Generalizations of Partial Difference Sets from Cyclotomy to Nonelementary Abelian p-Groups

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

jpolhill@bloomu.edu

Submitted: Sep 3, 2007; Accepted: Sep 22, 2008; Published: Sep 29, 2008
Mathematics Subject Classification: 05B10, 05B15, 20C15

Abstract

A partial difference set having parameters $(n^2, r(n-1), n+r^2-3r, r^2-r)$ is called a *Latin square type* partial difference set, while a partial difference set having parameters $(n^2, r(n+1), -n+r^2+3r, r^2+r)$ is called a *negative Latin square type* partial difference set. In this paper, we generalize well-known negative Latin square type partial difference sets derived from the theory of cyclotomy. We use the partial difference sets in elementary abelian groups to generate analogous partial difference sets in nonelementary abelian groups of the form $(Z_p)^{4s} \times (Z_{p^s})^4$. It is believed that this is the first construction of negative Latin square type partial difference sets in nonelementary abelian p-groups where the p can be any prime number. We also give a generalization of subsets of Type Q, partial difference sets consisting of one fourth of the nonidentity elements from the group, to nonelementary abelian groups. Finally, we give a similar product construction of negative Latin square type partial difference sets in the additive groups of $(F_q)^{4t+2}$ for an integer $t \geq 1$. This construction results in some new parameters of strongly regular graphs.

Keywords: partial difference set, negative Latin square type partial difference set, strongly regular graph, cyclotomy, Type Q set, character theory

1 Introduction

Let G be a finite group of order v with a subset D of order k. Suppose further that the differences $d_1 d_2{}^{-1}$ for $d_1, d_2 \in D$, $d_1 \neq d_2$ represent each nonidentity element of D exactly λ times and the nonidentity element of $G-D$ exactly μ times. Then D is called a (v, k, λ, μ)-*partial difference set (PDS)* in G. The survey article of Ma provides an excellent treatment of these sets [11]. A partial difference set having parameters $(n^2, r(n-1), n+r^2-3r, r^2-r)$ is called a *Latin square type PDS*. Similarly, a partial difference set having parameters $(n^2, r(n+1), -n+r^2+3r, r^2+r)$ is called a *negative Latin square type PDS*. Originally, most constructions of both of these types of PDSs were in elementary abelian groups.

When the identity $e \notin D$ and $D^{(-1)} = D$ we call the PDS D *regular*. Regular partial difference sets are equivalent to strongly regular Cayley graphs [11] and [18]. Latin square and negative Latin square type partial difference sets have connections with amorphic association schemes. See for example [17] and [18].

In this paper, we will generalize partial difference sets derived from cyclotomy. For a more detailed decription of cyclotomic classes in finite fields, see for example Storer [15]. Let $q = p^r = \alpha f + 1$ for a prime p, and further let ω be a primitive element in F_q. Then the *αth cyclotomic classes* $C_0, C_1, \ldots, C_{\alpha-1}$ are given by:

$$C_i = \{\omega^{\alpha j+i} : j = 0, 1, \ldots, f-1.\}$$

Baumert, Mills, and Ward developed the theory of uniform cyclotomy [1], from which it can be shown that unions of these classes form negative Latin square type partial difference sets under certain conditions. Calderbank and Kantor also constructed these negative Latin square type partial difference sets [3].

We can create a product of such sets with certain Latin square type partial difference sets in nonelementary abelian groups to form negative Latin square type partial difference sets in the product group. Using such products we will derive negative Latin square type partial difference sets in groups of the form $(Z_p)^{4r} \times (Z_{p^r})^4$ for all primes p (Theorems 3.1 and 3.2). We will make use of this same product to generalize the Type Q sets given by Chen in [5] to certain nonelementary abelian groups of prime power for all odd primes p (Theorems 4.1 and 4.2). Finally, we again use the cyclotomic class partial difference sets for yet another construction of negative Latin square type partial difference sets in the additive groups of $(F_q)^{4t+2}$ for an integer $t \geq 1$ (Theorems 5.1 and 5.2).

The partial difference sets given in this paper will all be of negative Latin square type. There have been relatively few constructions of negative Latin square type partial difference sets, and nearly all of these have been in elementary abelian groups. Just recently, Davis and Xiang constructed the first such PDSs in groups other than elementary abelian [6] and [7]. Their constructions were in 2-groups with characteristic at most 4. More recently, Polhill constructed negative Latin square type partial difference sets in non-elementary abelian 2-groups and 3-groups [14]. The negative Latin square type partial difference sets constructed in this paper include nonelementary abelian p-groups for all primes p and any characteristic p^r.

Partial difference sets in abelian groups are often studied within the context of the group algebra $\mathbf{Z[G]}$. For a subset D of an abelian group G, $D = \sum_{d \in D} d$ and $D^{(-1)} = \sum_{d \in D} d^{-1}$. The following equations hold for a (v, k, λ, μ)-partial difference set, D, in the abelian group, G, with identity 0:

$$DD^{(-1)} = \lambda D + \mu(G - D - 0) + k0, 0 \notin D.$$

Character theory often is used when studying partial difference sets in abelian groups. A *character* on an abelian group G is a homomorphism from the group to the complex numbers with modulus 1. The *principal character* sends all group elements to 1. The following theorem shows how character sums can be used when studying partial difference sets. See Turyn [16] for a proof of similar results.

Theorem 1.1 *Let G be an abelian group of order v with a subset D of cardinality k with $k^2 = k + \lambda k + \mu(v - k - 1)$. Then D is a (v, k, λ, μ) partial difference set in G if and only if for every nonprincipal character χ on G, $\chi(D) = \frac{\lambda-\mu\pm\sqrt{(\lambda-\mu)^2+4(k-\mu)}}{2}$.*

2 Known Latin square type and negative Latin square type partial difference sets

The partial difference sets constructed by Calderbank and Kantor [3] are given in the following theorem. This can be found in the survey of Ma [11] as Corollary 10.4, and are also an immediate consequence of uniform cyclotomy [1].

Theorem 2.1 *Let q be a prime power and $C_0, C_1, \ldots, C_q$ be the $(q + 1)$-st cyclotomic classes in $F_{q^{2m}}$. For any $I \subset \{0, 1, \ldots, q\}$, $D = \cup_{i\in I} C_i$ is a regular $(q^{2m}, u\frac{q^{2m}-1}{q+1}, u^2\eta^2 + (3u - q - 1)\eta - 1, u^2\eta^2 + u\eta)$-PDS in the additive group of $F_{q^{2m}}$ where $u = |I|$ and $\eta = \frac{(-q)^m-1}{q+1}$.*

In the case when m is even, these PDSs will have parameters $(q^{4t}, r(q^{2t} + 1), -q^{2t} + r^2 + 3r, r^2 + r)$, where $r = \frac{q^{2t}-1}{q+1}$, and hence belong to the negative Latin square type family.

In [5], Chen had the following result.

Theorem 2.2 *For all odd prime powers q, the additive group of $(F_q)^4$ contains four partial difference sets with parameters $(q^4, \frac{q^4-1}{4}, -q^2 + r^2 + 3r, r^2 + r)$ for $r = \frac{q^2-1}{4}$. These partial difference sets, known as subsets of Type Q, partition the nonzero elements of $(F_q)^4$.*

There are many constructions of Latin square type partial difference sets in abelian groups, see for example the articles [4], [9], [10], and [13]. We will use the PDSs from [13], and hence provide some background on their construction. They are constructed using Galois ring theory.

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 guarantees 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 $(Z_{p^r})^t$. MacDonald [12] has a thorough description of Galois rings.

An important subset of $R = GR(p^r,t)$ is the Teichmuller set $\mathcal{T} = \{0, 1, \omega, \omega^2, \ldots, \omega^{p^t-2}\}$ which can be viewed as the set of all solutions to the polynomial $x^{p^t} - x$ over $GR(p^r,t)$.

We will form the partial difference sets by using the structure of $R \times R$, and begin by forming what we will call a *1-array*:

$$S_i = \{(\alpha, i\alpha)|\alpha \in R\} \text{ for } i \in \mathcal{T}$$

$$S_\infty = \{(0,\alpha)|\alpha \in R\}$$

It is clear that each of the S_i forms an $R-$module, and that they intersect pairwise at $\{0\}$. Observe that the 1-array is in fact a (p^{rt}, p^t+1)-partial congruence partition (PCP) of the additive group of $R \times R$.

Now we will generalize this notion to an $l-$array for $1 \le l \le r$. Let: $S_{0,0,\ldots,0,i} = S_i$ $\forall\ i \in \mathcal{T} \cup \infty$.

Define additional subgroups by:

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

In the above definitions, the subscripts $i_j \in \mathcal{T}$. An $l-$*array* is a collection of subgroups $\{S_{i_r,\ldots,i_{l+1},x_l,\ldots,x_1}\}$ for which the i_j are fixed elements in $\mathcal{T}$, and the x_j are allowed to range over all possible values.

The entire collection, an $r-$array, of subgroups completely partitions the non-nilpotent elements of $R \times R$.

The following three theorems are proved in [13].

Theorem 2.3 *Let f be an integer with $1 \le f \le p^t + 1$ and let E be the union of any f subgroups $S_{x_r,\ldots,x_1}$ (excluding the element 0) with distinct values of x_1, so that they form a (p^{rt}, f)-PCP. Then E is a $(p^{2rt}, f(p^{rt}-1), p^{rt} + f^2 - 3f, f^2 - f)$-PDS in $G = (Z_{p^r})^{2t}$.*

Theorem 2.4 *Let D_r be defined as follows:*

$$D_r = \bigcup_{\alpha=2}^{r} \bigcup_{i \in H_\alpha} \bigcup_{x_{\alpha-1},\ldots,x_1} S_{j_r,j_{r-1},\ldots,j_{\alpha+1},i,x_{\alpha-1},\ldots,x_1} \cap (G - p^{r-(\alpha-1)}G)$$

where $H_\alpha \subset \mathcal{T}$ with $|H_\alpha| = e$ for $2 \le \alpha \le r$, $j_\beta \in \mathcal{T} - H_\beta$ for $3 \le \beta \le r$. Also $\bigcup_{x_{\alpha-1},\ldots,x_1} S_{j_r,j_{r-1},\ldots,j_{\alpha+1},i,x_{\alpha-1},\ldots,x_1}$ is the union of all subgroups with j_l and i fixed, so we have $x_l \in \mathcal{T}$ for $2 \le l \le \alpha - 1$ and $x_1 \in \mathcal{T} \cup \infty$. Then D_r is a $(p^{2rt}, ep^t n_r(p^{rt}-1), (ep^t n_r)^2 - 3(ep^t n_r) + p^{rt}, (ep^t n_r)^2 - (ep^t n_r))$-PDS in the group $(Z_{p^r})^{2t}$. Here $n_r = \frac{p^{(r-1)t}-1}{p^t-1}$ and $1 \le e < p^t$.

Theorem 2.5 *Let E and D_r be disjoint PDSs as constructed in the previous results. Then $P = E \cup D_r$ is a $(p^{2rt}, (ep^t n + f)(p^{rt}-1), p^{rt} + (ep^t n + f)^2 - 3(ep^t n + f), (ep^t n + f)^2 - (ep^t n + f))$-PDS in the group $(Z_{p^r})^{2t}$. e and f are integers with $0 \le e < p^t$, $0 \le f \le p^t + 1$ with $e + f > 0$, and $n = \frac{p^{(r-1)t}-1}{p^t-1}$.*

3 New negative Latin square type partial difference sets

We begin by constructing negative Latin square type partial difference sets by taking a product of the PDSs from Theorem 2.1 in $G = (Z_p)^{4(2)}$ with certain Latin square type PDSs in $G' = (Z_{p^2})^4$ from Theorem 2.5. In G we take the $(p+1)$-st cyclotomic classes $C_0, C_1, \ldots, C_p$. Since each of these classes is a $(p^8, r(p^4+1), -p^4+r^2+3r, r^2+r)$-PDS, where $r = (p-1)(p^2+1)$, it follows from Theorem 1.1 that for any nonprincipal character χ on G, $\chi(C_i) = r = (p-1)(p^2+1)$ or $\chi(C_i) = r - p^4 = (p-1)(p^2+1) - p^4$. Also, since $\chi(\cup_i C_i) = \chi(G - \{0\}) = -1$, it must be that $\chi(C_i) = r - p^4 = (p-1)(p^2+1) - p^4$ for exactly one i.

In G' we wish to form $p+1$ PDSs $D_0, D_1, \ldots, D_p$. In Theorem 2.5 we let $t = 2$ and $e_i = f_i = p-1$ for all i. Consider the following grid, which represents a 2-array:

$$\begin{bmatrix} S_{0,0} & S_{0,\beta} & S_{0,\beta^2} & \cdots & S_{0,\beta^{p^2-1}} & S_{0,\infty} \\ S_{\beta,0} & S_{\beta,\beta} & S_{\beta,\beta^2} & \cdots & S_{\beta,\beta^{p^2-1}} & S_{\beta,\infty} \\ S_{\beta^2,0} & S_{\beta^2,\beta} & S_{\beta^2,\beta^2} & \cdots & S_{\beta^2,\beta^{p^2-1}} & S_{\beta^2,\infty} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ S_{\beta^{p^2-1},0} & S_{\beta^{p^2-1},\beta} & S_{\beta^{p^2-1},\beta^2} & \cdots & S_{\beta^{p^2-1},\beta^{p^2-1}} & S_{\beta^{p^2-1},\infty} \end{bmatrix}$$

The above array has p^2 rows. Each of the D_i except for D_0 and D_p will consist of taking only those elements of order p^2 (elements in $G' - pG'$) from $p-1$ of the rows and combining that PDS with a PCP of $p-1$ subgroups taken from the first row. D_0 and D_p will also consist of taking only those elements of order p^2 from $p-1$ of the rows and combining that PDS with a PCP of $p-1$ subgroups taken from the first row, but then adding another entire subgroup (including the identity) from the first row. We can select these sets then so that the D_i are pairwise disjoint except that $D_0 \cap D_p = \{(0,0,0,0)\}$. By Theorem 2.5, for $1 \le i \le p-1$, D_i is a $(p^8, r(p^4-1), p^4+r^2-3r, r^2-r)$-Latin square type partial difference set, where $r = (p-1)(p^2+1)$, D_0 and D_p are each a union of a $(p^8, r(p^4-1), p^4+r^2-3r, r^2-r)$-Latin square type partial difference set with a subgroup of order p^4. Every nonidentity element is in exactly one D_i, while the identity element is in both D_0 and D_p. If we apply Theorem 1.1 to the sets D_i we get that any nonprincipal character χ will have the property that $\chi(D_i) = -r = -(p-1)(p^2+1)$ or $\chi(D_i) = p^4 - r = p^4 - (p-1)(p^2+1)$. Moreover, since $\chi(G) = 0$ for nonprincipal χ, it follows that $\sum_i \chi(D_i) = 1$ so that it will be the case that $\chi(D_i) = p^4 - (p-1)(p^2+1)$ for exactly one i. To reiterate, the key element is that the sets D_i can be selected with the following properties:

1. $\cup_{i=0}^{p} D_i = G'$;
2. $D_i \cap D_j = \emptyset$ except that $D_0 \cap D_p = \{(0,0,0,0)\}$;
3. For any nonprincipal character χ on G', $\chi(D_i) = p^4 - (p-1)(p^2+1)$ for exactly one i and $\chi(D_j) = -(p-1)(p^2+1)$ for $j \neq i$.

Theorem 3.1 *Let $G = (Z_p)^8$ and denote the $(p+1)$-st cyclotomic classes by $C_0, C_1, \ldots,$ C_p. Let $G' = (Z_{p^2})^4$ and let the sets $D_0, D_1, \ldots, D_p$ be constructed from Latin square type* *partial difference sets as above. Then set* $D = (C_0 \times D_0) \cup (C_1 \times D_1) \cup \cdots \cup (C_p \times D_p)$ *is a* $(p^{16}, r(p^8+1), -p^8+r^2+3r, r^2+r)$*-negative Latin square type partial difference set, where* $r = (p-1)(p^2+1)(p^4+1)$ *in the group* $(Z_p)^8 \times (Z_{p^2})^4$.

Proof: Let ϕ be a character on $G \times G'$. Then $\phi = \chi \otimes \psi$, where χ is a character on G and ψ is a character on G'.

If ϕ is the principal character, then for $j \neq 0$:

$$\begin{aligned}\phi(D) = |D| &= |C_0||D_0| + |C_1||D_1| + \cdots + |C_{p-1}||D_{p-1}| + |C_p||D_p| \\ &= (p-1)\big[(p-1)(p^2+1)(p^4+1)\big]\big[(p-1)(p^2+1)(p^4-1)\big] \\ &\quad + 2\big[(p-1)(p^2+1)(p^4+1)\big]\big[(p-1)(p^2+1)(p^4-1)+p^4\big] \\ &= (p-1)(p^2+1)(p^4+1)(p^8+1).\end{aligned}$$

Now suppose that ϕ is a nonprincipal character on $G \times G'$.

Case 1: χ is principal on G, but ψ is nonprincipal on G'. Then for all i, $\chi(C_i) = |C_i| = (p-1)(p^2+1)(p^4+1)$. ψ will take the values $-(p-1)(p^2+1)$ or $p^4-(p-1)(p^2+1)$, and in fact there will be exactly one D_j for which $\psi(D_j) = p^4-(p-1)(p^2+1)$ and for all $k \neq j$, $\psi(D_k) = -(p-1)(p^2+1)$. Then we have:

$$\begin{aligned}\phi(D) &= \chi(C_0)\psi(D_0) + \cdots + \chi(C_p)\psi(D_p) \\ &= (p-1)(p^2+1)(p^4+1)\big[p^4-(p-1)(p^2+1)+(p)\big(-(p-1)(p^2+1)\big)\big] \\ &= (p-1)(p^2+1)(p^4+1).\end{aligned}$$

Case 2: χ is nonprincipal on G, but ψ is principal on G'. Then $\psi(D_0) = \psi(D_p) = (p-1)(p^2+1)(p^4-1)+p^4$ and for $i \neq 0, p$, $\psi(D_i) = (p-1)(p^2+1)(p^4-1)$. χ will take the values $(p-1)(p^2+1)$ or $(p-1)(p^2+1)-p^4$, and in fact there will be exactly one C_j for which $\chi(C_j) = (p-1)(p^2+1)-p^4$ and for all $k \neq j$, $\chi(C_k) = (p-1)(p^2+1)$. If $j=0$ or $j=p$ then we have:

$$\begin{aligned}\phi(D) &= \chi(C_0)\psi(D_0) + \chi(C_p)\psi(D_p) + \chi(C_1)\psi(D_1) + \cdots + \chi(C_{p-1})\psi(D_{p-1}) \\ &= \big((p-1)(p^2+1)(p^4-1)+p^4\big)\big((p-1)(p^2+1)-p^4\big) \\ &\quad + \big((p-1)(p^2+1)(p^4-1)+p^4\big)\big((p-1)(p^2+1)\big) \\ &\quad + (p-1)\big((p-1)(p^2+1)(p^4-1)\big)\big((p-1)(p^2+1)\big) \\ &= (p-1)(p^2+1)(p^4+1)-p^8.\end{aligned}$$

If $j \neq 0$ and $j \neq p$, then we have:

$$\begin{aligned}\phi(D) &= \chi(C_0)\psi(D_0) + \chi(C_p)\psi(D_p) + \chi(C_1)\psi(D_1) + \cdots + \chi(C_{p-1})\psi(D_{p-1}) \\ &= 2\big((p-1)(p^2+1)(p^4-1)+p^4\big)\big((p-1)(p^2+1)\big) \\ &\quad + \big((p-1)(p^2+1)(p^4-1)\big)\big((p-1)(p^2+1)-p^4\big) \\ &\quad + (p-2)\big((p-1)(p^2+1)(p^4-1)\big)\big((p-1)(p^2+1)\big) \\ &= (p-1)(p^2+1)(p^4+1).\end{aligned}$$

Case 3: Suppose that both χ and ψ are nonprincipal. Then χ will take the values of $(p-1)(p^2+1)$ or $(p-1)(p^2+1)-p^4$, and in fact there will be exactly one C_j for which $\chi(C_j)=(p-1)(p^2+1)-p^4$ and for all $i\neq j$, $\chi(C_i)=(p-1)(p^2+1)$. ψ will take the values $-(p-1)(p^2+1)$ or $p^4-(p-1)(p^2+1)$, and in fact there will be exactly one D_k for which $\psi(D_k)=p^4-(p-1)(p^2+1)$ and for all $i\neq k$, $\psi(D_i)=-(p-1)(p^2+1)$. If $j=k$, we have:

$$\begin{aligned}\phi(D) &= \chi(C_j)\psi(D_j)+\sum_{i\neq j}\chi(C_i)\psi(D_i)\\ &= \big(p^4-(p-1)(p^2+1)\big)\big((p-1)(p^2+1)-p^4\big)\\ &\qquad + p\big(-(p-1)(p^2+1)\big)\big((p-1)(p^2+1)\big)\\ &= (p-1)(p^2+1)(p^4+1)-p^8.\end{aligned}$$

If $j\neq k$, we have instead:

$$\begin{aligned}\phi(D) &= \chi(C_k)\psi(D_k)+\chi(C_j)\psi(D_j)+\sum_{i\neq j,k}\chi(C_i)\psi(D_i)\\ &= \big(p^4-(p-1)(p^2+1)\big)\big((p-1)(p^2+1)\big)\\ &\qquad + \big(-(p-1)(p^2+1)\big)\big((p-1)(p^2+1)-p^4\big)\\ &\qquad + (p-1)\big(-(p-1)(p^2+1)\big)(p-1)(p^2+1)\\ &= (p-1)(p^2+1)(p^4+1).\end{aligned}$$

We have shown that for all nonprincipal characters ϕ, $\phi(D)=(p-1)(p^2+1)(p^4+1)-p^8$ or $(p-1)(p^2+1)(p^4+1)$. Therefore the result follows from Theorem 1.1. □

In the group $G'=(Z_{p^s})^4$ we can again use the techniques from [13] to find sets $D_0,D_1,\ldots,D_p$ such that for $1\leq i\leq p-1$, each D_i is a $(p^{4s},r(p^{2s}-1),p^{2s}+r^2-3r,r^2-r)$-Latin square type partial difference set of the type from Theorem 2.5, where $r=\frac{p^{2s}-1}{p+1}$. D_0 and D_p are each a union of such a partial difference set with a subgroup of order p^{2s}. We will then have the following:

1. $\cup_{i=0}^{p}D_i=G'$;
2. $D_i\cap D_j=\emptyset$ except that $D_0\cap D_3=\{(0,0,0,0)\}$;
3. For any nonprincipal character χ on G', $\chi(D_i)=p^{2s}-r$ for exactly one i and $\chi(D_j)=-r$ for $j\neq i$.

We can prove the following more general result. The proof here is essentially the same as for the case when $s=2$, so we omit it.

Theorem 3.2 *Let $G=(Z_p)^{4s}$ and denote the $(p+1)$-st cyclotomic classes by $C_0,C_1,\ldots,$ C_p. Let $G'=(Z_{p^s})^4$ and let the sets $D_0,D_1,\ldots,D_p$ be constructed from Latin square type partial difference sets as above. The set $D=(C_0\times D_0)\cup(C_1\times D_1)\cup\cdots\cup(C_p\times D_p)$ is a $(p^{8s},r(p^{4s}+1),-p^{4s}+r^2+3r,r^2+r)$-partial difference set, where $r=\frac{p^{4s}-1}{p+1}$ in the group $(Z_p)^{4s}\times(Z_{p^s})^4$. These partial difference sets are from the negative Latin square type family.*

Corollary 3.1 *The group* $(Z_p)^{4s} \times (Z_{p^s})^4$ *has negative Latin square type partial difference sets with parameters* $(p^{8s}, ar(p^{4s}+1), -p^{4s}+(ar)^2+3ar, (ar)^2+ar)$ *where* $r = \frac{p^{4s}-1}{p+1}$ *and* $1 \le a \le p+1$.

Proof: We can use Theorem 3.2 to obtain up to $\frac{p+1}{2}$ disjoint negative Latin square type partial difference sets with parameters $(p^{8s}, r(p^{4s}+1), -p^{4s}+r^2+3r, r^2+r)$, where $r = \frac{p^{4s}-1}{p+1}$. For example:

$$\begin{aligned} D_I &= (C_0 \times D_0) \cup (C_1 \times D_1) \cup \cdots \cup (C_p \times D_p) \\ D_{II} &= (C_0 \times D_2) \cup (C_1 \times D_3) \cup \cdots \cup (C_p \times D_1) \\ D_{III} &= (C_0 \times D_4) \cup (C_1 \times D_5) \cup \cdots \cup (C_p \times D_3) \\ &\text{etc.} \end{aligned}$$

Notice that we cannot form more than $\frac{p+1}{2}$ disjoint negative Latin square type partial difference sets with parameters $(p^{8s}, r(p^{4s}+1), -p^{4s}+r^2+3r, r^2+r)$ due to the fact that each will contain two sets of the form $C_i \times D_0$ and $C_j \times D_p$ and both D_0 and D_p contain the identity. A union of a of these negative Latin square type PDSs will yield PDSs with parameters $(p^{8s}, ar(p^{4s}+1), -p^{4s}+(ar)^2+3ar, (ar)^2+ar)$ where $r = \frac{p^{4s}-1}{p+1}$ and $1 \le a \le \frac{p+1}{2}$. We can get the remaining parameters by taking the complements of these unions. $\square$

4 Generalizing subsets of Type Q

In this section, instead of using $(q+1)$-st cyclotomic classes, we will use the fourth residues. Theorem 2.2 gives us that for all odd prime powers q, the additive group G of $(F_q)^4$ contains four partial difference sets C_0, C_1, C_2, C_3 with parameters $(q^4, \frac{q^4-1}{4}, -q^2+r^2+3r, r^2+r)$ for $r = \frac{q^2-1}{4}$. These sets will have the following properties:

1. $\cup_{i=0}^{3} C_i = G - \{0\}$;
2. $C_i \cap C_j = \emptyset$ for $i \neq j$;
3. For any nonprincipal character χ on G, the $\chi(C_i) = r - q^2$ for some i and $\chi(C_j) = r$ for all $j \neq i$.

Now we will have to consider two cases, $p \cong 1(\text{mod } 4)$ and s even versus $p \cong 3(\text{mod } 4)$ or $p \cong 1(\text{mod } 4)$ and s odd. For the case $p \cong 1(\text{mod } 4)$ and s even, we can consider the group $G' = (Z_{p^s})^2$. We form 4 sets D_0, D_1, D_2, D_3 such that D_1 and D_2 are partial difference sets from Theorem 2.5 with $e = f = \frac{p-1}{4}$. Therefore, D_1 and D_2 are $(p^{2s}, r(p^s-1), p^s+r^2-3r, r^2-r)$-Latin square type partial difference sets with $r = \frac{p^s-1}{4}$. D_0 and D_3 will each be a union of such a partial difference set with a subgroup of order p^s. Then the D_i have the following properties:

1. $\cup_{i=0}^{3} D_i = G'$;
2. $D_i \cap D_j = \emptyset$ except that $D_0 \cap D_3 = \{(0,0)\}$;

3. For any nonprincipal character χ on G', $\chi(D_i) = p^s - r$ for exactly one i and $\chi(D_j) = -r$ for $j \neq i$.

Then we can use a similar proof to Theorem 3.1 to give us the following result:

Theorem 4.1 *Let $p \cong 1 (mod\ 4)$. Let $G = (Z_p)^{2s}$ and $G' = (Z_{p^s})^2$ for s even. Also let C_0, C_1, C_2, C_3 be four subsets of Type Q that partition the nonidentity elements of G. Let D_0, D_1, D_2, D_3 be the sets above in G' derived from Latin square partial difference sets. Then the set $D = (C_0 \times D_0) \cup (C_1 \times D_1) \cup (C_2 \times D_2) \cup (C_3 \times D_3)$ is a $(p^{4s}, \frac{p^{4s}-1}{4}, -p^{2s} + R^2 + 3R, R^2 + R)$-negative Latin square type partial difference set for $R = \frac{p^{2s}-1}{4}$.*

The case where $p \cong 3 (\text{mod } 4)$ is similar, except that since 4 does not divide $p - 1$ we must use $G' = (Z_{p^s})^4$ and take advantage of the fact that then we can use $e = \frac{p^2-1}{4}$ with Theorem 2.5. For the case with $p \cong 1 (\text{mod } 4)$ and s odd we need for the power on p to be divisible by 4 in order to apply Theorem 2.2 to get the subsets of Type Q in $(Z_p)^{4s}$. We are able in either case to get the following result:

Theorem 4.2 *Let $G = (Z_p)^{4s}$ and $G' = (Z_{p^s})^4$. Also let C_0, C_1, C_2, C_3 be four subsets of Type Q that partition the nonidentity elements of G. Let D_0, D_1, D_2, D_3 be the sets above in G' derived from Latin square partial difference sets. Then the set $D = (C_0 \times D_0) \cup (C_1 \times D_1) \cup (C_2 \times D_2) \cup (C_3 \times D_3)$ is a $(p^{8s}, \frac{p^{8s}-1}{4}, -p^{4s} + R^2 + 3R, R^2 + R)$-negative Latin square type partial difference set for $R = \frac{p^{4s}-1}{4}$.*

5 A construction of negative Latin square type PDSs in elementary abelian groups

In this section we will use similar products to those of the previous sections to obtain negative Latin square type partial difference sets. However, the PDSs in this section will only be constructed in elementary abelian groups.

We begin with a pair of motivating examples. In $G = (Z_3)^4$ we can find sets C_0, C_1, C_2, C_3 as in Theorem 2.2, so that each is an $(81, 20, 1, 10)$-PDS in G. Let $C_i^+ = C_i \cup \{0\}$, In $G' = (Z_3)^2$, we can consider G' to be the additive group of $(GF(3))^2$ and take the 4 hyperplanes with the identity removed to be $H_0^*, H_1^*, H_2^*, H_3^*$. Then the set $D = (C_0^+ \times H_0^*) \cup (C_1^+ \times H_1^*) \cup (C_2^+ \times H_2^*) \cup (C_3^+ \times H_3^*)$ will be a negative Latin square type partial difference set in $G \times G'$.

Alternatively, we could let $G = (Z_3)^6$ viewed as the additive group of $(GF(27))^2$. There will be 28 hyperplanes $H_0, H_1, \ldots, H_{27}$, and let $D_0 = H_0 \cup H_1 \cdots \cup H_6$, $D_1 = H_7 \cup H_8 \cup \cdots \cup H_{13}$, $D_2 = H_{14} \cup H_{15} \cup \cdots \cup H_{20}$, and $D_3 = H_{21} \cup H_{22} \cup \cdots \cup H_{27}$. In this case we want $0 \in D_i$. Now we let $G' = (Z_3)^4$ and take the sets C_0, C_1, C_2, C_3 as in Theorem 2.2, so that each is an $(81, 20, 1, 10)$-PDS in G. Then $D = (D_0 \times C_0) \cup (D_1 \times C_1) \cup (D_2 \times C_2) \cup (D_3 \times C_3)$ will be a negative Latin square type partial difference set in $G \times G'$.

We now generalize the above examples with the following two theorems. The proof of the second is very similar to the first, so we omit the details.

Theorem 5.1 *Suppose that G is a group that contains $q+1$ partial difference sets $C_0, C_1, \ldots, C_q$ with parameters $(q^4, (q-1)(q^2+1), -q^2+(q-1)^2+3(q-1), (q-1)^2+(q-1))$. Suppose that G' is a group that contains $q+1$ partial difference sets $D_0, D_1, \ldots, D_q$ with parameters $(q^2, q-1, q-2, 0)$. Let $C_i^+ = C_i \cup \{0\}$. Then the set $D = (C_0^+ \times D_0) \cup (C_1^+ \times D_1) \cup \cdots \cup (C_q^+ \times D_q)$ is a $(q^6, r(q^3+1), -q^3+r^2+3r, r^2+r)$-negative Latin square type partial difference set in $G \times G'$, where $r = q(q-1)$.*

Proof: Let ϕ be a character on $G \times G'$. Then $\phi = \chi \otimes \psi$, where χ is a character on G and ψ is a character on G'. If χ is a nonprincipal character on G, then $\chi(C_i) = q - q^2$ for some i and $\chi(C_j) = q$ for $j \neq i$. If ψ is a nonprincipal character on G, then $\psi(C_i) = q-1$ for some i and $\chi(C_j) = -1$ for $j \neq i$.

If ϕ is the principal character, then for $j \neq 0$:

$$\begin{aligned}\phi(D) = |D| &= |C_0^+||D_0| + |C_1^+||D_1| + \cdots + |C_{q-1}^+||D_{q-1}| + |C_q^+||D_q| \\ &= (q+1)[(q-1)(q^2+1)+1](q-1) = q(q-1)(q^3+1).\end{aligned}$$

Now suppose that ϕ is a nonprincipal character on $G \times G'$.

Case 1: χ is principal on G, but ψ is nonprincipal on G'. Then for all i, $\chi(C_i^+) = |C_i^+| = (q-1)(q^2+1)+1$. ψ will take the values -1 or $q-1$, and in fact there will be exactly one D_j for which $\psi(D_j) = q-1$ and for all $k \neq j$, $\psi(D_k) = -1$. Then we have:

$$\begin{aligned}\phi(D) &= \chi(C_0^+)\psi(D_0) + \cdots + \chi(C_p^+)\psi(D_p) \\ &= \big((q-1)(q^2+1)+1\big)(q-1) + q\big((q-1)(q^2+1)+1\big)(-1) = -q^3 + (q^2-q).\end{aligned}$$

Case 2: χ is nonprincipal on G, but ψ is principal on G'. Then $\psi(D_i) = q-1$ for all i. χ will take the values $q-q^2$ or q, and in fact there will be exactly one C_j^+ for which $\chi(C_j^+) = q - q^2$ and for all $k \neq j$, $\chi(C_k^+) = q$. Then we have:

$$\phi(D) = \chi(C_0^+)\psi(D_0) + \cdots + \chi(C_q^+)\psi(D_q) = (q-1)(q-q^2) + q(q-1)(q) = q^2 - q.$$

Case 3: Suppose that both χ and ψ are nonprincipal. χ will take the values $q-q^2$ or q, and in fact there will be exactly one C_j^+ for which $\chi(C_j^+) = q-q^2$ and for all $i \neq j$, $\chi(C_i^+) = q$. ψ will take the values -1 or q^2-1, and in fact there will be exactly one D_k for which $\psi(D_k) = q^2-1$ and for all $i \neq k$, $\psi(D_i) = -1$. If $j = k$, we have:

$$\phi(D) = \chi(C_j^+)\psi(D_j) + \sum_{i \neq j} \chi(C_i^+)\psi(D_i) = (q-q^2)(q-1) + q(q)(-1) = -q^3 + (q^2-q).$$

If $j \neq k$, we have instead:

$$\begin{aligned}\phi(D) &= \chi(C_k^+)\psi(D_k) + \chi(C_j^+)\psi(D_j) + \sum_{i \neq j,k} \chi(C_i^+)\psi(D_i) \\ &= (q)(q-1) + (q-q^2)(-1) + (q-1)(q)(-1) = q^2 - q.\end{aligned}$$

We have shown that for all nonprincipal characters ϕ, $\phi(D) = -q^3 + (q^2-q)$ or q^2-q. Therefore the result follows from Theorem 1.1. $\square$

Corollary 5.1 *The additive group of* $(F_q)^4 \times (F_q)^2$ *has a* $(q^6, r(q^3+1), -q^3+r^2+3r, r^2+r)$*-negative Latin square type partial difference set for* $r = q(q-1)$*.*

Proof: Theorem 2.1 gives us the necessary $C_0, C_1, \ldots, C_q$ in the additive group of $(F_q)^4$, while we can partition the additive group of $(F_q)^2$ into $q+1$ subgroups that intersect pairwise in the identity (we remove the identity from each). $\square$

Theorem 5.2 *Suppose that* G *is a group that contains* $q+1$ *partial difference sets* $C_0, C_1, \ldots, C_q$ *with parameters* $(q^4, (q-1)(q^2+1), -q^2+(q-1)^2+3(q-1), (q-1)^2+(q-1))$*. Suppose that* G' *is a group that contains* $q+1$ *partial difference sets* $D_0, D_1, \ldots, D_q$ *with parameters* $(q^6, \frac{q^6-1}{q+1}, q^3+{r_b}^2-3r_b, {r_b}^2-r_b)$ *for* $r_b = q^2-q+1$*. Let* $D_i^+ = D_i \cup \{0\}$*. Then the set* $D = (C_0 \times D_0^+) \cup (C_1 \times D_1^+) \cup \cdots \cup (C_q \times D_q^+)$ *is a* $(q^{10}, r(q^5+1), -q^5+r^2+3r, r^2+r)$*-negative Latin square type partial difference set in* $G \times G'$*, where* $r = q(q^2+1)(q-1)$*.*

Corollary 5.2 *The additive group of* $(F_q)^4 \times (F_q)^6$ *has a* $(q^{10}, r(q^5+1), -q^5+r^2+3r, r^2+r)$*-negative Latin square type partial difference set for* $r = q(q-1)(q^2+1)$*.*

Proof: Theorem 2.1 gives us the necessary sets $C_0, C_1, \ldots, C_q$ in the additive group of $(F_q)^4$, while we can view the additive group of $(F_q)^6$ as $(GF(q^3))^2$, taking the q^3+1 hyperplanes. Each of the sets D_i will consist of a union of $\frac{q^3+1}{q+1}$ of these hyperplanes. $\square$

Using the constructions in the previous two theorems we can construct negative Latin square type partial difference sets in the additive groups of ${F_q}^{2t} \times {F_q}^{2t+2} \cong {F_q}^{4t+2}$.

A (v, k, λ, μ)*-strongly regular graph* is a graph with v vertices so that each vertex is connected to k other vertices, and with the additional property that distinct vertices x and y share edges with either λ or μ common vertices as x and y are either adjacent or non-adjacent. It is well known that a (v, k, λ, μ)-partial difference set is isomorphic to a (v, k, λ, μ)-strongly regular Cayley graph with a regular automorphism group. In this section we have constructed PDSs which in some cases represent new parameter sets for strongly regular graphs. We consider some examples. If we set $q = 2$ and $s = 1$ we obtain the parameters $(64, 18, 2, 6)$, which are well known to exist, [11]. If we set $q = 3$ and $s = 1$ we obtain a $(729, 168, 27, 42)$-strongly regular graph, which has the same parameters as that constructed by Gulliver using projective codes, [8]. On the other hand, when we set $q = 2$ and $s = 2$ we obtain a $(1024, 330, 98, 110)$-strongly regular graph, which seems to be new based upon a table of Brouwer, [2]. Other parameter sets have more vertices than those graphs in Brouwer's table, such as when $q = 4$ and $s = 1$ yielding $(4096, 780, 116, 156)$.

6 Some open problems

We conclude by giving some possible areas where the results in this paper could be generalized.

1. Theorems 3.1, 3.2, 4.1, and 4.2 were derived from the Latin square type partial difference sets from [13]. There are numerous other constructions of Latin square type partial difference sets that might be used to produce different negative Latin square type partial difference sets.

2. The cyclotomic classes form negative Latin square type partial difference sets, each of the same size, that partition the elementary abelian group. The negative Latin square type partial difference sets constructed in this paper do not have this property. Perhaps the constructions could be modified somehow to do so. If this were the case, they could be used recursively to generate more negative Latin square type partial difference sets.

3. The results in Section 5 were in elementary abelian groups. Is it possible to find partial difference sets with similar properties in nonelementary abelian groups that could be used with the constructions? At least, could one generalize these results to a more general class of elementary abelian groups?

References

[1] L. D. Baumert, W. H. Mills, and R. L. Ward, Uniform cyclotomy, *J. Number Theory.* 14 (1982) 67-82.

[2] A. E. Brouwer, Table of parameters of strongly regular graphs. http://www.win.tue.nl/~aeb/graphs/srg/srgtab.html.

[3] R. Calderbank and W. M. Kantor, The geometry of two-weight codes, *Bull.London Math Soc.* 18 (1986) 97-122.

[4] 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) 179-196.

[5] 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) 234-256.

[6] J. A. Davis and Q. Xiang, Negative Latin square type partial difference sets in nonelementary abelian 2-groups, *J. London Math Soc (2)* 70 (2004) 125-141.

[7] J. A. Davis and Q. Xiang, Amorphic association schemes with negative Latin square-type graphs, *Finite Fields Appl.*, 12 (2006) 595-612.

[8] T. A. Gulliver, A new two-weight code and strongly regular graph, *Appl. Math. Lett.*, 9(2) (1996) 17-20.

[9] X.-D. Hou, New partial difference in p-groups, *J. Combin. Des. (10)* 6 (2002) 396-402.

[10] 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.

[11] S. L. Ma, A Survey of partial difference sets. *Designs, Codes, and Cryptography*, 4 (1994) 221-261.

[12] B. MacDonald, *Finite Rings with Identity*, Marcel Dekker Inc., New York, 1974.

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

[14] J. Polhill, New negative Latin square type partial difference sets in nonelementary abelian 2-groups and 3-groups, *Designs, Codes, and Cryptography*, 46 (3) (2008) 365-377.

[15] T. Storer, Cyclotomy and difference sets, *Lectures in Advanced Mathematics*, 2, Markham Publishing Company, Chicago, Illinois, USA (1967).

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

[17] E.R. van Dam, Strongly regular decompositions of the complete graph, *J. Algebraic Combin.* 17 (2003) 181-201.

[18] J.H. Van Lint and R. M. Wilson, A Course in Combinatorics, second edition, Cambridge University Press, Cambridge, MA, USA 2001.