Hadamard matrix of order $4(r+(2^{2k-1}+1)^\alpha r')(2^{2k-1}m)^\alpha$, r, r' lengths of Golay sequences, α non-negative integer.

(ii) If there are two orthogonal pairs of order m, n, then for each positive integer k, there is an Hadamard matrix of order $4(r+(4^k+1)^\alpha r')(mn)^{k\alpha}$, r, r' lengths of Golay sequences, α non-negative integer.

Proof:

(i) This follows from Theorem 11, Corollary 12(i) and a method similar to the remark after Theorem 9.

(ii) This follows from Theorem 10, Corollary 12(ii) and a method similar to the remark after Theorem 9.

Next we consider a non-trivial orthogonal pair of order $2 \cdot 9^t, t > 0$.

Seberry and Whiteman [5] were the first to use a set of s matrices of order q to construct conference matrices. These are a set of s $(1,-1)$-matrices of order q, say, $Q_1, Q_2, \ldots, Q_s$ satisfying:

(i) $Q_i^2 = Q_iQ_j = J, \qquad i,j \in \{1,2,\dots,s\};$

(ii) $Q_iQ_j^t = Q_j^tQ_i = J, \qquad i \neq j;$

(iii) $\sum_{i=1}^{s} (Q_iQ_i^t + Q_i^tQ_i) = 4qI_q.$

J is the matrix whose entries are all 1.

Seberry and Whiteman [5] call this set of matrices a regular s-set of matrices and they show that if $q \equiv 3 \pmod 4$ is a prime power, then there exists a regular $\frac{1}{2}(q+1)$-set of matrices of order q^2.

Let $q = 3$, then there exists a regular 2-set of matrices of order 9. Recently Seberry and Zhang [4] proved that actually, there exists a regular 2-set of matrices of order $9^t, t > 0$.

Let Q_1, Q_2 be a regular 2-set of matrices of order $9^t, t > 0$. Let

$$P = \begin{pmatrix} Q_1 & Q_2 \\ Q_2 & Q_1 \end{pmatrix}, \qquad S = \begin{pmatrix} Q_1^t & -Q_2^t \\ -Q_2^t & Q_1^t \end{pmatrix}.$$

Then (S, P) is an orthogonal pair of order $2 \cdot 9^t, t > 0$.

Corollary 14: For each positive integer t, there is:

(i) a class of Hadamard matrices of order $4^2(r + 3r')9^t$, r, r' lengths of Golay sequences;

(ii) a class of Hadamard matrices of order $4^3(r + 17r')9^{4t}$, r, r' lengths of Golay sequences.

Proof:

(i) Let $k = 1, \alpha = 1, m = 2 \cdot 9^t$ in Theorem 13(i).

(ii) Let $k = 2, \alpha = 1, m = n = 2 \cdot 9^t$ in Theorem 13(ii).

Remarks

1. The existence of Hadamard matrices of order $4 \cdot 9^t, t > 0$ is well known (see Turyn [6]). Theorem 9 and the remark after it provides Hadamard matrices of

order $4^2(r+3r')$, $4^3(r+17r')$, r, r' lengths of Golay sequences. Nevertheless it is not possible to construct Hadamard matrices of Corollary 14 by applying other methods. This indicates that Corollary 14 is new and it is worthwhile to apply Corollary 12 to other non-trivial orthogonal pairs.

2. We have deliberately avoided introducing concepts like block T-sequences, block base sequences, etc.. There is a lot more to do in this direction.

Acknowledgements:

The author wishes to thank Professor J. Seberry and Dr. R. Craigen for useful comments and discussions.

The research is supported by NSERC grant 4972.

References

[1] R. Craigen, "Constructing Hadamard Matrices with Orthogonal Pairs," *Ars Combinatoria*, to appear.

[2] H. Kharaghani, "A New Class of Orthogonal Designs," *Ars Combinatoria*, to appear.

[3] J. Seberry and M. Yamada, "Hadamard Matrices, Sequences and Block Designs," *Surveys in Contemporary Design Theory*, to appear.

[4] J. Seberry and Xian-Mo Zhang, "Regular Sets of Matrices and Applications," *Graphs and Combinatorics*, to appear.

[5] J. Seberry and A.L. Whiteman, "New Hadamard Matrices and Conference Matrices Obtained via Mathon's Construction," *Graphs and Combinatorics*, 4 (1988), 355-377.

[6] R.J. Turyn, "A Special Class of Williamson Matrices and Difference Sets," *Journal of Combinatorial Ttheory* (Ser. A), **36** (1984), 111-115.

Department of Mathematics & Computer Science,
University of Lethbridge,
Lethbridge, Alberta,
CANADA T1K 3M4