5-25-1992

Construction of Relative Difference Sets in p-groups

James A. Davis
University of Richmond, jdavis@richmond.edu

Recommended Citation
Davis, James A. "Construction of Relative Difference Sets in P-groups." *Discrete Mathematics* 103, no. 1 (May 25, 1992): 7-15. doi: 10.1016/0012-365X(92)90034-D.

Discrete Mathematics 103 (1992) 7–15
North-Holland

Construction of relative difference sets in p-groups

James A. Davis*

Department of Mathematics, University of Richmond, Richmond VA 23173, USA

Received 6 September 1989
Revised 30 May 1990

Abstract

Davis, J.A., Construction of relative difference sets in p-groups, Discrete Mathematics 103 (1992) 7–15.

Jungnickel (1982) and Elliot and Butson (1966) have shown that $(p^{j+1}, p, p^{j+1}, p^j)$ relative difference sets exist in the elementary abelian p-group case (p an odd prime) and many 2-groups for the case $p = 2$. This paper provides two new constructions of relative difference sets with these parameters; the first handles any p-group (including non-abelian) with a special subgroup if j is odd, and any 2-group with that subgroup if j is even. The second construction shows that if j is odd, every abelian group of order p^{j+2} and exponent less than or equal to $p^{(j+3)/2}$ has a relative difference set. If j is even, we show that every abelian group of order 2^{j+2} and exponent less than or equal to $2^{(j+4)/2}$ has a relative difference set except the elementary abelian group. Finally, Jungnickel (1982) found $(p^{i+j}, p^i, p^{i+j}, p^j)$ relative difference sets for all i, j in elementary abelian groups when p is an odd prime and in $\mathbb{Z}_4^i \times \mathbb{Z}_2^j$ when $p = 2$. This paper also provides a construction for $i + j$ even and $i \leq j$ in many group with a special subgroup. This is a generalization of the construction found in a submitted paper.

1. Introduction

A relative difference set (RDS) in a finite group G relative to a subgroup H is a subset D so that every non-identity element of $G - H$ can be represented λ times as differences from elements in D (and no element of $H - 1$ is represented). For background on these, see [5]. In this paper, we will first be concerned with $(p^{j+1}, p, p^{j+1}, p^j)$, where $|H| = p$, $|D| = p^{j+1}$, and $\lambda = p^j$. In Sections 2 and 3, we will provide a construction if the rank of the group is big enough. This construction is relatively easy to set up, and it includes non-abelian examples. Sections 4 and 5 contain a second construction that shows that every abelian p-group meeting the exponent bound will have a RDS if j is odd, and every abelian 2-group meeting the exponent bound has a RDS except the elementary abelian when j is even. Section 6 will consider $(p^{i+j}, p^i, p^{i+j}, p^j)$ RDS, and we

* Supported by University of Richmond Summer Grant 89.013.

provide a construction if the group has a normal elementary abelian subgroup of rank $i+j$. The approach of this paper will follow the patterns found in [2, 3, 6, 7].

A good way to view any difference set is to consider the group ring $\mathbb{Z}[G]$. If we write $D = \sum_{d \in D} d$ and $D^{(-1)} = \sum_{d \in D} d^{-1}$, then by the definition,

$$DD^{(-1)} = p^{j+i} + p^j(G - H).$$

A character χ of G (an abelian group, and always when refering to characters) is a homomorphism from G to the complex numbers: the principal character χ_0 maps every group element to 1. If we extend the character to a homomorphism of the group ring, then we have two possibilities for the character sum $\chi(D)$. If χ is nonprincipal on H, then the sum is $p^{(j+i)/2}$; if χ is a nonprincipal character on G that is principal on H, then the sum is 0. This is a very useful way to check if we have a difference set; the orthogonality relationships on characters imply D is a RDS if and only if every character satisfies this sum condition. The orthogonality relationships on characters apply in several arguments found in this paper, so it is worth mentioning that any elements in the group ring that have the same character sum for every character of the abelian group must be the same.

An application of this is the exponent rule for RDS (the exponent of the group is the size of the largest cyclic subgroup). From character arguments similar to those in [7, Theorem 6], we see that (for $i = 1$) no group of order p^{j+2} with exponent larger than $p^{(j+3)/2}$ has a RDS with the above parameters (j is odd). The j even case is more difficult; the p case is not obvious, but the $p = 2$ case has a bound of $2^{(j+4)/2}$.

In [4], Elliot and Butson found RDS for odd prime and the $p = 2$, j odd case; both constructions are in elementary abelian groups. Jungnickel [5] extended the $p = 2$, j odd case to include any 2-group with exponent less than $2^{(j+3)/2}$ that has a Z_2 piece split off (note: his result also works on non-abelian groups, but what is stated above is his result together with [6] for abelian groups). Jungnickel also finds a RDS with $p = 2$, j even in a special group. Finally, Jungnickel [5] has constructed RDS having parameters $(p^{i+j}, p^i, p^{i+j}, p^j)$ for all i, j. These were obtained by first building a $(p^{i+j}, p^{i+j}, p^{i+j}, 1)$ RDS, then divide out by a subgroup of the forbidden group of order p^j. We will use this dividing out technique to find $(p^{i+j}, p^i, p^{i+j}, p^j)$ for $i+j$ even, $i \leq j$, and G containing a normal elementary abelian group of rank $i+j$.

2. High rank case, j odd, $i = 1$

We will write a subgroup generated by $g, h, \ldots, k$ as $\langle g, h, \ldots, k \rangle$. Suppose

$$H_1 = \langle x_1, x_2, \ldots, x_{(j+3)/2} \rangle \cong \mathbb{Z}_p^{(j+3)/2}$$

is a normal subgroup of G, where G has size p^{j+2} for j odd. Also suppose that $H = \langle x_1 \rangle$ is the forbidden subgroup. Define

$$D_{(k_2, k_3, \ldots, k_{(j+3)/2})} = D_{k_n} = \langle x_1^{k_2} x_2, x_1^{k_3} x_3, \ldots, x_1^{k_{(j+3)/2}} x_{(j+3)/2} \rangle$$

for $0 \leq k_n \leq p-1$, $2 \leq n \leq (j+3)/2$.

Lemma 2.1. (a) *If* $(k_1, \ldots, k_{(j+3)/2}) \neq (k'_1, \ldots, k'_{(j+3)/2})$, *then* $D_{k_n} D_{k'_n}^{(-1)} = p^{(j-1)/2} H_1$.

(b) $D_{k_n} D_{k_n}^{(-1)} = p^{(j+1)/2} D_{k_n}$.

(c) $\sum_{k_n} D_{k_n} = p^{(j+1)/2} + p^{(j-1)/2}(H_1 - H)$.

Proof. (a) Let χ be any nonprincipal character of H_1. $k_n \neq k'_n$ implies χ is nonprincipal on one of the D_{k_n}, so $\chi(D_{k_n} D_{k'_n}^{(-1)}) = 0$. Thus, $D_{k_n} D_{k'_n}^{(-1)}$ must be a multiple of H_1, and a counting argument yields $p^{(j-1)/2}$.

(b) This is obvious because D_{k_n} is a subgroup.

(c) Let χ be any nonprincipal character on H_1. If χ is principal on H, then χ is nonprincipal on every D_{k_n}. Thus, the character sum on both sides of (c) is 0. If χ is nonprincipal on H, then χ is nonprincipal on every D_{k_n} except one. Thus, the character sum on both sides of (c) is $p^{(j+1)/2}$. It is easy to check that the principal character has sum p^{j+1} on both sides, so (c) is true. □

The D_{k_n} are the building blocks of the RDS: we need to assign g_{k_n} to each D_{k_n}, where the g_{k_n} come from different cosets of H_1. If we choose them so that the map $\phi : D_{k_n} \to g_{k_n} D_{k_n} g_{k_n}^{-1}$ is a permutation of the D_{k_n}, then we will have a RDS.

Theorem 2.2. *Let G be a group of order p^{j+2} with a normal elementary abelian subgroup of order $p^{(j+3)/2}$. If we define $D = \bigcup_{k_n} g_{k_n} D_{k_n}$ as above so that ϕ is a permutation of the D_{k_n}, then D is a $(p^{j+1}, p, p^{j+1}, p^j)$ RDS.*

Proof. The following group ring equation uses Lemma 2.1, ϕ a permutation, and the fact that the g_{k_n} form a trivial $(p^{(j+1)/2}, p^{(j+1)/2}, p^{(j+1)/2})$ difference set in the group G/H_1 to prove the theorem.

$$\begin{aligned}
DD^{(-1)} &= \sum_{k_n} g_{k_n} D_{k_n} \sum_{k'_n} D_{k'_n}^{(-1)} g_{k'_n}^{-1} \\
&= p^{(j+1)/2} \sum_{k_n} g_{k_n} D_{k_n} g_{k_n}^{-1} + p^{(j-1)/2} \sum_{k_n \neq k'_n} g_{k_n} g_{k'_n}^{-1} H_1 \\
&= p^{(j+1)/2} \sum_{k_n} D_{k_n} + p^{(j-1)/2}[p^{(j+1)/2}(G - H_1)] \\
&= p^{j+1} + p^j(H_1 - H) + p^j(G - H_1) \\
&= p^{j+1} + p^j(G - H). \qquad \square
\end{aligned}$$

Notice that this theorem applies to abelian groups since ϕ will always be the identity permutation. It also applies to any non-abelian group where H_1 is contained in the center of the group for the same reason. It turns out that if the size of the subgroup

$$C(H_1) = \{g \in G \mid gh_1 = h_1 g \text{ for every } h_1 \in H_1\}$$

is big enough compared to the largest conjugacy class in H_1, then the theorem applies. We can see this by viewing the D_{k_n} as $H_1/\langle h_{k_n} \rangle$ for some $h_{k_n} \in H_1$. Thus,

the conjugates of D_{k_n}, say $\{D_{k_n}, D_{k_n,2}, \ldots, D_{k_n,p^m}\}$ are exactly related to the conjugacy class of h_{k_n}. Take any $g \in G - H_1$, and let $g = g_{k_n}$. If $gD_{k_n}g^{-1} = D_{k_n,2} \neq D_{k_n}$, then let $g_{k_n,2} = gh_2$ for $h_2 \in C(H_1) - H_1$. Do this again if $gh_2D_{k_n,2}h_2^{-1}g^{-1} \neq D_{k_n}$, set $g_{k_n,3} = gh_3$ for some $h_3 \in C(H_1) - H_1$ in a different coset of H_1 than h_2. Repeat this again until the process returns to D_{k_n}. Notice that we need enough distinct cosets of H_1 from elements in $C(H_1)$ to make this work. Then start with a g' in a different coset than anything before it, and repeat the process. This argument is the same one as in [2]. We have shown that the theorem applies to the following situation.

Corollary 2.3. *Let G be a group from Theorem 2.2, and suppose that $H = \langle x_1 \rangle$ is in the center of G, and that $\langle x_2, \ldots, x_{(j+3)/2} \rangle$ is normal in G. If the largest conjugacy class in H_1 has size p^t and $|C(H_1)| \geq p^{(j+3)/2+t}$, then G has a $(p^{j+1}, p, p^{j+1}, p^j)$ RDS.*

The condition on the subgroups is to insure that ϕ is a map from D_{k_n} to D_{k_n}, and the t gives us enough distinct cosets of H_1 in $C(H_1)$.

In the difference set case, it is conjectured that any 2-group with a normal elementary abelian subgroup of the appropriate size will have a difference set. That would appear to be a reasonable conjecture in this case as well, with some added hypotheses about H_1.

3. High rank case, j even, $i = 1$, $p = 2$

In this section, we will always have j even.

Lemma 3.1. *Let G be a group of order 2^{j+2} with a subgroup H of order 2. If there is a character of order 2 that is nonprincipal on H, then G does not have a $(2^{j+1}, 2, 2^{j+1}, 2^j)$ RDS.*

Proof. Since there is a character of order 2 that is nonprincipal on H, that character takes on values of ± 1. If D is a RDS, then the character sum is rational, but $2^{(j+1)/2}$ is not rational, so there is no RDS. □

Notice that this excludes the elementary abelian 2-group since all characters are of order 2. This was proved in [4], but not in the above generality.

The construction from Section 2 will carry over with some slight modifications. Let G be a group of order 2^{j+2}, and let H_1 be a normal elementary abelian subgroup of order $2^{j/2}$. If $H = \langle x_1 \rangle$, then Lemma 3.1 implies that there must be a $g \in G$ so that $g^2 = x_1$. If we choose the g_{k_n} using the same procedure as Section 2, then

$$D = \bigcup_{k_n} g_{k_n}(D_{k_n} \cup gD_{k_n})$$

is a RDS. Let $H_2 = \langle g, x_2, \ldots, x_{(j+2)/2} \rangle$, and suppose that g is in the center of the group.

Lemma 3.2. (a) *If* $k_n \neq k_n'$, *then* $D_{k_n} D_{k_n'}^{(-1)} = 2^{j/2-1} H_1$.
(b) $D_{k_n} D_{k_n}^{(-1)} = 2^{j/2} D_{k_n}$.
(c) $(2 + g + g^3) \sum_{k_n} D_{k_n} = 2^{j/2+1} + 2^{j/2}(H_2 - H)$.

The proof is the same as for Lemma 2.1, except the character for (c) comes from H_2.

Theorem 3.3. *Let G be a group of order 2^{j+2} with a normal elementary abelian subgroup of size $2^{(j+2)/2}$ with H_2 as above. If we define D as above so that ϕ is a permutation of the D_{k_n}, then D is a $(2^{j+1}, 2, 2^{j+1}, 2^j)$ RDS.*

Proof. Again, we will use a group ring argument with Lemma 3.2, ϕ a permutation, and the fact that the g_{k_n} form a $(2^{j/2}, 2^{j/2}, 2^{j/2})$ difference set in G/H_2.

$$\begin{aligned} DD^{(-1)} &= \sum_{k_n} g_{k_n}(1+g) D_{k_n} D_{k_n'}^{(-1)} (1+g^3) g_{k_n'}^{-1} \\ &= 2^{j/2}(2+g+g^3) \sum_{k_n} g_{k_n} D_{k_n} g_{k_n}^{-1} + 2^{j/2-1}(2+g+g^3) \sum_{k_n \neq k_n'} g_{k_n} H_1 g_{k_n}^{-1} \\ &= 2^{j/2}(2+g+g^3) \sum_{k_n} D_{k_n} + 2^{j/2} H_2 \sum_{k_n \neq k_n'} g_{k_n} g_{k_n'}^{-1} \\ &= 2^{j/2}(2^{j/2+1} + 2^{j/2}(H_2 - H)) + 2^{j/2}(2^{j/2}(G - H_2)) = 2^{j+1} + 2^j(G - H). \end{aligned}$$

□

From this, we have a similar corollary.

Corollary 3.4. *Let G be a group from Theorem 3.3, and suppose that g is in the center of the group. Also suppose that $\langle x_2, \ldots, x_{(j+2)/2} \rangle$ is normal in G. If the size of the largest conjugacy class in H_1 is 2^t, and $|C(H_2)| \geq 2^{j/2+2+t}$, then G has a $(2^{j+1}, 2, 2^{j+1}, 2^j)$ RDS.*

4. Construction for j odd, $i = 1$

Theorem 4.1. *Any abelian p-group of order p^{j+2} and exponent less than or equal to $p^{(j+3)/2}$ has a $(p^{j+1}, p, p^{j+1}, p^j)$ RDS.*

Proof. Suppose $G = \mathbb{Z}_{p^{a_1}} \times \mathbb{Z}_{p^{a_2}} \times \cdots \times \mathbb{Z}_{p^{a_k}} = \langle x_1, x_2, \ldots, x_k \rangle$ for

$$a_1 \leq a_2 \leq \cdots \leq a_{k-1} < a_k \leq (j+3)/2 \quad \text{and} \quad H = \langle x_k^{p^{a_k - 1}} \rangle$$

(we will consider the case $a_{k-1} = a_k$ at the end of the proof). Define the subgroup

$$A = \langle x_{k-1}, x_{k-2}, \ldots, x_{r+1}, x_r^{p^{a_r - t}} \rangle$$

so that $\sum_{i=r}^{k-1}(a_i) - t = (j+1)/2$. Next define

$$D_{(i_{k-1},i_{k-2},\ldots,i_r)} = D_{i_n} = \langle x_k^{i_{k-1}p^{a_k-a_{k-1}}} x_{k-1}, \ldots, x_k^{i_{k-n}p^{a_k-a_{k-n}}} x_{k-n}, \ldots, x_k^{i_r p^{a_k-a_r+t}} x_r^{a_r-t} \rangle$$

for $0 \leq i_{k-n} \leq p^{a_{k-n}} - 1$, $n \neq k-r$ and $0 \leq i_r \leq p^{a_r-t} - 1$. This is essentially the analogue of the D_{k_n} on the high rank cases. Let $g_{(0,\, i_{k-2},\ldots,i_r)}$ be in distinct cosets of

$$H_1 = \langle x^{p^{a_k-a_{k-1}-1}} \rangle \times A.$$

A counting argument shows that we have used all the cosets. If we define

$$g_{(i_{k-1},\ldots,i_r)} = g_{i_n} = g_{(0,i_{k-2},\ldots,i_r)} x_k^{i_{k-1}p^{a_k-a_{k-1}-1}},$$

then $D = \bigcup_{i_n} g_{i_n} D_{i_n}$ is the RDS. The first thing that we need to show is that there are no repeated elements in the union. Suppose that there is a repeated element. It must occur with $i_{k-n} = i'_{k-n}$, $n = 2, 3, \ldots, k-r$ since if any of these are not equal, the elements will be in different cosets of H_1. Thus, for $i_{k-1} \neq i'_{k-1}$,

$$(g_{(0,i_{k-2},\ldots,i_r)} x_k^{i_{k-1}p^{a_k-a_{k-1}-1}})(x_k^{i_{k-1}p^{a_k-a_{k-1}}} x_{k-1})^{j_{k-1}} \cdots (x_k^{i_r p^{a_k-a_r+t}} x_r^{a_r-t})^{j_j}$$
$$= (g_{(0,i_{k-2},\ldots,i_r)} x_k^{i'_{k-1}p^{a_k-a_{k-1}-1}})(x_k^{i'_{k-1}p^{a_k-a_{k-1}}} x_{k-1})^{j'_{k-1}} \cdots (x_k^{i_r p^{a_k-a_r+t}} x_r^{a_r-t})^{j'_r}.$$

Since the powers of the generators $x_{k-1}, \ldots, x_r$ must be the same on both sides, $j_{k-n} = j'_{k-n}$ for every n. After all the cancellation, we get

$$x_k^{p^{a_k-a_{k-1}-1} i_{k-1}(pj_{k-1}+1)} = x_k^{p^{a_k-k-1} i'_{k-1}(pj_{k-1}+1)}.$$

Thus, $i_{k-1} \equiv i'_{k-1} \pmod{p^{a_{k-1}+1}}$, which implies that $i_{k-1} = i'_{k-1}$. this shows that there are no repeated elements.

To show that it is a RDS, let χ be any nonprincipal character on G.

Case 1: *χ is nonprincipal on H.*

χ will map

$$x_k^{p^{a_k-a_{k-n}}}$$

to a primitive $p^{a_{k-n}}$ root of unity. Since x_{k-n} is mapped to a $p^{a_{k-n}}$ root of unity, exactly one i_{k-n} has the property that

$$x_k^{i_{k-n}p^{a_k-a_{k-n}}} x_{k-n}$$

is mapped to 1 by χ. This is true for every n, so there is only one D_{i_n} where χ is principal; it is nonprincipal on all the others. Thus, $|\chi(D)| = |D_{i_n}| = p^{(j+1)/2}$.

Case 2: *χ is principal on H but is nonprincipal on $\langle x_k^{p^{a_k-a_{k-1}-1}} \rangle$.*

Suppose that n is the minimum number so that χ maps

$$x_k^{p^{a_k-a_{k-1}+1}}$$

to 1. If χ is principal on $D_{(i_{k-1},\ldots,i_r)}$, then it is principal on $D_{(i_{k-1}+sp^n,\ldots,i_r)}$, $0 \leq s \leq p^{a_{k-1}-n} - 1$. Thus,

$$\sum_{s=0}^{p^{a_{k-1}-n}-1} \chi(g_{(i_{k-1}+sp^n,\ldots,i_r)} D_{(i_{k-1}+sp^n,\ldots,i_r)}) = p^{(j+1)/2} \sum_s \chi(x_k^{p^{a_k-a_{k-1}-1+n}})^s$$
$$= p^{(j+1)/2} \sum_s (\eta)^s = 0.$$

Here, η is a primitive pth root of unity. Thus, $\chi(D) = 0$.

Case 3: *χ is principal on H and is principal on $\langle x_k^{p^{a_k - a_{k-1}}} \rangle$, but is nonprincipal on H_1.*

Then χ is nonprincipal on every D_{i_n}, so $\chi(D) = 0$.

Case 4: *χ is principal on H_1.*

Then it is principal on every D_{i_n} and it induces a nonprincipal character on G/H_1. Thus,

$$\chi(D) = p^{(j+1)/2 + a_{k-1}} \sum_{i_n} \chi(g_{(0, i_{k-2}, \ldots, i_r)}) = 0.$$

This proves the theorem in the case where $a_{k-1} < a_k$. The case where $a_{k-1} = a_k$ simply needs a modification of the g_{i_n}. We set up the A and the D_{i_n} exactly the same. Since $a_{k-1} = a_k$, the subgroup $H_1 = \langle x_k \rangle \times A$ has order at most p^{j+1}: thus, there is a $z \in G - H_1$ so that zH_1 has order p in G/H_1. Define $g_{(i_{k-1}, \ldots, i_r)} = g_{(0, \ldots, i_r)}(x_k z)^{i_{k-1}}$, where the $g_{(0, \ldots, i_r)}$ are chosen from distinct cosets of $\langle z \rangle \times H_1$. To show that there are no repeated elements, we observe that the z forces $i_{k-1} \equiv i'_{k-1} \pmod{p}$ (otherwise, the elements would be in different cosets of H_1). Arguing as before, this implies that $i'_{k-1} \equiv i_{k-1} \pmod{p^{a_k}}$, which implies that $i_{k-1} = i'_{k-1}$. The only case where the character theory arguments is affected is Case 2, here that is χ nonprincipal on $\langle x_k \rangle$ but principal on H. We get the same argument for $n \geq 1$, and our final sum looks like

$$p^{(j+1)/2 + a_k} \sum_{s} \chi(x_k^{p^{n-1}})^s = 0.$$

Thus, the theorem holds for $a_k = a_{k-1}$ as well. □

Thus, the exponent bound is necessary and sufficient for existence of RDS with these parameters, Notice that the subgroup H had to be contained in the biggest exponent piece of the group. I am not sure if this is necessary, but it was required in this proof.

5. Construction for j even, $i = 1$, $p = 2$

Theorem 5.1. *Every abelian group of order 2^{j+2} and exponent less than or equal to $2^{(j+4)/2}$ has a $(2^{j+1}, 2, 2^{j+1}, 2^j)$ RDS except the elementary abelian group.*

Proof. Pick H and A (of order $2^{j/2}$) and the D_{i_n} as in Section 4. We note that $a_k \geq 2$: take the $g_{(0, \ldots, i_r)}$ to be in distinct cosets of $\langle x_k^{a_k - 2} \rangle \times A$, and define

$$D = \bigcup_{i_n} g_{i_n}(D_{i_n} \cup x_k^{a_k - 2} - D_{i_n}).$$

The only difference in the character theory arguments comes when χ is

nonprincipal on H: there, its character sum (in modulus) is

$$|\chi(D)| = |D_{i_n}|\,|(\chi(g_{i_n}))(\chi(1) + \chi(x_k^{a_k-2}))| = 2^{j/2}\,|(1 \pm i)| = 2^{(j+1)/2}. \qquad \square$$

6. Big subgroup construction

The following construction is modeled after [3]. Consider $E = EA(p^{2n})$ as a vector space of dimension 2 over GF(p^n). Let

$$H_1, \ldots, H_r, \qquad r = \frac{p^{2n}-1}{p^n-1} = p^n + 1$$

be the hyperplanes (1-dimensional subspaces) of E. Every non-identity element of E is in precisely one of these hyperplanes, so

$$\sum_{i=1}^{r} H_i = p^n + E.$$

Let G be any group of order p^{3n} that has E as a normal subgroup. If $\{g_1, \ldots, g_{r-1}\}$ are in distinct cosets of E, then define $\phi: H_i \to g_i H_i g_i^{-1}$ for $i \neq r$. In this setup, H_r will be the forbidden subgroup. Define

$$D = \bigcup_{i=1}^{r-1} g_i H_i.$$

Theorem 6.1. *If ϕ is a permutation of the (non-H_r) hyperplanes, then D is a RDS.*

Proof.

$$DD^{(-1)} = \sum_{i,j<r} g_i H_i H_j g_j^{-1} = p^n \sum_{i<r} g_i H_i g_i^{-1} + \sum_{i \neq j} g_i g_j^{-1} E$$

$$= p^n \sum_{i<r} g_i H_i g_i^{-1} + p^n(G - E).$$

The justification for the second sum is that the elements $g_i E$ form a trivial (p^n, p^n, p^n) difference set in G/E. If ϕ is a permutation of the hyperplanes, the first sum is $\sum_{i<r} H_i$. Thus,

$$DD^{(-1)} = p^n(p^n + E - H_r) + p^n(G - E) = p^{2n} + p^n(G - H_r). \qquad \square$$

The only difficulty here is to ensure that ϕ is a permutation. We get the following.

Corollary 6.2. *If E lies in the center of G, then D is a RDS for any choice of the g_i.*

The above corollary is true because ϕ is the identity permutation. Notice that this includes all abelian groups.

Using the same division technique as Jungnickel, we can get the following.

Corollary 6.3. *Any group G of order p^{2n+k} with a central subgroup isomorphic to Z_p^{n+k} will have a $(p^{2n}, p^k, p^{2n}, p^{2n-k})$-RDS.*

To prove this corollary, apply Theorem 2.1 to $G \times \mathbb{Z}_p^{n-k}$ and divide down to G. This corollary is a generalization of Theorem 2.2 in [2].

This leaves several questions:

(1) Is there an exponent bound for groups that have an RDS with these parameters (much like the ordinary difference set case)?

(2) What constructions will work if $i+j$ is odd?

(3) What constructions will work if $i > j$?

Note. Pott has observed that this construction can be generalized to non-p-groups. Consider $E = EA(q^d)$ as a vector space of dimension d over GF(q). There are $(q^d-1)/(q-1) = r$ hyperplanes of E (call them H_i). If G is any group containing E as a normal subgroup of index $r-1$, then $D = \bigcup_{i=1}^{r-1} g_i H_i$ is a

$$\left(q\left(\frac{q^d-1}{q-1}-1\right), q^{d-1}, q^{d-1}\left(\frac{q^d-1}{q-1}-1\right), q^d\left(\frac{q^{d-2}-1}{q-1}\right), q^{d-1}\left(\frac{q^{d-1}-1}{q-1}\right)\right)$$

divisible difference set with H_r as the forbidden subgroup ($d \geq 3$).

References

[1] K.T. Arasu and A. Pott, Group divisible designs with 2^a points, submitted.

[2] J.A. Davis, A result on Dillon's Conjecture in difference sets, submitted.

[3] J.F. Dillon, Variations on a scheme of McFarland for noncyclic difference sets, J. Combin. Theory Ser. A 40 (1973) 1–10.

[4] J.E.H. Elliot and A.T. Butson, Relative difference sets, Illinois J. Math. 10 (1966) 517–531.

[5] D. Jungnickel, On automorphism groups of divisible designs, Canad. J. Math. 34 (1982) 257–297.

[6] R.G. Kraemer, Proof of a conjecture on Hadamard 2-groups, submitted.

[7] R. Turyn, Character sums and difference sets, Pacific J. Math. (1965) 319–346.