<table>
<thead>
<tr>
<th>Title</th>
<th>On Relative Difference Sets In Non-Abelian Groups of Order $p^4$ (Algebraic Combinatorics)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Elvira, Dominic T.</td>
</tr>
<tr>
<td>Citation</td>
<td>数理解析研究所講究録 2003, 1299: 96-102</td>
</tr>
<tr>
<td>Issue Date</td>
<td>2003-01</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/2433/42710">http://hdl.handle.net/2433/42710</a></td>
</tr>
<tr>
<td>Type</td>
<td>Departmental Bulletin Paper</td>
</tr>
<tr>
<td>Textversion</td>
<td>publisher</td>
</tr>
</tbody>
</table>
On Relative Difference Sets In Non-Abelian Groups of Order $p^4$

Dominic T. Elvira*

1 Introduction

A $k$-element subset $R$ of a group $G$ of order $mu$ is called an $(m,u,k,\lambda)$ relative difference set (RDS) relative to a normal subgroup $U$ of order $u$ if the number of ordered pairs $(r_1,r_2) \in R \times R$ with $r_1 r_2^{-1} = g$ for every $g \in G$, $g \neq 1$ is $\lambda$ if $g \in G - U$ and $0$ if $g \in U$. The subgroup $U$ is often called the forbidden subgroup as its non-identity elements cannot be written in the above form. If $G$ is cyclic, abelian, and so on, its respective property is attached to the RDS $R$ in $G$.

In the study of RDS's, a subset $X$ of a group $G$ is often identified with the group ring element $X = \sum_{x \in X} x \in \mathbb{Z}[G]$ and we write $X^{(t)} = \sum_{x \in X} x^t$. With this notation, $R$ is an $(m,u,k,\lambda)$ RDS if and only if

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

If $k = u\lambda$, $R$ is called semi-regular and by (1.1), its parameters are $(u\lambda,u,u\lambda,\lambda)$. Also, in this case, $R$ is a complete set of coset representatives of $G/U$. If $u = 1$, $R$ is called a trivial semi-regular RDS. Any group $G$ is itself a trivial semi-regular RDS.

Many extensive studies have been done on relative difference sets, particularly the semi-regular case, in both abelian and non-abelian groups because of their close connection to other areas of combinatorics (see [1], [3], [4], [7], [12]). Readers may refer to Pott's book [10] or his survey [11] for more background information on RDS's.

Let $R_1$ and $R_2$ be RDS's in a group $G$ relative to normal subgroups $U_1$ and $U_2$, respectively. If there exists $\theta \in Aut(G)$, the full automorphism group of $G$ such that $\theta(R_1) = R_2$ and $\theta(U_1) = U_2$, then $R_1$ and $R_2$ are

*The author is a faculty member of Philippine Normal University (PNU), Manila on study leave at Kumamoto University under a Monbusho grant.
said to be equivalent. In our study, we only consider non-trivial and non-equivalent semi-regular RDS's. We also denote a prime number by \( p \) and \( I_p = \{0, 1, \ldots, p - 1\} \).

In this paper, we review the results on semi-regular RDS's in non-abelian groups of order \( p^4 \) with \( p \geq 3 \) and continue our study in [2].

2 Results on RDS's in \( p \)-Groups of Order \( \leq p^4 \)

A group \( G \) of order \( p \) can contain only a trivial RDS. If \( G \) is of order \( p^2 \) then we have the following result contained in [6].

**Result 2.1** Let \( G \) be a group of order \( p^2 \) containing a \((p, p, p, 1)\) RDS. Then

(i) \( G \simeq \mathbb{Z}_{p^2} \) if and only if \( p = 2 \), and

(ii) \( G \simeq \mathbb{Z}_p \times \mathbb{Z}_p \) if and only if \( p \geq 3 \).

In (i) above, \( R = \{1, x\} \) is a \((2, 2, 2, 1)\) RDS in \( \mathbb{Z}_4 = \langle x \rangle \) relative to \( U = \langle x^2 \rangle \).

In (ii) with \( G = \langle a, b \rangle \), the set \( R = \{a^i b^j | i \in I_p\} \) is an RDS relative to \( U = \langle a \rangle \). We note that there is only one equivalence class of RDS's in (ii) and all can be transformed into \( R \) by an appropriate translate or automorphism (see [6]). In fact, there exists a \((p^n, p^n, p^n, 1)\) RDS for every \( p \geq 2 \), \( n \geq 1 \) (see [10], pp. 46-47).

A non-trivial RDS in a group \( G \) of order \( p^3 \) has parameters \((p^3, p^2, p, p)\).

If \( G \) is abelian then \( G = \mathbb{Z}_{p^2} \times \mathbb{Z}_p \) or \( \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \) by Result 1.2 in [2].

The group \( \mathbb{Z}_{p^2} \times \mathbb{Z}_p \) contains non-trivial RDS's and these are characterized as follows:

**Result 2.2** (Ma-Pott, [6]) Let \( R \) be a \((p^2, p, p^2, p)\) RDS in \( G = \mathbb{Z}_{p^2} \times \mathbb{Z}_p \) relative to \( U \) with \( p \geq 3 \). Let \( H_1, \ldots, H_{p-1} \) denote \( p - 1 \) subgroups of \( G \) with \( |H_i| = p \), \( H_i \neq U \), and \( G/H_i \simeq \mathbb{Z}_{p^2} \). Let \( N \) be the subgroup of \( G \) with \( N \simeq \mathbb{Z}_p \times \mathbb{Z}_p \). Then there is a subgroup \( H_0 \neq H_i \) for \( i \neq 0 \) of \( N \), \( H_0 \neq U \), and \( p - 1 \) group elements \( h_i \) with \( \{1, h_1, \ldots, h_{p-1}\} \), a complete set of coset representatives of \( N \) such that \( R' = H_0 \cup \cup_{i=1}^{p-1} h_i H_i \) for some translate \( R' \) of \( R \). Conversely, any subset similar to \( R' \) is a \((p^2, p, p^2, p)\) RDS in \( G \).

The group \( G = \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p = \langle x, y, z \rangle \) contains non-trivial RDS's. The sets \( R_1 = \{x^i y^j z^k | i, j \in I_p\} \) and \( R_2 = \{x^i y^j z^{i+j} | i, j \in I_p\} \) are RDS's in \( G \) relative to \( U = \langle z \rangle \). More general constructions on RDS's in \( p \)-groups were obtained by Davis [1] and Pott [9].

When \( G \) is a non-abelian group of order \( p^3 \), we have:
Result 2.3 (Elvira-Hiramine, [3] and [4]) A non-abelian group $G$ of order $p^3$ contains a $(p^2, p, p^2, p)$ RDS relative to a normal subgroup $U$ unless $G = D_8$, the dihedral group of order 8.

As a consequence of Results 2.2, 2.3 and the contructions of RDS's in the elementary abelian group, we have:

Remark 2.4 Every non-cyclic group $G$ of order $p^3$ with $p \geq 3$ contains a $(p^2, p, p^2, p)$ RDS.

Problem: Classify the non-abelian $(p^2, p, p^2, p)$ RDS's and those in the elementary abelian group.

The parameters of a non-trivial semi-regular RDS in a group $G$ of order $p^4$ is either $(p^2, p^3, 1)$ or $(p^3, p, p^3, p^2)$.

Case: Abelian $(p^2, p^2, p^2, 1)$ RDS's

Result 2.5 (Ma-Pott, [6]) If an abelian group $G$ contains a $(p^2, p^2, p^2, 1)$ RDS with $p \geq 3$ then $G$ is elementary abelian.

A $(4, 4, 4, 1)$ RDS in an abelian group of order 16 exists only when $G \cong \mathbb{Z}_4 \times \mathbb{Z}_4$, $U \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ (see [10]) and so abelian groups of order $p^4$ containing a $(p^2, p^2, p^2, 1)$ RDS are determined.

Case: Abelian $(p^3, p, p^3, p^2)$ RDS's

By Result 1.2 in [2], the only abelian groups of order $p^4$ that can possibly contain a $(p^3, p, p^3, p^2)$ RDS are $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$, $\mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_p$, and $(\mathbb{Z}_p)^4$. If $p \geq 3$ it was shown by Ma and Schmidt [7] that each of these abelian groups contains a $(p^3, p, p^3, p^2)$ RDS relative to any subgroup $U$ except possibly in $\mathbb{Z}_{p^3} \times \mathbb{Z}_{p^2}$ [8].

Question: Does $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$ contain a $(p^3, p, p^3, p^2)$ RDS, $p \geq 5$?

If $G \cong \mathbb{Z}_9 \times \mathbb{Z}_9$, there exists no $(27, 3, 27, 3)$ RDS in $G$ as mentioned in [8]. When $p = 2$, an abelian group $G$ contains an $(8, 2, 8, 4)$ RDS relative to $U$ if and only if its exponent $\exp(G) \leq 8$ and $U$ is contained in a cyclic subgroup of $G$ of order 4 (see [7]). We extend these results by considering semi-regular RDS’s in non-abelian groups of order $p^4$.

Case: $G$ is non-abelian of order $p^4$

A classification of groups of order $p^4$, $p \geq 3$ can be found in Huppert’s book (see [5], pp. 346-347) or in Suzuki’s book (see [13], pp. 85-100). As
listed in [2], we denote by $G_{(i,p)}$, $1 \leq i \leq 15$ the non-isomorphic groups of order $p^4$. The first five are the abelian groups while the remaining denote the non-abelian groups. We note that the number of isomorphism classes of non-abelian groups of order $p^4$ with $p \geq 5$ is 10 only while that of order 81 is 11 with $G_{(16,3)}$ as an additional group. Refer to [2] for the definitions and properties of these groups.

Let $H_1$ and $H_2$ be subsets of a group $G$. If there exists $\theta \in Aut(G)$ such that $\theta(H_1) = H_2$ then $H_1$ and $H_2$ are called equivalent. In [2] and [4], we have determined all possible normal subgroups $U$ of order $p$ and $p^2$ in $G_{(i,p)}$, $i = 6, ..., 15$, $p \geq 3$ and $G_{(16,3)}$ up to equivalence for the forbidden subgroups and these computations are summarized in Table 1.

| Group Type | $|U| = p^2$ | $|U| = p$ |
|------------|------------|----------|
| $G_{(6,p)}$ | $\langle x^p \rangle, \langle x^p y, y \rangle, \langle x^p y \rangle$ | $\langle x^p \rangle$ |
| $G_{(7,p)}$ | $\langle x^p, y^p \rangle, \langle x \rangle$ | $\langle x^p \rangle, \langle y^p \rangle$ |
| $G_{(8,p)}$ | $\langle a_1 x \rangle, \langle a_1, a_3 \rangle, \langle x \rangle$ | $\langle x^p \rangle$ |
| $G_{(9,p)}$ | $\langle y, x^p \rangle$ | $\langle z^p \rangle$ |
| $G_{(10,p)}$ | $\langle y, z^p \rangle$ | $\langle z^p \rangle$ |
| $G_{(11,p)}$ | $\langle a_3, x \rangle, \langle a_1, a_3 \rangle$ | $\langle a_3 \rangle, \langle x \rangle$ |
| $G_{(12,p)}$ | $\langle a_1, a_2 \rangle$ | $\langle a_1 \rangle$ |
| $G_{(13,p)}$ | $\langle a_1, a_2 \rangle$ | $\langle x^p \rangle$ |
| $G_{(14,p)}$ | $\langle x^p, a_3 \rangle, \langle x \rangle, \langle x^p, a_2 \rangle$ | $\langle x^p \rangle, \langle a_3 \rangle$ |
| $G_{(15,p)}$ | $\langle a_1, a_2 \rangle, \langle a_2, a_3 \rangle$ | $\langle a_1 \rangle, \langle a_2 \rangle, \langle a_1 a_2 \rangle$ |
| $G_{(16,3)}$ | $\langle a_2, a_3 \rangle$ | $\langle a_3 \rangle$ |

Table 1: The non-equivalent normal subgroups $U$ of order $p$ and $p^2$ in $G_{(i,p)}$, $6 \leq i \leq 15$, $p \geq 3$ and $G_{(16,3)}$.

3 Results on Non-Abelian $(p^2, p^2, p^2, 1)$ RDS's

When $p = 2$, by simple computations and computer search we have the following:

**Theorem 3.1** There exists no $(4, 4, 4, 1)$ RDS in a non-abelian group of order 16 relative to a normal subgroup $U$ except in the following:

(i) $G = M_4(2) = \langle x, y|x^8 = y^2 = 1, y^{-1}xy = x^5\rangle$, $U = \langle x^4, y \rangle = Z(G)$,
(ii) $G = Q_8 \times \mathbb{Z}_2$ where $Q_8 = \langle x, y | x^2 = y^2 = m, m^2 = 1, y^{-1}xy = x^{-1} \rangle$ and $\mathbb{Z}_2 = \langle z \rangle$, $U = \langle x^2, z \rangle = Z(G)$.

In (i), the set $R = \{1, x^2y, x^3y, x^5y\}$ is an RDS (K. Akiyama) and in (ii), the set $R = \{1, x^3z, y, xy\}$ is an RDS.

For $p \geq 3$, we now enumerate all our results.

**Result 3.2 (Elvira-Hiramine, [4])** There exists no $(p^2, p^2, p^2, 1)$ RDS in the group $G_{(6,p)}$ relative to any normal subgroup of order $p^2$.

**Result 3.3 ([2])** There exists no $(p^2, p^2, p^2, 1)$ RDS in $G_{(7,p)}$ relative to any normal subgroup.

**Result 3.4 ([2])** There exists a $(p^2, p^2, p^2, 1)$ RDS in $G_{(11,p)}$, $p \geq 3$ relative to $\langle a_3, x \rangle$.

An example of an RDS in Result 3.4 is the set

$$R = \{a_1^ia_2^ja_3^{-\frac{ij(i-1)}{2}}x^{-i+\frac{ij(i-1)}{2}}, i, j \in I_p\}$$

where $s = \alpha^2 \in GF(p)$, $\alpha \in GF(p^2)$. We ask the following:

**Question:** Do $(p^2, p^2, p^2, 1)$ RDS's exist in $G_{(i,p)}$, $8 \leq i \leq 15$ with $p \geq 3$ aside from the RDS's in Result 3.4?

### 4 Results on Non-Abelian $(p^3, p, p^3, p^2)$ RDS's

When $p = 2$, we have the following:

**Result 4.1 (Elvira-Hiramine, [4])** A non-abelian group of order 16 containing a maximal cyclic subgroup of order 8 does not contain an $(8, 2, 8, 4)$ RDS except $Q_{16}$.

An example in $Q_{16} = \langle x, y | x^4 = y^2 = m, m^2 = 1, y^{-1}xy = x^{-1} \rangle$ relative to $\langle x^4 \rangle = Z(Q_{16})$ is $R = (1 + x^2)(1 + y)(1 + xy)$.

We now consider $(p^3, p, p^3, p^2)$ RDS’s in non-abelian groups when $p \geq 3$.

**Result 4.2 ([2])** Let $G$ be a group of order $p^4$, $p \geq 3$. If $G$ contains non-cyclic subgroups $G_1$ and $G_2$ of order $p^3$ and $p^2$, respectively, satisfying $G = G_1G_2$ and $G_1 \cap G_2 = U \simeq \mathbb{Z}_p \triangleleft G_1$ then $G$ contains a $(p^3, p, p^3, p^2)$ RDS relative to $U$. 
Table 2: Existence of a \((p^3, p, p^3, p^2)\) RDS in \(G_{(i,p)}\), \(8 \leq i \leq 15\), \(p \geq 3\) relative to a normal subgroup \(U\).

In the groups \(G_{(i,p)}\), \(8 \leq i \leq 15\), \(p \geq 3\), we can find examples of subgroups \(G_1\) and \(G_2\) satisfying the conditions of Result 4.2. Thus there exist \((p^3, p, p^3, p^2)\) RDS’s in these groups relative to the forbidden subgroups \(U\) given in Table 1. We summarize these results in Table 2.

**Remark 4.3** By using Table 2, we conclude that there exists a \((p^3, p, p^3, p^2)\) RDS in non-abelian groups of order \(p^4\), \(p \geq 3\) except possibly in the following:

(i) \(G_{(6,p)}\) with \(U = \langle x^p \rangle\), \(p \geq 5\),

(ii) \(G_{(7,p)}\) with \(U = \langle x^p \rangle\) or \(\langle y^p \rangle\), \(p \geq 3\) and

(iii) \(G_{(16,3)}\) with \(U = \langle a_1^3 \rangle\).

We note that each group \(G\) not covered by Remark 4.3 has \(\Omega_1(G) = \{g \in G | g^p = 1\} \simeq \mathbb{Z}_p \times \mathbb{Z}_p\). Also, a \((27, 3, 27, 9)\) RDS does not exist in \(G_{(6,3)}\) by a computer search done in [4]. We ask the following:

**Question:** Do \((p^3, p, p^3, p^2)\) RDS’s exist in the groups given in Remark 4.3?

If we consider groups \(G\) containing a normal subgroup \(N \subset U\) such that \(G/N \simeq \mathbb{Z}_{p^2} \times \mathbb{Z}_p\). Then by Result 2.2 in [2], we can obtain a simpler form for an RDS \(R\) in \(G\). The groups satisfying this condition are:

(1) \(G_{(6,p)}, U = \langle x^{p^2}, y \rangle, \langle x^p y \rangle, N = \langle x^{p^2} \rangle\)
(2) \( G_{(7,p)}, U = \langle x^p, y^p \rangle, \langle x \rangle, N = \langle x^p \rangle \), and

(3) \( G_{(15,p)} \), \( U = \langle a_1, a_2 \rangle, \langle a_2, a_3 \rangle, N = \langle a_2 \rangle \).

At present, only case (3) remains open.

References


Department of Mathematics
Graduate School of Science and Technology
Kumamoto University
Kurokami, Kumamoto, Japan
E-mail: dtelvira@math.sci.kumamoto-u.ac.jp