Existence of a difference set in the last group of order 256

William Yolland
Final report of summer 2016 USRA

August 19, 2016

Abstract

The existence or non-existence of a Hadamard difference set is known for all but one of the 56,092 groups of order 2^8. We use a search method to classify the final group of order 256, namely $G = \langle x, y : x^{64} = y^4 = 1, yx = x^{-17}y\rangle$. We take the quotient of G by the normal cyclic subgroup $\langle x^{32}\rangle$ and work with a homomorphic image of the putative difference set D in $H = G/\langle x^{32}\rangle$. We represent this image as a 4×32 array whose elements lie in $\{0, 1, 2\}$. A family of potential images of D in H was provided to us at the outset of the USRA project. The problem becomes to lift the image back to G to construct the difference set. In doing so, we must determine which elements (g or gx^{32}) contributed to 1s in the image. This leads to a search of size 2^{64} for each potential image, which is computationally infeasible. However, we constrain the search by imposing structure on the image. Using a representation theoretic approach we map the generators x, y of the group G to 4×4 complex matrices of primitive 64th roots of unity so that the search for D becomes a problem of controlling the magnitude of several sums of roots of unity simultaneously. The search thereby succeeds in finding three distinct difference sets in G. Subsequently we explain these three solutions using negacyclic Golay pairs over the alphabet $\{-1, 0, 1\}$. Using this understanding we develop a recursive construction method for suitable negacyclic Golay pairs and build a difference set in G by hand, beginning with a trivial length 1 pair.

Keywords: construction, Hadamard, difference set, existence, group, representation theory, negacyclic Golay pairs

W. Yolland is with Department of Mathematics, Simon Fraser University, 8888 University Drive, Burnaby BC V5A 1S6, Canada.

Email: wyolland@sfu.ca

This research was supported by NSERC via a USRA grant held by the author and a Discovery Grant held by the author's project supervisor J. Jedwab

1 Introduction

The project to classify which of the 267 groups of order 2^6 contain difference sets was completed in 1993. The final group was classified by Robert Liebler and Ken Smith, after which an undertaking was proposed to extend this classification to all groups of order 2^8. There has since been a collective effort, using various construction methods and two non-existence theorems, to determine whether or not each of these 56,092 groups contains a difference set.

In September 2014 Jim Davis gave a talk titled "The Final Four," [2] which outlined the progress thus far and specified the final four groups for which this question was still unanswered. In March 2016 my supervisor Jonathan Jedwab attended a small workshop at which he learned that only one group remained, namely SmallGroup(256, 536) [6]. My summer project was then to classify this final group. This group closely resembles the Modular group of order 64 which was the last of the order 64 groups to be classified in 1993 by Liebler and Smith. So we approached the problem in much the same way, using representation theory and in collaboration with Jim Davis and Ken Smith.

I began this project by learning the basics of group theory along with some knowledge of representation theory and how it applies to our method. The project then evolved over the following weeks from identifying plausible constraints to reduce the size of the search space, to implementing the search and finding three solutions, to examining and understanding the solutions and finally to developing a recursive construction method for building sequences, allowing us to construct numerous Hadamard difference sets in SmallGroup(256,536) by hand.

2 Background

The group of interest to us is SmallGroup(256,536), namely

$$G = \mathbb{Z}_{64} \rtimes_{-17} \mathbb{Z}_4 = \langle x, y : x^{64} = y^4 = 1, yx = x^{-17}y \rangle$$

Definition 1. *A (v, k, λ) -* difference set *D in a group G of order v is a subset of size k which has the property that the multiset $\{xy^{-1} : x, y \in D, x \neq y\}$ contains each nonidentity element of G exactly λ times.*

For our purposes it is convenient to refer to the difference set D as an element of the group ring $\mathbb{Z}[G]$ with coefficients in $\{0, 1\}$ as follows:

$$D = \sum_{d \in D} d,$$

(where D in the summation is the subset of G and D on the left hand side is the corresponding group ring element). We define

$$D^{(-1)} = \sum_{d \in D} d^{-1},$$

and then the difference set condition becomes

$$DD^{(-1)} = (k-\lambda)\cdot 1_G + \lambda \cdot G \quad \text{in } \mathbb{Z}[G]. \tag{1}$$

A difference set D in a group of order 256 must have parameters

$$(v, k, \lambda) = (256, 120, 56) \tag{2}$$

[1, p.85, Thm 3.17], belonging to the Hadamard family of difference sets, and so satisfies

$$DD^{(-1)} = 64 \cdot 1_G + 56 \cdot G \quad \text{in } \mathbb{Z}[G].$$

We define the natural homomorphism $\rho : G \to G/\langle x^{32}\rangle = H$. This maps pairs of distinct elements g, gx^{32} in G to elements $g\langle x^{32}\rangle$ in H where

$$H \simeq \langle x, y : x^{32} = y^4 = 1, yx = x^{15}y\rangle.$$

We can also think about the image of D in H, namely $\rho(D) = D/\langle x^{32}\rangle$. Coefficients in $\rho(D)$ (viewed as an element of the group ring $\mathbb{Z}[H]$) are bounded above by $|\langle x^{32}\rangle| = 2$, and $\rho(D)$ must satisfy the condition

$$\rho(D)\rho(D)^{(-1)} = (k-\lambda)\cdot 1_H + 2\lambda \cdot H \quad \text{in } \mathbb{Z}[H].$$

With the parameters defined in (2) this becomes

$$\rho(D)\rho(D)^{(-1)} = 64 \cdot 1_H + 112 \cdot H \quad \text{in } \mathbb{Z}[H]. \tag{3}$$

Coefficients in $\rho(D)$ are in $\{0, 1, 2\}$. We can derive counts (m_0, m_1, m_2) for the number of occurrences of each coefficient in $\rho(D)$ using the following three equations:

$$m_0 + m_1 + m_2 = |H| = 128,$$

$$0 \cdot m_0 + 1 \cdot m_1 + 2 \cdot m_2 = |D| = 120,$$

$$0^2 \cdot m_0 + 1^2 \cdot m_1 + 2^2 \cdot m_2 + = 64 + 112 = 176.$$

The first two equations come directly from the definition of m_j and the parameters given in (2). The third equation is given by the coefficient of the identity element in (3): an element g in $\rho(D)$, having coefficient 1, contributes $gg^{-1} = 1$ to the identity element in (3), whereas an element $2g$ in $\rho(D)$, having coefficient 2, contributes $(g+g)(g^{-1}+g^{-1}) = 4$.

Solving these three linear equations in three unknowns gives

$$(m_0, m_1, m_2) = (36, 64, 28). \tag{4}$$

ρ is a 2-to-1 mapping, whereby each subset of 2 elements in G is mapped to a single element in H. Since elements in D have coefficients in $\{0, 1\}$, reversing the quotient map is ambiguous only for elements in $\rho(D)$ which have a coefficient of 1, as follows:

count	coefficient in $\rho(D)$		coefficient in D
36	0	$\mapsto$	$\{0,0\}$
64	1	$\mapsto$	$\{0,1\}$ or $\{1,0\}$
28	2	$\mapsto$	$\{1,1\}$

Every possible image $\rho(D)$ contains $m_1 = 64$ elements with a coefficient of 1. Given a possible image $\rho(D)$ of a difference set D in G, the size of a brute force search to determine whether any subset D of G having the image $\rho(D)$ is actually a difference set in G is therefore $2^{64} \approx 2 \times 10^{19}$.

3 Choosing a suitable image $A = \rho(D)$ in H

A family of potential images $A = \rho(D)$ in H of a difference set D in G was provided to us by Jim Davis and Ken Smith [5]. It is worth spending time examining this family, as it leads to the development of one of our later constraints. The family is generated by the following five parameter function.

$$\begin{aligned} A(g_0,&g_1, g_2, g_3, g_4) = \\ &(1+x)(1+x^2)(1+x^4)(1+x^8)(1+x^{16})(1+y)(1+y^2) \\ &+ (1-x^8)(1+y^2)(1+x^{16}) \\ &- g_1(1+x^8)(1+y^2)(1+x^{16}) \\ &+ g_0(1-x^8)(1-y^2)(1+x^{16}) \\ &- g_0g_2(1+x^8)(1-y^2)(1+x^{16}) \\ &+ g_4(1+x^8)(1+x^8y)(1-y^2)(1-x^{16}) \\ &+ g_4g_3(1+x^8)(1+xy)(1+y^2)(1-x^{16}), \quad \text{where } g_0, g_1, g_2, g_3, g_4 \in H. \end{aligned} \tag{5}$$

The term $(1+x)(1+x^2)(1+x^4)(1+x^8)(1+x^{16})(1+y)(1+y^2)$ represents every element in H. The addition of the term $(1-x^8)(1+y^2)(1+x^{16})$ removes 4 of these elements and repeats 4 other elements. We regard the sum of these two terms (in light shading above) as a template which we write in (6) below as a 4×32 coefficient array: entry k in array position (i, j) corresponds to a contribution kx^jy^i in the group ring element $\rho(D)$.

$$\begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccccccccccccccccccccccccccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 & 25 & 26 & 27 & 28 & 29 & 30 & 31 \end{array} \\ \begin{pmatrix} 2 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 2 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 2 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \end{array} \tag{6}$$

The five terms
$-(1+x^8)(1+y^2)(1+x^{16})$,
$(1-x^8)(1-y^2)(1+x^{16})$,
$-(1+x^8)(1-y^2)(1+x^{16})$,
$(1+x^8)(1+x^8y)(1-y^2)(1-x^{16})$, and
$(1+x^8)(1+xy)(1+y^2)(1-x^{16})$
represent five sparse 4×32 arrays with nonzero entries in $\{-1,1\}$. We think of each of the quantities $g_1, g_0, g_0g_2, g_4, g_4g_3$ as shifting the positions of the nonzero entries within the corresponding 4×32 array. Provided the coefficient counts for 0s, 1s and 2s in A are as specified in (4), the image A given by (5) is guaranteed to satisfy the group ring equation (3) with $\rho(D) = A$. This condition on the coefficient counts translates to ensuring that the nonzero elements of the 5 shifted sparse arrays do not overlap among themselves and do not fall on the 8 entries of the template that are not equal to 1. Direct verification shows there are millions choices of g_0, g_1, g_2, g_3, g_4 for which these conditions hold (see Section 5).

For example, the coefficient array corresponding to $g_0(1-x^8)(1-y^2)(1+x^{16})$, where $g_0 = x^4y$ and $+$, $-$ represent 1 and -1 respectively, is

	0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*16*	*17*	*18*	*19*	*20*	*21*	*22*	*23*	*24*	*25*	*26*	*27*	*28*	*29*	*30*	*31*
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	+	0	0	0	0	0	0	0	−	0	0	0	0	0	0	0	+	0	0	0	0	0	0	0	−	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	−	0	0	0	0	0	0	0	+	0	0	0	0	0	0	0	−	0	0	0	0	0	0	0	+	0	0	0

and the following image A_1, given by the parameters $\{g_0, g_1, g_2, g_3, g_4\} = \{y, x^2, x^5, x^2, x^3\}$, satisfies (3):

	0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*16*	*17*	*18*	*19*	*20*	*21*	*22*	*23*	*24*	*25*	*26*	*27*	*28*	*29*	*30*	*31*
0	2	1	0	2	1	2	1	1	0	1	0	2	1	2	1	1	2	1	0	0	1	0	1	1	0	1	0	0	1	0	1	1
1	2	1	1	0	1	0	2	1	0	1	1	2	1	0	2	1	2	1	1	2	1	0	0	1	0	1	1	0	1	0	0	1
2	2	1	0	0	1	2	1	1	0	1	0	0	1	2	1	1	2	1	0	2	1	0	1	1	0	1	0	2	1	0	1	1
3	0	1	1	2	1	2	2	1	2	1	1	0	1	2	2	1	0	1	1	0	1	2	0	1	2	1	1	2	1	2	0	1

(7)

We observe that any resulting array $A = (a_{i,j})$ for which these non-overlapping conditions hold satisfies

$$a_{i,j} = 1 \iff a_{i+2,j} = 1 \quad \text{for } 0 \le i \le 1,\ 0 \le j \le 31. \tag{8}$$

4 Constraining the possible liftings of A to G

For each A chosen according to the procedure of Section 3, we wish to determine whether A is the image of a difference set D in G. In terms of group ring elements, we wish to know if there is an element B in $\mathbb{Z}[H]$ with all nonzero coefficients in $\{-1, 1\}$ for which

$$D = A\left(\frac{1+x^{32}}{2}\right) \; + \; B\left(\frac{1-x^{32}}{2}\right) \tag{9}$$

is a difference set in G. In terms of coefficient arrays, the element D defined in (9) is given by

$$D = \begin{array}{c} \begin{array}{cc} \scriptstyle 0 \;\ldots\; \scriptstyle 31 & \scriptstyle 32 \;\ldots\; \scriptstyle 63 \end{array} \\ \begin{array}{c} \scriptstyle 0 \\ \scriptstyle 1 \\ \scriptstyle 2 \\ \scriptstyle 3 \end{array} \left(\begin{array}{c|c} \dfrac{A+B}{2} & \dfrac{A-B}{2} \end{array}\right) \end{array}, \tag{10}$$

so the elements of the coefficient arrays D, A, B are related via

count	$d_{i,j}$	$d_{i,j+32}$	$a_{i,j}$	$b_{i,j}$
36	0	0	0	0
64	0	1	1	−1
	1	0	1	1
28	1	1	2	0

There are $36 + 28 = 64$ elements of B with a coefficient of 0, corresponding to elements in A with coefficients 0 or 2, which leaves 64 elements of B whose coefficients lie in $\{-1, 1\}$. Therefore for each A determined in Section 3, there are 2^{64} choices of B, each of which determines a potential difference set D in G. This large search size, which is infeasible even for a single array A, motivates imposing structure on A and constraining coefficients of B in order to bring the search into a feasible range.

Define a homomorphism ϕ from G to the multiplicative group of 4×4 complex matrices by

$$\phi: \; x \mapsto X = \begin{pmatrix} \xi & 0 & 0 & 0 \\ 0 & \xi^{-17} & 0 & 0 \\ 0 & 0 & -\xi & 0 \\ 0 & 0 & 0 & -\xi^{-17} \end{pmatrix}, \quad y \mapsto Y = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad \xi = e^{2\pi i}/64. \tag{11}$$

ϕ is one of 8 irreducible representations of degree 4 of G. Extend ϕ linearly to elements of the group ring $\mathbb{Z}[G]$. For group ring element

$$B = \sum_{i,j} b_{i,j} x^j y^i,$$

of $\mathbb{Z}[H]$, with corresponding coefficient array $(b_{i,j})$, we then have

$$\phi(B) = \sum_{i,j} b_{i,j} X^j Y^i. \tag{12}$$

To guarantee a difference set D, we require B to satisfy

$$\phi(B)\overline{\phi(B)}^T = 64 I_{4\times 4}. \tag{13}$$

For further information regarding the representation theory involved in this stage, and an explanation of how (9) and (13) guarantee a difference set D in G, see [4].

B has exactly 64 nonzero entries, so by (12) we see that $\phi(B)$ is a sum of 64 4×4 complex matrices. For B having coefficient array $(b_{i,j})$, we calculate $\phi(B)$ explicitly from (11) and (12) as the following sum of 32 4×4 complex matrices:

$$\phi(B) = \sum_{j=0}^{31} \begin{pmatrix} b_{0,j}\xi^j & b_{1,j}\xi^j & b_{2,j}\xi^j & b_{3,j}\xi^j \\ b_{3,j}\xi^{-17j} & b_{0,j}\xi^{-17j} & b_{1,j}\xi^{-17j} & b_{2,j}\xi^{-17j} \\ b_{2,j}(-\xi)^j & b_{3,j}(-\xi)^j & b_{0,j}(-\xi)^j & b_{1,j}(-\xi)^j \\ b_{1,j}(-\xi)^{-17j} & b_{2,j}(-\xi)^{-17j} & b_{3,j}(-\xi)^{-17j} & b_{0,j}(-\xi)^{-17j} \end{pmatrix}. \tag{14}$$

Numerical exploration in MatLab led us to believe it would be advantageous to additionally impose the following symmetry constraints on B:

$$b_{2,j} = -b_{0,j} \text{ and } b_{3,j} = b_{1,j}. \tag{15}$$

Given the constraint (15), set

$$\begin{aligned} u_j &= b_{0,j} \\ v_j &= b_{1,j}, \end{aligned} \tag{16}$$

and define length 32 sequences

$$\begin{aligned} U &= (u_j) \\ V &= (v_j) \end{aligned}$$

with entries in $\{-1, 0, 1\}$. Then the coefficient array B is given by

$$B = \begin{pmatrix} \cdots & U & \cdots \\ \cdots & V & \cdots \\ \cdots & -U & \cdots \\ \cdots & V & \cdots \end{pmatrix}. \tag{17}$$

The constraints in (15) can always be satisfied because of the observation made in (8). Under these constraints we have reduced the number of choices of B elements from 2^{64} to 2^{32} for any given A. Moreover, these constraints simplify the structure of the resulting product $\phi(B)\overline{\phi(B)}^T$, as we now describe.

Define sums

$$U_1 = \sum_{j=0}^{31} u_j \xi^j, \quad U_2 = \sum_{j=0}^{31} u_j \xi^{-17j}, \quad U_3 = \sum_{j=0}^{31} u_j (-\xi)^j, \quad U_4 = \sum_{j=0}^{31} u_j (-\xi)^{-17j},$$
$$V_1 = \sum_{j=0}^{31} v_j \xi^j, \quad V_2 = \sum_{j=0}^{31} v_j \xi^{-17j}, \quad V_3 = \sum_{j=0}^{31} v_j (-\xi)^j, \quad V_4 = \sum_{j=0}^{31} v_j (-\xi)^{-17j}. \tag{18}$$

Then, from (14), (15) and (16) we have

$$\phi(B) = \begin{pmatrix} U_1 & V_1 & -U_1 & V_1 \\ V_2 & U_2 & V_2 & -U_2 \\ -U_3 & V_3 & U_3 & V_3 \\ V_4 & -U_4 & V_4 & U_4 \end{pmatrix}, \tag{19}$$

and direct calculation gives

$$\phi(B)\overline{\phi(B)}^T = 2 \begin{pmatrix} |U_1|^2+|V_1|^2 & 0 & -U_1\overline{U_3} + V_1\overline{V_3} & 0 \\ 0 & |U_2|^2+|V_2|^2 & 0 & -U_2\overline{U_4} + V_2\overline{V_4} \\ -\overline{U_1}U_3 + \overline{V_1}V_3 & 0 & |U_3|^2+|V_3|^2 & 0 \\ 0 & -\overline{U_2}U_4 + \overline{V_2}V_4 & 0 & |U_4|^2+|V_4|^2 \end{pmatrix}. \tag{20}$$

We now see the effectiveness of (15) as not only substantially reducing the search size but also as forcing 8 off-diagonal entries in $\phi(B)\overline{\phi(B)}^T$ to be 0, partially fulfilling the requirements of (13). We are left to force the remaining 4 off-diagonal elements to be 0 and the 4 diagonal ones to be 64.

5 Search results

Having found a possible structure for A and B, we used MatLab to search for a difference set consistent with these structures.

As described in Section 3, all choices of g_0, g_1, g_2, g_3, g_4 in (5), for which the nonzero elements of the five associated sparse 4×32 arrays do not overlap among themselves and do not fall on the 8 entries of the template that are not equal to 1, give a group ring element $A(g_0, g_1, g_2, g_3, g_4)$ satisfying the condition (3). There are millions of such choices for $(g_0, g_1, g_2, g_3, g_4)$.

However, given a coefficient array A, the corresponding set of possible coefficient arrays B depends only on the set of 1 positions in A, not the positions of the 0 and 2 elements. We therefore need retain only one example array A for each set of distinct 1 positions. The set of 1 positions in each possible A repeats every eight columns and every two rows, and so can be represented just from the 1 positions of the upper left 2×8 block of A. For example, the 2×8 block corresponding to the array A_1 of (7) is

$$\begin{array}{cccccccc} 2 & 1 & * & * & 1 & * & 1 & 1 \\ * & 1 & 1 & * & 1 & * & * & 1 \end{array}$$

where each * represents either a 0 element or a 2 element. The template forces the upper left position of the 2×8 block to be 2. We find by computer that the number of such 2×8 blocks with distinct 1 positions, that arise from at least one choice of parameters g_0, g_1, g_2, g_3, g_4, is 5,328.

To reduce the number of permissible 2×8 blocks further and to force some regularity within A, we constrain the 1 positions of A to be equally distributed among the four rows. This is motivated by the following observation.

Given the form (14) for $\phi(B)$, observe that the leading diagonal of $\phi(B)$ depends only on row 0 of B, and that the three cyclic shifts of this diagonal depend only on rows 1, 2 and 3 of B respectively. This is because $\phi(B)$ is the sum of terms involving a diagonal matrix X^j right multiplied by a cyclic shift matrix Y^i. This motivates limiting the set of A which we consider as possible images to only those in which the 64 entries 1 in the corresponding coefficient array are equally distributed among the 4 rows. This ensures that each row of the coefficient array B contains 16 nonzero entries, which in turn ensures that each entry in $\phi(B)$ given by (14) is the sum of 16 primitive roots of unity. Imposing this regularity appeared to be a plausible step towards achieving the overall objective, that the entries of the matrix $\phi(B)$ satisfy (13).

This also limits the possible 2×8 blocks to only those which contain exactly four 1 entries in each of the first and second rows. When we include this additional constraint, the number of 2×8 blocks with distinct 1 positions is reduced to 2,185.

Each of these 2,185 blocks for A gives rise to 2^{32} choices for the corresponding coefficient array B constrained according to (15). The size of the resulting search is then $2,185 \cdot 2^{32} \approx 10^{13}$. This compares with a search size of $5,328 \cdot 2^{64} \approx 10^{23}$ had we not constrained A to contain equally many 1 entries in each row and not constrained B according to the simplification (15).

For historical accuracy, the following explanation of our search implementation is described in terms of the 4×4 matrices given in (11), rather than the sums defined in (18).

We begin by pre-calculating and storing numerical representations for each of the 128 4×4 complex matrices of the form X^jY^i. These are used throughout the search when checking whether the product $\phi(B)\overline{\phi(B)}^T$ satisfies (13). We select each of the 2,185 2×8 blocks described above, and repeat the chosen 2×8 block twice vertically and then the resulting 4×8 block 4 times horizontally to determine the nonzero positions in the 4×32 coefficient array of B.

The first two rows of the coefficient array of B are then exhaustively chosen as suitable length 32 $\{-1, 0, 1\}$ sequences U and V consistent with the positions of nonzero elements as decided in the previous step. This amounts to a size 2^{32} search for the 32 nonzero positions in the first two rows of the coefficient array of B. The last two rows of the coefficient array of B are then set as $-U$ and V respectively. For each B, we calculate $\phi(B)$ as a sum of 64 of the pre-calculated 4×4 complex matrices using (12) and the product $\phi(B)\overline{\phi(B)}^T$ is then taken numerically. The top leftmost entry of this product is compared against 64 to within a tolerance of 10^{-13}. If this tolerance is met, we write the corresponding coefficient array of B to a file.

The results of the search were immediate in producing hundreds of elements B for which $\phi(B)\overline{\phi(B)}^T$ has all 4 entries along the main diagonal equal to 64; each B whose top leftmost entry satisfied the tolerance also had the remaining entries along the diagonal equal to 64. Nearly all of these lacked zeros in the four locations where they were not forced by the constraint (15) (see (20)). Nonetheless, the program found three full solutions to the equation $\phi(B)\overline{\phi(B)}^T = 64I_{4\times 4}$. At this point the program was terminated and we began to examine these results.

For each of these solutions, we chose an example parameter set $\{g_0, g_1, g_2, g_3, g_4\}$ which produces an A element from (5) whose 1 positions match the nonzero positions of the coefficient array of B, and which necessarily satisfies $AA^{(-1)} = 64 \cdot 1_H + 112 \cdot H$. By combining A and B for each of the three solutions according to (9) to produce D and subsequently checking $DD^{(-1)}$, we confirmed that all three A and B combinations produce a difference set. The following is the coefficient array of B_1, which when combined with the coefficient array of A_1 from (7) by way of (10), gives the coefficient array of a difference set D.

$$B_1 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccccccccccccccccccccccccccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 & 25 & 26 & 27 & 28 & 29 & 30 & 31 \end{array} \\ \begin{pmatrix} 0 & - & 0 & 0 & - & 0 & - & - & 0 & - & 0 & 0 & - & 0 & - & + & 0 & - & 0 & 0 & - & 0 & + & + & 0 & - & 0 & 0 & - & 0 & - & - \\ 0 & - & - & 0 & - & 0 & 0 & + & 0 & + & - & 0 & - & 0 & 0 & + & 0 & - & + & 0 & + & 0 & 0 & - & 0 & + & - & 0 & + & 0 & 0 & - \\ 0 & + & 0 & 0 & + & 0 & + & + & 0 & + & 0 & 0 & + & 0 & + & - & 0 & + & 0 & 0 & + & 0 & - & - & 0 & + & 0 & 0 & + & 0 & + & + \\ 0 & - & - & 0 & - & 0 & 0 & + & 0 & + & - & 0 & - & 0 & 0 & + & 0 & - & + & 0 & + & 0 & 0 & - & 0 & + & - & 0 & + & 0 & 0 & - \end{pmatrix} \end{array} \tag{21}$$

We present the other two solutions below:

$A(y, xy, x^6y^3, x^2, x^3) =$

$$A_2 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccccccccccccccccccccccccccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 & 25 & 26 & 27 & 28 & 29 & 30 & 31 \end{array} \\ \begin{pmatrix} 2 & 1 & 1 & 2 & 1 & 2 & 0 & 1 & 0 & 1 & 1 & 2 & 1 & 2 & 0 & 1 & 2 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 2 & 0 & 1 & 0 & 1 & 1 & 2 & 1 & 0 & 0 & 1 & 2 & 1 & 1 & 2 & 1 & 2 & 0 & 1 & 2 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 2 & 1 & 1 & 0 & 1 & 2 & 2 & 1 & 0 & 1 & 1 & 0 & 1 & 2 & 2 & 1 & 2 & 1 & 1 & 2 & 1 & 0 & 2 & 1 & 0 & 1 & 1 & 2 & 1 & 0 & 2 & 1 \\ 0 & 0 & 1 & 2 & 1 & 1 & 2 & 1 & 2 & 0 & 1 & 0 & 1 & 1 & 2 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 2 & 0 & 1 & 2 & 1 & 1 & 0 & 1 \end{pmatrix} \end{array}$$

$$B_2 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccccccccccccccccccccccccccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 & 25 & 26 & 27 & 28 & 29 & 30 & 31 \end{array} \\ \begin{pmatrix} 0 & - & - & 0 & - & 0 & 0 & - & 0 & - & - & 0 & - & 0 & 0 & + & 0 & - & - & 0 & + & 0 & 0 & + & 0 & - & - & 0 & - & 0 & 0 & - \\ 0 & 0 & - & 0 & - & + & 0 & - & 0 & 0 & + & 0 & - & + & 0 & - & 0 & 0 & - & 0 & - & + & 0 & + & 0 & 0 & - & 0 & - & + & 0 & - \\ 0 & + & + & 0 & + & 0 & 0 & + & 0 & + & + & 0 & + & 0 & 0 & - & 0 & + & + & 0 & - & 0 & 0 & - & 0 & + & + & 0 & + & 0 & 0 & + \\ 0 & 0 & - & 0 & - & + & 0 & - & 0 & 0 & + & 0 & - & + & 0 & - & 0 & 0 & - & 0 & - & + & 0 & + & 0 & 0 & - & 0 & - & + & 0 & - \end{pmatrix} \end{array}$$

$A(y, x^2y, x^5y^3, x^2y, x^3) =$

$A_3 =$

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	2	1	1	2	1	0	2	1	0	1	1	2	1	0	2	1	2	1	1	0	1	0	0	1	0	1	1	0	1	0	0	1
1	2	1	0	0	1	2	1	1	0	1	0	2	1	2	1	1	2	1	0	2	1	0	1	1	0	1	0	0	1	0	1	1
2	2	1	1	0	1	2	2	1	0	1	1	0	1	2	2	1	2	1	1	2	1	2	0	1	0	1	1	2	1	2	0	1
3	0	1	0	2	1	2	1	1	2	1	0	0	1	2	1	1	0	1	0	0	1	0	1	1	2	1	0	2	1	0	1	1

$B_3 =$

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	−	−	0	−	0	0	−	0	−	−	0	−	0	0	+	0	−	−	0	+	0	0	+	0	−	−	0	−	0	0	−
1	0	−	0	0	−	0	−	+	0	+	0	0	−	0	−	+	0	−	0	0	+	0	+	−	0	+	0	0	−	0	+	−
2	0	+	+	0	+	0	0	+	0	+	+	0	+	0	0	−	0	+	+	0	−	0	0	−	0	+	+	0	+	0	0	+
3	0	−	0	0	−	0	−	+	0	+	0	0	−	0	−	+	0	−	0	0	+	0	+	−	0	+	0	0	−	0	+	−

6 Interpretation of solutions using sequence correlations

We began by examining $\phi(B)$ for each of the three search solutions. Each is a 4×4 complex matrix whose entries are sums of 16 primitive 64th roots of unity, as defined in (18) (see (19)). The two solutions (B_1 and B_3) which at the outset exhibited the most similarity, have the following connection: the four entries in each column of $\phi(B)$ comprise sums over the same 16 roots of unity, regardless of whether the sum in (18) is defined using ξ or ξ^{-17}. This we thought interesting, but not necessary as the third example does not exhibit this relationship. This lack of consistency led us to look more closely for answers within B, rather than $\phi(B)$. We were eventually able to explain all three solutions via the autocorrelations of each of the sequences U and V.

Definition 2. *For a real sequence $A = (a_0, a_1, \ldots, a_{n-1})$ of length n, the* negacyclic autocorrelation *at shift w is*

$$N_A(w) = \sum_{j=0}^{n-1-w} a_j a_{j+w} - \sum_{j=n-w}^{n-1} a_j a_{j+w-n} \quad \text{for } 0 \le w < n.$$

Definition 3. *Real sequences $A = (a_j)$, $B = (b_j)$ of length n form a* negacyclic Golay pair *if*

$$N_A(w) + N_B(w) = 0 \quad \text{for } w \neq 0.$$

Definition 4. *For a real sequence $A = (a_0, a_1, \ldots, a_{n-1})$ of length n, define the* negacyclic shift by v places *as the sequence (b_j) given by*

$$b_j = \begin{cases} a_{j-v} & \text{for } j \ge v \\ -a_{n+j-v} & \text{for } j < v \end{cases}$$

Each row of the coefficient array of B is a ternary sequence (having elements from $\{-1, 0, 1\}$) of length 32 as shown in (17), with exactly 16 nonzero elements (as described in Section 5). Using a symbolic algebra package we tested various relationships between the rows of B to find that:

Observation 5. *For each of the three solutions found for B, the sequences $U = (u_j)$ and $V = (v_j)$ defined in* (17) *form a ternary negacyclic Golay pair.*

Recall that the search produced many arrays B for which the diagonal entries of $\phi(B)\overline{\phi(B)}^T$ satisfy (13), yet very few of these B gave rise to a full solution to (13). This suggested that perhaps there was something special about those U and V sequences (apart from just forming negacyclic Golay pairs) which forces the resulting $\phi(B)$ to fully satisfy (13). We therefore worked to find some extra relationships between the sequences U and V corresponding to the three full solutions. In doing so we were led to more closely inspect the autocorrelation vectors corresponding to each U and V pair. The following autocorrelation vectors correspond to U and V from B_1 in (21).

$$\begin{aligned}
N_U(w): &\quad (16\ 2\ 0\ 4\ 0\ 2\ 0\ 0\ 0\ -4\ 0\ 2\ 0\ 0\ 0\ -2\ 0\ 2\ 0\ 0\ 0\ -2\ 0\ 4\ 0\ 0\ 0\ -2\ 0\ -4\ 0\ -2)\\
N_V(w): &\quad (16\ -2\ 0\ -4\ 0\ -2\ 0\ 0\ 0\ 4\ 0\ -2\ 0\ 0\ 0\ 2\ 0\ -2\ 0\ 0\ 0\ 2\ 0\ -4\ 0\ 0\ 0\ 2\ 0\ 4\ 0\ 2)\\
0 \le w < 32&
\end{aligned}$$

We see that the negacyclic autocorrelation of each of U and V for this first solution (along with the two other solutions) is 0 for all even $w \neq 0$. In light of this, we next separate the sequences and their autocorrelations into odd and even indices in order to gain further insight.

Definition 6. *For a real sequence $A = (a_0, a_1, \ldots, a_{n-1})$ of length n, define the even and odd negacyclic autocorrelation at shift w by*

$$\begin{aligned}
NE_A(w) &= \sum_{\substack{j=0\\ j\ even}}^{n-1-w} a_j a_{j+w} - \sum_{\substack{j=n-w\\ j\ even}}^{n-1} a_j a_{j+w-n}, \quad 0 \le w < n\\
NO_A(w) &= \sum_{\substack{j=0\\ j\ odd}}^{n-1-w} a_j a_{j+w} - \sum_{\substack{j=n-w\\ j\ odd}}^{n-1} a_j a_{j+w-n}, \quad 0 \le w < n
\end{aligned}$$

so that

$$N_A(w) = NE_A(w) + NO_A(w), \quad 0 \le w < n. \tag{22}$$

Observe the following even and odd autocorrelation vectors for U and V (again from B_1 in (21)):

$$\begin{aligned}
NE_U(w): &\quad (8\ 2\ 2\ 0\ 0\ 2\ 0\ 0\ 0\ -4\ 0\ 0\ 0\ 0\ 2\ 0\ 0\ 2\ -2\ 0\ 0\ -2\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ -4\ -2\ 0)\\
NO_U(w): &\quad (8\ 0\ -2\ 4\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 2\ 0\ 0\ -2\ -2\ 0\ 0\ 2\ 0\ 0\ 0\ 0\ 4\ 0\ 0\ 0\ -2\ 0\ 0\ 2\ -2)\\
NE_V(w): &\quad (8\ 0\ 2\ -4\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ -2\ 0\ 0\ 2\ 2\ 0\ 0\ -2\ 0\ 0\ 0\ 0\ -4\ 0\ 0\ 0\ 2\ 0\ 0\ -2\ 2)\\
NO_V(w): &\quad (8\ -2\ -2\ 0\ 0\ -2\ 0\ 0\ 0\ 4\ 0\ 0\ 0\ 0\ -2\ 0\ 0\ -2\ 2\ 0\ 0\ 2\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 4\ 2\ 0)\\
0 \le w < 32&
\end{aligned}$$

In the above example we find that the even negacyclic autocorrelation of U together with the odd negacyclic autocorrelation of V sum to zero for all nonzero shifts w, and similarly for U and V replaced by V and U. This stronger property of U and V is exhibited in all three solutions. With the following lemma, we outline some relationships which are a consequence of taking the transformation of a sequence and comparing its autocorrelation to the original. These will be subsequently used to explain how the properties of U and V described above ensure that $\phi(B)\overline{\phi(B)}^T$, as calculated in (20), satisfies the required property (13).

Lemma 7. *Let $A = (a_0, a_1, \ldots, a_{2m-1})$ be a real sequence of length $2m$, and let $B = (b_0, b_1, \ldots, b_{2m-1})$ be a transformation of A as specified below. Then $N_A(w)$, $NE_A(w)$, $NO_A(w)$ transform as shown:*

	$N_B(w)$	$NE_B(w)$	$NO_B(w)$
$b_j = a_{2m-1-j}$ *(reverse)*	$N_A(w)$	$\begin{cases} NO_A(w) & \text{for } w \text{ even} \\ NE_A(w) & \text{for } w \text{ odd} \end{cases}$	$\begin{cases} NE_A(w) & \text{for } w \text{ even} \\ NO_A(w) & \text{for } w \text{ odd} \end{cases}$
$b_j = (-1)^j a_j$ *(change alternate sign)*	$(-1)^w N_A(w)$	$(-1)^w NE_A(w)$	$(-1)^w NO_A(w)$
(negacyclically shift v places, v odd)	$N_A(w)$	$NO_A(w)$	$NE_A(w)$

Lemma 7 can be proved by straightforward manipulation of sums, similar to the proof of Lemma 8 below.

Lemma 8. *For a real sequence $A = (a_0, a_1, \ldots, a_{n-1})$ and for complex τ satisfying $\tau^n = -1$,*

$$\left|\sum_{j=0}^{n-1} a_j \tau^j\right|^2 = \sum_{w=0}^{n-1} N_A(w)\tau^w.$$

Proof.

$$\begin{aligned}
\left|\sum_{j=0}^{n-1} a_j \tau^j\right|^2 &= \sum_{j=0}^{n-1} a_j \tau^j \overline{\sum_{k=0}^{n-1} a_k \tau^k} \\
&= \sum_{k=0}^{n-1}\sum_{j=0}^{n-1} a_j a_k \tau^{j-k} \\
&= \sum_{k=0}^{n-1}\left(\sum_{j=0}^{k-1} a_j a_k \tau^{j-k} + \sum_{j=k}^{n-1} a_j a_k \tau^{j-k}\right) \\
&= \sum_{k=0}^{n-1}\left(-\sum_{j=0}^{k-1} a_j a_k \tau^{j-k+n} + \sum_{j=k}^{n-1} a_j a_k \tau^{j-k}\right) \quad \text{by } \tau^n = -1 \\
&\quad \text{put } w = j-k+n \qquad \text{put } w = j-k \\
&= -\sum_{k=0}^{n-1}\sum_{w=n-k}^{n-1} a_{k+w-n} a_k \tau^w + \sum_{k=0}^{n-1}\sum_{w=0}^{n-1-k} a_{k+w} a_k \tau^w
\end{aligned}$$

switch order of summation

$$
\begin{aligned}
&= -\sum_{w=0}^{n-1}\sum_{k=n-w}^{n-1} a_{k+w-n}a_k\tau^w + \sum_{w=0}^{n-1}\sum_{k=0}^{n-1-w} a_{k+w}a_k\tau^w \\
&= \sum_{w=0}^{n-1}\left(\sum_{k=0}^{n-1-w} a_k a_{k+w} - \sum_{k=n-w}^{n-1} a_k a_{k+w-n}\right)\tau^w \\
&= \sum_{w=0}^{n-1} N_A(w)\tau^w.
\end{aligned}
$$

□

The following result shows how the diagonal entries of $\phi(B)\overline{\phi(B)}^T$ can be made to satisfy (13).

Corollary 9. *Let $U = (u_j)$ and $V = (v_j)$ be length 32 sequences forming a ternary negacyclic Golay pair, each with exactly 16 nonzero entries. The sums U_1 to U_4 and V_1 to V_4 defined in (18) satisfy $|U_j|^2 + |V_j|^2 = 32$ for $j = 1, 2, 3, 4$.*

Proof. We have

$$
\begin{aligned}
|U_1|^2 + |V_1|^2 &= \left|\sum_{j=0}^{31} u_j\xi^j\right|^2 + \left|\sum_{j=0}^{31} v_j\xi^j\right|^2, \\
&= \sum_{w=0}^{31}\left(N_U(w) + N_V(w)\right)\xi^w \quad \text{by Lemma 8 with } n = 32 \text{ and } \tau = \xi \\
&= N_U(0) + N_V(0) \quad U, V \text{ form a negacyclic Golay pair} \\
&= 16 + 16 = 32 \quad \text{by assumption.}
\end{aligned}
$$

$$
\begin{aligned}
|U_3|^2 + |V_3|^2 &= \left|\sum_{j=0}^{31} u_j(-\xi)^j\right|^2 + \left|\sum_{j=0}^{31} v_j(-\xi)^j\right|^2, \\
&= \sum_{w=0}^{31}\left(N_U(w) + N_V(w)\right)(-\xi)^w \quad \text{by Lemma 8 with } n = 32 \text{ and } \tau = -\xi \\
&= 32 \quad \text{as above.}
\end{aligned}
$$

$$
\begin{aligned}
|U_2|^2 + |V_2|^2 &= \left|\sum_{j=0}^{31} u_j\zeta^j\right|^2 + \left|\sum_{j=0}^{31} v_j\zeta^j\right|^2 \quad \text{where } \zeta = \xi^{-17}, \\
&= \sum_{w=0}^{31}\left(N_U(w) + N_V(w)\right)\zeta^w \quad \text{by Lemma 8 with } n = 32 \text{ and } \tau = \zeta \\
&= 32.
\end{aligned}
$$

$$|U_4|^2 + |V_4|^2 = \left|\sum_{j=0}^{31} u_j(-\zeta)^j\right|^2 + \left|\sum_{j=0}^{31} v_j(-\zeta^j)\right|^2 \quad \text{where } \zeta = \xi^{-17},$$
$$= \sum_{w=0}^{31} \left(N_U(w) + N_V(w)\right)(-\zeta)^w \quad \text{by Lemma 8 with } n = 32 \text{ and } \tau = -\zeta$$
$$= 32.$$

□

This completes our examination of the diagonal entries of $\phi(B)\overline{\phi(B)}^T$ and we will now examine how each of the off-diagonal entries can be made to satisfy (13).

In the following proposition we start with a negacyclic Golay pair S, T and construct a second negacyclic Golay pair U, V of twice the length having additional properties. We shall show that these additional properties are sufficient to force the off-diagonal entries of $\phi(B)\overline{\phi(B)}^T$ to satisfy (13).

Proposition 10. *Let $S = (s_j)$, $T = (t_j)$ be length m real sequences forming a negacyclic Golay pair. Let $U = (u_j)$ be the length $2m$ interleaving of S and T ($u_{2j} = s_j$, $u_{2j+1} = t_j$, for $0 \le j \le m-1$) and let $V = (v_j)$ be the negacyclic shift by an odd number of places of the length $2m$ sequence $((-1)^j u_{2m-1-j})$. Then*

(i) $N_U(w) = N_V(w) = 0$ *for even* $w \neq 0$

(ii) $NE_U(w) + NO_V(w) = 0$ *for* $w \neq 0$, *and*
$NO_U(w) + NE_V(w) = 0$ *for* $w \neq 0$.

In particular, adding the relations in (ii) shows by (22) that U, V form a length $2m$ negacyclic Golay pair.

Proof. (i) For integer $y \neq 0$,

$$N_U(2y) = \sum_{j=0}^{2m-1-2y} u_j u_{j+2y} - \sum_{j=2m-2y}^{2m-1} u_j u_{j+2y-2m},$$
$$= \sum_{j=0}^{m-1-y} u_{2j}u_{2j+2y} - \sum_{j=m-y}^{m-1} u_{2j}u_{2j+2y-2m}$$
$$+ \sum_{j=0}^{m-1-y} u_{2j+1}u_{2j+1+2y} - \sum_{j=m-y}^{m-1} u_{2j+1}u_{2j+1+2y-2m},$$
by separating into even and odd indices,
$$= \sum_{j=0}^{m-1-y} s_j s_{j+y} - \sum_{j=m-y}^{m-1} s_j s_{j+y-m}$$

$$+ \sum_{j=0}^{m-1-y} t_j t_{j+y} - \sum_{j=m-y}^{m-1} t_j t_{j+y-m},$$

by definition of U,

$$= N_S(y) + N_T(y)$$

$$= 0 \quad \text{because } S, T \text{ form a negacyclic Golay pair} \tag{23}$$

and from Lemma 7, $N_V(2y) = (-1)^{2y} N_U(2y) = 0$.

(ii) From Lemma 7,

$$NE_U(w) + NO_V(w) = \begin{cases} NE_U(w) + NO_U(w) & \text{for } w \text{ even} \\ NE_U(w) - NE_U(w) & \text{for } w \text{ odd} \end{cases}$$

$$= \begin{cases} N_U(w) & \text{for } w \text{ even by (22)} \\ 0 & \text{for } w \text{ odd} \end{cases}$$

$$= 0 \text{ for } w \neq 0 \text{ by (23)}$$

$$\text{and } NO_U(w) + NE_V(w) = \begin{cases} NO_U(w) + NE_U(w) & \text{for } w \text{ even} \\ NO_U(w) - NO_U(w) & \text{for } w \text{ odd} \end{cases}$$

$$= 0 \text{ for } w \neq 0 \text{ as above.}$$

□

Proposition 10 captures the relationship which is shared by each U and V pair from our three search solutions. The following examples all use $U = (u_j)$ and $V = (v_j)$ from B_1 in (21).

$U = (u_j) =$ (0 − 0 0 − 0 − − 0 − 0 0 − 0 − + 0 − 0 0 − 0 + + 0 − 0 0 − 0 − −) ,
$S = (u_{2j}) =$ (0 0 − − 0 0 − − 0 0 − + 0 0 − −) ,
$T = (u_{2j+1}) =$ (− 0 0 − − 0 0 + − 0 0 + − 0 0 −) ,
$N_S(w)$: (8 2 0 0 0 0 0 0 2 0 −2 0 0 0 0 0 0 −2) ,
$N_T(w)$: (8 −2 0 0 0 0 0 0 −2 0 2 0 0 0 0 0 0 2) ,
and $N_S(w) + N_T(w) = 0$ for all $w \neq 0$, therefore S and T form a negacyclic Golay pair.

This shows that U is the interleaving of two length 16 sequences which themselves form a negacyclic Golay pair. We now show that V is a transformation of U as described above.

$(u_{31-j}) =$ (− − 0 − 0 0 − 0 + + 0 − 0 0 − 0 + − 0 − 0 0 − 0 − − 0 − 0 0 − 0)
$(-1)^j(u_{31-j}) =$ (− + 0 + 0 0 − 0 + − 0 + 0 0 − 0 + + 0 + 0 0 − 0 − + 0 + 0 0 − 0)
and negacyclically shifting $(-1)^j(u_{31-j})$ by 17 places gives:
(0 − − 0 − 0 0 + 0 + − 0 − 0 0 + 0 − + 0 + 0 0 − 0 + − 0 + 0 0 −) ,
which equals the sequence V taken directly from the second row of B_1 in (21).

This completes the demonstration that V is a transformation of U, which itself is the interleaving of two sequences which form a negacyclic Golay pair. We previously observed that these sequences U,V each individually satisfies the property that their negacyclic autocorrelation is 0 for even shifts $w \neq 0$. Furthermore, we showed that this pair U,V has the properties described directly after Definition 6, involving relationships between the even and odd negacyclic autocorrelations of the sequences. We now see that these properties are guaranteed by the single condition involving S and T as described in Proposition 10. We will soon demonstrate how this second relationship relates to condition (13).

Lemma 11. *For a real sequence $A = (a_0, a_1, \ldots, a_{n-1})$, and for complex τ satisfying $\tau^n = -1$,*

$$\left(\sum_{j=0}^{n-1} a_j \tau^j\right) \overline{\left(\sum_{k=0}^{n-1} (-1)^k a_k \tau^k\right)} = \sum_{w=0}^{n-1} (NE_A(w) - NO_A(w))\tau^w.$$

Proof. Following the method of the proof for Lemma 8 gives

$$\begin{aligned}
\text{LHS} &= \sum_{w=0}^{n-1} \left(\sum_{k=0}^{n-1-w} (-1)^k a_k a_{k+w} - \sum_{k=n-w}^{n-1} (-1)^k a_k a_{k+w-n} \right) \tau^w \\
&= \sum_{w=0}^{n-1} \left(\left(\sum_{\substack{k=0 \\ k \text{ even}}}^{n-1-w} a_k a_{k+w} - \sum_{\substack{k=n-w \\ k \text{ even}}}^{n-1} a_k a_{k+w-n} \right) \right. \\
&\qquad \left. - \left(\sum_{\substack{k=0 \\ k \text{ odd}}}^{n-1-w} a_k a_{k+w} - \sum_{\substack{k=n-w \\ k \text{ odd}}}^{n-1} a_k a_{k+w-n} \right) \right) \tau^w \\
&= \sum_{w=0}^{n-1} (NE_A(w) - NO_A(w))\tau^w.
\end{aligned}$$

□

In the following corollary, we use Lemma 11 and Proposition 10 to show how to force off-diagonal entries of $\phi(B)\overline{\phi(B)}^T$ in (20) to be zero.

Corollary 12. *Let $S = (s_j)$ and $T = (t_j)$ be length 16 sequences forming a negacyclic Golay pair, and $U = (u_j)$ be the interleaving of S and T. Let $V = (v_j)$ be the negacyclic shift by an odd number of places of the length 32 sequence $((-1)^j u_{31-j})$. The sums U_1 to U_4 and V_1 to V_4 defined in (18) satisfy $-U_j\overline{U_{j+2}} + V_j\overline{V_{j+2}} = 0$ for $j = 1, 2$.*

Proof.

$$
\begin{aligned}
-U_1\overline{U_3} + V_1\overline{V_3} &= -\left(\sum_{j=0}^{31} u_j\xi^j\right)\overline{\left(\sum_{k=0}^{31}(-1)^k u_k\xi^k\right)} + \left(\sum_{j=0}^{31} v_j\xi^j\right)\overline{\left(\sum_{k=0}^{31}(-1)^k v_k\xi^k\right)} \\
&= \sum_{w=0}^{31}(-NE_U(w) + NO_U(w) + NE_V(w) - NO_V(w))\xi^w \quad \text{by Lemma 11 with } n = 32 \text{ and } \tau = \xi \\
&= \sum_{w=0}^{31}((NO_U(w) + NE_V(w)) - (NE_U(w) + NO_V(w)))\xi^w \\
&= NO_U(0) + NE_V(0) - NE_U(0) - NO_V(0) \quad \text{by Proposition 10 (ii)} \\
&= (NO_U(0) - NO_V(0)) - (NE_U(0) - NE_V(0)) \\
&= 0 \quad \text{by construction of } V \text{ from } U.
\end{aligned}
$$

$-U_2\overline{U_4} + V_2\overline{V_4} = 0$ by the same argument, with $\zeta = \xi^{-17}$ replacing ξ.

□

Corollary 13. *Let S, T be a ternary length* 16 *negacylic Golay pair having a total of* 16 *nonzero entries, and $U = (u_j)$ be the interleaving of S and T. Let $V = (v_j)$ be the negacyclic shift by an odd number of places of the length* 32 *sequence $((-1)^j(u_{31-j})$. Form the coefficient array of an element B from U and V by* (17)*. Then $\phi(B)$ satisfies the equation $\phi(B)\overline{\phi(B)}^T = 64I_{4\times 4}$.*

Proof. Because B satisfies (17), $\phi(B)\overline{\phi(B)}^T$ has the form given in (20) with U_1 to U_4 and V_1 to V_4 defined as in (18). This guarantees that eight entries of $\phi(B)\overline{\phi(B)}^T$ are zero, matching the eight corresponding entries in $64I_{4\times 4}$ regardless of which S and T are used to build U. This leaves eight remaining entries, four on the diagonal and four off it.

Since U is constructed by interleaving the sequences of a ternary length 16 negacyclic Golay pair, and V is constructed as the transformation of U specified above, then by Proposition 10 U, V form a ternary length 32 negacyclic Golay pair. Since S, T have a total of 16 nonzero entries, so does U. Then by construction, so does V. By Corollary 9 the four diagonal entries of $\phi(B)\overline{\phi(B)}^T$ are 64 and by Corollary 12 the four remaining off-diagonal entries are 0. □

Corollary 14. *Let B be an element formed as in Corollary 13. Suppose there is a parameter set $(g_0, g_1, g_2, g_3, g_4)$ which produces an element A from* (5) *whose coefficient array has its* 1 *positions matching the nonzero positions of the coefficient array of B. The element D formed from A and B as in* (9) *is a $(256, 120, 56)$ difference set in the group G.*

This concludes the explanation for how U and V with the appropriate properties give the coefficient array of an element B, where B satisfies the matrix condition in (13), and how this can be combined with a suitable element A to guarantee a difference set D in the group G.

7 Construction of a difference set in G by hand

We now understand how to build a coefficient array B from sequences U and V so that the matrix $\phi(B)\overline{\phi(B)}^T$ satisfies (13), which ensures that D built by (9) (using any A whose 1 positions match the nonzero positions in B) is a difference set in G. Our next objective was to construct a difference set by hand using a recursive implementation of the construction described in Proposition 10 to produce suitable sequences U and V.

By Corollary 13, we require a (length 32) sequence $U = (u_j)$ which is the interleaving of the sequences of a ternary length 16 negacyclic Golay pair having a total of 16 nonzero entries and which has a repetitive structure consistent with our five parameter function for A in (5). To achieve this, we recursively implement an interleaving of negacyclic Golay pairs according to Proposition 10 (which produces a negacyclic Golay pair of length $2m$ from one of length m), while taking care that U contains exactly 16 nonzero entries and that U and V give a B in (17) which achieves a repetitive pattern consistent with (5). We demonstrate a recursive construction beginning with trivial length 1 sequences, satisfying both of these conditions by adding an extra step: to interleave intermediate sequences with zeros at a specific recursive step. We demonstrate this process below.

Let S_1 and T_1 be a length 1 negacyclic Golay pair as follows,

$$S_1 = (+) \quad \text{and} \quad T_1 = (+).$$

Let S_2 be the interleaving of S_1 and T_1,

$$S_2 = \qquad (+\ +)\ ,$$

and, as in Proposition 10, let T_2 be the negacyclic shift by 1 place of the reversal of the sequence S_2 whose odd elements have alternated signs, so that

$$T_2 = \qquad (+\ +)\ .$$

S_2 and T_2 form a negacyclic Golay pair. Continuing this process recursively, we will always take the negacylic shift in Proposition 10 as a shift by exactly 1 place, which gives

$$\begin{aligned} S_3 &= \qquad (+\ +\ +\ +)\ , \quad \text{and} \\ T_3 &= \qquad (+\ +\ -\ +)\ . \end{aligned}$$

S_3 and T_3 form a negacyclic Golay pair. Knowing that we need this process to produce two ternary length 32 sequences, each with exactly 16 nonzero entries, we will now interleave the sequences S_3 and T_3 with zeros as follows.

$$\begin{aligned} S_4 &= \qquad (0\ +\ 0\ +\ 0\ +\ 0\ +)\ , \quad \text{and} \\ T_4 &= \qquad (0\ +\ 0\ +\ 0\ -\ 0\ +)\ . \end{aligned}$$

S_4 and T_4 form a negacyclic Golay pair, because S_3 and T_3 do. Continuing the recursive interleaving and transformation process according to Proposition 10 gives

$$\begin{aligned} S_5 = &\quad (0\ 0\ +\ +\ 0\ 0\ +\ +\ 0\ 0\ +\ -\ 0\ 0\ +\ +) \ , \\ T_5 = &\quad (0\ +\ -\ 0\ 0\ -\ -\ 0\ 0\ +\ -\ 0\ 0\ +\ -\ 0) \ . \end{aligned}$$

S_5 and T_5 form a ternary length 16 negacyclic Golay pair having a total of 16 nonzero elements. We may therefore form $U = S_6$ and $V = T_6$ according to Corollary 13:

$$\begin{aligned} S6 = &\quad (0\ 0\ 0\ +\ +\ -\ +\ 0\ 0\ 0\ 0\ -\ +\ -\ +\ 0\ 0\ 0\ 0\ +\ +\ -\ -\ 0\ 0\ 0\ 0\ +\ +\ -\ +\ 0) \ , \quad \text{and} \\ T6 = &\quad (0\ 0\ -\ -\ -\ +\ 0\ 0\ 0\ 0\ +\ -\ -\ +\ 0\ 0\ 0\ 0\ -\ -\ -\ -\ 0\ 0\ 0\ 0\ -\ -\ -\ +\ 0\ 0) \ , \end{aligned}$$

and then form the coefficient array of B from U and V as in (17) to give

$$B_4 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccccccccccccccccccccccccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 & 25 & 26 & 27 & 28 & 29 & 30 & 31 \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & + & + & - & + & 0 & 0 & 0 & 0 & - & + & - & + & 0 & 0 & 0 & 0 & + & + & - & - & 0 & 0 & 0 & 0 & + & + & - & + & 0 \\ 0 & 0 & - & - & - & + & 0 & 0 & 0 & 0 & + & - & - & + & 0 & 0 & 0 & 0 & - & - & - & - & 0 & 0 & 0 & 0 & - & - & - & + & 0 & 0 \\ 0 & 0 & 0 & - & - & + & - & 0 & 0 & 0 & 0 & + & - & + & - & 0 & 0 & 0 & 0 & - & - & + & + & 0 & 0 & 0 & 0 & - & - & + & - & 0 \\ 0 & 0 & - & - & - & + & 0 & 0 & 0 & 0 & + & - & - & + & 0 & 0 & 0 & 0 & - & - & - & - & 0 & 0 & 0 & 0 & - & - & - & + & 0 & 0 \end{pmatrix} \end{array} .$$

By Corollary 13, we have $\phi(B_4)\overline{\phi(B_4)}^T = 64I_{4\times 4}$. Moreover, the nonzero positions of the B_4 repeat every eight columns and two rows. We must now choose a parameter set $(g_0, g_1, g_2, g_3, g_4)$ which under (5) gives an element A_4 whose 1 positions match these well-behaved nonzero positions of the coefficient array of B_4. We use the parameter set $(y, x^6y, xy^3, x^2y, x^7)$, but stress that any parameter set giving an element A whose 1 positions in the corresponding coefficient array are identical to those in the following will suffice.

$A(y, x^6y, xy^3, x^2y, x^7) =$

$$A_4 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccccccccccccccccccccccccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 & 25 & 26 & 27 & 28 & 29 & 30 & 31 \end{array} \\ \begin{pmatrix} 2 & 0 & 0 & 1 & 1 & 1 & 1 & 2 & 0 & 0 & 2 & 1 & 1 & 1 & 1 & 2 & 2 & 0 & 2 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 2 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 2 & 1 & 1 & 1 & 1 & 0 & 2 & 2 & 2 & 1 & 1 & 1 & 1 & 0 & 2 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 2 & 2 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 2 & 2 & 1 & 1 & 1 & 1 & 0 & 2 & 2 & 2 & 1 & 1 & 1 & 1 & 2 & 0 & 2 & 0 & 1 & 1 & 1 & 1 & 2 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 2 & 2 & 2 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 2 & 1 & 1 & 1 & 1 & 0 & 0 & 2 & 0 & 1 & 1 & 1 & 1 & 0 & 2 \end{pmatrix} \end{array} .$$

Now by Corollary 14, the element $D = A_4\left(\frac{1+x^{32}}{2}\right) + B_4\left(\frac{1-x^{32}}{2}\right)$ is a $(256, 120, 56)$ difference set in the group G.

Acknowledgements

I would like to thank my supervisor Jonathan Jedwab for the constant support and guidance throughout the project. I would like to also thank Jim Davis and Ken Smith for both their contribution of a five-parameter family of potential images A of difference sets D in the group G, as well as a representation theoretic approach for determining a sufficient element B. Without all of the help, this project would surely have been unapproachable.

References

[1] T. Beth, D. Jungnickel, and H. Lenz. *Design Theory volume* 1, second edition, Cambridge University Press, 1999.

[2] J.A Davis. The Final Four. Presentation to *Finite Geometries, 4th Irsee Conference*. Irsee, Germany, Sept 2014.

[3] J.A. Davis and J.E. Iiams. Hadamard difference sets in non-abelian 2-groups with high exponent, *J. Alg.* 199 (1998), 62-87.

[4] J.A. Davis and K.W. Smith. A construction of difference sets in high exponent 2-groups using representation theory, *J. Algebraic Combin.* 3 (1994), 137-151.

[5] J.A. Davis and K.W. Smith. Personal communication, May 2016.

[6] The GAP Group. E.A. O'Brien, B. Eick, and H.U. Besche. The SmallGroups data library, 2016.