6-28-1998

New Semiregular Divisible Difference Sets

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

Recommended Citation

Davis, James A. "New Semiregular Divisible Difference Sets." *Discrete Mathematics* 188, no. 1-3 (June 28, 1998): 99-109. doi: 10.1016/S0012-365X(98)00002-8.

ELSEVIER Discrete Mathematics 188 (1998) 99–109

DISCRETE MATHEMATICS

New semiregular divisible difference sets

James A. Davis*,[1]

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

Received 18 July 1995; revised 16 October 1997; accepted 27 October 1997

Abstract

We modify and generalize the construction by McFarland (1973) in two different ways to construct new semiregular divisible difference sets (DDSs) with $\lambda_1 \neq 0$. The parameters of the DDS fall into a family of parameters found in Jungnickel (1982), where his construction is for divisible designs. The final section uses the idea of a K-matrix to find DDSs with a nonelementary abelian forbidden subgroup. © 1998 Elsevier Science B.V. All rights reserved

1. Introduction

Let G be a group of order mn and N a normal subgroup of G of order n. If D is a k-subset of G then D is a $(m,n,k,\lambda_1,\lambda_2)$ *divisible difference set* (DDS) in G relative to N provided that the differences dd'^{-1} for $d,d' \in D$, $d \neq d'$, contain every nonidentity element of N exactly λ_1 times and every element of $G \backslash N$ exactly λ_2 times. If $k > \lambda_1$ and $k^2 = mn\lambda_2$, then the DDS is called *semi-regular*. Families of semi-regular DDS with $\lambda_1 \neq 0$ are rare, as mentioned in [8]. A family of semi-regular divisible designs with parameters

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

$$\left(a \geqslant \frac{d-1}{2}\right)$$

is constructed in [8]. We will show that there are DDS associated to designs with these same parameters.

The following well-known lemma describes a method used to show that a subset of a group is a DDS (see [11] for a general discussion of this approach). A character of an abelian group is a homomorphism from the group to the Complex numbers.

* Tel.: 1 804 2898094; fax: 1 804 2876444; e-mail: jdavis@richmond.edu.

[1] This work is partially supported by a University of Richmond summer grant.

PII S0012-365X(98)00002-8

Lemma 1.1. *A subset D of a group G is a $(m,n,k,\lambda_1,\lambda_2)$ DDS if and only if* (i) *every character that is nonprincipal (nontrivial) on the subgroup N has character sum* $|\chi(D)| = \sqrt{k-\lambda_1}$, (ii) *every character that is principal on N but nonprincipal on G has character sum* $|\chi(D)| = \sqrt{k-\lambda_1+n(\lambda_1-\lambda_2)}$, (iii) *the principal character χ_0 has sum $\chi_0(D)=k$.*

In McFarland's important paper [10], he shows that the hyperplanes of an elementary abelian p-group can be used to build a difference set. This has been generalized in many directions, including the building of DDS from hyperplanes (see [1,3,4,6] for examples). From the character theoretic point of view, the reason why the hyperplanes work so well in all of these constructions is the fact that each nonprincipal character on the elementary abelian subgroup will be principal on one of the hyperplanes and nonprincipal on all of the others. One easy character theoretic result is that any time a character is nonprincipal on a subgroup, the character sum over that subgroup will be 0. Thus, the character sum for a nonprincipal character will have modulus the size of the hyperplane. Any principal character will have a sum the size of the hyperplane for all of the hyperplanes, so the character sum reduces to the sum of the coset representatives in the quotient group. In Section 2, we use this way of looking at the hyperplane constructions to 'increase the exponent' of the hyperplane: we will start with the group $Z^b_{p^{a+1}}$, and our 'hyperplanes' will be subgroups isomorphic to $Z^{b-1}_{p^{a+1}}$. The difficulty is making sure that these subgroups are pieced together in such a way that the smaller order characters have the correct character sum. In Section 3, we return to the idea of real hyperplanes, and we use the fact that the quotient group of the p-group with the hyperplane will have a RDS with the parameters (p^a, p, p^a, p^{a-1}). The RDS is multiplied to each hyperplane, and the result is a DDS. Two different constructions are given in this section. Finally, Section 4 will give a construction of divisible difference sets which are not semiregular, but which have a forbidden subgroup which is not elementary abelian. The construction will use the same sorts of ideas which are used in the previous two sections, and it has parameters that are found in [3].

2. Construction based on $Z^b_{p^{a+1}}$

Let G be an abelian group of order $p^{a(b-2)+(a+1)b}(p^b-1)/(p-1)$ with a subgroup $H \cong Z^b_{p^{a+1}}$, p a prime. The generators of H are $x_1,x_2,\dots,x_b$ (all of order p^{a+1}), and we will write the coset representatives of H as $g_{i,i_2,i_3,\dots,i_{b-1}}$, where $1 \leqslant i \leqslant (p^b-1)/(p-1)$ and $0 \leqslant i_2,i_3,\dots,i_{b-1} \leqslant p^a-1$. The subgroup N is the group $\langle x_1^{p^a}, x_2^{p^a}, \dots, x_b^{p^a}\rangle \cong Z^b_p$. The next lemma counts the number of subgroups that are isomorphic to $Z^{b-1}_{p^{a+1}}$: we leave the proof to the reader.

Lemma 2.1. *There are $p^{a(b-1)}(p^b-1)/(p-1)$ subgroups isomorphic to $Z^{b-1}_{p^{a+1}}$ in the group $Z^b_{p^{a+1}}$.*

Every character of order p^{a+1} has one of these subgroups as its kernel. We need to arrange cosets of these subgroups so that the other lower-order characters sum to 0. The following lemma describes how to do that.

Lemma 2.2. *Let* $\langle u_1, u_2, \ldots, u_{b-1}\rangle$ *be a subgroup isomorphic to* $Z_{p^{a+1}}^{b-1}$ *in* $Z_{p^{a+1}}^{b}$. *If* w *is an element so that* $w\langle u_1, u_2, \ldots, u_{b-1}\rangle$ *has order* p^{a+1} *in the quotient group* $Z_{p^{a+1}}^{b}/\langle u_1, u_2, \ldots, u_{b-1}\rangle$, *then the cosets* $w^i\langle w^{pi}u_1, u_2, \ldots, u_{b-1}\rangle$, $i = 0, 1, \ldots, p^a - 1$ *are mutually disjoint.*

Proof. Suppose that there is a repeated element, say $w^i(w^{pi}u_1)^{j_1}u_2^{j_2}\cdots u_{b-1}^{j_{b-1}} = w^{i'}(w^{pi'}u_1)^{j_1'}u_2^{j_2'}\cdots u_{b-1}^{j_{b-1}'}$. This implies that $w^{i(1+pj_1)-i'(1+pj_1')}u_1^{j_1-j_1'}u_2^{j_2-j_2'}\cdots u_{b-1}^{j_{b-1}-j_{b-1}'} = 1$. Since w is not in the subgroup and $w^{i(1+pj_1)-i'(1+pj_1')}$ is the inverse of $u_1^{j_1-j_1'}u_2^{j_2-j_2'}\cdots u_{b-1}^{j_{b-1}-j_{b-1}'}$, this forces $u_1^{j_1-j_1'}u_2^{j_2-j_2'}\cdots u_{b-1}^{j_{b-1}-j_{b-1}'} = 1$. Thus, $j_k = j_k'$ for every k. Since $(1 + pj_1)$ is invertible $\bmod\, p^{s+1}$, we get that $i = i'$, so these were really the same element. □

We use this to choose a candidate divisible difference set. Take any subgroup $U = \langle u_1, u_2, \ldots, u_{b-1}\rangle$ of $Z_{p^{a+1}}^{b}$ that is isomorphic to $Z_{p^{a+1}}^{b-1}$, and form the p^a cosets as described in the previous lemma. The union $\bigcup_{i_1=0}^{p^a-1} w^{i_1}\langle w^{pi_1}u_1, u_2, \ldots, u_{b-1}\rangle$ will be placed in the coset whose representative is $g_{1,0,0,\ldots,0}$. We repeat this process on subgroups of the form $\langle w^{pi_1}u_1, w^{pi_2}u_2, \ldots, w^{pi_{b-1}}u_{b-1}\rangle$, yielding a union

$$D_1 = \bigcup_{i_{b-1}=0}^{p^a-1}\ \bigcup_{i_{b-2}=0}^{p^a-1} \cdots \bigcup_{i_2=0}^{p^a-1} g_{1,i_2,\ldots,i_{b-1}} \bigcup_{i_1=0}^{p^a-1} w^{i_1}\langle w^{pi_1}u_1, w^{pi_2}u_2, \ldots, w^{pi_{b-1}}u_{b-1}\rangle.$$

This subset is associated to the hyperplane $\langle u_1^{p^a}, \ldots, u_{b-1}^{p^a}\rangle$. For the ith hyperplane, we repeat this process using a different w and using the coset representatives $g_{i,i_1,\ldots,i_b}$ to form D_i. The set $D = \bigcup_{i=1}^{(p^b-1)/(p-1)} D_i$ is a DDS, as proved in the following theorem.

Theorem 2.1. *The set D defined above is a*

$$\left(p^{2a(b-1)}\frac{p^b-1}{p-1}, p^b, p^{(2a+1)(b-1)}\frac{p^b-1}{p-1}, p^{(2a+1)(b-1)}\frac{p^{b-1}-1}{p-1},\right.$$
$$\left. p^{(2a+1)(b-1)-1}\frac{p^b-1}{p-1}\right)$$

divisible difference set in any abelian group that contains $Z_{p^{a+1}}^{b}$ *as a subgroup (relative to the elementary abelian subgroup of rank b inside* $Z_{p^{a+1}}^{b}$*). Moreover, the design associated to this divisible difference set is semi-regular.*

Proof. To show that this is a divisible difference set, we must show that the character sums work out the way they should. We break the characters into cases depending on their order when restricted to the subgroup $Z_{p^{a+1}}^{b}$. The first case is when the character has order p^{a+1} on this subgroup. In that case, the kernel of the character is one of the subgroups, and the character is nonprincipal on all of the other subgroups. Thus, the character sum is 0 on all of the subgroups except one, and the sum on that subgroup has modulus $p^{(a+1)(b-1)} = \sqrt{p^{(2a+1)(b-1)}\frac{p^b-1}{p-1} - p^{(2a+1)(b-1)}\frac{p^{b-1}-1}{p-1}} = \sqrt{k-\lambda_1}$.

Suppose the character χ has order less than p^{a+1} on $Z^b_{p^{a+1}}$ but is nonprincipal. In this case, χ will be principal on more than just one of the subgroups. If $U = \langle u_1, \dots, u_{b-1}\rangle$ is one of the subgroups that χ is principal on, then χ will also be principal on $\langle w^{(p^{a+1-r})i_1}u_1, \dots, u_{b-1}\rangle$, $i_1 = 0, 1, \dots, p^r - 1$, where p^r is the order of χ. The coset representative in front of this other subgroup is $w^{p^{a-r}i}$. When we sum χ over all of these subgroups, we get $p^{a+1}\sum_{i=0}^{p^r-1}\chi(w^{p^{a-r}i}) = p^{a+1}\sum_{i=0}^{p^r-1}\chi(w^{p^{a-r}})^i$. Since $\chi(w^{p^{a-r}})$ is a primitive pth root of unity, this sum is 0. This will be true for all of the subgroups where χ is principal, so the sum over the whole set is 0.

Finally, if χ is principal on the subgroup $Z^b_{p^{a+1}}$ but nonprincipal on the whole group, then the character sum will be

$$p^{(a+1)(b-1)+a}\sum_{i=1}^{(p^b-1)/(p-1)}\sum_{i_{b-1}=0}^{p^a-1}\sum_{i_{b-2}=0}^{p^a-1}\cdots\sum_{i_1=0}^{p^a-1}\chi(g_{i,i_1,\dots,i_{b-1}}) = 0$$

(since χ is nonprincipal on G/H). Thus, the character sums are correct in all cases, so this is a DDS.

To show that it is semi-regular, we need to show that $k^2 = mn\lambda_2$. This is left to the reader. □

The case when $b=2$ can be found in [4]. We note that the parameters of the DDS are found in [8], but there the construction is only for a design and not a DDS.

This construction can be modified so that $k-\lambda_1$ is not a square. To do this, take the direct product of the group G above with $Z_p = \langle u\rangle$. For each subgroup $U = \langle u_1, \dots, u_{b-1}\rangle$, there is a $w \in G$ that has order p^{a+1} in the quotient group as well as in the original group (like in the construction above): take the subgroup $\langle u, w^{p^a}\rangle \cong Z_p \times Z_p$, and choose any $(p, p, p, 1)$ RDS in this group relative to $\langle w^{p^a}\rangle$. Multiply the RDS by the subgroup U, and do this in each case (the w depends on the subgroup). There will be

$$k = p\left(p^{(2a+1)(b-1)}\frac{p^b-1}{p-1}\right)$$

elements in this new set. Every character of order p^{a+1} will still pick out exactly one of these subgroups, and the sum will be 0 on all the other subgroups. Since this subgroup is multiplied by an RDS, and since the character will be nonprincipal on the subgroup $\langle w^{p^a}\rangle$, the character sum will be $\sqrt{p}p^{(a+1)(b-1)}$. That implies that

$$\lambda_1 = p\left(p^{(2a+1)(b-1)}\frac{p^{b-1}-1}{p-1}\right).$$

When the character is of order less than p^{a+1}, then the character will either be nonprincipal on $\langle u\rangle$, in which case all of the RDS will sum to 0, or the character will be principal on $\langle u\rangle$, in which case the sum will be p times the previous construction. In either case, all of these character sums will be 0, which implies that

$$\lambda_2 = p\left(p^{(2a+1)(b-1)-1}\frac{p^b-1}{p-1}\right).$$

Finally, the size of the group has increased by a factor of p, but we are working with the same forbidden subgroup for the DDS. Thus,

$$m = p\left(p^{2a(b-1)}\frac{p^b-1}{p-1}\right).$$

This is a DDS, and it is semiregular with the property that $k-\lambda_1$ is not a square. This is summarized in the following theorem.

Theorem 2.2. *The set defined above is a*

$$\left(p^{2a(b-1)+1}\frac{p^b-1}{p-1}, p^b, p^{(2a+1)(b-1)+1}\frac{p^b-1}{p-1}, p^{(2a+1)(b-1)+1}\frac{p^{b-1}-1}{p-1},\right.$$
$$\left. p^{(2a+1)(b-1)}\frac{p^b-1}{p-1}\right)$$

divisible difference set in any abelian group that contains $Z^b_{p^{a+1}}$ as a subgroup and a Z_p split off. Moreover, the design associated to this divisible difference set is semiregular.

The strategy used in this previous theorem should work in any difference setting where the difference set is being constructed by using cosets of subgroups of a p-group. The idea is to use a RDS in a quotient group to get a new DDS. That is the strategy that is employed in the next section.

3. Using RDS to construct new DDS

In this section, we will use a combination of RDSs in p-groups together with the hyperplanes of an elementary abelian p-group to construct a semiregular DDS in higher groups. These results are generalizations of ideas found in [5,3].

Let P be any abelian p-group (p a prime) of order p^s with an elementary abelian subgroup of rank r. Further, suppose that P satisfies $\exp(P)\leqslant p^{(s-r)/2+1}$ if $s-r$ is even and $\exp(P)\leqslant p^{(s-r-1)/2+1}$ if $s-r$ is odd. There will be $(p^r-1)/(p-1)$ hyperplanes of the elementary abelian group $Z_p^r\subset P$; label them $H_1,H_2,\dots,H_{(p^r-1)/(p-1)}$. For all of these hyperplanes, the order of the quotient group P/H_i is p^{s-r+1}. There is an element of the quotient of order p whose preimage in P also has order p, call that element p_i. We will use a RDS from this quotient group to build the RDS. The next theorem explains why we need the exponent restrictions on P (see [9,6]).

Theorem 3.1 (Ma and Schmidt [9] and Davis and Jedwab [6]). 1. *Let G be an arbitrary group of order p^{2c+1} with* $\exp(G)\leqslant p^{c+1}$. *Then G contains a* $(p^{2c},p,p^{2c},p^{2c-1})$ RDS *relative to any subgroup N of order p.*

2. *Let G be an arbitrary group of order 2^{2c+2} with* $\exp(G)\leqslant 2^{c+2}$. *Then G contains a* $(2^{2c+1},2,2^{2c+1},2^{2c})$ RDS *relative to any nonsplitting subgroup N of order* 2.

3. *Let G be an arbitrary group of order p^{2c+2} (p an odd prime) and N any subgroup of order p so that G/N is not isomorphic to $Z_{p^{c+1}}\times Z_{p^c}$. Then G contains a* $(p^{2c+1},p,p^{2c+1},p^{2c})$ RDS *relative to N.*

Thus, we have a RDS in any of the quotient groups P/H_i. Take any preimages of those elements in the RDS in P and label them $a_{i1},a_{i2},\dots,a_{ip^{s-r}}$. Finally, let G be any abelian group of order $(p^r-1)/(p-1)$ with elements $g_1,g_2,\dots,g_{(p^r-1)/(p-1)}$, and consider the following subset of $G\times P$.

$$D=\bigcup_{i=1}^{(p^r-1)/(p-1)}(a_{i1}+a_{i2}+\cdots+a_{ip^{s-r}})H_ig_i.$$

Theorem 3.2. *The set D defined above is a*

$$\left(p^{s-r}\frac{p^r-1}{p-1},p^r,p^{s-1}\frac{p^r-1}{p-1},p^{s-1}\frac{p^{r-1}-1}{p-1},p^{s-2}\frac{p^r-1}{p-1}\right),$$

DDS *in $G\times P$ relative to the elementary abelian subgroup of P of rank r (the exponent of P has to meet the bound in the previous theorem, where $c=(s-r)/2$ when $s-r$ is even, similar if it is odd). This* DDS *generates a semiregular divisible design.*

Proof. We need to check the character equations, and there are three different cases to consider. First, if χ is a character that is nonprincipal on the elementary abelian subgroup, then the kernel of χ is a hyperplane H_i. The sum over all of the other H_j will be 0 since χ is nonprincipal on those subgroups. Since χ is principal on H_i, χ will induce a nonprincipal character on the quotient group P/H_i, and the character sum over $(a_{i1}+a_{i2}+\cdots+a_{ip^{s-r}})$ will be $\sqrt{p^{s-r-1}}$. Thus, $|\chi(D)|=p^{r-1}\sqrt{p^{s-r-1}}=\sqrt{k-\lambda_1}$.

The second case is when χ is principal on the elementary abelian subgroup of P but nonprincipal on P. In this case, χ sums to p^{r-1} on all of the hyperplanes, and it induces a nonprincipal character on P/H_i that is principal on the forbidden subgroup generated by p_i. The character sum over the RDS associated to every hyperplane will be 0, so $\chi(D)=0=\sqrt{k-\lambda_1+n(\lambda_1-\lambda_2)}$.

Finally, suppose that χ is a character that is principal on P but nonprincipal on G. In this case,

$$\chi(D)=p^{s-r}p^{r-1}\sum_{i=1}^{(p^r-1)/(p-1)}\chi(g_i)=0=\sqrt{k-\lambda_1+n(\lambda_1-\lambda_2)}.$$

Since the character sums are all what we want them to be, the inversion formula implies that this is a DDS with the parameters listed. In order to show the semiregular condition, we leave it to the reader to verify that $k^2=mn\lambda_2$. □

We note again that these parameters are found in [8] as the parameter of a divisible design, and our new construction shows that there are DDSs with those same parameters.

We can modify this construction to allow higher exponent groups P by a factor of p^2 if we shrink the forbidden subgroup by a factor of p, and this yields another semiregular DDS. Let P be any abelian p-group (p a prime) of order p^{s+1} with an elementary abelian subgroup of rank r. Also suppose that P satisfies $\exp(P) \leqslant p^{(s-r)/2+3}$ if $s-r$ is even and $\exp(P) \leqslant p^{(s-r-1)/2+3}$ if $s-r$ is odd, and we require that there can be at most one factor of exponent $p^{(s-r)/2+3}$ or $p^{(s-r-1)/2+3}$. Let χ be any character of the highest possible order, and consider the kernel when χ is restricted to the elementary abelian subgroup of rank r. This will be a hyperplane H_0, and we will use H_0 as the forbidden subgroup of the construction (in the previous example, we used the whole elementary abelian group as the forbidden subgroup). The other hyperplanes will be labeled H_i, $i = 1,2,\ldots,(p^r-1)/(p-1)-1$. If χ is the character of highest possible order, say p^e, then let P' be the kernel of $\chi^{p^{e-1}}$: the size of P' is p^s. We will attach a RDS to each of these hyperplanes, where the RDS comes from the quotient group P'/H_i. By the restrictions on the exponent, this quotient group will have a $(p^{s-r}, p, p^{s-r}, p^{s-r-1})$ RDS (as long as we avoid the one case of Theorem 3.2), where the forbidden subgroup of this RDS is H_0/H_i (note that this quotient subgroup has order p because the hyperplanes intersect in p^{r-2} elements). Take any preimage of this RDS $a_{i1},\ldots,a_{ip^{s-r}}$. Finally, let G be any abelian group of order $[(p^{r-1}-1)/(p-1)]p^{s+1}$ with coset representatives for P' labeled $g_1, g_2, \ldots, g_{((p^r-1)/(p-1))-1}$ (note that $|G/P'|$ is divisible by p, so some of these coset representatives will be in P), and consider the following subset of G.

$$D = \bigcup_{i=1}^{[(p^r-1)/(p-1)]-1} (a_{i1} + \cdots + a_{ip^{s-r}})H_i g_i.$$

Theorem 3.3. *The set D above is a*

$$\left(p^{s-r+1}\left(\frac{p^r-1}{p-1}-1\right), p^{r-1}, p^{s-1}\left(\frac{p^r-1}{p-1}-1\right), p^{s-1}\left(\frac{p^{r-1}-1}{p-1}-1\right),\right.$$
$$\left. p^{s-1}\left(\frac{p^{r-1}-1}{p-1}\right)\right),$$

RDS *in the group $G \times P$ relative to the subgroup H_0. Moreover, this* DDS *generates a semiregular divisible design.*

Proof. The proof of this theorem is identical to the last theorem with the first case split depending on whether the character is principal on H_0 or not. □

An example of this construction is the (108, 9, 324, 81, 108) semiregular DDS in the group $Z_4 \times Z_{27} \times Z_3 \times Z_3$ relative to $Z_3 \times Z_3$, and that would not work in the first construction in this section because the exponent of P is too big (we can get a DDS with these parameters from Theorem 3.2, but the only in groups whose exponent is less than 9).

This construction very naturally generalizes to using prime powers q instead of just primes p when we are talking about hyperplanes. The reason why it is stated in terms of primes is because the RDSs with the parameters (p^a, p, p^a, p^{a-1}) are almost completely determined as far as existence is concerned, but not nearly as much is known about (q^a, q, q^a, q^{a-1}) and so it is more difficult to state the results.

4. K-matrix construction

In this section, we combine the ideas used in the constructions of the previous 2 sections with the idea of a K-matrix found in [2,9]. The idea of a K-matrix construction is to start with a p-group P, and take the equivalence classes of characters of P where two characters are the same if they have the same kernel. To each kernel, a matrix is attached that has the property that the columns will sum to 0 for any character that is not in the appropriate equivalence class, and the rows will sum to a power of p (in modulus) for exactly one of the rows and 0 for the others for any character that is in the equivalence class associated to that matrix. When viewed in the correct way, the K-matrix is simply a (p^a, p, p^a, p^{a-1}) RDS in the quotient group relative to the unique subgroup of order p contained inside $P/\mathrm{Ker}(\chi)$ (the subgroup is unique because $P/\mathrm{Ker}(\chi)$ is cyclic). Thus, the K-matrix constructions start with subgroups (in the references above, the subgroups can be different sizes) and attaches a RDS to each subgroup of the correct size (which depends on the size of the subgroup). We modify that in this section to get a new construction of a divisible difference set.

Let $P = Z_{p^2}^a \times Z_p^b$, where p is a prime and $a \neq 0$ and b are integers. There are

$$\frac{p^{2a+b} - p^{a+b}}{p^2 - p} = p^{a+b-1}\frac{p^a - 1}{p - 1}$$

kernels associated to the equivalence classes of the characters of order p^2. The quotient group $P/\mathrm{Ker}(\chi)$ is isomorphic to Z_{p^2}, and we will attach a $Z_p = \langle z \rangle$ to P so that the quotient $(P \times Z_p)/\mathrm{Ker}(\chi) \cong Z_{p^2} \times Z_p$. The group $Z_{p^2} \times Z_p$ has a (p^2, p, p^2, p) RDS relative to the subgroup generated by a pth power of an element of order p^2. Attach this RDS to the Kernel as in the previous sections, and do this for every equivalence class. This takes care of the characters of order p^2.

There are $(p^{a+b} - 1)/(p - 1)$ kernels associated to characters of order p. If the kernels are $K_1, K_2, \dots, K_{p^{a+b-1}+\dots+p}, K_{p^{a+b-1}+\dots+p+1}$, then we will use the grouping of cosets

$$\{K_1, zK_2, \dots, z^{p-1}K_p\}, \{K_{p+1}, zK_{p+2}, \dots, z^{p-1}K_{2p}\}, \dots, \{K_{p^{a+b-1}+\dots+p^2+1},$$

$$zK_{p^{a+b-1}+\dots+p^2+2}, \dots, z^{p-1}K_{p^{a+b-1}+\dots+p^2+p}\}, \{K_{p^{a+b-1}+\dots+p+1}\}.$$

The z being used above is the same z as in the last paragraph, where $z \notin P$. Notice that the last grouping only contains one of the kernels, and all of the other groupings contain p.

There are $p^{a+b-1}(p^a-1)/(p-1)$ kernels from the characters of order p^2, and there are $(([(p^{a+b}-1)/(p-1)]-1)/p)+1$ groupings from the characters of order p. We will use an abelian group H of order

$$p^{a+b-1}\frac{p^a-1}{p-1}+\left(\left(\frac{p^{a+b}-1}{p-1}-1\right)\Big/p\right)+1=\frac{p^{2a+b-1}-1}{p-1}+1$$

to separate the group elements, where

$$h=\left\{h_1,h_2,\dots,h_{\frac{p^{2a+b-1}}{p-1}+1}\right\}.$$

If we denote the the kernels associated to the characters of order p^2 by

$$K_{p^{a+b-1}+\dots+p+2},\dots,K_{p^{a+b-1}+\dots+p+1+p^{a+b-1}\frac{p^a-1}{p-1}}$$

and the RDS associated to those kernels by

$$R_{p^{a+b-1}+\dots+p+2},\dots,R_{p^{a+b-1}+\dots+p+1+p^{a+b-1}\frac{p^a-1}{p-1}},$$

then the following is the set we will show is a DDS.

$$D=\left(\bigcup_{i=1}^{p^{a+b-1}\frac{(p^a-1)}{(p-1)}} h_iK_{p^{a+b-1}+\dots+p+1+i}R_{p^{a+b-1}+\dots+p+1+i}\right)$$

$$\cup\left(\bigcup_{j=1}^{((\frac{p^{a+b}-1}{p-1}-1)/p)}\ \bigcup_{k=1}^{p} h_{p^{a+b-1}\frac{p^a-1}{p-1}+j}z^{k-1}K_{p(j-1)+k}\right)$$

$$\cup\, h_{\frac{p^{2a+b-1}-1}{p-1}+1}K_{p^{a+b-1}+\dots+p+1}.$$

Theorem 4.1. *The set D defined above is a*

$$\left(\frac{p^{2a+b-1}-1}{p-1}+1,\ p^{2a+b+1},\ p^{2a+b-1}\frac{p^{2a+b}-1}{p-1},\ p^{2a+b-1}\frac{p^{2a+b-1}-1}{p-1},\right.$$
$$\left.p^{2a+b}\frac{p^{2a+b-2}-1}{p-1}+2p^{2a+b-2}\right),$$

DDS *in the group $H\times P\times\langle z\rangle$ relative to the subgroup $P\times\langle z\rangle$.*

Proof. We need to show that the character theory works out according to Lemma 1.1. We break this into cases. First, suppose that χ is a character that has order p^2 when it is restricted to P. In this case, χ will be nonprincipal on all the K_i except one, so the sum over all of the other kernels will be 0. On the one kernel associated to χ, the sum will be p^{2a+b-2}. There is a RDS $R_{i'}$ associated to $K_{i'}$, and χ is nonprincipal on the forbidden subgroup of this RDS, so the character sum on the RDS has modulus p. Thus, when we multiply the character values together, we get a sum of modulus $p^{2a+b-1}=\sqrt{k-\lambda_1}$. Now suppose that χ has order p on P. In this case, χ will be principal on several of the kernels associated to characters of order p^2; however, χ will be a nonprincipal character on the quotient group associated to the RDS that is principal on the forbidden subgroup (the forbidden subgroup is the power of elements of order p^2). Therefore, the sum over the RDS will be 0, so this will cause the sum to be 0 over all of the kernels associated to characters of order p^2. The character χ will be principal on one of the other kernels, and nonprincipal on all the others, so the character sum is again $p^{2a+b-1}=\sqrt{k-\lambda_1}$. Now suppose that the character χ is principal on P but nonprincipal on $\langle z\rangle$. The part of the DDS that is associated to the characters of order p^2 will again have a sum of 0 because the subgroup $\langle z\rangle$ is part of all of the RDS, so the RDS will again sum to 0. The other kernels are grouped together by z, so they will all sum to 0 with the exception of the one subgroup that is at the end. This subgroup will have a sum of $p^{2a+b-1}=\sqrt{k-\lambda_1}$. Finally, if χ is a character that is principal on $P\times\langle z\rangle$ but nonprincipal on H, then

$$|\chi(D)|=(p-1)p^{2a+b-1}=\sqrt{k-\lambda_1+n(\lambda_1-\lambda_2)}$$

(this is true since all of the cosets of $P\times\langle z\rangle$ have p^{2a+b} elements in them except one which has p^{2a+b-1}). This completes the proof. □

The parameters of the DDS in the previous theorem are found in [3], but there the forbidden subgroup had to be elementary abelian whereas here the forbidden subgroup has exponent p^2. Many of the construction that are based on using hyperplanes can be generalized by using this combination of kernels of subgroups and relative difference sets (K-matrices) to give examples with the same parameters but in groups with lower rank.

References

[1] K.T. Arasu, D. Jungnickel, A. Pott, Divisible difference sets with multiplier −1, J. Algebra 133 (1990) 35–62.

[2] J.A. Davis, Difference sets in abelian 2-groups, J. Combin. Theory (A) 57 (2) (1991) 262–286.

[3] J.A. Davis, Almost difference sets and reversible divisible difference sets, Archiv der Mathematik 59 (1992) 595–602.

[4] J.A. Davis, New constructions of divisible designs, Discrete Math. 120 (1993) 261–268.

[5] J.A. Davis, J. Jedwab, A note on new semi-regular divisible difference sets, Designs, Codes, and Cryptography 3 (1993) 379–381.

[6] J.A. Davis, J. Jedwab, A unifying construction for difference sets, preprint.

[7] J.F. Dillon, Variations on a scheme of McFarland for noncyclic difference sets, J. Combin. Theory (A) 40 (1985) 9–21.

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

[9] S.L. Ma, B. Schmidt, On (p^a, p, p^a, p^{a-1}) relative difference sets, Designs, Codes, and Cryptography 6 (1995) 57–71.

[10] R.L. McFarland, A family of difference sets in non-cyclic groups, J. Combin. Theory (A) 15 (1973) 1–10.

[11] R.J. Turyn, Character sums and difference sets, Pac. J. Math. 15 (1965) 319–346.