J Algebr Comb (2009) 29: 91–106
DOI 10.1007/s10801-008-0124-5

Relative (pn, p, pn, n)-difference sets with $GCD(p, n) = 1$

Tao Feng

Received: 31 August 2007 / Accepted: 17 January 2008 / Published online: 24 January 2008

Abstract Let p be an odd prime. We first get some non-existence and structural results on (pn, p, pn, n) relative difference sets with $gcd(p, n) = 1$ through a group ring approach. We then give a construction of $(p(p+1), p, p(p+1), p+1)$ relative difference sets with p a Mersenne prime.

Keywords Relative difference set · Group ring · Semi-regular relative difference set

1 Introduction

Let G be a finite (multiplicative) group of order mn, and let N be a subgroup of G of order n. A k-subset R of G is called an (m, n, k, λ) *relative difference set* (RDS) in G relative to N if every element $g \in G \setminus N$ has exactly λ representations $g = r_1 r_2^{-1}$ with $r_1, r_2 \in R$, and no non-identity element of N has such a representation. The subgroup N is usually called *the forbidden subgroup*. We say that R is a *splitting* RDS if the forbidden subgroup N is a direct factor G. If the group G is Abelian (resp. non-Abelian), then D is called an *Abelian (resp. non-Abelian) relative difference set*. When $n = 1$, R is an (m, k, λ) difference set in the usual sense. If $k = n\lambda$, then R is called *semi-regular*.

For a subset X of G, we set $X^{(-1)} = \{x^{-1} \mid x \in X\}$; also we use the same X to denote the group ring element $\sum_{x \in X} x \in \mathbb{Z}[G]$. Then, a k-subset R of G is an (m, n, k, λ) relative difference set in G relative to N if and only if it satisfies the following equation in the group ring $\mathbb{Z}[G]$:

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

Supported by National Natural Science Foundation of China (10331030).

T. Feng (✉)
School of Mathematical Sciences, Peking University, Beijing 100871, People's Republic of China
e-mail: ift@pku.edu.cn

A prime p is called self-conjugate modulo an integer n if there is some integer j such that $p^j \equiv -1 \bmod n'$ where n' is the largest divisor of n coprime with p. For a positive integer m, we denote by ξ_m a primitive m-th root of unity in $\mathbb{C}$.

The following lemma is very useful in the study of semi-regular relative difference sets.

Lemma 1 [13, Theorem 4.1.1] *Let R be an Abelian $(m, n, m, m/n)$ RDS in G relative to N. Then $exp(G)|m$ or $G = \mathbb{Z}_4$, $n = 2$.*

There has been extensive research on (p^a, p^b, p^a, p^{a-b}) RDSs with p a prime, see [10, 13, 14] and the references there. In this present paper, we study Abelian relative (pn, p, pn, n) difference sets with p an odd prime not dividing n through a group ring approach. In [9], the authors showed that there is no Abelian (pq, q, pq, p) RDS in $\mathbb{Z}_p \times \mathbb{Z}_q^2$ with p, q being two distinct odd primes such that $p > q$, extending the result in [5]. In [7], the authors showed that there is no Abelian $(3pq, 3, 3pq, pq)$ RDS in $\mathbb{Z}_3^2 \times \mathbb{Z}_p \times \mathbb{Z}_q$ with p, q being two distinct primes larger than 3. According to Lemma 1, they have shown that there is no Abelian relative difference set with the corresponding parameters. In both papers the authors investigated the character values of the corresponding relative difference sets.

Now we assume p is an odd prime and n is a positive integer such that $gcd(p, n) = 1$. Let G be an Abelian group containing a (pn, p, pn, n) RDS R relative to a subgroup N of size p. Then in view of Lemma 1, we must have the Sylow p-subgroup of G elementary Abelian. Hence $G = \mathbb{Z}_{p^2}$ does not contain a $(p, p, p, 1)$ RDS. When $G = \mathbb{Z}_p^2$, $N = \{0\} \times \mathbb{Z}_p$, according to a result in [6], a $(p, p, p, 1)$ RDS in G relative to N must be of the form

$$L_{u,v,w} := \{(i, ui^2 + vi + w) : i \in \mathbb{Z}_p\}, \quad u, v, w \in \mathbb{Z}_p, u \neq 0.$$

In the sequel, we will assume that $n > 1$. Throughout this paper, we will fix the following notations: We write $G = E \times W$, where $|E| = n$, and $W = \langle a, b : a^p = b^p = 1, ab = ba \rangle$, $N = \langle b \rangle < W$. Also write $e := exp(E)$, $L := \langle a \rangle$, $H := E \times L$, and suppose R is a (pn, p, pn, n) RDS in G relative to N.

We will frequently view an integer m as an element of $\mathbb{Z}_p$ in the natural way, and will indicate which ring it is considered in if necessary. We make no distinction between $\mathbb{Z}_p$ and $\mathbb{F}_p$, the finite field with p elements. Since we will take summations over $\mathbb{Z}_p$ most of the time, we abbreviate $\sum_x$ for $\sum_{x \in \mathbb{Z}_p}$. The Legendre symbol for $\mathbb{Z}_p$ is written as $\left(\frac{\cdot}{p}\right)$. A constant we will use is defined by $\Delta = \sum_{i=1}^{p-1} \left(\frac{i}{p}\right) \xi_p^i$, which is a Gauss sum and satisfies $\Delta\overline{\Delta} = p$, see [2, p. 11].

In Section 2, we give the basic facts about group rings and some lemmas we need. In Section 3, we take a group ring approach and get some non-existence and structural results when p is self-conjugate modulo $exp(E)$. In the last section, we give a construction of $(p(p+1), p, p(p+1), p+1)$ RDSs with p a Mersenne prime. A Mersenne prime is an odd prime p such that $p + 1 = 2^r$ for some integer $r > 0$.

2 Preliminaries

In this section, we introduce the basic facts about the group ring $\mathbb{F}_p[G]$, see [12] or [11]. First we list some basic equations which holds in $\mathbb{F}_p[G]$. Let x be an element of order p in G. Then

$$(x-1)^{p-1} = \sum_{i=0}^{p-1} \binom{p-1}{i} (-1)^{p-1-i} x^i = \sum_{i=0}^{p-1} x^i,\ (x-1)^p = x^p - 1 = 0, \quad (2.1)$$

$$(x^{-1}-1)^i = (1-x)^i (x-1+1)^{p-i} = (-1)^i \sum_{k=0}^{p-i} \binom{p-i}{k} (x-1)^{k+i}, \quad (2.2)$$

for each $0 \le i \le p-1$. A standard $\mathbb{F}_p$-basis for $\mathbb{F}_p[G]$ is given by $\{hb^i : h \in H, i \in \mathbb{Z}_p\}$, but the following basis will be more convenient for our purpose:

$$\{h(b-1)^i : h \in H, i \in \mathbb{Z}_p\}.$$

The fact that this is a basis follows from that $hb^i = h(b-1+1)^i = \sum_{k=0}^{i} \binom{i}{k} h(b-1)^k$ for each $0 \le i \le p-1$, $h \in H$. Therefore each element $\alpha \in \mathbb{F}_p[G]$ can be written in the form $\alpha = \sum_{i=0}^{p-1} \alpha_i (b-1)^i$ with $\alpha_i \in \mathbb{F}_p[H]$. The merit of this basis is that, denoting by I_i the principal ideal generated by $(b-1)^i$ in $\mathbb{F}_p[G]$ for each $0 \le i \le p$, we have

$$\mathbb{F}_p[G] = I_0 \supset I_1 \supset \cdots \supset I_p = 0,$$

which is a chain of descending ideals in $\mathbb{F}_p[G]$ such that $I_i I_j \subseteq I_{i+j}$, where we define $I_k := 0$ when $k > p$. An $\mathbb{F}_p$-basis for $\mathbb{F}_p[H]$ can be obtained in the same fashion as above with a, E in place of b, H.

The augmentation homomorphism $\omega : \mathbb{F}_p[G] \mapsto \mathbb{F}_p$ is defined by $\omega(\sum_{g\in G} a_g g) = \sum_{g\in G} a_g$, with $a_g \in \mathbb{F}_p$. The kernel of ω is called the augmentation ideal, which is generated by elements of the form $g-1$, $\forall g \in G$. If $\beta = \sum_{g\in G} b_g g$ is annihilated by the augmentation ideal, i.e.,

$$\beta(h-1) = \sum_{g\in G} b_g gh - \sum_{g\in G} b_g g = 0$$

for all $h \in G$, then $b_1 = b_h$ for any $h \in G$ by comparing the coefficients of h on both sides, so $\beta = b_1 G$. The following lemmas will be the starting point for our study in the next section.

Lemma 2 *Let p be an odd prime and $H = E \times \langle a : a^p = 1\rangle$ be an Abelian group with $|E| = n$, $(p,n) = 1$. Write $L := \langle a\rangle$. Suppose $T \in \mathbb{F}_p[H]$ satisfies $TT^{(-1)} = \lambda XL$ for some $X \in \mathbb{F}_p[E]$ and $\lambda \in \mathbb{F}_p$. Write $T = \sum_{i=0}^{p-1} A_i (a-1)^i$, with $A_i \in \mathbb{F}_p[E]$. Then we have $\left(\frac{-1}{p}\right)\lambda\,\omega(X)$ is a square in $\mathbb{F}_p$ and*

$$A_i A_j^{(-1)} = 0, \forall\, i + j < p-1. \quad (2.3)$$

Proof By direct computations using (2.2) with $x = a$, we have

$$T^{(-1)} = \sum_{k=0}^{p-1} \left(\sum_{i=0}^{k} (-1)^i A_i^{(-1)} \binom{p-i}{k-i} \right) (a-1)^k.$$

Write $TT^{(-1)} = \sum_k B_k (a-1)^k$ with $B_k \in \mathbb{F}_p[E]$. Then after expansion, we have

$$B_u = \sum_{k=0}^{u} A_{u-k} \left(\sum_{i=0}^{k} (-1)^i A_i^{(-1)} \binom{p-i}{k-i} \right), \forall\, 0 \le u \le p-1.$$

Here we have used the fact that $1,\ a-1, \cdots, (a-1)^{p-1}$ are linearly independent over $\mathbb{F}_p[E]$. From $TT^{(-1)} = \lambda X (a-1)^{p-1}$, we have $B_0 = \cdots = B_{p-2} = 0,\ B_{p-1} = \lambda X$.

We show that (2.3) holds by induction on $i + j$. When $i = j = 0,\ B_0 = A_0 A_0^{(-1)} = 0$. When $i + j = 1,\ B_1 = -A_0 A_1^{(-1)} + A_1 A_0^{(-1)} = 0$, multiplying both sides with $A_0 A_1^{(-1)}$, we have $(A_0 A_1^{(-1)})^2 = A_0 A_1^{(-1)} A_1 A_0^{(-1)} = 0$. Since $(p, |E|) = 1$, we know that $\mathbb{F}_p[E]$ is semisimple and hence contains no non-zero nilpotent elements, so we must have $A_0 A_1^{(-1)} = 0$; after taking conjugation, we have $A_1 A_0^{(-1)} = 0$. This proves the claim for $i + j = 0, 1$. Now assume this is true when $i + j = k$ and $k + 1 < p - 1$. By $B_{k+1} = 0$ and the induction, we have $\sum_{l=0}^{k+1} (-1)^l A_{k+1-l} A_l^{(-1)} = 0$. Notice that $A_{k+1-l} A_l^{(-1)} A_{k+1-r} A_r^{(-1)} = 0$ whenever $l \neq r$, since $A_{k+1-l} A_r^{(-1)} = 0$ or $A_{k+1-r} A_l^{(-1)} = 0$ by the induction. Multiplying both sides with $A_i A_{k+1-i}^{(-1)},\ 0 \le i \le k+1$, we have $(A_i A_{k+1-i}^{(-1)})^2 = 0$, and hence $A_i A_{k+1-i}^{(-1)} = 0$. This proves (2.3).

From (2.3) we have $\omega(A_i A_i^{(-1)}) = \omega(A_i)^2 = 0$, i.e., $\omega(A_i) = 0, \forall\, i < \frac{p-1}{2}$. Now from $B_{p-1} = \lambda X$, we have $\sum_{l=0}^{p-1} (-1)^l A_{p-1-l} A_l^{(-1)} = \lambda X$. By taking augmentation, we have $(-1)^{\frac{p-1}{2}} \omega(A_{\frac{p-1}{2}})^2 = \lambda\, \omega(X)$, i.e. $\omega(A_{\frac{p-1}{2}})^2 = \left(\frac{-1}{p}\right) \lambda\, \omega(X)$. This completes the proof of the lemma. □

Lemma 3 *Take the same notations as in Lemma 2. If we assume that $X = E$, then*

$$A_i A_j^{(-1)} = 0,\ \forall i + j \le p-1, (i,j) \neq (\frac{p-1}{2}, \frac{p-1}{2}); \tag{2.4}$$

$$A_{\frac{p-1}{2}} A_{\frac{p-1}{2}}^{(-1)} = \left(\frac{-1}{p}\right) \lambda E. \tag{2.5}$$

Further, if p is self-conjugate modulo $exp(E)$, then $A_i = 0$ for $i < \frac{p-1}{2}$, and $A_{\frac{p-1}{2}} = tE$ for some $t \in \mathbb{F}_p$ such that $\lambda = \left(\frac{-1}{p}\right) t^2 n$.

Proof Now we assume that $X = E$ and continue the induction process in the proof of Lemma 2 with $k + 1 = p - 1$. Multiplying both sides of $\sum_{l=0}^{p-1} (-1)^l A_{p-1-l} A_l^{(-1)} = \lambda E$ with $A_{p-1-i} A_i^{(-1)},\ i \neq \frac{p-1}{2}$, we have $A_{p-1-i} A_i^{(-1)} E = \omega(A_{p-1-i}) \omega(A_i) E = 0$ since $\omega(A_{p-1-i}) = 0$ or $\omega(A_i) = 0$ depending on whether $i > \frac{p-1}{2}$ or $i < \frac{p-1}{2}$.

Hence $(A_{p-1-i}A_i^{(-1)})^2 = 0$, and it follows that $A_{p-1-i}A_i^{(-1)} = 0$ when $i \neq \frac{p-1}{2}$. It follows that

$$\left(\frac{-1}{p}\right)A_{\frac{p-1}{2}}A_{\frac{p-1}{2}}^{(-1)} = \sum_{l=0}^{p-1}(-1)^l A_{p-1-l}A_l^{(-1)} = \lambda E.$$

Now further assume that $p^j \equiv -1 \bmod e = exp(E)$ for some j. Then $A_i^{(-1)} = A_i^{(p^j)} = A_i^{p^j}$. From $A_i A_i^{(-1)} = 0$, $\forall i < \frac{p-1}{2}$, we have $A_i^{1+p^j} = 0$. It follows that A_i is a nilpotent element in $\mathbb{F}_p[E]$ which has got to be 0. From $A_{\frac{p-1}{2}}^{1+p^j} = A_{\frac{p-1}{2}}A_{\frac{p-1}{2}}^{(-1)} = \left(\frac{-1}{p}\right)\lambda E$, we have $\left((g-1)A_{\frac{p-1}{2}}\right)^{1+p^j} = \left(\frac{-1}{p}\right)\lambda E(g-1)^{1+p^j} = 0$, so $(g-1)A_{\frac{p-1}{2}}$ is nilpotent and hence is 0 for any $g \in E$. It follows that $A_{\frac{p-1}{2}} = tE$ for some $t \in \mathbb{F}_p$, and $t^2 nE = (tE)(tE^{(-1)}) = \left(\frac{-1}{p}\right)\lambda E$, that is, $\lambda = \left(\frac{-1}{p}\right)t^2 n$ in $\mathbb{F}_p$. This completes the proof of the lemma. □

3 The group ring approach

In this section, we mainly use Lemmas 2 and 3 to get some non-existence and structural results, especially when $p = 5, 7$. We take the same notations as introduced in Section 1, and assume that $p > 3$. Because R intersects each coset of N in a unique element, we have $R \cap hN = \{b^{f(h)}h\}$ for each $h \in H$, where $f(h)$ is some element in $\{0, 1, \cdots, p-1\}$ depending on h. It follows that $R = \sum_{h\in H} b^{f(h)}h$ since a set of coset representatives for N in G is H. In $\mathbb{F}_p[G]$, we have

$$R = \sum_{h\in H}(b-1+1)^{f(h)}h = \sum_{h\in H}\sum_{i=0}^{f(h)}\binom{f(h)}{i}(b-1)^i h = \sum_{i=0}^{p-1}\sum_{h\in H}\binom{f(h)}{i}(b-1)^i h,$$

since $\binom{n}{k} = 0$ when $k > n$. Write $R = \sum_{i=0}^{p-1} R_i(b-1)^i$ with $R_i \in \mathbb{F}_p[H]$. Then we have

$$R_i = \sum_{h\in H}\binom{f(h)}{i}h \tag{3.1}$$

by comparing the coefficients of $(b-1)^i$, $\forall\, 0 \leq i \leq p-1$; especially, $R_0 = H$, $R_1 = \sum_{h\in H} f(h)h$. We can recover $R \cap hN$ from the coefficient $f(h)$ of h in R_1, namely, $R \cap hN = \{b^{f(h)}h\}$. Therefore R_1 determines R completely, and this fact will be utilized below.

Now let us check the group ring equation

$$RR^{(-1)} = pn + n(G-N) = n(HN-N) = n(H-1)(b-1)^{p-1}$$

in $\mathbb{F}_p[G]$, where we have used the fact $N = (b-1)^{p-1}$, see (2.1) . First,

$$R^{(-1)} = H - R_1^{(-1)}(b-1) + (R_1+R_2)^{(-1)}(b-1)^2 + X(b-1)^3$$

for some $X \in \mathbb{F}_p[G]$ by direct computations using (2.2). Write $RR^{(-1)} = \sum_{i=0}^{p-1} C_i(b-1)^i$. Then we have from the above:

$$C_0 = H^2 = pnH = 0;$$
$$C_1 = -HR_1^{(-1)} + R_1H = -\omega(R_1^{(-1)})H + \omega(R_1)H = 0;$$
$$C_2 = -R_1R_1^{(-1)} + \lambda_1 H = 0,$$

for some $\lambda_1 \in \mathbb{F}_p$. The first two equations are trivially true and the expressions of C_k for $k > 2$ are complicated for a general p and we do not need them except when $p = 5$, so we will mainly study the equation $C_2 = 0$ at first, i.e.,

$$R_1R_1^{(-1)} = \lambda_1 H. \tag{3.2}$$

If we can get some information about R_1, then we get information about R by our earlier observation. For this purpose, we need to determine λ_1. We first define the number $a_i := |f^{-1}(i)|$, the number of pre-images of $i \in \{0, 1, \cdots, p-1\}$ under f, and we shall regard i as an element of $\mathbb{Z}_p$ below. By computing the coefficients of the group identity 1_H on both sides of (3.2), we have

$$\lambda_1 = \sum_i a_i i^2. \tag{3.3}$$

To determine λ_1, we need to shift to $\mathbb{Z}[G]$ for a moment. For the character χ of G which is principal on H and maps b to ξ_p, we have $\chi(R)\overline{\chi(R)} = pn$. By a standard process of analyzing the prime ideal decompositions of both sides in $\mathbb{Z}[\xi_p]$, see [1] for example, we have $\chi(R) = g(\xi_p)\Delta$, where $g(x) \in \mathbb{Z}[x]$ and $|g(\xi_p)|^2 = n$. On the other hand, $\chi(R) = \sum_i a_i\xi_p^i$, so $\sum_i a_i\xi_p^i = g(\xi_p)\Delta$. Multiplying both sides with $\overline{\Delta} = \left(\frac{-1}{p}\right)\Delta$, we get that p divides

$$\sum_k b_k\xi_p^k := \left(\sum_i a_i\xi_p^i\right)\left(\sum_j \left(\frac{-j}{p}\right)\xi_p^j\right),$$

where $b_k = \sum_i \left(\frac{-k+i}{p}\right)a_i$. That is, $p|\sum_{k=1}^{p-1}(b_k - b_0)\xi_p^k$. Since $\xi_p, \cdots, \xi_p^{p-1}$ forms an integral basis of $\mathbb{Z}[\xi_p]$, we have $p|(b_k - b_0)$, i.e., $b_k \equiv c \bmod p$ for some constant c. Write $b_k = pd_k + c$. Then from the fact that $\sum_k b_k\xi_p^k = p\sum_k d_k\xi_p^k$ has modulus $p\sqrt{n}$, we have $\sum_k d_k\xi_p^k$ has modulus $\sqrt{n}$, i.e.,

$$\left(\sum_k d_k\xi_p^k\right)\left(\sum_k d_k\xi_p^{-k}\right) = n.$$

It follows that $(\sum_k d_k)^2 \equiv n \bmod (1-\xi_p)\mathbb{Z}[\xi_p] \cap \mathbb{Z}$, i.e., $(\sum_k d_k)^2 \equiv n \bmod p$. Meanwhile,

$$\sum_k b_k = p\left(\sum_k d_k + c\right) = \sum_k\sum_i \left(\frac{-k+i}{p}\right)a_i = \sum_i\sum_k \left(\frac{-k+i}{p}\right)a_i = 0,$$

so $c = -\sum_k d_k$. Therefore, we have $c^2 \equiv n \bmod p$.

Now we shift back to $\mathbb{F}_p[G]$ again. We have

$$b_k = \sum_i \left(\frac{-k+i}{p}\right) a_i = \sum_i (i-k)^{\frac{p-1}{2}} a_i.$$

Direct computations show that

$$(i^{\frac{p-1}{2}}, (i+1)^{\frac{p-1}{2}}, \cdots, (i+\frac{p-1}{2})^{\frac{p-1}{2}}) = (i^{\frac{p-1}{2}}, i^{\frac{p-3}{2}}, \cdots, 1) M_1 M_2,$$

where $M_1 = diag(1, \binom{\frac{p-1}{2}}{1}, \cdots, \binom{\frac{p-1}{2}}{\frac{p-1}{2}})$, and M_2 is a Vandermonde matrix with (k,t)-th entry t^{k-1}. Both of M_1, M_2 are non-degenerate, so

$$(i^{\frac{p-1}{2}}, i^{\frac{p-3}{2}}, \cdots, 1) = (i^{\frac{p-1}{2}}, (i+1)^{\frac{p-1}{2}}, \cdots, (i+\frac{p-1}{2})^{\frac{p-1}{2}}) M_2^{-1} M_1^{-1},$$

and hence we can write i^2 as a $\mathbb{F}_p$-linear combination of $i^{\frac{p-1}{2}}, (i+1)^{\frac{p-1}{2}}, \cdots, (i+\frac{p-1}{2})^{\frac{p-1}{2}}$. It follows that we can find a set of $\alpha_k \in \mathbb{F}_p$ such that $\sum_k \alpha_k (i-k)^{\frac{p-1}{2}} = i^2$. Then we have

$$\sum_k \alpha_k b_k = \sum_k \alpha_k \sum_i (i-k)^{\frac{p-1}{2}} a_i = \sum_i a_i \sum_k \alpha_k (i-k)^{\frac{p-1}{2}} = \sum_i i^2 a_i.$$

On the other hand, $b_k = c$ in $\mathbb{F}_p$ for each $k \in \mathbb{Z}_p$. Therefore, from (3.3), we have $\lambda_1 = (\sum_k \alpha_k) c$. Notice that $\sum_k \alpha_k$ is the coefficient of $i^{\frac{p-1}{2}}$ in $\sum_k \alpha_k (i-k)^{\frac{p-1}{2}} = i^2$, so $\lambda_1 = c$, $\lambda_1^2 = n$ when $p = 5$, and $\lambda_1 = 0$ when $p > 5$. This completes the determination of λ_1. We record it below.

Proposition 4 *Notations as above. Then $\lambda_1^2 = n$ in $\mathbb{F}_p$ when $p = 5$, and $\lambda_1 = 0$ when $p > 5$.*

When $p = 5$, set $T := R_1$, $X := E$, $\lambda := \lambda_1$ and invoke Lemma 2, we have the following result:

Proposition 5 *Suppose there is an Abelian $(5n, 5, 5n, n)$ RDS with $5 \nmid n$. Then $n \equiv 1$ mod 5.*

Proof Assume that $n > 1$. We have $\lambda_1 n = (\frac{-1}{5}) \lambda_1 n$ is a non-zero square in $\mathbb{F}_5$ by Lemma 2, so $(\lambda_1 n)^2 = 1$. From the above arguments, we have $\lambda_1^2 = n$ in $\mathbb{F}_5$. Therefore, $(\lambda_1 n)^2 = \lambda_1^6 = \lambda_1^2 = 1$, and hence $n \equiv 1 \bmod 5$. □

Now, we consider the case $p = 5$ and 5 is self-conjugate mod $\exp(E)$.

Theorem 6 *If there is an Abelian $(5n, 5, 5n, n)$ RDS in G with $(5, n) = 1$, $n > 1$, then there is no integer j such that $5^j \equiv -1$ mod $exp(G)_{5'}$, the largest divisor of $exp(G)$ which is coprime with 5.*

Proof Notations as before. By Lemma 3, we have that

$$R_1 = tE(a-1)^2 + A_3(a-1)^3 + A_4(a-1)^4 \tag{3.4}$$

for some $A_3, A_4 \in \mathbb{F}_5[E]$, $t \neq 0$. Expanding, we have

$$\begin{aligned} R_1 = {} & (tE - A_3 + A_4) + (-2tE + 3A_3 + A_4)a + (tE - 3A_3 + A_4)a^2 \\ & + (A_3 + A_4)a^3 + A_4 a^4. \end{aligned}$$

Write $A_3 = \sum_{x\in E} a_x x$, $A_4 = \sum_{x\in E} b_x x$, with $a_x, b_x \in \mathbb{F}_p$, and define

$$B_{r,s} := \{x \in E : \ a_x = r, b_x = s\}$$

for each pair of $r, s \in \mathbb{Z}_p$. Then $\{B_{r,s} : r, s \in \mathbb{Z}_p\}$ forms a partition of E, and $A_3 = \sum_{r,s} r B_{r,s}$, $A_4 = \sum_{r,s} s B_{r,s}$. We can rewrite R_1 as

$$R_1 = \sum_{r,s}\sum_i \left(\frac{(i+1)(i+2)}{2}t - r(i+1) + s\right) a^i B_{r,s}.$$

Correspondingly, in $\mathbb{Z}[G]$, we have

$$R = \sum_{r,s}\sum_i b^{\frac{(i+1)(i+2)}{2}t - r(i+1)+s} a^i B_{r,s}. \tag{3.5}$$

This gives a structural characterization of R. We note that letting the automorphism of G which fixes H and maps b^t to b act on R if necessary, we can assume that $t = 1$, so the indeterminant t adds no complexity. From now on, we set $t = 1$.

We look at the expressions for C_3, C_4, and obtain by direct computations:

$$\begin{aligned} & R_1 R_2^{(-1)} = R_2 R_1^{(-1)}; \\ & R_2 R_2^{(-1)} - R_1 R_2^{(-1)} - R_1 R_3^{(-1)} - R_3 R_1^{(-1)} = -1 + \lambda_2 H, \end{aligned}$$

for some $\lambda_2 \in \mathbb{F}_5$. Here we have used the fact that $n = 1$ in $\mathbb{F}_5$. We have seen that $R_1 \in (a-1)\mathbb{F}_5[H]$ in (3.4). Take the homomorphism

$$\pi : \mathbb{F}_5[H] \mapsto \mathbb{F}_5[E] \cong \mathbb{F}_5[H]/(a-1)\mathbb{F}_5[H].$$

Then $\pi(R_2)\pi(R_2)^{(-1)} = -1 \in \mathbb{F}_5[E]$ from the second equation above. From (3.1) and (3.5), we have

$$\begin{aligned} R_2 = {} & \frac{1}{2}\sum_{r,s}\sum_i \left(\frac{(i+1)(i+2)}{2} - r(i+1) + s\right) \\ & \times \left(\frac{(i+1)(i+2)}{2} - r(i+1) + s - 1\right) a^i B_{r,s}, \\ \pi(R_2) = {} & \frac{1}{2}\sum_{r,s}\sum_i \left(\frac{(i+1)(i+2)}{2} - r(i+1) + s\right) \end{aligned}$$

$$\times\left(\frac{(i+1)(i+2)}{2}-r(i+1)+s-1\right)B_{r,s}$$
$$=\frac{-1}{8}\sum_{r,s}B_{r,s}=-2E\in\mathbb{F}_5[E].$$

Now we have $\pi(R_2)\pi(R_2)^{(-1)}=(-2E)^2=-nE=-E=-1$: a contradiction unless $E=1$! This completes the proof of the theorem. □

Example Take the notations introduced in Section 1. Theorem 6 says that $exp(E)$ can not be a divisor of 5^j+1 for any $j\geq 0$. For example, $exp(E)$ can not divide $5^3+1=2\times 9\times 7$. This rules out the existence of $(5n,\ 5,\ 5n,\ n)$ RDS in $G=\mathbb{Z}_5^2\times\mathbb{Z}_2^r\times\mathbb{Z}_3^s\times\mathbb{Z}_9^t\times\mathbb{Z}_7^u$ with $n=2^r\cdot 3^{s+2t}\cdot 7^u>1$. When p is an odd prime such that $p\equiv 2,3 \bmod 5$, we have by the quadratic reciprocity law, $(\frac{5}{p})=(\frac{p}{5})=-1$, so $5^{\frac{p-1}{2}}\equiv -1 \bmod p$, and we can not have $exp(E)|\,2p$.

For a general prime $p>5$, write $R=\sum_{h\in E}h\sum_i a^i b^{f_h(i)}$, with $f_h:\mathbb{Z}_p\mapsto\mathbb{Z}_p$. When p is self-conjugate mod $exp(E)$, Lemma 3 applies again, and we get

$$R_1=A_{\frac{p+1}{2}}(a-1)^{\frac{p+1}{2}}+\cdots+A_{p-1}(a-1)^{p-1},$$

with $A_i\in\mathbb{F}_p[E]$, $\frac{p+1}{2}\leq i\leq p-1$. We have

$$\begin{aligned}(a-1)^{p-1-k}&=\sum_{i=0}^{p-1-k}\binom{p-1-k}{i}(-1)^{p-1-k-i}a^i\\&=\sum_{i=0}^{p-1-k}\frac{(p-1-k)(p-2-k)\cdots(p-k-i)}{i!}(-1)^{k+i}a^i\\&=(-1)^k\sum_{i=0}^{p-1-k}\frac{(i+k)\cdots(k+1)}{i!}a^i\\&=(-1)^k\sum_{i=0}^{p-1-k}\binom{i+k}{k}a^i,\end{aligned}$$

when $0\leq k<\frac{p-1}{2}$. As a polynomial of i, $\binom{i+k}{k}=\frac{(i+k)\cdots(i+1)}{k!}$ has degree $k<\frac{p-1}{2}$. Now take a partition of E as in the case $p=5$, we see that $deg(f_h)<\frac{p-1}{2}$.

Especially when $p=7$, we have $R_1=A_4(a-1)^4+A_5(a-1)^5+A_6(a-1)^6$ with $A_i\in\mathbb{F}_7[E]$, $i=4,5,6$. Take the partition $\{B_{r,s,t}:r,s,t\in\mathbb{Z}_7\}$ of E such that

$$A_4=\sum_{r,s,t}rB_{r,s,t},\qquad A_5=\sum_{r,s,t}sB_{r,s,t},\qquad A_6=\sum_{r,s,t}tB_{r,s,t}.$$

Then by the same process as in the case $p = 5$, we have

$$R = \sum_{r,s,t} B_{r,s,t} \sum_i a^i b^{r\frac{(i+2)(i+1)}{2} - s(i+1)+t}.$$

When r, s, t ranges over $\mathbb{Z}_7 \times \mathbb{Z}_7 \times \mathbb{Z}_7$, $\sum_i a^i b^{r\frac{(i+2)(i+1)}{2} - s(i+1)+t}$ ranges over the set $\{L_{u,v,w} := \sum_i a^i b^{ui^2+vi+w} \mid u, v, w \in \mathbb{Z}_7\}$. Relabeling $B_{r,s,t}$, we have the result below.

Theorem 7 *Let n be a positive integer coprime with 7. Suppose R is a putative $(7n, 7, 7n, n)$ RDS in $G = E \times \langle a, b : a^7 = b^7 = 1, ab = ba\rangle$ relative to $N = \langle b\rangle$, and 7 is self-conjugate mod $exp(E)$. Then R is of the form*

$$R = \sum_{u,v,w} B_{u,v,w} \sum_i a^i b^{ui^2+vi+w},$$

where $\{B_{u,v,w} : u, v, w \in \mathbb{Z}_7\}$ forms a partition of E.

As a final application of Lemma 2, we have the following result which extends Proposition 5.

Proposition 8 *Let p be an odd prime and $n > 1$ be a positive integer coprime with p. If there is a (pn, p, pn, n) RDS R in an Abelian group G, then n is a square in $\mathbb{F}_p$.*

Proof We take the notations introduced at the beginning of this section. Write $R = \sum_{i=0}^{p-1} D_i(a-1)^i$ with $D_i \in \mathbb{F}_p[E \times N]$. Then from $RR^{(-1)} = pn + n(G - N)$ we have $D_0 D_0^{(-1)} = -nN$ in $\mathbb{F}_p[E \times N]$. Now an application of Lemma 2 gives that $-(\frac{-1}{p})n$ is a square in $\mathbb{F}_p$. When $p \equiv 1 \bmod 4$, -1 is a square in $\mathbb{F}_p$, hence $-(\frac{-1}{p})n$ is a square if and only if n is a square. When $p \equiv 3 \bmod 4$, $(\frac{-1}{p}) = -1$, and hence $n = -(\frac{-1}{p})n$ is a square. □

4 A family of RDSs with new parameters

Most known semi-regular RDSs have parameters (p^a, p^b, p^a, p^{a-b}) with p a prime. As far as we know, there are only three constructions ([3, 4, 8]) of semi-regular RDSs in groups of sizes not a prime power when the forbidden subgroup has size larger than 2. The RDSs constructed in [3, 8] have parameters

$$(p^{2t}(p+1), p+1, p^{2t}(p+1), p^{2n}),$$

where t is a positive integer, and $p = 2$ or p a Mersenne prime. The RDSs constructed in [4] have parameters

$$(4q, q, 4q, 4),$$

where q is an odd prime power greater than 9, $q \equiv 1 \pmod 4$. In this section, we give a construction of $(p(p+1), p, p(p+1), p+1)$ RDSs in the elementary Abelian group $G = \mathbb{F}_p \times \mathbb{F}_p \times \mathbb{F}_{p+1}$, where p is a Mersenne prime.

For an odd prime power $q = p^n$, $n \geq 1$, p prime, let $K := \mathbb{F}_q$ be the finite field with q elements, $K^* = K \setminus \{0\}$, and tr: $\mathbb{F}_q \mapsto \mathbb{F}_p$ be the absolute trace function. The quadratic character ℓ on K is defined by

$$\ell(x) = \begin{cases} -1, & \text{if } x \text{ is a non-square in } K, \\ 1, & \text{if } x \text{ is a non-zero square in } K, \\ 0, & \text{if } x = 0. \end{cases}$$

For each $u \in K^*$, define

$$S(u) := \sum_{x \in K} \xi_p^{tr(ux^2)},$$

and write $S := S(1)$. Then $S + S(u) = 2\sum_{x \in K} \xi_p^{tr(x)} = 0$ if u is a non-square in K and $S = S(u)$ if u is a square in K^*. It follows that $S(u) = \ell(u)S$ for each $u \in K^*$. Besides, it is easy to see that $S = \sum_{x \in K} \ell(x)\xi_p^{tr(x)}$ which is a Gauss sum, so it has modulus $\sqrt{q}$, see [2, p. 11].

In $K \times K$, each K-subspace is given by one of the following:

$$L_u := \{(x,\ ux) : x \in K\}, \qquad L_\infty = \{(0, x) : x \in K\}.$$

It is standard fact that

$$\sum_{u \in K} L_u + L_\infty = q + K \times K,$$

$$L_i L_j = K \times K, \forall i, j \in K \cup \{\infty\}, i \neq j.$$

By [13, Theorem 2.2.9], the set $R_0 := \{(x, x^2) : x \in K\}$ is a $(q, q, q, 1)$ RDS in $K \times K$ relative to $0 \times K$. For each non-principal character χ of $K \times K$, it is principal on exactly one of the above K-subspaces. Suppose χ is non-principal on $\{0\} \times K$, and is defined by $\chi(u', v') = \xi_p^{tr(uu' + vv')}$, $\forall (u', v') \in K$. Then $v \neq 0$, and

$$\chi(R_0) = \sum_{x \in K} \xi_p^{tr(ux + vx^2)} = \sum_{x \in K} \xi_p^{tr(v(x + \frac{u}{2v})^2 - \frac{u^2}{4v})} = \ell(v) S \xi_p^{-tr(\frac{u^2}{4v})}. \tag{4.1}$$

Theorem 9 *Suppose p is a Mersenne prime. Let $H = \mathbb{F}_p \times \mathbb{F}_p$, $N = \{0\} \times \mathbb{F}_p < H$, $E = \mathbb{F}_{p+1}$ be regarded as subgroups of $G = H \times E$ in the natural way. Take any bijection $\tau : \mathbb{F}_{p+1}^* \mapsto \mathbb{F}_p$, and define*

$$H_a := \{(z, \tau(a)z) : z \in \mathbb{F}_p\} \subset H$$

for each $a \in \mathbb{F}_{p+1}^*$. Also define

$$H_0 := \{(z, z^2) : z \in \mathbb{F}_p\}.$$

Then

$$R := \sum_{a\in E} H_a z_a a$$

is a $(p(p+1)), p, p(p+1), p+1)$ *RDS in* G *relative to* N, *where*

$$z_0 = 0, z_a = (x_a, \tau(a)x_a - \frac{1}{4}\tau(a)^2) \in H,$$

with $x_a \in \mathbb{F}_p$ *for each* $a \in \mathbb{F}_{p+1}^*$.

Proof By definition, we need to show

$$RR^{(-1)} = \sum_{b\in E}\Big(\sum_{a\in E} H_a H_{a+b}^{(-1)} z_a z_{a+b}^{-1}\Big)b = p(p+1) + (p+1)(G-N).$$

Because the elements of E are linearly independent over $\mathbb{Z}[H]$, by comparing the terms involving each $b \in E$, we need to check the following group ring equations.

(1) $\sum_{a\in E} H_a H_a^{(-1)} = p(p+1) + (p+1)(H-N)$.

This is true since $H_a = H_a^{(-1)}$, $H_a H_a = pH_a$ for $a \in E^*$, and $\sum_{a\in E^*} H_a = p + H - N$, $H_0 H_0^{(-1)} = p + H - N$ as we have exhibited above.

(2) $\sum_{a\in E} H_a H_{a+b}^{(-1)} z_a z_{a+b}^{-1} = (p+1)H$ for each $b \in E^*$.

Since $H_a H_{a'} = H$ for distinct elements $a, a' \in E^*$, we see that this is equivalent to the following equation

$$H_0 H_b z_b^{-1} + H_b H_0^{(-1)} z_b = 2H \tag{4.2}$$

for each $b \in E^*$. We check this by showing that both sides have the same character value under the action of each character of H.

Fix an element $b \in E^*$. Let χ be a character of H. The case χ is principal is trivial, so we assume that χ is non-principal, and suppose χ is defined by $\chi(u', v') = \xi_p^{uu'+vv'}, \forall (u', v') \in H$, with $(u, v) \neq 0$. The case $v = 0$ is easy. We have $\chi(H_0) = \sum_{x\in\mathbb{F}_q} \xi_p^{ux} = 0$ because $u \neq 0$, so both sides are equal to 0.

Now suppose $v \neq 0$. If χ is principal on H_a, $a \in E^*$, then

$$\chi(H_a) = \sum_{x\in\mathbb{F}_p} \xi_p^{(u+v\tau(a))x} = p,$$

so we must have $u + \tau(a)v = 0$. When $b \neq a$, we have $\chi(H_b) = 0$, so both sides of (4.2) are again both 0. When $b = a$, we have

$$\chi(H_0) = S\ell(v)\xi_p^{-\frac{u^2}{4v}} = S\ell(v)\xi_p^{-\frac{\tau(a)^2 v}{4}}$$

from (4.1). We compute

$$\begin{aligned}\chi(H_0 H_a z_a^{-1}) &= \chi(H_0)\chi(H_a)\chi(z_a^{-1}) \\ &= pS\ell(v)\xi_p^{-\frac{\tau(a)^2 v}{4} - (ux_a + v\tau(a)x_a - v\frac{\tau(a)^2}{4})} = pl(v)S,\end{aligned}$$

and similarly, $\chi(H_a H_0^{(-1)} z_a) = pl(-v)S$. Since $p \equiv -1 \bmod 4$, we have $\ell(-1) = -1$. Therefore, $\chi(H_0 H_a z_a^{-1} + H_a H_0^{(-1)} z_a) = 0 = \chi(2H)$. This proves (4.2) and hence the whole theorem. □

Remark When $p = 7$, we have $7 \equiv -1 \bmod 2$, and the above construction are in accordance with our conclusion in Theorem 7.

This construction allows the following slight variation. Let p, H, N be as in Theorem 9 and E be a multiplicative group of order $p+1$, and the semidirect product $G := H \rtimes E$ is defined by

$$(u, v)^e = e^{-1}(u, v)e = (a(e)u, v),\ \forall (u, v) \in H, e \in E$$

for some homomorphism $a : E \mapsto \mathbb{F}_p^*$. Suppose we can find a bijection $\tau : E \setminus \{1_E\} \mapsto \mathbb{F}_p$, such that

$$\tau(e)a(e') \neq \tau(e'e)\ \forall e, e' \in E \setminus \{1_E\}, e'e \neq 1_E; \tag{C1}$$

$$\tau(e^{-1}) = \tau(e)a(e^{-1}), \forall e \neq 1_E. \tag{C2}$$

Now define

$$H_e := \{(z, \tau(e)z) : z \in \mathbb{F}_p\},\ \forall e \neq 1_E, \quad H_1 := \{(z, z^2) : z \in \mathbb{F}_p\}.$$

Then the set

$$R := \sum_{e \in E} H_e z_e e$$

is a $(p(p+1)), p, p(p+1), p+1)$ RDS in G relative to N, where

$$z_1 = 0, z_e = (x_e, \tau(e)x_e - \frac{1}{4}\tau(e^{-1})^2) \in H,$$

with $x_e \in \mathbb{F}_p$ for each $e \neq 1_E$. The proof is essentially the same as that of the above theorem. The equations to check are the following:

(1) $\sum_{a \in E} H_a H_a^{(-1)} = p(p+1) + (p+1)(H - N)$.

(2) $\sum_{e \in E} H_e H_{e'e}^{(-e')} z_e z_{e'e}^{-e'} = (p+1)H,\ \forall e' \neq 1_E$.

The analogy of (4.2) is

$$H_1 H_e^{(-e)} z_e^{-e} + H_{e^{-1}} H_1^{(-e)} z_{e^{-1}} = 2H. \tag{4.3}$$

We observe that condition (C1) is to make sure that $H_{e'e}^{(e')} \neq H_e$ when $e, e', e'e \neq 1_E$, and condition (C2) is to make sure that $H_e^{(e)} = H_{e^{-1}}$ when $e \neq 1_E$, and the choice of z_e is to make (4.3) hold.

Theorem 10 *Let p, H, N be as in Theorem 9. Let E be a finite group of order $p+1$ such that $E_2 := \{e \in E : e^2 = 1\}$ is a normal subgroup of index 2 in E and*

$exp(E) = 4$. Take the homomorphism $a : E \mapsto \{\pm 1\} \subset \mathbb{F}_p^*$ with $ker(a) = E_2$. The semidirect product $G := H \rtimes E$, defined by

$$(u, v)^e = e^{-1}(u, v)e = (a(e)u, v),\ \forall (u, v) \in H, e \in E,$$

contains a $(p(p + 1)), p, p(p + 1), p + 1)$ RDS relative to N.

This follows from the lemma below.

Lemma 11 *There are exactly two types of groups E such that there is a bijection $\tau : E \setminus \{1_E\} \mapsto \mathbb{F}_p$ and a homomorphism $a : E \mapsto \mathbb{F}_p^*$ satisfying the conditions (C1), (C2):*

(1) *E is elementary Abelian.*
(2) *$E_2 := \{e \in E : e^2 = 1\}$ is a normal subgroup of index 2 in E, and $exp(E) = 4$. Obviously, E_2 is elementary Abelian in this case.*

Proof Let E be a group of order $p+1$. Suppose there is a bijection $\tau : E \setminus \{1_E\} \mapsto \mathbb{F}_p$ and a homomorphism $a : E \mapsto \mathbb{F}_p^*$ satisfying the two conditions (C1), (C2). Because $(p+1, p-1) = 2$, from $a(e)^{p+1} = a(e^{p+1}) = 1$ and $a(e)^{p-1} = 1$, we have $a(e)^2 = 1$ for each $e \in E$, so $Im(a) \leq \{\pm 1\}$, and correspondingly $ker(a)$ has size $\frac{p+1}{2}$ or $p + 1$.

(1) First, we assume $|ker(a)| = p + 1$. Then $ker(a) = E$, and we must have $\tau(e^{-1}) = \tau(e), \forall e \in E, e \neq 1_E$ by (C2). It follows that $e^{-1} = e$ for any $e \in E$, which means $E = E_2 := \{e \in E : e^2 = 1\}$ and hence is elementary Abelian. In this case, just take a to be the trivial homomorphism and τ any bijection from $E \setminus \{1_E\}$ to $\mathbb{F}_p$.

(2) Second, we assume $|ker(a)| = \frac{p+1}{2}$. Then $ker(a)$ is a subgroup of index 2 in E. We first show that $ker(a) = E_2$. If $e \in ker(a), e \neq 1_E$, then $\tau(e) = \tau(e^{-1})$ by (C2) and we must have $e = e^{-1}$, i.e., $e \in E_2$. Hence $ker(a)$ is a subgroup of E_2 which is either $ker(a)$ or E. If $e \in E_2$, $e \neq 1_E$, then $\tau(e) = \tau(e)a(e)$ by (C2), so either $\tau(e) = 0$ or $a(e) = 1$, i.e., $e \in ker(a)$. Therefore at most one element of E_2 is not contained in $ker(a)$ since τ is a bijection. It follows that $ker(a) = E_2$ since $\frac{p+1}{2} > 1$, and hence E_2 is a subgroup of index 2 which has got to be normal in E.

For any $e \in E$, we have $a(e^2) = a(e)^2 = 1$, so $e^2 \in ker(a)$,and hence $exp(E)|4$. Because $E \neq E_2$, we must have $exp(E) = 4$, and if $e \in E \setminus E_2$, then $o(e) = 4$.

In this case, let $a : E \mapsto \{\pm 1\} \subset \mathbb{F}_p^*$ be defined by: $a(e) = 1$ if $e \in E_2$ and $a(e) = -1$ otherwise. This is a well defined homomorphism, and maps all elements of order 4 to -1 and all elements of order 2 to 1. It is easily checked that the condition (C2) becomes

$$\tau(e^3) = -\tau(e),\ \forall e \text{ with } o(e) = 4, \tag{4.4}$$

and condition (C1) becomes

$$\tau(e'e) \neq -\tau(e), \tag{4.5}$$

for any pair of (e', e) with $o(e') = 4$, $e \neq 1_E$, $e'e \neq 1_E$.

Suppose (4.4) holds, and we show that (4.5) always holds. When e has order 4, from (4.4), we have that (4.5) is equivalent to

$$\tau(e'e) \neq \tau(e^{-1}),\ \forall e' \text{ with } o(e') = 4,\ e'e \neq 1_E, \tag{4.6}$$

that is, $e'e \neq e^{-1}$ which is always true since otherwise $e' = e^{-2}$ has order 2, contradicting $o(e') = 4$. When e has order 2, we have $e'e$ is not in E_2 and hence has order 4 when $o(e') = 4$, and from (4.4), we have that (4.5) is equivalent to

$$\tau((e'e)^{-1}) \neq \tau(e),\ \forall e' \text{ with } o(e') = 4, \tag{4.7}$$

that is, $e'e \neq e^{-1}$ which is always true since otherwise $e' = e^{-2} = 1$, again contradicting $o(e') = 4$. Therefore, (4.5) always holds provided (4.4) holds.

Therefore, the two conditions (C1), (C2) reduce to (4.4). It is clear that such bijection exists. This completes the proof of the lemma. □

Example 1 Take $E = \langle \alpha : \alpha^4 = 1 \rangle$. Then $G = \langle x, \alpha : x^3 = \alpha^4 = 1, x^\alpha = x^{-1} \rangle \times \langle y : y^3 = 1 \rangle$, $N = \langle y \rangle < G$. Take $\tau : E \setminus \{1\} \mapsto \mathbb{F}_3$ by $\tau(\alpha) = 1$, $\tau(\alpha^2) = 0$, $\tau(\alpha^3) = 2$. Then we see that the two conditions are satisfied, and we thus get a $(12, 3, 12, 4)$ RDS in G relative to N. This is the only case that our parameter family overlaps with the three parameter families mentioned at the beginning of this section.

Example 2 Let $p + 1 = 2^{2m+1}$ with $m \geq 1$. It is easy to see that $E = \mathbb{Z}_4 \times \mathbb{Z}_2^{2m-1}$ is of type (2) in Lemma 11. Now we exhibit some non-Abelian groups E of type (2). We fix an integer i between 1 and m. Let $H = \mathbb{Z}_2^{2m}$,

$$A_i = diag\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \cdots, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right) \in GL(2m, \mathbb{Z}_2),$$

with the first i blocks being $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, and the remaining blocks being $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. We regard H as a vector space over $\mathbb{Z}_2$ with $GL(2m, \mathbb{Z}_2)$ acting on the right. Now for a given $v_0 \in H$ which is not in the image of $A_i + I_{2m}$, define the following group

$$G_i := \langle \alpha,\ H : \alpha^2 = v_0 \in H, v^\alpha = \alpha^{-1} v \alpha = v A_i,\ \forall v \in H \rangle,$$

where we regard H as a multiplicative subgroup of G_i. It is easy to see that G_i is of type (2) with $G_{i,2} := \{g \in G_i : g^2 = 1\} = H$. We compute the size of the center $Z(G_i)$ which turns out to be different for different i, so each G_i, $1 \leq i \leq m$, are not isomorphic.

First we show $Z(G_i) \leq H$. If $h_0\alpha \in Z(G_i)$ for some $h_0 \in H$, then $\alpha^{-1} h h_0 \alpha = h_0 \alpha \alpha^{-1} h$, i.e., $(hh_0)^\alpha = hh_0$ for all $h \in H$. In the vector form, $(h + h_0)A_i = h + h_0$ for all $h \in H$, leading to the contradiction $A_i = I_{2m}$. Because $G_i = H \cup H\alpha$, we see that $Z(G_i) \leq H$.

Next we show that $|Z(G_i)| = 2^{2m-i}$. For any $h \in H$ to be in $Z(G_i)$, it is necessary and sufficient to have $h^\alpha = \alpha^{-1} h \alpha = h \alpha^{-1} \alpha = h$, that is, $h(A_i + I_{2m}) = 0$. We thus have $Z(G_i) = ker(A_i + I_{2m})$. It follows that $dim_{\mathbb{Z}_2} Z(G_i) = 2m - rank(A_i + I_{2m}) = 2m - i$.

Acknowledgement The author would like to thank Professor Weisheng Qiu and Professor Qing Xiang for their supervision and encouragement. He also thanks the referees for helpful suggestions and comments.

References

1. Baumert, L.D.: Cyclic Difference Sets. Lecture Notes in Mathematics. Springer, New York (1971)
2. Berndt, B.C., Evans, R.J., Williams, K.S.: Gauss and Jacobi Sums. Wiley, New York (1998)
3. Davis, J.A., Jedwab, J., Mowbray, M.: New Families of semi-regular relative difference sets. Des. Codes Cryptogr. **13**, 131–146 (1998)
4. Feng, T., Xiang, Q.: Semi-regular relative difference sets with large forbidden subgroups. Submitted
5. Hiramine, Y.: Planar functions and related group algebras. J. Algebra **15**, 135–145 (1992)
6. Hou, X.D.: p-ary and q-ary versions of certain results about bent functions and resilient functions. Finite Fields Appl. **10**, 566–582 (2004)
7. Leung, K.H., Ma, S.L., Tan, V.: Planar functions from $\mathbb{Z}_n$ to $\mathbb{Z}_n$. J. Algebra **224**, 427–436 (2000)
8. Leung, K.H., Ling, S., Ma, S.L.: Constructions of semi-regular relative difference sets. Finite Fields Appl. **7**, 397–414 (2001)
9. Ma, S.L.: Planar functions, relative difference sets and character theory. J. Algebra **185**, 342–356 (1996)
10. Ma, S.L., Schmidt, B.: Relative (p^a, p^b, p^a, p^{a-b})-difference sets: a unified exponent bound and a local ring construction. Finite Fields Appl. **1**, 1–22 (2000)
11. McDonald, B.R.: Finite Rings with Identity. Marcel Dekker, New York (1974)
12. Passman, D.S.: The Algebraic Structure of Group Rings. Wiley, New York (1977)
13. Pott, A.: Finite Geometry and Character Theory. Lecture Notes in Mathematics, vol. 1601. Springer, Berlin (1995)
14. Schmidt, B.: On (p^a, p^b, p^a, p^{a-b})-relative difference dets. J. Algebr. Comb. **6**, 279–297 (1997)