Investigations into a possible new family of Partial Difference Sets

Peter A. Magliaro
University of Richmond
Richmond, VA 23173
email: pmagliar@richmond.edu

Adam D. Weaver
University of Richmond
Richmond, VA 23173
email: aweaver@richmond.edu

Abstract

We investigated partial difference set constructions for the parameter family $(2^{3e}, 2^{2e}+2^e+1, 2^e+4, 2^e+2)$. After working through the simple construction examples, the Fiedler-Klin construction, and the DeLange construction, we attempted to extend these methods to create new partial difference sets. Along with these constructions, we tried some original ideas involving vector spaces and embedding partial difference sets into larger groups.

1 Introduction

The most important question in the area of partial difference sets (PDS) is the following: given a parameter family that survives known nonexistence results, can we find a group that supports a PDS with these same parameters. The second most important question is related: given a parameter family with known PS constructions, can we find other groups supporting a PDS with the same parameters. We examined both of these questions for the parameter family $(2^{3e}, 2^{2e} + 2^e + 1, 2^e + 4, 2^e + 2)$. Trivial examples exist in the $e = 1$ and $e = 2$ cases. The $e = 3$ case presented by Fiedler and Klin involves constructing permutation groups and using them to build a partial difference set. The $e = 4$ case presented by DeLange uses cyclotomic classes in finite fields. Initially, we inspected ways to expand the known partial difference sets to larger values of e. Then, we spent a majority of our time trying to build structural relationships between the different examples in the hopes of finding a pattern that could be used to build larger partial difference sets. In most cases, we were working with finding these partial difference sets in the elementary abelian groups of appropriate order. In order to better understand our work, we provided a preliminary section explaining difference sets, partial difference sets, strongly regular graphs, character theory, finite fields, Galois rings, wreath products, and a list of families of partial difference sets. The third section outlines the known constructions for the parameter family of interest. The fourth section describes out attempts to understand these examples and possibly extend their constructions to build new examples for values of $e > 4$.

2 Preliminaries

A *difference set* D is a subset of a group G with the property that every nonidentity element of G can be represented exactly λ times as a difference between the elements of D. Difference sets are described by three parameters (v, k, λ) where $v = |G|$, $k = |D|$, and λ is as described above.

- **Example:** $\mathbf{(7, 3, 1)}$
  Let $G = \mathbb{Z}_7$ and consider the subset $D = \{1, 2, 4\}$. We claim this is a difference set. To show this, we will explicitly show all non-zero differences.
  $1 - 2 = 6 \quad 2 - 1 = 1 \quad 4 - 1 = 3$
  $1 - 4 = 4 \quad 2 - 4 = 5 \quad 4 - 2 = 2$
  As you can see, each non-zero element of $\mathbb{Z}_7$ appears exactly once, making this a $(7, 3, 1)$ difference set.

To construct this difference set, we simply take all the quadratic residues of each element in $\mathbb{Z}_7$. This is example is associated to two families of difference sets. One is the Singer Family of Difference Sets, $(\frac{q^{d+1}-1}{q-1}, \frac{q^d-1}{q-1}, \frac{q^{d-1}-1}{q-1})$ where q is prime power and $d \geq 2$, with parameters $q = 2$ and $d = 2$. The other is the Paley Family of Difference Sets, $(q, \frac{q-1}{2}, \frac{q-3}{4})$ where $q \equiv 3(mod 4)$ and q is a prime power, with $q = 7$.

- **Examples:** $\mathbf{(16, 6, 2)}$
  $G = \mathbb{Z}_4^2 \quad D_1 = \{(0,0), (0,2), (1,0), (3,0), (0,1), (2,3)\}$
  $G = \mathbb{Z}_4 \times \mathbb{Z}_2^2 \quad D_2 = \{(0,0,0), (0,0,1), (1,0,0), (0,1,0), (2,0,0), (3,1,1)\}$
  $G = \mathbb{Z}_2^4 \quad D_3 = \{(0,0,0,0), (0,0,0,1), (0,1,0,0), (0,1,1,0), (1,0,0,0), (1,0,1,1)\}$

Here we have given three difference examples of difference sets in non-isomorphic groups of order 16. These are examples of the McFarland parameter family, $(q^{d+1}(1+\frac{q^{d+1}-1}{q-1}), q^d(\frac{q^{d+1}-1}{q-1}), q^d(\frac{q^d-1}{q-1}))$. These difference sets follow the construction in a group $E \times K$ where $E = \mathrm{EA}(q^{d+1})$ and K is any group of order $1 + \frac{q^{d+1}-1}{q-1}$. In the first example, D_1, $q = 4$ and $d = 0$ making $E = Z_4$ and $|K| = 4$. The third example, D_3, has $q = 2$ and $d = 1$ making $E = \mathbb{Z}_2 \times \mathbb{Z}_2$ and $|K| = 4$. Finally, the second example is somewhat special because it can be viewed as having parameters $q = 4, d = 0$ making $E = Z_4$ and $K = \mathbb{Z}_2 \times \mathbb{Z}_2$ or $q = 2, d = 1$ making $E = \mathbb{Z}_2 \times \mathbb{Z}_2$ and $K = Z_4$ related to it.

There are two useful observations of difference sets
(a) translates of difference sets are difference sets.
(b) complements of difference sets are difference sets.

Proof: (a) Let D be a difference set in group G. Written additively, consider $D' = x + D$ where $x \in G$. Let $d_i, d_j \in D, x + d_i, x + d_j \in D', \forall d_i, d_j, i \neq j$. Since $d_i + x - (d_j + x) = d_i - d_j = g \in G$, this implies D' will have the same number of differences between the elements of D, making D' a partial difference set with the same parameters as D. □

Proof: (b) Let D be a (v, k, λ) difference set in a group G. There are v ways to represent any $g \in G$ as $g = x - y$, $x, y \in G$. Of these, k have $x \in D$, k have $y \in D$, and λ have both x and y in D. This leaves exactly $v - 2k + \lambda$ differences which involve no elements of D. Thus the complement of D is a $(v, v-k, v-2k+\lambda)$ difference set. □

Lemma 2.1 *The parameters of a (v, k, λ) difference set satisfy $k(k-1) = (v-1)\lambda$.*

Proof: Let D be a (v, k, λ) difference set. There are $k(k-1)$ differences that are not equal to the identity. Also, there are $v - 1$ non-identity elements, each of which is the result of λ differences. □

Difference sets can be used to construct symmetric designs. A *symmetric (v, k, λ) design* is a collection of v points and v blocks; each block containing k points and each point is on k blocks, and each pair of points are on exactly λ blocks, while each pair of blocks intersect in λ points.

To get a design from a (v, k, λ) difference set D in a group G, take all the translates of D as the blocks, and the elements of G as the points. It is easy to see that there are v points and v blocks because $|G| = v$ and there are v translations possible of D. Since $|D| = k$, each block contains k points. A point p is on a block $x + D$ if and only if there is a $d \in D$ such that $x + d = p$, or $x = p - d$. There are k

values for d so each point is on k blocks. It remains to show that each pair of points has λ common blocks, and each pair of blocks shares λ points. Two points p_1 and p_2 are in the same block $x + D$ if there exists $d_1, d_2 \in D$ such that $p_1 = x + d_1$ and $p_2 = x + d_2$. Combining these expressions, we get $p_1 - p_2 = d_1 - d_2$ which has λ solutions, so p_1 and p_2 are in λ blocks. Two blocks $x + D$ and $y + D$ have a point in common if there are d_1 and d_2 such that $x + d_1 = y + d_2$. This can be written $x - y = d_1 - d_2$ which has λ solutions, so $x + D$ and $y + D$ have λ common points. We can then conclude that this construction gives us a (v, k, λ) design.

Difference sets can also be associated with binary sequences. For example, we can take a (v, k, λ) difference set in Z_v, and place a -1 in every position that contains an element of the difference set and a $+1$ everywhere else.
Now we will consider the periodic autocorrelation of this sequence. For any sequence $a_0a_1 \dots a_{n-1}$, the periodic autocorrelation A_u is defined as

$$A_u = \sum_{i=0}^{n-1} a_i \cdot a_{i+u(modn)}.$$

It is easy to see that for a binary sequence of length n with elements ± 1, $A_0 = \sum_{i=0}^{n-1} a_i a_i = \sum_0^{n-1} 1 = n$.

- **Example:** $D = \{1, 2, 4\} \subset \mathbb{Z}_7$

The sequence associated with D is $+1-1-1+1-1+1+1$. For simplicity, we will represent this $+--+-++$. We will now take one of the periodic autocorrelations.

$$\begin{array}{llllllll} A_1 & = a_0a_1 & +a_1a_2 & +a_2a_3 & +a_3a_4 & +a_4a_5 & +a_5a_6 & +a_6a_0 \\ & = (+-) & +(--) & +(-+) & +(+-) & +(-+) & +(++) & +(++) \\ & = -1 & +1 & -1 & -1 & -1 & +1 & +1 = \text{-1} \end{array}$$

In fact, for sequences associated with a difference set, all periodic autocorrelations except A_0 will have the same value. Each cyclically shifted sequence is the sequence associated a translate of the difference set. We know that any two translates of a difference set have λ elements in common. This means there will be λ copies of $(--) = +1$ in the sum. The complement is also a difference set, so there will be some λ' copies of $(++) = +1$ in the sum. The rest of the sum will be made of -1.

This can be extended to groups other than $\mathbb{Z}_v$. We can associate a difference set in a group $Z_n \times \mathbb{Z}_n$ to a 2-dimensional array $a_{i,j}$ of ± 1, again with -1 in the positions corresponding to the elements of the difference set. We can define the periodic autocorrelation $A_{(u_1,u_2)} = a_{i,j}a_{i+u_1(mod4),j+u_2(mod4)}$.

- **Example:** $(16, 6, 2)$ difference set in $\mathbb{Z}_4 \times \mathbb{Z}_4$ D={(0,0),(0,2),(1,0),(3,0),(0,1),(2,3)}

$$a_{i,j} = \begin{array}{l} - - - + \\ - + + + \\ + + + - \\ - + + + \end{array} \qquad a_{i+2(mod4),j+1(mod4)} = \begin{array}{l} + + - + \\ + + + - \\ - - + - \\ + + + - \end{array}$$

It can be quickly verified that there are $\lambda = 2$ positions where both these arrays contain a -1. There are six more positions where both contain a $+1$ for a total of eight positions where they are the same. This means $A_{(2,1)} = +8 - 8 = 0$. As before, $A_{(u_1,u_2)}$ will be the same for all $(u_1, u_2) \neq (0, 0)$.

This type of array is actually used in electronics manufacturing for precision placement. A moving piece has a sheet with holes in places corresponding to our -1. The surface over which the piece is moving is painted black with white dots also corresponding to the -1, so if the piece is positioned correctly all the dots will line up with the holes. A detector on the moving piece determines how much white it can see. If it is not in the correct place, the autocorrelation will be 0 and it will see two white dots. If it is in the right place, it will detect six white dots. This is a significant jump, so it is easy to determine whether it is in the right place.

A *partial difference set* D is a subset of a group G with the property that every nonidentity element of D can be represented λ times as a difference between a pair of elements in D while every nonidentity element of $G \setminus D$ can be represented μ times as a difference between a pair of elements in D. Likewise, partial difference sets have parameters associated with them, (v, k, λ, μ), where $v = |G|$, $k = |D|$, and λ and μ are as described above.

- **Example:** $(\mathbf{5}, \mathbf{2}, \mathbf{0}, \mathbf{1})$
  Let $G = \mathbb{Z}_5$ and take the subset $D = \{1, 4\}$. Doing all non-zero subtractions explicitly,
  $1 - 4 = 2 \qquad 4 - 1 = 3$
  we see that each member of D does not appear and each nonzero member of the complement of D appears exactly once. This makes the set a $5, 2, 0, 1)$ partial difference set.

The construction of this set is similar to one of our difference set examples. The partial difference set D contains all the quadratic residues of $\mathbb{Z}_5$. Similarly, it is associated with a parameter family of partial difference sets.

Lemma 2.2 *The parameters describing (v, k, λ, μ) partial difference set satisfy*
(a) $k(k-1) = (k-1)\lambda + (v-k)\mu$ if the identity element of G is in D and
(b) $k(k-1) = k\lambda + (v-k-1)\mu$ if the identity element of G is in $G \setminus D$.

<u>Proof:</u> Let D be a (v, k, λ, μ) partial difference set in G. There are $k(k-1)$ differences that do not equal the identity of G. If the identity of G is in D, then there are $k-1$ non-identity elements in D that occur as differences λ times and $v-k$ elements in $G \setminus D$ that occur as differences μ times. If the identity of G in in $G \setminus D$, then there are k elements in D that occur as differences λ times and $v-k-1$ non-identity elements in $G \setminus D$ that occur as differences μ times. □

Partial difference sets can be used to construct strongly regular graphs. A connected graph with v vertices is strongly regular if
(a) each vertex has exactly k edges going into it; and
(b) given v_1, v_2, the number of vertices adjacent to both v_1 and v_2 is λ if v_1 is adjacent to v_2 and μ if v_1 is not adjacent to v_2.

Suppose D is a (v, k, λ, μ) partial difference set in G; let the elements of G be vertices of a graph, and join two vertices v_1, v_2 with an edge if $v_1 - v_2 \in D$. For all vertices v, they will have k edges going into them because each will be connected to $v_1 + d$ for all $d \in D$. If we consider two vertices v_1, v_2 connected to a vertex x, then $x - v_1 \in D$ and $x - v_2 \in D$. By taking $(x - v_1) - (x - v_2) = v_1 - v_2$, this shows that there must be λ values for x if $v_1 - v_2 \in D$ and μ values for x if $v_1 - v_2 \in G \setminus D$.

- **Strongly Regular Graph example:**()

There are a few ways to verify whether a set is a difference set or a partial difference set. Brute force methods are inefficient in both time and storage space when implemented in a computer program. Consequently, we need a faster way to determine this. Character Theory provides one way of making the process more efficient.

Definition 2.3 *A* ***character*** χ *is a homomorphism from a group* G *into* $(\mathbb{C}, \times)$*, the complex numbers under multiplication.*
The character $\chi_0 : G \to \mathbb{C}$ *such that* $\chi_0(g) = 1\ \forall g \in G$ *is called the* ***principal character****.*

Lemma 2.4 *If* χ *is a non-principal character on a group* G *then* $\chi(G) = \sum_{g \in G} \chi(g) = 0$*.*

<u>**Proof:**</u> If χ is non-principal on G then $\exists g' \in G$ such that $\chi(g') \neq 1$. We now compute $\chi(g' + G)$ in two ways assuming G is an additive group.

$$\begin{aligned} \chi(g' + G) &= \sum_{g \in G} \chi(g' + g) = \sum_{g \in G} \chi(g')\chi(g) = \chi(g') \sum_{g \in G} \chi(g) = \chi(g')\chi(G) \\ \chi(g' + G) &= \sum_{g'' \in G} \chi(g'') = \chi(G) \end{aligned}$$

This shows that $\chi(g')\chi(G) = \chi(G)$ and since $\chi(g') \neq 1$,$\chi(G) = 0$. □

Definition 2.5 *For a group* G*, define a* ***group ring*** $\mathbb{Z}[G]$ *as the set of formal sums* $\sum_{g \in G} a_g g$ *where* $a_g \in \mathbb{Z}$*.*

For $D \subseteq G$ we define an element of the group ring $D = \sum_{g \in G} a_g g$ where $a_g = 1$ if $g \in D$ and $a_g = 0$ otherwise. Also define $D^{(-1)} = \sum_{g \in G} a_g g^{-1}$. Here we give an example of apply a $(7, 3, 1)$ difference set $D = \{1, 2, 4\}$ to the group ring setting.

Example: $G = \mathbb{Z}_7 = \langle x | x^7 = 1 \rangle \qquad D = \{x, x^2, x^4\}$
$\mathbb{Z}[G] = \{a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^5 + a_5 x^5 + a_6 x^6 | a_i \in \mathbb{Z}\}$
$D = x + x^2 + x^4, D^{(-1)} = x^6 + x^5 + x^2$

Note that the product $DD^{(-1)}$ is the formal sum of all the "differences" of D. It follows that if D is a difference set in a multiplicative group G, then $DD^{(-1)} = k + \lambda(G \setminus \{1\}) = (k - \lambda) + \lambda G$. If we are dealing with a partial difference set, we must consider whether the identity element is in the set D or not. If $1 \in D$, $DD^{(-1)} = k + \lambda(D \setminus \{1\}) + \mu(G \setminus D) = (k - \lambda) + \lambda D + \mu(G \setminus D)$. Similarly, if $1 \notin D$, $DD^{(-1)} = (k - \mu) + \lambda D + \mu(G \setminus D)$. For a partial difference set every difference $a - b = c$ has a corresponding $b - a = -c$ so c and $-c$ are made by the same number of differences, so both or neither must be in D. This means $D = D^{(-1)}$ for partial difference sets.

We can extend the homomorphism to $\chi : \mathbb{Z}[G] \rightarrow \mathbb{C}$. This is defined by $\chi(\sum a_g g) = \sum a_g \chi(g)$ This new mapping can be applied to the group ring equations above. For a difference set,

$$\begin{aligned} \chi(DD^{(-1)}) &= \chi((k-\lambda)\{1\} + \lambda G) \\ &= k - \lambda + \lambda\chi(G) \end{aligned}$$

Since χ is a homomorphism, $\chi(D^{(-1)}) = \overline{\chi(D)}$. We can now write $|\chi(D)|^2 = \chi(D)\overline{\chi(D)} = k-\lambda+\lambda\chi(G)$. That is, for all non-principal characters,$|\chi(D)|^2 = k-\lambda$. We now have a way to check whether a set is a difference set without taking all the possible differences. If $|\chi(D)| \neq \sqrt{k-\lambda}$ for any $\chi \neq \chi_0$, D is not a difference set. Conversely, if $|\chi(D)| = \sqrt{k-\lambda}$ for all $\chi \neq \chi_0$ then D is a difference set.
We can find a similar equation for partial difference sets. For D containing the identity,

$$\begin{aligned} \chi(DD^{(-1)}) &= \chi((k-\lambda)\{1\} + \lambda D + \mu(G \setminus D)) \\ &= k - \lambda + (\lambda-\mu)\chi(D) + \mu\chi(G) \end{aligned}$$

Since we know $D = D^{(-1)}$, $\chi(D)^2 = (\lambda-\mu)\chi(D) + (k-\lambda)$ for all $\chi \neq \chi_0$. This is simply a quadratic equation in $\chi(D)$. Solving, we get $\chi(D) = \frac{(\lambda-\mu)\pm\sqrt{(\mu-\lambda)^2-4(\lambda-k)}}{2}$. Similarly, if the identity is not in D,$\chi(D) = \frac{(\lambda-\mu)\pm\sqrt{(\mu-\lambda)^2-4(\mu-k)}}{2}$. Thus $\chi(D)$ can take only two distinct values if D is a partial difference set. It is also true that if the character values for a set takes exactly two different values, then the set is a partial difference set.

This result can be used to show that complements of partial difference sets are partial difference sets. For any character which is non-principal on G, $0 = \chi(G) = \chi(D) + \chi(G \setminus D)$. This means $\chi(D) = -\chi(G \setminus D)$ so the character sums for the complement take exactly two values as well, and is thus a partial difference set.

Once we have a way to check whether a subset of a group is a difference set or a partial difference set, we must have methods that help us construct these subsets. In all cases, we use algebraic structures to find difference sets and partial difference sets. Permutation groups, finite fields, and Galois rings are some of these helpful structures.

A field $\mathbb{F}$ is a set with two binary operations, + and ×. $\mathbb{F}$ is an abelian group over + and $\mathbb{F}^*$ is an abelian group over ×. $\mathbb{F}$ is distributive on the left and right, that is $a(b+c) = ab+ac$ and $(a+b)c = ac+bc$. Finite fields exist only with orders that are powers of primes.

- **Example:** $\mathbb{Z}_p$ where p is a prime is a field with normal + and × mod p.

Finite fields of order p^n are constructed by $\mathbb{F}_{p^n} \cong \mathbb{Z}_p[x]/\langle g(x)\rangle$ where $\langle g(x)\rangle$ is the ideal generated by $g(x)$, a degree n polynomial that is irreducible in $\mathbb{Z}_p[x]$. The additive group is isomorphic to $\mathbb{Z}_p^n$ and the multiplicative group is cyclic of order $p^n - 1$. For ease of notation, an element $f(x) + \langle g(x)\rangle \in \mathbb{Z}_p[x]/\langle g(x)\rangle$ is written as $f(x)$.

- **Example:** $\mathbb{F}_{16}$

$$\mathbb{Z}_2[x]/\langle x^4+x+1\rangle$$

$$\begin{array}{ll}
x = x & x^2 = x^2 \\
x^3 = x^3 & x^4 = x+1 \\
x^5 = x^2+x & x^6 = x^3+x^2 \\
x^7 = x^3+x+1 & x^8 = x^2+1 \\
x^9 = x^3+x & x^{10} = x^2+x+1 \\
x^{11} = x^3+x^2+x & x^{12} = x^3+x^2+x+1 \\
x^{13} = x^3+x^2+1 & x^{14} = x^3+1 \\
x^{15} = 1 & 0
\end{array}$$

In this example we have provided the multiplicative and additive notation for each element in $\mathbb{F}_{16}$. This is easily done by reducing all x^4 to $x+1$, modulo 2.

A Galois Ring is a similar algebraic structure. It is also associated with two binary operations, + and ×. The additive group is an abelian group, but the ring is not necessarily a group under multiplication. The construction is similar: $\mathrm{GR}(n,k) \cong \mathbb{Z}_n[x]/\langle g(x)\rangle$ where $g(x)$ is a polynomial of degree k that is irreducible in $\mathbb{Z}_n[x]$. The additive structure is isomorphic to $\mathbb{Z}_n^k$. Again, an element $f(x)+\langle g(x)\rangle \in \mathbb{Z}_n[x]/\langle g(x)\rangle$ is simply called $f(x)$.

- **Example:** $\mathrm{GR}(4,2) \cong \mathbb{Z}_4[x]/\langle x^2+x+1\rangle$

$$\{0,1,2,3,x,2x,3x,1+x,1+2x,1+3x,2+x,2+2x,2+3x,3+x,3+2x,3+3x\}$$

The construction of this example requires finding a degree two irreducible polynomial modulo 4. To do this simply take a polynomial that is irreducible modulo 2, then take the square of the even degree terms and subtract from them the square of the odd degree term modulo 4. Then take the square root of all the terms of the polynomial while leaving their coefficients the same. Here is an example of how to find a degree 4 irreducible polynomial modulo 4.

First, take an irreducible polynomial of degree 4 modulo 2: x^4+x+1.
Then subtract the odd degree terms from the square of the even degree terms modulo 4.

$$(x^4+1)^2-(x)^2 = x^8+2x^4+1-x^2 \equiv x^8+2x^4+3x^2+1 (mod 4)$$

Take the square root of all the terms leaving the coefficients the same to get the degree 4 irreducible polynomial modulo 4: $x^4 + 2x^2 + 3x + 1$.

Along with finite fields and Galois Rings, permutation groups have provided us with a method of constructing partial difference sets. We work with two operations of permutation groups called the wreath product and exponentiation.

Consider two permutation groups (G, A) and (H, B), where $A = \{0, 1, 2, \ldots, a-1\}$. $H^A \times G$, where H^A is the set of all functions from A to H, is a group under the operation $((h_0, h_1, \ldots, h_{a-1}), g) \circ ((h'_0, h'_1, \ldots, h'_{a-1}), g') = ((h_0 h'_{0^g}, h_1 h'_{1^g}, \ldots, h_{a-1} h'_{a-1^g}), gg')$. One way of representing this group is with the wreath product. Each element of $H^A \times G$ is associated with a permutation $\pi((h_1, h_2, \ldots, h_a), g)$, where $(i, j)^{\pi((h_1, h_2, \ldots, h_a), g)} = (i^g, j^{h_i})$ for $(i, j) \in A \times B$. The wreath product is simply another permutation group $((G, A) \wr (H, B), A \times B)$ denoted $G \wr H$.

Example: Let $A = \{0, 1\}$, $B = \{0, 1, 2\}$, $G = \langle (0, 1) \rangle$, and $H = \langle (0, 1, 2) \rangle$
$A \times B = \{(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2)\}$
The element $\pi((0, 1, 2), (0)), (0, 1)$ acts on the elements of $A \times B$ as follows:
$(0, 0) \rightarrow (0^{(0,1)}, 0^{(0,1,2)}) = (1, 1)$ $\quad$ $(1, 0) \rightarrow (1^{(0,1)}, 0^{(0)}) = (0, 0)$
$(0, 1) \rightarrow (0^{(0,1)}, 1^{(0,1,2)}) = (1, 2)$ $\quad$ $(1, 1) \rightarrow (1^{(0,1)}, 1^{(0)}) = (0, 1)$
$(0, 2) \rightarrow (0^{(0,1)}, 2^{(0,1,2)}) = (1, 0)$ $\quad$ $(1, 2) \rightarrow (1^{(0,1)}, 2^{(0)}) = (0, 2)$
Representing $A \times B$ with $\{0, 1, 2, 3, 4, 5\}$, this is the permutation $(0, 4, 1, 5, 2, 3)$
The entire permutation group $G \wr H$ is:
{(0),(3,4,5),(3,5,4),(0,1,2),(0,1,2)(3,4,5),(0,1,2)(3,5,4),(0,2,1),(0,2,1)(3,4,5),
(0,2,1)(3,5,4),(0,3)(1,4)(2,5),(0,3,1,4,2,5),(0,3,2,5,1,4),(0,4,1,5,2,3),
(0,4,2,3,1,5),(0,4)(1,5)(2,3),(,5,2,4,1,3),(0,5)(1,3)(2,4),(0,5,1,3,2,4)}

Another way of representing $H^A \times G$ is as a permutation group that acts on B^A. In this case, each element is associated with a permutation $\tau((h_1, h_2, \ldots, h_a), g)$, where $(j_1, j_2, \ldots, j_a)^{\tau((h_1, h_2, \ldots, h_a), g)} = (j_{1'}^{h_{1'}}, j_{2'}^{h_{2'}}, \ldots, j_{a'}^{h_{a'}})$. For readability, i' is used to represent $i^{g^{-1}}$ for $i \in A$. This is called the exponentiation of (H, B) and (G, A), which we write $H \uparrow G$.

Example: Let $A = \{0,1\}$, $B = \{0,1,2\}$, $G = \langle(0,1)\rangle$, and $H = \langle(0,1,2)\rangle$
$B^A = \{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2),(2,0),(2,1),(2,2)\}$
The element $\tau((0,1,2),(0)),(0,1)$ acts on the elements of B^A as follows:
$(0,0) \rightarrow (0^{(0,1,2)}, 0^{(0)}) = (1,0)$ $\quad$ $(0,1) \rightarrow (1^{(0,1,2)}, 0^{(0)}) = (2,0)$
$(0,2) \rightarrow (2^{(0,1,2)}, 0^{(0)}) = (0,0)$ $\quad$ $(1,0) \rightarrow (0^{(0,1,2)}, 1^{(0)}) = (1,1)$
$(1,1) \rightarrow (1^{(0,1,2)}, 1^{(0)}) = (2,1)$ $\quad$ $(1,2) \rightarrow (2^{(0,1,2)}, 1^{(0)}) = (0,1)$
$(2,0) \rightarrow (0^{(0,1,2)}, 2^{(0)}) = (1,2)$ $\quad$ $(2,1) \rightarrow (1^{(0,1,2)}, 2^{(0)}) = (2,2)$
$(2,2) \rightarrow (2^{(0,1,2)}, 2^{(0)}) = (0,2)$
Labelling B^A as $\{0,1,2,3,4,5,6,7,8\}$, this is $(0,3,4,7,8,2)(1,6,5)$
The entire permutation group $H \uparrow G$ is:
{(0),(0,1,2)(3,4,5)(6,7,8),(0,2,1)(3,5,4)(6,8,7),(0,3,6)(1,4,7)(2,5,8),
(0,4,8)(1,5,6)(2,3,7),(0,5,7)(1,3,7)(2,4,6),(0,6,3)(1,7,4)(2,8,5),
(0,7,5)(1,7,3)(2,6,4),(0,8,4)(1,6,5)(2,7,3),(1,3)(2,6)(5,7),
(0,3,4,7,8,2)(1,6,5),(0,6,8,5,4,1)(2,3,7),(0,2,8,7,4,3)(1,5,6),
(0,5)(1,8)(4,6),(0,8,4)(1,2,5,3,6,7),(0,1,4,5,8,6)(2,7,3),
(0,4,8)(1,7,6,3,5,2),(0,7)(2,4)(3,8)}

Difference sets and partial difference sets do not appear sporadically. Instead, these sets are typically associated with some generalization of parameters. Along with the parameter family, each type of set has a specific construction to follow in order to find the difference set or partial difference set associated with those parameters. Here are some partial difference set families.

Paley Partial Difference Sets

$$(q, \frac{q-1}{2}, \frac{q-1}{4} - 1, \frac{q-1}{4})$$

where $\mathbf{q \equiv 1 (mod 4)}$ and q is a prime power.
The construction of these partial difference sets can be done in this manner $D = \{s \in \mathbb{F}_q^* : s = x^2, x \in F_q^*\}$.

- **Examples**
  $(5,2,0,1):$ $\quad G = \mathbb{F}_5^+ \cong \mathbb{Z}_5 \setminus \{0\}$ $\quad D = \{1^2 = 1, 2^2 = 4, 3^2 = 4, 4^2 = 1\}$
  $(9,4,1,2):$ $\quad G = \mathbb{F}_9^+$ $\quad D = \{1, 2\alpha + 1, 2, \alpha + 2\}$
  $(13,6,2,3):$ $\quad G = \mathbb{F}_{13}^+ \cong \mathbb{Z}_{13} \setminus \{0\}$ $\quad D = \{1,4,9,3,12,10\}$

Latin square type partial difference sets

$$(n^2, r(n-1), n + r^2 - 3r, r^2 - r)$$

The construction of this family involves finding r subgroups, $H_i \ni 1 \leq i \leq r$, of order n such that $H_i \cap H_j = \{0\} \ni 1 \leq i,j \leq r, i \neq j$. The partial difference set is $\bigcup H_i \setminus \{0\} \ni 1 \leq i \leq r$.

- **Examples**
  $(16, 9, 4, 6)$ Latin square PDS
  $G = \mathbb{Z}_2^4 \;\; n = 4 \;\; r = 3$
  $H_1 = \langle (0, 0, 1, 0), (0, 0, 0, 1) \rangle$
  $H_2 = \langle (1, 0, 0, 0), (0, 1, 0, 0) \rangle$
  $H_3 = \langle (1, 0, 1, 0), (0, 1, 0, 1) \rangle$
  $D = H_1 \cup H_2 \cup H_3 \setminus \{(0, 0, 0, 0)\}$

  Moreover, the choices for H_i can be done systematically in order to find any Latin square type partial difference set where $G = K \times K$. If $K = \{e, a, b\}$ the list of possible subgroups is $H_1 = \langle (e, a) \rangle, H_2 = \langle (a, e) \rangle, H_3 = \langle (a, a) \rangle, H_4 = \langle (a, b) \rangle$.

Negative Latin square type partial difference sets

$$(n^2, r(n-1), n + r^2 - 3r, r^2 - r)$$

The way to construct this type of partial difference set is through the help of a quadratic form. A quadratic form, $Q : G^n \to G$, is a polynomial defined over the finite field $\mathbb{F}$ that satisfies $Q(\alpha x) = \alpha^2 Q(x)$ for $x \in G, \alpha \in \mathbb{F}$. It follows, that the set $D = \{x | Q(x) = 0, x \neq 0, x \in G^n\}$ is a partial difference set.

- **Example**
  $(625, 144, 43, 30)$ Negative Latin square PDS
  $Q : Z_5^4 \to Z_5$
  $Q(x, y, z, w) = x^2 + xy + y^2 + z^2 + zw + w^2$
  $D = \{(x, y, z, w) | Q(x, y, z, w) = 0, (x, y, z, w) \neq (0, 0, 0, 0)\}$

Note: Partial Difference Set Families can overlap. If we take the example where q = 9 for the $q \equiv 1(mod 4) \wedge q$ is a prime power family and build a Latin square type partial difference set where $G = \mathbb{Z}_3^2, n = 3, r = 2$, and $H_1 = \langle (1, 0) \rangle, H_2 = \langle (0, 1) \rangle$ then we have two different constructions for the same partial difference set with the parameters $(9, 4, 1, 2)$.

A new family?

There are several examples of partial difference sets which satisfy the parameters $(2^{3e}, 2^{2e} + 2^e + 1, 2^e + 4, 2^e + 2)$ for small values of e. There is no known general construction for this family, and it is not known whether such a partial difference set exists for $e > 4$. The small examples are constructed in a variety of ways, so we are hopeful that there will be more members of this family.

We noticed that this could be part of a more general family $(n^3, n^2+n+1, n+4, n+2)$ for even n. This passes all non-existence criteria. We choose to work in he specific case $n = 2^e$ because this allows us to work in the setting of a finite field where we can exploit a multiplicative structure to help us search for new partial difference sets.

3 Known constructions for partial difference sets in this new parameter family

There are a number of partial difference sets with the desired parameters, $(2^{3e}, 2^{2e}+2^e+1, 2^e+4, 2^e+2)$. A few simple examples are given below.

When $e = 1$, a (8,7,6,4) partial difference set is found by selecting all nonidentity elements in any group of order 8. Each element x of the group can be written as a difference of group elements $x = a - b$ 8 different ways. If we restrict a and b to nonidentity elements, this leaves $\lambda = 6$ possible representations as differences for each x. Since there are no nonidentity elements outside the set, μ is irrelevant and this is also a $(8, 7, 6)$ difference set.

For $e = 2$, the parameters (64,21,8,6) have two different constructions. The first constructions uses the Latin square family of partial difference sets, $(n^2, r(n-1), n+r^2-3r, r^2-r)$, because the parameters are the same with $r = 3$ and $n = 8$. In groups of the form $H \times H$ where H is any group of order 8, select the subgroups $\{(h,0)|h \in H\}$,$\{(0,h)|h \in H\}$,and $\{(h,h)|h \in H\}$. These subgroups are pairwise disjoint except at the identity element; satisfying the conditions for the Latin square construction. This construction will not work for all groups of order 64. For example, $\mathbb{Z}_{64}$ has only one subgroup of order 8, so it is impossible to find three subgroups of order 8. It will be shown in section 4 that no other abelian group of order 64 can support a Latin squares partial difference set.

The second construction involves using the finite field $\mathrm{GF}(2,6)$. If we take the multiplicative subgroup of order 21 in $\mathbb{F}_{64}$, it is a (64,21,8,6) partial difference set in the additive group. We will see that this is a special case of another construction.

When $e = 3$, Frank Fiedler and Mikhail Klin demonstrate a construction for a (512,73,438,12,10) strongly regular graph. This graph is equivalent to a (512,73,12,10) partial difference set. The 512 vertices of the graph were generated through a series of wreath products and exponentiations of permutation groups. A computer search was then used to choose orbits which formed a strongly regular graph with valency 73.

They begin with two permutation groups, (G, A) and (H, B). In this case, $A = \{0,1\}$, $G = \mathbb{Z}_2 = \langle(0,1)\rangle$, $B = \{0,1,2\}$, and $H = \mathbb{Z}_3 = \langle(0,1,2)\rangle$. The exponentiation $\mathbb{Z}_3 \uparrow \mathbb{Z}_2$ is a permutation group on the elements of B^A. For ease of notation, we let $B^A = \{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2),(2,0),(2,1),(2,2)\}$ be identified with $Y = \{0,1,2,3,4,5,6,7,8\}$. We then consider the exponentiation $\mathbb{Z}_2 \uparrow (\mathbb{Z}_3 \uparrow \mathbb{Z}_2)$ which is a permutation group on A^Y. Here $|A^Y| = |A|^{|Y|} = 2^9$, the desired group size. At this point, Fiedler and Klin calculated all the 2-orbits of $(\mathbb{Z}_3 \uparrow \mathbb{Z}_2) \wr \mathbb{Z}_2$ and chose 10 of them with total valency of $k = 73$.

In our last known example, $e = 4$, C.L.M. DeLange demonstrated the construction of a (4096,273,20,18) partial difference set in the additive field generated by $\mathbb{Z}_2[x]/\langle x^{12} + x^9 + x^3 + x^2 + 1\rangle$, $\mathbb{F}_{4096}$. This is the partial difference set $D = ZK$ where $Z = \{1, \alpha^5, \alpha^{10}\}$ and $K = \langle \alpha^{45} \rangle$. That is, three cosets of the multiplicative subgroup of order 91. DeLange notes that this set can be viewed another way. If we consider $\mathbb{F}_{4096}$ to be a 3-dimensional vector space $\mathbb{F}_{16}^3$ and look at the graph which corresponds to D, each vertex has exactly one neighbor in every direction.

4 Our Research

The majority of our work has been done to better understand the examples of partial difference sets that satisfy the specified parameters. Along with this, we attempted to extend some of the constructions to larger values of e. Almost all the testing required the use of writing computer programs in C++.

Most of our research has involved different ways to construct subsets of $k = 2^{2e} + 2^e + 1$ for various values of e. Brute force testing of a set would prove to be infeasible for even moderate sizes. In order to do that sort of calculation, there are two possibilities. First, the number of times each of the v elements of the group can be represented as differences could be stored. This would require far too much memory. For example when $e = 6$, we have $|G| = 2^{18}$, $\lambda = 68$, and $\mu = 66$, both of which cannot be stored in a single byte. Alternately for each element of G, compute all $k(k-1)$ to determine how often it occurs. This becomes prohibitive in runtime and can be difficult when working in groups other than EA(2^{3e}). Using characters provides a method for determining whether a set is a partial difference set which is both time and memory efficient to program. In addition, we know what value our character sums should be through the help of simple algebra using equation.... Hence, for every value of e, the character sums must be 1 ± 2^e. In all our work we used character theory to verify partial difference sets.

We noted that the Latin square construction could be used as an example of an $e = 2$ partial difference set. This does not work, however in any other case.

Proof: We need v to be equal to both n^2 and 2^{3e} for some n and e. We can write $n = 2^{\frac{3}{2}e}$. Also, we need k to be $2^{2e} + 2^e + 1$ and $r(n-1)$. Thus $2^{2e} + 2^e + 1 = r(n-1) = r(2^{\frac{3}{2}e} - 1)$. Solving for r we get

$$r = \frac{2^{2e} + 2^e + 1}{2^{\frac{3}{2}e} - 1} = 2^{\frac{e}{2}} + \frac{1}{2^{\frac{e}{2}} - 1}$$

It is easy to see that the only value of e for which r is an integer is $e = 2$. □

It is also interesting to determine which groups of order 64 support a Latin square type partial difference set. In groups of the form $H \times H$ where H is any group of order 8, select the subgroups $\{(h,0)|h \in H\}$,$\{(0,h)|h \in H\}$,and $\{(h,h)|h \in H\}$. We will show that none of the other 8 abelian groups of order 64 contain Latin square partial difference sets.

For each group, we will show that it is impossible to distribute the elements of order 2 into three distinct subgroups. Since all these groups are abelian, the subgroups of order 8 must be isomorphic to $\mathbb{Z}_8$,$\mathbb{Z}_4 \times \mathbb{Z}_2$ or $\mathbb{Z}_2^3$, which have 1,3,and 7 elements of order 2 respectively. We will list the abelian groups (along with how many elements of order 2 they contain) and then explain why we cannot have a Latin square PDS in that group.

- $\mathbb{Z}_{32} \times \mathbb{Z}_2, \mathbb{Z}_{16} \times \mathbb{Z}_4(3)$: Since there are only three elements of order 3, we must have all subgroups isomorphic to $\mathbb{Z}_8$. This is not possible, however, because all subgroups of order 8 contain the same order 2 element, $(16,0)$ and $(8,0)$ respectively.

- $\mathbb{Z}_{16} \times \mathbb{Z}_2^2, \mathbb{Z}_4^3(7)$: Since there are only 7 elements of order 2, we must have no Z_2^3 and at most two $\mathbb{Z}_4 \times \mathbb{Z}_2$, and the rest $\mathbb{Z}_8$. This is clearly not possible in $\mathbb{Z}_4^3$ since there are no $\mathbb{Z}_8$ subgroups. In $\mathbb{Z}_{16} \times \mathbb{Z}_2^2$, all the allowable subgroups contain $(8,0,0)$, so they cannot be disjoint.

- $\mathbb{Z}_8 \times \mathbb{Z}_2^3(15), \mathbb{Z}_4 \times \mathbb{Z}_2^4(31)$ All subgroups of order 8 not isomorphic to $\mathbb{Z}_2^3$ contain a common element, $(4,0,0,0)$ in $\mathbb{Z}_8 \times \mathbb{Z}_2^3$ and $(2,0,0,0,0)$ in $\mathbb{Z}_4 \times \mathbb{Z}_2^4$. There must then be at least two subgroups of the form $\mathbb{Z}_2^3$. These subgroups will be $\langle g_1, g_2, g_3 \rangle$ and $\langle g_4, g_5, g_6 \rangle$ and where each g_i is an element of order 2. Assume we can choose five of the six generators required. For the sixth, to allow the subgroups to be disjoint, we cannot choose anything in $\langle g_1, g_2, g_3 \rangle + \langle g_4, g_5 \rangle$ where $A + B = \{a + b | a \in A, b \in B\}$. This eliminates 31 possibilities, so we cannot find two disjoint $\mathbb{Z}_2^3$ subgroups.

• $\mathbb{Z}_8 \times \mathbb{Z}_4 \times \mathbb{Z}_2(7)$: There can clearly be no $\mathbb{Z}_2^3$ and at most two $\mathbb{Z}_4 \times \mathbb{Z}_2$. There can be at most one $\mathbb{Z}_8$ because they all contain $(4, 0, 0)$. We must then have exactly one $\mathbb{Z}_8$ and two $\mathbb{Z}_4 \times \mathbb{Z}_2$. It is sufficient to show that there cannot be two $\mathbb{Z}_2^2$ subgroups. This argument is similar to the previous case. We need four generators, and when we choose 3 we eliminate all 7 elements of order two.

In another of our simple examples, we noted that the multiplicative subgroup of order 21 of $\mathbb{F}_{64}^*$ is a partial difference set in the additive group of F_{64}. This is an example of an $e = 2$ partial difference set. When we attempted to extend this to higher values of e, the subgroups did not form partial difference sets. For example, when $e = 3$ we took the subgroup of order 73 from $\mathbb{F}_{512}^*$, the character sums did not equal 9 or -7. The $e = 2$ case is in fact a specific case of the next construction.

The DeLange example provided us with a partial difference set construction for the $e = 4$ case by looking at the multiplicative field $\mathbb{F}_{4096}$. From this, he used the multiplicative subgroup of order 91 to make 3 cosets. The union of these cosets is a partial difference set. This provided us with an example that could easily be modified by taking the field $\mathbb{F}_{2^{3e}}$ and finding subgroup of order $k/3$. In order to extend the field size, we needed to find irreducible primitive polynomials in $\mathbb{F}(2, 3e)$ of degree $3e$. Meaning, $\alpha \in \mathbb{F}(2, 3e) \ni \langle\alpha\rangle = \mathbb{F}(2, 3e)^*$. Then, with each subgroup of order $k/3$, we used a computer search to test out different coset representatives as the possible set Z in DeLange's notation to see if they would provide us with a partial difference set. In every case, the tested triple of coset leaders is of the form $\{alpha^a, \alpha^b, \alpha^c\} \ni 0 \leq a, b, c < k/3, a \neq b \neq c$.

Our initial reaction for this example was to check whether or not if provided us with a partial difference set in the case where $e = 2 : (64, 21, 8, 6)$. Here, we are working in the field $\mathbb{F}_{64}$ generated by $\mathbb{Z}_2[x]/\langle x^6 + x + 1\rangle$. The multiplicative subgroup of order 7 is generated by $\langle\alpha^9\rangle$ is our K as noted in the DeLange construction. Then, we search over different coset leaders to find that any combination of three coset leaders of the form $\{\alpha^a, \alpha^b, \alpha^c\} \ni 0 \leq a, b, c < 9, a \neq b \neq c$, along with the multiplicative subgroup of order 7 gives us a partial difference set such that $Z = \{\alpha^a, \alpha^b, \alpha^c\}, K = \langle\alpha^9\rangle$ and $D = Z \times K$. This is no real surprise because the cosets of the multiplicative subgroup of order 7 are additive subgroups of order 8 that pairwise intersect in only the identity. Hence, we fall back into the Latin square type partial difference construction in which $n = 8$ and $r = 3$.

Next, we looked at constructing the example DeLange presented in his paper. After recreating his difference set, we further tested for all combinations of coset representatives that could produce another difference set for the $e = 4$ case. Our computer search found 135 combinations of coset representatives, including De-

Lange's example, that produced a difference set in the additive field $\mathbb{F}_{4096}$. These 135 combinations of coset representatives do find distinct partial difference sets; however, we shall note that each of these partial difference sets will relate to one of these three representations of Z.

$$\{1, \alpha^5, \alpha^{10}\} \quad \{1, \alpha^5, \alpha^{25}\} \quad \{1, \alpha^5, \alpha^{40}\}$$

The rest of the partial difference sets build off of these three examples in this manner, $x^i * Z$ where $1 \leq i < 45$.

We attempted to extend the DeLange construction to higher values of e. Here we will compare the circumstances for $e = 6, e = 8$ against the $e = 4$ case.

e	Group	primitive irreducible polynomial	K	$\|K\|$	(v, k, λ, μ)
4	$\mathbb{F}_{4096}$	$\alpha^{12} = \alpha^9 + \alpha^3 + \alpha^2 + 1$	$\langle\alpha^{45}\rangle$	91	$(4096, 273, 20, 18)$
6	$\mathbb{F}_{262144}$	$\alpha^{18} = \alpha^7 + 1$	$\langle\alpha^{189}\rangle$	1387	$(262144, 4161, 68, 66)$
8	$\mathbb{F}_{16777216}$	$\alpha^{24} = \alpha^{23} + \alpha^{22} + \alpha^7 + 1$	$\langle\alpha^{765}\rangle$	21931	$(16777216, 65793, 260, 258)$

The parameters of these partial difference sets grow very quickly making computer search a lengthy process. Still, our tests came back with no positive results for a new partial difference set when searching over different selections of coset representatives.

Note: We attempted this method only when e is even because when e is odd, 3 does not divide k. The idea of using more than three coset representatives for a subgroup was discussed. Here is an example of such a setup: for $e = 4$, use the multiplicative subgroup of order 39, $\langle\alpha^7\rangle$, as K, and test for $Z = \{\alpha^{i_0}, \alpha^{i_1}, \alpha^{i_2}, \alpha^{i_3}, \alpha^{i_4}, \alpha^{i_5}, \alpha^{i_6}\} \ni \forall i_x, i_y, 0 \leq i_x < k/7$ and $i_x \neq i_y$. Unfortunately, this example does not lead to a partial difference set.

Another example of a partial difference set from this parameter family was constructed through permutation groups. We reproduced the $e = 3$ PDS which Fiedler and Klin constructed and verified that it was a partial difference set. Then we attempted to extend their construction for larger values of e.

We hoped to find other permutation groups (G, A) and (H, B) such that $G \uparrow (H \uparrow G)$ would be a permutation group which acts on a group with order 2^{3e}.

If $|B| = 1$ we could choose $|A| = 2^{3e}$ and this would give us a group of the correct size. This does not help in finding a partial difference set because $G \uparrow (H \uparrow G) = G$ and we would have to choose k of 2^3e 2-orbits which is the equivalent to choosing the elements of our partial difference set directly.

We know that $G \uparrow (H \uparrow G)$ acts on a set of order $|A|^{(|B|^{|A|})}$. In order for $|A|^{(|B|^{|A|})}$ to be a power of 2, $|A|$ must be a power of 2. Assume $|B| \neq 1$ and $|A| > 2$. The smallest example is $|A| = 4$,$|B| = 2$ which has $|A|^{(|B|^{|A|})} = 2^{32}$. The smallest set with order 2^{3e} is $2^{3(54)}$.

Thus, if we are going to find a reasonably sized partial difference set, we must let $|A|$ have order 2. Since $|A|^{(|B|^{|A|})} = 2^{3e}$, $|B|$ must be a multiple of 3. $|B| = 3$ is the case studied by Fiedler and Klin. The next smallest is $|B| = 6$ which corresponds to $e = 12$. This is infeasible for us, but could be possible for someone with more computing power and time.

DeLange concluded his paper describing the $e = 4$ strongly regular graphs as a graph with a vertex set $\mathbb{F}_{16}^3$ such that each vertex has a unique neighbor in each of the 273 directions. In other words, if we take an element of the 3-dimensional vector space $\mathbb{F}_{16}^3$, then it has one neighbor in each of the 1-dimensional subspaces of $\mathbb{F}_{16}^3$. In general, the number of one dimensional vector spaces in a three dimensional vector space $\mathbb{F}_{2^e}^3$ is found by taking the number of non-zero elements in the vector space and dividing by the number of non-zero elements in the base field. The latter is the number of non-zero elements in each subspace. This shows that the number of one-dimensional subspaces is $\frac{2^{3e}-1}{2^e-1} = 2^{2e} + 2^e + 1 = k$. This gave us hope that we could generalize this result for our entire family.

We began with trying to associate this property with the $e = 2$ case. A computer search showed that we could select a basis for $\mathbb{F}_4^3$ such that each subspace contained one element of our partial difference set. We hoped to find that this would also be true for $e = 3$.

We first tried to find a basis for the vector space that would allow the set to spread out to one in each subspace. We used the partial difference set from Fiedler and Klin. We used a computer search to generate the vector space $\mathbb{F}_8^3$ and its subspaces and determine how many elements were in each subspace. We were unable to complete this search because the number of ways to represent $\mathbb{F}_8^3$ as a three-dimensional vector space is prohibitive.

In another attempt, we used the canonical basis $\{(0,0,1),(0,1,0),(1,0,0)\}$ to define the vector space and tried to fit the partial difference set into it. We used automorphisms of $\mathbb{F}_5 12$ to see if it would send one element to each vector space. This approach is more intuitive, but equivalent to choosing the elements of the basis. There are equally many ways to do this, so we did not have time to exhaust all possible automorphisms.

In either attempt, the search space involved was extremely large. Nothing conclusive was discovered while the programs ran. After the programs ran for a few minutes, we soon realized that they could run for several years before finishing. We decided not to continue with this approach.

Another approach we decided to look at was possibly embedding the $e = 2$ partial difference set in $\mathbb{F}_{64}$ inside of $\mathbb{F}_{4096}$. When looking at the prime factorization of $v - 1$ and k, these numbers build off of one another, especially for k .

e	$v - 1$	k
2	$3^2 * 7 - 1 = 63$	$3 * 7 = 21$
4	$3^2 * 5 * 7 * 13 - 1 = 4095$	$3 * 7 * 13 = 273$
8	$3^2 * 5 * 7 * 13 * 17 * 241 - 1 = 1677215$	$3 * 7 * 13 * 241 = 65793$

Hence, we tried to take 13 "cosets" of the multiplicative subgroup of order 21 in $\mathbb{F}_{4096}$ to see if that would build a new partial difference set with the $e = 4$ parameters. Combinatorially, the search space would be $\binom{195}{13} \approx 6 * 10^{19}$ which makes testing this approach a very lengthy matter. After running a program for several hours, we managed to barely scratch the surface of the entire search space. Thus, we abandoned this approach.

As we have mentioned earlier, the second most important question when dealing with partial difference sets is if there exists a partial difference set of size k in a group of order v, are there any other non-isomorphic groups of order v that support a partial difference set of the same size.

Earlier we discussed that there are examples known for the $e = 2$ case in groups other than $\mathbb{Z}_2^6$, namely $\mathbb{Z}_8^2$ and $\mathbb{Z}_4^2 \times \mathbb{Z}_2^2$. These groups used the Latin square construction to find partial difference sets; however, no other abelian groups supported Latin square type partial difference sets. Hence, we attempted to find a partial difference sets in the group $\mathbb{Z}_4^3$ with the help of Galois Rings. Then we extended this method to the $e = 4$ case to see if it would produce are partial difference set in $\mathbb{Z}_4^6$.

We use Galois Rings to help us because $\mathrm{GR}(4, 3)^+ \cong \mathbb{Z}_4^3$. As noted above in the preliminary section, if you have an irreducible polynomial, $x^3 + 2x^2 + x + 3$, in $\mathbb{Z}_4[x]$, $\mathrm{GR}(4, 3) \cong \mathbb{Z}_4[x]/\langle x^3 + 2x^2 + x + 3\rangle$. If we look at Galois Ring in the multiplicative setting, replacing x^3 with $2x^2 + 3x + 1$, we notice that $x^7 = 1$. These 7 elements $\{1, x, x^2, x^3 = 2x^2 + 3x + 1, x^4 = 3x^2 + 3x + 2, x^5 = x^2 + 3x + 3, x^6 = x^2 + 2x + 1\}$ do not form an additive group when we union 0 with this list. This prevents us from falling into the Latin square construction of taking the union of 3 additive subgroups of order 8 that pairwise intersect in only the identity to construct a partial difference set. We then took the union of all the possible combinations of three cosets of these elements to see if this would construct a partial difference set. Unfortunately it did not.

We extended this method to $e = 4$ to see what would happen in $\mathbb{Z}_4^6$. Again, $\mathrm{GR}(4, 6)^+ \cong \mathbb{Z}_4^6$ and we constructed $\mathrm{GR}(4, 6)$ by $\mathbb{Z}_4[x]/\langle x^6 + 2x^3 + 3x + 1\rangle$. Then we looked at the multiplicative structure of $\mathrm{GR}(4, 6)$, and notice $x^{63} = 1$ when replacing

x^6 with $2x^3 + x + 3$. We then used the multiplicative subgroup of order 21, $\langle x^3 \rangle$ and took 13 cosets of it to see if this would construct a partial difference set. Again, our attempt did not work.

5 Concluding Remarks

We were unable to produce a new partial difference set in the $(2^{3e}, 2^{2e} + 2^e + 1, 2^e + 4, 2^e + 2)$ family. We have reproduced and verified all known examples, and attempted to extend the techniques used. Large search spaces prohibited us from testing many possibilities for most of our attempted methods of construction. Still, we are hopeful that more partial difference sets in this family exist, and that a general construction can be found.