数理解析研究所講究録
1109巻 1999年 80-89

On Nonabelian Semiregular Relative Difference Sets

Dominic ELVIRA （ドミニク エルヴィラ） and
Yutaka HIRAMINE （平峰 豊）

Department of Mathematics, Faculty of Education
Kumamoto University
Kurokami, Kumamoto, Japan

1. Introduction

A (m, u, k, λ) *relative difference set* (RDS) in a group G of order mu relative to a normal subgroup U of order u is a k-element subset R of G such that the number of elements in the set $\{(r_1, r_2) \mid r_1, r_2 \in R,\ r_1 r_2^{-1} = g\}$ for every $g \in G$, $g \neq 1$ is λ if $g \in G \setminus U$ or 0 if $g \in U$. If $k = u\lambda$, we call R a *semiregular* RDS and its parameters are given by $(u\lambda, u, u\lambda, \lambda)$. Semiregular RDS's in abelian groups have been studied intensively in [1], [7], [8], [10], [11]. Recently, J.A. Davis, J. Jedwab and M. Mowbray made two constructions of abelian semiregular RDS's in [3]. In one of their constructions, they considered (a, m, t)-building sets(BS) on abelian groups and by applying group characters, they were able to construct new sets of semiregular RDS's in groups of non-prime power order.

In this article, we study semiregular RDS's in some *nonabelian* groups, especially groups G containing an abelian subgroup A of index 2 inverted by an element of $G - A$, say t. If G has a semiregular RDS R relative to a normal subgroup U contained in A, then we can represent R in the form $R = S \cup Tt$ for some subsets S and T of A. We may also show that $\{S, T\}$ is an $(a, m, 2)$BS when $4 \nmid o(t)$ for some suitable $a \in \mathbf{N}$ and $m \in \mathbf{R}$.

In Section 3, we focus on (a, m, t)BS in a cyclic p-group where p is a prime and show that

Theorem 3.9 *Let $\{S_1, \ldots, S_t\}$ be an (a, m, t)BS in a cyclic p-group G relative to U. Then $|U| \geq p^t$.*

As an application of this theorem, we show that for $t = 2$ we have

Theorem 5.1 *There is no semiregular RDS in* D_{2p^n}.

As corollaries, we show that for a generalized quaternion or semidihedral group G, the order of the forbidden subgroup U is at most 2 as stated in Corollaries 5.2 and 5.3 of Section 5. In addition, we show in Theorem 5.4 that every generalized quaternion group G of order 2^{n+1} always contains a $(2^n, 2, 2^n, 2^{n-1})$ RDS relative to $U = Z(G)$, $(U \cong Z_2)$.

2. Preliminaries

In this section, we define a semiregular RDS in a group and provide some basic concepts essential to prove the main results.

Definition 2.1 *A* (m, u, k, λ) *RDS in a group* G *of order* mu *relative to a normal subgroup* U *of order* u *is a* k*-element subset* R *of* G *such that the number of elements in the set* $\{(r_1, r_2) \mid r_1, r_2 \in R,\ r_1 r_2^{-1} = g\}$ *for every* $g \in G$, $g \neq 1$ *is* λ *if* $g \in G \setminus U$ *or* 0 *if* $g \in U$.

We note that when $k = u\lambda$, we call R a *semiregular RDS*. In this case, R has parameters of the form $(u\lambda, u, u\lambda, \lambda)$. If $U = 1$, R is called a *trivial semiregular RDS*.

The next result about abelian RDS's is well-known. A proof can be found in Pott's book [1], for example.

Result 2.2 *Let* G *be an abelian group and* $f \in \mathbf{C}[G]$. *If* $\chi(f) = 0$ *for every non-principal character* χ *of* G, *then* $f = k\widehat{G}$ *for some* $k \in \mathbf{C}$.

Result 2.3 R *is a* (m, u, k, λ) *RDS in a group* G *relative to a normal subgroup* U *if and only if* $|Ux \cap R| = 1$ *for every* $x \in G$.

Proof. Assume $a_1 x,\ a_2 x \in R$, $(a_1, a_2 \in U,\ a_1 \neq a_2)$ and set $r_1 = a_1 x$, $r_2 = a_2 x$. Then $r_1 r_2^{-1} = a_1 a_2^{-1} \in U$, a contradiction. Hence $|Ux \cap R| \leq 1$. By semiregularity, R has parameters $(u\lambda, u, u\lambda, \lambda)$. As $|G : U| = |R| = u\lambda$, we have $|Ux \cap R| = 1$ for every $x \in G$.

Conversely, if $|Ux \cap R| = 1$ then $|G : U| = m = k$. But R satisfies $RR^{-1} = k \cdot 1 + \lambda(G - U)$ and so $k = \lambda u$, $k > 1$. Thus R is semiregular.

The following result due to Elliot and Butson[4] is basic in the study of relative difference sets.

Result 2.4 *Let* R *be a* (m, u, k, λ) *RDS in a group* G *relative to a normal subgroup* U *and let* U_1 *be a normal subgroup of* G *contained in* U. *Set* $\overline{G} = G/U_1$. *Then* $\overline{R}$ *is a* $(m, u/u_1, k, u_1\lambda)$ *RDS in* $\overline{G}$ *relative to* $\overline{U}$.

The next result is called the product construction for RDS's in an abelian group. For a proof, see [2] and [11].

Result 2.5 ([2] , [11]) *Let G be a group of order $u^3k_1k_2$. Let G_1 be a normal subgroup of G and G_2 a subgroup of G such that $G \rhd U = G_1 \cap G_2$ with $|U| = u$, $|G_1| = u^2k_1$, and $|G_2| = u^2k_2$. If R_1 is a (uk_1, u, uk_1, k_1) RDS in G_1 relative to U and R_2 is a (uk_2, u, uk_2, k_2) RDS in G_2 relative to U then $R = R_1R_2$ is a $(u^2k_1k_2, u, u^2k_1k_2, uk_1k_2)$ RDS in G relative to U.*

For ease of computations, we distinguish a group ring element from a set. If $X = \{x_1, x_2, \ldots, x_n\}$ is a given set, then by $\widehat{X}$ we mean $\widehat{X} = \sum_{i=1}^{n} x_i$, $x_i \in X$. Also, $\widehat{X^{-1}} = \sum_{i=1}^{n} x_i^{-1}$ for $x_i \in X$.

3. An (a, m, t)-Building Set in $\mathbf{Z}_{p^n}$

In this section, we define building blocks and building sets of an abelian group as given by Davis and Jedwab [2]. We then consider building sets in a cyclic p-group.

Definition 3.1 *A building block in an abelian group G with modulus m is a subset S of G such that $\chi(S) \in \{0, m\}$ for every non-principal character χ of G.*

Definition 3.2 *An $(a, m, t)BS$ $(t > 1)$ on an abelian group G relative to a subgroup U is a collection $\{S_1, \ldots, S_t\}$ of building blocks in G with modulus m, $|S_i| = a$ for each $i \in \{1, \ldots, t\}$ and*

(i.) *There exists a unique $i \in \{1, \ldots, t\}$ such that $\chi(S_i) \neq 0$ if χ is non-principal on U,* and

(ii.) $\chi(S_i) = 0$ *for every $i \in \{1, \ldots, t\}$ if χ is principal on U.*

We next define the m-th cyclotomic polynomial. For a more detailed discussion about this topic, consult the book by Ireland and Rosen [5].

Definition 3.3 *Let m be a positive integer and $\zeta_m = e^{2\pi i/m}$, a m-th root of unity. We call $F_m(x) = \prod_{(a,m)=1} (x - \zeta_m^a)$ where $1 \leq a < m$, the mth cyclotomic polynomial.*

Throughout the rest of this section, we use the following hypothesis.

Hypothesis 3.4 *Let $G = \langle g \rangle \cong Z_{p^n}$ and U be a subgroup of G of order p^r. Assume the existence of $\{S_1, \ldots, S_t\}$, an $(a, m, t)BS$ in G relative to U.*

Notation 3.5 For ease of computations, we define the following:

$$\widehat{S_i} := \sum_{0 \leq k < p^n} a_{ik} g^k \quad \text{and} \quad f_i(x) := \sum_{0 \leq k < p^n} a_{ik} x^k, \quad a_{ik} \in \{0, 1\}.$$

Remark 3.6 *Let $\chi \in G^*$ and set $\zeta = \chi(g)$. Then $\chi(\widehat{S_i}) = f_i(\zeta)$.*

Lemma 3.7 $\chi(\widehat{S_i}) = 0$ *if and only if* $F_{p^d}(x) \mid f_i(x)$.

Proof. By Remark 3.6, we have the lemma.

Theorem 3.8 *Under Hypothesis 3.4, the following hold:*

(i.) *for every* $d > n - r$, *there exists a unique* $j \in \{1, 2, \ldots, t\}$ *such that* $F_{p^d}(x) \nmid f_j(x)$, *and*

(ii.) $F_p(x)F_{p^2}(x)\cdots F_{p^{n-r}}(x) \mid f_i(x)$ *for every* $i \in \{1, 2, \ldots, t\}$.

Proof. Let ζ be a primitive p^d-th root of unity, $1 \leq d \leq n$. Then $\zeta^{p^{n-r}} = 1$ if and only if $p^{n-r} \geq p^d$ if and only if $n - r \geq d$. Let $\chi \in G^*$ such that $\chi(g) = \zeta$. Then $\chi_{|U} = \chi_0$ if and only if $n - r \geq d$ and therefore $\chi_{|U} \neq \chi_0$ if and only if $n - r < d$. We consider the following cases:

(i.) Assume $d > n - r$ so that $\chi_{|U} \neq \chi_0$. By the definition of a BS, there exists a unique j such that $|\chi(S_j)| = m \neq 0$. Now $|f_j(\zeta)| = m$ and so by Lemma 3.7, $F_{p^d}(x) \nmid f_j(x)$.

(ii.) Assume $n - r \geq d$ so that $\chi_{|U} = \chi_0$. By the definition of a BS, $\chi(S_i) = 0$ for every $i \in \{1, 2, \ldots, t\}$. Now $f_i(\zeta) = 0$ if and only if $F_{p^d}(x) \mid f_i(x)$ for every $d = 1, 2, \ldots, n-r$. Since $F_p(x), F_{p^2}(x), \cdots, F_{p^{n-r}}(x)$ are relatively prime, we have $F_p(x)F_{p^2}(x)\cdots F_{p^{n-r}}(x) \mid f_i(x)$ for every $i \in \{1, 2, \ldots, t\}$.

The next theorem is of great importance to prove the results in the proceeding sections. It establishes that the order of the forbidden subgroup U of an RDS in a cyclic p-group must be greater than or equal to p^t, where t is the number of building blocks in the corresponding building set contained in the given cyclic p-group relative to U.

Theorem 3.9 *Let* $\{S_1, \ldots, S_t\}$ *be an* (a, m, t)*BS in a cyclic* p*-group* G *relative to* U. *Then* $|U| \geq p^t$.

Proof. Set $F(x) = F_p(x)F_{p^2}(x)\cdots F_{p^{n-r}}(x)$ and $I = \{n - r + 1, \ldots, n\}$. Then there exist $s_{id} \in \{0, 1\}$ for $1 \leq i \leq t$, $d \in I$ and $q_i(x)$ such that

$$f_i(x) = F(x)\Big(\prod_{d\in I} F_{p^d}(x)^{s_{i,d}}\Big)q_i(x).$$

For a fixed $d \in I$, we have $s_{1d} + s_{2d} + \ldots + s_{td} = t - 1$ by Theorem 3.8(i). Assume $s_{i,n-r+1} = s_{i,n-r+2} = \cdots = s_{i,n} = 1$ for some i. Then $F_p(x)F_{p^2}(x)\cdots F_{p^n}(x) \mid f_i(x)$ and so $\chi(\widehat{S_i}) = 0$ for every $\chi \in G^*$, $\chi \neq \chi_0$. By Result 2.2 $S_i = G$, a contradiction. Thus $\sum_{d\in I} s_{id} \leq r - 1$.

We next compute $\sum_{1\leq i\leq t, d\in I} s_{id}$ in two ways. First, we have

$$\sum_{1\leq i\leq t, d\in I} s_{id} = \sum_{1\leq i\leq t} \Big(\sum_{d\in I} s_{id}\Big) \leq t(r-1) = tr - t.$$

On the other hand,

$$\sum_{1\leq i\leq t, d\in I} s_{id} = \sum_{d\in I}(\sum_{1\leq i\leq t} s_{id}) = \sum_{d\in I}(t-1) = r(t-1) = tr - r.$$

Thus $t \leq r$ and so $|U| = p^r \geq p^t$.

4. RDS in Dihedral Groups

Lemma 4.1 *Let G be a group containing an abelian subgroup A of index 2 inverted by an element $t \in G$. Assume that a Sylow 2-subgroup of A is cyclic. If $U(\neq G)$ is a normal subgroup of G, then either $U \leq A$ or $|G:U| = 2$.*

Proof. We suppose $U \not\leq A$ and show that $|G:U| = 2$.

(Step 1) We may assume that $t \in U$:

Let $w \in U - A$. Then $w = at$ for some $a \in A$ and so $w^{-1}xw = t^{-1}a^{-1}xat = t^{-1}xt$ for any $x \in A$. Hence w inverts A and $G = \langle w\rangle A$.

(Step 2) We may assume that $o(t) = 2$ or 4:

Set $P = O_2(A)$, $Q = O(A)$ and $s = t^d$, where $o(t) = 2^c \cdot d$ $(2 \not| d)$. Then $G = \langle s\rangle A$ and s inverts A. As s is an element of order 2^c and inverts $A(\ni s^2)$, we have $s^2 = s^{-1}s^2s = (s^2)^{-1}$. Hence $s^4 = 1$.

(Step 3) $Z(G) = C_A(t)$ or $G \cong Z_4$:

Assume $Z(G) \not\leq A$. Then $G = Z(G)A$ and so A is abelian. Hence, for any $x \in A$, $x = t^{-1}xt = x^{-1}$ and so $x^2 = 1$. Thus $A \cong Z_2$ by assumption. Hence $G \cong Z_4$. Assume $Z(G) \leq A$. Then $Z(G) \leq A \cap C_G(t) = C_A(t)$. Clearly $C_A(t) \leq C_G(\langle A, t\rangle) = Z(G)$. Thus $Z(G) = C_A(t)$.

By steps 1-3, we may assume that $t \in U$ and $o(t) = 2$ or 4.

First assume that $2 \not| |A|$. Then $C_G(t) = \langle t\rangle C_A(t) = \langle t\rangle$. Hence $|G : C_G(t)| = |G|/2$ and so $|U| \geq 1 + |\{t^x \mid x \in G\}| = 1 + |G|/2$. Thus $U = G$, a contradiction.

Assume that $2 \mid |A|$. Then $|C_G(t)| = |\langle t\rangle \cdot C_A(t)| = 4$. Hence $|\{t^x \mid x \in G\}| = |G : C_G(t)| = \frac{1}{4}|G|$ and so $|U| \geq \frac{1}{4}|G| + 1$. In particular, $|G:U| \leq 3$. Let x be any element of G of odd order. Then, as $t^{-1}xt = x^{-1}$ and $t^{-2}xt^2 = x$, we have $x^{-1}tx = x^{-1}t^2(t^{-1}xt)t^{-1} = x^{-1}t^2x^{-1}t^{-1} = x^{-2}t$. Thus $t, x^{-2}t \in U$. From this we have, $x^2 \in U$ and so $x \in U$. Therefore we have $U \geq O(G)$. Thus $|G:U| = 2$.

Remark 4.2 *Under the hypothesis of Lemma 4.1, we may assume that $o(t) = 2$ or 4.*

Throughout the rest of this section, we assume following:

Hypothesis 4.3 *Let G be a group having a normal subgroup A of index 2 inverted by an element $t \in G - A$ of order 2 or 4. Assume that G has a $(\lambda u, u, \lambda u, \lambda)$ RDS R relative to U and that $G \ncong Z_4$.*

Lemma 4.4 $U \leq A$

Proof. Suppose false. Then $|G : U| = 2$ by Lemma 4.1. Hence $u\lambda = 2$ and so $G \cong Z_4$, contrary to Hypothesis 4.3.

Lemma 4.5 *Set $S = R \cap A$ and $T = Rt^{-1} \cap A$. Then*
(i) $S, T \subset A$ and $R = S \cup Tt$
(ii) $|S| = |T| = \frac{1}{2}\lambda u$
(iii) $\widehat{S}\widehat{T}(1+t^2) = \lambda\widehat{A}$
(iv) $\widehat{S}\widehat{S^{(-1)}} + \widehat{T}\widehat{T^{(-1)}} = u\lambda + \lambda(\widehat{A} - \widehat{U})$.

Proof. By Result 2.3, each coset Ux $(x \in G)$ contains exactly one element of R. Hence we have $|S| = |A/U| = \frac{1}{2}\lambda u$ and $|Tt| = |At|/|U| = \frac{1}{2}\lambda u$. Moreover, $S \cup Tt \subset R$. Thus (i) and (ii) hold.

By (i), $\widehat{R}\widehat{R^{(-1)}} = (\widehat{S} + \widehat{T}t)(\widehat{S^{(-1)}} + t^{-1}\widehat{T^{(-1)}})$
$= \widehat{S}\widehat{S^{(-1)}} + \widehat{T}t\widehat{S^{(-1)}} + \widehat{S}t^{-1}\widehat{T^{(-1)}} + \widehat{T}\widehat{T^{(-1)}}$.

On the other hand, $\widehat{T}t\widehat{S^{(-1)}} = \widehat{T}t^2(t^{-1}\widehat{S^{(-1)}}t)t^{-1} = \widehat{T}t^2\widehat{S}t^{-1} = \widehat{S}\widehat{T}t$ as A is abelian and $t^2 \in A$. Similarly, $\widehat{S}t^{-1}\widehat{T^{(-1)}} = \widehat{S}\widehat{T}t^{-1} = (\widehat{S}\widehat{T}t^2)t$. Hence we have $\widehat{R}\widehat{R^{(-1)}} = \widehat{S}\widehat{S^{(-1)}} + \widehat{T}\widehat{T^{(-1)}} + (1+t^2)\widehat{S}\widehat{T}t$. Since

$$\widehat{R}\widehat{R^{(-1)}} = \lambda u + \lambda(\widehat{G} - \widehat{U}) = \lambda u + \lambda(\widehat{A} - \widehat{U}) + \lambda\widehat{A}t,$$

we have $\widehat{S}\widehat{S^{(-1)}} + \widehat{T}\widehat{T^{(-1)}} = \lambda u + \lambda(\widehat{A} - \widehat{U})$ and $(1+t^2)\widehat{S}\widehat{T} = \lambda\widehat{A}$. Therefore (iii) and (iv) hold.

For the rest of this section, we consider the case $o(t) = 2$.

Corollary 4.6 *If $o(t) = 2$, then $2 \mid \lambda$.*

Proof. Since $t^2 = 1$, we have by Lemma 4.5, $\widehat{S}\widehat{T} = \frac{1}{2}\lambda\widehat{A}$. Thus $2 \mid \lambda$.

Theorem 4.7 *Assume that $o(t) = 2$ and let S and T be as defined in Lemma 4.5. Then $\{S, T\}$ is a $(\frac{1}{2}u\lambda, \sqrt{u\lambda}, 2)BS$ in A relative to U.*

Proof. As we have seen in the proof of Corollay 4.6, $\widehat{S}\widehat{T} = \frac{1}{2}\lambda\widehat{A}$. Let χ be a non-principal character of A. Then

$$\chi(\widehat{S})\chi(\widehat{T}) = 0 \tag{4.7.1}$$

Assume that $\chi_{|U}$ is non-principal. By Lemma 4.5 (iv),

$$|\chi(\widehat{S})|^2 + |\chi(\widehat{T})|^2 = c \cdot u\lambda$$

where $c = 0$ or 1 depending on whether $\chi_{|U}$ is principal or non-principal.

This fact together with (4.7.1) gives the proof of the theorem.

Theorem 4.8 *Let S_1 and T_1 be a $(a, m, 2)$BS with $m^2 = 2a$ in an abelian group A_1 relative to a subgroup U_1. Let $G_1 = \langle t_1 \rangle A_1$ be a semidirect product of A_1 with $\langle t_1 \rangle$, where t_1 is the automorphism of A_1 that inverts A_1. Then $R_1 = S_1 \cup T_1 t_1$ is a semiregular RDS in G_1 relative to U_1.*

Proof. Set $u_1 = |U_1|$. By assumption, $\chi(\widehat{S_1})\chi(\widehat{T_1}) = 0$ and

$$\chi(\widehat{S_1}\widehat{S_1^{(-1)}}) + \chi(\widehat{T_1}\widehat{T_1^{(-1)}}) - m^2 + \frac{m^2}{u_1}\chi(U_1) = 0.$$

By Result 2.1,

$$\widehat{S_1}\widehat{T_1} = \alpha\widehat{A_1} \tag{4.8.1}$$

and

$$\widehat{S_1}\widehat{S_1^{(-1)}} + \widehat{T_1}\widehat{T_1^{(-1)}} - m^2 + \frac{m^2}{u_1}\widehat{U_1} = \beta\widehat{A_1} \tag{4.8.2}$$

for some $\alpha, \beta \in \mathbf{C}$. By (4.8.1), α is a positive integer and

$$a^2 = \alpha|A_1|. \tag{4.8.3}$$

By (4.8.2), we have

$$2a - m^2 + \frac{m^2}{u_1} = \beta \qquad \text{and} \qquad 2a^2 = \beta|A_1|. \tag{4.8.4}$$

Hence $\beta = 2\alpha$ and $\frac{m^2}{u_1} = \beta$ as $m^2 = 2a$. In particular $u_1\alpha = a$. By a similar argument as in the proof of Lemma 4.5 (iii) (iv), we have

$$\begin{aligned}
\widehat{R_1}\widehat{R_1^{(-1)}} &= (\widehat{S_1} + \widehat{T_1}t_1)(\widehat{S_1^{(-1)}} + t_1^{-1}\widehat{T_1^{(-1)}}) \\
&= \widehat{S_1}\widehat{S_1^{(-1)}} + \widehat{T_1}\widehat{T_1^{(-1)}} + 2\widehat{S_1}\widehat{T_1}t \\
&= 2a + 2\alpha\widehat{A_1} - 2\alpha\widehat{U_1} + 2\alpha\widehat{A_1}t \\
&= 2a + 2\alpha(\widehat{G_1} - \widehat{U_1}).
\end{aligned}$$

Therefore R_1 is a $(\frac{2|A_1|}{u_1}, u_1, 2a, 2\alpha)$ RDS relative to U_1. Since $2\alpha \cdot u_1 = 2a$, we have shown that R is a semiregular RDS relative to U_1.

5. Applications

In this section, we consider the group $G = \langle t \rangle A \cong D_{2p^n}$. Note that G is a dihedral group satisfying $t^2 = 1$ and $A = \langle x \rangle$, a cyclic group generated by $x \in G$ of order p^n where p is any prime.

Theorem 5.1 *There is no semiregular RDS in D_{2p^n}.*

Proof. Let R be a semiregular RDS in $G = \langle t \rangle A$ relative to U. Then t inverts A where $A \cong Z_{p^n}$ and $U \cong Z_{p^r}$, $r \geq 1$. Let U_0 be a maximal subgroup of U, i.e., $|U_0| = p^{r-1}$. Consider $\overline{G} = G/U_0$. Then $\overline{R}$ is a semiregular RDS in $\overline{G} = \langle \overline{t} \rangle \overline{A} \cong D_{2p^{n-r+1}}$ relative to $\overline{U} \cong Z_p$ by Result 2.4. By Theorem 4.7, there exist subsets $\overline{S}$ and $\overline{T}$ of $\overline{A}$ such that $\{\overline{S}, \overline{T}\}$ is a $(a, m, 2)$ BS. Applying Theorem 3.9, we have $|\overline{U}| \geq p^2$, a contradiction.

Now we consider the generalized quaternion group

$$Q_{2^{n+1}} = \langle x, y \mid x^{2^{n-1}} = y^2,\ y^4 = 1,\ y^{-1}xy = x^{-1} \rangle \quad (n \geq 2)$$

of order 2^{n+1} and the semidihedral group

$$S(2^{n+1}) = \langle x, y \mid x^{2^n} = y^2 = 1,\ z = x^{2^{n-1}},\ yxy = x^{-1}z \rangle \quad (n \geq 2)$$

of order 2^{n+1}. We then apply Theorem 5.1 to show existence or non-existence of semiregular RDS's in these groups.

Corollary 5.2 *Let R be a semiregular RDS in $Q_{2^{n+1}}$ relative to a normal subgroup U. Then $|U| \leq 2$.*

Proof. Assume $|U| \geq 4$. Then there exists $1 \neq U_0 \leq U$ such that $|U : U_0| = 2$. Consider $\overline{G} = G/U_0$. Then $\overline{G}$ is a dihedral 2-group and $\overline{R}$ is a semiregular RDS in $\overline{G}$ relative to $\overline{U}$ as $U_0 \leq U$ by applying Result 2.4. By the above theorem, $|\overline{U}| \geq 4$, a contradiction. Thus there exists no $(u\lambda, u, u\lambda, \lambda)$ RDS in $Q_{2^{n+1}}$ when $u > 2$.

The next result is also a consequence of the above theorem. The proof of the next corollary is similar to the proof of Corollary 5.2

Corollary 5.3 *Let R be a semiregular RDS in $S(2^{n+1})$ relative to U. Then $|U| \leq 2$.*

The next theorem provides an infinite sequence of RDS's in the non-abelian group $Q_{2^{n+1}}$, $n \geq 2$. The proof is done by induction using the product construction of RDS as basis.

Theorem 5.4 *There exist $(2^n, 2, 2^n, 2^{n-1})$ RDS in $Q_{2^{n+1}}$ relative to $Z(Q_{2^{n+1}})(\cong Z_2)$ for every $n \geq 2$.*

Proof. We prove by induction on n.

It is well known and easy to verify that $R = \{1, x, y, xy\}$ is a $(4, 2, 4, 2)$ RDS in $Q_8 = \langle x, y \rangle$ relative to $Z(Q_8) = \langle x^2 \rangle$(See Jungnickel[6], Examples 2.4(ii)). Thus the theorem is true for $n = 2$.

Assume the existence of a $(2^{n-1}, 2, 2^{n-1}, 2^{n-2})$ RDS in Q_{2^n} relative to $\langle z \rangle$ where z is the unique involution in Q_{2^n}. Let

$$G = Q_{2^{n+1}} = \langle x, y \mid x^{2^{n-1}} = y^2,\ y^4 = 1,\ y^{-1}xy = x^{-1} \rangle.$$

Consider $G_1 = \langle x^2, y\rangle$ and $G_2 = \langle xy\rangle$. Then $G_1 \cong Q_{2^n}$ and $G_2 \cong Z_4$. Set $U = \langle y^2\rangle \cong Z_2$.

By the induction hypothesis, let R_1 be a $(2^{n-1}, 2, 2^{n-1}, 2^{n-2})$ RDS in G_1 relative to U. On the other hand, it is easy to check that $R_2 = \{1, xy\}$ is a $(2,2,2,1)$ RDS is G_2 relative to U. Applying Result 2.5 , it follows that R_1R_2 is a $(2^n, 2, 2^n, 2^{n-1})$ RDS in G relative to U. Thus the theorem holds.

Example 5.5 Let A be an abelian subgroup of G of index 2. Let R_0 be a $(2\lambda, 2, 2\lambda, \lambda)$ RDS in an abelian group A relative to a subgroup $U(\cong Z_2)$. Assume that an element $t \in G$ inverts A and $\langle t^2\rangle = U$. Then $R = R_0 \cup R_0t$ is a $(4\lambda, 2, 4\lambda, 2\lambda)$ RDS in G relative to U.

Proof. See Jungnickel ([6]).

Remark 5.6 *Among the examples of Theorem 5.4, one is given by $R \subset G$ such that*

$$\widehat{R} = (1 + x^{2^{n-2}})(1 + y)(1 + x^{2^{n-3}}y)(1 + x^{n-4}y) \times \cdots \times (1 + x^2y)(1 + xy).$$

Remark 5.7 *There is no semiregular RDS in $S(2^4)$.*

Proof. Using Corollary 5.3, it suffices to consider the case $(m, u, k, \lambda) = (8, 2, 8, 4)$. By a computer search, we have Remark 5.7.

It is conceivable that there is no semiregular RDS in $S(2^{n+1})$.

References

1. J.A. Davis, *Constructions of Relative Difference Sets in p-Groups*, Discrete Math. **103** (1992), 7-15.

2. J.A. Davis and J. Jedwab, *A Unifying Construction for Difference Sets*, J. Comb. Th. (A) **80** (1997), 13-78.

3. J.A. Davis, J. Jedwab and M. Mowbray, *New Families of Semi-Regular Relative Difference Sets*, Designs, Codes and Cryptography **13** (1998), 131-146.

4. J.E.H. Elliot and A.T. Butson, *Relative Difference Sets*, Illinois J. Math. **10** (1966), 517 - 531.

5. K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory (2nd ed.)*, Springer-Verlag, New York/Berlin/Heidelberg, (1990).

6. D. Jungnickel, *On Automorphism Groups of Divisible Designs*, Can. J. Math. **34** (1982), 257-297.

7. S.L. Ma and A. Pott, *Relative Difference Sets, Planar Functions and Generalized Hadamard Matrices*, J. Algebra **175** (1995), 505-525.

8. S.L. Ma and B. Schmidt, *On* (p^a, p, p^a, p^{a-1}) *Relative Difference Sets*, Designs, Codes and Cryptography **6** (1995), 57-71.

9. A. Pott, *Finite Geometry and Character Theory*, Lecture Notes in Mathemaics 1601, Springer-Verlag, Berlin (1995).

10. A. Pott, *A Survey of Relative Difference Sets* in Groups, Difference Sets and the Monster (K.T.Arasu, et.al., eds.), de Gruyter, Berlin-New York (1996), 195-232.

11. B. Schmidt, *On* (p^a, p^b, p^a, p^{a-b}) *Relative Difference Sets*, J. Algebraic Combin. **6** (1997), 279-297.