Partial Difference Sets in New Groups

Tiffany L. Broadbent
University of Richmond
Richmond, VA 23173
email: tbroadbe@richmond.edu

Edward P. Kenney
University of Richmond
Richmond, VA 23173
email: ekenney2@richmond.edu

Abstract

We investigate the connections between partial difference sets and projective planes of several different orders in an attempt to locate a family of partial difference sets in new groups. We first show several Galois ring constructions, and then describe work using quadratic forms and Mathon-constructed maximal arcs to provide insight into their geometry and structure.

Acknowledgement: We thank the University of Richmond Undergraduate Research Committee for their support of this research. We also thank Dr. Jim Davis for his guidance and support.

1 Introduction

We examine partial difference sets constructed by Davis and Xiang in the projective plane of order 16. A partial difference set is a subset D of a group A, such that a multiset M, which contains the difference between every pair of elements in D, contains each element of the subset D exactly μ number of times, and contains each non-zero element of the $A\backslash D$ exactly λ number of times. Partial difference sets can be constructed using both Algebraic and Geometric techniques. Davis and Xiang use an algebraic construction that produces partial difference sets of both the largest and smallest possible sizes within a given group. We attempt to connect the Davis-Xiang algebraic construction to the geometry of Mathon's construction, in an effort to gain insight into the possible existence of Davis-Xiang constructions of intermediate sizes. We first examine the relationship between Davis-Xiang and Mathon in the projective plane of order 8. We then attempt to form a connection in the projective plane of order 16, and finally we attempt to utilize a Denniston construction in a direct attempt to construct a partial difference set of intermediate size in the projective plane of order 16. In section 2 we address the necessary background information in finite fields, Galois rings, projective planes, partial difference sets, quadractic forms, and character theory. In section 3 we describe three different methods for constructing partial difference sets. Section 4 provides Java and Mathematica implementation details pertaining to the evaluation of partial difference sets. In section 5, we provide details about the problem being addressed. Section 6 describes the process of searching for insight into this problem. Section 7 provides our conclusion.

2 Preliminaries

2.1 Finite Fields

Finite fields provide the algebraic setting in which we will examine partial difference sets. A field consists of a set F, together with two binary operations $(+, *)$ such that both $(F, +)$ and $(F^*, *)$ are Abelian groups. A finite field satisfies the same set of conditions, with the additional condition that the set be finite.

Example 2.1 *The following are finite fields:*
$(\mathbb{Z}_2, +, *)$
$(\mathbb{Z}_p, +, *)$, *where p is any prime number*
$(\mathbb{F}_4, +, *)$

Example 2.2 *The following are not finite fields:*
$(\mathbb{Z}+, *)$
$(\mathbb{Z}_4, +, *)$

The integers modulo any prime will form a finite field since all multiplicative inverses are contained in the set. The integers modulo a non-prime, however, will not have a

multiplicative inverse for every element. For example, $\mathbb{Z}_4$ is not a field because 2 does not have a multiplicative inverse modulo 4. There is a finite field of order four though, namely $\mathbb{F}_4$, which consists of the elements 0, 1, α, and $\alpha + 1$. This set is produced by the expression

$$\mathbb{Z}_2[x]/ < x^2 + x + 1 >$$

$\mathbb{Z}_2[x]$ denotes the set of polynomials with coefficient ring $\mathbb{Z}_2$. All polynomials in the set are reduced modulo $\langle x^2 + x + 1\rangle$. Reducing by this polynomial can be thought of as replacing all instances of x^2 with $x + 1$, modulo 2. $< x^2 + x + 1 >$ satisfies the condition of "irreducibility", namely there do not exist polynomials $g(x)$ and $h(x)$, $deg(g(x)), deg(h(x)) < deg(f(x))$, such that

$$f(x) = g(x)h(x)$$

We will use the notation $\alpha = x + \langle x^2 + x + 1\rangle$, and note that $\alpha^2 = \alpha + 1$.

Elements in a finite field can be written in both multiplicative and additive notation. Additive notation describes an element in terms its coefficients. Elements appear in the following form:

$$a + bx + cx^2 + ... + rx^{r-1}$$

Multiplicative notation describes an element in terms of a power of a primitive element. A finite field F contains the following elements in multiplicative notation:

$$1, x, x^2, x^3, x^4, x^5, ...x^{q-2}, \text{ where } q = |F|$$

The multiplicative group of a finite field is always cyclic [3]. Thus any nonzero element in the field can be represented as a power of a primitive element.

2.2 Galois Rings

Galois rings also prove useful in providing a setting for the construction of partial difference sets. A Galois ring is a generalization of a finite field, formed by a relaxation of the definition. A ring R is a nonempty set with two associated binary operations (+,*), such that (R,+) is an Abelian group, and such that the multiplication operation displays associative and identity properties, and distributes over the addition operation, but is not necessarily a multiplicative group. Standard notation for a Galois ring consisting of polynomials is GR(a, b), where a is the order of the coefficient ring, and b is the degree of the polynomial modulus. We will be examining Galois rings with coefficient ring $\mathbb{Z}_4$. For example, GR$(4, 3)$ is produced by the expression $\mathbb{Z}_4[x]/ < x^3 + 2x^2 + x + 3 >$

A Teichmuller set, τ, is a key component of a Galois ring. It consists of 0, together with the powers of a primitive element. A primitive element is a generator of an Abelian multiplicative group, so the Teichmuller set behaves essentially like the finite field with which the Galois ring is associated. Every element of a Galois ring can be written as a

combination of two elements from its corresponding Teichmuller set. Consider a Galois ring $GR(4,t)$. Then for every g $\in GR(4,t)$, there exist $\xi_1, \xi_2 \in \tau$ such that g $= \xi_1 + 2\xi_2$.

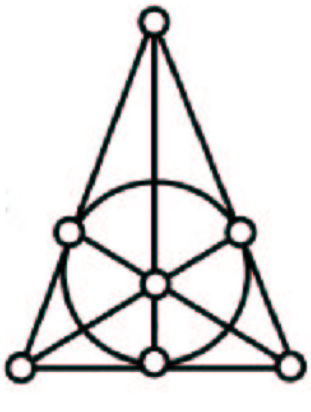
Example 2.3 *In the Galois ring* GR$(4,2) : \mathbb{Z}_4[x]/ < x^2+x+1 >$*:* $\{0, 1, 2, 3, \beta, 2\beta, 3\beta, 1+\beta, 1+2\beta, 1+3\beta, 2+\beta, 2+2\beta, 2+3\beta, 3+\beta, 3+2\beta, 3+3\beta\}$
Teichmuller Set: $\{0, 1, \beta, \beta^2 = 3+3\beta\}$
Consider $\{3+2\beta\} \in GR$.
$\{3+2\beta\} = 1+2(3+3\beta)$.
Thus it can be represented as a linear combination of the pair of Teichmuller set elements $(1, 3+3\beta)$.

2.3 Projective Planes

Our goal is to gain insight into the existence of a partial difference set by connecting geometry to algebra. As such, it is first imperative that we explore this geometry, the geometry of the projective plane.
A projective plane is an incidence structure satisfying:

1. Any two points determine a line.
2. Any two lines intersect in a point

We can construct projective planes by considering vector spaces of dimension 3, defined over a finite field GF(q). Consider a given vector space, V. A projective plane defined within V will have each distinct one-dimensional subspace being a point and each distinct two-dimensional subspace being a line. This means that the points on a projective plane represent a collapse of several scalar multiples onto a single representative vector. The following diagram depicts the projective plane of order 2, defined over $\mathbb{Z}_2$.



The size of a given projective plane is a result of the order of the finite field over which it is defined. We define the order of a projective plane, therefore, to be equal to the order of the finite field over which the vector space was defined.

Theorem 2.4 *Let P be a projective plane constructed as above, over a finite field F. Then*

1. *Any two lines intersect in a point.*
2. *Every pair of distinct points uniquely determines a line.*
3. *P contains $\frac{|V|-1}{|F|-1}$ points.*
4. *P contains $\frac{|V|-1}{|F|-1}$ lines.*
5. *There are $|F|+1$ points per line.*
6. *$|F|+1$ lines intersect in each point.*

Proof:

1. Consider 2 distinct lines, l_1 and l_2, two 2-dimensional subspaces, represented by the basis vectors (v_1,v_2) and (w_1,w_2) respectively. Then all points on l_1 are of the form $av_1 + bv_2$ and all points on l_2 are of the form $cw_1 + dw_2$, where a, b, c, and d are scalars and consider the intersection of l_1 and l_2. There exist a, b, c, d, such that $av_1 + bv_2 = cw_1 + dw_2$. This can be written as the following system of equations:

$$\begin{pmatrix} v_1 & v_2 & -w_1 & -w_2 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = (0)$$

   The solution to this system is the null space. Observe that the rank of the system is three, and that row space is contained in a space of dimension 4. It follows, then, that:

$$\text{Total Dimension} = \text{Dimension of the null space} + \text{rank}$$

   By algebra,

$$\text{Total Dimension} = 4 = \text{dimension null space} + 3$$
$$\text{dimension null space} = 1$$

   Since the null space is a solution to this system of equations the intersection of any two lines is a one-dimensional subspace, or a point in the projective plane. Thus any two lines intersect in a point.

2. Two one-dimensional subspaces form the basis for a two-dimensional subspace. In the projective world, then, two points uniquely form the basis for a line.

3. The zero vector does not exist on the projective plane, so there are $|V|-1$ useable vectors in the vector space V. Recall that P is composed of points representing themselves as well all of their non-zero scalar multiples in F. $|F|-1$ represents the number of non-zero scalar multiples of any given point in the finite field F. Thus the $|V|-1$ points in V collapse onto the points in the projective plane $|F|-1$ at a time. Thus there are $\frac{|V|-1}{|F|-1}$ points on the projective plane.

4. A counting argument similar to the above proves this property.

5. Let l be a line contained in P, defined by two basis vectors v_1 and v_2. Then there are $|F| * |F|$ linear combinations of v_1 and v_2 in V, $|F|^2 - 1$ without the zero vector. In projective space, however, $|F| - 1$ vector space points collapse onto each projective point. Thus there are $\frac{|F|^2-1}{|F|-1} = |F|+1$ projective points that can be written as scalar multiples of v_1 and v_2, or $|F| + 1$ points per line.

6. A similar argument provides proof of this property.

□

2.4 Partial Difference Sets

A partial difference set is a subset D, of order k, of an algebraic setting A, of order v, such that a multiset M, which contains the difference between every pair of elements in D, contains each element of the subset exactly μ number of times, and contains each non-zero element of A not in D exactly λ number of times. A partial difference set is described as four-tuple of its parameters: (v, k, μ, λ).

Example 2.5 *A* $(5, 2, 0, 1)$ *partial difference set:*
$A = Z_5$
$D = \{1, 4\}$
$M = \{2, 3\}$
$\mu = 0$
$\lambda = 1$

In a partial difference set the following relationship between parameters holds.

$$(v - k - 1)\lambda + \mu * k = k(k - 1)$$

In a symmetric difference set S, every nonzero element of A appears exactly λ times in M. A symmetric difference set is described by its parameters as a three-tuple: (v, k, λ).

Example 2.6 *A* $(7, 3, 1)$ *symmetric difference set:*
$A = Z_7$
$D = 1, 2, 4$
$M = 1, 2, 3, 4, 5, 6$
$\lambda = 1$

In a symmetric difference set, the following relationship between parameters holds.

$$(v-1)\lambda = k(k-1)$$

.

2.5 Character Theory

Character theory provides the ability to determine whether or not a set is a partial difference set without computing the multiset associated with the subset D. A character χ, of an Abelian group, G, is a homomorphism from G to the multiplicative group C^*. As a homomorhpism, χ must satisfy $\chi(\alpha+\beta) = \chi(\alpha) \times \chi(\beta)$. For example, consider the group Z_2^3, and define χ as the mapping

$$(1,0,0) \mapsto -1$$
$$(0,1,0) \mapsto 1$$
$$(0,0,1) \mapsto -1$$

Note that once the homomorphism is defined for the basis vectors of the group, the rest of the homomorphism is uniquely determined. Given a character χ, we can evaluate that character over a given element in a partial difference set. For example, take the point $(1,1,0)$ in G. The point is evaluated coordinate by coordinate. The first coordinate corresponds to the basis vector (1,0,0), and $\chi(1,0,0) = -1$, so to evaluate the first coordinate, -1 is raised to the corresponding coordinate, in this case 1. Complete evaluation of the point would look like the following:

- χ evaluated over$(1,1,0) : \{1,0,0\} \mapsto -1, -1^1 = -1\ \{(0,1,0)\} \mapsto 1, 1^1 = 1\ \{(0,0,1)\} \mapsto -1, -1^0 = 1$ Product of coordinate values $= -1 * 1 * 1 = -1$

This process continues over every point in the difference set, with the sum of the evaluations representing the character sum for χ. If we repeat this process with every possible character χ of a given group, and look at all the character sums that result, we can determine whether or not a set is a partial difference set. If the character sums are "well behaved", then we have a difference set. Typically, a "well behaved" character sum is considered to be a set of sums with only two different values, although a set with more than two values could be interesting as well. We will be considering characters over $\mathbb{Z}_2$ and $\mathbb{Z}_4$. Since χ is a homomorphism, the mapped group must behave exactly like the original group. Therefore, elements in $\mathbb{Z}_4$ map to powers of the imaginary number i, and elements in $\mathbb{Z}_2$ map to powers of -1.

2.6 Quadratic Forms

A quadratic form, Q, is a polynomial, defined over a finite field F, of the form $\alpha x^2 + xy + \beta y^2 : \alpha, \beta \in F$, such that $Q(x)$ satisfies $Q(\gamma x) = \gamma^2 Q(x)$ (plus another technical condition). Non-degeneracy requires a condition similar to that of "irreducibility", described earlier. A non-degenerative quadratic form $Q(x,y)$ is such that there do not exist polynomials

$f(x,y)$ and $g(x,y)$, where $deg(f), deg(g) < deg(Q)$ such that $Q(x,y) = f(x,y) * g(x,y)$. For example, over $\mathbb{F}_8$, $Q(x,y) = x^2+xy+\alpha^3y^2$ is nondegenerate. $Q(x,y) = \alpha^5x^2+xy+\alpha^4y^2$ is not, however, since it can be written as $(\alpha^5x+\alpha^4y)(x+y)$. It is also important to note that a quadratic form "covers" each element in the finite field an equal number of times. In other words, there are an equal number of solutions when the expression is set equal to each element of the field. We have thus far written quadratic forms as $Q(x,y)$, but they can also be defined as $Q(x,y,z) = \alpha x^2 + xy + \beta y^2 + \lambda z^2 : \alpha, \beta, \lambda \in F$. Quadratic forms defined over (x,y,z) such that the $\alpha x^2 + xy + \beta y^2$ portion is non-degenerative are known as conics, and can be thought of as a generalization of quadratic forms defined over a pair (x,y). We will denote this conic $F_{\alpha,\beta,\lambda}$, where each component of the subscript triple represents a coefficient.

3 Partial Difference Set Constructions

3.1 Maximal Arcs

Maximal arcs are geometric constructs within the projective plane. In general, an (m,k)-arc is a set of m points, no $k+1$ of which are collinear. For a given value of k, a maximal arc is an arc with the largest number m points possible.

Lemma 3.1 *The upper bound for m is defined as*

$$|A| = m \leq 1 + (n+1)(k-1)$$

Proof: Consider an arc A in a projective plane of order n, and a point $a \in A$. There are $n+1$ lines going through a, and at most $(k-1)$ other points $\in A$ on each of those lines. The upper bound follows, as $|A| = 1$, for the original point a, plus $(k-1)$ points on each of $(n+1)$ lines. □

A maximal arc meets this upper bound. Also, observe the following theorems.

Theorem 3.2 *Let A be a maximal arc in a projective plane P of order n, then $k|n$.*

Proof: Let A be a maximal arc in the projective plane P. Let $x \in P \backslash A$. There are $n+1$ lines through x. By the maximal arc bound result above, any line with x on it must have k points of A on it. Suppose that this not the case. Choose $x' \in A$. Consider the $n+1$ lines intersecting x'. Of these $n+1$ lines, there exists a line with strictly less than k points of A on it. Then

$$|A| = m < 1 + (n+1)(k-1)$$

which contradicts maximality. Thus, there are q lines with k points on A, and $(n+1-q)$ lines with zero points on A. Then

$$qk + (n+1-q) * 0 = 1 + (k+1)(n-1)$$

$$qk = nk + k - n$$
$$q = n + 1 - \frac{n}{k}$$

Since q is an integer, $\frac{n}{k}$ is an integer, and $k|n$. □

Theorem 3.3 *If $q = 2^t : t \in \mathbb{Z}$, and $k|q$, then there is an (m, k) maximal arc in the projective plane of order $q = 2^t : t \in \mathbb{Z}$.*

We will show this in the next section, by constructing such maximal arcs using Denniston's technique. [1]

Maximal arcs are equivalent to partial difference sets in elementary Abelian groups. Let A be a maximal arc in the a projective plane defined over the finite field F. Then $\cup_{n \in F^*}(n * A)$, all of the non-zero scalar multiples of the set, is a partial difference set in the projective plane.

3.2 Denniston Constructed Partial Difference Sets

Let P be a projective plane of order n, defined over a finite field F. Denniston constructed maximal arcs in P by utilizing a quadratic form, Q, and subgroup, K. The process is to set the quadratic form equal to each element of the subgroup, and calculate the solutions. The union of each of these solution sets results in a maximal arc, which can then be "lifted" by taking all of the non-zero scalar multiples in the F to produce a partial difference set.

Example 3.4 *In the projective plane of order 4 over F_4, the following construction yields a partial difference set:*

$$Q(x, y) = \alpha x^2 + xy + y^2$$
$$K = 0, 1$$

These elements produce the $(6, 2)$ maximal arc

$$(0, 0, 1), (0, 1, 1,), (\alpha, 0, 1), (\alpha, \alpha, 1), (\alpha^2, 1, 1), (\alpha^2, \alpha, 1)$$

The non-zero scalar multiples of this set produce a (64,18,2,6) partial difference set.

3.3 Mathon Constructed Partial Difference Sets

Mathon constructed partial difference sets in Galois fields of order 2^m by combining conics to create maximal arcs. Conics, just like any other type of element, can be grouped together to form a collection. Subsets of conics can form a closed collection under the operation $\oplus$, which is both associative and commutative, and is described as below:

- $F_{(\alpha,\beta,\lambda)} \oplus F_{(\alpha',\beta',\lambda')} = F_{(\alpha\oplus\alpha',\beta\oplus\beta',\lambda\oplus\lambda')}$
- $\alpha \oplus \alpha' = \frac{(\alpha\lambda+\alpha'\lambda')}{(\lambda+\lambda')}$

- $\beta \oplus \beta' = \frac{(\beta\lambda+\beta'\lambda)}{(\lambda+\lambda')}$
- $\lambda \oplus \lambda' = \lambda + \lambda'$

It turns out that a closed group of conics form a maximal arc, which can then be lifted to form a partial difference set. For example, consider the projective plane of order 8, defined over F_8.

Example 3.5 *Take the conics* $F_{(1,\alpha^3,\alpha^4)}, F_{(\alpha^5,1,\alpha^3)}, and F_{(\alpha^3,\alpha^2,\alpha^6)}$.
$F_{(1,\alpha^3,\alpha^4)} \oplus F_{(\alpha^5,1,\alpha^3)} = ...$

$\alpha \oplus \alpha' = \frac{(\alpha\lambda+\alpha'\lambda')}{(\lambda+\lambda)} = \frac{1\times\alpha^4+\alpha^5\times\alpha^3}{\alpha^4+\alpha^3} = \alpha^3$

$\beta \oplus \beta' = \frac{(\beta\lambda+\beta'\lambda')}{(\lambda+\lambda')} = \frac{\alpha^3\times\alpha^4+1\times\alpha^3}{\alpha^4+\alpha^3} = \alpha^2$

$\lambda \oplus \lambda' = \lambda + \lambda' = \alpha^4 + \alpha^3 = \alpha^6$

$... = F_{(\alpha^3,\alpha^2,\alpha^6)}$, *the third element in the set.*

It is easily verified by computing $F_{(1,\alpha^3,\alpha^4)} \oplus F_{(\alpha^3,\alpha^2,\alpha^6)}$ *and* $F_{(\alpha^5,1,\alpha^3)} \oplus F_{(\alpha^3,\alpha^2,\alpha^6)}$ *that this collection is indeed closed.*

Recall also that Denniston used quadratic forms defined over pairs (x, y), and that conics can be thought of as generalizations of these quadratic forms, where Q is defined over the triple (x, y, z). The parallel extends to Denniston and Mathon constructions of maximal arcs. A Denniston construction arises from a Mathon construction composed of three conics with the same values of α and β, but with different values of λ.

Example 3.6 *In the projective plane of order 8, the conics* $F_{(\alpha^2,\alpha^5,\alpha^5)}, F_{(\alpha^2,\alpha^5,\alpha)}, and F_{(\alpha^2,\alpha^5,\alpha^6)}$ *form a closed collection, and form a Denniston maximal arc.*

3.4 Davis-Xiang Constructed Partial Difference Sets

Both Mathon and Denniston give constructions of partial difference sets in the projective plane. As such, they reside in an algebraic setting of the form:

$$FiniteField \times FiniteField \times FiniteField$$

Partial difference sets that reside in this type of setting will be referred to as being "in GF^3". Davis and Xiang [2] give constructions for partial difference sets in an algebraic setting of the form:

$$GaloisRing \times GaloisField$$

Partial difference sets that reside in this type of setting will be referred to as being "in GR $\times$ GF". The Davis-Xiang constructions utilize polynomial equations.

Example 3.7 *The following expression produces a Davis-Xiang partial difference set in* $GR(4,2) \times F_4$*:*

$$\cup_{j=0}^{2}(h^i + h^{2i-j} + 2(h^{j+2} + h^{j+1}) + K_j) \cup_{i=0}^{2} g^i, \text{ where } K_j = \{0, 2h^j\}$$

The first construction we will consider in depth resides in $\mathrm{GR}(4,3) \times F_8$. This partial difference set is constructed with the following formula:

$$\cup_{j=0}^{6}(h^i + h^{2i-j} + 2h^j + K_j) \cup_{i=0}^{6} g^i \in \mathrm{GR}(4,3) \times F_8$$

where g is the generator of the multiplicative group of F_8, h is the corresponding element in GR(4,3), and K_j is a set of four elements in F_8 of the form $\{0, 2h^j, 2h^{j+1}, 2h^{j+3}\}$. The actual partial difference set generated by this expression can be found in Appendix A, Section 1. Notice the structure of the partial difference set. The equation produces pairs. The first union produces a set of 28 points, and creates elements that reside in the first component of the pair. The second union combines those 28 points with the 7 powers of the primitive element g, making the power of g the second component of each pair . The value of j in the second union, however, is also utilized in the first union, so as the powers of g increase, the 28 points produced by the first union change as well. The result is a partial difference set with 7 subsets of 28 points, where each subset has points with the same second coordinate. This structure plays a key role in our analysis of the Davis-Xiang construction later on.

4 Evaluation of Potential Partial Difference Sets

A note about implementation. As previously described, the process of taking a character sum is extremely involved and time consuming. For this reason, we implemented it using Java 2.0. In combination with the multiset method of evaluating a potential partial difference set, the z4xz2Analysis.java file provides a complete package for evaluating partial difference sets in projective planes of order 8 and lower. At the order 16 threshold, the calculations necessary to perform the multiset method of evaluating a partial difference set becomes computationally impractical, the machines we had at our disposal ran out of memory before the calculation could complete. Thus at this level, it is solely the above character theory method that is used to analyze a potential partial difference set. The implementation of both these processes, along with a toolbox of Java methods that are particularly useful in Java implementations throughout this work, can be found in Appendix A: "Partial Difference Set Evaluation".

5 The Problem

Recall that Davis and Xiang construct partial difference sets by using polynomial equations that result in PDSs residing in GR $\times$ GF format. These constructions exist in Galois fields of several different orders. Recall also that the Denniston approach constructs PDSs by setting quadratic forms equal to the elements in a subgroup. Since there exist subgroups

of several different sizes within a given Galois field, there are Denniston constructions of several different sizes within a Galois field of a given order. In GF(8) and GF(16), Davis and Xiang construct PDSs in GR $\times$ GF of the same size as Denniston constructions with subgroups of order 2 and 4, and of orders 2 and 8, in GF(8) and $GF(16)$ respectively. It turns out that out of possible Denniston constructions in $GF(32)$ with subgroups of sizes 2,4,8, and 16, Davis-Xiang constructions can be derived corresponding to sizes 2 and 16. In other words, there is a Davis-Xiang construction corresponding to Denniston constructions with subgroups of both the maximum and minimum values, but not for subgroups of intermediate size. This pattern continues in Galois fields of higher and higher order. Several questions follow. Do Davis-Xiang constructions exist for the intermediate sizes? If so, how could they be created? Is there a way to connect the algebraic work of Davis and Xiang to geometry, in order to provide insight that might generalize GR $\times$ GF PDSs? These questions we seek to provide insight into in this paper.

6 Attempt 1: Connecting Mathon to Davis-Xiang partial difference sets in GF(8)

Note: All Java and Mathematica implementations, outputs, and data sets pertaining to the above objective may be found in Appendix B: "Connecting Mathon to Davis-Xiang Partial Difference Sets".

In order to provide insight into the geometry of the Davis-Xiang constructions, we look first to the projective plane of order 8. The Davis-Xiang construction corresponding to the PDS produced by a Denniston construction with subgroup of order 4 was described in section 3.4. Recall that it consists of 7 subsets of 28 points, where each subset has a unique last coordinate shared by all points in that subset.

Now consider that a conic in GF(8) consists of nine points. A Mathon construction of the same size consists of three conics and a nucleus element. In general, given a projective plane P of order n, a conic contains $n+1$ points, so in the projective plane of order 8, a conic consists of 9 points. It follows that three conics, together with the "nucleus" element yields 28 points. Taking the non-zero scalar multiples of these elements yields a partial difference set of the exact same structure as the Davis-Xiang example. This suggests that the Davis-Xiang construction can be written in Mathon notation, which could lend geometric meaning to the algebra.

In order to find a Mathon construction yielding the exact same set as the Davis-Xiang construction, we attempt to find three conics residing in the Davis-Xiang PDS. The logical progression dictates that, along with a "nucleus" element, their scalar multiples would produce the rest of the PDS. The projective plane of order 8 is small enough to make an exhaustive search feasible. First we determine the quadratic forms describing every conic residing in the projective plane of order eight. Next we determine the points on each of those conics. With this information, it is possible to run a comparison between the points on each conic and the partial difference set, thus determining if there exist conics that lie completely within the PDS.

The following calculations are automated using a combination of Java 2.0 programs and

Mathematica notebooks. Determining the equations for every conic in the projective plane requires us to determine all of the pairs α and β such that $\alpha x^2+xy+\beta y^2$ is non-degenerative in the Galois field of order 8, F_8. Since a quadratic form is of degree less than or equal to 3, determining whether the polynomial is "irreducible" within the given field requires only that we evaluate the polynomial over every pair $(x, y) : x, y \in F_8$. A polynomial Q such that every pair produces a nonzero value is considered non-degenerative. A comprehensive list of all conics is produced by combining each pair (α, β) with all possible values of λ, namely every non-zero element of the Galois field. This entire process is automated using Mathematica 4.1.

We next determine the nine points that lay on each conic. This amounts to evaluating each conic equation over every possible triple $(x, y, z) : x, y, z \in F_8$. Algebra shows that assuming $z = 1$ produces the same set of points as would allowing z to be any other value in the Galois field. Thus we are able to search all points of the form $(x, y, 1)$.

Our goal is to compare the points on each conic with the points in the PDS. Recall, however that conics are geometric structures in the projective plane. As such, their points reside in GF^3. Our Davis-Xiang partial difference set is in GR $\times$ GF. This means that a mapping from GF^3 to GR $\times$ GF is needed in order to compare the partial difference set with the points on each conic. It should further be noted that since both PDSs reside in fields consisting of polynomials, a process of pulling off the coefficients from those polynomials is used to facilitate comparison, and allows us to produce several of our mappings.

Example 6.1 $(1, \alpha, 1 + \alpha^2) \rightarrow (100, 010, 101)$
$(2 + \beta, 3 + 2\beta^2, 1) \rightarrow (210, 302, 100)$

6.1 Mappings

Intuition directs the search for a mapping to the concept of the Teichmuller set. Recall that any Galois ring component can be written as two elements of the Teichmuller set, and that the Teichmuller set's behavior is similar to that of the corresponding Galois field. Since each Teichmuller element corresponds to a Galois field element, the following mapping follows. For a given pair in the Davis-Xiang PDS, the first component (the GR component) is replaced by an ordered pair. The idea is to determine which values $\xi_1, \xi_2 \in \tau$ would produce the desired element in the Galois ring. The Galois field elements corresponding to these Teichmuller values become the first and second components of the new mapped triple. The original second component of the Davis-Xiang point becomes the third component, yielding a mapping $M : (GR, GF) \rightarrow (GF, GF, GF)$

Example 6.2 $(1 + 2\alpha, 1) = 1 + 2(\alpha)$. *Thus the mapping* $(1 + 2\alpha, 1) \rightarrow (1, \alpha, 1)$ *follows.*

A logical progression from this straightforward mapping is to make ξ_2 the first component and ξ_1 the second component in the GF^3 mapped point.

Example 6.3 $(1 + 2\alpha, 1) = 1 + 2(\alpha)$, *so* $(1 + 2\alpha, 1) \rightarrow (\alpha, 1, 1)$ *would follow in this "psi-swapped" mapping.*

As previously mentioned, comparing the points on the conics with the points on the partial difference set is facilitated by pulling off the coefficients. This process offers another opportunity for a mapping. Instead of pulling the coefficients off in a straightforward manner, as previously described, we pull them off in reverse order. In other words, the component $\alpha + \alpha^2$ is represented by the coefficients $(1, 1, 0)$ rather than $(0, 1, 1)$.

Example 6.4 *Take the mapped triple* $(1, \alpha, 1)$*. Pulling off the coefficients previously resulted in the nine-tuple* $1, 0, 0, 0, 1, 0, 1, 0, 0$*. With this "order-swap" mapping, the mapped nine-tuple is* $0, 0, 1, 0, 1, 0, 0, 0, 1$*.*

In addition to the mappings modelled after the Teichmuller set concept, several mappings were derived which resulted from first pulling off the coefficients in the Davis-Xiang PDS.

1. (A, B, C, D, E, F) goes to (a, b, c, d, e, f, g, h, i)
   such that: A = a+2b, B = c+2d C = e+2f, D = g, E = h, F = i
2. (A, B, C, D, E, F) goes to (a, b, c, d, e, f, g, h, i)
   such that: A = a+2d, B = b+2e C = c+2f, D = g, E = h, F = i
3. (A, B, C, D, E, F) goes to (a, b, c, d, e, f, g, h, i)
   such that: A = e+2f, B = a+2b C = c+2d, D = g, E = h, F = i

Also tested were several variations of the above mappings, essentially every possible rotation of a, b, c, d, e, and f.

6.2 Conic Analysis of the Mapped PDSs

Now we apply each of the described mappings to the Davis-Xiang partial difference set, taking it to GF^3. The next step is to compare the previously generated conics with this mapped PDS. This comparison searches the mapped PDS for each point on each conic, and determines how many conics, if any, have all points residing in the partial difference set. Analysis of the "order swapped" Davis-Xiang PDS yields the only results of this test. It is found that the conic $Q(x, y, z) = \alpha^3 x^2 + xy + y^2 + \alpha^6 z^2$ resided completely within the Davis-Xiang partial difference set. There are also three conics with only one point missing from the PDS.

To gain more insight into this conic, we look to its character sums. We take the set containing the GF^3 points on the conic, plus the nucleus point, and take all of their scalar multiples in the Galois field. We then calculate the character sums over this set. This produces a partial difference set with two, nice character sums, as expected. We need to examine the points in the Galois ring, however, not in the Galois field. To do this, we take the original Davis-Xiang PDS points corresponding to those on the conic, along with the nucleus element, and take all of their Galois field scalar multiples. This set, it turns out, is not a partial difference set. The character sums are not well behaved, and we conclude that this will not lead us anywhere. Because the points on conics have a third coordinate of 1, they always reside in the first "set" of the Davis-Xiang partial difference set, which

has second coordinate 1. In reality, then, we are searching for conics whose points reside in this first set of 28 points in the PDS. With one conic found, then, the idea would be to find other sets of 9 points that behave in the same way as the conic, or have "well behaved" character sums. The "ill behaved" character sums of the conic leave us nothing with which to compare those sets of nine points. We reason, however, that perhaps there exist other sets of 9 points whose Galois field scalar multiples have similar character sums. We exhaust every possible combination of 9 points out of the remaining 18 points in the first "set" of the Davis-Xiang partial difference set, but find no other sets of nine points with that property.

No conics are found in any of the other Teichmuller-based partial difference set mappings. The results prove to be similar for the various alternative mappings, although several conics are found to be missing only one point. These "close" conics seem to hold potential, but there are too few of them to be of real interest. Thus our attempt to connect the geometry of Mathon to the algebra of Davis and Xiang in the projective plane of order 8 comes to a halt.

6.3 Attempt 2: Connecting Mathon to Davis-Xiang Partial Difference Sets in $GF(16)$

Note: All Java and Mathematica implementations, outputs, and data sets pertaining to the above objective may be found in Appendix C: "Connecting Mathon to Davis-Xiang Partial Difference Sets in $GF(16)$".

To provide a new perspective, we move closer to the actual partial difference set we want to examine, to the projective plane of order 16, where we analyze the Davis-Xiang construction of equal size to the set produced by a Denniston construction with subroup of order 8, again in an attempt to connect the geometry of Mathon to the algebra of Davis-Xiang. We first construct the partial difference set in $GR(4,4) \times GF(16)$, which results from the following polynomial expression:

$$\cup_{j=0}^{1} 4(h^i + h^{2i-j} + 2[h^i(1+\beta^3) + h^j\beta^3] + k_j) \cup_{i=0}^{14} g^i$$

where g is the generator of the multiplicative group of F_16, h is the corresponding element in $GR(4,4)$, and k_j is a set of 8 elements in $GR(4,4)$, of the form $0, 2h^j, 2h^{j+1}, 2h^{j+2}, 2h^{j+4}, 2h^{j+5}, 2h^{j+8}, 2h^{j+10}$. We reconstruct the process used for the projective plane of order 8, first calculating the irreducible conics and their points, then converting the PDS to GF^3 with our three Teichmuller mappings, and finally evaluating the conics versus the mapped versions of the PDS. This search is more successful. We find complete conics within the partial difference set in both the straightforward mapping and the psi-swap mapping. Though they are different conics, both correspond to the exact same set of points in the original partial difference set. With a conic obtained, there are plenty of searches and analyses that we would like to try. Unfortunately, in the Galois field of order 16, searches take too long and calculations become too large, making further analysis computationally infeasible.

6.4 Attempt 3: Utilizing Denniston to look at the PDS directly

Note: All Java and Mathematica implementations, outputs, and data sets pertaining to the above objective may be found in Appendix D: "Connecting Denniston to Davis-Xiang Partial Difference Sets".

Considering the limitations encountered in Attempt 2, we decide to take a more direct approach. We know a great deal about the structure of the partial difference set we are attempting to create. It should have 15 subsections(equal to the number of non-zero elements in the Galois field of order 16), and 52 points within each section, yielding 780 elements. This structure can be mimicked with a Denniston construction. We set the quadratic form $\alpha x^2 + xy + \beta y^2$ equal to the subgroup $(0, 1, \alpha, \alpha + 1)$ in GF(16). This forms a set of 52 elements. Evaluation of the character sums of this set reveals a set with nice, 4 character behavior in both the Galois field case, as would be expected from a Denniston construction, and in the Galois ring version. It is the existence of these nice character sums in the GR case that brings us to the hypothesis that the GR scalar multiples might lead us to a PDS in GRxGF of the correct size. We first verify that the Galois field scalar multiples do form a PDS, and then compute the GRxGF versions of those multiples. Unfortunately, the converted elements lack the same composure exhibited by the Galois field elements, and do not form a partial difference set. Let us then suppose the levels are simply interacting in an incorrect manner, so we switch up the way that the second components are arranged. Recall the levelled structure of a Davis-Xiang PDS. Each level has a common second coordinate: change the way those coordinates are assigned, and you change the nature of the character sums. Unfortunately, with 15 non-zero elements in GF(16), there are 15 factorial arrangements of powers, and that is far too many to exhaust, considering the complex computation that follows each arrangement. We first automate a process to use every rotation of the powers in ascending order. With no results there, we automate the process, to use a long series of swaps that result in essentially a random test, again, with no results.

To provide some insight into why the $GR \times GF$ version of the Denniston construction doesn't work out, we examine the structure of the 52 points in the above section. Davis and Xiang developed their construct that make up the first "set". Davis and Xiang produced their constructions by putting a Hadamard difference set together with subgroups of the Galois field, and then taking their scalar multiples . In this case, that would mean a Hadamard PDS of order 28, and 3 subgroups of order 8.by combining Hadamard difference sets with subgroups, and then taking their scalar multiples. In this case, such a set would consist of a Hadamard difference set of order 28, and three subgroups of order 8. We decide to see if it is possible to write the set of 52 GRxGF points in that structure. The difficulty here is finding subgroups of order eight. We do, however, manage to find two such subgroups, but fail to find a third, despite an exhaustive search. This could indeed be the reason that our set of 72 GR $\times$ GF points do not result in a partial difference set, due to lack of the correct structure in the first "set" of points.

7 Conclusion

It is significant that we find a conic residing completely within the two Davis-Xiang partial difference sets we test, both in the projective plane of order 8, and of order 16. This suggests that there is indeed some Geometric structure to Davis-Xiang partial difference sets. It is possible, of course, that there is a difference geometry that would provide the connection, or a different way of looking at the geometry that we have already. Regardless, the Davis-Xiang construction seems to have so much structure in common with both Mathon and Denniston constructions, that it seems highly likely that there is some connection lying beneath. Finding that connection is only a matter of computational power, geometric insight, and further work.

8 Appendix A: Evaluation of a Partial Difference Set

- In the Projective Plane of Order 8
  - pdsAnalysisGF8.java: Uses the character sum and multiset analysis methods to determine if a given set is a partial difference set
- In the Projective Plane of Order 16
  - pdsCharacterAnalysisGF16.java: Uses the character sum method to determine if a given set is a partial difference set
- Toolbox.java: Contains Java methods used frequently in the programs

9 Appendix B: Connecting Mathon to Davis-Xiang Partial Difference Sets in the Galois field of Order 8

- pointAnalysis.java: Searches for conics in a given partial difference set, outputs any complete conics found, those that are close, within 2 points, and all points and their connections with the partial difference set
- DavisXiangPDSGF8.nb: Generates the partial difference set created by the Davis-Xiang polynomial equation for the Galois field of order 8, corresponding to the Denniston construction in the Galois field of order 8 of subgroup size 4
- GRdiffSetGF8.txt: The partial difference set created by the Davis-Xiang polynomial equation for the Galois field of order 8, corresponds to the Denniston construction in the Galois field of order 8 of subgroup size 4
- irreducibleConicEquationsGF8.nb: Produces all triples (α, β, λ) that make the equation $\alpha x^2 + xy + \beta y^2$ irreducible in the Galois field of order 8
- allConicPointsGF8.nb: Generates all points on a conic in the Galois field of order 8
- allConicPointsGF8.txt: Contains all points on all conics in the Galois field of order 8
- coeffRotation1GF8.java: Using combinations of coefficients, maps elements from GR $\times$ GF to GF^3 in the Galois field of order 8
- coeffRotation1MappingGF8.txt: The set of points in GF^3 generated by the coefficient rotation in the Galois field of order 8
- coeffRotation1MappingGF8full.txt: The set of mapped points in GF^3 and the corresponding GR $\times$ GF points created by the coefficient rotation in the Galois field of order 8

- coeffRotation1ResultsGF8.txt: The results of the pointAnalysis.java program search for conics within the mapped difference set created by the coefficient rotation in the Galois field of order 8
- coeffRotation2GF8.java: Using combinations of coefficients, maps elements from GR $\times$ GF to GF^3 in the Galois field of order 8
- coeffRotation2MappingGF8.txt: The set of points in GF^3 generated by the coefficient rotation in the Galois field of order 8
- coeffRotation2MappingGF8full.txt: The set of mapped points in GF^3 and the corresponding GR $\times$ GF points created by the coefficient rotation in the Galois field of order 8
- coeffRotation2ResultsGF8.txt: The results of the pointAnalysis.java program search for conics within the mapped difference set created by the coefficient rotation in the Galois field of order 8
- coeffRotation3GF8.java: Using combinations of coefficients, maps elements from GR $\times$ GF to GF^3 in the Galois field of order 8
- coeffRotation3MappingGF8.txt: The set of points in GF^3 generated by the coefficient rotation in the Galois field of order 8
- coeffRotation3MappingGF8full.txt: The set of mapped points in GF^3 and the corresponding GR $\times$ GF points created by the coefficient rotation in the Galois field of order 8
- coeffRotation3ResultsGF8.txt: The results of the pointAnalysis.java program search for conics within the mapped difference set created by the coefficient rotation in the Galois field of order 8
- coeffRotation4GF8.java: Using combinations of coefficients, maps elements from GR $\times$ GF to GF^3 in the Galois field of order 8
- coeffRotation4MappingGF8.txt: The set of points in GF^3 generated by the coefficient rotation in the Galois field of order 8
- coeffRotation4MappingGF8full.txt: The set of mapped points in GF^3 and the corresponding GR $\times$ GF points created by the coefficient rotation in the Galois field of order 8
- coeffRotation4ResultsGF8.txt: The results of the pointAnalysis.java program search for conics within the mapped difference set created by the coefficient rotation in the Galois field of order 8
- orderSwapMapGF8.java: Switches the order of the coefficients of the Teichmuller mapping to map elements from GR $\times$ GF to GF^3 in the Galois field of order 8

- orderSwapMappingGF8.txt: The set of points in GF^3 generated by the order swap mapping in the Galois field of order 8
- orderSwapMappingGF8full.txt: The set of mapped points in GF^3 and the corresponding GR $\times$ GF points created by the order swap mapping in the Galois field of order 8
- orderSwapResultsGF8.txt: The results of the pointAnalysis.java program search for conics within the mapped difference set created by the order swap mapping in the Galois field of order 8
- psiSwapMapGF8.java: Switches the values of ξ_1 and xi_2 of the Teichmuller mapping to map elements from GR $\times$ GF to GF^3 in the Galois field of order 8
- psiSwapMappingGF8.txt: The set of points in GF^3 generated by the psi swap mapping in the Galois field of order 8
- psiSwapMappingGF8full.txt: The set of mapped points in GF^3 and the corresponding GR $\times$ GF points created by the psi swap mapping in the Galois field of order 8
- psiSwapResultsGF8.txt: The results of the pointAnalysis.java program search for conics within the mapped difference set created by the psi swap mapping in the Galois field of order 8
- teichmullerMapGF8.java: Reverses the Teichmuller construction to map elements from GR $\times$ GF to GF^3 in the Galois field of order 8
- teichmullerMappingGF8.txt: The set of points in GF^3 generated by the Teichmuller mapping in the Galois field of order 8
- teichmullerMappingGF8full.txt: The set of mapped points in GF^3 and the corresponding GR $\times$ GF points created by the Teichmuller mapping in the Galois field of order 8
- teichmullerResultsGF8.txt: The results of the pointAnalysis.java program search for conics within the mapped difference set created by the Teichmuller mapping in the Galois field of order 8

10 Appendix C: Connecting Mathon to Davis-Xiang Partial Difference Sets in the Galois field of Order 16

- GRdiffSetGF16.txt: The partial difference set created by the Davis-Xiang polynomial equation for the Galois field of order 16, corresponds to the Denniston construction in the Galois field of order 16 of subgroup size 8
- irreducibleConicEquationsGF16.nb: Produces all pairs (α, β, λ) that make the equation $\alpha x^2 + xy + \beta y^2$ irreducible in the Galois field of order 16

- allConicPointsGF16.nb: Generates all points on a conic in the Galois field of order 16
- allConicPointsGF16: Folder containing the text files of all points on all conics, divided into subgroups of one hundred for easier analysis
- orderSwapMapGF16.java: Switches the order of the coefficients of the Teichmuller mapping to map elements from GR $\times$ GF to GF^3 in the Galois field of order 16
- orderSwapMappingGF16.txt: The set of points in GF^3 generated by the order swap mapping in the Galois field of order 16
- orderSwapMappingGF16full.txt: The set of mapped points in GF^3 and the corresponding GR $\times$ GF points created by the order swap mapping in the Galois field of order 16
- orderSwapResultsGF16.txt: The results of the pointAnalysis.java program search for conics within the mapped difference set created by the order swap mapping in the Galois field of order 16
- psiSwapMapGF16.java: Switches the values of x1 and x2 of the Teichmuller mapping to map elements GR $\times$ GF to GF^3 in the Galois field of order 16
- psiSwapMappingGF16.txt: The set of points in GF^3 generated by the psi swap mapping in the Galois field of order 16
- psiSwapMappingGF16full.txt: The set of mapped points in GF^3 and the corresponding GR $\times$ GF points created by the psi swap mapping in the Galois field of order 16
- psiSwapResultsGF16.txt: The results of the pointAnalysis.java program search for conics within the mapped difference set created by the psi swap mapping in the Galois field of order 16
- teichmullerMapGF16.java: Reverses the Teichmuller construction to map elements from GR $\times$ GF to GF^3 in the Galois field of order 16
- teichmullerMappingGF16.txt: The set of points in GF^3 generated by the Teichmuller mapping in the Galois field of order 16
- teichmullerMappingGF16full.txt: The set of mapped points in GF^3 and the corresponding GR $\times$ GF points created by the Teichmuller mapping in the Galois field of order 16
- teichmullerResultsGF16.txt: The results of the pointAnalysis.java program search for conics within the mapped difference set created by the Teichmuller mapping in the Galois field of order 16

11 Appendix D: Connecting a Denniston Construction to the Davis-Xiang Partial Difference set in the Galois Field of order 16

- Searching for Subgroups of Order 8
  - subGroupsOfOrder8.java: Creates subgroups of order 8 in the Galois ring
  - subGroupsOfOrder8inGF.java: Creates subgroups of order 8 in the Galois field
  - subGroupsOfOrder8inGF2.java: Creates subgroups of order 8 in the Galois field using an alternate method
- Second Coordinate Variation
  - SecondCoordVariation.java: Creates all possible combinations of second coordinates and checks the set for nice character sums
  - SecondCoordVariationResults.txt: A sampling of the character sums produced by altering the second coordinate of the set
- Searching for Additional Conics
  - GR16pairs.java: Creates all possible combinations of 4 pairs and a self-invertible element from a set of 8 pairs and 2 self-invertible elements, and checks the set for nice character sums
  - GR16pairsPlusConic.java: Creates all possible combinations of 4 pairs and a self-invertible element from a set of 8 pairs and 2 self-invertible elements, adding in a specified conic, and checks the set for nice character sums
  - nonPairSubsets.java: Creates all possible combinations of 9 elements from an 18 element set, and checks the set for nice character sums
  - selfInvAndPairsGR16.txt: All self-invertible elements and all invertible pairs in the Galois ring of order 16
- Size K=4 Analysis
  - size4.txt: The partial difference set that corresponds to the Denniston construction using a subgroup of size 4 in the Galois field of order 16
  - size4GR.txt: The partial difference set that corresponds to the Denniston construction using a subgroup of size 4 in the Galois field of order 16 using the straight Teichmuller mapping
  - size4GRMult.txt: The partial difference set that corresponds to the Denniston construction using a subgroup of size 4 in the Galois field of order 16 and all of its scalar multiples converted to the Galois ring using the straight Teichmuller mapping

- size4GROrderSwapMult.txt: The partial difference set that corresponds to the Denniston construction using a subgroup of size 4 in the Galois field of order 16 and all of its scalar multiples converted to the Galois ring using the order swap mapping
- size4GRPsiSwapMult.txt: The partial difference set that corresponds to the Denniston construction using a subgroup of size 4 in the Galois field of order 16 and all of its scalar multiples converted to the Galois ring using the psi swap mapping
- size4MultiplesOrderSwap.nb: Generates the scalar multiples of the partial difference set that corresponds to the Denniston construction using a subgroup of size 4 in the Galois field of order 16 after conversion to the order-swap Galois ring mapping
- size4MultiplesPsiSwap.nb: Generates the scalar multiples of the partial difference set that corresponds to the Denniston construction using a subgroup of size 4 in the Galois field of order 16 after conversion to the psi-swap Galois ring mapping

- Results of K=4 Analysis
  * outputCharSumsForSize4GF.txt: The character sums produced from the size 4 set in the Galois field
  * outputCharSumsForSize4GR.txt: The character sums produced from the size 4 set in the Galois ring using the straight Teichmuller mapping
  * outputCharSumsForSize4OrderSwap.txt: The character sums produced from the size 4 set in the Galois ring using the order swap mapping
  * outputCharSumsForSize4PsiSwap.txt: The character sums produced from the size 4 set in the Galois ring using the psi swap mapping

References

[1] R. H. F. Denniston, Some maximal arcs in finite projective planes, *Journal of Combinatorial Theory*, **6** (1969), 317–319.

[2] Q. Xiang and J. A. Davis, A Family of Partial Difference Sets with Denniston Parameters in Nonelementary Abelian 2-Groups, submitted.

[3] Joseph A. Gallian, Contemporary Abstract Algebra, Fifth Edition, Houghton Mifflin Company, Boston, MA, 2002.