Journal of Algebraic Combinatorics **6** (1997), 279–297

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

BERNHARD SCHMIDT
Mathematisches Institut, Universität Augsburg, Universitätsstr. 15, 86135 Augsburg, Germany

Received October 14, 1994; Revised June 14, 1996

Abstract. This paper provides new exponent and rank conditions for the existence of abelian relative (p^a, p^b, p^a, p^{a-b})-difference sets. It is also shown that no splitting relative $(2^{2c}, 2^d, 2^{2c}, 2^{2c-d})$-difference set exists if $d > c$ and the forbidden subgroup is abelian. Furthermore, abelian relative (16, 4, 16, 4)-difference sets are studied in detail; in particular, it is shown that a relative (16, 4, 16, 4)-difference set in an abelian group $G \ncong \mathbf{Z}_8 \times \mathbf{Z}_4 \times \mathbf{Z}_2$ exists if and only if $\exp(G) \leq 4$ or $G = \mathbf{Z}_8 \times (\mathbf{Z}_2)^3$ with $N \cong \mathbf{Z}_2 \times \mathbf{Z}_2$.

Keywords: relative difference set, exponent bounds, abelian character

1. Introduction

A relative (m, n, k, λ)-difference set (RDS) in a finite group G of order mn relative to a normal subgroup N of order n is a k-subset R of G such that every element of $g \in G \backslash N$ has exactly λ representations $g = r_1 r_2^{-1}$ with $r_1, r_2 \in R$ and no nonidentity element of N has such a representation. The notion of relative difference sets was introduced by Bose [2] and Elliott and Butson [9]. For a detailed survey on RDSs, see [19]. The investigation of relative difference sets is of great interest because of their connection to design theory: Relative difference sets are equivalent to certain divisible designs with point regular automorphism group, see [1]; in particular, certain types of projective planes correspond to relative difference sets (see [19]).

Furthermore, relative difference sets can be used to construct generalized Hadamard matrices and sequences with good autocorrelation properties (see [8] and [19]).

Recently, the research concentrated on RDSs with parameters $(m, n, k, \lambda) = (p^a, p^b, p^a, p^{a-b})$ [3–8, 15, 16]. In his above mentioned survey, Pott says that in his opinion, the existence problem of (p^a, p^b, p^a, p^{a-b})-RDSs is one of the most interesting questions about RDSs. In this paper, we will focus on this problem.

In order to describe RDSs effectively we will use the notation of the group ring $\mathbf{Z}G$. A subset R of G is a relative (m, n, k, λ)-difference set in G relative to N if and only if the equation

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

holds in $\mathbf{Z}G$, where we identify a subset A of G with the element $\sum_{g \in A} g$ in $\mathbf{Z}G$ and write $R^{(-1)} = \{r^{-1} : r \in R\}$.

Two RDSs R, R' in G are called equivalent if there is an automorphism α of G and an element g of G such that $\{\alpha(r)g : r \in R\} = R'$.

It is well-known that, if G is abelian, a k-subset R of G is a relative (m, n, k, λ)-difference set relative to N if and only if

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

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

In the following, we list some results which will be needed in the further sections. Throughout this paper, group homomorphisms will be extendend to the group rings in the natural way. We begin with a well-known lemma.

Lemma 1.1 *Let G be a finite group of order mn, let U be a normal subgroup of order u of G and let $\rho : G \to G/U$ be the canonical epimorhism. If R is an (m, n, k, λ)-RDS in G relative to a normal subgroup N of G, then*

$$\rho(R)\rho(R)^{(-1)} = k + u\lambda(G/U) - |N \cap U|\lambda(NU/U).$$

In particular, if $U \leq N$ then $\rho(R)$ is a $(m, n/u, k, u\lambda)$-RDS in G/U relative to N/U (in this situation we say that R is a **lifting** *of $\rho(R)$).*

Before we can state a very useful result of Turyn we need a definition.

Definition 1.2 Let p be a prime and let m be a positive integer. We write $m = p^a m'$ with $(m', p) = 1)$. We call p **selfconjugate mod m** iff there exists a positive integer i with $p^i \equiv -1 \bmod m'$.

Remark In particular, p is selfconjugate mod p^b for every $b \geq 0$.

Result 1.3 [21] *Let ξ be a complex mth root of unity and let p be a prime which is selfconjugate* mod *m. If $X \in \mathbf{Z}[\xi]$ satisfies*

$$X\bar{X} \equiv 0 \bmod p^{2a}$$

then we have

$$X \equiv 0 \bmod p^a.$$

Result 1.3 is frequently used in connection with Ma's Lemma, which is one of the most important tools in the theory of difference sets and relative difference sets.

Lemma 1.4 (Ma's Lemma [14]) *Let p be a prime and let G be a finite abelian group with a cyclic Sylow p-subgroup. If $Y \in \mathbf{Z}G$ satisfies*

$$\chi(Y) \equiv 0 \bmod p^a$$

for all nontrivial characters χ of G then there exist $X_1, X_2 \in \mathbf{Z}G$ such that

$$Y = p^a X_1 + P X_2,$$

where P is the unique subgroup of order p of G.

Furthermore, if Y has only nonnegative coefficients then X_1 and X_2 can be chosen to have nonnegative coefficients only.

The following lemma due to Ma and Pott [15] has the same goal as Ma's Lemma: Conversion of character equations into equations in $\mathbf{Z}G$.

Lemma 1.5

(a) *Let P be a cyclic group of order p^t where p is a prime. Let P_i be the unique subgroup of order p^i of P $(0 \le i \le t)$. If $A \in \mathbf{Z}P$ satisfies*

$$\chi(A)\overline{\chi(A)} = p^{2a}$$

for all $\chi \in P^* \backslash P_n^{\perp}$ where $1 \le n \le t$ and $n \le a$, then we have

$$A = \sum_{m=0}^{n-1} \epsilon_m (p^{a-m} P_m - p^{a-m-1} P_{m+1}) g_m + P_n Y$$

with $\epsilon_m = \pm 1$, $g_m \in P$ and $Y \in \mathbf{Z}P$.

(b) *Let $G = \langle g \rangle$ be a cyclic group of order 2^t and let G_i be the unique subgroup of order 2^i of G $(0 \le i \le t)$. If $A \in \mathbf{Z}G$ satisfies*

$$\chi(A)\overline{\chi(A)} = 2^{2a+1}$$

for all $\chi \in G^* \backslash G_n^{\perp}$, where $1 \le n \le t-1$ and $n \le a+1$, then we have

$$A = \sum_{m=0}^{n-1} X_m G_m g_m + G_n Y$$

with $g_m \in G$,

$$X_m = 2^{a-m-1}\left(1 + g^{2t-m-2} - g^{2 \cdot 2^{t-m-2}} - g^{3 \cdot 2^{t-m-2}}\right)$$

for $m \le a-1$ and

$$X_a = 1 - g^{t-a-2}.$$

Finally, we recall a well-known theorem of Kronecker.

Result 1.6 (Kronecker) *Let ξ be a complex mth root of unity. If $x \in \mathbf{Z}[\xi]$ has modulus 1 then $x = \pm \xi^i$ for a suitable rational integer i.*

2. Existence results

In this section we summarize the known existence results for (p^a, p^b, p^a, p^{a-b})-RDS. It should be mentioned that for $b = 1$ there are more constructions than in the general case. We refer the reader to Ma and Schmidt [16] where the case $b = 1$ is studied in detail.

Result 2.1 [9]
(a) *Let p be an odd prime and let a, b be positive integers with $a \geq b$. Then there is a (p^a, p^b, p^a, p^{a-b})-RDS in $EA(p^{a+b})$.*
(b) *Let c be a positive integer. Let $G \cong (\mathbf{Z}_4)^c$ and let N be the unique subgroup of G isomorphic to $(\mathbf{Z}_2)^c$. Then there is a $(2^c, 2^c, 2^c, 1)$-RDS in G relative to N.*

Result 2.2 [5] *Let p be a prime and let G be an abelian group of order p^{2c+k} where $k \leq c$. Furthermore, we assume rank$(G) \geq p^{c+k}$. Let N be an arbitrary subgroup of G isomorphic to $(\mathbf{Z}_p)^k$. Then G contains a $(p^{2c}, p^k, p^{2c}, p^{2c-k})$-RDS relative to N.*

Result 2.3 [13] *Let s, d, r, t be positive integers with $r \leq s$ and $t \leq d$. We write $s = ar + b$ where a and b are nonnegative integers with $b < r$. Let p be a prime and let N be an arbitrary (possibly nonabelian) group of order p^t. Then there is a $(p^{2sd}, p^t, p^{2sd}, p^{2sd-t})$-RDS in*

$$(\mathbf{Z}_{p^{a+1}})^{2db} \times (\mathbf{Z}_{p^a})^{2d(r-b)} \times N$$

relative to N.

The following product construction essentially goes back to Davis [4].

Result 2.4 *Let G be a group of order $m_1 m_2 n$. Let H_1 be a subgroup of G and let H_2 and N be normal subgroups of G with $|H_1| = m_1 n$, $|H_2| = m_2 n$, $|N| = n$ and $H_1 \cap H_2 = N$.*
If R_i is an $(m_i, n, m_i, m_i/n)$-RDS in H_i relative to N, $i = 1, 2$, then

$$R_1 R_2 = \{r_1 r_2 : r_1 \in R_1,\ r_2 \in R_2\}$$

is an $(m_1 m_2, n, m_1 m_2, m_1 m_2/n)$-RDS in G relative to N.

3. Exponent bounds

Using the arguments of Turyn [21] one can prove the validity of following the exponent bound.

Result 3.1 [6, 18] *Let G be an abelian group of order p^{a+b} and let N be a subgroup of order p^b of G. A (p^a, p^b, p^a, p^{a-b})-RDS in G relative to N can only exist if*

$$\exp(G) \leq p^{\frac{a+1}{2}} \exp(N).$$

This bound is not entirely satisfactory as it ignores the position of N in the underlying group which sometimes is relevant. With a more detailed analysis we can prove a slightly stronger result.

Theorem 3.2 *Let G be an abelian group of order p^{a+b} and let N be a subgroup of order p^b of G. We write N as direct product of cyclic groups*:

$$N = \langle n_1 \rangle \times \langle n_2 \rangle \times \cdots \times \langle n_t \rangle.$$

Let Z be a cyclic subgroup of G. If $U := Z \cap N \neq 1$, then we write $U = \langle u \rangle$, $|U| = p^y$,

$$u = \prod_{i=1}^{t} \left(n_i^{p^{x_i} a_i}\right)$$

with $(a_i, p) = 1$ and we set $m = \min\{x_i : i = 1, 2, \ldots, t\}$. If G contains a (p^a, p^b, p^a, p^{a-b})-RDS relative to N then
(a) $|Z| \leq p^{\frac{a+3}{2}}$ *if* $Z \cap N = 1$ *and*
(b) $|Z| \leq p^{\frac{a+1}{2}+y+m}$ *if* $Z \cap N \neq 1$.

Proof: Let R be a (p^a, p^b, p^a, p^{a-b})-RDS in G relative to N.

(a) Let $Z \cap N = 1$. By elementary character theory we can choose a character χ of G with $\operatorname{Ker}\chi|_Z = 1$ and $|\operatorname{Ker}\chi|_N| = |N|/p$. We write $K = \operatorname{Ker}\chi$. Let $\rho : g \to G/K$ be the canonical epimorphism. The coefficients of $\rho(R)$ are obviously $\leq |K|/|K \cap N| \leq p^{a+1}/|Z|$. Now the assertion follows from Result 1.3 and Ma's Lemma.
(b) Let $Z \cap N \neq 1$. We choose a character χ' of G with $|\operatorname{Ker}\chi'|_Z| = p^{y-1}$ and $|\operatorname{Ker}\chi'|_N| = |N|/p^{m+1}$. The assertion follows as in (a). □

Example By Theorem 3.2(a) there is no (p^4, p^3, p^4, p)-RDS in $\mathbf{Z}_{p^4} \times N$ relative to N where N is cyclic of order p^3. This RDS can not be excluded by Result 3.1.

Another exponent bound is due to Pott [18] who generalized an ad-hoc argument of Hoffmann [11]:

Result 3.3 *Let G be an abelian group of order p^{a+b} and let N be a subgroup of order p^b of G. If G contains a (p^a, p^b, p^a, p^{a-b})-RDS relative to N then*

$$\exp(G) \leq p^a$$

or $p = 2, a = b = 1$.

Ma and Pott [15] were able to prove the following strong bounds.

Result 3.4 *Let p be a prime.*

(a) *Let G be an abelian group of order p^{2a+b+1} and let N be a subgroup of order p^b of G. If there exists a $(p^{2a+1}, p^b, p^{2a+1}, p^{2a-b+1})$-RDS in G relative to N then*

$$\exp(G) \leq p^{a+1}$$

if p is odd and

$$\exp(N) \leq 2^{a+1}$$

if $p = 2$.

(b) *Let G be an abelian group of order p^{2a+b} and let N be a subgroup of G of order p^b. If there exists a $(p^{2a}, p^b, p^{2a}, p^{2a-b})$-RDS in G relative to N then*

$$\exp(N) \leq p^a.$$

Using the method of Ma and Pott [15] and some additional arguments we can improve Result 3.4(a) for $p = 2$.

Theorem 3.5 *Let G be an abelian group of order 2^{2a+b+1} and let N be a subgroup of order 2^b of G. If G contains a $(2^{2a+1}, 2^b, 2^{2a+1}, 2^{2a-b+1})$-RDS relative to N then*

$$\exp(G) \leq 2^{a+2}.$$

Furthermore, if $\exp(N) < \exp(G)$ then

$$\exp(N) \leq 2^a.$$

Proof: Let R be a $(2^{2a+1}, 2^b, 2^{2a+1}, 2^{2a-b+1})$-RDS relative to N. We write $\exp(G) = 2^t$.

(a) By Result 3.4(a) we have $\exp(N) \leq 2^{a+1}$. We will show that the assumption $\exp(N) = 2^{a+1} < 2^t$ leads to a contradiction proving the second assertion of the Theorem 3.5. Let G' be a cyclic group of order 2^t and let $\rho : G \to G'$ be an epimorphism with $|\rho(N)| = 2^{a+1}$.
Application of Lemma 1.5(b) yields

$$\rho(R) = \sum_{m=0}^{a-1} G_m X_m g_m + \epsilon_a G_a \left(1 - g^{2^{t-a-2}}\right) g_a + G_{a+1} Y$$

using the notation of 1.5(b). Without loss of generality we assume $g_a = 1$. Let χ be a character of G'/G_{a+1}. If we view Y as an element of $\mathbf{Z}(G'/G_{a+1})$ we get

$$\chi(Y) = \begin{cases} 2^a & \text{if } \chi = \chi_0 \\ 0 & \text{if } 2 \leq o(\chi) \leq 2^{t-a-2} \\ -1 & \text{if } o(\chi) = 2^{t-a-1} \end{cases}$$

Hence the coefficient of 1 in Y is

$$2^{-t+a+1}(2^a - 2^{t-a-2}) = 2^{2a+1-t} - \frac{1}{2} \notin \mathbf{Z},$$

a contradiction.

(b) We have to show $\exp(G) \leq 2^{a+2}$. By Result 3.4(a) and part (a) of the proof we can assume $\exp(N) =: 2^n \leq 2^a$. Let G' be a cyclic group of order 2^t and let $\rho : G \to G'$ be an epimorphism with $|\rho(N)| = 2^n$. By Lemma 1.5(b) we get (using the notation of this lemma)

$$\rho(R) = \sum_{m=0}^{n-1} \epsilon_m G_m X_m g_m + G_n Y$$

with

$$X_m = 2^{a-1-m}\left(1 + g^{2^{t-m-2}} - g^{2\cdot 2^{t-m-2}} - g^{3\cdot 2^{t-m-2}}\right)$$

for all m. Since $\chi(Y) = 0$ for all characters χ of G' which are nonprincipal on G_n we infer

$$G_n Y = 2^{2a+1-t} G'.$$

Without loss of generality let $g_0 = 1$. We write

$$\rho(R) = A + B + C$$

with

$$\begin{aligned} A &= 2^{a-1}\left(1 + g^{2^{t-2}} - g^{2\cdot 2^{t-2}} - g^{3\cdot 2^{t-2}}\right) \\ &\quad + 2^{a-2}\left(1 + g^{2^{t-3}} - g^{2\cdot 2^{t-3}} - g^{3\cdot 2^{t-3}}\right), \\ B &= \sum_{m=2}^{n-1} G_m X_m g_m, \\ C &= 2^{2a+1-t} G'. \end{aligned}$$

It is easy to see that we always can find an element of G' whose coefficient in A is less or equal -2^{a-1}. The coefficients of B are less or equal $2^{a-3} + 2^{a-4} + \cdots + 2^{a-n} < 2^{a-2}$. This implies

$$-2^{a-1} + 2^{a-2} + 2^{2a+1-t} > 0,$$

hence $t < a + 3$. □

4. Further exponent and rank conditions

In this section we prove two new nonexistence theorems using the techniqes developed by Ma and Schmidt [16, 17]. To this end we will need the following lemmas contained in [16, 17].

Lemma 4.1 *Let p be a prime, let G be a finite abelian group with Sylow p-subgroup P and let $g_0 \in G$ be an element of order $\exp(P)$. We write $p^c = |P|/\exp(P)$ and $\mathcal{P} = \{U < P : |U| = p^c,\ U \cap \langle g_0 \rangle = 1$ and P/U is cyclic$\}$. Furthermore, we set $U' = \{g : g^{p^s} \in U\}$ for $U \in \mathcal{P}$ where s is a positive integer with $p^s \le \exp(P)$.*

Moreover, we assume that there is a subset D of G such that for every $U \in \mathcal{P}$ and $g \in G$ either

(1) *$|D \cap Uh| \ge \delta$ and $|D \cap (U' \backslash U)h| \le \epsilon$ for a suitable $h \in U'g$ or*

(2) *$|D \cap U'g| \le \epsilon'$*

where $\delta, \epsilon, \epsilon'$, $\delta > \epsilon'$ are fixed positive integers not depending on U. Furthermore, we assume that there is at least one coset $U'g$ satisfying condition (1).

We write $t = rank(P)$, $P = \langle g_0 \rangle \times \langle g_1 \rangle \times \cdots \times \langle g_{t-1} \rangle$ where $o(g_0) = \exp(P)$ and $o(g_i) = p^{a_i}$ for $i = 1, 2, \ldots, t-1$. We set $b_i = \min\{s, a_i\}$. Then

$$\delta - m\epsilon \le p^{c - \sum_{i=1}^{m} b_i}$$

for $m = 1, 2, \ldots, t-1$.

Lemma 4.2 *Let p be a prime and let $G = A \times B \times H$ be an abelian group with $A \cong (\mathrm{Z}_{p^a})^s$, $B = \langle \beta_1 \rangle \times \langle \beta_2 \rangle \times \cdots \times \langle \beta_t \rangle$, $o(\beta_j) = p^{b_j} \le p^a$ for $1 \le j \le t$ and $(p, |H|) = 1$. We set $e = a(s-1) + \sum_{j=1}^{t} b_j$,*

$$\mathcal{P} = \{W \le A : |W| = p^{a(s-1)} \text{ and } A/W \text{ is cyclic}\}$$

and

$$\mathcal{R} = \{W \times \langle \beta_1 \gamma_1 \rangle \times \cdots \times \langle \beta_t \gamma_t \rangle : W \in \mathcal{P}, \gamma_j \in A, o(\gamma_j) \le p^{b_j}\}.$$

If a subset D of G satisfies

$$\chi(D) \equiv 0 \bmod p^e$$

for all nonprincipal characters χ of G then D can be written as

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

with $X_U, Y \subset G$, where K is the unique maximal elementary abelian subgroup of A.

Now we are ready to prove our main theorems.

Theorem 4.3 *Let p be an odd prime, let G be an abelian group of order p^{2a+b} and let N be a subgroup of G of order p^b. Let R be a $(p^{2a}, p^b, p^{2a}, p^{2a-b})$-RDS in G relative to N. Furthermore, we assume that G contains an element g_0 of order p^{a+r+2} $(r \geq 0)$. We write G as a direct product of cyclic groups*:

$$G = \langle g_0 \rangle \times \langle g_1 \rangle \times \cdots \times \langle g_{t-1} \rangle$$

with $o(g_i) = p^{a_i}$ for $i = 1, 2, \ldots, t-1$. We set

$$b_i^{(s)} = \min\{a_i, s\}$$

for $s = 1, 2, \ldots, r+1$, $i = 1, 2, \ldots, t-1$ and

$$p^y = \max\left\{ \frac{|N|}{|U \cap N|} : U \leq G, |U| = p^{a+b-r-2}, U \cap \langle g_0 \rangle = 1, G/U \cong \mathbf{Z}_{p^{a+r+2}} \right\}$$

(*note that by Result* 3.4(b) $p^y \leq \exp(N) \leq p^a$). *Then*

$$p^a - m(p^s - 1)(p^{a-r-2} - p^{a-y}) \leq p^{a+b-r-2-\sum_{i=1}^{m} b_i^{(s)}}$$

for $s = 1, 2, \ldots, r+1$ and $m = 1, 2, \ldots, t-1$.

Proof: Let U be an arbitrary subgroup of order $p^{a+b-r-2}$ of G such that G/U is cyclic and $U \cap \langle g_0 \rangle = 1$. From Theorem 3.2(a) it is clear that $N \not\leq U$. Let $\rho : G \to G/U$ be the canonical epimorphism. By Result 1.3 and Ma's Lemma $\rho(R)$ must have at least one coefficient greater or equal p^a. On the other hand, the coefficients of $\rho(R)$ are obviously less or equal $|U|/|U \cap N|$. This implies $p^a \leq |U|/|U \cap N|$, and hence we have

$$|\rho(N)| = \frac{|N|}{|U \cap N|} \geq \frac{p^a |N|}{|U|} = p^{r+2}.$$

We write $|\rho(N)| = p^x$ with $x \geq r+2$. By Result 3.4(b) we can assume $x \leq a$. By Lemma 1.5(a) we get (using the notation of this lemma)

$$\rho(R) = \sum_{m=0}^{x-1} \epsilon_m p^{a-m-1}(pP_m - P_{m+1})g_m + p^{a-r-2} P_{a+r+2}. \tag{1}$$

We claim

$$\epsilon_0 = \epsilon_1 = \cdots = \epsilon_{r+1} = 1 \quad \text{and} \quad P_i g_0 = P_i g_i \tag{2}$$

for $i = 0, 1, \ldots, r+1$.
We prove (2) by induction. For $g \in G/U$ let $C(g)$ be the coefficient of g in $\rho(R)$.

(a) We assume $\epsilon_0 = -1$. Then by (1) (recall that $p \neq 2$)

$$\begin{aligned} C(g_0) &\leq -p^a + p^{a-1} + p^{a-1} - p^{a-2} + p^{a-2} + - \cdots + p^{a-x+1} - p^{a-x} + p^{a-r-2} \\ &= -p^a + 2p^{a-1} - p^{a-x} + p^{a-r-2} < 0, \end{aligned}$$

a contradiction. Hence $\epsilon_0 = 1$.

(b) Let $1 \leq l \leq r+1$, $\epsilon_0 = \epsilon_1 = \cdots = \epsilon_{l-1} = 1$ and $P_i g_0 = P_i g_i$ for $i = 0, 1, \ldots, l-1$. We have to show $\epsilon_l = 1$ and $P_l g_0 = P_l g_l$. From (1) we have

$$\rho(R) = (p^a - p^{a-l} P_l) g_0 + \sum_{m=l}^{x-1} \epsilon_m p^{a-m-1} (p P_m - P_{m+1}) g_m + p^{a-r-2} P_{a+r+2}.$$

Let $g' \in P_l g_0 \backslash \{g_0\}$. If $\epsilon_l = -1$ or $P_l g_0 \neq P_l g_l$, then

$$\begin{aligned} C(g') &\leq -p^{a-l} + p^{a-l-1} + p^{a-l-1} - p^{a-l-2} + - \cdots + p^{a-x+1} - p^{a-x} + p^{a-r-2} \\ &= -p^{a-l} + 2p^{a-l-1} - p^{a-x} + p^{a-r-2} < 0, \end{aligned}$$

a contradiction. Thus we have proved (2). Hence we get

$$\rho(R) = (p^a - p^{a-r-2} P_{r+2}) g_0 + \sum_{m=r+2}^{x-1} \epsilon_m p^{a-m-1} (p P_m - P_{m+1}) g_m + p^{a-r-2} P_{a+r+2}$$

from (1). We infer

$$\begin{aligned} C(g_o) &\geq p^a - p^{a-r-2} + p^{a-r-3} - p^{a-r-3} + - \cdots - p^{a-x+1} + p^{a-x} \\ &= p^a - p^{a-r-2} + p^{a-x}, \\ C(h) &\leq -p^{a-r-2} + p^{a-r-2} - p^{a-r-3} + - \cdots + p^{a-x+1} - p^{a-x} + p^{a-r-2} \\ &= p^{a-r-2} - p^{a-x} \end{aligned}$$

for $h \in P_{r+2} g_0 \backslash \{g_0\}$ and

$$\begin{aligned} C(h') &\leq p^{a-r-2} - p^{a-r-3} + p^{a-r-3} - + \cdots + p^{a-x+1} - p^{a-x} + p^{a-r-2} \\ &= 2p^{a-r-2} - p^{a-x} \end{aligned}$$

for $h' \in (G/U) \backslash P_{r+2} g_0$. As $\rho(R)$ has at least one coefficient greater or equal to p^a we get $C(g_0) \geq p^a$. Now we apply Lemma 4.1 with

$$\begin{aligned} \delta &= p^a, \\ \epsilon &= (p^s - 1)(p^{a-r-2} - p^{a-y}), \\ \epsilon' &= p^s (2p^{a-r-2} - p^{a-y}) \end{aligned}$$

proving the theorem. □

The following theorem deals with an extreme case of Theorem 3.2.

Theorem 4.4 *Let G be an abelian group of order p^{2a+b} and let N be a subgroup of order p^b of G. We write N as a direct product of cyclic groups*:

$$N = \langle n_1 \rangle \times \langle n_2 \rangle \times \cdots \times \langle n_s \rangle.$$

Let Z be a cyclic subgroup of G with $U := Z \cap N \neq 1$. We write $U = \langle u \rangle$, $|U| = p^y$,

$$u = \prod_{i=1}^{t} \left(n_i^{p^{x_i} a_i}\right)$$

with $(a_i, p) = 1$ and we set $m = \min\{x_i : o(n_i^{p^{x_i}}) \geq p^y\}$.
If G contains a $(p^{2a}, p^b, p^{2a}, p^{2a-b})$-RDS relative to N and if

$$|Z| = p^{a+y+m},$$

then $y = 1$ and $m = 0$.

Proof: Without loss of generality let $a \geq 2$. By elementary character theory we can choose a character χ of G with $\operatorname{Kern} \chi|_Z = 1$ and $|\operatorname{Kern} \chi|_N| = p^{b-y-m}$. We set $K = \operatorname{Kern} \chi|_N$. Let $\rho : G \to G/K$ be the canonical epimorphism. We write $\bar{R} = \rho(R)$, $\bar{G} = \rho(G)$, $\bar{Z} = \rho(Z)$ and $\bar{N} = \rho(N)$. Then $\bar{R}$ is a $(p^{2a}, p^{y+m}, p^{2a}, p^{2a-y-m})$-RDS in $\bar{G}$ relative to $\bar{N}$. We write

$$\bar{G} = \langle g_0 \rangle \times \langle g_1 \rangle \times \cdots \times \langle g_t \rangle.$$

with $o(g_0) = p^{a+y+m}$, $\langle g_o \rangle = \bar{Z}$ and $o(g_i) = p^{a_i}$ for $i = 1, 2, \ldots, t$. By Result 1.3 and Lemma 4.2 we get

$$\bar{R} = \sum_{i_1=0}^{p^{a_1}-1} \sum_{i_2=0}^{p^{a_2}-1} \cdots \sum_{i_t=0}^{p^{a_t}-1} \left(\bigotimes_{l=1}^{t} \left\langle g_l g_0^{i_l p^{a+y+m-a_l}} \right\rangle \right) X_{i_1,i_2,\ldots,i_t} + \left\langle g_0^{p^{a+y+m-1}} \right\rangle Y$$

($\bigotimes$ denotes the internal direct product) for suitable Y, $X_{i_1,i_2,\ldots,i_t} \subset \bar{G}$. Let η be a primitive complex p^{a+y+m}th root of unity. Let $\chi_{i_1,i_2,\ldots,i_t}$ be the characters defined by

$$\chi_{i_1,i_2,\ldots,i_t}(g_0) = \eta$$

and

$$\chi_{i_1,i_2,\ldots,i_t}(g_l) = \eta^{-i_l p^{a+y+m-a_l}}.$$

Since $\bar{N} \not\subset \bigotimes_{l=1}^{t} \langle g_l g_0^{i_l p^{a+y+m-a_l}} \rangle$ we have

$$p^a = |\chi_{i_1,i_2,\ldots,i_t}(\bar{R})| = p^a |\chi_{i_1,i_2,\ldots,i_t}(X_{i_1,i_2,\ldots,i_t})|. \tag{3}$$

This implies $|X_{i_1,i_2,\ldots,i_t}| = 1$ for all $i_1, i_2, \ldots, i_t$ and $Y = 0$. Hence we have

$$\bar{R} = \sum_{i_1=0}^{p^{a_1}-1} \sum_{i_2=0}^{p^{a_2}-1} \cdots \sum_{i_t=0}^{p^{a_t}-1} \left(\bigotimes_{l=1}^{t} \left\langle g_l g_0^{i_l p^{a+y+m-a_l}} \right\rangle \right) g_0^{\epsilon_{i_1,i_2,\ldots,i_t}} \tag{4}$$

with suitable integers $\epsilon_{i_1,i_2,\ldots,i_t}$.
Let $\chi_{j_0,j_1,\ldots,j_t}$ be the characters defined by

$$\chi_{j_0,j_1,\ldots,j_t}(g_0) = \eta^{j_0 p}$$

and

$$\chi_{j_0,j_1,\ldots,j_t}(g_l) = \eta^{j_l p^{a+y+m-a_l}}$$

for $j_0 = 0, 1, \ldots, p^{a+y+m-1} - 1$ and $j_l = 0, 1, \ldots, p^{a_l} - 1$. Obviously, we have $\chi_{j_0,j_1,\ldots,j_t}(\bar{R}) = 0$, if $(j_l, p) = 1$ for at least one $l \geq 1$. Hence

$$|N^{\perp}| = p^{2a} > p^{a+y+m-1}(p-1)p^{a-1} = (p-1)p^{2a+y+m-2} \tag{5}$$

if $t > 1$. If $t = 1$, then there surely exists a character χ apart from the characters $\chi_{j_0,j_1,\ldots,j_t}$ with $\chi(R) = 0$ (recall $a > 1$). Thus (5) holds in every case. Hence $y + m = 1$ which implies $y = 1$ and $m = 0$. □

Corollary 4.5 *A $(p^{2a}, p^b, p^{2a}, p^{2a-b})$-RDS in an abelian group G of exponent p^{a+b} exists if and only if $b = 1$.*

Proof: For $b > 1$ the assertion follows from Theorem 3.2 and Theorem 4.4, and for $b = 1$ it is contained in Theorem 2.4 of Ma and Schmidt [16]. □

5. $(2^{2a}, 2^b, 2^{2a}, 2^{2a-b})$-RDSs with b > a are special

By Result 2.2 a $(2^{2a}, 2^b, 2^{2a}, 2^{2a-b})$-RDS in an abelian group G exists if $b \leq a$ and $\text{rank}(G) \geq 2^{a+b}$. Let us compare this with the following remarkable result is due to Ganley [10] (for a short proof we refer the reader to Jungnickel [12]).

Result 5.1 *Let G be an abelian group of order 2^{2c} and let N be a subgroup of order 2^c of G. A $(2^c, 2^c, 2^c, 1)$-RDS in G relative to N exists if and only if G is isomorphic to $(\mathbf{Z}_4)^c$ and N is isomorphic to $(\mathbf{Z}_2)^c$.*

Something must have happened with the $(2^{2a}, 2^b, 2^{2a}, 2^{2a-b})$-RDS "on the way" from $b = a$ to $b = 2a$. Our next theorem shows what happens and where it happens.

Theorem 5.2 *Let H be an arbitrary (possibly nonabelian) group of order 2^{2a} and let N be an abelian group of order 2^{a+1}. Then the group $G = H \times N$ cannot contain a $(2^{2a}, 2^{a+1}, 2^{2a}, 2^{a-1})$-RDS relative to N.*

Proof: Let R be a $(2^{2a}, 2^{a+1}, 2^{2a}, 2^{a-1})$-RDS in G relative to N. We write $\exp(N) = 2^e$. Let $\rho : G \to G/H$ the canonical epimorphism. We write $\bar{R} = \rho(R)$ and $\bar{N} = \rho(N)$. Let ξ a primitive complex 2^eth root of unity. By Result 1.3 and Result 1.6 we have

$$\chi(\bar{R}) \in \{2^a \xi^i : i = 0, 1, \ldots, 2^e - 1\}$$

for all $\chi \in \bar{N}^* \backslash \{\chi_0\}$, where χ_0 is the principal character of $\bar{N}$. Furthermore, $\chi_0(\bar{R}) = 2^{2a}$. We set

$$T = \{\chi \in \bar{N}^* : \chi(\bar{R}) \notin Z\}.$$

Since the minimum polynomial of ξ is $x^{2^{e-1}} + 1$ and

$$\sum_{\chi \in \bar{N}^*} \chi(\bar{R}) \in \mathbf{Z},$$

we conclude $|T| \equiv 0 \bmod 2$ and $\sum_{\chi \in T} \chi(\bar{R}) = 0$. This implies

$$\begin{aligned} \sum_{\chi \in \bar{N}^*} \chi(\bar{R}) &= 2^{2a} + \sum_{\substack{\chi \in \bar{N}^* \backslash T \\ \chi \neq \chi_0}} \chi(\bar{R}) \\ &\equiv 2^a \bmod 2^{a+1}. \end{aligned}$$

However, by the Fourier inversion formula this is impossible as the coefficient of 1 in $\bar{R}$ is an integer. □

6. (16, 4, 16, 4)-RDSs: An unimaginative approach

This section is designed to stress our ignorance about (p^a, p^b, p^a, p^{a-b})-RDS with $b > 1$. We will see that even the smallest interesting case, i.e., $p = 2$, $a = 4$ and $b = 2$, requires a lot of work. First of all, we summarize what we know about (16, 4, 16, 4)-RDS from the previous sections.

Theorem 6.1
(a) *There is no* (16, 4, 16, 4)*-RDS in any abelian group of exponent* ≥ 16.
(b) *The groups* $(\mathbf{Z}_2)^6$ *and* $\mathbf{Z}_4 \times (\mathbf{Z}_2)^4$ *contain* (16, 4, 16, 4)*-RDS for all possible N.*
(c) *The groups* $(\mathbf{Z}_4)^2 \times (\mathbf{Z}_2)^2$ *and* $\mathbf{Z}_8 \times (\mathbf{Z}_2)^3$ *contain* (16, 4, 16, 4)*-RDS for all* $N \cong \mathbf{Z}_2 \times \mathbf{Z}_2$.

Proof: Part (a) follows from Result 3.1 and Corollary 4.5.
The parts (b) and (c) follow from the Results 2.2 and 2.3. □

There is one further result due to Davis and Seghal [7]:

Result 6.2 *There is a* $(16, 4, 16, 4)$*-RDS in* $(\mathbf{Z}_4)^3$ *for all* $N \cong \mathbf{Z}_2 \times \mathbf{Z}_2$.

Nevertheless, it is clear that we are still far away from having a necessary and sufficient condition for the existence of abelian $(16, 4, 16, 4)$-RDSs. In the following we will prove some interesting new results on these RDSs using the "lifting-method": By the results of Ma and Schmidt [16] we can determine the structure of $(16, 2, 16, 4)$-RDSs in abelian groups of exponent 8 completely; using some character arguments we will decide if a lifting of such an RDS to a $(16, 4, 16, 4)$-RDS is possible. In the case of $(16, 4, 16, 4)$-RDSs in abelian groups of exponent 8 which can **not** be projected down to a $(16, 2, 16, 4)$-RDS in an abelian group of exponent 8, we will have to use Lemma 1.5.

We begin with the characterisation of some $(16, 2, 16, 4)$-RDSs. For the proof of Theorem 6.3 and Theorem 6.4 see Example 3.7 and Example 3.10 of Ma and Schmidt [16].

Theorem 6.3 *Let R be a* $(16, 2, 16, 8)$*-RDS in* $G = \mathbf{Z}_8 \times \mathbf{Z}_4$ *relative to* $N = \langle(0, 2)\rangle$. *Then* (*up to equivalence*)

$$R = \langle(2, 1)\rangle(1, 0) + \langle(6, 1)\rangle(3, 0) + \langle(4, 0)\rangle[(0, i_1) + (2, i_1) + (0, i_2) + (2, i_2 + 2)]$$

where $(i_1, i_2) \in \{(0, 1), (0, 3), (1, 0), (1, 2), (2, 1), (2, 3), (3, 0), (3, 2)\}$.
Conversely, each of the sets R defined above is a $(16, 2, 16, 8)$*-RDS in G relative to N.*

Theorem 6.4 *Let R be a* $(16, 2, 16, 8)$*-RDS in* $G = \mathbf{Z}_8 \times \mathbf{Z}_4$ *relative to* $N = \langle(4, 0)\rangle$. *Then* (*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 $(s_1, s_2) \in \{(1, 3), (1, 7), (3, 1), (3, 5)\}$.
Conversely, each of the sets R defined above is a $(16, 2, 16, 8)$*-RDS in G relative to N.*

Theorem 6.5 *Let R be a* $(16, 2, 16, 8)$*-RDS in* $G = \mathbf{Z}_8 \times \mathbf{Z}_2 \times \mathbf{Z}_2$ *relative to* $N = \langle(0, 1, 0)\rangle$. *Then* (*up to equivalence*)

$$R = \langle(4, 1, 0), (0, 0, 1)\rangle + \langle(4, 1, 0), (4, 0, 1)\rangle(y, 0, 0) + \langle(4, 0, 0)\rangle R_0$$

where either $y = 1$ *and*

$$R_0 = g_1(2, 0, 0) + g_2(2, 0, 1) + g_3(3, 0, 0) + g_4(3, 0, 1)$$

or $y = 2$ *and*

$$R_0 = g_1(1, 0, 0) + g_2(1, 0, 1) + g_3(3, 0, 0) + g_4(3, 0, 1)$$

with $g_i \in N$, where exactly one element or exactly three elements of the multiset $\{g_1, g_2, g_3, g_4\}$ are equal to $(0, 0, 0)$.
Conversely, each of the sets R defined above is a $(16, 2, 16, 8)$*-RDS in G relative to N.*

Proof: By Theorem 3.9 of Ma and Schmidt [16] we have

$$R = \langle (4, 1, 0), (0, 0, 1)\rangle(x, 0, 0) + \langle (4, 1, 0), (4, 0, 1)\rangle(y, 0, 0) + \langle (4, 0, 0)\rangle R_0,$$

where x and y are integers and R_0 is a 4-element subset of G. Considering some automorphisms and translates, we obviously can assume $x = 0$ and $y \in \{1, 2\}$. If $y = 1$ then w.l.o.g.

$$R_0 = g_1(2, 0, 0) + g_2(2, 0, 1) + g_3(3, 0, 0) + g_4(3, 0, 1)$$

where $g_i \in N$, and it is easy to see that R is a $(16, 2, 16, 8)$-RDS in G relative to N if and only if the condition given in the theorem is satisfied.

Similarly we settle the case $y = 2$. □

Theorem 6.6 *Let R be a* $(16, 2, 16, 8)$*-RDS in* $G = \mathbf{Z}_8 \times \mathbf{Z}_2 \times \mathbf{Z}_2$ *relative to* $N = \langle (4, 0, 0)\rangle$. *Then* (*up to equivalence*)

$$\begin{aligned} R = {} & \langle (0, 1, 0), (0, 0, 1)\rangle + \langle (0, 1, 0), (4, 1, 0)\rangle(x_1, 0, 0) \\ & + \langle (4, 1, 0), (0, 0, 1)\rangle(x_2, 0, 0) + \langle (4, 1, 0), (4, 0, 1)\rangle(x_3, 0, 0) \end{aligned}$$

where (x_1, x_2, x_3) *is from*

$$\{(1, 2, 3), (1, 2, 7), (1, 3, 6), (1, 6, 7), (2, 1, 3), (2, 1, 7), (2, 3, 5), (2, 5, 7)\}.$$

Conversely, each of the sets R defined above is a $(16, 2, 16, 8)$*-RDS in G relative to N.*

Proof: The assertion follows easily from Theorem 3.6 of Ma and Schmidt [16]. □

Using these characterizations as described above we get the following theorem.

Theorem 6.7
(a) *A* $(16, 4, 16, 4)$*-RDS in an abelian group* $G \ncong \mathbf{Z}_8 \times \mathbf{Z}_4 \times \mathbf{Z}_2$ *exists if and only if* $\exp(G) \leq 4$ *or* $G = \mathbf{Z}_8 \times (\mathbf{Z}_2)^3$ *with* $N \cong \mathbf{Z}_2 \times \mathbf{Z}_2$.
(b) *Let* $G = \mathbf{Z}_8 \times \mathbf{Z}_4 \times \mathbf{Z}_2$.
  (i) *There is a* $(16, 4, 16, 4)$*-RDS in G relative to* $\langle (4, 0, 0), (0, 2, 0)\rangle$.
  (ii) *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* $\langle (0, 2, 0), (0, 0, 1)\rangle$.

The existence part of Theorem 6.7 follows from Theorem 6.1, Result 6.2 and the following theorem that gives some new RDSs. These were constructed (by hand) by lifting suitable $(16, 2, 16, 8)$-RDSs which can be found in Ma and Schmidt [16], Theorem 2.1.

Theorem 6.8
(a) *There is a* $(16, 4, 16, 4)$*-RDS in* $(\mathbf{Z}_4)^2 \times (\mathbf{Z}_2)^2$ *relative to* $\langle(1, 0, 0, 0)\rangle$.
(b) *There is a* $(16, 4, 16, 4)$*-RDS in* $\mathbf{Z}_8 \times \mathbf{Z}_4 \times \mathbf{Z}_2$ *relative to* $\langle(4, 0, 0), (0, 2, 0)\rangle$.
(c) *There is a* $(16, 4, 16, 4)$*-RDS in* $(\mathbf{Z}_4)^3$ *relative to* $\langle(1, 0, 0)\rangle$.

Proof:

(a) We set

$$\begin{aligned} R = {} & \langle(0, 2, 0, 0), (0, 0, 1, 0)\rangle(0, 1, 0, 0) + (2, 0, 0, 0) + (0, 0, 1, 0) + (1, 2, 0, 0) \\ & + (3, 2, 1, 0) + [(2, 0, 0, 0) + (1, 0, 1, 0) + (0, 2, 0, 0) + (3, 2, 1, 0)](0, 3, 0, 1) \\ & + [(0, 0, 0, 0) + (3, 0, 1, 0) + (1, 2, 0, 0) + (2, 2, 1, 0)(0, 0, 0, 1). \end{aligned}$$

(b) We set

$$\begin{aligned} R' = {} & (0, 0, 0) + (0, 1, 0) + (0, 0, 1) + (0, 3, 1) + [(0, 0, 0) + (4, 3, 0) + (0, 0, 1) \\ & + (4, 1, 1)](1, 0, 0) + [(0, 0, 0) + (0, 3, 0) + (4, 0, 1) + (4, 1, 1)](2, 0, 0) \\ & + [(0, 2, 0) + (4, 3, 0) + (4, 2, 1) + (0, 1, 1)](3, 0, 0). \end{aligned}$$

(c) We set

$$\begin{aligned} R'' = {} & \langle(0, 2, 0), (0, 0, 2)\rangle + (0, 1, 0) + (3, 3, 0) + (2, 1, 2) + (1, 3, 2) + (0, 0, 1) \\ & + (2, 2, 1) + (1, 0, 3) + (3, 2, 3) + (0, 1, 1) + (3, 3, 1) + (1, 1, 3) + (2, 3, 3). \end{aligned}$$

Using characters it is easily seen that R, R' and R'' are the required RDS. □

Now we turn to the nonexistence part of Theorem 6.7. Since this requires lenghty proofs with lots of case distinctions we only give some examples for the nonexistence proofs; all other proofs are similar. The complete proof of Theorem 6.7 can be found in Schmidt [20].

Theorem 6.9 *There is no* $(16, 4, 16, 4)$*-RDS in* $G = \mathbf{Z}_8 \times \mathbf{Z}_8$ *relative to* $N = \langle(2, 0)\rangle$.

Proof: Let R be such an RDS. By Theorem 4.3 it is clear that we can assume

$$\begin{aligned} R = {} & (0, 1)g_1 + (1, 3)g_2 + (2, 5)g_3 + (3, 7)g_4 + (0, 3)g_5 + (1, 1)g_6 + (2, 7)g_7 \\ & + (3, 5)g_8 + (i_1, 0)g_9 + (i_1, 2)g_{10} + (i_2, 0)g_{11} + (i_2 + 2, 2)g_{12} + (i_1, 4)g_{13} \\ & + (i_1, 6)g_{14} + (i_2, 4)g_{15} + (i_2 + 2, 2)g_{16} \end{aligned}$$

where $g_j \in \langle(4, 0)\rangle$ for $j = 1, 2, \ldots, 16$ and $(i_1, i_2) \in \{(0, 1), (0, 3), (1, 0), (1, 2), (2, 1), (2, 3), (3, 0), (3, 2)\}$. We set $\epsilon_j = 1$ if $g_j = (0, 0)$, and $\epsilon_j = -1$ if $g_j = (4, 0)$. We define the characters χ_0, χ_1, χ_2, χ_3 of G by $\chi_k(1, 0) = \xi$ for $k = 0, 1, 2, 3$, $\chi_0(0, 1) = 1$ and

$\chi_k(0,1) = \xi^k$ for $k = 1, 2, 3$, where ξ is a complex eighth root of unity. We put the ϵ_j into a matrix:

$$\begin{pmatrix} \epsilon_1 & \epsilon_2 & \epsilon_3 & \epsilon_4 \\ \epsilon_5 & \epsilon_6 & \epsilon_7 & \epsilon_8 \\ \epsilon_9 & \epsilon_{10} & \epsilon_{11} & \epsilon_{12} \\ \epsilon_{13} & \epsilon_{14} & \epsilon_{15} & \epsilon_{16} \end{pmatrix}.$$

In the following matrices we write an m in the position of ϵ_j if the character value of the term of R belonging to ϵ_j is ξ^m. We get for $\chi_0, \chi_1, \chi_2, \chi_3$:

$$\begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 3 \\ i_1 & i_1 & i_2 & (i_2+2) \\ i_1 & i_1 & i_2 & (i_2+2) \end{pmatrix}, \tag{6}$$

$$\begin{pmatrix} 1 & 4 & 7 & 2 \\ 3 & 2 & 1 & 0 \\ i_1 & (i_1+2) & i_2 & (i_2+4) \\ (i_1+4) & (i_1+6) & (i_2+4) & i_2 \end{pmatrix}, \tag{7}$$

$$\begin{pmatrix} 2 & 7 & 4 & 1 \\ 6 & 3 & 0 & 5 \\ i_1 & (i_1+4) & i_2 & (i_2+6) \\ i_1 & (i_1+4) & i_2 & (i_2+6) \end{pmatrix}, \tag{8}$$

$$\begin{pmatrix} 3 & 2 & 1 & 0 \\ 1 & 4 & 7 & 2 \\ i_1 & (i_1+6) & i_2 & i_2 \\ (i_1+4) & (i_2+2) & (i_2+4) & (i_2+4) \end{pmatrix}. \tag{9}$$

If for example $i_1 = 0$ and $i_2 = 1$, then we get (using Result 1.3 and Result 1.6) $\epsilon_3 = -\epsilon_7$ from (6), $\epsilon_3 = \epsilon_5$ from (7), $\epsilon_1 = \epsilon_5$ from (8) and $\epsilon_1 = \epsilon_7$ from (9), a contradiction. Similarly we get contradictions for all other values of i_1 and i_2. □

Theorem 6.10 *There is no* $(16, 4, 16, 4)$*-RDS in* $G = \mathbf{Z}_8 \times (\mathbf{Z}_2)^3$ *relative to* $N = \langle (2,0,0,0) \rangle$.

Proof: Let R be such an RDS. We write $G = \langle g \rangle \times H$ and $N = \langle g^2 \rangle$ with $o(g) = 8$. Let $\rho_1 : G \to \bar{G} = G/\langle g^4 \rangle$ and $\rho_2 : \bar{G} \to \bar{G}/\rho_1(H)$ be the canonical epimorphisms. By

Result 1.3 and Lemma 1.5(a) we have (using the notation of Lemma 1.5)

$$\rho_2(\rho_1(R)) = \pm(4 - 2P_1)g_0 + 4P_2.$$

W.l.o.g. we can assume

$$\rho_2(\rho_1(R)) = 2 + 6h^2 + 4(h + h^3)$$

with $\rho_2(\rho_1(G)) = \langle h \rangle$. This implies

$$R = A + g^2B + gC + g^3D$$

with $A, B, C, D \subset \langle g^4 \rangle H$, $|A| = 2$, $|B| = 6$, $|C| = |D| = 4$ and $\rho_1(A + B) = \rho_1(H)$. W.l.o.g we assume $A = \{1, a\}$ with $a \in \langle g^4 \rangle H \backslash \{1\}$. Let χ be the character of G defined by $\chi(g) = \xi$ and $\chi \in H^\perp$. Hence $a = g^4h'$ for a suitable $h' \in H \backslash \{1\}$. Let τ be a character of H with $\tau(h') = -1$. Obviously, we have $|\chi \otimes \tau(R)| \neq 4$, a contradiction. □

We conclude our paper with some remarks on Theorem 6.7.

1) Note that Theorem 6.7 settles the existence problem of abelian (16, 4, 16, 4)-RDS completely.
2) Theorem 6.7 implies that—contrary to the case $b = 1$—in general the necessary and sufficient condition for the existence of abelian (p^a, p^b, p^a, p^{a-b})-RDSs can not be an exponent bound.
3) It seems to be very difficult to extend the lifting method used in Theorem 6.7 to attack the general case of abelian (p^a, p^b, p^a, p^{a-b})-RDSs. Despite the results of this paper, a really satisfactory method is still missing.

References

1. T. Beth, D. Jungnickel, and H. Lenz, *Design Theory*, Cambridge University Press, Cambridge, 1986.
2. R.C. Bose, "An affine analogue of Singer's theorem," *J. Indian Math. Soc.* **6** (1942), 1–15.
3. B.W. Brock, "A new construction of circulant $GH(p^2, \mathbf{Z}_p)$," *Discrete Math.* **112** (1993), 249–252.
4. J.A. Davis, "A note on products of relative difference sets," *Designs, Codes and Cryptography* **1** (1991), 117–119.
5. J.A. Davis, "Construction of relative difference sets in p-groups," *Discrete Math.* **103** (1992), 7–15.
6. J.A. Davis, "An exponent bound for relative difference sets in p-groups," *Ars. Comb.* **34** (1992), 318–320.
7. J.A. Davis and S.K. Seghal, "Using the simplex code to construct relative difference sets in 2-groups," *Designs, Codes and Cryptography* (1994), submitted.
8. W. de Launey and P. Viyaj Kumar, "On circulant generalized Hadamard matrices of prime power order," *Designs, Codes and Cryptography* (1994), (to appear).
9. J.E.H. Elliott and A.T. Butson, "Relative difference sets," *Illinois J. Math.* **10** (1966), 517–531.
10. M.J. Ganley, "On a paper of Dembowski and Ostrom," *Arch. Math.* **27** (1976), 93–98.
11. A.J. Hoffman, "Cyclic affine planes," *Can. J. Math.* **4** (1952), 135–145.
12. D. Jungnickel, "On a theorem of Ganley," *Graphs and Comb.* **3** (1987), 141–143.
13. K.H. Leung and S.L. Ma, "Constructions of partial difference sets and relative difference sets on p-groups," *Bull. Lond. Math. Soc.* (1990), 533–539.

14. S.L. Ma, Polynomial Addition Sets, Ph.D. Thesis, University of Hong Kong, 1985.
15. S.L. Ma and A. Pott, "Relative difference sets, planar functions and generalized Hadamard matrices," *J. Algebra* **175** (1995), 505–525.
16. S.L. Ma and B. Schmidt, "On (p^a, p, p^a, p^{a-1})-relative difference sets," *Designs, Codes and Cryptography* **6** (1995), 57–72.
17. S.L. Ma and B. Schmidt, "The structure of abelian groups containing McFarland difference sets," *J. Comb. Theory* A**70** (1995), 313–322.
18. A. Pott, "On the structure of abelian groups admitting divisible difference sets," *J. Combin. Theory* A**2** (1994), 202–213.
19. A. Pott, "A survey on relative difference sets," in *Groups, Difference Sets and the Monster*, K.T. Arasu, J.F. Dillon, K. Harada, S.K. Seghal, and R.L. Solomon (Eds.), DeGruyter Verlag Berlin/New York, pp. 195–233, 1996.
20. B. Schmidt, "Abelian (16,4,16,4)-RDS," manuscript.
21. R.J. Turyn, "Character sums and difference sets," *Pacific J. Math.* **15** (1965), 319–346.