Complex Golay Sequences

R. Craigen*
Dept. of Mathematics and Computer Science
University of Lethbridge
Lethbridge, Alberta
Canada T1K 3M4
email: craigen@alpha.uleth.ca

Abstract

We introduce a complex version of Golay sequences and show how these may be applied to obtain new Hadamard matrices and complex Hadamard matrices. We also show how to modify the Goethals-Seidel array so that it can be used with complex sequences.

1 Preliminaries

For background on Hadamard matrices and complex Hadamard matrices, see [7] and [8]. Hadamard matrices are conjectured to exist in all orders $4p$, and complex Hadamard matrices are conjectured to exist in all orders $2p$, where p is any positive integer. With a couple of trivial exceptions, these are the only possible orders in both cases. One of the most effective methods for obtaining Hadamard matrices uses sequences with zero autocorrelation. We introduce here some conventions for working with sequences.

A sequence $a = (a_1, \ldots, a_n)$ (of real numbers) is said to have *length* n. To each sequence we associate a polynomial $f_a(x) = \sum_{i=1}^n a_i x^i$. We define an involution on the set of (Laurent) polynomials by $f^*(x) = f(x^{-1})$. The *autocorrelation* (respectively *periodic autocorrelation* of period p) of a sequence a is the sequence associated with the positive degree terms of the polynomial $f_a f_a{}^*$ (respectively $f_a f_a{}^* \bmod (x^p - 1)$)[1]. We define the *autocorrelation* of a set of sequences to be the sum of the autocorrelations of the sequences in the set. When dealing with (nonperiodic) autocorrelation,

*Supported by an NSERC Postdoctoral Fellowship

[1] Autocorrelation is usually defined as a function based on convolution of sequences, which amounts to the same thing.

we generally understand every sequence to have an arbitrary number of zeros appended to it, although these are not neccesarily counted in its length.

k sequences $a, b, \dots, z$ are *complementary* if they have zero autocorrelation. The *weight* of a set of complementary sequences is the constant term (ie, the *only* nonzero term) of the polynomial $f_a f_a{}^* + f_b f_b{}^* + \cdots + f_z f_z{}^*$. Displaying sequences, we use the convention that $-$ represents -1.

For example, the sequences

$$\begin{aligned} a &= (1000100) \\ b &= (01010-0) \\ c &= (0010000) \\ d &= (0000001) \end{aligned}$$

comprise a set of four complementary $(0, \pm 1)$-sequences of length 7 with weight 7, for

$$\begin{aligned} &(f_a f_a{}^* + f_b f_b{}^* + f_c f_c{}^* + f_d f_d{}^*)(x) \\ &= (1 + x^4)(1 + x^{-4}) + (x + x^3 - x^5)(x^{-1} + x^{-3} - x^{-5}) + x^2 x^{-2} + x^6 x^{-6} \\ &= (2 + x^4 + x^{-4}) + (3 - x^4 - x^{-4}) + 1 + 1 \\ &= 7. \end{aligned}$$

We use a^* to denote the sequence whose elements are those of a, in reverse order (Warning: $f_a{}^* = x^{1-n} f_{a^*}$, in general, rather than f_{a^*}). If a, b are sequences of lengths m, n respectively, we use $a \otimes b$ to denote their *direct product,* $(a_1 b, \dots, a_n b)$, which will have length mn (here $a_i b$ represents the "scalar" product of the number a_i and the n-tuple b; commas indicate concatenation of sequences).

To each sequence, $a = (a_1, \dots, a_n)$, we associate the $n \times n$ circulant matrix A with first row $(a_1, \dots, a_n)$ (denoted $A = circ(a_1, \dots, a_n)$). We can also write $A = f_a(X)$, where $X = circ(0, 1, 0, \dots, 0)$, and note that $A^t = f_a{}^*(X)$, and so if $A = circ(a)$, $B = circ(b)$, etc., the set $\{a, b, \dots\}$ has zero autocorrelation with weight w precisely when $AA^t + BB^t + \cdots = wI$. The matrices A, B, etc. naturally commute, since they are all polynomials in X.

One last observation: if R is any back-circulant matrix, then AR is backcirculant, and therefore symmetric, when A is circulant. It follows that $AR^t = RA^t$. Henceforth, we shall use R to denote some fixed back-circulant permutation matrix of appropriate size.

2 Hadamard matrices from sequences

Two complementary (± 1)-sequences, a, b of length g are called *Golay sequences.* If $A = circ(a)$ and $B = circ(b)$, it can be verified directly that the matrix $\begin{pmatrix} A & -B \\ B^t & A^t \end{pmatrix}$ is an Hadamard matrix of order $2g$.

There are Golay sequences of lengths 1,2,10 and 26, as follows.

$$\begin{array}{ll} g=1: & a=(1),\ b=(1) \\ g=2: & a=(11),\ b=(1-) \\ g=10: & a=(11-1-1--11),\ b=(11-11111--) \\ g=26: & a=(1111-11--1-1-1--1-111--111), \\ & b=(1111-11--1-11111-1---11---) \end{array} \tag{1}$$

The following result is well-known [7].

Lemma 1 *If a, b are Golay sequences of length g_1 and c, d are Golay sequences of length g_2, then*

$$h = \frac{1}{2}[(a+b) \otimes c + (a-b) \otimes d^*]$$

and

$$k = \frac{1}{2}[(a+b) \otimes d - (a-b) \otimes c^*]$$

are Golay sequences of length $g_1 g_2$.

It follows that there are Golay sequences for all lengths $g = 2^a 10^b 26^c$, $a, b, c \geq 0$, and Hadamard matrices constructed as above from each of these.

Theorem 2 *There is an Hadamard matrix of order $2^a 10^b 26^c$ (constructed from Golay sequences), for any $a > 0$, $b, c \geq 0$.*

We may also use the circulant matrices corresponding to four complementary (± 1)-sequences of length n in the *Goethals-Seidel array,*

$$\begin{pmatrix} A & -BR & -CR & -DR \\ BR & A & -D^tR & C^tR \\ CR & D^tR & A & -B^tR \\ DR & -C^tR & B^tR & A \end{pmatrix}, \tag{2}$$

To obtain an Hadamard matrix of order $4n$. There are a good many constructions for such sequences [7], but we mention here one which uses Golay sequences.

Lemma 3 *If u, v are Golay sequences of length g_1 and x, y are Golay sequences of length g_2, then $a = (u, x)$, $b = (u, -x)$, $c = (v, y)$ and $d = (v, -y)$ are four complementary sequences of length $g_1 + g_2$.*

This has the following immediate consequence.

Theorem 4 *There is an Hadamard matrix of order $4(g_1+g_2)$ (constructed from the Goethals-Seidel array), where g_1 and g_2 are the lengths of any Golay sequences.*

Powerful as these results may be when they apply, they are nevertheless quite minor in their impact on the known orders for Hadamard matrices, for a couple of reasons. First, in spite of much work on the part of some rather good mathematicians armed with computers, no new lengths for Golay sequences have been found to add to the rather sparse set used for theorem 2. In fact all lengths up to 100, except 68, 74 and 82 have been eliminated and Eliahou, Kervaire and Saffari [4] have recently shown that Golay sequences do not exist for any length divisible by a number $\equiv 3 \bmod 4$. Some researchers are now of the opinion that no new ones are likely to be found. Second, the only possible odd length for Golay sequences is 1, and for any t there are only finitely many known Golay sequences not divisible by 2^t, and so there are only finitely many Hadamard matrices of orders $2^t p$, odd p, known to be obtained by theorem 2, and theorem 4 gives only a very sparse, albeit infinite, set of matrices of orders $2^{t+1} q$, odd q.

3 Complex sequences and Hadamard matrices

Theorem 5 *If A, B are $(0, \pm 1)$-matrices such that $A + Bi$ is a complex Hadamard matrix of order n, then $A \otimes \begin{pmatrix} 1 & 1 \\ 1 & - \end{pmatrix} + B \otimes \begin{pmatrix} - & 1 \\ 1 & 1 \end{pmatrix}$ is an Hadamard matrix of order $2n$.*

It was this fact that motivated Turyn [8] to study complex Hadamard matrices. We shall consider how to use *complex* sequences to obtain complex Hadamard matrices.

We adopt the same conventions for complex sequences as for real ones, except that for a sequence $a = (a_1, \ldots, a_n)$, a^* is defined as $(\overline{a}_n, \ldots, \overline{a}_1)$, and $f_a{}^*(x) = \sum_{i=1}^{n} \overline{a}_i x^{-i}$.

We say that complementary complex $(\pm 1, \pm i)$-sequences a, b of length g are *complex Golay sequences*. As before, if $A = circ(a)$ and $B = circ(b)$, then $\begin{pmatrix} A & -B \\ B^* & A^* \end{pmatrix}$ is a complex Hadamard matrix of order $2g$.

Every (real) pair of Golay sequences is obviously also a pair of complex Golay sequences. In addition to these, we offer the following examples.

$$\begin{array}{lll} g=3: & a=(11-), & b=(1i1) \\ g=5: & a=(ii1-1), & b=(i11i-) \end{array} \tag{3}$$

Evidently, some of the theoretical restrictions associated with Golay sequences do not apply to complex Golay sequences, for both these lengths are odd, and $3 \equiv 3 \bmod 4$. Now, as with Golay sequences, it is possible to multiply the lengths of complex Golay sequences, although if neither pair is real, there is an extra factor of 2 in the resulting length.

Lemma 6 *Let a, b be complex Golay sequences of length g_1 and c, d be complex Golay sequences of length g_2. Then*

1. *$(a \otimes c, b \otimes d^*)$ and $(a \otimes d, -b \otimes c^*)$ are complex Golay sequences of length $2g_1g_2$;*

2. *if we further assume that a and b are real, $\frac{1}{2}[(a+b) \otimes c + (a-b) \otimes d^*]$ and $\frac{1}{2}[(a+b) \otimes d - (a-b) \otimes c^*]$ are complex Golay sequences of length g_1g_2.*

This gives us complex Golay sequences of all lengths $2^a3^b5^c26^d$, $a, b, c, d \geq 0$, $a \geq b+c-1$.

Theorem 7 *There is a complex Hadamard matrix of every order $2^{a+1}3^b5^c26^d$ (constructed from complex Golay sequences), $a, b, c, d \geq 0$, $a \geq b+c-1$. Consequently, there is also an Hadamard matrix of order $2^{a+2}3^b5^c26^d$.*

Obviously, the next step is to use complex Golay sequences to obtain sets of four complementary complex $(\pm 1, \pm i)$-sequences.

Lemma 8 *If u, v are complex Golay sequences of length g_1 and x, y are complex Golay sequences of length g_2, then $a = (u, x)$, $b = (u, -x)$, $c = (v, y)$ and $d = (v, -y)$ are four complementary sequences of length $g_1 + g_2$.*

To use such sequences, we can no longer rely on strict analogy to the real case, for we see that a *complex* circulant matrix A does not neccesarily satisfy $AR^* = RA^*$, and because of this, complementary sequences used in the obvious complex version of the Goethals-Seidel array do not neccesarily give a complex Hadamard matrix.

To resolve this difficulty, we require only a very simple application of *signed groups*. See [2] for a brief introduction to these; this, however, is not neccesary in order to follow the method given here. Here, we simply consider the group, S, of all 2×2 signed permutation matrices (this is an example of what we call a signed group), and the ring of 2 × 2 (real) matrices, which contains it. There is a well-known embedding of the set of complex numbers into this ring given by the identifications

$$1 \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{4}$$

and

$$i \leftrightarrow \begin{pmatrix} 0 & - \\ 1 & 0 \end{pmatrix}. \tag{5}$$

Let us introduce another symbol, s, such that $s^2 = 1$, $is = -is$, thereby extending the complex numbers to a larger ring, $\mathbf{R}$, with subgroup $\{\pm 1, \pm i, \pm s, \pm is\}$, which is identified with S by the (unique) ring isomorphism extending (4), (5) and

$$s \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & - \end{pmatrix}. \tag{6}$$

Complex conjugation extends to an involution in $\mathbf{R}$ such that $\overline{s} = s$, which corresponds to the transpose of 2 × 2 matrices. Now we say that an $n \times n$ matrix H with entries in S is a *signed group Hadamard matrix* $SH(n, S)$ if $HH^* = nI$, where $*$ is the extension of the Hermitian adjoint to matrices with entries in $\mathbf{R}$, using this involution in place of complex conjugation. This is a simple generalization of the notion of a complex Hadamard matrix. There is no "penalty" (in terms of higher powers of 2 in the order of the resulting matrix) associated with converting these signed group Hadamard matrices to ordinary Hadamard matrices, beyond that already present in theorem 5.

Theorem 9 *If A, B, C and D are $(0, \pm 1)$ matrices such that $A+Bs+Ci+Dis = SH(n, S)$, 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 $2n$.*

Now consider the fact that, for all complex numbers λ, we have $\lambda\overline{s} = s\overline{\lambda}$. It follows that if A is any complex circulant matrix, $A(Rs)^* = (Rs)A^*$. Therefore we may modify the Goethals-Seidel array as follows so that it can be used with complex sequences.

Theorem 10 *If a, b, c and d are complementary $(\pm 1, \pm i)$-sequences of length n, then*

$$\begin{pmatrix} A & -BRs & -CRs & -DRs \\ BRs & A & -D^*Rs & C^*Rs \\ CRs & D^*Rs & A & -B^*Rs \\ DRs & -C^*Rs & B^*Rs & A \end{pmatrix} = SH(4n, S). \tag{7}$$

Table 1: Some "new" Hadamard matrices $2^t p$, p odd

$p =$	419	479	491	653	659	839	1257	1319	2033	3749
"new" t	3	4	5	3	4	4	4	4	3	3
"previous best"	4	5	15	4	17	8	5	18	4	4

Consequently, there is an Hadamard matrix of order $8n$.

Lemma 8 and theorem 10 together give a large new class of Hadamard matrices.

Corollary 11 *There are signed group Hadamard matrices* $SH(4n, S)$, *and therefore Hadamard matrices of orders* $8n$, *for any* $n = 2^{a_1}3^{b_1}5^{c_1}26^{d_1} + 2^{a_2}3^{b_2}5^{c_2}26^{d_2}$, $a_i, b_i, c_i, d_i \geq 0$, $a_i \geq b_i + c_i - 1$, $i = 1, 2$.

Table 1 indicates some Hadamard matrices that can be obtained in this fashion, that are "new" in the sense that they are not found in the most comprehensive tables to date, [5] and [7][2].

4 Concluding remarks

1. The results of theorem 10 are somewhat less sparse than those of theorem 4. Our method is not bound by the same theoretical constraints as the original, so the possibility remains, and indeed seems quite likely, that it can be further extended by finding more complex Golay sequences, particularly of odd order. In any case, it is evident that *every* new complex Golay sequence found will give new infinite classes of Hadamard matrices. A search for more complex Golay sequences may therefore be worthwhile.

2. For simplicity, we have not considered more general sets of four complementary complex sequences, but these clearly exist in greater abundance than is known for real ones. One way to get more is to use a complex version of *base sequences* (for example, complex Golay sequences of lengths g_1 and g_2 give complex base sequences of lengths g_1, g_1, g_2, g_2). *Yang multiplication* [7], [9] happens to work for complex base sequences, and so we have four complementary complex sequences of lengths $y(g_1 + g_2)$, where some known admissible values

[2] These are not truly new in all cases, as we have elsewhere used signed groups to provide comprehensive constructions for Hadamard matrices which equal or better these results in some—but not all—cases. See, for example, [2], [3].

of y are 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 31, 33, 37, 41, 45, 51, 53, 59 and $2g+1$, where g is the length of Golay sequences.

3. We can also perform a complex version of Yang multiplication, multiplying real or complex base sequences by $2g+1$ (for example), where g is the length of complex Golay sequences.

4. We can apply the methods given in [2], [3] to get $SH(4(n+1), SP_{2^5})^3$ from four complementary complex sequences of length n. This gives an Hadamard matrix of order $2^7(n+1)$. A few examples (all new) are Hadamard matrices of orders 2^7p, $p = g_1 + g_2 + 1 = 1447$, 1571, 2039, 2671, 3359, 3437, improving on the previous best known 2^tp, namely $t = 19$, 8, 10, 9, 22, 9 respectively.

5. There are other uses for complex sequences, such as the construction of complex orthogonal designs [6]. There are complex versions of T-matrices, which can be used in combination with complex versions of *Williamson-type* matrices to further multiply the possibilities, as in the method of Cooper and J. Wallis [1].

Note added in proof. Holzmann and Kharaghani report that an exhaustive computer search turned up no complex Golay sequences of lengths 7 or 9.

References

[1] J. Cooper and J. S. Wallis, *A construction for Hadamard arrays*, Bull. Austral. Math. Soc., 7 (1972), pp. 269–278.

[2] R. Craigen, *The structure of weighing matrices having large weights.* to appear in *Designs, Codes and Cryptography*, 1993.

[3] R. Craigen and H. Kharaghani, *Hadamard matrices from weighing matrices via signed groups.* preprint, 1992.

[4] S. Eliahou, M. Kervaire, and B. Saffari, *A new restriction on the lengths of Golay complementary sequences*, J. Combinatorial Thry., 55 (1990), pp. 49–59.

[5] J. Seberry. unpublished (1990) tables of Hadamard matrices of order up to 16,000.

[3] A signed group Hadamard matrix over SP_{2^5}—the signed group of 32 × 32 signed permutation matrices. In this notation, S would be denoted SP_2.

[6] J. SEBERRY AND A. L. WHITEMAN, *Complex weighing matrices and orthogonal designs*, Ars Comb., 9 (1980), pp. 149–162.

[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, eds., John Wiley & Sons, Inc., 1992, pp. 431–560.

[8] R. J. TURYN, *Complex Hadamard matrices*, in Combinatorial Structures and their Applications, New York, 1970, pp. 435–437.

[9] C. H. YANG, *On composition of four-symbol δ-codes and Hadamard matrices*, Proc. Amer. Math. Soc., 107 (1989), pp. 763–776.