Designs, Codes and Cryptography, 6, 57–71 (1995)

On (p^a, p, p^a, p^{a-1})-Relative Difference Sets

S. L. MA matmasl@nusvm.bitnet; matmasl@leonis.nus.sg
Department of Mathematics, National University of Singapore, Kent Ridge, Singapore 0511, Republic of Singapore

BERNHARD SCHMIDT
Mathematisches Institut, Universität Augsburg, Universitätsstraße 2, 86135 Augsburg, Germany

Received September 14, 1994

Abstract. Abelian relative difference sets of parameters $(m, n, k, \lambda) = (p^a, p, p^a, p^{a-1})$ are studied in this paper. In particular, we show that for an abelian group G of order p^{2c+1} and a subgroup N of G of order p, a $(p^{2c}, p, p^{2c}, p^{2c-1})$-relative difference set exists in G relative to N if and only if $\exp(G) \le p^{c+1}$. Furthermore, we have some structural results on $(p^{2c}, p, p^{2c}, p^{2c-1})$-relative difference sets in abelian groups of exponent p^{c+1}. We also show that for an abelian group G of order 2^{2c+2} and a subgroup N of G of order 2, a $(2^{2c+1}, 2, 2^{2c+1}, 2^{2c})$-relative difference set exists in G relative to N if and only if $\exp(G) \le 2^{c+2}$ and N is contained in a cyclic subgroup of G of order 4. New constructions of $(p^{2c+1}, p, p^{2c+1}, p^{2c})$-relative difference sets, where p is an odd prime, are given. However, we cannot find the necessary and sufficient condition for this case.

1. Introduction

Let G be a group of order mn which has a subgroup N of order n. An (m, n, k, λ)-*relative difference set* (RDS) R in G relative to N is a k-element subset of G such that the expressions $r_1 r_2^{-1}$, with $r_1, r_2 \in R$ and $r_1 \neq r_2$, represent each element in $G\backslash N$ exactly λ times and represent no nonidentity element in N. The concept of RDSs was introduced by Butson [4], [5] and Elliott and Butson [13] as a generalization of difference sets. For general descriptions of RDSs and their relation with designs, please consult [14].

Using the notation of the group ring $\mathcal{F}[G]$, where $\mathcal{F}$ is either the ring of rational integers or the field of complex numbers, a subset R of G is an (m, n, k, λ)-RDS in G relative to N if and only if

$$RR^{(-1)} = ke_G + \lambda(G - N) \tag{1}$$

where we identify a subset A of G with the element $\sum_{g \in A} g$ in $\mathcal{F}[G]$ and write $R^{(-1)} = \{r^{-1} : r \in R\}$. Furthermore, if G is abelian, then R is an (m, n, k, λ)-RDS in G relative to N if and only if for every character χ of G

$$\chi(R)\overline{\chi(R)} = \begin{cases} k & \text{if } \chi \in G\backslash N^{\perp} \\ k - \lambda n & \text{if } \chi \in N^{\perp}\backslash\{\chi_0\} \\ k^2 & \text{if } \chi = \chi_0 \end{cases} \tag{2}$$

where $N^{\perp} = \{\chi \in G^* : \chi \text{ is principal on } N\}$ and χ_0 is the principal character of G.

Recently, RDSs with parameters $(m, n, k, \lambda) = (p^a, p^b, p^a, p^{a-b})$, where p is a prime, have been studied intensively, for examples, see [3], [7], [8], [12], [19]. RDSs with these parameters have a lot of important applications. For example, some of these RDSs can be used to construct sequences with ideal auto-correlation and cross-correlation properties, see [12].

In this paper, we continue the work of Davis [8] on (p^a, p, p^a, p^{a-1})-RDSs. For a given abelian group G of order p^a and a subgroup N of G of order p, we shall study the conditions under which a (p^a, p, p^a, p^{a-1})-RDS exists in G relative to N. Complete answers for $(m, n, k, \lambda) = (p^{2c}, p, p^{2c}, p^{2c-1})$ and $(2^{2c+1}, 2, 2^{2c+1}, 2^{2c})$ will be given.

In the following, we list some theorems on the exponent bounds of groups containing these RDSs.

THEOREM 1.1 (Pott [23]). *Let p be a prime, G an abelian group of order p^{a+1} and N a subgroup of G of order p. If there exists a (p^a, p, p^a, p^{a-1})-RDS in G relative to N, then* $\exp(G) \leq p^{\lceil a/2\rceil+1}$ *where $\lceil x\rceil$ denote the smallest integer greater than x.*

THEOREM 1.2 (Ma and Pott [19]). *Let p be an odd prime, G an abelian group of order p^{2c+2} and N a subgroup of G of order p. If there exists a $(p^{2c+1}, p, p^{2c+1}, p^{2c})$-RDS in G relative to N, then* $\exp(G) \leq p^{c+1}$.

2. The Constructions of $(p^{2c}, p, p^{2c}, p^{2c-1})$-RDSs

By Theorem 1.1, an abelian group of order p^{2c+1} containing a $(p^{2c}, p, p^{2c}, p^{2c-1})$-RDS must have exponent not exceeding p^{c+1}. In the following, we shall study three construction methods of these RDSs. Theorem 2.1 is a slightly improved version of a result by Davis [8]. Theorem 2.2 is based on the K-matrix construction developed by Davis [6] and Kraemer [16]. Finally, Theorem 2.3 is an inductive construction.

For convenience, throughout this paper, the cross product of groups will be regarded as the internal direct product.

THEOREM 2.1 *Let p be a prime. Let G be an abelian group of order p^{2c+1} which contains a subgroup $E = \langle\alpha\rangle \times H$ where $|H| = p^c$ and* $\exp(H) = o(\alpha) = p^e \leq p^{c+1}$. *Then there exists a $(p^{2c}, p, p^{2c}, p^{2c-1})$-RDS in G relative to $N = \langle\alpha^{p^{e-1}}\rangle$.*

Proof. Let $H = \bigotimes_{j=1}^{t}\langle\beta_j\rangle$ where $o(\beta_j) = p^{b_j}$ and $b_1 = \max_{1\leq j\leq t} b_j = e$. For $0 \leq i_j \leq p^{b_j} - 1$, $1 \leq j \leq t$, define

$$D_{i_1,i_2,\ldots,i_t} = \bigotimes_{j=1}^{t}\langle\beta_j\alpha^{i_j p^{e-b_j}}\rangle \subset E$$

and choose $g_{i_1,i_2,\ldots,i_t} \in G$ so that

$$\{g_{i_1,i_2,\ldots,i_t} : 0 \leq i_k \leq p^{b_k} - 1 \text{ for } 2 \leq k \leq t \text{ and } 0 \leq i_1 \leq p - 1\}$$

is a system of distinct coset representatives of E in G and

$$g_{i_1,i_2,\ldots,i_t} = \alpha^m g_{n,i_2,\ldots,i_t}$$

for $i_1 = pm + n$ where $0 \leq n \leq p-1$. Let

$$R = \bigcup_{i_1=0}^{p^{b_1}-1} \bigcup_{i_2=0}^{p^{b_2}-1} \cdots \bigcup_{i_t=0}^{p^{b_t}-1} D_{i_1,i_2,\ldots,i_t} g_{i_1,i_2,\ldots,i_t}.$$

We claim that R is a $(p^{2c}, p, p^{2c}, p^{2c-1})$-RDS in G relative to N.

If $\chi \notin N^{\perp}$, it is obvious that χ is principal on exactly one $D_{i_1,i_2,\ldots,i_t}$ and hence $|\chi(R)| = p^c$. It remains to show $|R \cap Nh| = 1$ for all $h \in G$. To prove this, it suffices to show

$$(D_{i_1,i_2,\ldots,i_t} g_{i_1,i_2,\ldots,i_t} N) \cap (D_{i'_1,i'_2,\ldots,i'_t} g_{i'_1,i'_2,\ldots,i'_t}) = \emptyset$$

for all $(i_1, i_2, \ldots, i_t) \neq (i'_1, i'_2, \ldots, i'_t)$. Suppose

$$\left[\prod_{j=1}^{t} \left(\beta_j \alpha^{i_j p^{e-b_j}}\right)^{k_j}\right] g_{i_1,i_2,\ldots,i_t} \alpha^{\omega p^{e-1}} = \left[\prod_{j=1}^{t} \left(\beta_j \alpha^{i'_j p^{e-b_j}}\right)^{k'_j}\right] g_{i'_1,i'_2,\ldots,i'_t}$$

for some $(i_1, i_2, \ldots, i_t)$ and $(i'_1, i'_2, \ldots, i'_t)$. Let $i_1 = pm + n$ and $i'_1 = pm' + n'$ where $0 \leq m, m' \leq p^{e-1} - 1$ and $0 \leq n, n' \leq p-1$. The equation above can be possible only if $g_{i_1,i_2,\ldots,i_t}$ and $g_{i'_1,i'_2,\ldots,i'_t}$ are in the same coset of E. But by the definition of $g_{i_1,i_2,\ldots,i_t}$, we have $i_j = i'_j$ for $2 \leq j \leq t$, $n = n'$ and

$$\alpha^{-m} g_{i_1,i_2,\ldots,i_t} = \alpha^{-m'} g_{i'_1,i'_2,\ldots,i'_t}.$$

Then $k_j \equiv k'_j \bmod p^{b_j}$ for $1 \leq j \leq t$ which imply

$$i_1 k_1 + \omega p^{e-1} + m \equiv i'_1 k_1 + m' \bmod p^e.$$

Hence $(m - m')(pk_1 + 1) \equiv 0 \bmod p^{e-1}$ and $m \equiv m' \bmod p^{e-1}$. It forces $m = m'$ and so $i_1 = i'_1$. ■

We remark that the construction described in the proof of Theorem 2.1 can be generalized to nonabelian groups by the method of Dillon [11] and Davis [8]. For example, if G is a group of order p^{2c+1} and the center of G contains a subgroup $E = \langle\alpha\rangle \times H$ where H is an abelian group of order p^c and $\exp(H) = o(\alpha) = p^e$, then there exists a $(p^{2c}, p, p^{2c}, p^{2c-1})$-RDS in G relative to $N = \langle\alpha^{p^{e-1}}\rangle$. Using the same construction as above, we only need to prove that the subsets $Q_{i_1,i_2,\ldots,i_t}$, where $0 \leq i_1 \leq p-1$ and $0 \leq i_j \leq p^{b_j-1}$ for $2 \leq j \leq t$, of E defined by

$$Q_{i_1,i_2,\ldots,i_t} = \bigcup_{m=1}^{p^{e-1}-1} \alpha^m D_{pm+i_1,i_2,\ldots,i_t}$$

satisfy

$$\sum_{i_1=0}^{p-1} \sum_{i_2=0}^{p^{b_2}-1} \cdots \sum_{i_t=0}^{p^{b_t}-1} Q_{i_1,i_2,\ldots,i_t} Q^{(-1)}_{i_1,i_2,\ldots,i_t} = p^{2c} e_E + p^{2c-1} E - p^{2c-1} N \tag{3}$$

and for $(i_1, i_2, \dots, i_t) \neq (i'_1, i'_2, \dots, i'_t)$,

$$Q_{i_1,i_2,\dots,i_t} Q^{(-1)}_{i'_1,i'_2,\dots,i'_t} = p^{c+e-2} E. \tag{4}$$

Let χ be a character of E. If $\chi \notin N^{\perp}$, it is obvious that χ is principal on exactly one $D_{i_1,i_2,\dots,i_t}$ and hence exactly one $|\chi(Q_{i_1,i_2,\dots,i_t})|$ has the value p^c while all the others are zero. If $\chi \in N^{\perp}$, then $\chi(Q_{i_1,i_2,\dots,i_t}) = p^{e-1}\chi(H)$. Hence Equations (3) and (4) follow. Finally, we want to point out that similar generalizations can also be applied to other constructions in this paper.

THEOREM 2.2 *Let p be a prime. Let G be an abelian group of order p^{2c+1}, which contains a subgroup $E = \langle\alpha\rangle \times H$ where $|H| = p^{c+1}$ and $\exp(H) = o(\alpha) \leq p^c$, and let N be any subgroup of H of order p. Then there exists a $(p^{2c}, p, p^{2c}, p^{2c-1})$-RDS in G relative to N.*

Proof. Define an equivalence relation on G^* by

$$\chi \sim \chi' \quad \text{if and only if} \quad \ker \chi|_H = \ker \chi'|_H.$$

Let $[\chi_1], [\chi_2], \dots, [\chi_n]$ be the equivalence classes with $\chi_i \notin N^{\perp}$. Let $K_t = \ker \chi_t|_H$.

For each $t \in \{1, 2, \dots, n\}$, let h_t, y_t, z_t be elements with $h_t \in H\backslash K_t$ and $y_t, z_t \in G\backslash H$, let $p^{s_t} = p^c/|K_t|$ $(= o(\chi_t|_H)/p)$ and define a $p^{s_t} \times p^{s_t}$ matrix $M_t = (m^{(t)}_{ij})$ by $m^{(t)}_{ij} = y_t z_t^j h_t^{i-(pi+1)j}$ for $i, j = 0, 1, \dots, p^{s_t} - 1$. Suppose the matrices M_t satisfy the following conditions:

(A) If $\chi \in (K_t^{\perp} \cap N^{\perp})\backslash[\chi_0]$, where χ_0 is the principal character of G, then the sum of the values of χ on any column of M_t is 0.

(B) If $\chi \in [\chi_t]$, then the sum of the values of χ on any row of M_t is 0 except for one row, which depends on χ, where the sum has absolute value p^{s_t}.

(C) The set $\{y_t z_t^j : 0 \leq j \leq p^{s_t} - 1 \text{ and } 1 \leq t \leq n\}$ forms a complete system of distinct coset representatives of H in G.

Let

$$R = \bigcup_{t=1}^{n} \bigcup_{i,j=0}^{p^{s_t}-1} m^{(t)}_{ij} K_t.$$

Then $|R| = \sum_{t=1}^{n} p^{2s_t}|K_t| = p^c \sum_{t=1}^{n} p^{s_t} = p^{2c}$ since $|\{y_t z_t^j : 0 \leq j \leq p^{s_t} - 1 \text{ and } 1 \leq t \leq n\}| = p^c$. Let χ be a nonprincipal character of G. If $\chi \in H^{\perp}$, then $\chi(R) = 0$ because of (C). If $\chi \in N^{\perp}\backslash H^{\perp}$, then $\chi(R) = 0$ because of (A). If $\chi \notin N^{\perp}$, then $|\chi(R)| = p^c$ because of (A) and (B). Hence R is a $(p^{2c}, p, p^{2c}, p^{2c-1})$-RDS in G relative to N.

Now, it remains to show that h_t, y_t, z_t can be chosen in the way that the matrices M_t satisfy the conditions (A), (B) and (C):

(i) $h_t \in H\backslash K_t$ is chosen so that $H/K_t = \langle h_t K_t\rangle$.

(ii) $z_t = h_t \alpha^{p^{e-s_t}}$ where $p^e = o(\alpha)$.

(iii) Let $\gamma_1, \gamma_2, \dots, \gamma_f$ be distinct coset representatives of E in G where $f = p^{c-e}$. Also, assume $s_1, s_2, \dots, s_n$ are in descending order. Choose y_t by the following algorithm:

Step1. Let $\mathcal{L}$ be an $f \times p^e$ matrix of integers, each row of which contains the integers from 0 to $p^e - 1$ in order, all initially unmarked.

Step2. Let $t = 1$.

Step3. Let d_t be an unmarked entry of $\mathcal{L}$. Mark out all entries in that row of the form $d_t + kp^{e-s_t} \bmod p^e$ for $0 \le k \le p^{s_t} - 1$. Call the row where d_t lies r_t.

Step4. Let $y_t = \gamma_{r_t}\alpha^{d_t}$.

Step5. Increase the value of t by 1. Stop if $t > n$; otherwise, go to step 3.

Following the same argument as [16], it is not hard to see that these h_t, y_t, z_t satisfy our requirements. ∎

THEOREM 2.3 *Let p be a prime. Let $G = \langle\alpha\rangle \times B$ be an abelian group of order p^{2c+1}, where B contains a subgroup H of order p^c with $\exp(H) < o(\alpha) \le p^{c+1}$, and let N be a subgroup of H of order p. If there exists a $(p^{2c-2}, p, p^{2c-2}, p^{2c-3})$-RDS in $\langle\alpha^{p^2}\rangle \times B$ relative to N, then there exists a $(p^{2c}, p, p^{2c}, p^{2c-1})$-RDS in G relative to N.*

Proof. Let R_0 be a $(p^{2c-2}, p, p^{2c-2}, p^{2c-3})$-RDS in $\langle\alpha^{p^2}\rangle \times B$ relative to N. Let $o(\alpha) = p^e$. Define

$$R_1 = \{\alpha^{ip}\gamma : 0 \le i < p^{e-2}, \gamma \in B \text{ and } \alpha^{ip^2}\gamma \in R_0\}.$$

Let $H = \bigotimes_{j=1}^{t}\langle\beta_j\rangle$ where $o(\beta_j) = p^{b_j}$ and $N = \langle\beta_1^{p^{b_1-1}}\rangle$. Suppose $b_s = \max_{1\le j\le t} b_j$. For $0 \le i_j \le p^{b_j} - 1$, $1 \le j \le t$, and $(i_1, p) = 1$, define

$$D_{i_1,i_2,\dots,i_t} = \bigotimes_{j=1}^{t}\langle\beta_j\alpha^{i_j p^{e-b_j}}\rangle \subset \langle\alpha^{p^{e-b_s}}\rangle \times H$$

and choose $g_{i_1,i_2,\dots,i_t} \in G$ so that

$$\{g_{i_1,i_2,\dots,i_t} : 0 \le i_k \le p^{b_k} - 1 \text{ for } 1 \le k \le t, (i_1, p) = 1 \text{ and } 0 \le i_s \le p - 1\}$$

is a system of distinct coset representatives of $\langle\alpha^{p^{e-b_s}}\rangle \times H$ in $G\backslash(\langle\alpha^p\rangle \times B)$ and

$$g_{i_1,i_2,\dots,i_t} = \alpha^{mp^{e-b_s}} g_{i_1,i_2,\dots,i_{s-1},n,i_{s+1},\dots,i_t}$$

for $i_s = pm + n$ where $0 \le n \le p - 1$. Then

$$R = \bigcup_{0\le i_1\le p^{b_1}-1,\,(i_1,p)=1}\ \bigcup_{i_2=0}^{p^{b_2}-1}\cdots\bigcup_{i_t=0}^{p^{b_t}-1} D_{i_1,i_2,\dots,i_t} g_{i_1,i_2,\dots,i_t} \cup \langle\alpha^{p^{e-1}}\rangle R_1$$

is a $(p^{2c}, p, p^{2c}, p^{2c-1})$-RDS in G relative to N. The proof is similar to Theorem 2.1. ∎

Combining Theorems 2.1, 2.2 and 2.3, we have a necessary and sufficient conditions for the existence of $(p^{2c}, p, p^{2c}, p^{2c-1})$-RDSs.

THEOREM 2.4 *Let p be a prime. Let G be an abelian group of order p^{2c+1} and N a subgroup of G of order p. Then there exists a $(p^{2c}, p, p^{2c}, p^{2c-1})$-RDS in G relative to N if and only if* $\exp(G) \leq p^{c+1}$.

Proof. The necessary part follows by Theorem 1.1. For the sufficient part, Theorems 2.1 and 2.2 provide the constructions of all the required RDSs except when $G \cong \langle\alpha\rangle \times B$ where $o(\alpha) = p^{c+1}$ and $N < B$. But the existence of these RDSs can be shown inductively by applying Theorem 2.3. ∎

3. $(p^{2c}, p, p^{2c}, p^{2c-1})$-RDSs in Abelian Groups of Exponent p^{c+1}

In Section 2, we have studied the constructions of $(p^{2c}, p, p^{2c}, p^{2c-1})$-RDSs. In this section, we shall work on the special case that the abelian groups have exponent p^{c+1}. For this case, we have detailed knowledge of the structure of the RDSs. We remark that this is of particular interest for the study of the much more difficult case of $(p^{2c}, p^b, p^{2c}, p^{2c-b})$-RDSs with $b > 1$. As an example, we shall discuss the existence problem of abelian $(16, 4, 16, 4)$-RDSs at the end of this section.

Before we state our main results, we list some useful lemmas.

LEMMA 3.1 (Ma [18]). *Let p be a prime. Let Z be an element in $\mathbb{Z}[G]$ where G is an abelian group with a cyclic Sylow p-subgroup. Let P denote the unique subgroup of G of order p. If $\chi(Z) \equiv 0 \bmod p^a$ for all nonprincipal characters χ of G, then*

$$Z = p^a X + PY$$

where $X, Y \in \mathbb{Z}[G]$. Furthermore, if the coefficients of Z are nonnegative, then X and Y can be chosen to have nonnegative coefficients.

LEMMA 3.2 *Let p be a prime. Let $G = A \times B \times H$ be an abelian group such that $A \cong (\mathbb{Z}_{p^a})^s$, $B = \bigotimes_{j=1}^{t} \langle\beta_j\rangle$, $o(\beta_j) = p^{b_j} \leq p^a$ for $1 \leq j \leq t$, and $(p, |H|) = 1$. Define $e = a(s-1) + \sum_{j=1}^{t} b_j$ and*

$$\mathcal{R} = \{W \times \bigotimes_{j=1}^{t} \langle\beta_j\gamma_j\rangle : W \text{ is a subgroup of } A \text{ of order } p^{a(s-1)} \text{ such that } A/W \text{ is cyclic; and } \gamma_j \in A, o(\gamma_j) \leq p^{b_j}\}.$$

(Note that every element in $\mathcal{R}$ is a subgroup of $A \times B$ of order p^e.) Suppose there exists a subset D of G such that $\chi(D) \equiv 0 \bmod p^e$ for all nonprincipal characters of G. Then

$$D = \sum_{U \in \mathcal{R}} U X_U + KY$$

where $X_U, Y \subset G$ and K is the maximal elementary abelian p-subgroup of A.

Proof. Write $D = \sum_{U \in \mathcal{R}} UX_U + L$ where $X_U, L \subset G$ such that $gU \not\subset L$ for all $g \in G$ and $U \in \mathcal{R}$. We have to show $L \equiv 0 \bmod K$. For any $U \in \mathcal{R}$, let $\rho_U : G \to G/U$ be the canonical epimorphism. Note that the Sylow p-subgroup of G/U is cyclic and

$$\chi(L) = \chi(D) - \sum_{U \in \mathcal{R}} \chi(U)\chi(X_U) \equiv 0 \bmod p^e$$

for all nonprincipal characters of G. By Lemma 3.1,

$$\rho_U(L) = p^e Y_U + P_U Z_U$$

where $Y_U, Z_U \in \mathbb{Z}[G/U]$ with nonnegative coefficients and P_U is the unique subgroup of G/U of order p. By the definition of L, we have $Y_U = 0$. Thus we get

$$UL \equiv 0 \bmod K$$

for all $U \in \mathcal{R}$. Since every element of $T = \{\sigma \in Aut(A \times B) : \sigma(A) = A\}$ permutes $\mathcal{R}$ and all orbits $\neq \{1\}, K\backslash\{1\}$ of T on $A \times B$ are multiples of K, we have

$$\sum_{U \in \mathcal{R}} U \equiv \frac{1}{|T|}\sum_{\sigma \in T}\sum_{U \in \mathcal{R}} U \equiv |\mathcal{R}|e_G - \frac{1}{|K|-1}\sum_{U \in \mathcal{R}} |U \cap (K\backslash\{1\}|e_G \equiv ne_G \bmod K$$

for some positive integer n. Since $\sum_{U \in \mathcal{R}} UL \equiv 0 \bmod K$, we conclude that $L \equiv 0 \bmod K$. ∎

We want to point out that in this paper, we only need the particular version of Lemma 3.2 when $s = 1$ and $H = \{e_G\}$. Since we believe that this lemma is useful in the study of other difference sets, we state it in the most general form. As an example, we give a corollary which provides a generalization of a result of difference sets by Arasu and Sehgal [2]. Since in this paper we are not mainly interested in this subject, we omit the proof. The readers are referred to [15], [17] for the terminology of difference sets used in the corollary.

COROLLARY 3.3 *Let p be a prime. Let $G = A \times B \times H$ be an abelian group where A is a cyclic p-group, $|B| = p^b$, $\exp(B) \leq \exp(A)$ and $(|H|, p) = 1$. Furthermore, assume that D is a (v, k, λ)-difference set in G, $p^{2b} \mid n = k - \lambda$ and p is self-conjugate modulo $\exp(H)$. Let K be the maximal elementary abelian p-subgroup of G and $\rho : G \to G/K$ the canonical epimorphism. Then $\rho(D) \equiv 0 \bmod p$.*

EXAMPLE 3.4 *Corollary 3.3 can be applied together with the sub-difference set argument developed by McFarland [20]. The condition $\rho(D) \equiv 0 \bmod p$ often forces $\rho(D)$ to be two-valued, i.e. the coefficients of $\rho(D)$ take only two integer values. If, for example, p is odd, $|A| = p^b$ and D is a Menon difference set, then by a result of Arasu, Davis and Jedwab [1], B must be cyclic and by Corollary 3.3 and McFarland's argument, every group $G' \cong \mathbb{Z}_{p^c} \times \mathbb{Z}_{p^c} \times H$ with $c \leq b$ also must have a Menon difference set. This result has also been obtained by Davis and Jedwab [9] independently.*

The following is a well-known result of RDSs, e.g. see [19].

LEMMA 3.5 *Let p be a prime. If R is a $(p^{2c}, p, p^{2c}, p^{2c-1})$-RDS in an abelian group G, then $\chi(R) \equiv 0 \bmod p^c$ for all characters χ of G.*

Now, we are ready to state and prove our theorems on the characterization of $(p^{2c}, p, p^{2c}, p^{2c-1})$-RDSs in abelian groups of exponent p^{c+1}.

THEOREM 3.6 *Let p be a prime. Let $G = \langle\alpha\rangle \times \bigotimes_{j=1}^{t}\langle\beta_j\rangle$ be an abelian group where $o(\alpha) = p^{c+1}$, $o(\beta_j) = p^{b_j}$, and $\sum_{j=1}^{t} b_j = c$. Then a subset R of G is a $(p^{2c}, p, p^{2c}, p^{2c-1})$-RDS in G relative to $N = \langle\alpha^{p^c}\rangle$ if and only if*

$$R = \sum_{i_1=0}^{p^{b_1}-1}\sum_{i_2=0}^{p^{b_2}-1}\cdots\sum_{i_t=0}^{p^{b_t}-1}\bigotimes_{j=1}^{t}\langle\beta_j\alpha^{i_j p^{c+1-b_j}}\rangle\alpha^{\varepsilon_{i_1,i_2,\ldots,i_t}},$$

for some integers $\varepsilon_{i_1,i_2,\ldots,i_t}$, and $|R \cap N\gamma| = 1$ for all $\gamma \in G$.

Proof. Let R be a $(p^{2c}, p, p^{2c}, p^{2c-1})$-RDS in G relative to N. By Lemmas 3.2 and 3.5, we can write

$$R = \sum_{i_1=0}^{p^{b_1}-1}\sum_{i_2=0}^{p^{b_2}-1}\cdots\sum_{i_t=0}^{p^{b_t}-1}\bigotimes_{j=1}^{t}\langle\beta_j\alpha^{i_j p^{c+1-b_j}}\rangle X_{i_1,i_2,\ldots,i_t} + NY$$

for some $X_{i_1,i_2,\ldots,i_t}, Y \subset G$. Since $|R \cap N\gamma| = 1$ for all $\gamma \in G$, it is obvious that $Y = \emptyset$. Applying suitable characters that are nonprincipal on N to the equation above yields $|X_{i_1,i_2,\ldots,i_t}| \neq 0$ for all $i_1, i_2, \ldots, i_t$. Since $|R| = p^{2c}$, we have $|X_{i_1,i_2,\ldots,i_t}| = 1$. Hence without loss of generality, we can assume $X_{i_1,i_2,\ldots,i_t} = \{\alpha^{\varepsilon_{i_1,i_2,\ldots,i_t}}\}$ for all $i_1, i_2, \ldots, i_t$. ∎

EXAMPLE 3.7 *Let R be a $(16, 2, 16, 8)$-RDS in $\mathbb{Z}_8 \times \mathbb{Z}_4$ relative to $\langle(4, 0)\rangle$. Then by Theorem 3.6, it is not difficult to see that, up to equivalence,*

$$R = \langle(0, 1)\rangle + \langle(2, 1)\rangle(s_1, 0) + \langle(4, 1)\rangle(2, 0) + \langle(6, 1)\rangle(s_2, 0)$$

where $(s_1, s_2) \in \{(1, 3), (1, 7), (3, 1), (3, 5)\}$.

The following lemma is needed for studying the case when N is not contained in the biggest exponent piece of G.

LEMMA 3.8 (Ma and Pott [19]). *Let p be a prime and G a cyclic group of order p^a. Suppose $Z \in \mathbb{Z}[G]$ such that $|\chi(Z)| = 1$ for a character χ of G of order p^a. Then*

$$Z = \pm g + PY$$

for some $g \in G$ and $Y \in \mathbb{Z}[G]$ where P is the unique subgroup of G of order p.

THEOREM 3.9 *Let p be a prime. Let $G = \langle\alpha\rangle \times \bigotimes_{j=1}^{t}\langle\beta_j\rangle$ be an abelian group where $o(\alpha) = p^{c+1}$, $o(\beta_j) = p^{b_j}$, and $\sum_{j=1}^{t} b_j = c$. If a subset R of G is a $(p^{2c}, p, p^{2c}, p^{2c-1})$-RDS in G relative to $N = \langle\beta_1^{p^{b_1-1}}\rangle$, then*

$$R = \sum_{0\le i_1\le p^{b_1}-1,\,(i_1,p)=1}\ \sum_{i_2=0}^{p^{b_2}-1}\cdots\sum_{i_t=0}^{p^{b_t}-1}\bigotimes_{j=1}^{t}\langle\beta_j\alpha^{i_j p^{c+1-b_j}}\rangle\alpha^{\varepsilon_{i_1,i_2,\ldots,i_t}} + \langle\alpha^{p^c}\rangle R_1$$

for some integers $\varepsilon_{i_1,i_2,\ldots,i_t}$ and $R_1 \subset G$ with $|R_1| = p^{2c-2}$.

Proof. Let R be a $(p^{2c}, p, p^{2c}, p^{2c-1})$-RDS in G relative to N. By Lemmas 3.2 and 3.5, we can write

$$R = \sum_{i_1=0}^{p^{b_1}-1}\sum_{i_2=0}^{p^{b_2}-1}\cdots\sum_{i_t=0}^{p^{b_t}-1}\bigotimes_{j=1}^{t}\langle\beta_j\alpha^{i_j p^{c+1-b_j}}\rangle X_{i_1,i_2,\ldots,i_t} + \langle\alpha^{p^c}\rangle R_1$$

for some $X_{i_1,i_2,\ldots,i_t}$, $R_1 \subset G$. Since $|R \cap N\gamma| = 1$ for all $\gamma \in G$, it is obvious that $X_{i_1,i_2,\ldots,i_t} = \emptyset$ if $(i_1, p) \ne 1$.

For any $i_1, i_2, \ldots, i_t$ with $(i_1, p) = 1$, let $\rho : G \to G/U$ be the canonical epimorphism where $U = \bigotimes_{j=1}^{t}\langle\beta_j\alpha^{i_j p^{c+1-b_j}}\rangle$. Let χ be any character of G/U of order p^{c+1}. Since $|\chi(\rho(R))| = p^c$ and $\chi(\langle\alpha^{p^c}\rangle) = 0$, we have $|\chi(\rho(X_{i_1,i_2,\ldots,i_t}))| = 1$. By Lemma 3.8, we have

$$\rho(X_{i_1,i_2,\ldots,i_t}) = \pm g + PY$$

where $g \in G/U$, $Y \in \mathbb{Z}[G/U]$ and P is the unique subgroup of G/U of order p. Taking the inverse image of ρ, we have

$$\bigotimes_{j=1}^{t}\langle\beta_j\alpha^{i_j p^{c+1-b_j}}\rangle X_{i_1,i_2,\ldots,i_t} = \pm\bigotimes_{j=1}^{t}\langle\beta_j\alpha^{i_j p^{c+1-b_j}}\rangle g_1 + MY_1$$

where $g_1 \in G$, $Y_1 \in \mathbb{Z}[G]$ and $M = \rho^{-1}(P) = N\bigotimes_{j=1}^{t}\langle\beta_j\alpha^{i_j p^{c+1-b_j}}\rangle$. Since $|R \cap N\gamma| = 1$ for all $\gamma \in G$, we have $Y_1 = 0$ unless $p = 2$ and $MY_1 = Mg_1$. Both cases imply $|X_{i_1,i_2,\ldots,i_t}| = 1$. Without loss of generality, we can assume $X_{i_1,i_2,\ldots,i_t} = \{\alpha^{\varepsilon_{i_1,i_2,\ldots,i_t}}\}$. ■

EXAMPLE 3.10 *Let R be a $(16, 2, 16, 8)$-RDS in $\mathbb{Z}_8 \times \mathbb{Z}_4$ relative to $N = \langle(0, 2)\rangle$. Then by Theorem 3.9, up to equivalence, $R = \langle(2, 1)\rangle(1, 0) + \langle(6, 1)\rangle(j, 0) + \langle(4, 0)\rangle R_1$ where $j \in \{2, 3\}$.*

First, we show that $j = 2$ is impossible: If $j = 2$, then $R_1/\langle(0, 2)\rangle = \bar{h}_1 + \bar{h}_2 + \bar{h}_3 + \bar{h}_4$ where $h_1 = (3, 0)$, $h_2 = (0, 0)$, $h_3 = (1, 1)$ and $h_4 = (2, 1)$. We define $\varepsilon_i = 1$ if $h_i \in R_1$ and $\varepsilon_i = -1$ if $h_i(0, 2) \in R_1$. Let χ_1, χ_2 be the characters defined by $\chi_1(0, 1) = \chi_2(0, 1) = \sqrt{-1}$, $\chi_1(1, 0) = \sqrt{-1}$ and $\chi_2(1, 0) = -1$. Then

$$\chi_1(R)/2 = -\varepsilon_1\sqrt{-1} + \varepsilon_2 - \varepsilon_3 - \varepsilon_4\sqrt{-1} \quad \textit{and}$$
$$\chi_2(R)/2 = -\varepsilon_1 + \varepsilon_2 - \varepsilon_3\sqrt{-1} + \varepsilon_4\sqrt{-1}.$$

Since $|\chi_1(R)| = |\chi_2(R)| = 4$, *this implies*

$$[(\varepsilon_1 = \varepsilon_4) \wedge (\varepsilon_2 = \varepsilon_3)] \vee [(\varepsilon_1 = -\varepsilon_4) \wedge (\varepsilon_2 = -\varepsilon_3)] \text{ and}$$
$$[(\varepsilon_1 = \varepsilon_2) \wedge (\varepsilon_3 = -\varepsilon_4)] \vee [(\varepsilon_1 = -\varepsilon_2) \wedge (\varepsilon_3 = \varepsilon_4)]$$

which is impossible.

Hence without loss of generality, $R = \langle(2,1)\rangle(1,0) + \langle(6,1)\rangle(3,0) + \langle(4,0)\rangle R_1$. *Let* χ_3 *be the character defined by* $\chi_3(1,0) = -1$ *and* $\chi_3(0,1) = 1$. *Then* $\chi_3(R) = -8 + 2\chi_3(R_1) = 0$. *Thus* $R_1 \subset \ker\chi_3 = \langle(2,0),(1,0)\rangle$. *Hence* $R_1/\langle(4,0)\rangle$ *is a RDS in* $\langle(2,0),(1,0)\rangle/\langle(4,0)\rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_4$ *relative to* $\langle\overline{(0,2)}\rangle$. *By Theorem 3.6,*

$$R_1/\langle(4,0)\rangle = \langle\overline{(2,0)}\rangle\overline{(0,s_1)} + \langle\overline{(2,2)}\rangle\overline{(0,s_2)}$$

where $(s_1,s_2) \in \{(0,1),(0,3),(1,0),(1,2),(2,1),(2,3),(3,0),(3,2)\}$. *So up to equivalence,*

$$R = \langle(2,1)\rangle(1,0) + \langle(6,1)\rangle(3,0) + \langle(4,0)\rangle[(0,s_1) + (2,s_1) + (0,s_2) + (2,s_2+2)].$$

Finally, we show that using our Theorems 3.6 and 3.9 and a lemma by Ma and Pott [19], it is possible to settle the existence problem of abelian $(16,4,16,4)$-RDSs in $G \not\cong \mathbb{Z}_8 \times \mathbb{Z}_4 \times \mathbb{Z}_2$.

Result 3.11. A $(16,4,16,4)$-RDS in an abelian group $G \not\cong \mathbb{Z}_8 \times \mathbb{Z}_4 \times \mathbb{Z}_2$ exists if and only if $\exp(G) \le 4$ or $G = \mathbb{Z}_8 \times (\mathbb{Z}_2)^3$ with $N \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

The case $G \cong \mathbb{Z}_8 \times \mathbb{Z}_4 \times \mathbb{Z}_2$ is not more difficult but it involves too many cases (there are a lot of possibilities for the forbidden subgroup). By some ad hoc calculations, we have the following result (it is clear from our calculations that all the other cases can be treated similarly):

Result 3.12. Let $G = \mathbb{Z}_8 \times \mathbb{Z}_4 \times \mathbb{Z}_2$.
(a) There is a $(16,4,16,4)$-RDS in G relative to $\langle(4,0,0),(0,2,0)\rangle$.
(b) There is no $(16,4,16,4)$-RDS in G relative to $\langle(2,0,0)\rangle$, $\langle(0,1,0)\rangle$, $\langle(4,0,0),(0,0,1)\rangle$ or $\langle(0,2,0),(0,0,1)\rangle$.

For the existence parts of Results 3.11 and 3.12, the $(16,4,16,4)$-RDS in $(\mathbb{Z}_4)^3$ relative to $N \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ is due to Davis and Seghal [10]; and other RDSs whose existence is not previously known are all constructed by lifting suitable $(16,2,16,8)$-RDSs (Result 3.12(a) has also been obtained independently by Davis and Seghal [10]). For the nonexistence parts, it is known that there is no abelian $(16,4,16,4)$-RDS in G if $\exp(G) \ge 32$, see [24]. The nonexistence in the case $\exp(G) = 16$ follows from a theorem by Schmidt [21]. If $\exp(G) = 8$ and there is a cyclic subgroup of order 8 which does not contain the forbidden subgroup, then we can project the RDS to a $(16,2,16,8)$-RDS R' in an abelian group G' with $\exp(G') = 8$. The structure of R' has been determined by Theorems 3.6 and 3.9 and we can use this together with some character arguments to obtain the results mentioned above. If the forbidden subgroup is contained in every cyclic subgroup of order 8, then we use Lemma 4.7 of [19] together with some character arguments. For the details, please see [22].

4. $(2^{2c+1}, 2, 2^{2c+1}, 2^{2c})$-RDSs

Let us consider $(2^{2c+1}, 2, 2^{2c+1}, 2^{2c})$-RDSs. It is interesting that these RDSs are quite different from the RDSs that we have seen in the previous sections. For example, no such RDSs exist in elementary abelian groups. Using the method of Davis [8] and the constructions in Section 2, we have the following three existence theorems. The first one is also an improved version of a result by Davis.

THEOREM 4.1 *Let G be an abelian group of order 2^{2c+2} which contains a subgroup $E = \langle\alpha\rangle \times H$ where $|H| = 2^c$ and $\max\{4, \exp(H)\} = o(\alpha) = 2^e \leq 2^{c+2}$. Then there exists a $(2^{2c+1}, 2, 2^{2c+1}, 2^{2c})$-RDS in G relative to $N = \langle\alpha^{2^{e-1}}\rangle$.*

Proof. Let $H = \bigotimes_{j=1}^{t}\langle\beta_j\rangle$ where $o(\beta_j) = 2^{b_j}$ and $b_1 = \max_{1\leq j\leq t} b_j = 1$ or e. For $0 \leq i_j \leq 2^{b_j} - 1$, $1 \leq j \leq t$, define

$$D_{i_1,i_2,\ldots,i_t} = \bigotimes_{j=1}^{t}\langle\beta_j\alpha^{i_j 2^{e-b_j}}\rangle \cup \alpha^{2^{e-2}} \bigotimes_{j=1}^{t}\langle\beta_j\alpha^{i_j 2^{e-b_j}}\rangle \subset E$$

and choose $g_{i_1,i_2,\ldots,i_t} \in G$ so that
(i) if $b_1 = 1$ (and $e = 2$), then

$$\{g_{i_1,i_2,\ldots,i_t} : 0 \leq i_k \leq 1 \text{ for } 1 \leq k \leq t\}$$

is a system of distinct coset representatives of E in G; and
(ii) if $b_1 = e \geq 2$, then

$$\{g_{i_1,i_2,\ldots,i_t} : 0 \leq i_k \leq 2^{b_k} - 1 \text{ for } 1 \leq k \leq t \text{ and } 0 \leq i_1 \leq 3\}$$

is a system of distinct coset representatives of E in G and

$$g_{i_1,i_2,\ldots,i_t} = \alpha^m g_{n,i_2,\ldots,i_t}$$

for $i_1 = 4m + n$ where $0 \leq n \leq 3$.

Then

$$R = \bigcup_{i_1=0}^{2^{b_1}-1}\bigcup_{i_2=0}^{2^{b_2}-1}\cdots\bigcup_{i_t=0}^{2^{b_t}-1} D_{i_1,i_2,\ldots,i_t} g_{i_1,i_2,\ldots,i_t}.$$

is a $(2^{2c+1}, 2, 2^{2c+1}, 2^{2c})$-RDS in G relative to N. ■

THEOREM 4.2 *Let G be an abelian group of order 2^{2c+2}, which contains a subgroup $E = \langle\alpha\rangle \times H$ where $|H| = 2^{c+2}$ and $4 \leq \exp(H) = o(\alpha) \leq 2^c$, and let $N' = \langle\beta\rangle$ be any cyclic subgroup of H of order 4. Then there exists a $(2^{2c+1}, 2, 2^{2c+1}, 2^{2c})$-RDS in G relative to $N = \langle\beta^2\rangle$.*

Proof. Define an equivalence relation on G^* by

$$\chi \sim \chi' \quad \text{if and only if} \quad \ker \chi|_H = \ker \chi'|_H.$$

Let $[\chi_1], [\chi_2], \ldots, [\chi_n]$ be the equivalence classes with $\chi_i \notin N^\perp$. Let $K_t = \ker \chi_t|_H$. Following the same argument as Theorem 2.2, there exist $h_t \in H\backslash K_t$ and $y_t, z_t \in G\backslash H$, $1 \le t \le n$, such that the $2^{s_t} \times 2^{s_t}$ matrices $M_t = (m_{ij}^{(t)})$, where $2^{s_t} = 2^c/|K_t| (= o(\chi_t|_H)/4)$, defined by $m_{ij}^{(t)} = y_t z_t^j h_t^{i-(4i+1)j}$, for $i, j = 0, 1, \ldots, 2^{s_t} - 1$, satisfy the conditions (B) and (C) of the proof of Theorem 2.2 and the following condition:

(A$'$) If $\chi \in (K_t^\perp \cap N'^\perp)\backslash[\chi_0]$, where χ_0 is the principal character of G, then the sum of the values of χ on any column of M_t is 0.

Then

$$R = \bigcup_{t=1}^{n} \bigcup_{i,j=0}^{2^{s_t}-1} m_{ij}^{(t)}(K_t \cup \beta K_t)$$

is a $(2^{2c+1}, 2, 2^{2c+1}, 2^{2c})$-RDS in G relative to N. ∎

THEOREM 4.3 *Let $G = \langle\alpha\rangle \times B$ be an abelian group of order 2^{2c+2}, where B contains a subgroup H of order 2^c with $4 \le \exp(H) < o(\alpha) \le 2^{c+2}$, and let $N' = \langle\beta\rangle$ be a cyclic subgroup of H of order 4. If there exists a $(2^{2c-1}, 2, 2^{2c-1}, 2^{2c-2})$-RDS in $\langle\alpha^4\rangle \times B$ relative to $N = \langle\beta^2\rangle$, then there exists a $(2^{2c+1}, 2, 2^{2c+1}, 2^{2c})$-RDS in G relative to N.*

Proof. Let R_0 be a $(2^{2c-1}, 2, 2^{2c-1}, 2^{2c-2})$-RDS in $\langle\alpha^4\rangle \times B$ relative to N. Let $o(\alpha) = 2^e$. Define

$$R_1 = \{\alpha^{2i}\gamma : 0 \le i < 2^{e-2}, \gamma \in B \text{ and } \alpha^{4i}\gamma \in R_0\}.$$

Let $H = \bigotimes_{j=1}^{t}\langle\beta_j\rangle$ where $o(\beta_j) = 2^{b_j}$ and $\beta = \beta_1^{2^{b_1-2}}$. Suppose $b_s = \max_{1\le j\le t} b_j$. For $0 \le i_j \le 2^{b_j} - 1$, $1 \le j \le t$, and $(i_1, 2) = 1$, define

$$D_{i_1,i_2,\ldots,i_t} = \bigotimes_{j=1}^{t}\langle\beta_j\alpha^{i_j 2^{e-b_j}}\rangle \cup \beta_1^{2^{b_1-2}} \bigotimes_{j=1}^{t}\langle\beta_j\alpha^{i_j 2^{e-b_j}}\rangle \subset \langle\alpha^{2^{e-b_s}}\rangle \times H$$

and choose $g_{i_1,i_2,\ldots,i_t} \in G$ so that

$$\{g_{i_1,i_2,\ldots,i_t} : 0 \le i_k \le 2^{b_k} - 1 \text{ for } 1 \le k \le t, (i_1, 2) = 1 \text{ and } 0 \le i_s \le 3\}$$

is a system of distinct coset representatives of $\langle\alpha^{2^{e-b_s}}\rangle \times H$ in $G\backslash(\langle\alpha^2\rangle \times B)$ and

$$g_{i_1,i_2,\ldots,i_t} = \alpha^{m2^{e-b_s}} g_{i_1,i_2,\ldots,i_{s-1},n,i_{s+1},\ldots,i_t}$$

for $i_s = 4m + n$ where $0 \leq n \leq 3$. Then

$$R = \bigcup_{0\leq i_1\leq 2^{b_1}-1,\,(i_1,2)=1} \bigcup_{i_2=0}^{2^{b_2}-1} \cdots \bigcup_{i_t=0}^{2^{b_t}-1} D_{i_1,i_2,\ldots,i_t} g_{i_1,i_2,\ldots,i_t} \cup \langle \alpha^{2^{e-1}} \rangle R_1$$

is a $(2^{2c+1}, 2, 2^{2c+1}, 2^{2c})$-RDS in G relative to N. ∎

Combining Theorems 4.1, 4.2 and 4.3, we have a necessary and sufficient condition for the existence of $(2^{2c+1}, 2, 2^{2c+1}, 2^{2c})$-RDSs.

THEOREM 4.4 *Let G be an abelian group of order 2^{2c+2} and N a subgroup of G of order 2. Then there exists a $(2^{2c+1}, 2, 2^{2c+1}, 2^{2c})$-RDS in G relative to N if and only if* $\exp(G) \leq 2^{c+2}$ *and N is contained in a cyclic subgroup of G of order 4.*

Proof. The sufficient part follows by Theorems 4.1, 4.2 and 4.3. For the necessary part, $\exp(G) \leq 2^{c+2}$ follows by Theorem 1.1. Also, by Lemma 3.1 of [8], N must be contained in a larger cyclic subgroup of G. ∎

5. $(p^{2c+1}, p, p^{2c+1}, p^{2c})$-RDSs when p is an Odd Prime

The constructions of $(p^{2c+1}, p, p^{2c+1}, p^{2c})$-RDSs are more difficult than the other cases. By Theorem 1.2, we know that the exponent of an abelian group containing such a RDS cannot exceed p^{c+1}.

The following lemma is a variation of the product construction of Davis [7].

LEMMA 5.1 *Let G be an abelian group, K and N subgroups of G such that $K \cap N = \{e_G\}$, and $\rho : G \to G/K$ the canonical epimorphism. If R_1 is a subset of G of size m_1 such that $\rho(R_1)$ is an $(m_1, n, m_1, m_1/n)$-RDS in G/K relative to $\rho(N)$ and $|\chi(R_1)|^2 = m_1$ for every character $\chi \in G^*\backslash N^\perp$, and R_2 is an $(m_2, n, m_2, m_2/n)$-RDS in $K \times N$ relative to N, then R_1R_2 is an $(m_1m_2,\ n,\ m_1m_2,\ m_1m_2/n)$-RDS in G relative to N.*

Proof. It follows by the character argument. ∎

THEOREM 5.2 *Let p be an odd prime. Let G be an abelian group of order p^{2c+2} which contains a subgroup $E = \langle\alpha_1\rangle \times \langle\alpha_2\rangle \times H$ where $|H| = p^c$, $\exp(H) = o(\alpha_1) = p^e \leq p^{c+1}$ and $o(\alpha_2) = p$. Then there exists a $(p^{2c+1}, p, p^{2c+1}, p^{2c})$-RDS in G relative to $N = \langle\alpha_1^{p^{e-1}}\rangle$.*

Proof. Apply Lemma 5.1 where $K = \langle\alpha_2\rangle$, R_1 is a subset of G of size p^{2c} such that $\rho(R_1)$ is a $(p^{2c}, p, p^{2c}, p^{2c-1})$-RDS constructed in the proof of Theorem 2.1 (using the same H and $\alpha = \alpha_1$), and R_2 is a $(p, p, p, 1)$-RDS in $N \times K$ relative to N. ∎

Similarly, the following theorem is obtained by applying Lemma 5.1 to the construction of Theorem 2.2.

THEOREM 5.3 *Let p be an odd prime. Let G be an abelian group of order p^{2c+2}, which contains a subgroup $E = \langle\alpha_1\rangle \times \langle\alpha_2\rangle \times H$ where $|H| = p^{c+1}$ and $\exp(H) = o(\alpha_1) \leq p^c$ and $o(\alpha_2) = p$, and let N be any subgroup of H of order p. Then there exists a $(p^{2c+1}, p, p^{2c+1}, p^{2c})$-RDS in G relative to N.*

Finally, similar to Theorem 2.3, we have an inductive construction.

THEOREM 5.4 *Let p be an odd prime. Let $G = \langle\alpha_1\rangle \times B$ be an abelian group of order p^{2c+2}, where B contains a subgroup $\langle\alpha_2\rangle \times H$ such that $|H| = p^c$, $\exp(H) < o(\alpha_1) \leq p^{c+1}$ and $o(\alpha_2) = p$, and let N be a subgroup of H of order p. If there exists a $(p^{2c-1}, p, p^{2c-1}, p^{2c-2})$-RDS in $\langle\alpha_1^{p^2}\rangle \times B$ relative to N, then there exists a $(p^{2c+1}, p, p^{2c+1}, p^{2c})$-RDS in G relative to N.*

Proof. Let R_0 be the $(p^{2c-1}, p, p^{2c-1}, p^{2c-2})$-RDS in $\langle\alpha_1^{p^2}\rangle \times B$ relative to N. Let $o(\alpha_1) = p^e$. Define

$$R_1 = \{\alpha_1^{ip}\gamma : 0 \leq i < p^{e-2}, \gamma \in B \text{ and } \alpha_1^{ip^2}\gamma \in R_0\}.$$

Let $H = \bigotimes_{j=1}^{t}\langle\beta_j\rangle$ where $o(\beta_j) = p^{b_j}$ and $N = \langle\beta_1^{p^{b_1-1}}\rangle$. Suppose $b_s = \max_{1\leq j\leq t} b_j$. Let R_2 be a $(p, p, p, 1)$-RDS in $\langle\alpha_2\rangle \times N$ relative to N. For $0 \leq i_j \leq p^{b_j} - 1$, $1 \leq j \leq t$, and $(i_1, p) = 1$, define

$$D_{i_1,i_2,\ldots,i_t} = R_2 \bigotimes_{j=1}^{t}\langle\beta_j\alpha_1^{i_j p^{e-b_j}}\rangle \subset \langle\alpha_1^{p^{e-b_s}}\rangle \times \langle\alpha_2\rangle \times H$$

and choose $g_{i_1,i_2,\ldots,i_t} \in G$ so that

$$\{g_{i_1,i_2,\ldots,i_t} : 0 \leq i_k \leq p^{b_k} - 1 \text{ for } 1 \leq k \leq t, (i_1, p) = 1 \text{ and } 0 \leq i_s \leq p - 1\}$$

is a system of distinct coset representatives of $\langle\alpha_1^{p^{e-b_s}}\rangle \times \langle\alpha_2\rangle \times H$ in $G\backslash(\langle\alpha_1^p\rangle \times B)$ and

$$g_{i_1,i_2,\ldots,i_t} = \alpha_1^{mp^{e-b_s}} g_{i_1,i_2,\ldots,i_{s-1},n,i_{s+1},\ldots,i_t}$$

for $i_s = pm + n$ where $0 \leq n \leq p - 1$. Then

$$R = \bigcup_{0\leq i_1\leq p^{b_1}-1,\,(i_1,p)=1} \bigcup_{i_2=0}^{p^{b_2}-1} \cdots \bigcup_{i_t=0}^{p^{b_t}-1} D_{i_1,i_2,\ldots,i_t} g_{i_1,i_2,\ldots,i_t} \cup \langle\alpha_1^{p^{e-1}}\rangle R_1$$

is a $(p^{2c+1}, p, p^{2c+1}, p^{2c})$-RDS in G relative to N. ■

It is unfortunate that Theorems 5.2, 5.3 and 5.4 cannot cover all the abelian groups of order p^{2c+2} and exponent not exceeding p^{c+1}. For examples, we cannot construct $(p^{2c+1}, p, p^{2c+1}, p^{2c})$-RDSs in the following groups:

(a) $\mathbb{Z}_{p^{c+1}} \times A$ where $|A| = p^{c+1}$ and A does not contain any maximal cyclic subgroup of order p.

(b) $\mathbb{Z}_{p^c} \times B$ where $|B| = p^{c+2}$ and B does not contain any maximal cyclic subgroup of order p or p^2.

References

1. K. T. Arasu, J. A. Davis, and J. Jedwab, A nonexistence result for Menon difference sets using perfect binary array, *Combinatorica*, to appear.
2. K. T. Arasu and S. K. Sehgal, Difference sets in abelian groups of p-rank two, *Designs, Codes and Cryptography*, to appear.
3. B. W. Brock, A new construction of circulant $GH(p^2; \mathbb{Z}_p)$, *Discrete Math.*, Vol. 112 (1993) pp. 249–252.
4. A. T. Butson, Generalized Hadamard matrices, *Proc. Amer. Math. Soc.*, Vol. 13 (1962) pp. 894–898.
5. A. T. Butson, Relations among generalized Hadamard matrices, relative difference sets, and maximal length linear recurring sequences, *Can. J. Math.*, Vol. 15 (1963) pp. 42–48.
6. J. A. Davis, *Difference Sets in Abelian 2-Groups*, Ph.D. Thesis, University of Virginia, 1987.
7. J. A. Davis, A note on products of relative difference sets, *Designs, Codes and Cryptography*, Vol. 1 (1991) pp. 117–119.
8. J. A. Davis, Constructions of relative difference sets in p-groups, *Discrete Math.*, Vol. 103 (1992) pp. 7–15.
9. J. A. Davis and J. Jedwab, Nested Hadamard difference sets, preprint.
10. J. A. Davis and S. K. Seghal, Using the simplex code to construct relative difference sets in 2-groups, preprint.
11. J. F. Dillon, Variations on a scheme of McFarland for noncyclic difference sets, *J. Combin. Theory Ser. A*, Vol. 40 (1985) pp. 9–21.
12. W. de Launey and P. Vijay Kumar, On circulant generalized Hadamard matrices of prime power order, *Designs, Codes and Cryptography*, to appear.
13. J. E. H. Elliott and A. T. Butson, Relative difference sets, *Illinois J. Math.*, Vol. 10 (1966) pp. 517–172.
14. D. Jungnickel, On automorphism groups of divisible designs, *Can. J. Math.*, Vol. 24 (1982) pp. 257–297.
15. D. Jungnickel, Difference sets, in J. H. Dinitz and D. R. Stinson (eds.), *Contemporary Design Theory*, Wiley, New York (1992) 241–324.
16. R. G. Kraemer, Proof of a conjecture on Hadamard 2-groups, *J. Combin. Theory Ser. A*, Vol. 63 (1993) pp. 1–10.
17. E. S. Lander, *Symmetric Designs: An Algebraic Approach*, Cambridge University Press, Cambridge (1983).
18. S. L. Ma, *Polynomial Addition Sets*, Ph.D. Thesis, University of Hong Kong, 1985.
19. S. L. Ma and A. Pott, Relative difference sets, planar functions and generalized Hadamard matrices, *J. Algebra*, to appear.
20. R. L. McFarland, Sub-difference sets of Hadamard difference sets, *J. Combin. Theory Ser. A*, Vol. 54 (1990) pp. 112–122.
21. B. Schmidt, On (p^a, p^b, p^a, p^{a-b})-relative difference sets, preprint.
22. B. Schmidt, Ph.D. thesis, Universität Augsburg, in preparation.
23. A. Pott, On the structure of abelian groups admitting divisible difference sets, *J. Combin. Theory Ser. A*, Vol. 65 (1994) pp. 202–213.
24. A. Pott, A survey on relative difference sets, preprint.