MATHEMATICS OF COMPUTATION
Volume 73, Number 246, Pages 967–985
S 0025-5718(03)01576-X
Article electronically published on July 1, 2003

A COMPLETE DESCRIPTION OF GOLAY PAIRS FOR LENGTHS UP TO 100

P. B. BORWEIN AND R. A. FERGUSON

ABSTRACT. In his 1961 paper, Marcel Golay showed how the search for pairs of binary sequences of length n with complementary autocorrelation is at worst a $2^{\frac{3n}{2}-6}$ problem. Andres, in his 1977 master's thesis, developed an algorithm which reduced this to a $2^{\frac{n}{2}-1}$ search and investigated lengths up to 58 for existence of pairs. In this paper, we describe refinements to this algorithm, enabling a $2^{\frac{n}{2}-5}$ search at length 82. We find no new pairs at the outstanding lengths 74 and 82. In extending the theory of composition, we are able to obtain a closed formula for the number of pairs of length $2^k n$ generated by a primitive pair of length n. Combining this with the results of searches at all allowable lengths up to 100, we identify five primitive pairs. All others pairs of lengths less than 100 may be derived using the methods outlined.

1. INTRODUCTION

Autocorrelation. Let $A = [a_0, a_1, \ldots, a_{n-1}]$ be a sequence of length n. For each k with $0 \le k \le n-1$ we define the kth *acyclic autocorrelation* coefficient, c_k, as the inner product of A on the overlap of a copy of itself displaced by k positions:

a_0	$\ldots$	a_k	a_{k+1}	$\ldots$	a_{n-1}		
		a_0	a_1	$\ldots$	a_{n-k-1}	$\ldots$	a_{n-1}

$$c_k = \sum_{i=0}^{n-k-1} a_i a_{i+k} = a_0 a_k + a_1 a_{k+1} + \cdots + a_{n-k-1} a_{n-1}.$$

From A we construct the polynomial

$$A(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}.$$

The coefficients c_k then appear in the expansion:

$$A(x)A(x^{-1}) = c_0 + c_1(x + x^{-1}) + \cdots + c_{n-1}\left(x^{n-1} + x^{-(n-1)}\right).$$

A *Golay pair* consists of two sequences

$$A = [a_1, a_2, \ldots, a_{n-1}],$$
$$B = [b_1, b_2, \ldots, b_{n-1}]$$

Received by the editor December 10, 2001 and, in revised form, November 28, 2002.
2000 *Mathematics Subject Classification.* Primary 11B83, 05B20; Secondary 94A11, 68R05.
Key words and phrases. Complementary pairs, composition of sequences.
Research of the authors was supported in part by grants from NSERC of Canada and MITACS Symbolic Analysis Project.

with ± 1 entries, such that the off-centre ($k > 0$) autocorrelations cancel, i.e.,

$$c_k + d_k = 0,$$

where c_k, d_k are the kth autocorrelation coefficients for A, B, respectively.

Example ($n = 8$)**.**

$$A = [\ 1,\ \ 1,\ \ 1, -1,\ \ 1, -1,\ \ 1,\ \ 1]\,,$$
$$B = [\ 1,\ \ 1,\ \ 1, -1, -1,\ \ 1, -1, -1]\,.$$

For $k = 3$, we obtain:

$$c_3 = -1 + 1 - 1 - 1 + 1 = -1 \quad \text{and} \quad d_3 = -1 - 1 + 1 + 1 + 1 = \ 1,$$

giving $c_3 + d_3 = 0$. This is true for all values $1 \le k \le 7$.

In polynomial terms, an equivalent formulation of the autocorrelation conditions is

$$A(x)A(x^{-1}) + B(x)B(x^{-1}) = 2n.$$

This polynomial is constant on the unit circle in the complex plane, which explains a number theoretic interest in such sequences.

From this we derive

$$2n = A(1)^2 + B(1)^2.$$

Thus $A(1)$ and $B(1)$ have the same parity and

$$n = \left(\frac{A(1) + B(1)}{2}\right)^2 + \left(\frac{A(1) - B(1)}{2}\right)^2$$

shows that n must be the sum of two integral squares.

Also derivable, except for the length 1, are the facts that n must be even (Golay [7], 1961) and that n is not divisible by a prime $\equiv 3 \pmod 4$ (Eliahou, Kervaire, Saffari [5], 1990).

Combining these, we formulate a list of the "allowable" lengths less than 100, namely,

$$1, 2, 4, 8, 10, 16, 20, 26, 32, 34, 40, 50, 52, 58, 64, 68, 74, 80, 82.$$

Searches for pairs. In searching for examples of Golay pairs, two considerations may be taken into account [7], reducing the total 2^{2n} cases under consideration to $2^{\frac{3n}{2}-6}$:

(1) *Equivalence:* There are six operations establishing equivalence classes of Golay pairs:
   - (a) interchanging the sequences in a pair,
   - (b) reversing the order in the first,
   - (c) or reversing the order in the second,
   - (d) changing the signs of the first,
   - (e) or changing the signs of the second,
   - (f) changing signs of alternate entries in both.

(2) *Reduction modulo* 4*:* This leads to the $\frac{n}{2}$ equations

$$a_i a_{n-1-i} + b_i b_{n-1-i} = 0,$$

$0 \le i \le \frac{n}{2} - 1$, involving entries in ± 1 sequences in a pair (A, B).

Through extended calculations made by hand, Golay demonstrated the existence of two inequivalent pairs at length 10 and a pair at length 26. He also gave rules of composition for forming pairs of lengths $2n$ and $2mn$ from existing pairs of length m and n. His constructions for lengths 2^k give all existing pairs for $0 \leq k \leq 6$.

In his 1974 paper, Turyn [11] gave a construction for forming pairs of length mn from existing pairs of length m and n.

The first exhaustive search for Golay pairs was conducted at length 26 (Jauregui), taking 75 hours to confirm the single example of inequivalent pairs. In his 1977 master's thesis, Andres [1] showed that a further reduction modulo 2 enables an initial search involving $2^{n/2}$ cases. A further reduction modulo 4 was applied for examples surviving this test. He used one of the equivalences, bringing this to a $2^{\frac{n}{2}-1}$ search, reducing the time taken at $n = 26$ to 1 minute. His work showed nonexistence of pairs at lengths 34, 50 and 58 and produced complete lists of representatives at lengths 8, 10, 16, 20 and 32. Later work by James [9] (1987) established the nonexistence of pairs at length 68. Djokovic [4] (1998) demonstrated how to choose a canonical pair from each class of equivalent pairs. He conducted exhaustive searches at lengths 32 and 40, producing complete lists of canonical pairs.

The present work outlines improvements which may be made to Andres' algorithm, enabling a $2^{\frac{n}{2}-5}$ search at length 82 with a running time of two weeks. Exhaustive searches have been conducted at all allowable lengths under 100, confirming earlier work and showing the nonexistence of pairs at lengths 74 and 82.

We call a Golay pair *primitive* if it cannot be derived through composition from pairs of shorter lengths. We present a context for the theory of the composition of pairs from which Golay's and Turyn's constructions are easily derived. This theory for producing pairs of length 2^n from a primitive pair of length n is developed, producing a closed formula for the number of pairs which may be generated:

Theorem 1.1. *From a primitive Golay pair of length n having 64 conjugates, there are exactly $2^{k+6}(k+1)(k+1)!$ pairs derivable at length $2^k n$.*

Combining this with the results of searches, we present a compact classification for all pairs of length up to 100 (see the following section for the definitions P, Q, P^*, Q^*):

Theorem 1.2. *For lengths $n < 100$, all Golay pairs are derivable from the following five primitive pairs (in our canonical form):*

Length 1 : $([1], [1])$.

Length 10 : $[P, P, -P, Q, Q^*]$:

$$[\ 1,\ \ 1, -1,\ \ 1, -1,\ \ 1, -1, -1,\ \ 1,\ \ 1],$$
$$[\ 1,\ \ 1, -1,\ \ 1,\ \ 1,\ \ 1,\ \ 1,\ \ 1, -1, -1]$$

and $[P, Q, -Q^*, P^*, Q]$:

$$[\ 1,\ \ 1,\ \ 1,\ \ 1,\ \ 1, -1,\ \ 1, -1, -1,\ \ 1],$$
$$[\ 1,\ \ 1, -1, -1,\ \ 1,\ \ 1,\ \ 1, -1,\ \ 1, -1].$$

Length 20 : $[P, Q, Q, P, -P, P, Q^*, -P^*, -P^*, P]$:

$$[\ 1,\ \ 1,\ \ 1,\ \ 1, -1,\ \ 1, -1, -1, -1,\ \ 1,\ \ 1, -1, -1,\ \ 1,\ \ 1, -1,\ \ 1, -1, -1,\ \ 1],$$
$$[\ 1,\ \ 1,\ \ 1,\ \ 1, -1,\ \ 1,\ \ 1,\ \ 1,\ \ 1,\ \ 1, -1, -1, -1,\ \ 1, -1,\ \ 1, -1,\ \ 1,\ \ 1, -1].$$

Length 26 : $[P,P,P,Q,-P,P,P,-Q,-P,P,-P,Q,Q^*]$:

$[1,1,1,1,-1,1,1,-1,-1,1,-1,1,-1,1,-1,-1,1,-1,1,1,1,-1,-1,1,1,1]$,
$[1,1,1,1,-1,1,1,-1,-1,1,-1,1,1,1,1,1,-1,1,-1,-1,-1,1,1,-1,-1,-1]$.

2. Reductions modulo 2 and 4

Reduction modulo 4. Where a, b are restricted to the values ± 1, we find

$$ab \equiv a + b - 1 \pmod 4.$$

Thus, polynomial equations involving variables taking only the values ± 1 become linear equations upon reduction modulo 4. We apply this to the $n-1$ quadratic equations

$$\begin{array}{ccccc}
a_0a_{n-1} & + & b_0b_{n-1} & = & 0,\\
a_0a_{n-2}+a_1a_{n-1} & + & b_0b_{n-2}+b_1b_{n-1} & = & 0,\\
a_0a_{n-3}+a_1a_{n-2}+a_2a_{n-1} & + & b_0b_{n-3}+b_1b_{n-2}+b_2b_{n-1} & = & 0,\\
\cdots & & \cdots & & \\
a_0a_1+a_1a_2+\cdots+a_{n-2}a_{n-1} & + & b_0b_1+b_1b_2+\cdots+b_{n-2}b_{n-1} & = & 0
\end{array}$$

defining a Golay pair (A, B), obtaining:

Proposition 2.1 (Golay [7])**.** *For a Golay pair (A, B) of length n:*
(i) *n must be even.*
(ii) *$a_ia_{n-1-i} + b_ib_{n-1-i} = 0$ for $0 \le i \le n/2$.*

Proof. Reducing the first set of $m = \lfloor \frac{n}{2} \rfloor$ of these leads to the conditions

$$a_i + a_{n-1-i} + b_i + b_{n-1-i} \equiv 2 \pmod 4,$$

which are equivalent to

$$a_ia_{n-1-i} + b_ib_{n-1-i} = 0,$$

$0 \le i < m$.

In case n were odd, the next equation would reduce to

$$2a_{(n-1)/2} + 2b_{(n-1)/2} \equiv 2 \pmod 4,$$

which is impossible for $a_{(n-1)/2}, b_{(n-1)/2} = \pm 1$. Hence n must be even.

Continuing this reduction, we find the remaining equations to be linearly dependent on the first m relations. □

Thus, for a Golay pair (A, B), exactly three of $a_i, a_{n-1-i}, b_i, b_{n-1-i}$ have the same sign, for $0 \le i < m = n/2$.

Quads (Andres [11])**.** We now identify the pair with a sequence of m nested *quads*,

$$(A, B) = (X_0, X_1, \ldots, X_{m-1}).$$

These quads are the 2×2 matrices defined by

$$X_i = \begin{bmatrix} a_i & a_{n-1-i} \\ b_i & b_{n-1-i} \end{bmatrix}, \qquad 0 \le i \le m-1.$$

There are eight possible quads, which we classify in the following way:

$$P = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad P^*, \ -P, \ -P^*,$$
$$Q = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}, \quad Q^*, \ -Q, \ -Q^*.$$

The superscript * is used to indicate the interchanging of columns in a matrix.

The sequence $(X_0, X_1, \ldots, X_{m-1})$ is completely described by three binary vectors:

(1) the *horizontal orientation vector* $H = [h_0, h_1, \ldots, h_{m-1}]$, where $h_i = 0$ or 1 for the odd term in X_i being on the right or left,

(2) the *vertical orientation vector* $V = [v_0, v_1, \ldots, v_{m-1}]$, where $v_i = 0$ or 1 for the odd term being on the top or bottom,

(3) the *sign vector* $S = [s_0, s_1, \ldots, s_{m-1}]$, where $s_i = 1$ or -1 according to the sign of X_i. An equivalent formulation is as a binary vector $B_s = [b_0, b_1, \ldots, b_{m-1}]$, where $b_i = \frac{1}{2}(s_i + 1)$.

Multiplication of quads is defined by

$$\begin{aligned} XY &= \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} \begin{bmatrix} y_1 & y_2 \\ y_3 & y_4 \end{bmatrix} \\ &= \frac{1}{4}\left(x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4\right). \end{aligned}$$

Divisibility by 4 follows from the above proposition. This is really an inner product and not to be confused with matrix multiplication. With this interpretation, the autocorrelation conditions become:

$$\begin{aligned} X_0X_1^* &= 0, \\ X_0X_2^* &= 0, \\ X_0X_3^* + X_1X_2^* &= 0, \\ &\cdots \\ X_0X_{m-1}^* + X_1X_{m-2}^* + X_2X_{m-3}^* + \cdots + X_{m-1}X_0^* &= 0, \\ X_0X_{m-1} + X_1X_{m-1}^* + X_3X_{m-2}^* + \cdots + X_{m-2}X_0^* &= 0, \\ X_0X_{m-2} + X_1X_{m-1} + X_3X_{m-1}^* + \cdots + X_{m-3}X_0^* &= 0, \\ &\cdots \\ X_0X_2 + X_1X_3 + \cdots + X_{m-3}X_{m-1} + X_{m-2}X_{m-1}^* &= 0, \\ X_0X_1 + X_1X_2 + \cdots + X_{m-3}X_{m-2} + X_{m-2}X_{m-1} &= 0. \end{aligned}$$

We obtain the following multiplication table for basic quads:

	P	P^*	Q	Q^*
P	1	0	0	0
P^*	0	1	0	0
Q	0	0	1	0
Q^*	0	0	0	1

which is extended by $(-X)Y = X(-Y) = -XY$.

Reduction molulo 2. All of the nonzero products obtained by multiplying quads are ± 1. Reducing modulo 2, we derive the following:

$$X_iX_j \equiv (1 + v_i + v_j)(1 + h_i + h_j),$$
$$X_iX_j^* \equiv (1 + v_i + v_j)(h_i + h_j).$$

After specifying the value of either the H or V vector, the autocorrelation equations become linear in the coordinates of the other orientation vector by reducing modulo 2 ($2^{\frac{n}{2}}$ search, Andres, 1977).

Reduction modulo 4 (again). We note now that

$$X_i X_j = s_i s_j \left[X_i X_j \pmod 2\right].$$

Once the values of H and V are set, we are left with a quadratic system in the components of S, the sign vector.

Reducing modulo 4 converts this to a linear system. The final search is no more than exponential in the number of free variables of this system.

Further reductions. In cases where these numbers of free variables are large in relation to n, further reduction modulo 2 or 4 may be made to narrow the search. This can be applied to known solutions for H and V obtained in the reduction molulo 2 for larger values of n.

3. Equivalence

Each of the six operations establishing equivalence classes of Golay pairs is of order 2. Together they generate a noncommutative group of order 64. In his 1998 paper, Djokovic [4] outlined a method for choosing a canonical representative from each class. For our purposes, we need to describe the effects of these operations on the H-, V- and S-vectors, leading, as well, to the determination of a canonical representative, though our choice varies slightly. The operations are as follows:

(1) Interchanging the sequences, defined by $\tau(A, B) = (B, A)$. This transforms all quads of P-type into Q-type and vice versa. The binary entries of the vertical orientation vector V are complemented without changing the H- or S-vectors.

(2) Reversing the first sequence A, defined by $\rho_Q(A, B) = (A^*, B)$. This exchanges the columns for any quad of Q-type, while leaving those of P-type unchanged; e.g., $\rho_Q(Q) = Q^*$ and $\rho_Q(P) = P$. The H-vector is changed by the addition of the complement of the V-vector modulo 2.

(3) Reversing the second sequence B, defined by $\rho_P(A, B) = (A, B^*)$. The quads of P-type are reversed; those of Q-type remain fixed. The H-vector is changed by the addition of the V-vector modulo 2.

(4) Changing the signs of the first sequence, defined by $\sigma_1(A, B) = (-A, B)$. Quads of Q-type are reversed, i.e., $\sigma_1(Q) = Q^*$. Quads of P-type are reversed and also change sign, i.e., $\sigma_1(P) = -P^*$. Thus, the H-vector is complemented; the B_s-vector is changed by the addition of the H-vector modulo 2.

(5) Changing the signs of the second sequence, σ_2. Here $\sigma_2(A, B) = (A, -B)$. Quads of P-type are reversed; quads of Q-type are reversed and change sign. The H-vector is complemented; the B_s-vector is changed by the addition of the complement of the H-vector modulo 2.

(6) Changing the signs of alternate entries in both sequences, denoted by σ_a. In the polynomial representation, we choose $\sigma_a(A(x), B(x)) = (A(-x), B(-x))$, specifying that σ_a changes the sign of entries in even positions. The effect on quads, then, depends on whether their positions are even or odd. In odd position, $\sigma_a(P) = Q$, $\sigma_a(P^*) = -Q^*$. In even position, $\sigma_a(P) = -Q$, $\sigma_a(P^*) = Q^*$. The vertical orientation vector V is complemented and entries in B_s are changed as well. The signs which change are determined by finding the sum of the vector

$[0,1,0,1,\ldots]$ (every second entry 1) and the H-vector modulo 2. We add this to B_s modulo 2 to obtain the new sign vector.

Golay pairs which are in a common orbit for this group, i.e., are interchangeable through successive operations from this group, we call *conjugates*. Already, we have one test which is a necessary property for conjugates.

Lemma 3.1. *If two series are conjugates, then their V-vectors are either identical or complementary.*

Proof. This is true for each operation in the generating set. □

We will redefine a generating set for the equivalence group, to better align them with the P/Q split of the quad sequence. We define $\sigma_P = \rho_P\rho_Q\sigma_1$ and $\sigma_Q = \rho_P\rho_Q\sigma_2$. The effect of σ_P is to change the signs of all the P-type quads. This changes the S-vector by adding the V-vector mod 2. Here σ_Q changes the signs of all the Q-type quads. This changes the S-vector by adding the complement of the V-vector mod 2. Thus, through conjugation, we are able to reverse the direction or change the sign of either the P- or Q-type quads independently.

The new generating set is $\{\tau, \rho_P, \rho_Q, \sigma_P, \sigma_Q, \sigma_a\}$, where now the first five operations listed commute. These enable the first steps in choosing the canonical representative from each set of conjugates. Specifically, for a canonical pair:

(1) The first quad will be of type P and will have right orientation and positive sign, i.e., $X_0 = P$.

(2) The first quad of Q-type in the series will also have right orientation and positive sign, i.e., the first quad of Q-type will be Q.

Through conjugation, there are eight possible choices for the first quad. The subgroup of the conjugation group fixing the first quad at P must have order eight as well. The only case where the quads have the same vertical orientation is where $n = 2$, i.e., the series consists of a single quad. This has eight conjugates. The autocorrelation conditions force longer sequences to have quads of both P- and Q-type. With the first quad fixed at P, there are now four options for the first quad of type Q, all attainable through conjugation. Thus, any Golay pair of length greater than 2 will have at least the 32 distinct conjugates obtainable using the first five operations of our generating set. There will be 64 conjugates if and only if the subgroup fixing the quads described in (1) and (2) has index 2.

Any additional conjugates are obtained using σ_a. The operator $\rho_P\rho_Q\tau\sigma_a$ changes only the sign vector B_s by adding $B_a = H + [0,1,0,1,\ldots]$ modulo 2. There are two cases to consider, depending on whether the position for the first Q in the quad sequence is even or odd. We define $\sigma_{A_1} = \rho_P\rho_Q\tau\sigma_a$ and $\sigma_{A_2} = \sigma_Q\rho_P\rho_Q\tau\sigma_a = \sigma_2\tau\sigma_a$. The first changes signs, adding $B_A = B_a$ to B_s; the second changes signs, adding $B_A = B_a + V^c$ to B_s, where V^c is the complement of V. To leave the first Q fixed, we set $\sigma_A = \sigma_{A_1}$ if this Q occurs in odd position and $\sigma_A = \sigma_{A_2}$, otherwise. If $\sigma_A \neq id$, then there are 64 conjugates.

These considerations lead us to the final condition for a canonical pair:

(3) The sign of the quad corresponding to the first nonzero entry in S_A will be positive.

If, after (1) and (2), the sign of this quad is negative, we change B_s by adding B_A (mod 2).

Using equivalences. In conducting an exhaustive search, we are able to restrict ourselves to locating a canonical representative of each equivalence class. In the

reduction modulo 2, we have a choice of specifying either the H- or V-vectors. Specifying that $X_0 = P$ sets $h_0 = 0, v_0 = 1, b_0 = 1$, leaving $\frac{n}{2} - 1$ values to be set in either case ($2^{\frac{n}{2}-1}$ search, Andres [1]). Specifying the first quad of Q-type to be Q itself narrows the search further, but its full effect is not immediately apparent. Our algorithm starts by supplying values for the H-vector. An initial consequence is the following, allowing a $2^{\frac{n}{2}-2}$ search, in line with Eliahou, Kervaire, and Saffari [5]:

Lemma 3.2. *For a canonical pair:*
(i) $h_1 = 0$,
(ii) $b_1 = 1$.

Proof. (i) We have

$$X_0X_1 \equiv (1 + v_0 + v_1)(h_0 + h_1) \equiv v_1h_1 \equiv 0 \pmod 2.$$

$h_1 = 1$ would imply that $v_1 = 0$, giving the first quad of Q-type to be Q^*, not Q as specified.

(ii) $v_1 = 0$ would mean the second quad is of Q-type and $b_1 = 1$ by specification. Otherwise, the B_A-vector given above would have the value 1 in the second position, so that again $b_1 = 1$. □

The implications have not yet been exhausted, however. For example, $h_0 = h_1 = h_3 = 0,\ h_2 = 1$ is also inconsistent, so another 1/4 of the cases can be eliminated. Its effect is progressive in the length of the sequences. The above lemma could be extended again and again. However, a test routine in the search program takes care of this. There are blocks of cases to be eliminated during run time, so that at $n = 82$, about 7/8 of the cases are "stepped over" ($2^{\frac{n}{2}-5}$ search).

The final specification, induced either by σ_A if it is not the identity or by setting the sign of the first Q-quad if this has not been used in the lemma, can be applied in the reduction modulo 4 to reduce the number of free variables is solving for the sign vector.

4. Composition

A pair of multivariate functions $(F(x_1, x_2, \ldots, x_n), G(x_1, x_2, \ldots, x_n))$ is *complementary* if

$$F(x_1, x_2, \ldots, x_n)\, F(x_1^{-1}, x_2^{-1}, \ldots, x_n^{-1}) + G(x_1, x_2, \ldots, x_n)\, G(x_1^{-1}, x_2^{-1}, \ldots, x_n^{-1})$$

is the constant function.

A pair of sequences (A, B) is complementary if and only if the functions $(A(x), B(x))$ are complementary. We easily see that (A, B) complementary implies that each of $(A(x^k), B(x^k))$, $(A(x), B(x)x^k)$ and $(\alpha A(x), \alpha B(x))$ are complementary for any numbers k and α. We may use the following theorem to obtain combinations of pairs.

Theorem 4.1. *Suppose each of the pairs $(C(r), D(r))$ and $(A(s), B(s))$ is complementary. Then the pair*

$$F(r, s, t, u) = C(r)A(s) + D(r^{-1})B(s)t,$$
$$G(r, s, t, u) = (D(r)A(s) - C(r^{-1})B(s)t)u$$

is complementary.

Proof. Substituting, we find that

$$F(r,s,t,u)F(r^{-1},s^{-1},t^{-1},u^{-1}) + G(r,s,t,u)G(r^{-1},s^{-1},t^{-1},u^{-1})$$

simplifies to

$$\left(C(r)C(r^{-1}) + D(r)D(r^{-1})\right)\left(A(s)A(s^{-1}) + B(s)B(s^{-1})\right),$$

which is constant by our hypothesis. □

A simple application where (A,B) is complementary and $C(r) = D(r) = t = u = 1$ shows that $(A+B, A-B)$ is complementary. By making other apppropriate substitutions, we obtain the following construction due to Turyn:

Corollary 4.2 (Turyn [11], 1974)**.** *Where (C,D) and (A,B) are Golay pairs of lengths m and n, respectively, the combination*

$$C(x^n)(A(x)+B(x))/2 + D^*(x^{-n})(A(x)-B(x))/2,$$
$$D(x^n)(A(x)+B(x))/2 - C^*(x^{-n})(A(x)-B(x))/2$$

is a Golay pair.

Proof. Starting with the complementary pairs $(C(r), D(r))$ and $((A(s)+B(s))/2, (A(s)-B(s))/2)$, we apply the theorem using the substitutons $r \to x^n$, $s \to x$, $t \to x^{(m-1)n}, u \to 1$. The coefficients in the expansion are ± 1, yielding a Golay pair of length mn. □

Remark. Adapting to $(C(r), D^*(r))$ and $(A(s), B(s))$, the substitutions $r \to x^n$, $s \to x$, $z \to x^{(m-1)n}, w \to x^{mn}$ generate the Golay pairs

$$C(x^n)A(x) + D(x^n)B(x)x^{mn},\quad D^*(x^n)A(x) - C^*(x^n)B(x)x^{mn} \quad \text{and} \quad C(x^{2n})A(x^2) + D(x^{2n})B(x^2)x,\quad D^*(x^{2n})A(x^2) - C^*(x^{2n})B(x^2)x.$$

These are Golay's contructions [7], yielding pairs of length $2mn$. These are derivable using Turyn's construction combined with equivalences. For example, combining Golay pairs $([1,1],[1,-1])$ and (C,D), we obtain the Golay pair $(x^m d(x) + C(x),\ x^m D(x) - C(x))$. We apply equivalence operations to obtain $(x^m D(x) + C(x),\ x^m C^*(x) + D^*(x))$. Combining now with (A,B) and simplifying, we obtain $(C(x^n)A(x) + D(x^n) + D(x^n)B(x)x^{mn},\ -D^*(x^n)A(x) + C^*(x^n)B(x)x^{mn})$.

Using only Turyn's multiplicative construction and equivalences is insufficient to give a good classification for Golay pairs of increasing length. Djokovic [4], for example, lists two sequences at length 16 and 44 at length 32 as being nonconstructible. In fact, these are derivable using a procedure for lengths of the form 2^k which is outlined in Golay's 1961 paper [7]. Starting from Golay pairs, Turyn's construction produces Golay pairs with coefficients ± 1. We obtain more flexibility if at each stage we stipulate only that complementary pairs be produced at intermediate stages, without demanding that all entries be ± 1. In the process described below, the extension is to allow entries $0, \pm 1$ at intermediate stages.

To conveniently identify the pairs which may be derived from a pair (A,B) through successive combinations, we use the following matrix notation. To compose the sequence identified through the notation

$$\begin{bmatrix} A & B & A & B \\ A & -B & -A & B \\ -B^* & A^* & -B^* & A^* \\ -B^* & -A^* & B^* & A^* \end{bmatrix},$$

we form series by interleaving elements of series running down the rows and we juxtapose these resulting series running across the columns. Thus, this gives a representation for the series

$$a_1, a_1, -b_n, -b_n, a_2, \ldots, b_1, -b_1, a_n, -a_n, \ldots, a_1, -a_1, \ldots, b_1, b_1, \ldots, b_n, b_n, a_1, a_1$$

of length $16n$. The number of rows determines the separation between entries in A or B as they appear in the sequences.

Let (A, B) be a Golay pair of length n, and let O be a sequence of length n consisting of 0's. There are two basic processes of combination for forming pairs of length $2n$ that involve adding and subtracting the component series after displacement or separation of their entries:

(1) Golay's first construction, $(\begin{bmatrix} A & B \end{bmatrix}, \begin{bmatrix} A & -B \end{bmatrix})$, involves addition and subtraction of the complementary series $(\begin{bmatrix} A & O \end{bmatrix}, \begin{bmatrix} O & B \end{bmatrix})$. This is the same up to equivalences as that obtained from Turyn's construction using pairs $(C = [1, 1], D = [1, -1])$ and (A, B).

(2) Golay's second construction

$$\left(\begin{bmatrix} A \\ B \end{bmatrix}, \begin{bmatrix} A \\ -B \end{bmatrix} \right),$$

involves addition and subtraction of the complementary series

$$\left(\begin{bmatrix} A \\ O \end{bmatrix}, \begin{bmatrix} O \\ B \end{bmatrix} \right).$$

This is equivalent to Turyn's construction using (A, B) and $([1, 1], [1, -1])$, with their order now reversed.

These processes of (1) juxtaposition and (2) interleaving in terms of matrix addition and subtraction are generalized to produce Golay pairs of length $2^k n$. We start with a pair of $2^{k_1} \times 2^{k_2}$ matrices with $k_1 + k_2 = k$. The first matrix has all O entries except for a single entry A and represents a sequence of length $2^k n$ having the A entries 2^{k_1} positions apart with 0's elsewhere. The second has O's except for a single B. These represent a complementary pair. If we are able to add and subtract appropriately k times so that the resulting matrices have only A and B entries, the corresponding series will form a Golay pair. This motivates the following inductive process:

(i) We start with A in the $(1, 1)$ position in the first matrix and B either in the $(2^i + 1, 1)$ or $(1, 2^j + 1)$ position in the second matrix, where $1 \le i < k_1$, $1 \le j < k_2$. Adding and subtracting these matrices yields a complementary pair.

(ii) The matrices in pair, (M_1, M_2), entered at a succeeding step have nonzero sequences in the $(1, 1)$ position. Consider the smallest submatrix of M_2 such that all entries outside consist of O's. However we translate this submatrix within this second matrix, keeping O entries outside, the sequences represented remain complementary. This translation is done to place the nonzero entry in the upper left corner of this submatrix in either the $(2^i + 1, 1)$ or $(1, 2^j + 1)$ position in the second matrix, where $1 \le i < k_1$, $1 \le j < k_2$, and where this entry is O in the first matrix. Where M_2' is the matrix formed by this internal translation, we form the two new pairs $(M_1 + M_2', M_1 - M_2')$ and $(M_1 + M_2', -M_1 + M_2')$, each of which represents a complementary pair.

This process is reversible. Adding and subtracting in the same order, and then dividing by 2, we obtain (M_1, M_2') and (M_2', M_1), respectively, from these two pairs.

Only M_1 has a nonzero entry in the $(1,1)$ position. Taking this as the first choice, i.e., (M_1, M_2'), re-establishes the original order. In this fashion, we may trace the process back to the original pair (A,B). Hence, each conjugate of (A,B) produces a different set of matrices.

Lemma 4.3. *The matrices formed after k steps in the above inductive process represent a Golay pair.*

Proof. From the entries in a matrix produced at the k'th step we compose a polynomial $f_{k'}(x,y)$, where the coefficient of the term $x^{i-1}y^{j-1}$ represents the number of copies of A or B added or subtracted to obtain the (i,j)th entry in this matrix. Thus

(i) $f_1(x,y) = 1 + x^{2^i}$ if B is placed in the $(2^i+1,1)$th position or $1+y^{2^j}$ if B is placed in the $(1,2^j+1)$th position during the first step.

(ii) Before adding or subtracting at the k'th step, the polynomial for the first matrix is $f_{k'-1}(x,y)$. The second matrix, after translation, has either the polynomial $f_{k'-1}x^{2^i}$, giving $f_{k'}(x,y) = f_{k'-1}(x,y)(1+x^{2^i})$, or the polynomial $f_{k'-1}y^{2^j}$, giving $f_{k'}(x,y) = f_{k'-1}(x,y)(1+y^{2^j})$.

In running through the allowable values for i and j in the k steps, we obtain

$$\begin{aligned} f_k(x,y) &= \prod_{i=0}^{k_1-1}\prod_{j=0}^{k_2-1}(1+x^{2^i})(1+y^{2^j}) \\ &= (1+x+\cdots+x^{2^{k_1}-1})(1+y+\cdots+y^{2^{k_2}-1}). \end{aligned}$$

The term corresponding to each position in the final matrix has coefficient 1 so that each entry in this matrix is one of $A, -A, B, -B$. Therefore, the final sequences have only the entries ± 1 and are Golay pairs. □

Completing equivalence classes. As stated above, the pairs generated by different conjugates compose distinct classes. However, conjugation is not an operation confined to classes. For example, the pair $([A\ B],[A\ -B])$ belongs to the class generated by (A,B) while its conjugate $([-A\ -B],[A\ -B])$ belongs to the class generated by $(-A,-B)$. This leads to difficulty in comparing lists of canonical pairs generated by a search program to pairs generated by composition. This may be reconciled by comparing total counts or by eliminating derivable pairs from the search.

We still need, however, to see if conjugation at longer lengths will increase the numbers of derivable pairs:

(1) *Changing order*: We see that

$$(M_1 - M_2', M_1 + M_2') = (M_1 + (-M_2'), M_1 - (-M_2'))$$

is produced from the pair $(M_1, -M_2)$, a conjugate at the previous step. The same is true for $(M_1 + M_2', -M_1 + M_2')$.

(2) *Changing signs*: Changing the sign of the second pair has been included. Changing the sign of the first, e.g.,

$$(-M_1 - M_2', M_1 - M_2') = ((-M_1) + (-M_2'), -(-M_1) + (-M_2')),$$

is covered by conjugation at the previous step. Changing even positioned signs depends upon the positioning of M_2'. Even positioned signs in M_1 are changed but for M_2' the signs changed may be either in the even or odd positions. Both cases are covered by conjugation at the previous step.

(3) *Reversing the order of a sequence*: We denote by M^* this operation applied to a component matrix M. It is achieved by rotating M a half turn and reversing the order of all its entries. We may have to expand our inductive process to include this operation on the second sequence. Once this is done, application to the first sequence produces no new pairs. For example,

$$(M_1^* + M_2'^*, M_1 - M_2') = (M_1^* + M_2'^*, (M_1^* - M_2'^*)^*)$$

is achieved by combining conjugation at the previous step with reversal of the second sequence.

We see below that it can be applied at most once in the derivation of a particular pair. At each step, therefore, there is a separation into two classes of complementary pairs.

Lemma 4.4. *If reversal of the second sequence has been applied at one step of the inductive process, its later application is equivalent to conjugation at earlier steps.*

Proof. Let $(M_1 + M_2', M_1 - M_2')$ be a pair produced in the inductive process, where reversal of the second sequence has been applied at an earlier step. This is equivalent to the polynomial form $\big(M_1(x) + M_2(x)x^{k_1}, M_1(x) - M_2(x)x^{k_1}\big)$, where k_1 is some power of 2. Our inductive assumption is that the pair (M_1, M_2^*) is derivable from a previous pair (M_3, M_4), i.e., $M_1(x) = M_3(x) + M_4(x)x^{k_2}$, $M_2^*(x) = M_3(x) - M_4(x)x^{k_2}$, either because the reversal was applied at this step or by extension of the assumption. Our claim is that the pair $(M_1 + M_2', M_1^* - M_2'^*)$ is derivable from the pair $(M_3, -M_4^*)$ with one reversal in the intermediate step.

Indeed, the polynomial representation of $(M_1 + M_2', M_1^* - M_2'^*)$ is

$$\begin{pmatrix} M_1(x) + M_2(x)x^{k_1}, \\ M_1^*(x)x^{k_1} - M_2^*(x) \end{pmatrix} = \begin{pmatrix} M_3(x) + M_4(x)x^{k_2} + \big(M_3^*(x)x^{k_2} - M_4^*(x)\big)\, x^{k_1}, \\ \big(M_3^*(x)x^{k_2} + M_4^*(x)\big)\, x^{k_1} - \big(M_3(x) - M_4(x)x^{k_2}\big) \end{pmatrix}.$$

The other derivation is

$$\begin{pmatrix} M_3(x) - M_4^*(x)x^{k_1}, \\ M_3(x) + M_4^*(x)x^{k_1} \end{pmatrix} \rightarrow \begin{pmatrix} M_3(x) - M_4^*(x)x^{k_1}, \\ M_3^*(x)x^{k_1} + M_4(x) \end{pmatrix}$$
$$\rightarrow \begin{pmatrix} M_3(x) - M_4^*(x)x^{k_1} + \big(M_3^*(x)x^{k_1} + M_4(x)\big)\, x^{k_2}, \\ -M_3(x) + M_4^*(x)x^{k_1} + \big(M_3^*(x)x^{k_1} + M_4(x)\big)\, x^{k_2} \end{pmatrix}.$$

The final pairs are the same. The proof is similar for the pair $(M_1 + M_2', -M_1 + M_2')$. □

Pairs of length 2^k. We consider Golay pairs which are derivable from the pair $(A = [1], B = [1])$. This has four conjugates corresponding to changes in signs. All derivable pairs are representable by single row matrices. At length 2, we derive the pairs $([1\ 1], [1\ -1])$ and $([1\ 1], [-1\ 1])$. Using the four equivalences on the initial pair (A, B) will then generate the eight pairs of length 2.

At this first step no new pairs are obtained by reversing the second sequence. By the lemma, no new pairs will be produced by reversal of the second sequence in a pair at any later step.

This is extendable to the following theorem.

Theorem 4.5 (Golay [7], [3])**.** *Using the above inductive process, there are exactly $2^{k+2}k!$ Golay pairs of length 2^k derivable from the initial pair $([1], [1])$.*

Proof. In the operations to form a pair of length 2^k, there are k positions for placing the first nonzero entry in the second matrix, namely, $2^0+1, 2^1+1, \ldots, 2^{k-1}+1$. There are $k!$ choices for the order in which these are chosen. At each step we may independently choose the order of addition and subtraction at each step, giving an additional 2^k choices. Independently again we may apply the four equivalences of the original pair to form a total of $2^{k+2}k!$ Golay pairs at length 2^k. □

Pairs of length $2^k n$. Let (A, B) be a primitive pair of length greater than 1. The entries in a pair $(M_1 + M_2', \pm(M_1 - M_2'))$ produced at the k'th step are the same except for signs. Where there has been no reversal in the process, the $(1,1)$ entries in these matrices will be $\pm A$. The smallest submatrix of the second matrix containing all the non-O entries will have $\pm B$ in its bottom right corner. Reversing the order of the second sequence and repositioning this submatrix so that this (now) B^* entry is in the $(1,1)$ position, we have the following:

(1) With $n > 1$, we have $A \neq \pm B^*$, so that entries in the two matrices no longer match up in sign. Hence, this reversal has, in fact, produced a different pair.

(2) Each of these matrices is seen, inductively, to retain the same function $f_{k'}(x, y)$ described in a previous lemma. Thus, the non-O entries in the two matrices are in the same positions and the inductive process can continue. This allows the following derivation:

Theorem 4.6. *From a primitive Golay pair of length n having 64 conjugates, there are exactly $2^{k+6}(k+1)(k+1)!$ pairs derivable at length $2^k n$.*

Proof. There are $k+1$ choices for the dimensions $2^{k_1} \times 2^{k-k_1}$ of a matrix, with $0 \leq k_1 \leq k$. There are the same k positions for placing the first nonzero entry in the second matrix, and therefore $k!$ choices for the order in which these are chosen. With no reversals of the second sequence, we produce $2^k(k+1)k!$ Golay pairs from an initial pair. There are k steps at which this reversal can occur to generate new pairs, each reversal producing $2^k(k+1)k!$ more pairs, for a total count of $2^k(k+1)k! + k(2^k(k+1)k!) = 2^k(k+1)(k+1)!$ from the initial pair. From the 2^6 conjugates of the initial pair we obtain the final count. □

Remark. We note that after the $k-1$ step we have produced matrices where either blocks of 2^i rows which have no O entries are interspersed with blocks of 2^i rows of all O's or we have the corresponding configurations with blocks of 2^j columns. Deleting all the O entries will reduce the matrices to having 2^{k-1} entries each. We can generate these matrices by the same inductive process starting from matrices of these new dimensions. Hence, this deletion produces Golay pairs. This permits the following interpretation of the inductive process, where after each step Golay pairs of double the length are produced.

(i) Starting with the matrices $([A], [B])$, we either add O-rows to produce the pairs

$$\left(\begin{bmatrix} A \\ O \end{bmatrix}, \begin{bmatrix} O \\ B \end{bmatrix} \right)$$

or O-columns to produce $(\begin{bmatrix} A & O \end{bmatrix}, \begin{bmatrix} O & B \end{bmatrix})$. Adding and subtracting produce Golay pairs of length $2n$.

(ii) The k'th step begins with two $2^{k_1} \times 2^{k_2}$ matrices M_1, M_2 with $A, -A, B, -B$ entries where $k_1 + k_2 = k' - 1$. We may either form $2^{k_1+1} \times 2^{k_2}$ matrices, the first by taking successive blocks of 2^{k_3} rows from M_1 followed by blocks of 2^{k_3} rows of

O's, the second by taking blocks of 2^{k_3} rows of O's followed by successive blocks of 2^{k_3} rows from M_2, where $0 \le k_3 \le k_1$, or we may form $2^{k_1} \times 2^{k_2+1}$ matrices in the same manner by inserting O-columns appropriately. Adding and subtracting yield Golay pairs of length $2^{k'}n$.

5. H-REGULARITY

A Golay pair A, B is *H-regular* (of period $2k$) if the pair is composed of blocks of length k where the entries in A and B are the same interspersed with blocks of length k where they are different.

Note that for such a pair the H-vector consists of alternating blocks of 0's and 1's, each of length k. The regularity of this vector is not quite equivalent to H-regularity. However, if we extend this vector by its mirror image, the 0 entries indicate positions where A and B agree and the 1 entries indicate positions where they disagree. Regularity of this vector is equivalent to H-regularity of the pair.

H-regularity is invariant under reversal of signs in one or both sequences in the pair or under reversal of direction of both sequences.

Examples. The pair

$$\begin{aligned} A &= [1, \quad 1, \quad 1, \quad 1, \quad 1, -1, \quad 1, -1, -1, \quad 1, \quad 1, -1, -1, -1, \quad 1, \quad 1], \\ B &= [1, \quad 1, \quad 1, \quad 1, -1, \quad 1, -1, \quad 1, -1, \quad 1, \quad 1, -1, \quad 1, \quad 1, -1, -1] \end{aligned}$$

is H-regular with period 8. It has H-vector $[0, 0, 0, 0, 1, 1, 1, 1]$.

The pair

$$\begin{aligned} A &= [1, \quad 1, \quad 1, \quad 1, \quad 1, -1, \quad 1, -1, -1, \quad 1], \\ B &= [1, \quad 1, -1, -1, \quad 1, \quad 1, \quad 1, -1, \quad 1, -1] \end{aligned}$$

is not H-regular. Its H-vector is $[0, 0, 1, 1, 0]$. This extends to

$$[0, 0, 1, 1, 0, 1, 0, 0, 1, 1],$$

which we see is not regular.

Theorem 5.1. *Let A, B be a Golay pair of length n. If A, B or A, B^* is H-regular, then A, B is derivable from a Golay pair of length $n/2$.*

Proof. Suppose A, B is H-regular of period $2k$. Then $C = (A + B)/2$ and $D = (A - B)/2$ are complementary, each having blocks of consecutive indices of length k for which values are ± 1 interspersed with blocks of length k for which the values are 0. Removing the 0's, we obtain two sequences, $C' = [c'_1, c'_2, \ldots, c'_{n/2}]$ and $D = [d'_1, d'_2, \ldots, d'_{n/2}]$. Consider the jth autocorrelation coefficients $\sum_{i=1}^{n/2-j} c'_i c'_{i+j}$ for C and $\sum_{i=1}^{n/2-j} d_i d_{i+j}$ for D.

Let $j = sk + j'$, where $0 \le j < k$. If c'_i comes from an entry in C at the beginning of a nonzero block in $(A+B)/2$, then c'_{i+j} will come from the entry $2sk+j'$ positions ahead. When c'_i comes from a later entry in a nonzero block, then c'_{i+j} will come from the entry which is $2sk + j'$ positions ahead if this is nonzero, and from the entry $(2s + 1)k + j'$ positions ahead otherwise. We obtain

$$\sum_{i=1}^{n/2-j} c'_i c'_{i+j} = \sum_{i=1}^{n-(2sk+j')} c_i c_{i+2sk+j'} + \sum_{i=1}^{n-((2s+1)k+j')} c_i c_{i+(2s+1)k+j'}.$$

The contributions to the sums on the right not coming from terms on the left are all 0. Each autocorrelation coefficient for C' is the sum of two autocorrelation

coefficients for C. In the same way, each autocorrelation coefficient for D' is the sum of two corresponding autocorrelation coefficients for D. So C' and D' inherit the defining autocorrelation conditions from C and D and are Golay pairs. □

In the sense of derivability outlined in the previous section we have:

Corollary 5.2. *Let (A, B) be a Golay pair of length not divisible by a product mn, where m and n are not powers of 2 but are the lengths of existing Golay pairs. (A, B) is derivable if and only if it or one of its conjugates is H-regular.*

Proof. Suppose the length of (A, B) is of the form $2^k m$, where m is the length of some smaller Golay pair. A pair derived from the process outlined in the last section without reversal of the second sequence at the final step is H-regular. Hence, if (A, B) is derivable either it or its conjugate obtained by reversing the second sequence is H-regular. □

Combining results from searches conducted at allowable lengths under 100 with those from applying the composition process, we are able to make the following summary:

Theorem 5.3. *For lengths $n < 100$, all Golay pairs are derivable from the following five primitive pairs (in canonical form):*

Length 1: $([1], [1])$.
Length 10: $[P, P, -P, Q, Q^*]$ *and* $[P, Q, -Q^*, P^*, Q]$.
Length 20: $[P, Q, Q, P, -P, P, Q^*, -P^*, -P^*, P]$.
Length 26: $[P, P, P, Q, -P, P, P, -Q, -P, P, -P, Q, Q^*]$.

Proof. Previous searches were conducted by Andres [1] (lengths 8, 16, 20, 26, 32, 34, 50, 58), James [9] (length 68), Djokovic [4] (lengths 32, 40). Our own searches were conducted at all allowable lengths under 100, confirming previous results and extending these at lengths 52, 64, 74, 80 and 82. The four pairs listed for lengths 10, 20, 26 above are the only canonical pairs of length less than 100 for which no conjugate is H-regular. At lengths 8, 16, 20, 26, 32, 40, 52 and 64, all canonical pairs were found during the searches. Our search at length 80 was restricted to finding canonical pairs for which no conjugate is H-regular. □

6. The Algorithm

The search program is written in C. A bit vector is used to specify H, using 32 bit integers for lengths $n \leq 64$ and 64 bit integers for lengths $64 < n \leq 128$. The run time, even at $n = 100$, however, becomes excessive.

Reduction modulo 2. Matrices are set up as bit arrays, each autocorrelation equation supplying a row bit vector of coefficients of variables v_i in V. A set of matices is composed for each bit of H, corresponding to its contribution to the set of equations. Using a Gray code for H allows the matrix of coefficients to be updated by addition of the single set of these matrices corresponding to the bit change. This matrix is kept separate from the matrix used in the reduction, rows being transferred in order as required.

The higher order bits in the H-bit vector correspond to the lower index values $h_0, h_1, h_2, \ldots$. Then, with $h_0 = h_1 = 0$, the first nonzero autocorrelation equation becomes

$$X_0 X_2 \equiv (1 + h_2) v_2 \equiv 0 \pmod 2.$$

The next $m-3$ equations introduce the variables $h_3, h_4, \ldots, h_{m-1}$ successively. In updating the Gray code, we change the lowest order bit possible, so that the fewest number of equations are affected. Rows are not interchanged in the matrix reduction. Instead, a list of the nonzero rows and the pivot variables associated with each is maintained as a bit vector as the matrix reduction proceeds. Forward substitution is performed on updated rows as they are introduced.

The lowest order bit in each row vector corresponds to the constant term. Inconsistency in the set of equations is recognized, therefore, by an integer value of 1, and further reduction is abandoned for this H value.

If the row is consistent and nonzero, the pivot variable chosen has the lowest index. By saving the partial reductions, we are able to begin an updated matrix reduction at the first equation changed.

An inconsistency in the first $m-2$ equations, implies inconsistency for a block of H values, allowing the Gray code for H to be updated so that these values are overstepped. This can be incorporated into the algorithm, but, in practice, this does not seem to occur. Specifying that the first i for which $v_i = 0$ (the first Q) has $h_i = 0$, does bring about such economies.

When a bit in the Gray code is changed, setting a value for an entry h_i, we want to be able to solve for each value $v_1, v_2, \ldots, v_{m-1}$ as soon as this is possible. This requires updating a set of back substitution matrices for each equation. We look for a solved string $v_1, v_2, \ldots, v_j$ for which v_j is the first 0. If h_j is set at 0, the system is inconsistent. If this occurs in the first $m-2$ equations, it means that the beginning entries in H are inconsistent, down to the entry introduced for the first time at this equation. This means inconsistency for a block of H values and the Gray code is updated accordingly.

Back substitution is performed after all equations are reduced. After the free variables are isolated, each set of their possible values will provide a solution in this reduction.

Solutions where $4 \nmid n$. The program runs most smoothly for lengths not divisible by 4. In these cases, the number of solutions to this first linear system is quite small, with no free variables being found:

n	# of solutions to 1st system
10	2
26	9
34	11
50	14
58	32
74	43
82	38

There are two patterns recurring in the solutions at each of these lengths, namely,

$$H = [0,0,0,0,0,0,0,0,\ldots,0,0,0,0,1],$$
$$V = [1,1,1,0,1,1,1,0,\ldots,1,1,1,0,0]$$

and

$$H = [0, 0, 1, 1, 0, 0, 1, 1, \ldots, 0, 0, 1, 1, 0],$$
$$V = [1, 0, 0, 1, 1, 0, 0, 1, \ldots, 1, 0, 0, 1, 0].$$

Both yield Golay pairs at $n = 10$. The first yields a solution at $n = 26$.

Solutions where $4|n$. We find that this first linear system:

(1) always has a solution when $h_{2i} = h_{2i+1}, 0 \le i \le m/2 - 1$,

(2) has $\frac{m}{2} - 1$ free variables when H corresponds to an H-regular pair.

From (1), the number of solutions is exponential in the length n. For most of these, the corresponding pair or a conjugate pair is H-regular. From (2), the number of solutions passing to the second stage, for any H having such a regular pattern, is exponential in the length n.

In these cases, however, any complete solution is derivable from a solution at half the length. We can treat these cases separately and include them in the search. In particular, if there is no solution at half the length, there is no need to include these cases at all. This is true for lengths 68 and 100, allowing for considerable efficiency to be included in the search at these lengths.

Reduction modulo 4. From $X_iX_j = s_is_j\,|X_iX_j|$, we have

$$X_iX_j \equiv (s_i + s_j - 1)\,|X_iX_j| \equiv (2b_i + 2b_j)\,|X_iX_j| + |X_iX_j|\,,$$
$$X_iX_j^* \equiv (2b_i + 2b_j)\,\left|X_iX_j^*\right| + \left|X_iX_j^*\right|,$$

(mod 4). The solution of the first system sets the values of each X_iX_j and $X_iX_j^*$ up to sign, with the number of nonzero values being even in each autocorrelation equation. We may therefore divide each of these equations by 2 to produce another linear system molulo 2, which may be reduced as before. Solutions from the first reduction often lead to inconsistencies at this next stage, or the number of free variables is very small, so that all cases may be tested to see if they yield Golay pairs. For the two patterns listed above where $4 \nmid n$ and in other cases where $4|n$, the number of free variables is linear in n. At $n = 82$, the numbers of free variables are 13 and 18, respectively; there is still no problem in the substitution of S values for all 2^{13} and 2^{18} cases. However, a more careful analysis reveals the relations between the signs to be quite simple. Substituting these followed by further reductions leads to an explicit solution for signs but no Golay pair for the first pattern and an inconsistency for the second pattern.

7. Search results

The result of our searches is summarized in the following table. For all lengths other than 1, 2, 4, and 80, complete lists of canonical pairs were compiled by the search program. The total numbers of pairs agree exactly with those obtained by compositions from the primitive pairs. At length 80, the search was restricted to canonical pairs for which no conjugate is H-regular. The total number of pairs is that determined by composition from the two primitive pairs at length 10 and the single primitive pair of length 20. (The superscript ^{s} indicates work done at SFU.)

Length	# of pairs	Equivalence classes	Primitive pairs
1	4	1	1
2	8	1	0
4	32	1	0
8	192	5	0
10	128	2	2
16	1536	36	0
20	1088	25	1
26	64	1	1
32	15,360	336	0
34	0	0	0
40	9728	220	0
50	0	0	0
52	512^s	12^s	0^s
58	0	0	0
64	$184,320^s$	3840^s	0^s
68	0	0	0
74	0^s	0^s	0^s
80	$102,912^s$	?	0^s
82	0^s	0^s	0^s

Running times. Following is a list of running times drawn from the literature and from our own experiments showing the evolution from the first searches to our present work:

Length	Time	Year	Reference
26	75 hrs.	1962	Jauregui [10]
26	1 min.	1977	Andres [1], [2],
58	4 mos.?		U. Manitoba
32	8 min.	1995	Djokovic [4],
40	35 hrs.		U. Waterloo
40	5 sec.	2001	SFU
58	6 min.		
74	1 day		
82	2 wks.		

8. Final notes

A partial search was conducted at $n = 100$, finding 96 canonical pairs at three separate H values. A total number of 128, matching the value suggested by previous authors using theoretical considerations, seems likely. Each has 64 conjugates. The recurring patterns indicated have been tested for lengths of the form $2p$ (prime $p \equiv 1 \pmod 4$) up to $n = 500$. The further reductions outlined for length 82 were repeated with the same results—the first pattern has an explicit solution for signs

yielding no Golay pair; the second has no solution for signs. The exact equations leading to failures are predictable.

The likelihood of finding new primitive pairs becomes more remote. Can more restrictions be identified? Complete searches using present methods for some lengths over 100 should soon be possible. Further improvements in the method may be found.

The theory of composition can be further developed. An extension of the method used for lengths of the form $2^k n$ should lead to closed forms for numbers of Golay pairs at other length combinations.

The method of repeated reductions modulo 2 and 4 may apply well in other problems where variables take only ± 1 values.

References

[1] T.H. Andres, *Some combinatorial properties of complementary sequences*, M.Sc. Thesis, University of Manitoba, Winnipeg, 1977.

[2] T.H. Andres, R.G. Stanton, *Golay Sequences*, Lecture Notes in Mathematics, **622**, 44-54, 1977. MR **57:**5380

[3] James A. Davis, Jonathan Jedwab, *Peak-to mean power control in OFDM, Golay complementary sequences and Reed-Muller codes*, IEEE Transactions on Information Theory **45**: 2397-2417, 1999.

[4] Dragomir Djokovic, *Equivalence classes and representatives of Golay sequences*, Discrete Math. **189**, 79-92, 1998. MR **99j:**94031

[5] S. Eliahou, M. Kervaire, B. Saffari, *A new restriction on the lengths of Golay complementary sequences*, J. Comb. Theory (A) **55**: 49-59, 1990. MR **91i:**11020

[6] S. Eliahou, M. Kervaire, B. Saffari, *On Golay polynomial pairs*, Adv. in Appl. Math. **12**, No. 3: 235-292, 1991. MR **93b:**68066

[7] M.J.E. Golay, *Complementary Series*, IRE Trans. Inform. Theory, **IT-7**: 82-87, 1961. MR **23:**A3096

[8] M.J.E. Golay, *Note on complementary series*, Proc. IRE: 84, Jan. 1962.

[9] M. James, *Golay sequences*, Honours Thesis, University of Sydney, 1987.

[10] Stephen Jauregui, Jr., *Complementary series of length 26*, IRE Trans. Inform. Theory, **IT-7**: 323, 1962.

[11] R.J. Turyn, *Hadamard matrices, Baumert-Hall units, four-symbol sequences, pulse compression, and surface wave encodings.* J. Combinatorial Theory Ser. (A) **16**: 313-333, 1974. MR **49:**10577

Department of Mathematics and Statistics, Simon Fraser University, Burnaby, British Columbia V5A 1S6 Canada

E-mail address: pborwein@cecm.sfu.ca

Department of Mathematics and Statistics, Simon Fraser University, Burnaby, British Columbia V5A 1S6 Canada

E-mail address: rferguson@pims.math.ca