Relative (p^a, p^b, p^a, p^{a-b})-difference sets: A Unified Exponent Bound and a Local Ring Construction

Siu Lun Ma
Department of Mathematics
National University of Singapore
Kent Ridge
Singapore 119260
Republic of Singapore

Bernhard Schmidt
253-37 Caltech
Pasadena, CA 91125
USA

April 25, 2001

Abstract

We show that for an odd prime p the exponent of an abelian group of order p^{a+b} containing a relative (p^a, p^b, p^a, p^{a-b})-difference set cannot exceed $p^{\lfloor a/2 \rfloor + 1}$. Furthermore, we give a new local ring construction of relative $(q^{2u}, q, q^{2u}, q^{2u-1})$-difference sets for prime powers q. Finally, we discuss an important open case concerning the existence of abelian relative (p^a, p, p^a, p^{a-1})-difference sets.

AMS Subject Classification 05B10, 05B25

1 Introduction

An $(\mathbf{m}, \mathbf{n}, \mathbf{k}, \lambda)$**-difference set (RDS)** in a group G relative to a subgroup N is a k-subset R of G, such that every element g of $G \setminus N$ has exactly λ representations $g = r_1 r_2^{-1}$ with $r_1, r_2 \in R$ while no element of $N \setminus \{1\}$ has such a representation. Here n denotes the order of N and m is the index of

N in G. Usually N is called the **forbidden subgroup**. We say that R is **abelian, cyclic** etc. if G has this property. For $N = \{1\}$ we speak of an **ordinary** difference set with parameters (m, k, λ).

The concept of RDSs is a generalization of the notion of difference sets and was introduced by Bose (1942), Butson (1962) and Elliott and Butson (1966). For a detailed introduction to RDSs, please consult the survey by Pott (1996). Recently, semiregular RDSs, i.e. RDSs with parameters of the form $(k, n, k, k/n)$ have been studied intensively, see Chen, Ray-Chaudhuri, Xiang (1996), Davis, Jedwab, Mowbray (1998), Davis, Sehgal (1997), Ma, Schmidt (1995) and Schmidt (1997). Semiregular RDSs are closely connected to other parts of combinatorics. For instance, $(n, n, n, 1)$-RDSs are equivalent to projective planes with semiregular automorphism group, see Pott (1996). Semiregular RDSs can also be used to construct sequences with ideal auto- and cross-correlation and are closely related to generalized Hadamard matrices, see de Launey, Vijay Kumar (1985). Recently, a very important application of semiregular RDSs to ordinary difference sets was discovered in the major work of Davis and Jedwab (1997). These authors used semiregular RDSs in a recursive construction process which works for a large class of (ordinary) difference sets, including a new infinite family.

In this paper, we study semiregular RDSs with parameters (p^a, p^b, p^a, p^{a-b}). Pott (1995, p. 109) raises two problems concerning these RDSs, namely to find new constructions for (p^a, p^b, p^a, p^{a-b})-RDSs and to find new exponent bounds, in particular, for even a. We will provide new results on both of this problems.

In order to understand the need for a new exponent bound in the case that a is even, say $a = 2c$, a comparison with the case where a is odd, say $a = 2d + 1$, is enlightening. We will only consider odd primes p. The case $p = 2$ is quite different. Ma and Pott (1995) proved that the exponent of an abelian group of order p^{2d+b+1} containing a $(p^{2d+1}, p^b, p^{2d+1}, p^{2d-b+1})$-RDS cannot exceed p^{d+1}. This exponent bound is quite satisfactory, as it is known from constructions of Davis (1991, 1992) that it can be attained for all d and all $b \leq d$. For $(p^{2c}, p^b, p^{2c}, p^{2c-b})$-RDSs, the situation had not been that nice. There are a lot of rather strong nonexistence results [see Pott (1994) and Schmidt (1997)], but no exponent bound comparable to the one for $(p^{2d+1}, p^b, p^{2d+1}, p^{2d-b+1})$-RDSs had been known. In the present paper, we will close this gap by showing that for an odd prime p an abelian group of order p^{2c+b}, containing a $(p^{2c}, p^b, p^{2c}, p^{2c-b})$-RDS cannot have an exponent exceeding p^{c+1}. This bound is quite satisfactory, because it is known that it can be attained for all c and all $b \leq c$, see Davis (1992).

Concerning the second of Pott's problems, we will give a new construction of RDSs with parameters of the form $(q^{2u}, q, q^{2u}, q^{2u-1})$ using local principle ideal domains. Such rings, which are also called **chain rings** [see MacDonald (1974, chapter 17)], have proved very useful for the construction of various types of difference sets. Examples can be found in Leung, Ma (1990), Chen, Ray-Chaudhuri, Xiang (1996) and Ray-Chaudhuri, Xiang (1996). Although Davis and Jedwab (1997) have alternative constructions, our construction has the advantage to give the RDSs explicitly without using recursive procedures.

Finally, we will discuss an important open problem concerning the existence of abelian (p^a, p, p^a, p^{a-1})-RDSs, i.e., the case $b = 1$. For $b = 1$, a complete solution of the existence problem is already in sight. We do not obtain the final answer, but we are able to present a promising method to attack the last open cases. For $p = 2$ and for $p > 2$ and even a, the existence problem of abelian (p^a, p, p^a, p^{a-1})-RDSs was already completely settled in our previous paper Ma, Schmidt (1995). Roughly speaking, in these cases the RDS exists if and only if the exponent of the underlying group does not exceed $p^{\lfloor a/2 \rfloor + 1}$. In the case were both p and a are odd the situation is quite similar, but there are two open cases left. The results in Ma, Schmidt (1995) were improved by Davis and Jedwab (1997, Cor. 8.2) who showed the following.

Result 1.1 *Let G be an abelian group of order p^{2d+2}, and let N be a subgroup of G of order p. Then G contains a $(p^{2d+1}, p, p^{2d+1}, p^{2d})$-RDS if and only if $\exp(G) \leq p^{d+1}$, except possibly when $G \cong \mathbf{Z}_{p^{d+1}} \times \mathbf{Z}_{p^{d+1}}$ or $d > 1$ and $G \cong \mathbf{Z}_{p^{d+1}} \times \mathbf{Z}_{p^d} \times N$.*

The two cases left open in Result 1.1 seem to be very difficult. We will focus on the first of these cases, and we will prove that a putative (p^3, p, p^3, p^2)-RDS in $\mathbf{Z}_{p^2} \times \mathbf{Z}_{p^2}$ necessarily is a union of translates of $(p, p, p, 1)$-RDSs living in the subgroup isomorphic to $\mathbf{Z}_p \times \mathbf{Z}_p$. For $p = 3$, it can be shown in this way that such an RDS cannot exist.

As usual, we will use the group ring $\mathbf{Z}G$ together with characters for the study of RDSs. 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 $A^{(-1)} = \sum_{g\in A} g^{-1}$. We also use the notation $|B| = \sum_{g\in G} b_g$ for $B = \sum_{g\in G} b_g g \in \mathbf{Z}G$. The following lemma is well known and can easily be proven by using the inversion formula for abelian characters [see Pott (1996, Lemma 1.2.2)].

Lemma 1.2 *Let R be a k-subset of an abelian group G and denote the character group of G by G^*.*
a) R is an (m, n, k, λ)-difference set relative to N if and only if

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

for every $\chi \in G^*$ where $N^\perp = \{\chi \in G^* : \chi \text{ is principal on } N\}$ and χ_0 is the principal character of G.
b) If $(m, n, k, \lambda) = (p^{2c}, p^b, p^{2c}, p^{2c-b})$, then R is a difference set with these parameters relative to N if and only if

$$\chi(R) = \begin{cases} \xi_\chi p^c & \text{if } \chi \in G \setminus N^\perp \\ 0 & \text{if } \chi \in N^\perp \setminus \{\chi_0\} \\ p^{2c} & \text{if } \chi = \chi_0 \end{cases}$$

for every $\chi \in G^*$ where the ξ_χ are roots of unity.

2 Preliminaries

In this section, we summarize some useful results that will be needed later. First we recall a lemma from Ma, Schmidt (1997, Lemma 2.1) which was used there to study McFarland difference sets.

Let G be a finite abelian group, and let P be be the Sylow p-subgroup of G. For any $h \in P$ and any subgroup $A = \langle b_1\rangle \times \cdots \langle b_r\rangle$ of P such that $A \cap \langle h\rangle = \{1\}$ and $o(h) \geq \exp(A)$, define

$$\mathcal{S}(h, A) = \{U < P | \; U = \langle a_1 b_1\rangle \times \cdots \langle a_r b_r\rangle, \; a_i \in \langle h\rangle, \; o(a_i) \leq o(b_i)\}.$$

Let $D = \sum_{g\in G} a_g g$ be an element of $\mathbf{Z}G$. For $U \leq G$ and $f \in G$, we define $D(Uf) = \sum_{g\in Uf} a_g$. Now we are ready to state the lemma.

Lemma 2.1 *Let $D = \sum_{g \in G} a_g g$ be an element of $\mathbf{Z}G$ with $a_g \geq 0$ for all g. Let $h \in P$, and let $A = \langle b \rangle \times W$ be a subgroup of P, such that $A \cap \langle h \rangle = \{1\}$, $o(h) = p^t \geq \exp(A)$ and $o(b) \geq p$. Assume that there exists a positive integer δ, such that for any $U \in \mathcal{S}(h, A)$ and $g \in G$ either*

$$\begin{array}{ccc} (1a) & D(Ug) - D(Ugh^{p^{t-1}}) \geq \delta & \text{and} \\ (1b) & D(Ugh^{ip^{t-1}}) < \delta/p \text{ for } i = 1, ..., p-1 & \text{or} \\ (2) & D(Ug) < \delta/p, & \end{array}$$

and there is at least one coset Ug satisfying (1a) and (1b). Let $B = \langle b^p > \times W$. Then for any $U' \in S(h, B)$ and $g \in G$, the coset $U'g$ satisfies either (1) or (2); and there is at least one coset $U'g$ satisfying (1).

Corollary 2.2 (Ma, Schmidt (1997)) *In the situation of the Lemma 2.1 we have*

$$\delta \leq \max\{a_g : g \in G\}.$$

Lemma 2.3 (Ma (1985)) *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 nonnegative coefficients only, then X_1 and X_2 also can be chosen to have nonnegative coefficients only.

We now state a result due to Ma and Pott (1995) which will be needed for the proof of the unified exponent bound as well as for the study of abelian (p^a, p, p^a, p^{a-1})-RDSs.

Lemma 2.4 *Let P be a cyclic group of order p^t where p is an odd prime, and let P_i be the unique subgroup of order p^i of P $(0 \leq i \leq t)$.*
a) If $A \in \mathbf{Z}P$ satisfies

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

for all $\chi \in P^* \setminus P_n^\perp$ *where* $1 \le n \le t$ *and* $n \le c+1$, *then we have*

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

with $\epsilon_m = \pm 1$, $g_m \in P$ *and* $Y \in \mathbf{Z}P$.
b) If $A \in \mathbf{Z}P$ *satisfies*

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

for all $\chi \in P^* \setminus P_n^\perp$ *where* $1 \le n \le t$ *and* $n \le c+1$, *then we have*

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

where $\epsilon_m = \pm 1$,$g_m \in P$, $X_m = p^{c-m} \sum_{i=0}^{p-1} \left(\frac{i}{p}\right) h^{ip^{t-m-1}}$, *and* $Y \in \mathbf{Z}P$. *Here* $\left(\frac{\cdot}{p}\right)$ *denotes the Legendre symbol.*

3 A unified exponent bound

A lot of previous work has been done on the problem of finding the best possible exponent bounds for abelian (p^a, p^b, p^a, p^{a-b})-RDSs, see Davis (1992), Pott (1994), Ma, Pott (1995), Schmidt (1997), but the complete answer has not been found for $p > 2$, a even, and in the case $p = 2$. These remaining cases are by far the most difficult. In this section, we will provide the answer for $p > 2$, a even, by showing that the exponent of an abelian group of order p^{2c+b} containing a $(p^{2c}, p^b, p^{2c}, p^{2c-b})$-RDS cannot exceed p^{c+1}. This bound is best possible since it is known from constructions of Davis (1991,1992) that it can be achieved for all pairs (c, b) with $b \le c$. Parts of the proof of Theorem 3.2 have already been obtained in Schmidt (1997). For the convenience of the reader, we will recall these arguments here.
Before we state our theorem, we recall an exponent bound on the forbidden subgroup due to Ma, Pott (1995) which will help us avoiding an undesired case distinction in the proof of Theorem 3.2.

Result 3.1 *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*

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

The following is the main result of this paper.

Theorem 3.2 *Let p be an odd prime. If an abelian group G of order p^{a+b} contains a (p^a, p^b, p^a, p^{a-b})-RDS, then* $\exp(G) \leq p^{\lfloor a/2 \rfloor +1}$.

Proof For odd a, the assertion was already proved by Ma, Pott (1995). Hence we only need to consider even a, say $a = 2c$. Let R denote the RDS and assume $\exp(G) \geq p^{c+2}$, say $\exp(G) = p^t = p^{c+r+2}$ where $r \geq 0$. We show that this assumption leads to a contradiction. Write $G = \langle g \rangle \times H$ where g is an element of G of order p^t. We will show that the assumptions of Lemma 2.1 are satisfied for $P = G$, $A = H$, $D = R$, $h = g$ and $\delta = p^c$. Then Corollary 2.2 will imply $\delta \leq 1$ which is the desired contradiction.

We note that, in the notation of Lemma 2.1, $S(g, H)$ is the set of all complements of $\langle g \rangle$ in G. Let U be any of these complements. Then G/U is cyclic of order p^t. First of all, we want to show that the forbidden subgroup N cannot be contained in U. Assume the contrary. By elementary character "theory" we can choose a character χ of G with $Ker\chi \cap \langle g \rangle = \{1\}$ and $|Ker\chi \cap N| = |N|/p$. Write $K = Ker\chi$ and let $\tau : G \to G/K$ denote the canonical epimorphism. Since no two elements of R are in the same coset of N, the coefficients of $\tau(R)$ cannot exceed $|K|/|K \cap N| \leq p^{c-r-1}$. However, we know from Lemma 1.2 b) and Ma's Lemma that $\tau(R) = p^c X_1 + P' X_2$ where P' is the subgroup of order p of G/K and X_1, X_2 are elements of the group ring $\mathbf{Z}[G/K]$ with nonnegative coefficients. If we also view χ as a character of G/K, we obtain $\chi(R) = p^c \chi(X_1)$, and this implies $X_1 \neq 0$, since $\chi(R) \neq 0$ by Lemma 1.2 b). Hence $\tau(R)$ has a coefficient $\geq p^c$, which contradicts the upper bound for the coefficients of $\tau(R)$ obtained above. This shows that N indeed cannot be contained in U.

Let $\rho : G \to G/U$ be the canonical epimorphism. By the same argument as above we see that the coefficients of $\rho(R)$ cannot exceed $|U|/|U \cap N|$ and that $\rho(R)$ has at least one coefficient $\geq p^c$ (note that the argument for the existence of a coefficient $\geq p^c$ requires that N is not contained in U). Hence $p^c \leq |U|/|U \cap N|$ and

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

We write $|\rho(N)| = p^x$ with $x \geq r + 2$. By Result 3.1 we can assume $x \leq c$. From Lemma 1.2 b) and Lemma 2.4 a) we get (using the notation of Lemma

2.4)

$$\rho(R) = \sum_{m=0}^{x-1} \epsilon_m p^{c-m-1}(pP_m - P_{m+1})g_m + P_xY.$$

Since $\psi(\rho(R)) = 0$ and $\psi(pP_m - P_{m+1}) = 0$ for $m = 0, ..., x-1$ for all $\psi \in P_x^\perp$ by Lemma 1.2 b), we conclude $\varphi(P_xY) = 0$ for all nontrivial $\varphi \in (G/U)^*$. By the Fourier inversion formula, P_xY must be a multiple of $G/U = P_{c+r+2}$. As $|R| = p^{2c}$, we must have $P_xY = p^{c-r-2}P_{c+r+2}$; thus

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

We claim

$$\epsilon_0 = \epsilon_1 = \cdots = \epsilon_{r+1} = 1 \text{ and } P_ig_0 = P_ig_i \tag{2}$$

for $i = 0, 1, ..., r+1$.

We prove (2) by induction. For $h \in G/U$ let $C(h)$ be the coefficient of g in $\rho(R)$.

(a) Assume $\epsilon_0 = -1$. Then by (1) (recall that $p > 2$)

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

a contradiction. Hence $\epsilon_0 = 1$.

(b) Let $1 \leq l \leq r+1$, $\epsilon_0 = \epsilon_1 = \cdots = \epsilon_{l-1} = 1$ and $P_ig_0 = P_ig_i$ for $i = 0, 1, ..., l-1$. We have to show $\epsilon_l = 1$ and $P_lg_0 = P_lg_l$. From (1) we have

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

Let $g' \in P_lg_0 \setminus \{g_0\}$. If $\epsilon_l = -1$ or $P_lg_0 \neq P_lg_l$, then

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

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

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

from (1). We infer

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

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

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

for $h' \in (G/U) \setminus P_{r+2}g_0$. As $\rho(R)$ has at least one coefficient $\geq p^c$ we get $C(g_0) \geq p^c$.

Together with the upper bounds on $C(h)$ and $C(h')$ obtained above, this shows that U satisfies the conditions of Lemma 2.1 (with $\delta = 1$). Since U was chosen as an arbitrary element of $S(g, H)$, we have indeed verified that Lemma 2.1 can be applied, and this proves the theorem. □

4 A construction using local rings

Constructions of (p^a, p^b, p^a, p^{a-b})-RDSs with $b > 1$ are quite rare. It is for this reason that Pott (1995) raises the problem to find new constructions for RDSs of this type. In this section, we present a construction of $(q^{2u}, q, q^{2u}, q^{2u-1})$-RDSs where q is an arbitrary prime power using local rings.

First we describe the elementary properties of the rings we need. For a reference on the algebraic background, please consult McDonald (1974). A finite ring R with identity is called **local** if $R/\mathrm{Rad}(R)$ is a finite field where $\mathrm{Rad}(R)$ denotes the radical of R. For our construction, we need a special type of local rings, namely, **local principal ideal rings** which are also called **chain rings**, see (MacDonald, p. 339). A complete characterization of these rings can be found in MacDonald (1974, Theorem XVII.5). Let us summarize some of their most important properties, see also MacDonald (1974, chapter XV-XVII).

Let $q = p^r$ be any prime power, let n, s and t be positive integers with $t \leq s$ and define $u := (n-1)s + t - 1$. By GR(p^n, r) we denote the Galois ring over

$\mathbf{Z}_{p^n}$ of degree r, see MacDonald (1974, chapter XVI). Let g be an Eisenstein polynomial of degree s over $\mathrm{GR}(p^n,\ r)$ [MacDonald (1974, p. 342)]. Then

$$R = \mathrm{GR}(p^n,\ r)[x]/(g(x), p^{n-1}x^t)$$

is a chain ring of characteristic p^n with the following properties.
a) R contains a unique maximal ideal I, and R/I is a finite field of order q.
b) The set of units of R is $R \setminus I$.
c) $|I^a| = q^{u-a+1}$ for $1 \leq a \leq u+1$, in particular, $I^{u+1} = \{0\}$.
d) If π is a generator of I, then every element x of R can be written in the form $x = \pi^b \delta$ where δ is a unit, $0 \leq b \leq u+1$, and b is uniquely determined by $x \in I^b$ and $x \notin I^{b+1}$.
e) If $x = \pi^b \delta$ as in d), then $Rx = I^b$ and $Ix = I^{b+1}$.
f) Concerning the additive groups, we have

$$\begin{aligned}(R,+) &\cong \mathbf{Z}_{p^n}^t \times \mathbf{Z}_{p^{n-1}}^{s-t},\\ (I,+) &\cong \mathbf{Z}_{p^n}^{t-1} \times \mathbf{Z}_{p^{n-1}}^{s-t},\\ (I^u,+) &\cong \mathbf{Z}_p^r.\end{aligned}$$

The following consequence of Lemma 3.2 of Leung, Ma (1990) will be needed in the proof of the correctness of our construction. Here by a "character" we mean a complex character of the additive group.

Lemma 4.1 *Let R and I be defined as above, and let τ be a character of R, which is nonprincipal on I^u. Then for every character χ of $I \times I$ there are $c, d \in R$, such that*

$$\chi(x,y) = \tau(cx + dy)$$

for all $(x,y) \in I \times I$.

Now we are ready to state the construction. Using the notation introduced above, let G be any group of order q^{2u+1} containing $(I \times I, +)$ in its center. Let $\{x_1, ..., x_{q^{u-1}}\}$, $\{y_1, ..., y_q\}$ and $\{z_1, ..., z_q\}$ be complete systems of coset representatives of I^u in I, I in R and $I \times I$ in G, respectively. For $i = 1, 2, ..., q^{u-1}$ and $j = 1, ..., q$ we define

$$D_{ij} = \{([x_i + y_j]a, a) : a \in I\} \subset I \times I$$

and

$$D_j = \bigcup_{i=1}^{q^{u-1}} [D_{ij} + (x_i, 0)].$$

Finally, let

$$D = \bigcup_{j=1}^{q} (D_j + z_j).$$

Theorem 4.2 *The set D is a $(q^{2u}, q, q^{2u}, q^{2u-1})$-RDS in G relative to the subgroup $N = I^u \times \{0\}$ contained in $I \times I$.*

Corollary 4.3 *Let $q = p^r$ be any prime power, let n, s, t be any positive integers with $t \leq s$ and let $u = (n-1)s + t - 1$. Then there exists a $(q^{2u}, q, q^{2u}, q^{2u-1})$-RDS in any group of order q^{2u+1} which contains a subgroup isomorphic to $\mathbf{Z}_{p^n}^{2t-2} \times \mathbf{Z}_{p^{n-1}}^{2(s-t)}$ in its center.*

For the proof of Theorem 4.2, we need the following lemmas.

Lemma 4.4 *If $j \neq j'$, then $D_{ij} + D_{i'j'} = I \times I$ for all i, i'.*

Proof Since the D_{ij}'s are subgroups of order q^u of $I \times I$, it suffices to prove $D_{ij} \cap D_{i'j'} = \{(0,0)\}$. Let $x \in D_{ij} \cap D_{i'j'}$. Then $x = ([x_i + y_j]a, a) = ([x_{i'} + y_{j'}]b, b)$ for some $a, b \in I$. This implies $a = b$ and $[x_i - x_{i'} + y_j - y_{j'}]a = 0$. But $x_i - x_{i'} + y_j - y_{j'}$ is a unit in R, since $x_i - x_{i'} \in I$ and $y_j - y_{j'} \notin I$. Hence $a = 0$ and $x = (0,0)$. □

Lemma 4.5 *Let χ be a nontrivial character of $I \times I$ which is principal on $N = I^u \times \{0\}$. Then $\chi(D_j) = 0$ for all j. Furthermore, D_j has no repeated elements.*

Proof Since $|D_j| = q^{2u-1} = |(I \times I)/N|$, it suffices to show that each coset of N in $I \times I$ contains at most one element of D_j. Suppose $N + (x_i + [x_i + y_j]a), a) = N + (x_{i'} + [x_{i'} + y_j]b, b)$ for some $a, b \in I$ and i, i'. This implies $a = b$ and $(x_i - x_{i'})(1 + a) \in I^u$. But $1 + a$ is a unit in R since $a \in I$. Hence $x_i - x_{i'} \in I^u$ implying $i = i'$ by the choice of the x_i. □

Lemma 4.6 *Let χ be a character of $I \times I$ which is nonprincipal on N. Then $\chi(D_{i_0 j_0}) = q^u$ for exactly one pair (i_0, j_0) and $\chi(D_{ij}) = 0$ for all $(i,j) \neq (i_0, j_0)$.*

Proof Choose τ, c, d as described in Lemma 4.1. Write $z_{ij} = c(x_i + y_j) + d$. Since χ is nontrivial on N, c must be a unit in R. Hence, by the choices of the x_i and y_j, we have $z_{i_0,j_0} \in I^u$ for exactly one pair (i_0, j_0) and $z_{ij} \notin I^u$ for all $(i,j) \neq (i_0, j_0)$. We also have

$$\chi(D_{ij}) = \sum_{a \in I} \tau(z_{ij}a).$$

Since $z_{i_0 y_0} \in I^u$, it follows that $\chi(D_{i_0 j_0}) = |I| = q^u$. Now fix a pair $(i,j) \neq (i_0, j_0)$. Since $I^u \subset I z_{ij}$ (see property e) of R mentioned above) and τ is nontrivial on I^u, we can find $v \in I$ with $\tau(z_{ij}v) \neq 1$. From $[1 - \tau(z_{ij}v)] \sum_{a \in I} \tau(z_{ij}a) = \sum_{a \in I} \tau(z_{ij}a) - \sum_{a \in I} \tau(z_{ij}[a+v]) = 0$ we conclude $\chi(D_{ij}) = 0$. □

Proof of Theorem 4.2 From Lemma 4.5 we know that D has no repeated elements. Since we want to work in the group ring, we have to introduce a suitable notation in order to avoid confusion of the multiplications in the local ring and the group ring. Let $\bar{G}$ be a *multiplicatively* written group isomorphic to G and denote the isomorphism $G \to \bar{G}$ by a bar. Using the group ring notation, we have to prove $\bar{D}\bar{D}^{(-1)} = q^{2u} + q^{2u-1}(\bar{G} - \bar{N})$. W.l.o.g., we may assume $\bar{z_1} \in \bar{I} \times \bar{I}$. We have

$$\bar{D}\bar{D}^{(-1)} = \sum_{i=2}^{q} [\sum_{\bar{z_k}\bar{z_l}^{(-1)} \in (\bar{I} \times \bar{I})\bar{z_i}} \bar{D}_k \bar{D_l}^{(-1)}] \bar{z_i} + \sum_{j=1}^{q} \bar{D}_j \bar{D_j}^{(-1)}. \tag{3}$$

It follows from Lemma 4.4 that the first sum in (3) equals $q^{2u-1}(\bar{G} - [\bar{I} \times \bar{I}])$. It remains to show

$$\sum_{j=1}^{q} \bar{D}_j \bar{D_j}^{(-1)} = q^{2u} + q^{2u-1}[(\bar{I} \times \bar{I}) - \bar{N}]. \tag{4}$$

By the Fourier inversion formula it suffices to show that both sides of equation (4) have the same character values. For the principal character χ_0 this is true, since $|\bar{D}_j| = q^{2u-1}$ for all j and $|(\bar{I} \times \bar{I}) - \bar{N}| = q^{2u} - q$. For a character in $\bar{N}^\perp \setminus \{\chi_0\}$ or $\bar{G}^* \setminus \bar{N}^\perp$ the character values of both sides of (4) are equal in view of Lemma 4.5 and Lemma 4.6, respectively. □

Example 4.7 Let $R = \mathbf{Z}_4[\alpha]$ where $\alpha^2 = 1+\alpha$. Then R is a chain ring with maximal ideal $I = (2) = \{0, 2, 2\alpha, 2+2\alpha\}$ and $I^2 = \{0\}$ (i.e. $u = 1$). Let $x_1 = 0$, $y_1 = 0$, $y_2 = 1$, $y_3 = \alpha$, $y_4 = 1+\alpha$ and $z_i = (y_i, 0)$, $i = 1, 2, 3, 4$. Then

$$\begin{aligned} R &= \{(0,0),\ (0,2),\ (0,2\alpha),\ (0,2+2\alpha),\ (1,0),\ (3,2),\ (1+2\alpha,2\alpha),\\ &\quad (3+2\alpha,2+2\alpha),\ (\alpha,0),\ (2\alpha,2),\ (2+3\alpha,2\alpha),\ (2+\alpha,2+\alpha),\\ &\quad (1+\alpha,0),\ (3+3\alpha,2),\ (3+\alpha,2\alpha),\ (1+3\alpha,2+2\alpha) \end{aligned}$$

is a $(16, 4, 16, 4)$-RDS in $R \times I$ relative to $N = I \times \{0\}$. In terms of the additive groups, we have $R \times I = \mathbf{Z}_4 \times \mathbf{Z}_4 \times \mathbf{Z}_2 \times \mathbf{Z}_2$, $N = \langle 2000, 0200 \rangle$ and

$$\begin{aligned} R &= \{0000,\ 0010,\ 0001,\ 0011,\ 1000,\ 3010,\ 1201,\ 3211,\\ &\quad 0100,\ 0310,\ 2301,\ 2100,\ 1100,\ 3310,\ 3101,\ 1311\}. \end{aligned}$$

5 Abelian relative $(\mathrm{p^a}, \mathrm{p}, \mathrm{p^a}, \mathrm{p^{a-1}})$-difference sets

It was already mentioned in the introduction that the existence problem for abelian (p^a, p, p^a, p^{a-1})-RDSs is almost completely settled. However, there are the following two obstinate cases remaining for odd p and odd a. Write $a = 2c+1$ and denote the forbidden subgroup by N.

Case 1
$G = \mathbf{Z}_{p^{c+1}} \times \mathbf{Z}_{p^{c+1}}$, N arbitrary.

Case 2
$G = \mathbf{Z}_{p^{c+1}} \times \mathbf{Z}_{p^c} \times N$.

Here we encounter a situation frequently occurring in the study of difference sets: The really hard cases are those with high exponent and low rank. A widely known example for this phenomenon is Hadamard difference sets in $\mathbf{Z}_{2^d} \times \mathbf{Z}_{2^d}$ and $\mathbf{Z}_{2^{d+1}} \times \mathbf{Z}_{2^{d-1}}$. Here a **Hadamard difference set** means an ordinary difference set with parameters $(4u^2, 2u^2-u, u^2-u)$ for some positive integer u. After the cases $\mathbf{Z}_{2^d} \times \mathbf{Z}_{2^d}$ and $\mathbf{Z}_{2^{d+1}} \times \mathbf{Z}_{2^{d-1}}$ had been settled by Davis (1991), the way was cleared for the complete solution of the existence problem for Hadamard difference sets in abelian 2-groups by Kraemer (1993). We would like to stress here that there are interesting connections between Hadamard difference sets and (p^a, p^b, p^a, p^{a-b})-RDSs. The most obvious ones are the exponent bounds and the construction methods. An important open case of abelian HDSs which should be compared with Case 1 from above, is groups of the form $H \times \mathbf{Z}_{p^d} \times \mathbf{Z}_{p^d}$, $\gcd(p, |H|) = 1$, see Arasu, Davis, Jedwab (1995).

In this paper, we will study Case 1. Our main result will be that for $c = 1$ the RDS must be a union of translates of $(p, p, p, 1)$-RDSs which reduces the original problem considerably, since *all* $(p, p, p, 1)$-RDSs are known. It seems probable that our method also can be used for $c > 1$, see the remark following Lemma 5.8. We think that our technique also may be useful for the study of other difference sets, in particular, for Hadamard difference sets.

Let $G = \mathbf{Z}_{p^{c+1}} \times \mathbf{Z}_{p^{c+1}} = \langle a \rangle \langle b \rangle$ and assume that R is a $(p^{2c+1}, p, p^{2c+1}, p^{2c})$-RDS in G relative to $N = \langle a^{p^c} \rangle$. Let $\left(\frac{\cdot}{p}\right)$ denote the Legendre symbol.

Lemma 5.1 *Let $U_{k,l} = \langle a^{pk+l} b \rangle$, $0 \le k \le p^c - 1$, $0 \le l \le p - 1$. Then*

$$\rho_{k,l}(R) = p^c[\bar{G} + \delta(k,l)\bar{a}^{\epsilon(k,l)} \sum_{i=1}^{p-1} \left(\tfrac{i}{p}\right) \bar{a}^{ip^c}]$$

where $\rho_{k,l} : G \to \bar{G} := G/U_{k,l}$ is the natural epimorphism, $\delta(k,l) \in \{-1, 1\}$, $\epsilon(k,l) \in \{0, ..., p^{c+1} - 1\}$, $\bar{a} = \rho_{k,l}(a)$.

Proof From Lemma 1.2 a) and Lemma 2.4 b) we get

$$\rho_{k,l}(R) = p^c \delta(k,l)\bar{a}^{\epsilon(k,l)} \sum_{i=1}^{p-1} \left(\tfrac{i}{p}\right) \bar{a}^{ip^c} + P_1 Y$$

where P_1 is the subgroup of order p of $\bar{G}$. Let χ be any nontrivial character of $\bar{G}$ which is trivial on $\langle \bar{a}^{p^c} \rangle$. Since $\chi(R) = 0$ by Lemma 1.2 a) and $\chi(\sum_{i=1}^{p-1} \left(\frac{i}{p}\right) \bar{a}^{ip^c}) = 0$, we conclude $\psi(P_1 Y) = 0$ for *all* nontrivial $\psi \in \bar{G}^*$. By the Fourier inversion formula, $P_1 Y$ must be a multiple of $\bar{G}$. Because of $|R| = p^c |\bar{G}|$, we must have $P_1 Y = p^c \bar{G}$. □

The following lemma in particular shows that R can easily be recovered from the $\delta(k,l)$ and $\epsilon(k,l)$.

Lemma 5.2 *Let $\mathcal{P}_i = \{\langle a^{kp^i} b^{p^i} \rangle g : 0 \le k \le p^{c-i+1} - 1, \ g \in G\}$. Let $A = \sum_{g \in G} a_g g$ be an element of ZG, and write $A(X) = \sum_{g \in X} a_g$ for $X \subset G$. Furthermore, assume*

$$A(NU) = |U| \text{ for every } U \in \mathcal{P}_i, \ m \le i \le n, \tag{5}$$

for some m, n. Then, for every $U \in \mathcal{P}_n$, we have

$$A(U) = p^{c-n} - p^{c-m} + p^{m-n} \sum_{i=1}^{p^{n-m}-1} A(U_i)$$

where $U_0, ..., U_{p^{n-m}-1}$ are the elements of $\mathcal{P}_m$ containing U.

Proof The assertion is true for $n = m$. Assume that it is true for some $n \geq m$. It suffices to show that it is also true for $n + 1$.
Let $U \in \mathcal{P}_{n+1}$, say $U = \langle a^{kp^{n+1}} b^{p^{n+1}} \rangle g$. The elements of $\mathcal{P}_n$ containing U are $W_i = \langle a^{kp^n + ip^c} b^{p^n} \rangle g$, $0 \leq i \leq p - 1$. Let H_j, $0 \leq j \leq p^{n-m+1} - 1$, be the elements of $\mathcal{P}_m$ containing one of the W_i. The H_j are exactly the elements of $\mathcal{P}_m$ containing U. It is easy to see that

$$K := NU \cup \bigcup_{i=0}^{p-1} W_i = NW_0,$$

since each two of the cosets $NU, W_0, ..., W_{p-1}$ intersect in U. Hence

$$A(K) = A(U) + (A(NU) - A(U)) + \sum_{i=0}^{p-1} (A(W_i) - A(U)),$$

i.e.

$$A(U) = \frac{1}{p}(-A(K) + A(NU) + \sum_{i=0}^{p-1} A(W_i)).$$

Using (1) and induction gives

$$\begin{aligned} A(U) &= \frac{1}{p}[-p^{c-n+1} + p^{c-n} + p(p^{c-n} - p^{c-m}) \\ &\quad + p^{m-n} \sum_{i=0}^{p^{n-m+1}-1} A(H_j)] \\ &= p^{c-n-2} - p^{c-m-1} + p^{m-n-1} \sum_{i=1}^{p^{n-m+1}-1} A(H_j), \end{aligned}$$

proving the assertion. □

Corollary 5.3 *a) For every $W \in \mathcal{P}_0$ we have*

$$R(W) = p^c(\delta(W) + 1)$$

for some $\delta(W) \in \{-1, 0, 1\}$.
b) Let $U \in \mathcal{P}_n$ and let $W_0, .., W_{p^n-1}$ be the elements of $\mathcal{P}_0$ containing U. Then

$$R(U) = \frac{|U|}{p}(1 + \sum_{i=0}^{p^n-1} \delta(W_i)).$$

Proof a) This is immediate from Lemma 5.1.
b) From Lemma 5.2 we get

$$\begin{aligned} R(U) &= p^{c-n} - p^{c-1} + p^{-n} \sum_{i=0}^{p^n-1} R(W_i) \\ &= \frac{|U|}{p}(1 + \sum_{i=0}^{p^n-1} \delta(W_i)), \end{aligned}$$

completing the proof. □

We skip the straightforward proof of the next lemma.

Lemma 5.4 *Let $U_l = \langle a^{lp^c} b^{p^c} \rangle$, $0 \leq l \leq p-1$. The elements of $\mathcal{P}_0$ containing $U_l a^r b^s$ $(0 \leq r \leq p^{c+1} - 1,\ 0 \leq s \leq p^c - 1)$ are $U_{k,l} a^{r-s(pk+l)}$, $0 \leq k \leq p^c - 1$.*

We will need the following reformulation of Lemma 5.1.

Lemma 5.5 *Set $f(k, l, x) = 1$ if $\epsilon(k, l) \equiv x \mod p^c$ and $f(k, l, x) = 0$ otherwise. Then*

$$R(U_{k,l} a^x) = p^c(1 + f(k, l, x)\delta(k, l)\Big(\tfrac{(x-\epsilon(k,l))/p^c}{p}\Big).$$

Corollary 5.6 *Let $T(r, s, l) = \{k : 0 \leq k \leq p^c - 1,\ r - s(pk + l) \equiv \epsilon(k, l) \mod p^c\}$. Then*

$$R(U_l a^r b^s) = 1 + \sum_{k \in T(r,s,l)} \delta(k, l)\Big(\tfrac{(x-\epsilon(k,l))/p^c}{p}\Big).$$

Proof The assertion easily follows from Cor.5.3, Lemma 5.4 and Lemma 5.5 □

In the following, the numbers $F(r,s,l) := |T(r,s,l)|$ will play a central role. We first list two properties of these numbers which are immediate from the definition.

Lemma 5.7

a) $\sum_{r=0}^{p^c-1} F(r,s,l) = p^c$ *for all* r,s,l.

b) $F(r+ip^c+jlp^{c-1}, s+jp^c-1, l) = F(r,s,l)$ *for all* r,s,l,i,j.

We now come to a crucial lemma describing important properties of the numbers $F(r,s,l)$. Define $L := \langle a^{p^c}\rangle\langle b^{p^c}\rangle$.

Lemma 5.8

a) $\sum_{l=0}^{p-1} F(r,s,l) \geq p-1$ *for all* r,s.

b) If $\sum_{l=0}^{p-1} F(r,s,l) = p-1$, *then* $F(r,s,l_0) = p-1$ *for some* l_0, *and* $R \cap La^r b^s$ *is a coset of* U_{l_0}.

Remark

By a rather lengthy argument the following further property can be derived. As we do not need this result here, we state it without proof. We think that it could be useful in the further investigation of the problem.

c) If $\sum_{l=0}^{p-1} F(r,s,l) = p$, *then either* $F(r,s,l) = 1$ *for* $0 \leq l \leq p-1$ *or* $F(r,s,l_0) = p$ *for some* l_0 *and* $R \cap La^r b^s$ *is a coset of* U_{l_0}.

Proof of Lemma 5.8 a) Let $x \in R \cap La^r b^s$. Viewing $La^r b^s$ as an affine plane and considering all lines through x gives

$$\begin{aligned} p &= R(La^r b^s) \\ &= 1 + [\sum_{l=0}^{p-1}(R(U_l x) - 1)] + [R(Nx) - 1] \\ &= -p + 1 + \sum_{l=0}^{p-1} R(U_l x). \end{aligned}$$

Hence

$$\sum_{l=0}^{p-1} R(U_l x) = 2p - 1. \tag{6}$$

From Lemma 5.6 and Lemma 5.7 we know that

$$R(U_l x) \le 1 + F(r, s, l). \tag{7}$$

Hence

$$2p - 1 \le p + \sum_{l=0}^{p-1} F(r, s, l),$$

proving the assertion.

b) Assume $\sum_{l=0}^{p-1} F(r, s, l) = p - 1$. Then we have equality in (7) for all l, and hence $R(U_l x) = 1 + F(r, s, l)$ for $0 \le l \le p - 1$ and all $x \in R \cap La^r b^s$. Hence $p = R(La^r b^s)$ is divisible by $1 + F(r, s, l)$ for all l. Thus $F(r, s, l_0) = p - 1$ for some l_0, and $R \cap La^r b^s$ is a coset of U_{l_0}. □

The next lemma provides a condition implying $F(r, s, l) = 1$ for all r, s, l (we denote this by $F \equiv 1$ in the following). We think that $F \equiv 1$ always must be the case; unfortunately, we can prove this only for $c = 1$. We remark that $F \equiv 1$ would imply that, for any c, the subgroup $\langle a^p \rangle \langle b^p \rangle$ contains a $(p^{2c-1}, p, p^{2c-1}, p^{2c-2})$-RDS relative to N. Thus, assuming $F \equiv 1$, we presumably could dispose of all cases with $c > 1$ by an inductive argument.

Lemma 5.9 *Let* $0 \le r, s \le p^{c-1} - 1$. *If*

$$\sum_{i=0}^{p-1} F(r + ip^{c-1}, s, l) = p$$

for $0 \le l \le p - 1$, *then*

$$F(r + ip^{c-1}, s + jp^{c-1}, l) = 1$$

for all $0 \le i, j \le p - 1$.

Proof Write $G(i, j, l) = F(r + ip^{c-1}, s + jp^{c-1}, l)$. From Lemma 5.7 b) we have $G(i + kl, j + k, l) = G(i, j, l)$ for $0 \le k \le p - 1$. Let $H(i, l) = G(i, 0, l)$. By the assumption,

$$\sum_{i=0}^{p-1} H(i, l) = p \tag{8}$$

for $0 \le l \le p - 1$. Furthermore, from Lemma 5.8 we have
$\sum_{l=0}^{p-1} G(i, j, l) = \sum_{l=0}^{p-1} G(i - jl, 0, l) = \sum_{l=0}^{p-1} H(i - jl, l) \ge p - 1$ for all i, j,

and if $\sum_{l=0}^{p-1} H(i-jl,l) = p-1$, then $H(i-jl_0,l_0) = p-1$ for some l_0.
Consider H as a function on an affine plane A; for every line G of A write $H(G) = \sum_{x\in G} H(x)$. We know $H(G) \geq p-1$ for all G. Considering the parallel class of G, it follows that $H(G) \leq 2p-1$, and if $H(G_0) = 2p-1$, then $H(G) = p-1$ for all G parallel to G_0. We also know $H(G) = p$ for all G parallel to $\langle(1,0)\rangle$ (from (8)).
Assume $H(G_0) = p-1$ for some G_0, and let x be the point on G_0 with $H(x) = p-1$. Let $G_0, ..., G_p$ be the lines through x. Then $p^2 = \sum_{y\in A} H(y) = H(x) + \sum_{i=0}^{p-1}(H(G_i) - H(x)) = -pH(x) + \sum_{i=0}^{p-1} H(G_i)$.
W.l.o.g, assume that g_1 is parallel to $\langle(1,0)\rangle$. Then $H(G_1) = p$; recall $H(G_0) = p-1$. Hence $p^2+p(p-1)-p-(p-1) = 2p^2-3p+1 = \sum_{i=2}^{p-1} H(G_i)$. Thus $H(G_i) = 2p-1$ for $2 \leq i \leq p-1$ (recall $H(G_i) \leq 2p-1$). Hence $H(G) = p-1$ for all lines $G \neq G_2$ parallel to G_2. Hence there is a point y not on G_2 with $H(y) = p-1$. By the same argument as above, the line G_2' through y parallel to G_2 must satisfy $H(G_2') = 2p-1$. But this is impossible, since at most one line G parallel to G_2 has $H(G) = 2p-1$.
Thus $H(G) \geq p$ for all lines G. This implies $H(x) = 1$ for all points x. □

Theorem 5.10 *If p is an odd prime and R is a (p^3,p,p^3,p^2)-RDS in $G = \langle a\rangle\langle b\rangle \cong \mathbf{Z}_{p^2} \times \mathbf{Z}_{p^2}$ relative to $N = \langle a^p\rangle$, then*

$$R = \sum_{i,j=0}^{p-1} a^i b^j R_{ij}$$

where each R_{ij} is a $(p,p,p,1)$-RDS in $L = \langle a^p\rangle\langle b^p\rangle$ relative to N.

Proof By considering all translates of R we see that it suffices to show that $R \cap L$ is a $(p,p,p,1)$-RDS in L relative to N. By Lemma 5.7 a), the assumption of Lemma 5.9 is satisfied. Hence $F(r,s,l) = 1$ for all r,s,l. Write $T(0,0,l) = \{k(l)\}$. From Lemma 5.6 we have

$$R(U_l a^{ip}) = 1 + \delta(k(l),l)\Big(\tfrac{(ip-\epsilon(k(l),l))/p}{p}\Big)$$

foe $i = 0,...,p-1$. This implies $|\chi(R \cap L| = \sqrt{p}$ for all characters of L nontrivial on N. Since no two elements of R are in the same coset of N, the character sum is also correct for all characters trivial on N. □

It is important for our purpose that the $(p,p,p,1)$-RDSs can be characterized completely. This result was independently obtained by Gluck (1990), Hiramine (1989) and Ronayi, T. Szönyi (1989).

Result 5.11 *Let p be an odd prime. A subset R of $G = \langle g \rangle \langle h \rangle \cong \mathbf{Z}_p \times \mathbf{Z}_p$ is a $(p, p, p, 1)$-RDS in G relative to $\langle g \rangle$ if and only if*

$$R = z \sum_{j=0}^{p-1} g^{tj^2} h^j$$

for some $z \in G$ and $t \in \{1, 2, ..., p-1\}$.

Combining Theorem 5.10 with Result 5.11 yields the following.

Theorem 5.12 *If p is an odd prime and R is a (p^3, p, p^3, p^2)-RDS in $G = \langle a \rangle \langle b \rangle \cong \mathbf{Z}_{p^2} \times \mathbf{Z}_{p^2}$ relative to $N = \langle a^p \rangle$, then*

$$R = \sum_{i,j=0}^{p-1} a^{x(i,j)p+i} b^{y(i,j)p+j} \sum_{s=0}^{p-1} a^{pt(i,j)s^2} b^{ps}$$

with $0 \le x(i,j),\ y(i,j), \le p-1$, $1 \le t(i,j) \le p-1$.

We are now going to use Theorem 5.12 together with some further observations to derive a necessary and sufficient condition for the existence of a (p^3, p, p^3, p^2)-RDS in $\mathbf{Z}_{p^2} \times \mathbf{Z}_{p^2}$. This reduces the complexity of the problem considerably, and thus we believe that our condition will be useful for the further study of these RDSs.

Lemma 5.13 *Let g be a generator of $G = \mathbf{Z}_p$. If the equation*

$$\sum_{i=0}^{p-1} g^{a_i} \sum_{s=0}^{p-1} g^{t_i s^2} = pg^a \sum_{j=0}^{p-1} g^{ts^2} \tag{9}$$

holds in $\mathbf{Z}G$ with $0 \le a_i,\ a \le p-1$ and $1 \le t_i,\ t \le p-1$, then $a_0 = \cdots a_{p-1} = a$ and $\left(\frac{t_0}{p}\right) = \cdots \left(\frac{t_{p-1}}{p}\right) = \left(\frac{t}{p}\right)$.

Proof Let χ be the character of G defined by $\chi(x) = e^{2\pi i/p} =: \xi$. It is well known [Lidl, Niederreiter (1994, Thm. 5.15)] that $S := \sum_{i=1}^{p-1} \left(\frac{i}{p}\right) \xi^i = \sqrt{(-1)^{(p-1)/2} p}$. From (9) we get

$$S \sum_{i=0}^{p-1} \xi^{a_i} \left(\tfrac{t_i}{p}\right) = pS\xi^a \left(\tfrac{t}{p}\right).$$

Using the Cauchy-Schwarz inequality, we conclude $\xi^{a_i}\left(\frac{t_i}{p}\right) = \xi^a\left(\frac{t}{p}\right)$ for all i proving the lemma. □

In the following, we will consider $x(i,j)$, $y(i,j)$ and $t(i,j)$ from Theorem 5.12 as functions from $\mathbf{Z}_p \times \mathbf{Z}_p$ to $\mathbf{Z}_p$. We define a function f in the following way. For every triple (r,j,l), $0 \le r,\ j,l \le p-1$ there is exactly one pair $(i, f(r,j,l))$ with $0 \le i,\ f(r,j,l) \le p-1$ with $r + lj = i + pf(r,j,l)$. Using the notation of Lemma 5.1 and Theorem 5.12, a straightforward calculation gives

$$\rho_{k,l}(R) = \sum_{r=0}^{p-1} \bar{a}^r \sum_{j=0}^{p-1} \bar{a}^{pQ(r,j,k,l)} \sum_{s=0}^{p-1} \bar{a}^{pt(r+lj,j)s^2} \tag{10}$$

where

$$Q(r,j,k,l) = -f(r,j,l) + x(r+lj,j) - ly(r+lj,j) - kj - l^2(4t(r+lj,j))^{-1}$$

(note that t only takes values in $\mathbf{Z}_p \setminus \{0\}$, so the inverse of $4t(r+lj,j)$ in $\mathbf{Z}_p$ exists). On the other hand, we know from Lemma 5.1 that

$$\rho_{k,l}(R) = p(\bar{G} - \bar{a}^{\epsilon(k,l)}\langle \bar{a}^p \rangle) + p\bar{a}^{\epsilon(k,l)} \sum_{i=0}^{p-1} \bar{a}^{pd(k,l)i^2} \tag{11}$$

where $d(k,l) \in \mathbf{Z}_p$ with $\left(\frac{d(k,l)}{p}\right) = \delta(k,l)$. Now we compare coefficients in (10) and (11) and arrive at the following. We write $\epsilon(k,l) = p\alpha(k,l) + \beta(k,l)$ with $0 \le \alpha(k,l),\ \beta(k,l) \le p-1$.

(i) $Q(\beta(k,l),j,k,l) = \alpha(k,l)$ and $\left(\frac{t(\beta(k,l)+lj,j)}{p}\right) = \left(\frac{d(k,l)}{p}\right)$ for $j = 0,...,p-1$ and all k,l (this follows from Lemma 5.13).

(ii) $\{Q(\beta(k,l),j,k',l) : j = 0,...,p-1\} = \mathbf{Z}_p$ for all $k \neq k'$ (this follows from (i) togther with $Q(r,j,k',l) = (k'-k)j + Q(r,j,k,l)$).

(iii) $\{\beta(k,l) : k = 0,...,p-1\} = \mathbf{Z}_p$ (this follows from (ii)).

Let $\mathbf{Z}_p^{\square}$ denote the set of nonzero squares in $\mathbf{Z}_p$.

Theorem 5.14 *Let p be an odd prime. A (p^3,p,p^3,p^2)-RDS in $\mathbf{Z}_{p^2} \times \mathbf{Z}_{p^2}$ exists if and only if there are functions $x,y : \mathbf{Z}_p \times \mathbf{Z}_p \to \mathbf{Z}_p$ and $t : \mathbf{Z}_p \times \mathbf{Z}_p \to \mathbf{Z}_p^{\square}$ such that the function Q defined by*

$$Q(r,j,k,l) = -f(r,j,l) + x(r+lj,j) - ly(r+lj,j) - kj - l^2(4t(r+lj,j))^{-1}$$

satisfies the following condition.
$(*)$ *For every pair* (k,l)*,* $0 \leq k,\ l \leq p-1$*, there exists exactly one* $r(k,l)$*,* $0 \leq r(k,l) \leq p-1$ *with*

$$|\{Q(r(k,l),j,k,l) : j = 0,...,p-1\}| = 1.$$

Proof We first show that $(*)$ is necessary. From (i) we know that we have $|\{Q(\beta(k,l),j,k,l) : j = 0,...,p-1\}| = 1$ for all k,l. This shows that we can take $r(k,l) = \beta(k,l)$ in $(*)$. Furthermore, no $r' \neq \beta(k,l)$ can satisfy $(*)$ because of (ii).
It remains to show that t can be assumed to takes values in $\mathbf{Z}_p^{\square}$ only. W.l.o.g., we can assume $\left(\frac{d(0,0)}{p}\right) = 1$. Then (i) implies $\left(\frac{t(\beta(0,0),j)}{p}\right) = 1$ for $j = 0,...,p-1$. Let $(x,y) \in \mathbf{Z}_p \times \mathbf{Z}_p$ be arbitrary. We choose $j_0 \neq y$ and let $l = \frac{x-\beta(0,0)}{y-j_0}$. Then by (iii), we can find k with $\beta(k,l) = \frac{y\beta(0,0)}{y-j_0}$. Note that $x = \beta(k,l) + ly$ and $\beta(0,0) = \beta(k,l) + lj_0$. Thus by (i) we get $\left(\frac{t(x,y)}{p}\right) = \left(\frac{t(\beta(0,0),j_0)}{p}\right) = 1$. Hence t indeed can be assumed to take values in $\mathbf{Z}_p^{\square}$ only.

Now we show that $(*)$ is also sufficient for the existence of an RDS. Assume that $(*)$ holds and define $z(k,l)$ by $\{Q(r(k,l),j,k,l) : j = 0,...,p-1\} = \{z(k,l)\}$. Recall

$$\rho_{k,l}(R) = \sum_{r=0}^{p-1} \bar{a}^r \sum_{j=0}^{p-1} \bar{a}^{pQ(r,j,k,l)} \sum_{s=0}^{p-1} \bar{a}^{pt(r+lj,j)s^2}.$$

From $(*)$ we conclude $\{Q(r(k,l),j,k',l) : j = 0,...,p-1\} = \mathbf{Z}_p$ for all $k' \neq k$ and all l. Also, $\{r(k,l) : k = 0,...,p-1\} = \mathbf{Z}_p$ for all l. Hence, for fixed k and l, we have

$$\{Q(r,j,k,l) : j = 0,...,p-1\} = \mathbf{Z}_p$$

for all $r \neq r(k,l)$. Thus, recalling $\left(\frac{t(i,j)}{p}\right) = 1$ for all i,j, we get

$$\begin{aligned}\rho_{k.l}(R) &= \sum_{r\neq r(k,l)} \bar{a}^r \langle \bar{a}^p \rangle \sum_{s=0}^{p-1} \bar{a}^{pj^2} + p\bar{a}^{r(k,l)+pz(k,l)} \sum_{j=0}^{p-1} \bar{a}^{pj^2} \\ &= p(\bar{G} - \langle \bar{a}^p \rangle \bar{a}^r(k,l)) + p\bar{a}^{r(k,l)+pz(k,l)} \sum_{j=0}^{p-1} \bar{a}^{pj^2}.\end{aligned}$$

Hence the equation in Lemma 5.1 holds for all k,l with $\delta(k,l) = 1$ and $\epsilon(k,l) = r(k,l) + pz(k,l)$.

Since every character nontrivial on N is trivial on some $U_{k,l}$, we know that all these characters have a correct character sum on R. From the definition of R it is clear that every coset of N contains exactly one element of R. Hence the nontrivial characters trivial on N have also the right character sum, and this concludes the proof. □

Remark Condition $(*)$ seems to be too strong to admit solutions. We conjecture that actually there are no functions x, y and t satisfying $(*)$. For $p = 3$ this was shown by C. Remling (1996), hence there is no $(27, 3, 27, 9)$-RDS in $\mathbf{Z}_9 \times \mathbf{Z}_9$. We think that Theorem 5.14 is a good starting point for further investigation of these RDSs.

6 References

K.T. Arasu, J.A. Davis, J. Jedwab: A nonexistence result for abelian Menon difference sets using perfect binary arrays. Combinatorica, 15 (1995), 311-317.

R.C. Bose: An affine analogue of Singer's theorem. J. Indian Math. Soc. 6 (1942), 1-15.

A.T. Butson: Generalized Hadamard matrices. Proc. Amer. Math. Soc. 13 (1962), 894-898.

A.T. Butson: Relations among generalized Hadamard matrices, relative difference sets, and maximal length linear recurring sequences. Can. J. Math. 15 (1963), 42-48

Y.Q. Chen, D.K. Ray-Chaudhuri, Q. Xiang: Constructions of Partial Difference Sets and Relative Difference Sets Using Galois Rings II. J. Combin. Theory Ser. A 76 (1996), 179-196.

J.A. Davis: Difference sets in abelian 2-groups. J. Comb. Theory A 57 (1991), 262-286.

J.A. Davis: A note on products of relative difference sets. Des. Codes Cryptogr. 1 (1991), 117-119.

J.A. Davis: Constructions of relative difference sets in p-groups. Discrete Math. 103 (1992), 7-15.

J.A. Davis, J. Jedwab: A Unifying Construction for Difference Sets. J. Combin. Theory A 80 (1997), 13-78.

J.A. Davis, J. Jedwab, M. Mowbray: New Families of Semi-Regular Relative Difference Sets. Des. Codes Cryptogr. 13 (1998), 131-146.

J.A. Davis, S.K. Sehgal: Using the Simplex code to construct relative difference sets in 2-groups. Des. Codes Cryptogr. 11 (1997), 267-277.

W. de Launey, P. Vijay Kumar: On circulant generalized Hadamard matrices of prime power order. Unpublished manuscript (1985).

J.E.H. Elliott, A.T. Butson: Relative difference sets. Illinois J. Math. 10 (1966), 517-531.

D. Gluck: A note on permutation polynomials and finite geometries. Discrete Math. 80 (1990), 97-100.

Y. Hiramine: A conjecture on affine planes of prime order. J. Comb. Theory A 52 (1989), 44-50.

R.G. Kraemer: Proof of a conjecture on Hadamard 2-groups. J. Comb. Theory A (1993), 1-10.

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

R. Lidl, H. Niederreiter: Introduction to finite fields and their application. Cambridge University Press (1994).

S.L. Ma: Polynomial addition sets. Ph.D. thesis. University of Hong Kong (1985).

S.L. Ma, A. Pott: Relative difference sets, planar functions and generalized Hadamard matrices. J. Algebra 175 (1995), 505-525.

S.L. Ma, B.Schmidt: On (p^a, p, p^a, p^{a-1})-relative difference sets. Des. Codes Cryptogr. 6 (1995), 57-72.

S.L. Ma, B.Schmidt: A Sharp Exponent Bound for McFarland Difference Sets with $p = 2$. J. Combin. Theory A 80 (1997), 347-352.

B.R. MacDonald: Finite rings with identity. New York, Marcel Dekker (1974).

A. Pott: On the structure of abelian groups admitting divisible difference sets. J. Comb. Theory A 65 (1994), 202-213.

A.Pott: Finite Geometry and Character Theory. Springer Verlag, Berlin/ Heidelberg/New York (1995).

A. Pott: A survey on relative difference sets. In: Groups, Difference Sets and the Monster. Eds. K.T. Arasu, J.F. Dillon, K. Harada, S.K. Seghal, R.L. Solomon. DeGruyter Verlag, Berlin/New York (1996), 195-233.

L. Ronayi, T. Szönyi: Planar functions over finite fields. Combinatorica 9 (1989), 315-320.

D.K. Ray-Chaudhuri, Q. Xiang: Constructions of Partial Difference Sets and Relative Difference Sets Using Galois Rings. Des. Codes Cryptogr. 8 (1996), 215-227.

C. Remling: Nonexistence of $(27, 3, 27, 9)$-relative difference sets in $\mathbf{Z}_9 \times \mathbf{Z}_9$. Manuscript (1996).

B. Schmidt: On (p^a, p^b, p^a, p^{a-b})-relative difference sets. J. Alg. Combin. 6 (1997), 279-297.

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