A Survey of Relative Difference Sets

Christine Berkesch

Jeff Ginn

Erin Haller

Erin Militzer

September 5, 2003

Abstract

A (v, k, λ) difference set D in a group G is a subset of G such that every nonidentity element of G is covered exactly λ times by quotients $d_1 d_2^{-1},\ d_1, d_2 \in D$. In the group ring, this means that D obeys the equation $DD^{(-1)} = k \cdot 1 + \lambda(G - 1)$. An (m, n, k, λ) relative difference set R is a difference set relative to a normal subgroup N of G satisfying the similar equation $RR^{(-1)} = k \cdot 1 + \lambda(G - N)$. Difference sets may be used to construct symmetric designs with a nice automorphism group; relative difference sets are used to construct square divisible designs with a nice automorphism group. Symmetric designs and divisible designs are important combinatorial structures.

We will describe various search techniques for relative difference sets (RDS), including the exhaustive search method for small groups using the computer program GAP, as well as the multiplier theorem and group representations methods used for larger groups. We will provide a catalog of RDS found, as well as those eliminated, using these methods. A proof is presented of the non-existence of $(2m, 2, 2m, m)$ relative difference sets in quaternion groups of order $4m$ where m is odd. In conclusion, we will state several interesting results found for specific parameters, including (12,2,12,6) and (12,3,12,4).

Contents

1 Introduction - Difference Sets and Symmetric Designs

An important topic in the field of discrete mathematics is the study of block designs. A (n, k, λ) block design is a set of v points arranged into b blocks of size k where any 2 points are together on exactly λ blocks. A design is called symmetric if $v = b$.

Symmetric designs may be constructed using difference sets. Given a difference set D in a group G, define the points of the design as the elements of G and the blocks as the translates gD for $g \in G$ of the difference set. This construction gives a symmetric design with an automorphism group acting sharply transitive on the points of the design ([3], p. 8-10).

A group divisible design is a combinatorial structure with a slightly weaker condition than a symmetric block design ([3], p. 3). A group divisible design may be constructed from relative difference sets in the same way that symmetric designs are constructed from difference sets.

Much of the research on RDS has focused on families of semiregular difference sets (see [3], p. 40). This paper will survey small parameter sets for semiregular RDS and describe several semiregular RDS which were previously unknown.

In this paper, we exhausively determine the existence of RDS with certain small parameters and find new semiregular RDS.

Acknowledgements
This research was done during Summer 2002 at Central Michigan University under the guidance of Dr. Ken Smith and sponsorship of the National Science Foundation Research Experience for Undergraduates grant (NSF DMS-0097394).

2 Basics of Difference Sets and Relative Difference Sets

Throughout this paper, we use definitions and notation based on those of Alexander Pott [3].

Definition 1. A (v, k, λ) *difference set* D is a subset of a group G of order k such that in the list of quotients $d_1 \cdot d_2^{-1}$ with distinct elements $d_1, d_2 \in D$ each nonidentity element of G occurs exactly λ times.

Definition 2. An (m, n, k, λ) *relative difference set* R in a group G of order $m \cdot n$ relative to a forbidden normal subgroup N ($|N| = n$) is a k-subset of G with the following property: the list of quotients $r_1 \cdot r_2^{-1}$ with distinct elements $r_1, r_2^{-1} \in R$ contains each element in G/N exactly λ times and does not contain the elements of N. Thus, the following formula in the group ring ZG must be satisfied:

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

Difference sets are homomorphic images of relative difference sets (RDS). One can show that the existence of an (m, n, k, λ) relative difference set implies the existence of an $(m, k, n\lambda)$ difference set. Suppose a group G contains a relative difference set R relative to a normal subgroup N, then if a normal subgroup H of G is contained in N, there exists a relative difference set in G/H relative to N/H. Furthermore, if R has parameters (m, n, k, λ) then the RDS in G/H will have parameters $(m, \frac{n}{h}, k, \lambda h)$ where $|H| = h$. Hence, G/N will contain an $(m, k, n\lambda)$ difference set which is said to be a contraction of R. R is said to be an extension or lifting of this difference set. The contraction of a semiregular RDS is the trivial (m, m, m) difference set.

The existence of a (v, k, λ) difference set implies the existence of a (v, k, λ) *symmetric design*. Similarly, the existence of an (m, n, k, λ) RDS implies the existence of an (m, n, k, λ) *divisible design*. (See Section 1.1 of [3].)

Definition 3. An (m, n, k, λ) *divisible design* is an incidence structure with mn points and the same number of blocks such that every block has k points and every point is on k blocks. Also, every pair of points will be together on λ blocks except the points corresponding to the cosets of the normal subgroup N to which the (m, n, k, λ) RDS is relative.

Let the elements of a group G form the points of a divisible design. The translates of a relative difference set R in G form the set of blocks B of the design, so that $B = \{gR : g \in G\}$.

Divisible designs are often useful in projective geometries. If we are given a projective plane and remove one of the blocks and all those parallel to it, we are left with a divisible design [**?**].

Lemma 1. Given a group G and a normal subgroup N of G, R may contain no two elements of the same coset of N.

Proof. Let $x \in G$ and Nx be a right coset of N. Suppose r_1 and r_2 are distinct elements of R such that $r_1 = n_1 x$ and $r_2 = n_2 x$ where $n_1, n_2 \in N$. Then

$$r_1 r_2^{-1} = (n_1 x) x^{-1} n_2^{-1} = n_1 n_2^{-1} \in N,$$

but $r_1 r_2^{-1}$ is not supposed to be in N, a contradiction. □

Lemma 2. Given a group G with normal subgroup N and RDS R, then any translate $Rg := \{rg : r \in R\}$ of R is also a RDS.

Proof. If $x = r_1 r_2^{-1}$ for $r_1, r_2 \in R$ then $x = r_1(gg^{-1})r_2 = (r_1 g)(r_2 g)^{-1}$ and $r_1 g, r_2 g \in Rg$. □

Definition 4. A relative difference set is said to be *semiregular* if $m = k = n\lambda$.

Theorem 1 (Prime powers in RDS). (p^a, p^b, p^a, p^{a-b}) RDS exist whenever p is a prime and $a \geq b$ [**?**].

3 Search Techniques

In this section we describe the various techniques we used to search for relative difference sets in finite groups.

3.1 The Bose-Connor Theorem

Theorem 2 [3]. Let R be an (m, n, k, λ) RDS in a group G with respect to a subgroup N. If $k^2 \geq mn\lambda$ and $k > 0$ then

(1) if m is even then $k^2 - mn\lambda$ is a square. Moreover, if $m \equiv 2 \mod 4$ and n is even, then k is the sum of two squares.

(2) if m is odd and n is even then
(2a) k is a square and
(2b) the equation

$$(k^2 - mn\lambda)x^2 + (-1)^{m(m-1)/2} n\lambda y^2 = z^2$$

has nontrivial integer solutions (x, y, z).

(3) if both m and n are odd then the equation

$$kx^2 + (-1)^{n(n-1)/2} ny^2 = z^2$$

has nontrivial integer solutions.

The Bose-Connor theorem is useful in ruling out RDS parameters. For example, there exist no nontrivial integer solutions to the equation

$$10x^2 + ((-1)^{5(5-1)/2} \cdot 5)y^2 = z^2,$$

which corresponds with the $(19, 5, 10, 1)$ parameter set, where m and n are both odd. This implies that no $(19, 5, 10, 1)$ RDS exists.

3.2 Groups, Algorithms, and Programming (GAP)

For groups of small order, an exhaustive search can be the most effective method for finding all possible RDS. The computer program GAP [1] provides a complete listing of groups, along with the capability to search them for RDS. By modifying a GAP program written by Dr. Ken Smith, it was possible to search for RDS with various parameters, the results of which can be found in section 4.1.

The program checks all groups corresponding to a given set of parameters for a RDS. Within each group G, it finds each normal subgroup N of the appropriate order and also generates the cosets with respect to N. Each relative difference set has at most one element in a given coset of N, and so a RDS R is a subset of a transversal (a system of coset representatives) of N. If the RDS is semiregular, then it is equal to a transversal.

The GAP program chooses a transversal and checks to see if it provides a RDS. If not, it chooses another transversal. There are n^m transversals for a given subgroup N, but the search can be reduced to n^{m-2} possibilities by fixing two elements of R: the identity element and one element x from another coset. This is allowed by the following argument. Assume $x \notin N$. Then there exists $r_1, r_2 \in R$ such that $x = r_1 r_2^{-1}$. Since R is a RDS, so is Rr_2^{-1}. But since $r_1, r_2 \in R$ then $x = r_1 r_2^{-1}$ and $1 = r_2 r_2^{-1}$ are in Rr_2^{-1}. Thus the RDS R can be replaced by the RDS Rr_2^{-1}, which contains both 1 and x.

If the initial transversal choice fails, the elements in the cosets are permuted until a RDS is found or all possibilities have been exhausted. The problem, however, is that as the order of the group grows and the number of groups of the orders grow, the number of possibilities for transversals increases exponentially. For this reason, the exhaustive method should only be used for small groups. For larger groups, other methods had to be implemented. Exhaustively searching a group for an (m, n, k, λ) RDS required checking n^{m-2} putative difference sets to see if they satisfied the basic equation from definifion 2. If n^{m-2} was on the order of a million, this process took several hours on a Mac G3 laptop computer.

3.3 Multipliers

Lemma 3. If A is an Abelian group written in additive notation and t is relatively prime to the order of A, then $a \mapsto ta$ for all $a \in A$ is an automorphism of A.

Definition 5. If $tD = g + D$ for some $g \in G$, then t is said to be a *multiplier*.

Conjecture. Suppose t is relatively prime to the order of A and, in addition, $t|(k - \lambda)$ in a difference set or if $t|(k^2 - mn\lambda)$ in a RDS. Then, if there exists a (v, k, λ) difference set or an (m, n, k, λ) RDS then there is a difference set or RDS fixed by t (see [3], pp. 29-30).

Suppose we are searching for a $(7, 4, 2)$ difference set in Z_7; then $t = 2$ is a multiplier. The multiplier $t = 2$ generates the orbits $\{0\}, \{1, 2, 4\}, \{3, 5, 6\}$ in $\{Z_7, +\}$. We pick $\{0\}$ and one of $\{1, 2, 4\}$ or $\{3, 5, 6\}$ to be our difference set. Note that the sets $\{0, 1, 2, 4\}$ and $\{0, 3, 5, 6\}$ are isomorphic to one another under $a \mapsto 3a$.

A multiplier may also be "lifted." If we were to lift the $(7, 4, 2)$ difference set from the above example into a $(7, 2, 4, 2)$ RDS, then the multiplier $t = 2$ would be lifted to $t = 9$ where $a \mapsto 9a$ is an automorphism of Z_{14} and fixes a $(7, 2, 4, 2)$ RDS.

3.4 Representations

A *representation* Φ of a group G is an operation-preserving map from $(G, *)$ into $(GL_n(\mathbb{C}), \cdot)$. Representations will be used to distinguish between the elements in each coset while building a RDS.

A representation Φ is said to be *trivial* on a subgroup N of G if $\Phi(x) = 1$ for all $x \in N$.

Representations of finite groups may be built from a special set of representations called "irreducible representations" (see [**?**]). We extend a representation Φ on G to a representation of the group ring ZG by defining $\Phi(\sum a_g g) := \sum a_g \Phi(g)$. Thus, $\Phi : ZG \to \mathrm{Mat}_N(\mathbb{C})$ is an algebra homomorphism.

Theorem 3. Let N be a normal subgroup of G; let Φ be an irreducible representation of G. Then either Φ is trivial on N or $\sum_{x \in G} \Phi(x) = 0$.

In the case where $\Phi(N)$ is trivial on N, each element in a coset of N is treated the same. This only reiterates the fact that one element must be chosen from each coset without providing new information to aid in the actual selection of elements. Thus for the given purposes, the cases of interest occur when $\sum_{x\in G}\Phi(x)=0$. (For further reading and examples on this topic, see [**?**] and [**?**].)

When Φ is not trivial on N, it should be noted that both $\sum_{g\in G}\Phi(g)$ and $\sum_{n\in N}\Phi(n)=0$, and so $\Phi(G-N)=0$.

Example:

Search for an (8,2,8,4) RDS in the group $G=Q_8=<x,y:\ x^8=y^4=1,\ yxy^{-1}=x^{-1},\ x^4=y^2>$ with respect to the unique subgroup of order two: $N=\{1,x^4\}$. Let ζ be a primitive 8th root of unity. Here are the representations of G and their action on N.

Representations

	x	y	N	
	1	$\pm$ 1	2	trivial on N
	-1	$\pm$ 1	2	trivial on N
Φ_1	$\begin{pmatrix}\zeta & 0\\ 0 & \bar{\zeta}\end{pmatrix}$	$\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$	$\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$	
	$\begin{pmatrix}\zeta^2 & 0\\ 0 & \bar{\zeta}^2\end{pmatrix}$	$\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$	$\begin{pmatrix}2 & 0\\ 0 & 2\end{pmatrix}$	trivial on N
Φ_2	$\begin{pmatrix}\zeta^3 & 0\\ 0 & \bar{\zeta}^3\end{pmatrix}$	$\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$	$\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$	

Since Φ_1 and Φ_2 are the only cases which are non-trivial on N, they are the only two that need to be considered.

For Φ_1 and Φ_2, $RR^{(-1)}\mapsto 8I_2+4[\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}-\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}]=\begin{pmatrix}8 & 0\\ 0 & 8\end{pmatrix}$

First, let us consider Φ_1. The cosets with respect to N are:

$$\begin{array}{c|c|c|c|c|c|c|c} 1 & x & x^2 & x^3 & y & xy & x^2y & x^3y \\ x^4 & x^5 & x^6 & x^7 & x^4y & x^5y & x^6y & x^7y \end{array}$$

These elements map as follows under Φ_1:

$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$
$\begin{pmatrix}\zeta & 0\\ 0 & \bar{\zeta}\end{pmatrix}$
$\begin{pmatrix}\zeta^2 & 0\\ 0 & \bar{\zeta}^2\end{pmatrix}$
$\begin{pmatrix}\zeta^3 & 0\\ 0 & \bar{\zeta}^3\end{pmatrix}$
$\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$
$\begin{pmatrix}0 & \zeta\\ -\bar{\zeta} & 0\end{pmatrix}$
$\begin{pmatrix}0 & \zeta^2\\ -\bar{\zeta}^2 & 0\end{pmatrix}$
$\begin{pmatrix}0 & \zeta^3\\ -\bar{\zeta}^3 & 0\end{pmatrix}$
$\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}$
$\begin{pmatrix}-\zeta & 0\\ 0 & -\bar{\zeta}\end{pmatrix}$
$\begin{pmatrix}-\zeta^2 & 0\\ 0 & -\bar{\zeta}^2\end{pmatrix}$

$\begin{pmatrix} -\zeta^3 & 0 \\ 0 & -\bar{\zeta}^3 \end{pmatrix}$
$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$
$\begin{pmatrix} 0 & -\zeta \\ \bar{\zeta} & 0 \end{pmatrix}$
$\begin{pmatrix} 0 & -\zeta^2 \\ \bar{\zeta}^2 & 0 \end{pmatrix}$
$\begin{pmatrix} 0 & -\zeta^3 \\ \bar{\zeta}^3 & 0 \end{pmatrix}$

Let $R \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $R^{(-1)} \mapsto \begin{pmatrix} \bar{a} & \bar{c} \\ \bar{b} & \bar{d} \end{pmatrix}$, where $a = \epsilon_0 + \epsilon_1\zeta + \epsilon_2\zeta^2 + \epsilon_3\zeta^3$ and $b = \epsilon_4 + \epsilon_5\zeta + \epsilon_6\zeta^2 + \epsilon_7\zeta^3$. Here $\epsilon_i = \pm 1$, where 1 indicates the element from top row of a coset and -1 indicates the element from bottom row of a coset. The elements c and d follow from the values of a and b.

Therefore, $RR^{(-1)} \mapsto \begin{pmatrix} a\bar{a} + b\bar{b} & a\bar{c} + b\bar{d} \\ c\bar{a} + d\bar{b} & c\bar{c} + d\bar{d} \end{pmatrix} = \begin{pmatrix} 8 & 0 \\ 0 & 8 \end{pmatrix}$.

In other words, $||a||^2 + ||b||^2 = 8$ and $c\bar{a} + d\bar{b} = 0$.

One solution to these equations is $\epsilon_i = (1, 1, 1, 1, 1, 1, -1, 1)$, i.e. all of the elements for the relative difference set are from the top row in the cosets except for the second to last one.

Using these choices, $a = 1 + (\sqrt{2} + 1)i$ and $b = 1 + (\sqrt{2} - 1)i$.

So $||a||^2 = 4 + 2\sqrt{2}$, $||b||^2 = 4 - 2\sqrt{2}$, and $||a||^2 + ||b||^2 = 8$, as desired.

By working back through the mappings, we find that $R = 1 + x + x^2 + x^3 + y + xy + x^3y + x^6y$ is an $(8, 2, 8, 4)$ RDS in Q_8.

4 Results

4.1 GAP

The following tables describe the results of an exhaustive search in GAP, grouped according to the type of relative difference set. In each table we list parameters of relative difference sets and determine the existence of a RDS with those parameters. If we found the difference sets using GAP in an exhaustive search, we included, for each group with a RDS, the number of the group in GAP's small group library. For example, "16.2,3,4,5,9,10,11,12,13" in the "GAP library number" column in the first table indicates that of the fourteen groups of order sixteen, the groups numbered 2-5 and 9-13 have $(8, 2, 8, 4)$ relative difference sets.

$(m, 2, m, m/2)$

Parameters	RDS?	GAP library number
(6,2,6,3)	no	
(8,2,8,4)	yes	16.2, 3, 4, 5, 9, 10, 11, 12, 13
(10,2,10,5)	no	
(12,2,12,6)	yes	24.3, 4, 11
(14,2,14,7)	no	

$(m, m, m, 1)$

Parameters	RDS?	GAP library number
(4,4,4,1)	yes	16.2, 6, 12
(5,5,5,1)	yes	25.2
(6,6,6,1)	no	
(7,7,7,1)	yes*	
(8,8,8,1)	yes*	

*These exist by Theorem 1. No further search was performed.

Other

Parameters	RDS?	GAP library number
(8,2,8,4)	yes	16.2, 3, 4, 5, 9, 10, 11, 12, 13
(8,4,8,2)	yes	32.21, 23, 25, 26, 28, 29, 32, 33, 35
(9,3,9,3)	yes	27.2, 3, 4, 5

4.2 Quaternion Theorem

The quaternion groups, $Q_{2m} =< x, y : x^{2m} = y^4 = 1, yxy^{-1} = x^{-1}, x^m = y^2 >$, are a particularly interesting case for the $(2m, 2, 2m, m)$ parameters. We found the following when considering these groups:

Parameters	RDS?	Reason
(4,2,4,2)	Yes	
(6,2,6,3)	No	Exhaustive search (GAP)
(8,2,8,4)	Yes	
(10,2,10,5)	No	Exhaustive search (GAP)
(12,2,12,6)	Yes	
(14,2,14,7)	No	Bose-Connor Theorem
(16,2,16,8)	Yes	
(18,2,18,9)	No	Exhaustive search (GAP)
(20,2,20,10)	Yes	
(22,2,22,11)	No	Bose-Connor Theorem
(24,2,24,12)	Yes	

There is an obvious pattern in the existence of a RDS when m is even and nonexistence when m is odd. With this in mind, the following theorem arose.

Theorem 4. There do not exist any $(2m, 2, 2m, m)$ RDS in Q_{2m} when m is odd.

Proof. For $(2s, 2, 2s, s)$ RDS in Q_{2s} when s is odd, check two representations:

$$\Phi_1 : x \mapsto -1, \quad y \mapsto i.$$

$$\Phi_2 : x \mapsto \begin{pmatrix} \zeta & 0 \\ 0 & \bar{\zeta} \end{pmatrix}, \quad y \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

where ζ is a primitive $2s^{th}$ root of unity.

By constructing R from the cosets of Q_{2m} with respect to N, it is obvious that

$$R = \sum_{i=0}^{s-1} a_i x^i + (\sum_{i=0}^{s-1} b_i x^i) y.$$

Therefore, $RR^{(-1)} = 2s \cdot 1 + \lambda(0) = 2s \cdot 1$.

For Φ_2, $R \mapsto \begin{pmatrix} \sum_{i=0}^{s-1} a_i\zeta^i & 0 \\ 0 & \sum_{i=0}^{s-1} a_i\bar{\zeta}^i \end{pmatrix} + \begin{pmatrix} \sum_{i=0}^{s-1} b_i\zeta^i & 0 \\ 0 & \sum_{i=0}^{s-1} b_i\bar{\zeta}^i \end{pmatrix} y,$

$= \begin{pmatrix} A & 0 \\ 0 & \bar{A} \end{pmatrix} + \begin{pmatrix} B & 0 \\ 0 & \bar{B} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$

$= \begin{pmatrix} A & B \\ -\bar{B} & \bar{A} \end{pmatrix}.$

So, $RR^{(-1)} \mapsto \begin{pmatrix} A\bar{A} + B\bar{B} & 0 \\ 0 & A\bar{A} + B\bar{B} \end{pmatrix}.$

Therefore $A\bar{A} + B\bar{B} = 2s \in (2)$ but $\notin (4)$.

By (2) and (4), we mean the ideals generated by 2 and 4, respectively. While A and B are cyclotomic integers, the given statement still holds. For further reading on this topic, consult Ireland and Rosen [**?**].

Now, $A = \sum_{i=0}^{s-1} a_i\zeta^i$, where $a_i = \pm 1$, the indicator within each coset.

$$A + 0 = \sum_{i=0}^{s-1} a_i\zeta^i + \sum_{i=0}^{s-1} (-1)^i\zeta^i,$$

$$= \sum_{i=0}^{s-1} (a_i + (-1)^i)\zeta^i.$$

$\Rightarrow A \in (2)$ and similarly, $B \in (2)$.

$\Rightarrow$ Since $(2)(2) = (4)$, we have that $A\bar{A} + B\bar{B} \in (4)$, a contradiction. $\square$

This leaves the cases with m even open. We have not yet been able to prove the existence of a $(2m, 2, 2m, m)$ RDS in this case, but do believe it is true. We conjecture that there exists a $(2m, 2, 2m, m)$ RDS in all Q_{2m} when m is even.

After reaching this conclusion, we found Ito's conjecture, which states that there are $(4t, 2, 4t, 2t)$ RDS in Q_{8t} for all t such that $2t - 1$ or $4t - 1$ is a prime power [**?**]. This conjecture is strong and has been verified for all $t \leq 46$ [2]. It is important to point out that a proof for this conjecture would also imply the Hadamard conjecture, which has remained open since posed in 1893.

4.3 Specific Parameters

4.3.1 $(12, 2, 12, 6)$

It is worth noting that we found only three $(12, 2, 12, 6)$ RDS, all in nonabelian groups: $SL_2(3)$, Q_{12}, and $Z_3 \times Q_4$, which are all generated by three elements, x, y, z such that:

$SL_2(3) = < x, y, z : x^4 = y^4 = z^3 = 1, x^2 = y^2, yxy^{-1} = x^{-1}, zxz^{-1} = y, zyz^{-1} = xy >$,

$Q_{12} = < x, y, z : x^4 = y^4 = z^3 = 1, x^2 = y^2, yxy^{-1} = x^{-1}, xzx^{-1} = z^2, yz = zy >$, and

$Q_4 \times Z_3 = < x, y, z : x^4 = y^4 = z^3 = 1, x^2 = y^2, yxy^{-1} = x^{-1}, xz = zx, yz = zy >$.

This points out that investigating RDS in only Abelian groups will not give a full analysis of all working parameters. Nonabelian groups contain RDS that are also quite interesting.

A $(12, 2, 12, 6)$ relative difference set in all three groups is:

$$R = (x^2 + x + y + xy)(1 + z) + (1 + x + y + xy)(x^2z^2).$$

The idea that one "magic" formula will produce a RDS in all three groups is exciting. It suggests that all other RDS should be investigated to see if this phenomenon occurs with any other parameters.

4.3.2 $(12, 3, 12, 4)$

Alexander Pott stated, "$(m, 2, m, m/2)$ are the only examples of semiregular relative difference sets in groups which are not p-groups: All known examples with $n \neq 2$ live in p-groups" [3], p. 103.

However, we found $(12, 3, 12, 4)$ RDS in the three following groups: $Q_6 \times Z_3$, $A_4 \times Z_3$, and $(Z_6 \times Z_2) \times Z_3$. These groups provide examples outside p-groups which do contain RDS. This opens the door to a search for many other RDS. Notice also that all three groups are splitting, meaning that $Z_3 = N$ in each group.

A $(12, 3, 12, 4)$ RDS in $Q_6 \times Z_3 = < x, y, z : x^6 = y^4 = 1, yxy^{-1} = x^{-1}, x^3 = y^2, z^3 = 1, zx = xz, zy = yz >$ is:

$$(1 + y + x^2y + x^4y + x^5 + xy) + (x^3 + x^3y + x^2 + x^5y)z + (x^4 + x)z^2.$$

A $(12, 3, 12, 4)$ RDS in $A_4 \times Z_3 =< x, y_1, y_2 : x^3 = y_1^2 = y_2^2 = 1, y_2 = y_1^x, y_2^x = y_1y_2 > \times < z : z^3 = 1 >$ is:

$$(1 + x^2y_1 + xy_1 + xy_2 + y_2 + x^2) + (y_1 + x^2y_1y_2 + y_1y_2 + x^2y_2)z + (xy_1y_2 + x)z^2.$$

A $(12, 3, 12, 4)$ RDS in $(Z_6 \times Z_2) \times Z_3 =< x, y, z : x^6 = y^2 = z^3 >$ is:

$$(1 + x^2y + x^3 + x^5) + (x + xy)z + (y + x^2 + x^3y + x^4 + x^4y + x^5y)z^2.$$

4.3.3 (12,6,12,2)

The next logical step is to attempt a lift of the previous two parameters to a $(12, 6, 12, 2)$ RDS. In order to be eligible for such a RDS, a group G of order 72 must have a normal subgroup N of order six where the subgroups H_2 and H_3 of N, of orders two and three respectively, give factor groups corresponding to those which have $(12, 3, 12, 4)$ and $(12, 2, 12, 6)$ RDS.

Using GAP, it was determined that the possibility of such a RDS only exists in two groups: $SL_2(3) \times Z_3$ and $Q_4 \times Z_3^2$.

An exhaustive search of these groups, using GAP, would require, for each normal subgroup N of order six, examining $6^{10} \approx 60$ million transversals and running a relative difference set check on each transversal. Our current program would take approximately a month of computer time to exhaust one group. Therefore, at this time, the existence of a $(12, 6, 12, 2)$ RDS is still open.

References

[1] The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4.2;2002. (¡http://www.gap-system.org¿)

[2] B. Schmidt, Williamson Matrices and a Conjecture of Ito's, Designs, Codes, and Cryptography, Vol. 17 (1999) pp. 61-68.

[3] A. Pott, Finite Geometry and Character Theory, Springer-Verlag, Berlin-Heidelberg 1995.