A Construction of Layered Relative Difference Sets Using Galois Rings

John B. Polhill*

Abstract

Using a similar framework to [7], we construct a family of relative difference sets in $P \times (Z_{p^{2r}})^{2t}$, where P is the forbidden subgroup. We only require that P be an abelian group of order p^t. The construction makes use of character theory and the structure of the Galois ring $GR(p^{2r}, t)$, and in particular the Teichmüller set for the Galois ring.

1 Introduction

Let G be a finite group of order v with a normal subgroup N of order n, and assume that $v = mn$. A subset D of cardinality k is called an (m, n, k, λ)-*relative difference set* (RDS) in G relative to N if the differences $d_1 d_2^{-1}$ for $d_1, d_2 \in D, d_1 \neq d_2$ represent each nonidentity element of $G \setminus N$ exactly λ times and each element of N zero times. For this reason, N is called the *forbidden subgroup*. If $G = H \times N$, where H is a subgroup of G, then D is called a *splitting RDS*. RDSs are said to be *semiregular* when $k - \lambda n = 0$. The RDSs constructed in this paper will be semiregular $(p^a, p^b, p^a, p^{(a-b)})$-RDSs, which have been studied extensively. The text authored by Pott [8] is a good reference for these RDSs.

Relative difference sets in abelian groups are generally studied with group algebras or character theory. We will frequently use the following lemma relating RDSs to character theory; see Turyn [9] for a proof of similar results.

Lemma 1.1 *Let G be an abelian group of order mn with a subgroup N of order n, and let D be a subset of G with cardinality k. Then D is an (m, n, k, λ)-relative difference set in G relative to N if and only if, for any character χ of G,*

$$|\chi(D)| = \begin{cases} k & \text{if } \chi \text{ is principal on } G, \\ \sqrt{k - \lambda n} & \text{if } \chi \text{ is nonprincipal on } G \text{ but principal on } N, \\ \sqrt{k} & \text{if } \chi \text{ is nonprincipal on } N. \end{cases}$$

We will construct relative difference sets in the groups $P \times (Z_{p^{2r}})^{2t}$, where P is the forbidden subgroup. It is significant that P may be any abelian group of order p^t, since the majority of previous constructions require that the forbidden subgroup be elementary abelian. Our construction works for all primes p, and all positive integers r and t. The parameters and

groups for the relative difference sets formed here overlap with some known constructions, most notably those of Leung and Ma in [5]. For $r = 1$, the constructions in the paper of Chen, Ray-Chaudhuri, and Xiang [2] have the same parameters. The paper of Hou and Sehgal [4] gives a different construction of RDSs in similar groups. However, the constructions in this paper differ in that we make explicit use of the structure of the Teichmüller set of Galois rings and primarily use the additive subgroups to form the relative difference sets. The other constructions make use of the multiplicative structure of the rings.

2 Galois Rings

If $\phi_1(x)$ is a primitive irreducible polynomial of degree t over F_p, then $F_p[x]/\langle\phi_1(x)\rangle$ is a finite field of order p^t. Hensel's lemma states that there is a unique primitive irreducible polynomial $\phi_r(x)$ over Z_{p^r} so that $\phi_r(x) \equiv \phi_1(x) \bmod p$ and with a root ω of $\phi_r(x)$ satisfying $\omega^{p^t-1} = 1$. Then $Z_{p^r}[\omega]$ is the *Galois extension of Z_{p^r} of degree t*, and furthermore $Z_{p^r}[\omega]$ is called a Galois ring denoted $GR(p^r, t)$. Clearly the additive group of $GR(p^r, t)$ is isomorphic to $(Z_{p^r})^t$. See [1] or [6] for a detailed description of Galois rings.

An important subset of $GR(p^r, t)$ is the Teichmüller set $\mathcal{T} = \{0, 1, \omega, \omega^2, ..., \omega^{p^t-2}\}$, which can be viewed as the set of all solutions to the polynomial $x^{p^t} - x$ over $GR(p^r, t)$. A canonical way of uniquely expressing an element of $GR(p^r, t)$ is:

$$\alpha = \alpha_0 + p\alpha_1 + p^2\alpha_2 + ... + p^{r-1}\alpha_{r-1},$$

where $\alpha_i \in \mathcal{T}$. We see that the invertible elements are those with $\alpha_0 \neq 0$, and if we take the natural projection (modulo p reduction) from $GR(p^r, t)$ to $GF(p^t)$, then $\mathcal{T}$ maps onto $GF(p^t)$; this projection is given by $\pi(\alpha) = \alpha_0 \bmod p$ in the representation above.

Using the Teichmüller representation, we can completely describe the additive characters of the Galois ring $GR(p^r, t)$. Let the Frobenius map f from $GR(p^r, t)$ to $GR(p^r, t)$ be given by:

$$f : \alpha = (\alpha_0 + p\alpha_1 + \cdots + p^{r-1}\alpha_{r-1}) \to {\alpha_0}^p + p{\alpha_1}^p + \cdots + p^{r-1}{\alpha_{r-1}}^p,$$

for $\alpha_i \in \mathcal{T}$. Define the additive trace from $GR(p^r, t)$ to $GR(p^r, 1) = Z_{p^r}$ by:

$$Tr(\alpha) = \alpha + \alpha^f + \cdots + \alpha^{f^{t-1}}.$$

Then we have:

Lemma 2.1 *The additive characters of $GR(p^r,t)$ can be described by:*

$$\chi_a(x) = \xi_{p^r}{}^{Tr(ax)}, \quad a \in GR(p^r,t)$$

where ξ_{p^r} is a primitive $(p^r)^{th}$ root of unity.

See [10] for the proof of a similar result. By *order* of a character, $\chi : G \to C^*$, on a finite abelian group G, one means the smallest integer n so that $(\chi(g))^n = 1$ for all $g \in G$. Notice that all nonprincipal characters on $GR(p^r,t)$ will be of order p^i for $0 < i \leq r$. In fact, the order of χ_a is p^{r-j} where j is the smallest index with a_j nonzero in the Teichmüller expansion of a.

3 Forming a "Spread" of $GR(p^r,t) \times GR(p^r,t)$

A framework for analyzing the structure of $GR(p^r,t) \times GR(p^r,t)$ was developed in [7]. We include the details here without proof.

A *spread* of a $2s-$dimensional vector space, V, over F_p is a set of p^s+1 s-dimensional subspaces of V which have pairwise intersection $\{0\}$ and necessarily partition the 1-dimensional subspaces of V. Regarding V^4, the vector space associated with $\Sigma_3 = PG(3,p)$, as the product $GF(p^2) \times GF(p^2)$ a spread was given by Chen [3] as:

$$L_i = \{(\alpha, i\alpha) | \alpha \in GF(p^2)\} \text{ for } i \in GF(p^2),$$

$$L_\infty = \{(0,\alpha) | \alpha \in GF(p^2)\}.$$

Now let $R = GR(p^r,t)$. In this section, we identify a set of $R-$modules that will completely partition the non-nilpotent elements of $R \times R$, and which will be analogous to a spread. Let $\mathcal{T}$ be the Teichmüller set: $\mathcal{T} = \{0,1,\omega,...,\omega^{p^t-2}\}$ for ω a primitive root of the primitive irreducible polynomial $\phi_r(x)$ of degree t as in the previous section.

We define the subgroups in our spread analog by the following:

$$S_{i_r,i_{r-1},...,i_2,i_1} = \{\alpha, (i_1 + pi_2 + p^2 i_3 + ... + p^{r-2} i_{r-1} + p^{r-1} i_r)\alpha) | \alpha \in R\},$$

$$S_{i_r,i_{r-1},...,i_2,\infty} = \{((pi_2 + p^2 i_3 + ... + p^{r-2} i_{r-1} + p^{r-1} i_r)\alpha, \alpha) | \alpha \in R\}.$$

In the above, the subscripts $i_j \in \mathcal{T}$. Define an $l-$*array* to be a collection of subgroups $\{S_{i_r,...,i_{l+1},x_l,...,x_1}\}$ for which the i_j are fixed elements in $\mathcal{T}$, and the x_j are allowed to range over all possible values; that is, $x_1 \in \mathcal{T} \cup \infty$ and $x_i \in \mathcal{T}, i > 1$.

We will show that the entire collection, an $r-$array, of subgroups completely partitions the non-nilpotent elements of $R \times R$. It is easy to show

that these subgroups are in fact R-modules. The following lemma describes the intersection properties of the subgroups $S_{i_r,i_{r-1},\ldots,i_2,i_1}$.

Lemma 3.1 *$S_{a_r,\ldots,a_1} \cap S_{b_r,\ldots,b_1} = \{0\}$ for $a_1 \neq b_1$. $S_{a_r,\ldots,a_{j+1},a_j,\ldots,a_1} \cap S_{b_r,\ldots,b_{j+1},a_j,\ldots,a_1} = S_{0,\ldots,0,a_j,\ldots,a_1} \cap p^{r-j}G$ for $a_{j+1} \neq b_{j+1}$.*

So we see that the $S_{i_r,\ldots,i_1}$ are pairwise disjoint in the non-nilpotent elements of $R \times R$, which are the elements not of the form $p(r_1, r_2)$ for $r_1, r_2 \in R$. We have such a subgroup $S_{i_r,\ldots,i_1}$ for each r-tuple $(i_r, \ldots, i_1)$ where $i_j \in \mathcal{T}$ for $j > 1$ and $i_1 \in \mathcal{T} \cup \infty$. So there are $(p^t)^{r-1}(p^t+1)$ distinct subgroups, pairwise disjoint in the non-nilpotent elements. This gives us $(p^{rt}-p^{(r-1)t})[(p^t)^{r-1}(p^t+1)] = (p^{2rt}-p^{2(r-1)t})$ such elements, which is the total number of non-nilpotent elements in $R \times R$. So we have partitioned the elements of G which are not divisible by p. We can put these subgroups into an $r-$dimensional array. Within this framework we will construct the new family of RDSs in the additive group of $R \times R$.

4 Constructions of Relative Difference Sets

In this section, we construct a family of relative difference sets in $P \times (Z_{p^{2r}})^{2t}$, where P is the forbidden subgroup. Recall that P may be any abelian group of order p^t, and the construction works for any prime p and all positive integers r and t. Now we have $R = GR(p^{2r}, t)$. Recall an *l-array* is a collection of R-modules $\{S_{i_{2r},\ldots,i_{l+1},x_l,\ldots,x_1}\}$ for which the i_j are fixed elements in the Teichmüller set $\mathcal{T}$, and the x_i are allowed to vary over all possible values.

We now consider character sums on our collection of R-modules. All additive characters on $R \times R$ are of order p^i for i an integer with $0 \leq i \leq 2r$. Let G be the additive group of $R \times R$. If χ is of order p^i on G, then χ will be of order p^j when restricted to S where $j \leq i$. The following lemma describes the orders of the restrictions of characters on our collection of R-modules. The proof of a similar result may be found in [7].

Lemma 4.1 *Let $p^lS = S \cap p^lG$. If χ is a nonprincipal additive character of order p^k on the ring $R \times R$, then χ will be order p^{k-l} on p^lG if $k > l$ and principal on p^lG if $k \leq l$. For the case when $k > l$, if we consider a $(k-l)$-array, then χ is principal on exactly one subgroup, $p^lS_{i_{2r},\ldots,i_{k-l+1},j'_{k-l},j_{k-l-1}\ldots,j_1}$, of order p for all subgroups of the form $p^lS_{i_{2r},\ldots,i_{k-l+1},j_{k-l},j_{k-l-1}\ldots,j_1}$ for $j_{k-l} \neq j'_{k-l}$, and of order p^i with $i > 1$ for all other subgroups in the $(k-l)$-array.*

Before constructing our relative difference sets we state the following lemma describing character sums on the layers of elements in each subgroup S in our construction. This will be used frequently since we will construct our relative difference sets in layers of such elements. We say x is *strictly divisible* by p^s if $p^s|x$ and $p^{s+1} \not| x$. See [7] for the proof of a similar result.

Lemma 4.2 *Let $p^lS = S \cap p^lG$ for $2 \leq l \leq 2r$ for $S = S_{x_{2r},\ldots,x_1}$. Then let p^lS^* denote the elements of p^lS strictly divisible by p^l, so $p^lS = p^lS^* \cup p^{l+1}S$. If χ is a character on p^lS, then:*

$$\chi(p^lS^*) = \begin{cases} p^{(2r-l)t} - p^{(2r-l-1)t} & \text{if } \chi \text{ is principal on } p^lS, \\ -p^{(2r-l-1)t} & \text{if } \chi \text{ is of order } p \text{ on } p^lS, \\ 0 & \text{if } \chi \text{ is of order } p^s \text{ on } p^lS, s > 1. \end{cases}$$

Before we look at the general construction, we consider a specific example to serve as a guideline. Let $G = Z_3 \times Z_{81} \times Z_{81}$, where Z_3 is the forbidden subgroup.

Let $M = Z_{81} \times Z_{81}$, and let $I = 9M$ be the set of all elements of M that are divisible by 9. We form the RDSs in 2 stages/layers that we call stage 0 and stage 1. Stage 0 will involve the layer of nonnilpotent elements of M and stage 1 those from $3M \setminus I$, those elements strictly divisible by 3.

Stage 0:

In stage 0, we partition the nonnilpotent elements of M into $|Z_3| = 3$ sets, which we call $A_{0,i}$. We will use these sets later to form our relative difference sets, including in our construction those elements of the form $(i, A_{0,i})$. Define the sets as follows:

$$A_{0,0} = (< (1,0) > \cup < (1,1) > \cup < (1,2) > \cup < (1,3) > \cup \ldots \cup < (1,26) >$$

$$\cup < (0,1) > \cup < (3,1) > \cup \ldots \cup < (24,1) >) \cap M \setminus 3M =$$

$$(S_{0,0,0,0} \cup S_{0,0,0,1} \cup S_{0,0,0,2} \cup S_{0,0,1,0} \cup \ldots \cup S_{0,2,2,2} \cup S_{0,0,0,\infty}$$

$$\cup S_{0,0,1,\infty} \cup \ldots \cup S_{0,2,2,\infty}) \cap M \setminus 3M.$$

Notice that these are all the subgroups of the form $S_{0,i,j,k}$ where i, j, k are allowed to vary over all possible values. Then let

$$A_{0,1} = (< (1,27) > \cup < (1,28) > \cup < (1,29) > \cup < (1,30) > \cup \ldots \cup$$

$$< (1,53) > \cup < (27,1) > \cup < (30,1) > \cup \ldots \cup < (51,1) >) \cap M \setminus 3M =$$

$$(S_{1,0,0,0} \cup S_{1,0,0,1} \cup S_{1,0,0,2} \cup S_{1,0,1,0} \cup \ldots \cup S_{1,2,2,2} \cup S_{1,0,0,\infty}$$

$$\cup S_{1,0,1,\infty} \cup \ldots \cup S_{1,2,2,\infty}) \cap M \setminus 3M.$$

These are all subgroups of the form $S_{1,i,j,k}$ where i, j, k are allowed to vary over all possible values. Finally, let

$$A_{0,2} = (< (1,54) > \cup < (1,55) > \cup < (1,56) > \cup < (1,57) > \cup ... \cup$$

$$< (1,80) > \cup < (54,1) > \cup < (57,1) > \cup ... \cup < (78,1) >) \cap M \setminus 3M =$$

$$(S_{2,0,0,0} \cup S_{2,0,0,1} \cup S_{2,0,0,2} \cup S_{2,0,1,0} \cup ... \cup S_{2,2,2,2} \cup S_{2,0,0,\infty} \cup$$

$$S_{2,0,1,\infty} \cup ... \cup S_{2,2,2,\infty}) \cap M \setminus 3M.$$

These are the subgroups of the form $S_{2,i,j,k}$ where i, j, k are allowed to vary over all possible values.

Stage 1: In stage 1, we partition those elements in $3M \setminus I$ into 3 sets $A_{1,i}$. Again we will include those elements $(i, A_{1,i})$ from G in the construction of our RDS. Observe that each element in $3M \setminus I$ is contained in exactly one of the following set of subgroups:

$$\{< (1,0) >, < (1,1) >, < (1,2) >, < (1,3) >, ..., < (1,26) >, < (0,1) >,$$

$$< (3,1) >, ..., < (24,1) >\} =$$

$$\{S_{0,0,0,0}, S_{0,0,0,1}, S_{0,0,0,2}, S_{0,0,1,0}, ..., S_{0,2,2,2}, S_{0,0,0,\infty}, S_{0,0,1,\infty}, ..., S_{0,2,2,\infty}\}.$$

Again we will have exactly three sets in our partition of these elements. The 3 sets are respectively as follows: $A_{1,0}$ involves the set of all subgroups of the form $S_{0,i,0,j}$, $A_{1,1}$ involves the set of all subgroups of the form $S_{0,i,1,j}$, and $A_{1,2}$ involves the set of all subgroups of the form $S_{0,i,2,j}$ where i, j are allowed to vary over all allowed values.

$$A_{1,0} = (< (1,0) > \cup < (1,1) > \cup < (1,2) > \cup < (1,9) > \cup < (1,10) > \cup$$

$$< (1,11) > \cup < (1,18) > \cup < (1,19) > \cup < (1,20) > \cup < (0,1) >$$

$$\cup < (9,1) > \cup < (18,1) >) \cap 3M \setminus I =$$

$$S_{0,0,0,0} \cup S_{0,0,0,1} \cup S_{0,0,0,2} \cup S_{0,1,0,0} \cup S_{0,1,0,1} \cup S_{0,1,0,2} \cup S_{0,2,0,0} \cup S_{0,2,0,1} \cup$$

$$S_{0,2,0,2} \cup S_{0,0,0,\infty} \cup S_{0,1,0,\infty} \cup S_{0,2,0,\infty}) \cap 3M \setminus I.$$

$$A_{1,1} = (< (1,3) > \cup < (1,4) > \cup < (1,5) > \cup < (1,12) > \cup < (1,13) > \cup$$

$$< (1,14) > \cup < (1,21) > \cup < (1,22) > \cup < (1,23) > \cup < (3,1) > \cup$$

$$< (12,1) > \cup < (15,1) >) \cap 3M \setminus I =$$

$$(S_{0,0,1,0} \cup S_{0,0,1,1} \cup S_{0,0,1,2} \cup S_{0,1,1,0} \cup S_{0,1,1,1} \cup S_{0,1,1,2} \cup S_{0,2,1,0} \cup$$

$$S_{0,2,1,1} \cup S_{0,2,1,2} \cup S_{0,0,1,\infty} \cup S_{0,1,1,\infty} \cup S_{0,2,1,\infty}) \cap 3M \setminus I.$$

$$A_{1,2} = (< (1,6) > \cup < (1,7) > \cup < (1,8) > \cup < (1,15) > \cup < (1,16) > \cup$$

$$< (1,17) > \cup < (1,24) > \cup < (1,25) > \cup < (1,26) > \cup < (6,1) > \cup$$

$$< (15,1) > \cup < (24,1) >) \cap 3M \setminus I =$$

$$(S_{0,0,2,0} \cup S_{0,0,2,1} \cup S_{0,0,2,2} \cup S_{0,1,2,0} \cup S_{0,1,2,1} \cup S_{0,1,2,2} \cup S_{0,2,2,0} \cup$$

$$S_{0,2,2,1} \cup S_{0,2,2,2} \cup S_{0,0,2,\infty} \cup S_{0,1,2,\infty} \cup S_{0,2,2,\infty}) \cap 3M \setminus I.$$

So in the sets $A_{0,i}$ we only take elements of $M \setminus 3M$ and in the sets $A_{1,i}$ we take only elements of $3M \setminus 9M$. Then the RDS in the group $G = Z_3 \times Z_{81} \times Z_{81}$ is

$$D = (0, A_{0,0}) \cup (1, A_{0,1}) \cup (2, A_{0,2}) \cup (0, A_{1,0}) \cup (1, A_{1,1}) \cup (2, A_{1,2}) \cup (0, I).$$

We will use character sums via Lemma 1.1 in order to show that this set is a $(3^8, 3, 3^8, 3^7)$-relative difference set. We outline the idea of the proof for our example here and leave the rigorous proof for the theorem below. Let ϕ be a character on $G = Z_3 \times Z_{81} \times Z_{81}$, then $\phi = \lambda \otimes \chi$, where λ is a character on Z_3 and χ is a character on $Z_{81} \times Z_{81}$.

Case 1: Suppose ϕ is the principal character on $Z_3 \times Z_{81} \times Z_{81}$. Then $\phi(D) = |D| = 3^8$.

Case 2: If λ is principal on Z_3 but nonprincipal on G, then notice that D contains exactly one element (a, i, j) for every (i, j) in $Z_{81} \times Z_{81}$. Therefore $\phi(D) = \chi(Z_{81} \times Z_{81}) = 0$.

Case 3: Suppose λ is nonprincipal on Z_3. Now we have 3 subcases, whether χ be order 9 or lower, order 27, or order 81.

Case 3a: If χ is order 9 or less, it will be the case that $\chi(A_{i,j}) = \chi(A_{k,j})$ for all i, j, k, so let $\chi(A_{0,j}) = s$ and let $\chi(A_{1,j}) = t$. Notice that χ will be principal on I. Then

$$\phi(D) = \phi(0, A_{0,0}) + \phi(1, A_{0,1}) + \phi(2, A_{0,2}) + \phi(0, A_{1,0}) + \phi(1, A_{1,1}) +$$

$$\phi(2, A_{1,2}) + \phi(0, I) =$$

$$s(\lambda(0) + \lambda(1) + \lambda(2)) + t(\lambda(0) + \lambda(1) + \lambda(2)) + \lambda(0)|I| = 0 + 0 + 3^4 = 81.$$

Case 3b: If χ is order 27, then clearly $\chi(I) = 0$. It is the case that $\chi(A_{0,i}) = 0$ (shown in the proof below), and also that $\chi(A_{1,j}) = 54$ for one j while $\chi(A_{1,k}) = -27$ for all $k \neq j$. So we have:

$$\phi(D) = \phi(0, A_{0,0}) + \phi(1, A_{0,1}) + \phi(2, A_{0,2}) + \phi(0, A_{1,0}) + \phi(1, A_{1,1}) +$$

$$\phi(2, A_{1,2}) + \phi(0, I) = 0 + 0 + 0 + 54\lambda(x_0) - 27\lambda(x_1) - 27\lambda(x_2) + 0 =$$

$$81\lambda(x_0) - 27(\lambda(x_0) + \lambda(x_1) + \lambda(x_2)) = 81\lambda(x_0)$$

where $Z_3 = \{x_0, x_1, x_2\}$. So $\phi(D) = 81\lambda(x_0)$ (notice that x_0 could be any of the elements of Z_3), and $|\phi(D)| = 81$.

Case 3c: If χ is order 81, then clearly $\chi(I) = 0$. It is the case that $\chi(A_{1,i}) = 0$ (shown in the proof below), and also that $\chi(A_{0,j}) = 54$ for one j while $\chi(A_{0,k}) = -27$ for all $k \neq j$. So we have:

$$\phi(D) = \phi(0, A_{0,0}) + \phi(1, A_{0,1}) + \phi(2, A_{0,2}) + \phi(0, A_{1,0}) + \phi(1, A_{1,1}) +$$

$$\phi(2, A_{1,2}) + \phi(0, I) = 54\lambda(x_0) - 27\lambda(x_1) - 27\lambda(x_2) + 0 + 0 + 0 + 0 =$$

$$81\lambda(x_0) - 27(\lambda(x_0) + \lambda(x_1) + \lambda(x_2)) = 81\lambda(x_0),$$

where $Z_3 = \{x_0, x_1, x_2\}$. So $\phi(D) = 81\lambda(x_0)$, and again $|\phi(D)| = 81$.

We call these RDSs in $P \times M = P \times (Z_{p^{2r}})^{2t}$ layered because they are constructed in r stages, taking the elements in $M \setminus pM$ in the first stage, $pM \setminus p^2M$ in the second, and so on up to stage r where we use the elements of $p^{r-1}M \setminus p^rM$. The elements of p^rM are taken together as a whole.

General Construction: We construct RDSs in the groups $P \times (Z_{p^{2r}})^{2t} = P \times M$, where $P = \{x_0, x_1, x_2, ...x_{p^t-1}\}$ is any abelian group of order p^t and is also the forbidden subgroup. We use the spread $S_{y_{2r}, y_{2r-1}, ..., y_2, y_1}$ of the ring $GR(p^{2r}, t) \times GR(p^{2r}, t)$ from the previous section. Notice that M is the additive group of that particular ring. Then our relative difference set is given by:

$$D = (\bigcup_{i=0}^{r-1} \bigcup_{j=0}^{p^t-1} (x_j, A_{i,j})) \bigcup (x_0, I)$$

where the sets $A_{i,j}$ are given by:

$$A_{0,j} = \bigcup_{y_{2r-1}, y_{2r-2}, ..., y_1} S_{a_j, y_{2r-1}, y_{2r-2}, ..., y_1} \cap (M \setminus pM)$$

$$A_{i,j} = \bigcup_{y_{2r-i}, ..., y_{2r-2i+1}, y_{2r-2i-1}, ..., y_1} (S_{0,0,...,0, y_{2r-i}, ..., y_{2r-2i+1}, a_j, y_{2r-2i-1}, ..., y_1})$$

$$\cap (p^iM \setminus p^{i+1}M), \quad i \in \{1, 2, ..., r-1\},$$

where the a_j are fixed elements in the Teichmüller set $\mathcal{T}$ and the y_l are allowed to vary over all possible values, so $y_l \in \mathcal{T}$ for $l \neq 1$ and $y_1 \in \mathcal{T} \cup \infty$.

Before proving the main theorem, we need a lemma that describes the behavior of characters on the sets $A_{i,j}$.

Lemma 4.3 *Let χ be a character on $M = (Z_{p^{2r}})^{2t}$. Then χ is order p^k for some integer k with $0 \leq k \leq 2r$. If $k \neq 2r-l$, then $\chi(A_{l,i}) = \chi(A_{l,j})\ \forall i, j$. If $k = 2r-l$ then $\chi(A_{l,j'}) = p^{2rt} - p^{(2r-1)t}$ for some j' and $\chi(A_{l,j}) = -p^{(2r-1)t}$ for all $j \neq j'$.*

Proof: The fact that χ is order p^k for $0 \leq k \leq 2r$ follows from Lemma 2.1. The case that $l = 0$ is similar to the case $l \neq 0$, so we leave the case that $l = 0$ to the reader. We break our proof into 4 cases.

Case 1 Suppose that $k \leq l$. Then since $A_{l,j} \subset p^l M - p^{l+1}M$, χ is trivial on all $A_{l,j}$, $\chi(A_{l,j}) = |A_{l,j}|$, and the result follows.

Case 2: Suppose that $l < k < 2r - l$. Then since $A_{l,j} \subset p^l M - p^{l+1}M$, then χ has order p^{k-l} on $A_{l,j}$. Applying Lemma 4.1 to $p^l M$, we find that on every $(k-l)$-array there will be exactly one subgroup $S_{0,0,\ldots,0,y_{2r-l},\ldots,y_{2r-2l+1},a_j,y_{2r-l-1},\ldots,y_{k-2l+1},\alpha_{k-l},y_{k-l-1},\ldots,y_1}$ on which χ is principal and for all subgroups $S_{0,0,\ldots,0,y_{2r-l},\ldots,y_{2r-2l+1},a_j,y_{2r-2l-1},\ldots,y_{k-l+1},\beta_{k-l},y_{k-l-1},\ldots,y_1}$ with $\beta_{k-l} \neq \alpha_{k-l}$, χ will be order p. χ will have order p^s for $s > 1$ on all other subgroups in the $(k-l)$-array. This fact does not depend on the choice of a_j, so the character values on each of the $A_{l,j}$ will be the same.

Case 3: Suppose that $k = 2r-l$. Since $A_{l,j} \subset p^l M - p^{l+1}M$, then χ has order p^{2r-2l} on $A_{l,j}$. Applying Lemma 4.1 to $p^l M$, we find that on every $(k-l)$-array there will be exactly one subgroup $S_{0,0,\ldots,0,y_{2r-l},\ldots,y_{2r-2l+1},a_{2r-2l},a_{2r-2l-1},\ldots,a_1}$ on which χ is principal and for all other $S_{0,0,\ldots,0,y_{2r-l},\ldots,y_{2r-2l+1},b_{2r-2l},a_{2r-l-1},\ldots,a_1}$ (all a_i are fixed elements), χ will be order p. On all other subgroups in the array, χ will be order p^s for $s > 1$. Let $A_{l,j'} = \bigcup_{y_{2r-l},\ldots,y_{2r-2l+1},y_{2r-2l-1},\ldots,y_1} S_{0,0,\ldots,0,y_{2r-l},\ldots,y_{2r-2l+1},a_{2r-2l},y_{2r-2l-1},\ldots,y_1} \cap (p^i M \setminus p^{i+1}M)$ and $A_{l,j} = \bigcup_{y_{2r-l},\ldots,y_{2r-2l+1},y_{2r-2l-1},\ldots,y_1} S_{0,0,\ldots,0,y_{2r-l},\ldots,y_{2r-2l+1},b_{2r-2l},y_{2r-2l-1},\ldots,y_1} \cap (p^i M \setminus p^{i+1}M)$ be an arbitrary set $A_{l,j}$ other then $A_{l,j'}$. Lemma 4.2 ensures that we only have to consider the subgroups on which χ is principal or order p to compute $\chi(A_{l,j})$. The character values for χ on such subgroups will be $p^{(2r-l)t} - p^{(2r-l-1)t}$ and $-p^{(2r-l-1)t}$ respectively. Notice that we will have such subgroups for every choice $(x_{2r-l},\ldots,x_{2r-2l+1})$ that we use for $(y_{2r-l},\ldots,y_{2r-2l+1})$ in the subgroups of the sets $A_{l,j'}$ and $A_{l,j}$. There are p^t choices for each y_i in the l-tuple, and hence $(p^t)^l$ subgroups in our calculation. So we get that

$$\chi(A_{l,j'}) = \sum_{y_{2r-l},\ldots,y_{2r-2l+1}} \chi(S_{0,0,\ldots,0,y_{2r-l},\ldots,y_{2r-2l+1},a_{2r-2l},a_{2r-2l-1},\ldots,a_1}) =$$

$$(p^t)^l(p^{(2r-l)t} - p^{(2r-l-1)t}) = p^{2rt} - p^{(2r-1)t}$$

$$\chi(A_{l,j}) = \sum_{y_{2r-l},\ldots,y_{2r-2l+1}} \chi(S_{0,0,\ldots,0,y_{2r-l},\ldots,y_{2r-2l+1},b_{2r-2l},a_{2r-2l-1},\ldots,a_1}) =$$

$$(p^t)^l(-p^{(2r-l-1)t}) = -p^{(2r-1)t} \; \forall j \neq j'.$$

Case 4: Suppose that $k > 2r - l$. Since $A_{l,j} \subset p^l M - p^{l+1}M$, then χ has order p^{k-l} on $A_{l,j}$. Applying Lemma 4.1 to $p^l M$, we find that on every $(k-l)$-array there will be exactly one subgroup $S_{0,0,\ldots,0,y_{2r-l},\ldots,y_{k-l+1},a_{k-l},}$

$a_{k-l-1},\ldots,a_{2r-2l+1},a_{2r-2l},a_{2r-2l-1},\ldots,a_1$ on which χ is principal and for all other $S_{0,0,\ldots,0,y_{2r-l},\ldots,y_{k-l+1}b_{k-l},a_{k-l-1},\ldots,a_{2r-2l+1},a_{2r-2l},a_{2r-2l-1},\ldots,a_1}$ (all a_i are fixed elements), χ will be order p. All of these subgroups are contained in exactly one of the $A_{l,j'}$, so that

$$\chi(A_{l,j'}) = \sum_{y_{2r-l},\ldots,y_{k-l+1}} \chi(S_{0,0,\ldots,0,y_{2r-l},\ldots,y_{k-l+1},y_{k-l},a_{k-l-1},\ldots,a_{2r-2l+1},a_{2r-2l},a_{2r-2l-1},\ldots,a_1})$$

$$= (p^t)^{2r-k}[(p^{(2r-l)t} - p^{(2r-l-1)t}) - (p^t - 1)p^{(2r-l-1)t})] = 0.$$

Also $\chi(A_{l,j}) = 0\ \forall j \neq j'$, since χ will have order greater than p on all the subgroups used to form $A_{l,j}$.

□

Theorem 4.1 *The set D is a $(p^{4rt}, p^t, p^{4rt}, p^{4rt-t})$-RDS in the group $G = P \times (Z_{p^{2r}})^{2t}$, where P is the forbidden subgroup. $P = \{x_0, x_1, x_2, \ldots x_{p^t-1}\}$ is an arbitrary abelian group of order p^t.*

Proof: Let $\phi = \lambda \otimes \chi$ be an arbitrary character on $G = P \times (Z_{p^{2r}})^{2t}$, where λ is a character on P and χ is a character on $(Z_{p^{2r}})^{2t}$. We separate into cases.

Case 1: Suppose that λ is the principal character. Since we have partitioned the elements of $(Z_{p^{2r}})^{2t}$ into the sets $A_{i,j}$ and I, then in our construction we have exactly one element (x_i, α_i) in D for every element $\alpha_i \in (Z_{p^{2r}})^{2t}$. So we have that

$$\phi(D) = \chi((Z_{p^{2r}})^{2t}).$$

Therefore, if χ is principal on $(Z_{p^{2r}})^{2t}$, then $\phi(D) = |D| = p^{4rt}$, and if χ is nonprincipal on $(Z_{p^{2r}})^{2t}$ then $\phi(D) = 0$.

Case 2: Suppose that λ is nonprincipal on P. Now we again break this into cases.

Case 2a: Suppose that χ has order p^k where $k \leq r$. Then χ will be principal on $p^r M = I$, so $\chi(I) = |I| = p^{2rt}$. $\chi(A_{i,j}) = \chi(A_{i,j'}) = a_i$ for all i, j, j' by the previous lemma. Therefore we get that:

$$\phi(D) = \sum_{i=0}^{r-1} a_i \sum_{x_j \in P} \lambda(x_j) + \lambda(x_0)\chi(I) = 0 + p^{2rt}.$$

Case 2b: Suppose that χ has order p^k where $r < k \leq 2r$. Then χ is nonprincipal on $p^r M = I$, so $\chi(I) = 0$ since I is a subgroup of M. By the

previous lemma, $\chi(A_{i,j}) = \chi(A_{i,j'}) = a_i$ for $1 \leq i \leq r$ and $i \neq 2r-k$ and for exactly one $A_{2r-k,l'}$ we have that $\chi(A_{2r-k,l'}) = p^{2rt} - p^{(2r-1)t}$ and for all $l \neq l'$, $\chi A_{2r-k,l} = -p^{(2r-1)t}$. Then we have:

$$\phi(D) = \sum_{i \neq 2r-k} a_i \sum_{x_j \in P} \lambda(x_j) + \lambda(x_0)\chi(I) + \lambda(x_{l'})\chi(A_{2r-k,l'}) +$$

$$\sum_{l \neq l'} \lambda(x_l)\chi A_{2r-k,l} = 0 + 0 + \lambda(x_{l'})(p^{2rt} - p^{(2r-1)t}) + \sum_{l \neq l'} \lambda(x_l)(-p^{(2r-1)t})$$

$$= p^{2rt}\lambda(x_{l'}) + (-p^{(2r-1)t})\lambda(P) = p^{2rt}\lambda(x_{l'}).$$

By Lemma 1.1 we have that D is a $(p^{4rt}, p^t, p^{4rt}, p^{4rt-t})$-RDS in the group $G = P \times (Z_{p^{2r}})^{2t}$.

□

So we have constructed a family of semiregular RDSs in the groups $P \times (Z_{p^{2r}})^{2t}$ for P the forbidden subgroup. P may be any abelian group satisfying $|P| = p^t$. For the case when $r = 1$, the RDSs are very similar to some of those constructed in the paper of Chen, Ray-Chaudhuri, and Xiang [2]. There have been several constructions of relative difference sets and related sets with the Galois rings $GR(p^2, t)$. Perhaps the techniques from this paper could be applied to generalize some of these constructions to Galois rings $GR(p^s, t)$ for $s > 2$.

FOOTNOTES

* Affiliation of Author: Department of Mathematics, Computer Science, and Statistics, Bloomsburg University of Pennsylvania, Bloomsburg, PA 17815

Funding was provided by the 2002-2003 Bloomsburg University Research and Disciplinary competition. The author would also like to thank Dr. James A. Davis for his assistance in preparing this paper.

The AMS Classification is 05B10.

Mailing Address:

John Polhill
Department of Mathematics, Computer Science, and Statistics
1105 McCormick Center
Bloomsburg University
Bloomsburg, PA 17815

5 References

1. A.R. Calderbank and N.J.A. Sloane, Modular and p-adic Cyclic Codes, *Designs, Codes and Crytography*, 6 (1995) pp. 21-35.

2. Y.Q. Chen, D.K. Ray-Chaudhuri, and Q. Xiang, Constructions of Partial Difference Sets and Relative Difference Sets Using Galois Rings II, *J. Comb. Th. (A)* 76(2) (1996) pp. 179-196.

3. Y.Q. Chen, On the existence of abelian Hadamard difference sets and a new family of difference sets, *Finite Fields and their Applications*, 3 (1997) pp. 234-256.

4. X. Hou and S. K. Sehgal, An extension of building sets and relative difference sets, *J. Combin. Designs*, 8 (2000) pp. 50-57.

5. K. H. Leung and S.L. Ma, Constructions of partial difference sets and relative difference sets on p-groups, *Bull. London Math. Soc.*, 22 (1990) 533-539.

6. MacDonald, *Finite Rings with Identity*, Marcel Dekker Inc., New York (1974).

7. J. Polhill, Constructions of nested partial difference sets with Galois rings, *Designs, Codes and Cryptography*, 25 (2002) pp. 299-309.

8. A. Pott, *Finite Geometry and Character Theory*, Springer-Verlag, Berlin (1995).

9. R.J. Turyn, Character sums and difference sets, *Pacific J. Math.*, 15 (1965) pp. 319-346.

10. K. Yamamoto and M. Yamada, Hadamard difference sets over an extension of $Z/4Z$, *Utilitas Math.*, 34, (1988) pp. 169-178.