

# Nonexistence of some cyclic difference sets

Bridget Franklin\*      Steven Sam†

July 27, 2006

## Abstract

Many difference sets have been found and the existence of others disproved under certain parameter sets. The Center for Communications Research at La Jolla gives a list of many open cases in which the existence of a cyclic difference set is unknown. Using multiplier theorems and techniques from algebraic number theory, we tackle this list of open parameter sets, ruling out cyclic difference sets with parameters  $(2574, 249, 24)$ ,  $(817, 289, 102)$ ,  $(645, 161, 40)$ ,  $(1380, 197, 28)$ ,  $(2160, 255, 30)$ ,  $(465, 145, 45)$ .

## Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
<b>2</b>	<b>The second multiplier theorem</b>	<b>2</b>
2.1	$(2574, 249, 24)$ cyclic difference sets . . . . .	5
2.2	$(817, 289, 102)$ cyclic difference sets . . . . .	7
2.3	$(645, 161, 40)$ cyclic difference sets . . . . .	10
2.4	$(1380, 197, 28)$ cyclic difference sets . . . . .	12
<b>3</b>	<b>Some remarks on the multiplier conjecture</b>	<b>13</b>
3.1	$(1785, 224, 28)$ cyclic difference sets . . . . .	14
<b>4</b>	<b>Algebraic number theory</b>	<b>15</b>
4.1	$(2160, 255, 30)$ cyclic difference sets . . . . .	17
4.1.1	The $C_{27}$ image of $G$ . . . . .	18
4.1.2	The $C_2 \times C_{27}$ image of $G$ . . . . .	19
4.1.3	The $C_4 \times C_{27}$ image of $G$ . . . . .	20
4.2	$(465, 145, 45)$ cyclic difference sets . . . . .	20
4.3	$(1785, 224, 28)$ cyclic difference sets . . . . .	23
<b>5</b>	<b>Conclusion</b>	<b>25</b>

---

\*University of Kansas

†University of California, Berkeley

# 1 Introduction

Given a group  $G$  of order  $v$ , a  $(v, k, \lambda)$  **difference set**  $D$  is a  $k$ -subset of  $G$  such that the multiset of pairs  $d_1 d_2^{-1}$  where  $d_1, d_2 \in D$  gives every non-identity element of  $G$  exactly  $\lambda$  times.

By a **group ring**  $R[G]$ , we shall mean the set of all formal sums of a group  $G$  with coefficients in a ring  $R$ , with addition defined component-wise, and multiplication defined by distributivity and the group operation. The definition of group homomorphisms can be extended to the group ring in a natural way. If  $\phi : G_1 \rightarrow G_2$  is a group homomorphism, then the map  $\phi : R[G_1] \rightarrow R[G_2]$  is defined by  $\phi(\sum d_i g_i) = \sum d_i \phi(g_i)$ . For a subset  $S \subseteq G$ , we can associate to  $S$  an element of  $R[G]$  defined to have coefficient 1 for every element of  $S$  and 0 for all other elements. For convenience, we will use  $S$  to mean both the subset of  $G$  and the element of  $R[G]$  associated with it. Finally, let  $S^{(-1)}$  denote the formal sum of the inverses of the elements of  $S$ . Then we have the following relation for a  $(v, k, \lambda)$ -difference set  $D$  ( $1_G$  denotes the identity of  $G$ ):

$$DD^{(-1)} = (k - \lambda) \cdot 1_G + \lambda \cdot G \tag{1}$$

The reason for this identity is that the left hand side expanded out is precisely the sum of all the differences in  $D$ . Each non-identity element of  $G$  appears  $\lambda$  times, and the identity appears  $k$  times. This is represented in the right hand side appropriately.

We now give two examples of difference sets in cyclic groups. The second example illustrates looking at images of a difference set under some group homomorphism, and this technique will be used all throughout this paper.

**Example 1.** A  $(7, 3, 1)$  difference set in the group  $\mathbb{Z}/7\mathbb{Z}$  is given by the set  $D = \{1, 2, 4\}$ . In fact, the set of all translates of  $D$ , which are of the form  $g + D = \{g + 1, g + 2, g + 4\}$  where  $g \in \mathbb{Z}/7\mathbb{Z}$  gives the Fano plane, if we consider each translate to define a line.

**Example 2.** In the group  $C_{21} = \langle x \mid x^{21} = 1 \rangle$ ,  $D = \{x^7, x^9, x^{14}, x^{15}, x^{18}\}$  is a  $(21, 5, 1)$  difference set. If we think of  $D$  as an element in  $\mathbb{Z}[C_{21}]$ , then the homomorphism defined by  $x^7 \mapsto 1$  maps  $D$  to  $x + x^2 + x^4 + 2 \cdot 1$ .

# 2 The second multiplier theorem

We now present some facts about difference sets that will be needed in the following nonexistence proofs. A **translate** of a difference set  $D$  is  $gD = \{gd \mid d \in D\}$  for some element  $g \in G$ . By a **numerical multiplier**  $t$  of a difference set  $D$ , we mean the map  $g \mapsto g^t$  is an automorphism of  $G$ , and that this map sends  $D$  to one of its translates. The first result is that if  $\varphi$  is a multiplier of  $D$ , then there is some translate of  $D$  that is fixed by  $\varphi$  [5]. In the previous two examples, both difference sets are fixed by the map  $g \mapsto g^2$ . Our first step in proving nonexistence will be to suppose, without loss of generality, that  $D$  is

a translate fixed by some multiplier. The next result [8] gives a way of finding multipliers for  $D$ .

**Theorem 1.** (*Second Multiplier Theorem*) *Let  $D$  be a  $(v, k, \lambda)$ -difference set in an abelian group  $G$  with exponent  $v^*$ , and let  $m > \lambda$  be a divisor of  $k - \lambda$ . If  $t$  is an integer coprime with  $v$  such that for every prime  $p$  dividing  $m$ , there exists an integer  $i$  for which  $t \equiv p^i \pmod{v^*}$ , then  $t$  is a numerical multiplier of  $D$ .*

This means that once we find such a multiplier  $t$ , then knowing that  $g \in D$  implies that  $g^t \in D$  since  $D$  must remain fixed under the mapping. In fact, multipliers create a partition of  $D$ , and we can examine the orbits under the map  $g \mapsto g^t$ . The orbits can be computed using the GAP computer algebra system [2]. In the group ring  $\mathbb{Z}[G]$ , we can write  $D = \sum d_i g_i$ , where  $g_i$  are the elements of  $G$ ,  $d_i = 0$  if  $g_i \notin D$ , and  $d_i = 1$  if  $g_i \in D$ . The multiplier gives a way to group the coefficients together. That is, elements in the same orbit share the same coefficient.

The next step is to consider canonical homomorphisms  $\phi$  defined from  $G$  to one of its quotient groups. The image of such a homomorphism will have smaller order than  $G$ . It is a fact that if  $t$  is a numerical multiplier of  $D$ , then  $t$  is also a numerical multiplier of  $\phi(D)$ . We can write  $\phi(D) = \sum \alpha_i g'_i$  where  $g'_i$  are elements of  $\phi(G)$ . By applying  $\phi$  to (1), we get:

$$\phi(D)\phi(D^{(-1)}) = (k - \lambda) \cdot 1_{\phi(G)} + \lambda \cdot \frac{|G|}{|\phi(G)|} \cdot \phi(G) \quad (2)$$

We can solve for all  $\alpha_i$  by expanding the left hand side, matching the coefficients with those of the right hand side and using a computer to find all solutions in nonnegative integers.

The final step involves noting that there are relations among the variables  $d_i$  and  $\alpha_i$ . In particular, let  $\alpha_i$  be the coefficient of some element  $g'_i$  of  $\phi(D)$ . Then the sum of the coefficients of all elements in the preimage of  $g'_i$  must add up to  $\alpha_i$ . Again, choosing the right  $\phi$  will give equations that restrict the values that each  $d_i$  may assume. If we look at two different homomorphisms, we may find that these restrictions show that there are no valid values for some  $d_i$ , which completes the proof that  $D$  cannot exist. In some cases, the order of  $G$  may be too big to work with, so instead of starting with  $D$  and showing some images of it do not exist, we start with an image of  $D$  and show that the images of that image do not exist.

So in summary, we first assume  $D$  exists. We then find a numerical multiplier  $t$  for  $D$  and, without loss of generality, let  $D$  be fixed by  $g \mapsto g^t$ . We then look at some homomorphic images of  $D$  and derive restrictions on the coefficients  $d_i$  based on these. Finally, these restrictions will show that there are no valid values for the coefficients  $d_i$ , which implies  $D$  does not exist. We now present this method of contradiction on several examples taken from the list of open cases from the Center for Communications Research at La Jolla [3]. The list of open parameter sets is presented in figure 1.

$(v, k, \lambda)$	$n = k - \lambda$	$v$	Multiplier
(419, 133, 42)	$91 = 7 \cdot 13$	$419 = 419$	?
(465, 145, 45)	$100 = 2^2 \cdot 5^2$	$465 = 3 \cdot 5 \cdot 31$	?
(1123, 154, 21)	$133 = 7 \cdot 19$	$1123 = 1123$	7
(645, 161, 40)	$121 = 11^2$	$645 = 3 \cdot 5 \cdot 43$	11
(1093, 169, 26)	$143 = 11 \cdot 13$	$1093 = 1093$	11
(945, 177, 33)	$144 = 2^4 \cdot 3^2$	$945 = 3^3 \cdot 5 \cdot 7$	?
(1111, 186, 31)	$155 = 5 \cdot 31$	$1111 = 11 \cdot 101$	188
(1380, 197, 28)	$169 = 13^2$	$1380 = 2^2 \cdot 3 \cdot 5 \cdot 23$	13
(5859, 203, 7)	$196 = 2^2 \cdot 7^2$	$5859 = 3^3 \cdot 7 \cdot 31$	?
(469, 208, 92)	$116 = 2^2 \cdot 29$	$469 = 7 \cdot 67$	?
(1785, 224, 28)	$196 = 2^2 \cdot 7^2$	$1785 = 3 \cdot 5 \cdot 7 \cdot 17$	?
(1801, 225, 28)	$197 = 197$	$1801 = 1801$	197
(2291, 230, 23)	$207 = 3^2 \cdot 23$	$2291 = 29 \cdot 79$	23
(639, 232, 84)	$148 = 2^2 \cdot 37$	$639 = 3^2 \cdot 71$	37
(2869, 240, 20)	$220 = 2^2 \cdot 5 \cdot 11$	$2869 = 19 \cdot 151$	20
(2574, 249, 24)	$225 = 3^2 \cdot 5^2$	$2574 = 2 \cdot 3^2 \cdot 11 \cdot 13$	5
(2160, 255, 30)	$225 = 3^2 \cdot 5^2$	$2160 = 2^4 \cdot 3^3 \cdot 5$	?
(1925, 260, 35)	$225 = 3^2 \cdot 5^2$	$1925 = 5^2 \cdot 7 \cdot 11$	?
(1381, 276, 55)	$221 = 13 \cdot 17$	$1381 = 1381$	13
(817, 289, 102)	$187 = 11 \cdot 17$	$817 = 19 \cdot 43$	11
(781, 300, 115)	$185 = 5 \cdot 37$	$781 = 11 \cdot 71$	?
(3439, 1719, 859)	$860 = 2^2 \cdot 5 \cdot 43$	$3439 = 19 \cdot 181$	?
(4355, 2177, 1088)	$1089 = 3^2 \cdot 11^2$	$4355 = 5 \cdot 13 \cdot 67$	131
(8591, 4295, 2147)	$2148 = 2^2 \cdot 3 \cdot 179$	$8591 = 11^2 \cdot 71$	243
(8835, 4417, 2208)	$2209 = 47^2$	$8835 = 3 \cdot 5 \cdot 19 \cdot 31$	47
(9135, 4567, 2283)	$2284 = 2^2 \cdot 571$	$9135 = 3^2 \cdot 5 \cdot 7 \cdot 29$	16
(9215, 4607, 2303)	$2304 = 2^8 \cdot 3^2$	$9215 = 5 \cdot 19 \cdot 97$	2
(9423, 4711, 2355)	$2356 = 2^2 \cdot 19 \cdot 31$	$9423 = 3^3 \cdot 349$	1351

Figure 1: Open parameter sets from CCR website

Coef.	Elements of $\mathbb{Z}[C_{143}]$	Size
$d_0$	1	1
$d_1$	$y + y^5 + y^{12} + y^8$	4
$d_2$	$y^2 + y^{10} + y^{11} + y^3$	4
$d_3$	$y^4 + y^7 + y^9 + y^6$	4
$d_4$	$x + x^5 + x^3 + x^4 + x^9$	5
$d_5$	$(x + x^5 + x^3 + x^4 + x^9)(y + y^5 + y^{12} + y^8)$	20
$d_6$	$(x + x^5 + x^3 + x^4 + x^9)(y^2 + y^{10} + y^{11} + y^3)$	20
$d_7$	$(x + x^5 + x^3 + x^4 + x^9)(y^4 + y^7 + y^9 + y^6)$	20
$d_8$	$x^2 + x^{10} + x^6 + x^8 + x^7$	5
$d_9$	$(x^2 + x^{10} + x^6 + x^8 + x^7)(y + y^5 + y^{12} + y^8)$	20
$d_{10}$	$(x^2 + x^{10} + x^6 + x^8 + x^7)(y^2 + y^{10} + y^{11} + y^3)$	20
$d_{11}$	$(x^2 + x^{10} + x^6 + x^8 + x^7)(y^4 + y^7 + y^9 + y^6)$	20

Figure 2: Orbits for  $C_{143}$  under  $g \mapsto g^5$

## 2.1 (2574, 249, 24) cyclic difference sets

Let  $C_{2574}$  be the cyclic group of order 2574. Suppose  $D$  is a (2574, 249, 24) difference set. Since  $C_{2574}$  is cyclic, it contains a subgroup of order 18, so there is a quotient group of  $C_{2574}$  isomorphic to  $C_{143} = \langle x, y \mid x^{11} = y^{13} = 1, xy = yx \rangle$ , the cyclic group of order 143. We consider the natural homomorphism  $\phi$  from  $C_{2574}$  to this quotient group to show that  $D$  does not exist.

To find a multiplier, let  $m = 25$ . The only prime dividing  $m$  is 5, so 5 is a multiplier of  $D$ . We present the orbits of the  $C_{143}$  image under this automorphism in figure 2.

Then  $D$  can be expressed as  $\sum d_i O_i$  where  $O_i$  is the element of  $\mathbb{Z}[C_{143}]$  that corresponds to  $d_i$  in figure 2. Each  $d_i$  corresponds to the number of elements of  $D$  that get mapped to the orbit  $O_i$  by the homomorphism  $\phi$ , so it is enough to show that there are no satisfactory values for the coefficients  $d_i$ . First note that the  $C_{143}$  image has two homomorphic images, one isomorphic to  $C_{13}$  and the other isomorphic to  $C_{11}$ .

We first consider the  $C_{13}$  image of the homomorphism defined by  $x \mapsto 1, y \mapsto y$ . The orbits under  $g \mapsto g^5$  of this image are given in figure 3, and  $D = \alpha_0 + \alpha_1(y + y^5 + y^{12} + y^8) + \alpha_2(y^2 + y^{10} + y^{11} + y^3) + \alpha_3(y^4 + y^7 + y^9 + y^6)$ . Since this map is 11 to 1, and  $\phi$  is 18 to 1, we have the equation

$$DD^{(-1)} = 225 \cdot 1 + 24 \cdot 18 \cdot 11 \cdot (1 + y + \dots + y^{12}) \quad (3)$$

Expanding the polynomials for  $D$  and  $D^{(-1)}$  and matching coefficients gives

Coef.	Elements of $\mathbb{Z}[C_{13}]$	Size
$\alpha_0$	1	1
$\alpha_1$	$y + y^5 + y^{12} + y^8$	4
$\alpha_2$	$y^2 + y^{10} + y^{11} + y^3$	4
$\alpha_3$	$y^4 + y^7 + y^9 + y^6$	4

Figure 3: Orbits for  $C_{13}$  under  $g \mapsto g^5$

the following equations:

$$\alpha_0 + 4(\alpha_1 + \alpha_2 + \alpha_3) = 249 \quad (4)$$

$$\alpha_0^2 + 4(\alpha_1^2 + \alpha_2^2 + \alpha_3^2) = 4977 \quad (5)$$

$$\alpha_1^2 + 2(\alpha_0\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 + \alpha_3^2) + 4\alpha_1\alpha_2 = 4752 \quad (6)$$

$$\alpha_2^2 + 2(\alpha_1\alpha_2 + \alpha_0\alpha_3 + \alpha_1\alpha_3 + \alpha_1^2) + 4\alpha_2\alpha_3 = 4752 \quad (7)$$

$$\alpha_3^2 + 2(\alpha_0\alpha_1 + \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_2^2) + 4\alpha_1\alpha_3 = 4752 \quad (8)$$

Of course, the solution must be nonnegative integers, and a computer search gives  $\alpha_0 = 33, \alpha_1 = \alpha_2 = \alpha_3 = 18$ . Finally, note that 1 element from the orbit of  $d_0$ , and 5 elements from each of the orbits corresponding to  $d_4$  and  $d_8$  in the  $C_{143}$  image get mapped to the orbit of  $C_{13}$  corresponding to  $\alpha_0$ . This gives the equation  $\alpha_0 = d_0 + 5(d_4 + d_8)$ . Similar observations for the other  $\alpha_i$  give these equations:

$$\alpha_0 = d_0 + 5(d_4 + d_8) \quad (9)$$

$$\alpha_1 = d_1 + 5(d_5 + d_9) \quad (10)$$

$$\alpha_2 = d_2 + 5(d_6 + d_{10}) \quad (11)$$

$$\alpha_3 = d_3 + 5(d_7 + d_{11}) \quad (12)$$

Since  $d_i \in \mathbb{Z}_{\geq 0}$ , and  $\alpha_i \equiv 3 \pmod{5}$ , we conclude that  $d_i \equiv 3 \pmod{5}$ , and therefore  $d_i \geq 3$ , for  $0 \leq i \leq 3$ .

Now we do the same thing for the  $C_{11}$  image. We define a map  $x \mapsto x, y \mapsto 1$ , and the orbits are given in figure 4. We write  $D = \beta_0 + \beta_1(x + x^5 + x^3 + x^4 + x^9) + \beta_2(x^2 + x^{10} + x^6 + x^8 + x^7)$ , and have

$$DD^{(-1)} = 225 \cdot 1 + 24 \cdot 18 \cdot 13 \cdot (1 + x + \cdots + x^{10}) \quad (13)$$

Again, we expand the polynomials to get a set of equations:

$$\beta_0 + 5(\beta_1 + \beta_2) = 249 \quad (14)$$

$$\beta_0^2 + 5(\beta_1^2 + \beta_2^2) = 5841 \quad (15)$$

$$\beta_0\beta_1 + \beta_0\beta_2 + 2(\beta_1^2 + \beta_2^2) + 5\beta_1\beta_2 = 5616 \quad (16)$$

Coef.	Elements of $\mathbb{Z}[C_{11}]$	Size
$\beta_0$	1	1
$\beta_1$	$x + x^5 + x^3 + x^4 + x^9$	5
$\beta_2$	$x^2 + x^{10} + x^6 + x^8 + x^7$	5

Figure 4: Orbits for  $C_{11}$  under  $g \mapsto g^5$

Finally, using the observation of which orbits of  $C_{143}$  get mapped to which orbits of  $C_{11}$  give the following equations:

$$\beta_0 = d_0 + 4(d_1 + d_2 + d_3) \quad (17)$$

$$\beta_1 = d_4 + 4(d_5 + d_6 + d_7) \quad (18)$$

$$\beta_2 = d_8 + 4(d_9 + d_{10} + d_{11}) \quad (19)$$

Since  $d_i \geq 3$  for  $0 \leq i \leq 3$ , we conclude that  $\beta_0 \geq 39$ . But this restriction means there is no solution in nonnegative integers for  $\beta_0, \beta_1, \beta_2$ . Thus, since there is no  $C_{11}$  image for  $D$ , it does not exist.

## 2.2 (817, 289, 102) cyclic difference sets

Let  $C_{817} = \langle x, y \mid x^{19} = y^{43} = 1, xy = yx \rangle$  be the cyclic group of order 817, and suppose  $D$  is a (817, 289, 102) difference set in  $C_{817}$ . The prime factorization of  $m = 187$  is  $11 \cdot 17$ . Note that  $11 \equiv 17^3 \pmod{817}$ , and  $\gcd(11, 817) = 1$ , so without loss of generality, the map  $g \mapsto g^{11}$  fixes  $D$ . The orbits are presented in figures 5 and 5.

The image of the homomorphism defined by  $x \mapsto 1, y \mapsto y$  is isomorphic to  $C_{43}$ . The orbits for this image are presented in figure 7. Since this is a 19 to 1 mapping, the following formula must be satisfied:

$$DD^{(-1)} = 187 \cdot 1 + 102 \cdot 19 \cdot (1 + x + \cdots + x^{42}) \quad (20)$$

Expand  $DD^{(-1)}$  and match up coefficients to get a system of equations that must be satisfied. A computer search reveals the following solutions in the form  $(\alpha_0, \dots, \alpha_6)$ , up to equivalence (the other solutions are permutations of one of these three):

$$(2, 3, 6, 8, 9, 7, 8)$$

$$(9, 3, 9, 5, 8, 8, 7)$$

$$(16, 5, 8, 8, 5, 8, 5)$$

Finally, if we consider which elements of  $C_{817}$  get mapped to which elements of

Coef.	Elements of $\mathbb{Z}[C_{817}]$	Size
$d_0$	1	1
$d_1$	$x + x^{11} + x^7$	3
$d_2$	$x^2 + x^3 + x^{14}$	3
$d_3$	$x^4 + x^6 + x^9$	3
$d_4$	$x^5 + x^{17} + x^{16}$	3
$d_5$	$x^8 + x^{12} + x^{18}$	3
$d_6$	$x^{10} + x^{15} + x^{13}$	3
$d_7$	$y + y^{11} + y^{35} + y^{41} + y^{21} + y^{16} + y^4$	7
$d_8$	$(x + x^{11} + x^7)(y + y^{11} + y^{35} + y^{41} + y^{21} + y^{16} + y^4)$	21
$d_9$	$(x^2 + x^3 + x^{14})(y + y^{11} + y^{35} + y^{41} + y^{21} + y^{16} + y^4)$	21
$d_{10}$	$(x^4 + x^6 + x^9)(y + y^{11} + y^{35} + y^{41} + y^{21} + y^{16} + y^4)$	21
$d_{11}$	$(x^5 + x^{17} + x^{16})(y + y^{11} + y^{35} + y^{41} + y^{21} + y^{16} + y^4)$	21
$d_{12}$	$(x^8 + x^{12} + x^{18})(y + y^{11} + y^{35} + y^{41} + y^{21} + y^{16} + y^4)$	21
$d_{13}$	$(x^{10} + x^{15} + x^{13})(y + y^{11} + y^{35} + y^{41} + y^{21} + y^{16} + y^4)$	21
$d_{14}$	$y^2 + y^{22} + y^{27} + y^{39} + y^{42} + y^{32} + y^8$	7
$d_{15}$	$(x + x^{11} + x^7)(y^2 + y^{22} + y^{27} + y^{39} + y^{42} + y^{32} + y^8)$	21
$d_{16}$	$(x^2 + x^3 + x^{14})(y^2 + y^{22} + y^{27} + y^{39} + y^{42} + y^{32} + y^8)$	21
$d_{17}$	$(x^4 + x^6 + x^9)(y^2 + y^{22} + y^{27} + y^{39} + y^{42} + y^{32} + y^8)$	21
$d_{18}$	$(x^5 + x^{17} + x^{16})(y^2 + y^{22} + y^{27} + y^{39} + y^{42} + y^{32} + y^8)$	21
$d_{19}$	$(x^8 + x^{12} + x^{18})(y^2 + y^{22} + y^{27} + y^{39} + y^{42} + y^{32} + y^8)$	21
$d_{20}$	$(x^{10} + x^{15} + x^{13})(y^2 + y^{22} + y^{27} + y^{39} + y^{42} + y^{32} + y^8)$	21
$d_{21}$	$y^3 + y^{33} + y^{19} + y^{37} + y^{20} + y^5 + y^{12}$	7
$d_{22}$	$(x + x^{11} + x^7)(y^3 + y^{33} + y^{19} + y^{37} + y^{20} + y^5 + y^{12})$	21
$d_{23}$	$(x^2 + x^3 + x^{14})(y^3 + y^{33} + y^{19} + y^{37} + y^{20} + y^5 + y^{12})$	21
$d_{24}$	$(x^4 + x^6 + x^9)(y^3 + y^{33} + y^{19} + y^{37} + y^{20} + y^5 + y^{12})$	21

Figure 5: Orbits for  $C_{817}$  under  $g \mapsto g^{11}$

Coef.	Elements of $\mathbb{Z}[C_{817}]$	Size
$d_{25}$	$(x^5 + x^{17} + x^{16})(y^3 + y^{33} + y^{19} + y^{37} + y^{20} + y^5 + y^{12})$	21
$d_{26}$	$(x^8 + x^{12} + x^{18})(y^3 + y^{33} + y^{19} + y^{37} + y^{20} + y^5 + y^{12})$	21
$d_{27}$	$(x^{10} + x^{15} + x^{13})(y^3 + y^{33} + y^{19} + y^{37} + y^{20} + y^5 + y^{12})$	21
$d_{28}$	$y^6 + y^{23} + y^{38} + y^{31} + y^{40} + y^{10} + y^{24}$	7
$d_{29}$	$(x + x^{11} + x^7)(y^6 + y^{23} + y^{38} + y^{31} + y^{40} + y^{10} + y^{24})$	21
$d_{30}$	$(x^2 + x^3 + x^{14})(y^6 + y^{23} + y^{38} + y^{31} + y^{40} + y^{10} + y^{24})$	21
$d_{31}$	$(x^4 + x^6 + x^9)(y^6 + y^{23} + y^{38} + y^{31} + y^{40} + y^{10} + y^{24})$	21
$d_{32}$	$(x^5 + x^{17} + x^{16})(y^6 + y^{23} + y^{38} + y^{31} + y^{40} + y^{10} + y^{24})$	21
$d_{33}$	$(x^8 + x^{12} + x^{18})(y^6 + y^{23} + y^{38} + y^{31} + y^{40} + y^{10} + y^{24})$	21
$d_{34}$	$(x^{10} + x^{15} + x^{13})(y^6 + y^{23} + y^{38} + y^{31} + y^{40} + y^{10} + y^{24})$	21
$d_{35}$	$y^7 + y^{34} + y^{30} + y^{29} + y^{18} + y^{26} + y^{28}$	7
$d_{36}$	$(x + x^{11} + x^7)(y^7 + y^{34} + y^{30} + y^{29} + y^{18} + y^{26} + y^{28})$	21
$d_{37}$	$(x^2 + x^3 + x^{14})(y^7 + y^{34} + y^{30} + y^{29} + y^{18} + y^{26} + y^{28})$	21
$d_{38}$	$(x^4 + x^6 + x^9)(y^7 + y^{34} + y^{30} + y^{29} + y^{18} + y^{26} + y^{28})$	21
$d_{39}$	$(x^5 + x^{17} + x^{16})(y^7 + y^{34} + y^{30} + y^{29} + y^{18} + y^{26} + y^{28})$	21
$d_{40}$	$(x^8 + x^{12} + x^{18})(y^7 + y^{34} + y^{30} + y^{29} + y^{18} + y^{26} + y^{28})$	21
$d_{41}$	$(x^{10} + x^{15} + x^{13})(y^7 + y^{34} + y^{30} + y^{29} + y^{18} + y^{26} + y^{28})$	21
$d_{42}$	$y^9 + y^{13} + y^{14} + y^{25} + y^{17} + y^{15} + y^{36}$	7
$d_{43}$	$(x + x^{11} + x^7)(y^9 + y^{13} + y^{14} + y^{25} + y^{17} + y^{15} + y^{36})$	21
$d_{44}$	$(x^2 + x^3 + x^{14})(y^9 + y^{13} + y^{14} + y^{25} + y^{17} + y^{15} + y^{36})$	21
$d_{45}$	$(x^4 + x^6 + x^9)(y^9 + y^{13} + y^{14} + y^{25} + y^{17} + y^{15} + y^{36})$	21
$d_{46}$	$(x^5 + x^{17} + x^{16})(y^9 + y^{13} + y^{14} + y^{25} + y^{17} + y^{15} + y^{36})$	21
$d_{47}$	$(x^8 + x^{12} + x^{18})(y^9 + y^{13} + y^{14} + y^{25} + y^{17} + y^{15} + y^{36})$	21
$d_{48}$	$(x^{10} + x^{15} + x^{13})(y^9 + y^{13} + y^{14} + y^{25} + y^{17} + y^{15} + y^{36})$	21

Figure 6: Orbits for  $C_{817}$  under  $g \mapsto g^{11}$

Coef.	Elements of $\mathbb{Z}[C_{43}]$	Size
$\alpha_0$	1	1
$\alpha_1$	$y + y^{11} + y^{35} + y^{41} + y^{21} + y^{16} + y^4$	7
$\alpha_2$	$y^2 + y^{22} + y^{27} + y^{39} + y^{42} + y^{32} + y^8$	7
$\alpha_3$	$y^3 + y^{33} + y^{19} + y^{37} + y^{20} + y^5 + y^{12}$	7
$\alpha_4$	$y^6 + y^{23} + y^{38} + y^{31} + y^{40} + y^{10} + y^{24}$	7
$\alpha_5$	$y^7 + y^{34} + y^{30} + y^{29} + y^{18} + y^{26} + y^{28}$	7
$\alpha_6$	$y^9 + y^{13} + y^{14} + y^{25} + y^{17} + y^{15} + y^{36}$	7

Figure 7: Orbits for  $C_{43}$  under  $g \mapsto g^{11}$

$C_{43}$ , we get the following equations:

$$\alpha_0 = d_0 + 3(d_1 + d_2 + d_3 + d_4 + d_5 + d_6) \quad (21)$$

$$\alpha_1 = d_7 + 3(d_8 + d_9 + d_{10} + d_{11} + d_{12} + d_{13}) \quad (22)$$

$$\alpha_2 = d_{14} + 3(d_{15} + d_{16} + d_{17} + d_{18} + d_{19} + d_{20}) \quad (23)$$

$$\alpha_3 = d_{21} + 3(d_{22} + d_{23} + d_{24} + d_{25} + d_{26} + d_{27}) \quad (24)$$

$$\alpha_4 = d_{28} + 3(d_{29} + d_{30} + d_{31} + d_{32} + d_{33} + d_{34}) \quad (25)$$

$$\alpha_5 = d_{35} + 3(d_{36} + d_{37} + d_{38} + d_{39} + d_{40} + d_{41}) \quad (26)$$

$$\alpha_6 = d_{42} + 3(d_{43} + d_{44} + d_{45} + d_{46} + d_{47} + d_{48}) \quad (27)$$

Finally, observe that each  $d_i$  must be either 0 or 1 because it represents whether the orbit  $O_i$  is in  $D$ . This implies  $\alpha_i$  is either 0 or 1 modulo 3. Since each solution contains 8, there is no valid  $C_{43}$  image for  $D$ , which means  $D$  does not exist.

### 2.3 (645, 161, 40) cyclic difference sets

Let  $C_{645} = \langle x, y, z \mid x^3 = y^5 = z^{43} = 1 \rangle$  where  $x, y, z$  commute with one another be the cyclic group of order 645. We consider the quotient group  $C_{645}/\langle x \rangle \cong C_{215}$ . For convenience,  $C_{215} = \langle y, z \mid y^5 = z^{43} = 1, yz = zy \rangle$ . Suppose a (645, 161, 40) difference set  $D$  exists. Using the second multiplier theorem, let  $m = 121$ . The only divisor of 121 is 11, and  $\gcd(11, 645) = 1$ , so without loss of generality,  $D$  is a difference set fixed by the automorphism  $g \mapsto g^{11}$ . The list of orbits of the  $C_{215}$  image are given in figure 8. The natural homomorphism defined from  $C_{645}$  to  $C_{215}$  is a 3 to 1 mapping, which means that  $d_i \leq 3$  for all  $i$ .

Now we consider the  $C_5$  image of  $C_{645}$ . Each of the orbits is given by a single element, so  $D = \sum_{i=0}^4 \alpha_i y^i$  for some values of  $\alpha_i$ . The homomorphism from  $C_{215}$  to  $C_5$  defined by  $y \mapsto y, z \mapsto 1$  gives the equations:

$$\alpha_0 = d_0 + 7(d_1 + d_2 + d_3 + d_4 + d_5 + d_6) \quad (28)$$

$$\alpha_1 = d_7 + 7(d_8 + d_9 + d_{10} + d_{11} + d_{12} + d_{13}) \quad (29)$$

$$\alpha_2 = d_{14} + 7(d_{15} + d_{16} + d_{17} + d_{18} + d_{19} + d_{20}) \quad (30)$$

$$\alpha_3 = d_{21} + 7(d_{22} + d_{23} + d_{24} + d_{25} + d_{26} + d_{27}) \quad (31)$$

$$\alpha_4 = d_{28} + 7(d_{29} + d_{30} + d_{31} + d_{32} + d_{33} + d_{34}) \quad (32)$$

This suggests that  $0 \leq \alpha_i \pmod{7} \leq 3$  by the earlier remark that  $d_i \leq 3$ . Also, the identity in the group ring must also be satisfied:

$$DD^{(-1)} = 121 \cdot 1 + 40 \cdot 43 \cdot 3 \cdot (1 + y + \dots + y^4) \quad (33)$$

Expanding the polynomials on the left hand side and matching coefficients gives

Coef.	Elements of $\mathbb{Z}[C_{215}]$	Size
$d_0$	1	1
$d_1$	$z + z^{11} + z^{35} + z^{41} + z^{21} + z^{16} + z^4$	7
$d_2$	$z^2 + z^{22} + z^{27} + z^{39} + z^{42} + z^{32} + z^8$	7
$d_3$	$z^3 + z^{33} + z^{19} + z^{37} + z^{20} + z^5 + z^{12}$	7
$d_4$	$z^6 + z^{23} + z^{38} + z^{31} + z^{40} + z^{10} + z^{24}$	7
$d_5$	$z^7 + z^{34} + z^{30} + z^{29} + z^{18} + z^{26} + z^{28}$	7
$d_6$	$z^9 + z^{13} + z^{14} + z^{25} + z^{17} + z^{15} + z^{36}$	7
$d_7$	$y$	1
$d_8$	$y(z + z^{11} + z^{35} + z^{41} + z^{21} + z^{16} + z^4)$	7
$d_9$	$y(z^2 + z^{22} + z^{27} + z^{39} + z^{42} + z^{32} + z^8)$	7
$d_{10}$	$y(z^3 + z^{33} + z^{19} + z^{37} + z^{20} + z^5 + z^{12})$	7
$d_{11}$	$y(z^6 + z^{23} + z^{38} + z^{31} + z^{40} + z^{10} + z^{24})$	7
$d_{12}$	$y(z^7 + z^{34} + z^{30} + z^{29} + z^{18} + z^{26} + z^{28})$	7
$d_{13}$	$y(z^9 + z^{13} + z^{14} + z^{25} + z^{17} + z^{15} + z^{36})$	7
$d_{14}$	$y^2$	1
$d_{15}$	$y^2(z + z^{11} + z^{35} + z^{41} + z^{21} + z^{16} + z^4)$	7
$d_{16}$	$y^2(z^2 + z^{22} + z^{27} + z^{39} + z^{42} + z^{32} + z^8)$	7
$d_{17}$	$y^2(z^3 + z^{33} + z^{19} + z^{37} + z^{20} + z^5 + z^{12})$	7
$d_{18}$	$y^2(z^6 + z^{23} + z^{38} + z^{31} + z^{40} + z^{10} + z^{24})$	7
$d_{19}$	$y^2(z^7 + z^{34} + z^{30} + z^{29} + z^{18} + z^{26} + z^{28})$	7
$d_{20}$	$y^2(z^9 + z^{13} + z^{14} + z^{25} + z^{17} + z^{15} + z^{36})$	7
$d_{21}$	$y^3$	1
$d_{22}$	$y^3(z + z^{11} + z^{35} + z^{41} + z^{21} + z^{16} + z^4)$	7
$d_{23}$	$y^3(z^2 + z^{22} + z^{27} + z^{39} + z^{42} + z^{32} + z^8)$	7
$d_{24}$	$y^3(z^3 + z^{33} + z^{19} + z^{37} + z^{20} + z^5 + z^{12})$	7
$d_{25}$	$y^3(z^6 + z^{23} + z^{38} + z^{31} + z^{40} + z^{10} + z^{24})$	7
$d_{26}$	$y^3(z^7 + z^{34} + z^{30} + z^{29} + z^{18} + z^{26} + z^{28})$	7
$d_{27}$	$y^3(z^9 + z^{13} + z^{14} + z^{25} + z^{17} + z^{15} + z^{36})$	7
$d_{28}$	$y^4$	1
$d_{29}$	$y^4(z + z^{11} + z^{35} + z^{41} + z^{21} + z^{16} + z^4)$	7
$d_{30}$	$y^4(z^2 + z^{22} + z^{27} + z^{39} + z^{42} + z^{32} + z^8)$	7
$d_{31}$	$y^4(z^3 + z^{33} + z^{19} + z^{37} + z^{20} + z^5 + z^{12})$	7
$d_{32}$	$y^4(z^6 + z^{23} + z^{38} + z^{31} + z^{40} + z^{10} + z^{24})$	7
$d_{33}$	$y^4(z^7 + z^{34} + z^{30} + z^{29} + z^{18} + z^{26} + z^{28})$	7
$d_{34}$	$y^4(z^9 + z^{13} + z^{14} + z^{25} + z^{17} + z^{15} + z^{36})$	7

Figure 8: Orbits for  $C_{215}$  under  $g \mapsto g^{11}$

Coef.	Elements of $\mathbb{Z}[C_{115}]$	Size
$d_0$	1	1
$d_1$	$x + x^3 + x^4 + x^2$	4
$d_2$	$y + y^{13} + y^8 + y^{12} + y^{18} + y^4 + y^6 + y^9 + y^2 + y^3 + y^{16}$	11
$d_3$	$O_1 O_2$	44
$d_4$	$y^5 + y^{19} + y^{17} + y^{14} + y^{21} + y^{20} + y^7 + y^{22} + y^{10} + y^{15} + y^{11}$	11
$d_5$	$O_1 O_4$	44

Figure 9: Orbits for  $C_{115}$  under  $g \mapsto g^{13}$

the following set of equations:

$$\alpha_0 + \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 161 \quad (34)$$

$$\alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2 = 5281 \quad (35)$$

$$\alpha_0 \alpha_1 + \alpha_1 \alpha_2 + \alpha_2 \alpha_3 + \alpha_0 \alpha_4 + \alpha_3 \alpha_4 = 5160 \quad (36)$$

$$\alpha_0 \alpha_2 + \alpha_0 \alpha_3 + \alpha_1 \alpha_3 + \alpha_1 \alpha_4 + \alpha_2 \alpha_4 = 5160 \quad (37)$$

A computer search gives the following solutions up to equivalence (the other solutions are simply a permutation of the values):

$$(36, 24, 32, 36, 33)$$

$$(36, 26, 29, 38, 32)$$

$$(41, 30, 30, 30, 30)$$

However, the first two solutions contain a 32, which is 4 modulo 7, and the last equation contains a 41, which is 6 modulo 7, so none of these solutions are compatible with our previous results. This contradiction means that there is no valid  $C_5$  image for  $D$ , so  $D$  does not exist.

## 2.4 (1380, 197, 28) cyclic difference sets

Let  $C_{1380}$  be the cyclic group of order 1380. If  $H$  is a subgroup of  $C_{1380}$  of order 12, then consider the quotient group  $C_{115} \cong C_{1380}/H$ . Suppose  $D$  is a (1380, 197, 28) cyclic difference set. Using the second multiplier theorem, let  $m = 169$ . The only prime divisor of 169 is 13, and  $\gcd(13, 1380) = 1$ , so without loss of generality,  $D$  is fixed by  $g \mapsto g^{13}$ . Finally, denote  $C_{115} = \langle x, y \mid x^5 = y^{23} = 1, xy = yx \rangle$ . The orbits of  $D$  in  $C_{115}$  are given in figure 9. By  $O_i$ , we mean the orbit given with coefficient  $d_i$ .

Now consider the homomorphism defined by  $x \mapsto x, y \mapsto 1$ . The image is isomorphic to  $C_5$ . The two orbits are 1, with coefficient  $\alpha_0$ , and  $x + x^2 + x^3 + x^4$ , with coefficient  $\alpha_1$ . Then the following identity must be satisfied since we are considering a 276 to 1 mapping of  $D$  to its image in  $C_5$ :

$$DD^{(-1)} = 169 \cdot 1 + 28 \cdot 276 \cdot (1 + x + \cdots + x^4) \quad (38)$$

Coef.	Elements of $\mathbb{Z}[C_{23}]$	Size
$\beta_0$	1	1
$\beta_1$	$y + y^{13} + y^8 + y^{12} + y^{18} + y^4 + y^6 + y^9 + y^2 + y^3 + y^{16}$	11
$\beta_2$	$y^5 + y^{19} + y^{17} + y^{14} + y^{21} + y^{20} + y^7 + y^{22} + y^{10} + y^{15} + y^{11}$	11

Figure 10: Orbits for  $C_{23}$  under  $g \mapsto g^{13}$

Expanding the left hand side and solving, the answer is  $\alpha_0 = 29, \alpha_1 = 42$ . Considering which elements of  $C_{115}$  get mapped to the identity of  $C_5$  gives the equation

$$\alpha_0 = d_0 + 11(d_2 + d_4) \quad (39)$$

Since  $\alpha_0 = 29$ , it follows that  $d_0 \equiv 7 \pmod{11}$ . Since  $H$  is a subgroup of order 12, the cosets of  $C_{115}$  are of size 12, so each coefficient is no larger than 12, which implies that  $d_0 = 7$ .

We do the same with the homomorphism  $x \mapsto 1, y \mapsto y$ . The image is isomorphic to  $C_{23}$ , and the orbits are presented in figure 10. This is a 60 to 1 mapping, so the following identity holds:

$$DD^{(-1)} = 169 \cdot 1 + 28 \cdot 60 \cdot (1 + y + \dots + y^{22}) \quad (40)$$

Solving in a similar manner, the only solution is  $\beta_0 = 21, \beta_1 = \beta_2 = 8$ . Finally, seeing what gets mapped to the identity of  $C_{23}$  gives the equation

$$\beta_0 = d_0 + 4d_1 \quad (41)$$

which implies that  $d_0 \equiv 1 \pmod{4}$ . However,  $d_0 = 7$ , so there is a contradiction. Therefore,  $D$  does not have a valid  $C_{115}$  image, so does not exist.

### 3 Some remarks on the multiplier conjecture

A much stronger statement than the second multiplier theorem is the so called multiplier conjecture:

**Conjecture 2.** *Given a  $(v, k, \lambda)$  difference set  $D$  in an abelian group  $G$ , any prime  $p$  that divides  $k - \lambda$  but does not divide  $v$  is a multiplier of  $D$ .*

If we assume the conjecture to be true, a few more of the parameter sets can be shown not to exist:

- $(1123, 154, 21)$  – 19 divides 133, and gives three orbits of size 1, 561, and 561. The difference set must be a union of some of these, but also must be of size 154.
- $(1093, 169, 26)$  – 13 divides 143, and gives 28 orbits of size 39, and 1 of size 1. Since  $169 \equiv 5 \pmod{39}$ , there is no way to have union some of these orbits to get a set of size 169.

Coef.	Elements of $\mathbb{Z}[C_{35}]$	Size
$\alpha_0$	1	1
$\alpha_1$	$x + x^2 + x^4 + x^3$	4
$\alpha_2$	$y + y^2 + y^4$	3
$\alpha_3$	$(x + x^2 + x^4 + x^3)(y + y^2 + y^4)$	12
$\alpha_4$	$y^3 + y^6 + y^5$	3
$\alpha_5$	$(x + x^2 + x^4 + x^3)(y^3 + y^6 + y^5)$	12

Figure 11: Orbits for  $C_{35}$  under  $g \mapsto g^2$

- (469, 208, 92) – 2 divides 116, and gives 7 orbits of size 66, 2 of size 3, and 1 of size 1. But  $208 \equiv 10 \pmod{66}$ , and  $2 \cdot 3 + 1 < 10$
- (2291, 230, 23) – 3 divides 207, and gives one orbit each of the following sizes: 1, 78, and 28, and two of size 1092.
- (639, 232, 84) – 2 divides 148, and gives one orbit of each of the sizes 1, 2, and 6, and two orbits of each of the sizes 210, 70, and 35. Since  $232 \equiv 22 \pmod{210}$ , there is no way to get a set of size 232.
- (1381, 276, 55) – 17 divides 221, and gives one orbit of size 1, and four orbits of size 345.

The following parameter set can be shown not to exist using similar techniques from the previous section and assuming the multiplier conjecture. It is also presented in the next section using techniques from algebraic number theory and rational idempotents.

### 3.1 (1785, 224, 28) cyclic difference sets

Define  $C_{1785} = \langle w, x, y, z \mid w^3 = x^5 = y^7 = z^{17} = 1 \rangle$  with  $w, x, y, z$  each commuting with one another. Assume that a (1785, 224, 28) difference set  $D$  exists. Then the multiplier conjecture shows that 2 is a multiplier of  $D$ . The homomorphism defined by  $w \mapsto 1, x \mapsto x, y \mapsto y, z \mapsto 1$  has an image isomorphic to  $C_{35}$ . The orbits under  $g \mapsto g^2$  of this image are given in figure 11. An exhaustive search shows that the only valid solutions  $(\alpha_0, \dots, \alpha_5)$  for the values of the coefficients of the  $C_{35}$  image are

$$(17, 6, 3, 6, 10, 6)$$

$$(20, 6, 6, 6, 6, 6)$$

$$(17, 6, 10, 6, 3, 6)$$

Let  $c_{i,j,k,l}$  denote the coefficient of the orbit generated by  $w^i x^j y^k z^l$  under  $g \mapsto g^2$  in  $C_{1785}$ . There are 51 elements that get mapped to the identity of the  $C_{35}$  image by the homomorphism mentioned earlier. A simple check shows that 1

Coef.	Elements of $\mathbb{Z}[C_{17}]$	Size
$\beta_0$	1	1
$\beta_1$	$z + z^2 + z^4 + z^8 + z^{16} + z^{15} + z^{13} + z^9$	8
$\beta_2$	$z^3 + z^6 + z^{12} + z^7 + z^{14} + z^{11} + z^5 + z^{10}$	8

Figure 12: Orbits for  $C_{17}$  under  $g \mapsto g^2$

element comes from the orbit of 1, 2 from  $w$ , and 8 from the orbits generated by  $z, wz, w^2z, z^3, wz^3$ , and  $x^2z^3$ . So we get the following equation:

$$\alpha_0 = c_{0,0,0,0} + 2c_{1,0,0,0} + 8(c_{0,0,0,1} + \cdots + c_{2,0,0,3}) \quad (42)$$

where  $\alpha_0 \in \{17, 20\}$ . However, each  $c_{i,j,k,l}$  has to either be 0 or 1 since it represents whether the element is in  $D$  or not, so this immediately rules out 20, which forces  $c_{0,0,0,0} = 1$ , so the identity element must be in  $D$ .

Now consider the homomorphism defined by  $w \mapsto 1, x \mapsto 1, y \mapsto 1, z \mapsto z$ , with image isomorphic to  $C_{17}$ . The orbits of this image are given in figure 12. A search shows the only solution is  $\beta_0 = 0$  and  $\beta_1 = \beta_2 = 14$ . However, this implies that no elements in the kernel of this homomorphism are in  $D$ , but the identity is in the kernel, and is in  $D$ . Thus,  $D$  does not exist.

We present a few more of the parameter sets in the following section using techniques that do not rely on multipliers. The remaining parameter sets might also be shown not to exist through the multiplier conjecture using the computer search techniques of the previous section, but this was not heavily investigated.

## 4 Algebraic number theory

We will now introduce some definitions and facts of algebraic number theory to further search for difference sets using rational idempotents. If  $G$  is abelian, we define  $G^*$  to be the set of characters, or linear representations of  $G$ . This group,  $G^*$  will be the dual group and is isomorphic to  $G$ . Since  $G$  is finite and abelian in our cases, we know that  $G = \langle x_1 \rangle \times \langle x_2 \rangle \times \cdots \times \langle x_r \rangle$  where each  $x_i$  is the generator of a cyclic group. If the order of  $x_i$  in its cyclic group is  $b_i$ , we may uniquely define a character,  $\chi_j$ , which will be a function such that  $\chi_j(x_i) = \zeta_{b_i}^j$  for  $0 \leq j < b_i$  and where  $\zeta_{b_i}$  is a primitive  $b_i$ th root of unity. Then  $\chi_{j_1, j_2, \dots, j_r}$  will denote the character such that  $x_i \mapsto \zeta_{b_i}^{j_i}$  for all  $i$  and  $G^* := \{\chi_{j_1, j_2, \dots, j_r} \mid 0 \leq j_i < b_i\}$ . Note that  $\chi$  is a linear representation which is a homomorphism of  $G$  into the multiplicative group of  $\mathbb{C}$ .

An **idempotent** is an element  $e$  such that  $e^2 = e$ . It is important to note that in the rational group ring,  $\mathbb{Q}[G]$ , any subgroup  $H$  gives an idempotent  $e = \frac{H}{|H|}$ . Then, given any character,  $\chi \in G^*$ , we can define the group ring element

$$e_\chi := \frac{1}{|G|} \sum_{g \in G} \overline{\chi(g)} \cdot g \quad (43)$$

to be the idempotent associated with  $\chi$  [1]. Given a subfield  $K$  contained in  $\mathbb{C}$ , we can define the inner product of  $K[G]$  by  $\langle \alpha, \beta \rangle := \frac{1}{|H|} \sum a_g \cdot b_g$ . Then if  $\chi$  is a character of  $G^*$ , then  $\langle e_\chi, e_\chi \rangle = 1$ , or  $\chi(e_\chi) = 1$ . Also, if  $\chi_1 \neq \chi_2$ , then  $\langle e_{\chi_1}, e_{\chi_2} \rangle = 0$ , or  $\chi_1(e_{\chi_2}) = 0$ . Thus, the set of idempotents,  $\{e_\chi \mid \chi \in G^*\}$  forms an orthonormal basis for  $\mathbb{C}[G]$ , which we call the **dual basis**. It is known that every element in a vector space can be written as a unique combination of elements in the basis. Thus, for  $X$  in  $\mathbb{C}[G]$ , we can write  $X = \sum_{\chi \in G^*} x_\chi e_\chi$ . Next, since  $\chi_1(e_{\chi_2}) = 1$  if and only if  $\chi_1 = \chi_2$ , by applying  $\chi$  to both sides of the above equation, we have  $\chi(X) = x_\chi$ , and we have the following equation:

$$X = \sum_{\chi \in G^*} \chi(X) e_\chi \quad (44)$$

We define a  $\chi$ -**alias** for  $X$  to be an element  $A$  such that  $\chi(A) = \chi(X)$ . If  $\Phi = \chi_1, \chi_2, \dots, \chi_r$  is the set of characters of  $G$ , then  $A$  is a  $\Phi$ -alias for  $X$  if  $\chi_j(X) = \chi_j(A)$  for all  $\chi_j \in \Phi$ . There may be many such  $\Phi$ -aliases (see [1]).

It will be our focus to construct a difference set  $D$  in this manner, such that  $D = \sum_{\chi \in G^*} \alpha_\chi e_\chi$  where each  $\alpha_\chi$  is a  $\chi$ -alias. However, the difference set is a combinatorial object  $D \in \mathbb{Z}[G]$ , and the characters,  $\chi$ , and their associated idempotents,  $e_\chi$ , lie in  $\mathbb{C}[G]$ . This presents an interesting problem. First note that two characters are equivalent,  $\chi_1 \sim \chi_2$ , if and only if their kernels are equal ( $\ker(\chi_1) = \ker(\chi_2)$ ). We define the group ring element,  $[e_\chi]$  as follows:

$$[e_\chi] = \sum_{\chi' \sim \chi} e_{\chi'} \quad (45)$$

Because  $[e_\chi]$  and each of its coordinates are fixed by any Galois automorphism, the coordinates of  $[e_\chi]$  must be in the Galois group. So  $[e_\chi]$  is a **rational idempotent** in  $\mathbb{Q}[G]$  which makes looking for combinatorial objects easier. Thus, if  $\{\chi_1, \chi_2, \dots, \chi_t\}$  is a set of representatives from every equivalence class of characters in  $G^*$ , we can express our difference set as a rational idempotent decomposition:

$$D = \sum_{j=0}^t \alpha_j [e_{\chi_j}] \quad (46)$$

It is easy to show that if  $\chi_1$  and  $\chi_2$  have orders  $m_1$  and  $m_2$  that are relatively prime, then  $[e_{\chi_1, \chi_2}] = [e_{\chi_1}][e_{\chi_2}]$ . We will use this to give a “factoring” of rational idempotents. The next theorem [1] tells us what the rational idempotents of a cyclic group of prime power must look like.

**Theorem 3.** *Let  $\langle y \mid y^{p^b} = 1 \rangle$  be a cyclic group of order  $p^b$  generated by  $y$ . Then*

$$[e_{p^b}] = [e_0] = e_{p^b} = \frac{1}{p^b} \langle y \rangle$$

and for  $0 \leq j < b$

$$[e_{p^j}] = \frac{1}{p^{j+1}} (p \langle y^{p^{b-j}} \rangle - \langle y^{p^{b-j-1}} \rangle)$$

We can check the above theorem by taking the characters associated with the rational idempotents:  $\chi_{p^i}(e_{\chi_{p^j}}) = 1$  if and only if  $i = j$ . Otherwise,  $\chi_{p^i}(e_{\chi_{p^j}}) = 0$ .

Since difference sets must have the property  $DD^{(-1)} = n \cdot 1_G + \lambda \cdot G$ , the  $\chi$ -aliases must have values that will satisfy this equation. Thus,  $\chi(\alpha_0)$ , the image of the  $\chi$ -alias associated with the trivial idempotent, must be  $k$ . Furthermore,  $\chi(\alpha_i)\chi(\overline{\alpha_i}) = n$  for all  $0 < i \leq j$ ,  $\chi(\alpha_i) \in \mathbb{Z}[\zeta_v]$ , and  $(\chi(\alpha_i))(\overline{\chi(\alpha_i)}) = (n)$  where  $(x)$  means the principal ideal generated by  $x$  in  $\mathbb{Z}[\zeta_v]$ . Thus, we must consider how  $\chi(\alpha_i)$  will factor in the cyclotomic rings  $\mathbb{Z}[\zeta_m]$ . We will use the next result [1] extensively.

**Theorem 4.** *If  $n \in \mathbb{Z}$ , we first factor  $n$  over the integers to get  $n = \prod_i p_i^{\alpha_i}$ . Then, we factor each principal ideal  $(p_i)$  over  $\mathbb{Z}[\zeta_m]$ .*

1. *If  $m = p^a$ , then the ideal  $(1 - \zeta_m)$  is prime and*

$$(p) = (1 - \zeta_m)^{p^{a-1}(p-1)}$$

*We say  $p$  is completely ramified. In this case, the factors of  $p$  are fixed by conjugation. Thus, since we need choose factors of  $p$  to satisfy  $\delta$  in the equation  $\delta\overline{\delta} = n$ , these factors will not interest us.*

2. *If  $m$  and  $p$  are relatively prime, then  $p$  will factor into  $g = \frac{\varphi(m)}{|p|_m}$  distinct prime ideals, where  $\varphi(m)$  is the Euler totient function of  $m$ , and  $|p|_m$  is the order of  $p$  in the multiplicative group of units  $U(m)$ .*

$$(p) = \prod_{j=1}^g \pi_j$$

*We say  $p$  is unramified in this case, and the ideals  $\pi_j$  have order  $|p|_m$ .*

3. *If  $m = p^a s$  where  $s$  and  $p$  are relatively prime, then there are  $g = \frac{\varphi(s)}{|p|_s}$  distinct prime ideals  $\pi_j$  such that*

$$(p) = \prod_{j=1}^g \pi_j^{p^{a-1}(p-1)}$$

We look for these factorings by using software such as PARI, GAP, and by comparing the factoring of  $(p)$  in  $\mathbb{Z}[\zeta_m]$  with how  $(p)$  factors in smaller number rings  $\mathbb{Z}[\zeta_k]$  where  $k$  divides  $m$ . Using this information, we can build the difference set easily using a rational idempotent decomposition and studying the homomorphic images of the difference set.

#### 4.1 (2160, 255, 30) cyclic difference sets

We first look at the parameter set (2160, 255, 30). The interesting fact about this parameter set is that neither the second multiplier theorem nor even the

multiplier conjecture gives a multiplier to ease the search. This is because all primes that divide  $k - \lambda = 255 = 3^2 5^2$  also divide  $v = 2^4 3^3 5$ . Therefore, we have no choice but to rely upon algebraic number theory and rational idempotents as outlined above.

Let  $G = \langle x, y, z \mid x^{16} = y^{27} = z^5 = 1 \rangle$  be the cyclic group of order 2160, and suppose  $D$  is a  $(2160, 255, 30)$  difference set. Using rational idempotents, we show that there is no valid image for  $D$ . First, we compute the image of  $D$  in the  $C_{27}$  image of  $G$ , then for  $C_2 \times C_{27}$ , and show that there is no valid image in  $C_4 \times C_{27}$ . At many steps, we multiply by some power of  $x$  or  $y$  to cancel some terms, and this gives us a translate of  $D$ . However, for convenience, we will rename it to  $D$ , since all translates of a difference set are also difference sets.

#### 4.1.1 The $C_{27}$ image of $G$

The homomorphism on  $G$  defined by  $x \mapsto 1, y \mapsto y, z \mapsto 1$  gives an image isomorphic to  $C_{27}$ . It also gives an image of  $D$ , which can be written as the sum of four rational idempotents:

$$\begin{aligned} & \frac{1}{27}\langle y \rangle, \quad \frac{1}{27}(3\langle y^3 \rangle - \langle y \rangle) \\ & \frac{1}{9}(3\langle y^9 \rangle - \langle y^3 \rangle), \quad \frac{1}{3}(3 - \langle y^9 \rangle) \end{aligned}$$

The alias of the first one is 255, and for the rest, it is  $15y^j$  because 5 is prime in  $\mathbb{Z}[\zeta_{27}]$  (5 factors into one prime ideal) and 3 is completely ramified. The  $y^j$  is there because we can multiply by any 27th root of unity and still have an alias. So we have

$$D = \frac{85}{9}\langle y \rangle \pm_1 \frac{5}{9}y^{j_1}(3\langle y^3 \rangle - \langle y \rangle) \pm_2 \frac{5}{3}y^{j_2}(3\langle y^9 \rangle - \langle y^3 \rangle) \pm_3 5y^{j_3}(3 - \langle y^9 \rangle) \quad (47)$$

where subscripts on  $\pm$  denote that they are independent of one another. It is not hard to see that the coefficients of  $\langle y \rangle, \langle y^3 \rangle$ , and  $\langle y^9 \rangle$  all need to be integral. Since the two  $\langle y \rangle$  terms need to add to become integral,  $\pm_1$  must be minus. We can multiply everything by  $y^{-j_1}$  and rename variables accordingly. That is,  $Dy^{-j_1}$  can be renamed to  $D$  without loss of generality, and similarly,  $j_2$  can be reassigned to  $j_2 - j_1$ , etc.

$$D = 10\langle y \rangle - \frac{5}{3}\langle y^3 \rangle \pm_2 \frac{5}{3}y^{j_2}(3\langle y^9 \rangle - \langle y^3 \rangle) \pm_3 5y^{j_3}(3 - \langle y^9 \rangle) \quad (48)$$

Similarly, the two coefficients of  $\langle y^3 \rangle$  need to add up to an integer, so  $\pm_2$  must be minus. We again multiply everything by  $y^{-j_2}$  and rename variables to get

$$D = 10\langle y \rangle - 5\langle y^9 \rangle \pm 5y^{j_3}(3 - \langle y^9 \rangle) \quad (49)$$

At this point, everything has integral coefficient, so this is a valid  $C_{27}$  image.

#### 4.1.2 The $C_2 \times C_{27}$ image of $G$

This time we consider the image of the homomorphism defined by  $x \mapsto x^8, y \mapsto y, z \mapsto 1$ . There are eight rational idempotents now, and they are given by multiplying each of the four from the  $C_{27}$  image by either  $(1+x)/2$  or  $(1-x)/2$ . However, the idempotents given by multiplying by  $(1+x)/2$  sum up to the  $C_{27}$  image of  $D$ , so half of the work is already done. In  $\mathbb{Z}[\zeta_{54}]$ , 5 is still prime and 3 is completely ramified, so the alias remains 15. We write

$$\begin{aligned} D &= \frac{1+x}{2} (10\langle y \rangle - 5\langle y^9 \rangle \pm_1 5y^{j_0}(3 - \langle y^9 \rangle)) + \\ &\quad \frac{1-x}{2} (\pm_2 \frac{5}{9}\langle y \rangle \pm_3 \frac{5}{9}y^{j_1}(3\langle y^3 \rangle - \langle y \rangle) \\ &\quad \pm_4 \frac{5}{3}y^{j_2}(3\langle y^9 \rangle - \langle y^3 \rangle) \pm_5 5y^{j_3}(3 - \langle y^9 \rangle)) \end{aligned}$$

The coefficient of  $\langle y \rangle$  is  $5 \pm_2 \frac{5}{18} \mp_3 \frac{5}{18}y^{j_1}$ . The first term is already integral, so the last two must add up to be integral also, which implies that  $\pm_2 = \pm_3$ . Multiply everything by  $y^{-j_1}$  and rename variables to get

$$\begin{aligned} D &= \frac{1+x}{2} (10\langle y \rangle - 5y^{-j_1}\langle y^9 \rangle \pm_1 5y^{j_0}(3 - \langle y^9 \rangle)) + \\ &\quad \frac{1-x}{2} \left( \pm_2 \frac{5}{3}\langle y^3 \rangle \pm_4 \frac{5}{3}y^{j_2}(3\langle y^9 \rangle - \langle y^3 \rangle) \pm_5 5y^{j_3}(3 - \langle y^9 \rangle) \right) \end{aligned}$$

Similarly, to make the coefficient of  $\langle y^3 \rangle$  integral, we need  $\pm_2 = \pm_4$ .

$$\begin{aligned} D &= \frac{1+x}{2} (10\langle y \rangle - 5y^{-j_1}\langle y^9 \rangle \pm_1 5y^{j_0}(3 - \langle y^9 \rangle)) \\ &\quad + \frac{1-x}{2} (\pm_2 5\langle y^9 \rangle \pm_5 5y^{j_3}(3 - \langle y^9 \rangle)) \end{aligned}$$

If we have  $j_0 \neq 0$ , then either  $j_3 = 0$  or  $j_1 = 0$  because those are the only two terms of the coefficient of  $\langle y^9 \rangle$  that can cancel the  $\pm_2 \frac{5}{2}$ . But if this happens, then we also need that either  $j_3 = j_0$  or  $j_1 = j_0$ , but then we will have two noninteger coefficients (namely  $\frac{15}{2}y^{j_0}$  and  $\frac{15}{2}y^{j_3}$  because  $j_0 \neq j_3$ ). So  $j_0 = 0$ .

$$\begin{aligned} D &= 5(1+x)\langle y \rangle - \frac{5}{2}(1+x)\langle y^9 \rangle \pm_2 \frac{5}{2}(1-x)\langle y^9 \rangle \\ &\quad \pm_1 \frac{5}{2}(1+x)y^{j_0}(3 - \langle y^9 \rangle) \pm_5 \frac{5}{2}(1-x)y^{j_3}(3 - \langle y^9 \rangle) \\ &= 5(1+x)\langle y \rangle - 5x^{k_0}\langle y^9 \rangle + \frac{5}{2}(3 - \langle y^9 \rangle)(\pm_1(1+x)y^{j_0} \pm_5(1-x)y^{j_3}) \end{aligned}$$

The second part of the last equation implies that  $j_0 = j_3$ . If not, then there is no way to get integral coefficient for  $\langle y^9 \rangle$ . If both  $\pm$  agree, then the last part is  $\pm 2y^{j_0}$ . If they don't agree, it's  $\pm 2xy^{j_0}$ . Thus, we get the following:

$$D = 5(1+x)\langle y \rangle - 5x^{k_0}\langle y^9 \rangle \pm 5x^{k_1}y^{j_0}(3 - \langle y^9 \rangle)$$

Finally, multiply by  $x^{-k_0}$  and we have the following translate of  $D$ :

$$D = 5(1+x)\langle y \rangle - 5\langle y^9 \rangle \pm 5x^{k_1}y^{j_0}(3 - \langle y^9 \rangle) \quad (50)$$

### 4.1.3 The $C_4 \times C_{27}$ image of $G$

Finally, consider the image of the homomorphism defined by  $x \mapsto x^4, y \mapsto y, z \mapsto 1$ . There are 12 rational idempotents, and they are given by multiplying each of the 4 rational idempotents from the  $C_{27}$  image by either  $(1 + x + x^2 + x^3)/4$ ,  $(1 - x + x^2 - x^3)/4$ , or  $(1 - x^2)/2$ . The sum of the eight rational idempotents using the expressions  $(1 + x + x^2 + x^3)/4$  and  $(1 - x + x^2 - x^3)/4$  is the  $C_2 \times C_{27}$  image of  $D$ , so we consider only 4 new rational idempotents. In  $\mathbb{Z}[\zeta_{108}]$ , we can write  $5 = (2 + i)(2 - i)$ , where  $i$  is a primitive fourth root of unity, but 3 is still completely ramified. So the aliases are 15,  $3(3 + 4x)$ , or  $3(3 - 4x)$  possibly multiplied by some roots of unity  $x^k y^j$ . The image of the difference set is

$$D = \frac{1+x^2}{2} (5(1+x)\langle y \rangle - 5\langle y^9 \rangle \pm_1 5x^{k_0} y^{j_0} (3 - \langle y^9 \rangle)) + \frac{1-x^2}{2} (\pm_2 \frac{g_1}{9} x^{k_1} \langle y \rangle \\ \pm_3 \frac{g_2}{9} x^{k_2} y^{j_1} (3\langle y^3 \rangle - \langle y \rangle) \pm_4 \frac{g_3}{3} x^{k_3} y^{j_2} (3\langle y^9 \rangle - \langle y^3 \rangle) \pm_5 g x^{k_4} y^{j_3} (3 - \langle y^9 \rangle))$$

where  $g_i \in \{5, 3 + 4x, 3 - 4x\}$ . The coefficient of  $x\langle y \rangle$  is  $\frac{5}{2}$  plus ‘‘something else.’’ This ‘‘something else’’ can only be formed by  $\pm_2 \frac{g_1}{18} x^{k_1} \mp_3 \frac{g_2}{18} x^{k_2} y^{j_1}$ . To make the coefficient integral, there are two ways. The first is to let the  $\pm$  agree, and set  $k_1 = 1, k_2 = 0$  and  $g_1 = 5, g_2 = 3 - 4x$ . Alternatively, we could let the  $\pm$  disagree and let  $g_2 = 3 + 4x$ , but this only results in swapping the coefficients of  $x\langle y \rangle$  and  $x^3\langle y \rangle$ . We need them both to be integral, so it's enough to consider one. Also note that letting  $k_1 = 3$  is equivalent in a similar manner. The second way is to let the  $\pm$  agree and let  $k_1 = 0, k_2 = 1$  and  $g_1 = 3 - 4x, g_2 = 5$ . Again, we could let the  $\pm$  disagree, but this is equivalent to swapping the coefficients as mentioned earlier.

Now examine the coefficient of  $\langle y \rangle$  in both cases. In the first case, it is  $\frac{5}{2} \mp_3 \frac{y^{j_1}}{6}$ , which is not integral. The second case gives a coefficient of  $\frac{5}{2} \pm_2 \frac{1}{6}$ , which is also not integral. Thus, there is no way to make both the coefficients of  $\langle y \rangle$  and  $x\langle y \rangle$  integral, so there is no valid image of  $D$  in the  $C_4 \times C_{27}$  image of  $G$ , so we conclude that  $D$  does not exist.

## 4.2 (465, 145, 45) cyclic difference sets

We next look at the open parameter set (465, 145, 45). This is the second smallest open case for a cyclic difference set. Given the multiplier conjecture, since 2 divides  $k - \lambda = 100 = 5^2 2^2$ , 2 would be a multiplier of this difference set. Using techniques from the earlier sections, one can show that this implies a difference set does not exist. However, we can disprove the existence of the difference set using algebraic number theory and rational idempotents, which gives a much stronger result.

Let  $C_{465} = \langle x, y, z \mid x^3 = y^5 = z^{31} = 1 \rangle$  be the cyclic group of order 465, and let  $D$  be a (465, 145, 45) difference set of  $C_{465}$ . The homomorphism defined by  $x \mapsto 1, y \mapsto y, z \mapsto z$  gives an image isomorphic to  $C_{155}$ . In the group ring

$\mathbb{Z}[C_{155}]$ ,  $D$  can be decomposed into four rational idempotents:

$$\begin{aligned} & \frac{1}{155} \langle y \rangle \langle z \rangle, \quad \frac{1}{155} \langle y \rangle (31 - \langle z \rangle), \\ & \frac{1}{155} (5 - \langle y \rangle) \langle z \rangle, \quad \frac{1}{155} (5 - \langle y \rangle) (31 - \langle z \rangle) \end{aligned}$$

So we write

$$\begin{aligned} D = & \frac{g_0}{155} \langle y \rangle \langle z \rangle \pm_1 \frac{g_1}{155} \langle y \rangle (31 - \langle z \rangle) \pm_2 \\ & \frac{g_2}{155} (5 - \langle y \rangle) \langle z \rangle \pm_3 \frac{g_3}{155} (5 - \langle y \rangle) (31 - \langle z \rangle) \end{aligned}$$

where each  $g_i$  is a  $\chi$ -alias for the rational idempotents. Since  $g_0$  corresponds to the trivial rational idempotent,  $g_0 = 145$ . The rest of the  $g_i$  must satisfy  $g_i \bar{g}_i = 100$ ,  $g_i \in \mathbb{Z}[\zeta_{155}]$ , and  $(g_i)(\bar{g}_i) = (100)$ . The primes dividing 100 are 5 and 2, so we consider how (5) and (2) factor in  $\mathbb{Z}[\zeta_{155}]$ . Since  $\mathbb{Z}[\zeta_{155}]$  contains fifth roots of unity, 5 is completely ramified, so (5) factors in a trivial way.

The number of prime ideals that (2) factors into is given by  $\frac{\varphi(155)}{|2|_{155}}$ . We have that  $\varphi(155) = \varphi(31)\varphi(5) = 120$ , and  $2^{20} \equiv 1 \pmod{155}$ , while  $2^{10} \equiv 94 \pmod{155}$ , so  $|2|_{155} = 20$ . Thus, (2) factors into 6 prime ideals. So we can write

$$(2) = \pi_1 \pi_2 \pi_3 \overline{\pi_1 \pi_2 \pi_3}$$

where  $\pi_i$  is a prime ideal. However, in  $\mathbb{Z}[\zeta_{31}]$  we also have that (2) factors into  $\frac{\varphi(31)}{|2|_{31}} = \frac{30}{5} = 6$  prime ideals. Factorization into prime ideals in a ring of integers is unique, so it is enough to factor (2) in  $\mathbb{Z}[\zeta_{31}]$ .

An equivalence relation is defined for two ideals  $p_1$  and  $p_2$  if there exist nonzero  $\alpha, \beta$  such that  $(\alpha)p_1 = (\beta)p_2$ . It can be shown that the equivalence classes form a finite group called the **class group**. The class group of  $\mathbb{Z}[\zeta_{31}]$  is  $C_9$ , so there are 9 equivalence classes of ideals in this group ring. Let  $k_p$  denote the equivalence class of an ideal  $p$ . Then if for some ideal  $\rho$ ,  $k_\rho = 0$ ,  $\rho$  is a principal ideal. If  $k_\rho = 1$  for some ideal  $\rho$ , the equivalence class of  $\rho$  can be thought of as a generator in the class group and  $\rho^2$  has  $k_{\rho^2} = 2$ . A more thorough study of the class group can be found in [7] and [4]. PARI gives the values of  $k$  for each prime ideal  $\pi_j$  in the prime decomposition of (2) [6]:

$$\begin{array}{c|c|c|c|c|c} \pi_1 & \pi_2 & \pi_3 & \overline{\pi_1} & \overline{\pi_2} & \overline{\pi_3} \\ \hline 2 & 4 & 1 & 7 & 5 & 8 \end{array}$$

Since  $(2)(2) = (4)$ , we can write  $(4) = p\bar{p}$  where  $p$  is a product of 6 of the prime ideals in  $(2)(2)$  and  $\bar{p}$  is the conjugate of  $p$ . Since  $p$  must be principal, and an ideal is principal only when it belongs to the equivalence class with class number 0, we conclude that the only value for  $p$  is (2), so that (2) also factors trivially.

So far, the only alias we have is  $10y^i z^j$ . However, one more possibility shows up. That is, we can factor 5 into  $XY$  where  $X \in \mathbb{Z}[\zeta_{31}]$ , and  $Y$  is a Gauss sum (see [4]). We must have that  $Y = y - y^2 - y^3 + y^4$ , and  $X$  has the property

that  $X\bar{X} = 5$ . In  $\mathbb{Z}[\zeta_{31}]$ , (5) factors into  $\frac{\varphi(31)}{|5|_{31}} = \frac{30}{3} = 10$  prime ideals. The command `idealprimedec(bnfinit(polcyclo(31)),5)` in PARI gives

$$(5) = \rho_1 \overline{\rho_2 \rho_3 \rho_4 \rho_3} \overline{\rho_1 \rho_5 \rho_4 \rho_2 \rho_5}$$

where each  $\rho_i$  has class number 3, while  $\overline{\rho_i}$  has class number 6. To get  $X$ , we need to take a product of 5 of these prime ideals such that we do not choose a prime ideal and its conjugate, and the resulting product is principal. This leaves only the choice of picking four ideals with class number 3 and one of class number 6, or picking four ideals with class number 6 and one of class number 3 (the second choice can be considered picking  $\bar{X}$ ). We want the generators of these products, and they are:

$$\begin{aligned} z + z^{13} + z^{17} + z^{24} + z^{26} + z^{27}, & \quad z^4 + z^5 + z^7 + z^{14} + z^{18} + z^{30}, \\ z + z^3 + z^8 + z^{22} + z^{23} + z^{26}, & \quad z^5 + z^8 + z^9 + z^{23} + z^{28} + z^{30}, \\ z^3 + z^7 + z^{13} + z^{26} + z^{27} + z^{29}, & \quad z^2 + z^4 + z^5 + z^{18} + z^{24} + z^{28}, \\ z + z^3 + z^6 + z^{13} + z^{14} + z^{28}, & \quad z^3 + z^{17} + z^{18} + z^{25} + z^{28} + z^{30}, \\ z + z^4 + z^5 + z^{15} + z^{23} + z^{30}, & \quad z + z^8 + z^{16} + z^{26} + z^{27} + z^{30} \end{aligned}$$

where  $z$  can be thought of as a primitive 31st root of unity. They are all given by (31, 6, 1) difference sets, but we also need to consider those given by the complementary (31, 25, 20) difference sets. We will define the **length** of an alias to be its value when the trivial character is applied. Thus, the  $XY$  we have found have length 24, and their complements have length 100.

Now we return to the decomposition of  $D$  in the  $C_{155}$  image. Since 2 does not factor, we write

$$\begin{aligned} D = \frac{145}{155} \langle y \rangle \langle z \rangle \pm_1 \frac{2}{155} g_1 z^{j_1} \langle y \rangle (31 - \langle z \rangle) \pm_2 \frac{2}{155} g_2 y^{j_2} (5 - \langle y \rangle) \langle z \rangle \\ \pm_3 \frac{2}{155} g_3 y^{j_3} z^{j_4} (5 - \langle y \rangle) (31 - \langle z \rangle) \end{aligned}$$

Without loss of generality, we can multiply both sides by  $z^{-j_1} y^{-j_2}$  and rename  $D$ ,  $j_3$ ,  $j_4$  to get

$$\begin{aligned} D = \frac{145}{155} \langle y \rangle \langle z \rangle \pm_1 \frac{2}{155} g_1 \langle y \rangle (31 - \langle z \rangle) \pm_2 \frac{2}{155} g_2 (5 - \langle y \rangle) \langle z \rangle \\ \pm_3 \frac{2}{155} g_3 y^{j_3} z^{j_4} (5 - \langle y \rangle) (31 - \langle z \rangle) \end{aligned}$$

The coefficient of  $\langle z \rangle$  is  $\pm_2 \frac{2}{31} g_2 \mp_3 \frac{2}{31} g_3 y^{j_3}$ . This coefficient must be integral, so either  $\pm_2 = \pm_3$  and the length of  $g_2$  and  $g_3$  are the same (so that the coefficients add to zero), or  $\pm_2 = \mp_3$  and the length of one is 24, while the other is 100.

In the first case, the coefficient of  $\langle y \rangle \langle z \rangle$  is  $\frac{145}{155} \mp_1 \frac{2g_1}{155} \mp_2 \frac{2g_2}{155} \pm_2 \frac{2g_3}{155}$ . The last two terms add to zero. The equation becomes

$$D = \frac{145}{155} \langle y \rangle \langle z \rangle \pm_1 \frac{2}{155} g_1 \langle y \rangle (31 - \langle z \rangle) \pm_3 \frac{2}{5} g_3 y^{j_3} z^{j_4} (5 - \langle y \rangle) \quad (51)$$

To make the coefficient of  $\langle y \rangle \langle z \rangle$  integral, we need  $g_1 = 5$  and  $\pm_1$  must be minus.

$$D = \langle y \rangle \langle z \rangle - 2\langle y \rangle \pm_3 2g_3 y^{j_3} z^{j_4} \mp_3 \frac{2}{5} g_3 z^{j_4} \langle y \rangle \quad (52)$$

If  $g_3 = 5$ , then the equation becomes

$$D = \langle y \rangle \langle z \rangle - 2\langle y \rangle \pm_3 10y^{j_3} z^{j_4} \mp_3 2z^{j_4} \langle y \rangle \quad (53)$$

This appears to be a valid  $C_{155}$  image since all of the coefficients are integral now. However, the smallest we can make the coefficient of  $y^{j_3} z^{j_4}$  is  $10 + 1 - 2 - 2 = 7$ . But the cosets can be of size at most 3. So this is not valid. If  $g_3 = XY$ , then noting that  $Y = y - y^2 - y^3 + y^4$  causes the last term to become zero, we have

$$D = \langle y \rangle \langle z \rangle - 2\langle y \rangle \pm_3 2(y - y^2 - y^3 + y^4) X y^{j_3} z^{j_4} \quad (54)$$

Now note that of the elements  $1, y, y^2, y^3, y^4$ , some of them will be negative, and this is not valid either.

So now we consider the second case when  $\pm_2 = \mp_3$  and one of  $g_2$  and  $g_3$  is of length 24, while the other is of length 100. Since  $Y = y - y^2 - y^3 + y^4$ , the last two terms of  $\langle y \rangle \langle z \rangle$  will be 0.

$$D = \frac{145}{155} \langle y \rangle \langle z \rangle \pm_1 \frac{2}{155} g_1 \langle y \rangle (31 - \langle z \rangle) \pm_2 \frac{2}{31} g_2 \langle z \rangle \\ \mp_2 2g_3 y^{j_3} z^{j_4} \pm_2 \frac{2}{5} g_3 z^{j_4} \langle y \rangle \pm_2 \frac{2}{31} g_3 y^{j_3} \langle z \rangle$$

Again, we need  $g_1 = 5$  and  $\pm_1$  is minus to get the coefficient of  $\langle y \rangle \langle z \rangle$  to be integral.

$$D = \langle y \rangle \langle z \rangle - 2g_1 \langle y \rangle \pm_2 \frac{2}{31} g_2 \langle z \rangle \mp_2 2g_3 y^{j_3} z^{j_4} \pm_2 \frac{2}{5} g_3 z^{j_4} \langle y \rangle \pm_2 \frac{2}{31} g_3 y^{j_3} \langle z \rangle$$

We wind up in the same situation as in case 1, except for a few extra terms. However, these extra terms cannot make all of the coefficients of  $1, y, y^2, y^3, y^4$  positive, so since there is no valid  $C_{155}$  image for  $D$ , we conclude  $D$  does not exist.

### 4.3 (1785, 224, 28) cyclic difference sets

We next look at (1785, 224, 28). Above, we showed that assuming the multiplier conjecture, 2 would be a multiplier of the difference set and that no difference set could exist. Looking for stronger results, we examine the parameter set using algebraic number theory. However, we were unable to obtain definite results using these methods as PARI [6] could not construct  $\mathbb{Z}[\zeta_{119}]$  on our machines. Following is a compilation of information we were able to obtain as well as the difficulties we met.

Let  $C_{1785} = \langle w, x, y, z \mid w^3 = x^5 = y^7 = z^{17} = 1 \rangle$ . We first consider the image of the difference set under the homomorphism defined by  $w \mapsto w, x \mapsto 1,$

$y \mapsto 1, z \mapsto 1$ . Since  $k - \lambda = 196 = 7^2 2^2$ ,  $g_2 = \frac{\varphi(3)}{|2|_3} = 1$ , and  $g_7 = \frac{\varphi(3)}{|7|_3} = 2$ , we see that 2 is prime and 7 factors into two primes in  $\mathbb{Z}[\zeta_3]$ . Further inspection gives us  $7 = \pi_1 \bar{\pi}_1 = (2 - \zeta_3)(3 + \zeta_3)$ . The possible  $\chi$ -aliases,  $g_1$  are then  $\pm 14w^{i_1}$ ,  $\pm 2(2 - \zeta_3)^2 w^{i_1}$ , and  $\pm 2(3 + \zeta_3)^2 w^{i_1}$ . So, letting  $D_{1,5,7,17}$  denote the image of  $D$  under the previously defined homomorphism, we have:

$$D_{1,5,7,17} = \frac{224}{3} \langle w \rangle \pm \frac{g_1}{3} (3 - \langle w \rangle)$$

In order to obtain integral solutions, we must add the second term, and we obtain the following result:

$$D_{1,5,7,17} = \frac{224}{3} \langle w \rangle + \frac{g_1}{3} (3 - \langle w \rangle) \quad (55)$$

Under the  $C_5$  image of the difference set given by the homomorphism  $w \mapsto 1, x \mapsto x, y \mapsto 1, z \mapsto 1$ , we have  $g_2 = \frac{\varphi(5)}{|2|_5} = 1$  and  $g_7 = \frac{\varphi(5)}{|2|_5} = 1$ . Thus, the only possible  $\chi$ -alias is  $g_2 = \pm 14x^j$ .

$$D_{3,1,7,17} = \frac{224}{5} \langle x \rangle \pm \frac{14x^j}{5} (5 \langle x \rangle)$$

Again, in order to obtain integral results, we add the second term.

$$D_{3,1,7,17} = \frac{224}{5} \langle x \rangle + \frac{14x^j}{5} (5 \langle x \rangle) \quad (56)$$

Under the  $C_7$  image of the difference set given by the homomorphism  $w \mapsto 1, x \mapsto 1, y \mapsto y, z \mapsto 1$ , we have  $g_2 = \frac{\varphi(7)}{|2|_7} = 2$  and 7 will completely ramify. By looking at the  $(15, 7, 3)$  cyclic difference set, we are given a factoring of 2 in  $\mathbb{Z}[\zeta_7]$ ,  $2 = (\zeta_7 + \zeta_7^2 + \zeta_7^4)(\zeta_7^3 + \zeta_7^6 + \zeta_7^5)$ . Thus, the possible aliases under this image,  $g_3$  are  $\pm 14y^{k_1}$ ,  $\pm 7(\zeta_7 + \zeta_7^2 + \zeta_7^4)^2 y^{k_1}$ , and  $\pm 7(\zeta_7^3 + \zeta_7^6 + \zeta_7^5)^2 y^{k_1}$ . So we write:

$$D_{3,5,1,17} = \frac{224}{7} \langle z \rangle \pm \frac{g_3}{7} (7 - \langle y \rangle) \quad (57)$$

Under the  $C_{17}$  image given by the homomorphism defined by  $w \mapsto 1, x \mapsto 1, y \mapsto 1, z \mapsto z$ , we have  $g_7 = \frac{\varphi(17)}{|7|_{17}} = 1$  and  $g_2 = \frac{\varphi(17)}{|2|_{17}} = 2$ . Thus, 7 is prime and 2 will factor into two primes,  $(2) = \pi_1 \pi_2$  in  $\mathbb{Z}[\zeta_{17}]$ . Notice the Galois automorphism  $\sigma_2 : \zeta_{17} \mapsto \zeta_{17}^2$  will fix each ideal above since 2 is prime. Since  $\sigma_2^4 = -1$ , we have  $\sigma_2^4(\zeta_{17}) = -\zeta_{17} = \bar{\zeta}_{17}$  so  $\sigma_2^4(\pi_1) = \bar{\pi}_1$  and  $\sigma_2^4(\pi_2) = \bar{\pi}_2$ . Thus, these prime ideals are fixed by conjugation. That is,  $\pi_1 = \bar{\pi}_1$  and  $\pi_2 = \bar{\pi}_2$ . Since we are looking for factorings of  $n$  for  $\delta$  in the equation  $\delta \bar{\delta} = n$ , we must choose  $\pi_1 \pi_2 \in \delta$ . So our possible  $\chi$ -alias is  $g_4 = \pm 14z^{m_1}$ . We are given the following image of the difference set:

$$D_{3,5,7,1} = \frac{224}{17} \langle z \rangle \pm \frac{14z^{m_1}}{17} (17 - \langle z \rangle) \quad (58)$$

Again, we may simplify in order to obtain integral results.

$$D_{3,5,7,1} = \frac{224}{17} \langle z \rangle - \frac{14z^{m_1}}{17} (17 - \langle z \rangle) \quad (59)$$

From here, given the restrictions on the  $C_7$  and  $C_{17}$  images, it would be interesting to look at a  $C_7 \times C_{17}$  image which would be given by the homomorphism  $w \mapsto 1, x \mapsto 1, y \mapsto y, z \mapsto z$ . Under this image, 7 will completely ramify and  $g_2 = \frac{\varphi(119)}{|2|_{119}} = 4$ . Thus,  $2 = \pi_1 \pi_2 \bar{\pi}_1 \bar{\pi}_2$  in  $\mathbb{Z}[\zeta_{119}]$ . Using GAP [2], we find these results for  $\pi_i$  where we let  $\zeta = \zeta_{119}$  and  $\pi_i$  the prime ideal generated by 2 and the polynomial listed:

$$\begin{aligned} \pi_1 &= (2, \zeta^{24} + \zeta^{20} + \zeta^{18} + \zeta^{17} + \zeta^{12} + \zeta^{11} + \zeta^9 + \zeta^7 + \zeta^5 + \zeta^3 + 1) \\ \bar{\pi}_1 &= (2, \zeta^{24} + \zeta^{21} + \zeta^{19} + \zeta^{17} + \zeta^{15} + \zeta^{13} + \zeta^{12} + \zeta^7 + \zeta^6 + \zeta^4 + 1) \\ \pi_2 &= (2, \zeta^{24} + \zeta^{22} + \zeta^{20} + \zeta^{14} + \zeta^{12} + \zeta^{11} + \zeta^9 + \zeta^8 + \zeta^7 + \zeta^5 + \zeta^2 + \zeta + 1) \\ \bar{\pi}_2 &= (2, \zeta^{24} + \zeta^{23} + \zeta^{22} + \zeta^{19} + \zeta^{17} + \zeta^{16} + \zeta^{15} + \zeta^{13} + \zeta^{12} + \zeta^{10} + \zeta^4 + \zeta^2 + 1) \end{aligned}$$

These prime ideals are especially hard to work with, especially given that  $\mathbb{Z}[\zeta_{119}]$  is not a unique factorization domain. Furthermore, PARI [6] is unable to initialize the number field without taking more virtual memory than we can give it. However, we speculate that there will be no difference set in the  $C_{119}$  image. If we use the trivial  $\chi$ -alias,  $g_5 = \pm 14y^{k_2} z^{m_2}$ , we are given the following, which does not appear to be a valid difference set image.

$$\begin{aligned} D_{3,5,1,1} &= \frac{224}{7 \cdot 17} \langle y \rangle \langle z \rangle \pm_1 \frac{g_3}{7 \cdot 17} (7 - \langle y \rangle) \langle z \rangle \\ &\quad - \frac{14z^{m_1}}{7 \cdot 17} \langle y \rangle (17 - \langle z \rangle) \pm_2 \frac{14y^{k_2} z^{m_2}}{7 \cdot 17} (7 - \langle y \rangle) (17 - \langle z \rangle) \end{aligned}$$

## 5 Conclusion

Through our research using rational idempotents, algebraic number theory, and powerful computer programs such as PARI [6] and GAP [2], we were able to rule out existence of cyclic difference sets with parameters (465, 145, 45), (645, 161, 40), (817, 289, 102), (1380, 197, 28), (2160, 255, 30), and (2574, 249, 24), but we leave a number of interesting cases still unsolved. The parameter (1785, 224, 28) would be especially interesting and could potentially be ruled out using the above techniques. One more difficult example would be the smallest remaining open case listed on the CCR La Jolla website [3]: (419, 133, 42). Since  $v$  is prime, other techniques would be necessary to resolve the existence of a cyclic difference set with these parameters.

## Acknowledgements

This research was done at Central Michigan University in Summer 2006 as part of the Research Experience for Undergraduates program and was supported by

the NSF-REU grant 05-52594. We also thank our advisor Ken Smith for his encouragement and support.

## References

- [1] James A. Davis and Ken W. Smith, Rational Idempotents and the Integral Group Ring, preprint, 2006.
- [2] The GAP Group, Gap – Groups, Algorithms, and Programming, Version 4.4, 2006. (<http://www.gap-system.org>)
- [3] Dan Gordon, La Jolla Cyclic Difference Set Repository, 2006. <http://www.ccrwest.org/diffsets.html>
- [4] Kenneth Ireland and Michael Rosen, A Classical Introduction to Modern Number Theory, New York, Heidelberg, Berlin: Springer-Verlag New York Inc, 1982.
- [5] Dieter Jungnickel, Alexander Pott, and Ken W. Smith, Chapter 18: Difference Sets, CRC Handbook of Combinatorial Designs, second edition, 2006: p. 437.
- [6] PARI/GP, version 2.1.7, Bordeaux, 2005, <http://pari.math.u-bordeaux.fr>
- [7] Ian Stewart and David Tall, Algebraic Number Theory and Fermat's Last Theorem, third edition, Natick, Massachusetts: A K Peters, Ltd, 2002.
- [8] J. H. van Lint and R. M. Wilson, A Course in Combinatorics, Cambridge, England: Cambridge University Press, 1992: p. 349.