6-1991

A note on products of Relative Difference Sets

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

Designs, Codes and Cryptography, 1, 117–119 (1991)

A Note on Products of Relative Difference Sets

JAMES A. DAVIS
Department of Mathematics, University of Richmond, VA 23173 U.S.A.

Communicated by D. Jungnickel
Received June 26, 1990. Revised November 2, 1990.

Abstract. Relative Difference Sets with the parameters $k = n\lambda$ have been constructed many ways (see (Davis, forthcoming; Elliot and Butson 1966; and Jungnickel 1982)). This paper proves a result on building new RDS by taking products of others (much like (Dillon 1985)), and this is applied to several new examples (primarily involving (p^i, p^j, p^i, p^{i-j})).

Key words. relative difference sets, p-groups

1. Introduction

A Relative Difference Set (RDS) in a group G relative to a subgroup N is a subset D so that every element of $G - N$ is represented λ times as differences $d - d'$, $d, d', \in D$, and no element of N has such a representation. This is called a (m, n, k, λ) RDS, where $n = |N|$, $mn = |G|$, and $k = |D|$. These have been constructed for many possible parameters. This paper will focus on the case where $n = k\lambda$; mostly, we will be using the parameters (p^i, p^j, p^i, p^{i-j}). These were first studied by Elliot and Butson (1966). More recently, Jungnickel (1982) has constructed RDS with these parameters for all possibilities of i and j. The (abelian) groups he used were primarily elementary abelian for p odd and $Z_4^i \times Z_2^j$ for $p = 2$ (he also has some nonabelian examples). In (Davis, forthcoming), the author used techniques from difference sets (see (Dillon 1985)) to find many more groups that have a RDS; these examples were mainly when i is even. This paper considers a technique (similar to one found in (Dillon 1985)) to combine these two constructions to get RDS in many groups when i is odd. One other construction different from these parameters will be presented.

It is helpful to consider the group ring ZG when working with RDS. If we write the subset A of G as $A = \Sigma_{a\in A}a$, and $A^{(-1)} = \Sigma_{a\in A}a^{-1}$, then the definition of RDS implies that D is a RDS iff $DD^{(-1)} = k + \lambda(G - N)$. This is the equation that we will use in the next section to check our construction.

2. Main Result

Suppose G has a (m, n, k, λ) RDS D_1 relative to a normal subgroup N with $k = n\lambda$. Also suppose that H is a group of size m' so that $H' = N \times H$ has a (m', n, k', λ') RDS D_2 relative to N with $k' = n\lambda'$. We claim that the product D_1D_2 is an RDS in $G \times H$.

THEOREM 2.1. $G' = G \times H$ has a $(mm', n, kk', \lambda\lambda' n)$ RDS.

Proof. We first need to show that $D = D_1D_2$ has no repeated elements. Suppose that $d_1d_2 = d_1'd_2'$ for $d_1, d_1' \in D_1$ and $d_2, d_2' \in D_2$. Then $d_1^{-1}d_1' = d_2d_2'^{-1}$; $d_1^{-1}d_1' \in G$ and $d_2d_2'^{-1} \in H'$ implies that both are in $G \cap H' = N$. Since these are relative difference sets in their respective groups, this implies that $d_1^{-1}d_1' = d_2d_2'^{-1} = 1$. Thus, there are no repeated elements.

We also need to show that $D = D_1D_2$ satisfies the group ring equation.

$$\begin{aligned} DD^{(-1)} &= D_1D_2D_2^{(-1)}D_1^{(-1)} \\ &= D_1(k' + \lambda'(H' - N))D_1^{(-1)} \\ &= D_1D_1^{(-1)}(k' + \lambda'(H' - N)) \\ &= (k + \lambda(G - N))(k' + \lambda'(H' - N)) \\ &= kk' + k\lambda'(H' - N) + k'\lambda(G - N) + \lambda\lambda'(H' - N)(G - N) \\ &= kk' + n\lambda\lambda'(G - N + H' - N) + \lambda\lambda'(n(G' - H' - G + N)) \\ &= kk' + n\lambda\lambda'(G' - N). \end{aligned}$$

The referee asked if this construction can be extended to the more general case of divisible difference sets; the answer is no. A divisible difference set has the property that every element of the subset N is represented $\lambda_1 \neq 0$ times. If we try the above construction in this setting, the proof that there are no repeated elements will fail (there will be repeated elements in the product D_1D_2), so it will not fit the definition of a divisible difference set.

The theorem does show that we can build RDS from smaller RDS if they share the same forbidden subgroup, which we will use as follows.

3. Applications

1. In (Davis, forthcoming), $(p^{2n}, p, p^{2n}, p^{2n-1})$ RDS are constructed in two ways. First, these are constructed in any group (including nonabelian) which contain a normal elementary abelian subgroup of order p^{n+1}. Second, every abelian group of exponent less than or equal to p^{n+1} is shown to have an RDS with these parameters. If p is odd, we can use the $(p, p, p, 1)$ RDS found in (Jungnickel 1982) (in the group $Z_p \times Z_p$) and Theorem 2.1 to construct $(p^{2n+1}, p, p^{2n+1}, p^{2n})$ RDS in $G \times Z_p$. In the first case, we get both abelian and nonabelian examples in groups with a large normal elementary abelian subgroup. The second case implies that every abelian group that meets the exponent bound that has a Z_p split off will have an RDS.
2. Again in (Davis, forthcoming), we construct $(p^{2n}, p^n, p^{2n}, p^n)$ RDS in any group containing a normal elementary abelian subgroup of order p^{2n}. *For* p odd, combine that with the $(p^n, p^n, p^n, 1)$ RDS found in (Jungnickel 1982) ($H' = Z_p^{2n}$); Theorem 2.1

implies that $G' = G \times Z_p^n$ has a $(p^{3n}, p^n, p^{3n}, p^{2n})$ RDS. This also gives both abelian and nonabelian examples. Generalizing this application, we can put a $(p^{2mn}, p^n, p^{2mn}, p^{(2m-1)n})$ RDS together with a $(p^n, p^n, p^n, 1)$ RDS to get a $(p^{(2m+1)n}, p^n, p^{(2m+1)n}, p^{2mn})$ RDS. This gives examples for any odd power of the prime p.

3. Theorem 2.1 also applies to the $p = 2$ case, but not in exactly the same way. Application (1) is handled in (Davis, forthcoming), so we won't repeat it here. For application (2), take the $(2^n, 2^n, 2^n, 1)$ RDS in the group $G = Z_4^n$ relative to $N = Z_2^n$ (see (Jungnickel 1982)). The construction in (Davis, forthcoming) gives a $(2^{2mn}, 2^n, 2^{2mn}, 2^{(2m-1)n})$ RDS in any group with a normal elementary abelian subgroup of order 2^{2mn}. Thus, if we take the group $H' = N \times H$, where H is a group of order 2^{2mn} with a normal elementary abelian subgroup of order $2^{(2m-1)n}$, then Theorem 2.1 applies. This produces a $(2^{(2m+1)n}, 2^n, 2^{(2m+1)n}, 2^{2mn})$ RDS in $G \times H$. This gives both abelian and nonabelian examples for m any odd power of 2.
4. In (Jungnickel 1982), the author constructs a $(4u^2, 2, 4u^2, 2u^2)$ RDS for $u = 2^s3^r$, $s \geq r - 1$. These RDS are in groups $H' = Z_2 \times H$, where H is the direct product of r groups of order 36 (either Z_6^2 or S_3^2) and $s - r + 1$ groups of order 4 (either Z_2^2 or Z_4). The paper by Turyn (1984) extends this by giving examples of Menon difference sets for any u of the form 2^s3^r (even for $s < r - 1$). We can use Theorem 2.1 to combine this with any group G of order 2^{t+1} that has a $(2^t, 2, 2^t, 2^{t-1})$ RDS (see (Davis, forthcoming)) to yield a $(4u^2(2^t), 2, 4u^2(2^t), 4u^2(2^{t-1}))$ RDS. This includes many new abelian and nonabelian RDS with the parameters $(4u^2, 2, 4u^2, 2u^2)$ for $u = 2^{t/2+s}3^r$ when t is even, as well as $(8u^2, 2, 8u^2, 4u^2)$ for $u = 2^{t-1/2+s}3^r$ when t is odd.

It is worth making a few comments here. First, application (1) and (2) include the only nonelementary abelian examples known to the author other than a few nonabelian examples found in (Jungnickel 1982) for m an odd power of an odd prime. Second, the $p = 2$ case had to reverse the role of G and H' from the odd prime cases because the forbidden subgroup N is not split in the $(2^n, 2^n, 2^n, 1)$ RDS. Finally, this will also work for some semidirect products of G and H, but care must be taken to insure that H' is a subgroup.

References

Davis, J.A. (forthcoming). Construction of relative difference sets in p-groups. *Discrete Mathematics*.

Dillon, J.F. 1985. Variations on a scheme of McFarland for noncyclic difference sets. *J. Combin. Theory Ser. A* 40: 9–21.

Elliot, J.E.H., and Butson, A.T. 1966. Relative difference sets. *Illinois J. Math.* 10: 517–531.

Jungnickel, D. 1982. On automorphism groups of divisible designs. *Can. J. Math.* 34: 257–297.

Turyn, R.J. 1984. A special class of Williamson matrices and difference sets. *J. Combin. Theory Ser. A* 36: 111–115.