Dihedral Golay Sequences

F. Kamali

Institute for Studies in Theoretical Physics and Mathematics
P.O. Box 19395-1795, Tehran, Iran
E-mail: frhkam@rose.ipm.ac.ir

H. Kharaghani*

Department of Mathematics and Computer Science
University of Lethbridge, Alberta T1K 3M4, Canada
E-mail: hardi@uleth.ca

Abstract

Dihedral Golay sequences are introduced and found for lengths 7,9,15, and 19. Applications include new classes of signed group Hadamard matrices and 19 real Hadamard matrices of orders $2^t p$, $p \leq 4169$.

1. Preliminaries

Following Craigen [1], we consider the extension of complex numbers to a larger ring R, containing a copy of the (signed) dihedral group as a subgroup. This is an embedding of the ring $\mathbb{C}$ of complex numbers into the (real) ring $M_{2\times2}$ of all 2×2 matrices. Introducing a symbol, s, such that $s^2 = 1$ and $is = -si$, enables us to extend the ring of complex numbers to a larger ring, R, with subgroup $D = \{\pm1, \pm i \pm s, \pm is\}$, in such a way that the ring isomorphism $1 \to \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$, $i \to \left(\begin{smallmatrix}0&-\\1&0\end{smallmatrix}\right)$, and $s \to \left(\begin{smallmatrix}1&0\\0&-\end{smallmatrix}\right)$, where '$-$' denotes -1, is extended uniquely from R into $M_{2\times2}$. Complex conjugation extends to an involution in R such that $\overline{s} = s$ and corresponds to the transpose of 2×2 matrices in $M_{2\times2}$. (See [1] for details.)

An $n \times n$ matrix $H = [h_{ij}]$ with $h_{ij} \in \{\pm1\}$, satisfying $HH^t = nI$, is called an Hadamard matrix of order n. Craigen [2] has extended this definition to matrices with entries in a signed group. (See [2] for details.) In this note we are only interested in matrices with entries in D, identified here as dihedral matrices. A dihedral Hadamard matrix H of order n is an $n \times n$ matrix with entries in D such that $HH^* = nI$, where I is the identity matrix and * is the extension of complex conjugation to matrices in R. We need the following lemmas from Craigen [1].

*The work was completed while the author was on sabbatical leave visiting IPM. Supported in parts by IPM and an NSERC grant.

Lemma 1. (Craigen[1].) If A, B, C, and D are $\{0, \pm 1\}$-matrices such that $A+Bi+Cs+Dis$ is a dihedral Hadamard matrix of order n, then

$$A \otimes \begin{pmatrix} 1 & 1 \\ 1 & - \end{pmatrix} + B \otimes \begin{pmatrix} - & 1 \\ 1 & 1 \end{pmatrix} + C \otimes \begin{pmatrix} 1 & 1 \\ - & 1 \end{pmatrix} + D \otimes \begin{pmatrix} 1 & - \\ 1 & 1 \end{pmatrix}$$

is an Hadamard matrix of order 2n.

Lemma 2. (Craigen[1].) Let A, B, C, and D be $n \times n$ circulant matrices with all entries in $\{\pm 1, \pm i\}$, such that $AA^* + BB^* + CC^* + DD^* = 4nI$. Then

$$\begin{pmatrix} A & -BRs & -CRs & -DRs \\ BRs & A & -D^*Rs & C^*Rs \\ CRs & D^*Rs & A & -B^*Rs \\ DRs & -C^*Rs & B^*Rs & A \end{pmatrix},$$

where R is the back diagonal matrix of order n, is a (signed) dihedral Hadamard matrix of order $4n$.

2. Dihedral Golay Sequences

A sequence $\mathbf{a} = (\mathbf{a_0}, \mathbf{a_1}, \ldots, \mathbf{a_{n-1}})$ with a_is in a signed group G is called a G-sequence of length n. For each sequence $\mathbf{a}$, the Hall polynomial associated to $\mathbf{a}$ is the polynomial $f_{\mathbf{a}}$, defined by $f_{\mathbf{a}}(t) = \sum_{i=0}^{n-1} a_i t^i$.

A pair of $\{\pm 1\}$-sequences $\mathbf{a}, \mathbf{b}$ of length n is called a Golay sequence of length n, if

$$f_{\mathbf{a}}(t) f_{\mathbf{a}}(t^{-1}) + f_{\mathbf{b}}(t) f_{\mathbf{b}}(t^{-1}) = 2n, \quad \text{for all } t \neq 0.$$

Golay sequences were first introduced by Golay [7], and are known to exist for all lengths $2^a 10^b 26^c$, a, b, and c nonnegative integres. Eliahou, Kervaive, and Saffari [5,6] showed that no Golay sequence of length n exists if n has a prime factor $\equiv 3 \pmod 4$. Craigen extended the Golay sequences and allowed the entries to be selected from the set $\{\pm 1, \pm i\}$. In this case, a pair of $\{\pm 1, \pm i\}$-sequences $\mathbf{a}, \mathbf{b}$ of length n is called a complex Golay sequence, if

$$f_{\mathbf{a}}(t) f^*_{\mathbf{a}}(t) + f_{\mathbf{b}}(t) f^*_{\mathbf{b}}(t) = 2n, \text{ for all } t \neq 0,$$

where $f^*_{\mathbf{a}}(t) = \sum_{i=0}^{n-1} \overline{a}_i t^{-i}$ and $\overline{a}_i$ is the complex conjugate of a_i.

While Golay sequences of lengths 2, 10, and 26 were introduced a long time ago [7], complex Golay sequences of lengths 3, 5, 11, and 13 were obtained recently. We list all known such sequences below. We have used j to show $-i$. See Craigen [1], Holzmann and Kharaghani [4] for details.

$$
\begin{aligned}
n &= 1, & \mathbf{a} &= (\mathbf{1}), \mathbf{b} = (\mathbf{1}) \\
n &= 2, & \mathbf{a} &= (\mathbf{11}), \mathbf{b} = (\mathbf{1-}) \\
n &= 3, & \mathbf{a} &= (\mathbf{11-}), \mathbf{b} = (\mathbf{1i1}) \\
n &= 5, & \mathbf{a} &= (\mathbf{ii1-1}), \mathbf{b} = (\mathbf{i11i-}) \\
n &= 10, & \mathbf{a} &= (\mathbf{11-1-1--11}), \mathbf{b} = (\mathbf{11-11111--}) \\
n &= 11, & \mathbf{a} &= (\mathbf{1i-1-ij-ii1}), \mathbf{b} = (\mathbf{11jjj11i-1-}) \\
n &= 13, & \mathbf{a} &= (\mathbf{111i-11j1-1ji}), \mathbf{b} = (\mathbf{1i---i-11j-1j}) \\
n &= 26, & \mathbf{a} &= (\mathbf{1111-11--1-1-1--111--111}), \\
& & \mathbf{b} &= (\mathbf{1111-11--1-11111-1---11---})
\end{aligned}
$$

It follows from product properties of these sequences that complex Golay sequences exist for all lengths $2^a 3^b 5^c 10^d 11^e 13^f 26^h$, a, b, c, d, e, f, and h nonnegative integers, and a depending on b, c, e, and f.

Naturally, it is desirable to somehow fill the above list for the missing lengths. Knowing that complex Golay sequences of lengths 7, 9, and 15 do not exist, we had to introduce a new group. We selected the (signed) dihedral group for this purpose.

A pair of D-sequences $\mathbf{a}, \mathbf{b}$ of lengths n is called a dihedral Golay sequence (DGS) of length n, if

(i) $p(t)q(t) = q(t)p(t)$, for all t and $p, q \in \{f_{\mathbf{a}}, f_{\mathbf{b}}, f^*_{\mathbf{a}}, f^*_{\mathbf{b}}\}$ and

(ii) $f_{\mathbf{a}}(t)f^*_{\mathbf{a}}(t) + f_{\mathbf{b}}(t)f^*_{\mathbf{b}}(t) = 2n$, for all $t \neq 0$,

where $f^*_{\mathbf{a}}(t) = \sum_{i=0}^{n-1} \overline{a}_i t^{-i}$, and $-$ indicates the involution in R.

Condition (i) is essential for our purpose in this paper. This condition automatically holds for complex Golay sequences.

Let $A = \text{circ}(a)$ be the circulant matrix with the sequence $\mathbf{a}$ as its first row. It is not hard to see that if a pair of D-sequences $\mathbf{a}, \mathbf{b}$ of length n is a DGS, then

(i) $XY = YX$, $X, Y \in \{A, A^*, B, B^*\}$, and

(ii) $AA^* + BB^* = 2nI$.

In order to search for DGS we first decided to search for sequences $\mathbf{a}, \mathbf{b}$, where $\mathbf{a}$ is a D-sequence and $\mathbf{b}$ is a $\{\pm 1\}$-sequence. On the one hand we had a low expectation of finding such sequences, but on the other hand we hoped that such sequences would satisfy both conditions of the definition. Note that except for the condition $f^*_{\mathbf{a}}(t)f_{\mathbf{a}}(t) = f_{\mathbf{a}}(t)f^*_{\mathbf{a}}(t)$, the rest of the requirements of condition (i) holds automatically for such sequences. We were pleasantly surprised when our search, in a relatively short time, turned in sequences of lengths 7,9,15 and 19.

We now list DGSs of lenghts 7,9,15, and 19 below. ($\underline{x}$ denotes $-x$.)

$$
\begin{array}{ll}
n=7 & \mathbf{a}=(1,1,1,1,\underline{1},\underline{1},1), \\
 & \mathbf{b}=(\mathrm{s},1,\mathrm{i},\underline{\mathrm{i}},\mathrm{i},1,\underline{\mathrm{s}}) \\
n=9 & \mathbf{a}=(1,1,1,\underline{1},1,\underline{1},1,1,\underline{1}), \\
 & \mathbf{b}=(\mathrm{s},1,1,\mathrm{i},\mathrm{s},\underline{\mathrm{i}},\underline{1},\underline{1},\mathrm{s}) \\
n=15 & \mathbf{a}=(1,1,1,\underline{1},\underline{1},\underline{1},1,1,\underline{1},\underline{1},1,\underline{1},\underline{1},1,\underline{1}), \\
 & \mathbf{b}=(1,\mathrm{i},\mathrm{s},\mathrm{i},\mathrm{s},\mathrm{i},\mathrm{s},\underline{\mathrm{i}},\underline{\mathrm{s}},\mathrm{i},\underline{\mathrm{s}},\mathrm{i},\underline{\mathrm{s}},\mathrm{i},1) \\
n=19 & \mathbf{a}=(1,1,1,\underline{1},1,\underline{1},1,\underline{1},1,1,\underline{1},1,\underline{1},\underline{1},1,\underline{1},\underline{1},1,1), \\
 & \mathbf{b}=(1,1,\mathrm{i},\underline{1},\underline{\mathrm{i}},\underline{\mathrm{i}},\mathrm{s},\mathrm{is},\mathrm{s},\mathrm{s},\mathrm{s},\mathrm{is},\mathrm{s},\mathrm{i},\mathrm{i},1,\underline{\mathrm{i}},\underline{1},\underline{1})
\end{array}
$$

Golay sequences and complex Golay sequences, being elements of a commutative group, possess some very useful properties. Some of these properties carry over to DGS. Next we will identify these properties.

Let $\mathbf{a}=(\mathbf{a_0},\mathbf{a_1},\ldots,\mathbf{a_{n-1}})$ and $\mathbf{b}=(\mathbf{b_0},\mathbf{b_1},\ldots,\mathbf{b_{m-1}})$ be two sequences. Then $\mathbf{a}\otimes\mathbf{b}=:(\mathbf{a_0 b},\mathbf{a_1 b},\ldots,\mathbf{a_{n-1}b})$ and thus

$$
\begin{aligned}
f_{\mathbf{a}\otimes\mathbf{b}}(t) &= a_0 f_{\mathbf{b}}(t)+a_1 t^m f_{\mathbf{b}}(t)+\ldots+a_{n-1}(t^m)^{n-1}f_{\mathbf{b}}(t) \\
&= f_{\mathbf{a}}(t^m)f_{\mathbf{b}}(t).
\end{aligned}
$$

For the sequence $\mathbf{a}$, let $\mathbf{a}^*=(\overline{\mathbf{a}}_{\mathbf{n-1}},\overline{\mathbf{a}}_{\mathbf{n-2}},\ldots,\overline{\mathbf{a}}_{\mathbf{1}},\overline{\mathbf{a}}_{\mathbf{0}})$. Now

$$
\begin{aligned}
f_{\mathbf{a}^*}(t) &= \overline{a}_{n-1}+\overline{a}_{n-2}t+\ldots+\overline{a}_0 t^{n-1}=t^{n-1}(\overline{a}_0+\overline{a}_1 t^{-1}+\ldots+\overline{a}_{n-1}t^{-n+1}) \\
&= t^{n-1}f^*_{\mathbf{a}}(t).
\end{aligned}
$$

Consequently, $f^*_{\mathbf{a}}(t)=t^{-n+1}f_{\mathbf{a}^*}(t)$.

Lemma 3. If there is a DGS of length n and a (real) GS of length m, then there is a DGS of length nm.

Proof: Let $\mathbf{a},\mathbf{b}$ be a DGS of length n and $\mathbf{c},\mathbf{d}$ a GS of length m and let

$$
\begin{aligned}
\mathbf{e} &= (\tfrac{\mathbf{c}+\mathbf{d}}{2})\otimes\mathbf{a}+(\tfrac{\mathbf{c}-\mathbf{d}}{2})\otimes\mathbf{b}, \\
\mathbf{h} &= (\tfrac{\mathbf{c}-\mathbf{d}}{2})^*\otimes\mathbf{a}-(\tfrac{\mathbf{c}+\mathbf{d}}{2})^*\otimes\mathbf{b}.
\end{aligned}
$$

Then

$$
\begin{aligned}
f_{\mathbf{e}}(t) &= f_{\frac{\mathbf{c}+\mathbf{d}}{2}}(t^n)f_{\mathbf{a}}(t)+f_{\frac{\mathbf{c}-\mathbf{d}}{2}}(t^n)f_{\mathbf{b}}(t), \\
f_{\mathbf{h}}(t) &= f_{(\frac{\mathbf{c}-\mathbf{d}}{2})^*}(t^n)f_{\mathbf{a}}(t)-f_{(\frac{\mathbf{c}+\mathbf{d}}{2})^*}(t^n)f_{\mathbf{b}}(t).
\end{aligned}
$$

Thus

$$
\begin{aligned}
f^*_{\mathbf{e}}(t) &= f^*_{\frac{\mathbf{c}+\mathbf{d}}{2}}(t^n)f^*_{\mathbf{a}}(t)+f^*_{\frac{\mathbf{c}-\mathbf{d}}{2}}(t^n)f^*_{\mathbf{b}}(t), \\
f^*_{\mathbf{h}}(t) &= t^{n(1-m)}f_{\frac{\mathbf{c}-\mathbf{d}}{2}}(t^n)f^*_{\mathbf{a}}(t)-t^{n(1-m)}f_{\frac{\mathbf{c}+\mathbf{d}}{2}}(t^n)f^*_{\mathbf{b}}(t).
\end{aligned}
$$

Now the requirement of condition (i) of the definition is seen to be true, and

$$
\begin{aligned}
f_{\mathbf{e}}(t)f^*_{\mathbf{e}}(t)+f_{\mathbf{h}}(t)f^*_{\mathbf{h}}(t) &= 2/4[f_{\mathbf{c}}(t^n)f^*_{\mathbf{c}}(t^n)+f_{\mathbf{d}}(t^n)f^*_{\mathbf{d}}(t^n)][f_{\mathbf{a}}(t)f^*_{\mathbf{a}}(t)+f_{\mathbf{b}}(t)f^*_{\mathbf{b}}(t)] \\
&= 2nm, \quad \text{for all } t\neq 0.
\end{aligned}
$$

Therefore $\mathbf{e},\mathbf{h}$ is a DGS of length nm. $\square$

Corollary 4. There are DGS of lengths $2^a 10^b 26^c g$, a, b, and c nonnegative integers and g the length of a DGS.

Corollary 5. If g is the length of a DGS, then there exists a dihedral Hadamard matrix of order $2^{a+1}10^b 26^c g$, a, b, and c nonnegative integers.

Proof: Let $\mathbf{a}, \mathbf{b}$ be a DGS of length $2^a 10^b 26^c g$. Then $H = \begin{pmatrix} A & B \\ -B^* & A^* \end{pmatrix}$ is a dihedral Hadamard matrix of order $2^{a+1}10^b 26^c g$. Note that by utilizing condition (i) of the definition, we can show that $A^*A + B^*B = A^*A + B^*B = 2^{a+1}10^b 26^c gI$. $\square$

Similarities with complex Golay sequences do not carry over to include the product of lengths of two DGSs. Generally, condition (i) of the definition is hard to achieve. However, we have the following very useful result. We need a simple lemma first.

Lemma 6. Let A be a D-matrix of order n, free of $\pm is$-entries. Let R be the back diagonal matrix of order n. Then $A(Rs)^* = (Rs)A^*$.

Proof: Let $A = A_1 + A_2 i + A_3 s$, where A_1, A_2, A_3 are $(0, \pm 1)$-matrices of order n. Then

$$\begin{aligned} A(Rs)^* &= (A_1 + A_2 i + A_3 s)\bar{s}R = (A_1 s + A_2 is + A_3)R, \\ (Rs)A^* &= R(A_1^t s - A_2^t si + A_3^t) = (A_1 s + A_2 is + A_3)R \ . \end{aligned}$$

$\square$

Theorem 7. Let $\mathbf{a}, \mathbf{b}$ be a DGS of length m free of $\pm is$ entries and $\mathbf{c}, \mathbf{d}$ a GS of length n. Then $A = \text{circ}(\mathbf{a}, \mathbf{c})$, $\mathbf{B} = \text{circ}(\mathbf{a}, -\mathbf{c})$, $C = \text{circ}(\mathbf{b}, \mathbf{d})$, and $D = \text{circ}\ (\mathbf{b}, -\mathbf{d})$, where (α, β) denotes the sequence α followed by the sequence β, are suitable for a Craigen-Goethals-Seidel array and thus there is a dihedral Hadamard matrix of order $4(m + n)$.

Proof: The Hall polynomials associated to the sequences $(\mathbf{a}, \mathbf{c})$, $(\mathbf{a}, -\mathbf{c})$, $(\mathbf{b}, \mathbf{d})$, and $(\mathbf{b}, -\mathbf{d})$ are as follows:

$$\begin{aligned} f_{(\mathbf{a},\mathbf{c})}(t) &= f_{\mathbf{a}}(t) + t^m f_{\mathbf{c}}(t), \\ f_{(\mathbf{a},-\mathbf{c})}(t) &= f_{\mathbf{a}}(t) - t^m f_{\mathbf{c}}(t), \\ f_{(\mathbf{b},\mathbf{d})}(t) &= f_{\mathbf{b}}(t) + t^m f_{\mathbf{d}}(t), \\ f_{(\mathbf{b},-\mathbf{d})}(t) &= f_{\mathbf{b}}(t) - t^m f_{\mathbf{d}}(t). \end{aligned}$$

Thus

$$\begin{aligned} f^*_{(\mathbf{a},\mathbf{c})}(t) &= f^*_{\mathbf{a}}(t) + t^{-m} f^*_{\mathbf{c}}(t), \\ f^*_{(\mathbf{a},-\mathbf{c})}(t) &= f^*_{\mathbf{a}}(t) - t^{-m} f^*_{\mathbf{c}}(t), \\ f^*_{(\mathbf{b},\mathbf{d})}(t) &= f^*_{\mathbf{b}}(t) + t^{-m} f^*_{\mathbf{d}}(t), \\ f^*_{(\mathbf{b},-\mathbf{d})}(t) &= f^*_{\mathbf{b}}(t) - t^{-m} f^*_{\mathbf{d}}(t). \end{aligned}$$

It is easy to see that the above polynomials are all pairwise commuting, therefore A, B, C, D,
A^*, B^*, C^*, and D^* are pairwise commuting matrices. It is not hard to see that $AA^* + BB^* + CC^* + DD^* = 4(n+m)I$. Furthermore, by Lemma 6, $X(Rs)^* = (Rs)X^*$ for $X \in \{A, B, C, D\}$. Hence, A, B, C, and D are suitable for a Craigen-Goethals-Seidel array and thus there is a diheral Hadamard matrix of order $4(m + n)$. $\square$

Corollary 8. There is a dihedral Hadamard matrix of order $4(g_1 g + g_2)$, where g_1, g_2 are lengths of Golay sequences and $g = 7, 9$, and 15.
Proof: This follows from Theorem 7 and the fact that $DGSs$ of lengths 7,9, and 15 found here are free of $\pm is$-entries. □

Corollary 9. There is an Hadamard matrix of order $8(g_1 g + g_2)$, where g_1, g_2 are lengths of Golay sequences and $g = 7, 9$, and 15.
Proof: This follows from Corollary 8 and Lemma 1. □

Next we apply Corollary 9 to obtain new Hadamard matrices. Table 1 shows 19 new Hadamard matrices, all obtained from this Corollary. We have used Craigen's Table in the *CRC* Handbook of Combinatoral Designs [3] as our reference.

p	new t	previous t	$g_1 g + g_2$
491	4	5	$26.7 + 2^3 . 10^2$
839	3	4	$7 + 2^5 . 26$
1031	3	6	$7 + 2^{10}$
1571	5	7	$26^2 . 9 + 2 .10^2$
1793	3	4	$2^8 . 7 + 1$
1795	4	5	$26.15 + 2^5.10^2$
2039	5	7	$10^2. 15 + 2^8.26$
2063	3	7	$15 + 2^{11}$
2087	3	4	$7 + 2^3.10.26$
2287	6	7	$2^3. 10.9 + 26^3$
2371	4	7	$26^2. 7 + 10$
2677	4	6	$26.9 + 2^9.10$
2913	3	6	$2^4. 26.7 + 1$
3093	6	7	$2^{10}. 7 + 26^3$
3215	3	4	$15 + 2^5.10^2$
3343	3	8	$15 + 2^7.26$
4007	3	8	$7 + 2^2.10^3$
4167	3	6	$7 + 2^4.10.26$
4169	3	8	$9 + 2^4.10.26$

Table 1. New Hadamard matrices of order $2^t p$

References

[1] R. Craigen, *Complex Golay Sequences*, J. Combin. Math. and Comb. Comp. **15** (1994), 161-169.

[2] R. Craigen, *Signed Groups, Sequences and the Asymptotic Existence of Hadamard Matrices*, J. Combin. Theory (A) **71** (1995), 241-254.

[3] R. Craigen, *Hadamard Matries and Designs*, in: *The CRC Handbook of Combinatorial Designs*, (Charles J. Colbourn and Jeffrey H. Dinitz, ed.), CRC Press, New-York (1996), 370-377.

[4] W.H. Holzmann and H. Kharaghani, *A Computer Search for Complex Golay Sequences*, Australas. J. Combin. **10** (1994), 251-256.

[5] S. Eliahou, M. Kervaire, and B. Saffari, *A New Restriction on the Lengths of Golay Complementary Sequences*, J. Combin. Theory (A) **55** (1990), 49-59.

[6] S. Eliahou, M. Kervaire, and B. Saffari, *On Golay Polynomial Pairs*, Adv. in Appl. Math. **12** (1991), 235-292.

[7] J. Seberry and M. Yamada, *Hadamard Matrices, Sequences, and Block Designs*, in: *Contemporary Design Theory: A Collection of Surveys*, (J.H. Dinitz and D.R. Stinson, ed.), John Wiley & Sons, Inc., New-York, 1992, pp. 431-560.

(Received 27/8/97)