# An Exponent Bound for Relative Difference Sets in p-Groups

JAMES A. DAVIS

University of Richmond, VA 23173

**Abstract.** An exponent bound is presented for abelian $(p^{i+j}, p^i, p^{i+j}, p^j)$ relative difference sets: this bound can be met for $i \leq j$.

## RESULT

For background in Relative Difference Sets (RDS), see [3]. The basic group ring equation for a RDS $D$ in a group $G$ with a forbidden subgroup $N$ is

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

If $\chi$ is a character on the abelian group $G$, then we have three possibilities for $\mid \chi(D) \mid = \mid \sum_{d \in D} \chi(d) \mid$: if $\chi$ is the principal character (identically 1) on $G$, then $\chi(D) = k$. If $\chi$ is principal on $N$ but nonprincipal on $G$, then $\mid \chi(D) \mid = \sqrt{k - \lambda \mid N \mid}$. Finally, if $\chi$ is a nonprincipal character on $N$, then $\mid \chi(D) \mid = \sqrt{k}$. The last possibility is the case considered in this paper. We will consider the following parameters: $v = p^{2i+j}$, $\mid N \mid = p^i$, $k = p^{i+j}$, and $\lambda = p^j$. Many examples of RDS with these parameters can be found in [1],[2],and [3]. If $D$ is a RDS with these parameters, and $\chi$ is a character that is nonprincipal on $N$, then $\mid \chi(D) \mid = p^{\frac{i+j}{2}}$.

Consider the $i + j$ even case. This last equation transfers a group ring question into a number theoretic question; namely, when can the algebraic integer $\chi(D)$ have modulus $p^{\frac{i+j}{2}}$. This question was considered in the classical paper by Turyn [4]. He based many of the arguments in that paper on the result due to Kronecker that if $A$ and $B$ are algebraic integers in the number field $Q[\xi]$ ($\xi$ a $n^{th}$ root of unity), and $(A) = (B)$ as ideals, then $A = B\xi^j$ for some $j$ (see p.321 of [4]). This implies that $\chi(D) = p^{\frac{i+j}{2}}\xi^j$ for $\xi$ a $p^n$ root of unity. If we rewrite $\chi(D) = \sum_{i=1}^{n} Y_i \xi^i$, then all of the $Y_i$ will be 0 except one, which will be $p^{\frac{i+j}{2}}$. Since $\chi$ is a homomorphism of $G$, we can bound the $Y_i$ by $0 \leq Y_i \leq \mid Ker(\chi) \mid$. Thus, $\mid Ker(\chi) \mid$ has to be at least $p^{\frac{i+j}{2}}$ in order for the character sum to work. If we define the exponent of the group (written $exp(G)$) is the size of the largest cyclic subgroup, and the order of $\chi$ is the smallest $n$ so that $(\chi(g))^n = 1$ for every $g \in G$, then there is a character $\chi$ of

**ARS COMBINATORIA 34(1992), pp. 318-320**

order $exp(G)$. Elementary character theory tells us that $\mid Ker(\chi) \mid = \frac{|G|}{order(\chi)} = \frac{p^{2i+j}}{exp(G)} \geq p^{\frac{i+j}{2}}$; thus, $exp(G) \leq p^{\frac{i+j}{2}+i}$. This is essentially Turyn's exponent bound argument, and it is the goal of this paper to improve this in the relative difference set case. In order to do this, we need to consider $Ker(\chi) \cap N = Ker(\chi \mid_N)$, the kernel of $\chi$ restricted to $N$.

THEOREM 1. *If $G$ is an abelian group with a $(p^{i+j}, p^i, p^{i+j}, p^j)$ RDS with $i+j$ even, then $exp(G) \leq p^{\frac{i+j}{2}} exp(N)$.*

PROOF: It is easy to see that there is a character of order $exp(G)$ that has order $exp(N)$ on $N$. The discussion before this theorem implies that the size of the kernel must be at least $p^{\frac{i+j}{2}}$. However, in this subset of the kernel, we cannot have two elements $d_1$ and $d_2$ so that $d_1 d_2^{-1} \in N$. Thus, all elements of the subset need to be in different cosets of $Ker(\chi) \cap N = Ker(\chi \mid_N)$, so we must have at least $p^{\frac{i+j}{2}}$ distinct cosets of $Ker(\chi \mid_N)$ in $Ker(\chi)$.

$$\mid \frac{Ker(\chi)}{Ker(\chi \mid_N)} \mid = \frac{\frac{p^{2i+j}}{exp(G)}}{\frac{p^i}{exp(N)}} \geq p^{\frac{i+j}{2}}$$

$$exp(G) \leq p^{\frac{i+j}{2}} exp(N)$$

□

Many abelian examples have an elementary abelian forbidden subgroup. In this special case,

COROLLARY 2. *With the same hypotheses as above, but $N$ is elementary abelian, then $exp(G) \leq p^{\frac{i+j}{2}+1}$. This bound can be met for $i \leq j$.*

An example of a group that has an RDS with those parameters is $Z_{p^{\frac{i+j}{2}+1}} \times Z_p^{\frac{3i+j}{2}-1}$ (see [1]).

The number theory preliminaries are more difficult if $i+j$ is odd, but we indicate here how to modify the arguments. Using the same number theory from [4], we see that if $\chi$ is nonprincipal on $N$, $\mid \chi(D) \mid = p^{\frac{i+j}{2}}$, so $\chi(D) = p^{\frac{i+j-1}{2}} \xi^j (1 + 2\sum_{i=1}^{\frac{p^n-1}{2}} \xi^{i^2})$ for $p$ odd and $2^{\frac{i+j-1}{2}} \xi^j (1 + \sqrt{-1})$ for $p = 2$. (Note: the factors in parentheses have modulus $\sqrt{p}$). Thus, $\mid Ker(\chi) \mid \geq 2p^{\frac{i+j-1}{2}}$ for $p$ odd and $\geq 2^{\frac{i+j-1}{2}}$ for $p = 2$. The $p$ odd case can be improved to $\mid Ker(\chi) \mid \geq p^{\frac{i+j+1}{2}}$. Modifying the same argument as Theorem 1 produces the following.

THEOREM 3. *If $G$ is an abelian group with a $(2^{i+j}, 2^i, 2^{i+j}, 2^j)$ RDS with $i+j$ odd, then $exp(G) \leq 2^{\frac{i+j+1}{2}} exp(N)$. If $N$ is elementary abelian, $exp(G) \leq 2^{\frac{i+j+3}{2}}$. If $p$ is odd, then $exp(G) \leq p^{\frac{i+j-1}{2}} exp(N)$ (or $\leq p^{\frac{i+j+1}{2}}$ if $N$ is elementary abelian).*

The bounds in Corollary 2 and Theorem 3 are neccessary and sufficient for a group to have a RDS when $i = 1$ (see [1]). The sufficiency is an open question for $i > 1$.

## REFERENCES

1. J. Davis, *Construction of Relative Difference Sets in p-Groups*, to appear, Discrete Math.
2. J.E.H. Elliot and A.T. Butson, *Relative Difference Sets*, Ill. J. Math. **10**, 517-531.
3. D. Jungnickel, *On Automorphism Groups of Divisible Designs*, Can. J. Math. **34**, **no.2**, 257-297.
4. R.J.Turyn, *Character Sums on Difference Sets*, Pac. J. Math. **15** **no.1**, 319-346.