

New families of semi-regular relative difference sets

James A. Davis*, Department of Mathematics and Computer Science,
University of Richmond, Virginia 23173, U.S.A.

Jonathan Jedwab and Miranda Mowbray, Hewlett-Packard Laboratories,
Filton Road, Stoke Gifford, Bristol BS12 6QZ, U.K.

June 1996

Abstract

We give two constructions for semi-regular relative difference sets (RDSs) in groups whose order is not a prime power, where the order u of the forbidden subgroup is greater than 2. No such RDSs were previously known. We use examples from the first construction to produce semi-regular RDSs in groups whose order can contain more than two distinct prime factors. For u greater than 2 these are the first such RDSs, and for $u = 2$ we obtain new examples.

*The author thanks Hewlett-Packard for their generous support during his sabbatical year 1995–6

Keywords

Relative difference set

Difference set

Character theory

Combinatorics

1 Introduction

A k -element subset R of a finite multiplicative group G of order mu containing a normal subgroup U of order u is called a (m, u, k, λ) *relative difference set (RDS) in G relative to U* provided that the multiset of “differences” $\{r_1 r_2^{-1} \mid r_1, r_2 \in R, r_1 \neq r_2\}$ contains each element of $G \setminus U$ exactly λ times and contains no element of U . The subgroup U is sometimes called the *forbidden* subgroup. A (m, u, k, λ) RDS in G , relative to some normal subgroup U , is equivalent to a square divisible (m, u, k, λ) -design whose automorphism group G acts regularly on points and blocks [6]. For a recent survey of RDSs see Pott [11]. The central problem is to determine, for each parameter set (m, u, k, λ) , the groups G of order mu and the normal subgroups U of order u for which G contains a RDS relative to U with these parameters. (We have used U and u to represent the normal subgroup and its order, rather than the conventional notation N and n , so as to avoid confusion with the difference set parameter n introduced below.) By a counting argument the parameters (m, u, k, λ) of a RDS are related by $k(k - 1) = u\lambda(m - 1)$. If $k = u\lambda$ then the RDS is called *semi-regular* and the parameters are $(u\lambda, u, u\lambda, \lambda)$.

A k -element subset D of a finite multiplicative group G of order v is called a (v, k, λ, n) -*difference set in G* provided that the multiset $\{d_1 d_2^{-1} \mid d_1, d_2 \in D, d_1 \neq d_2\}$ contains each nonidentity element of G exactly λ times; we write $n = k - \lambda$. A difference set can be considered as a RDS with $u = 1$. For a recent survey of difference sets see Jungnickel [7]; for many new results on RDSs and difference sets see Davis and Jedwab [4].

In this paper we give two constructions for semi-regular RDSs in groups whose order is not a prime power. These are the first such examples which have $u > 2$ [11]. Using these RDSs we construct further new types of semi-regular RDS via known methods. One of our constructions combines the favourable properties of RDSs with those of certain difference sets to produce new RDSs. This approach is similar to that used in [2] for the construction of divisible difference sets.

Relative difference sets (and difference sets) are usually studied in the context of the group ring $Z[G]$ of the group G over the ring of integers Z . The definition of a (m, u, k, λ) RDS R in G relative to U is equivalent to the equation $RR^{(-1)} = k1_G + \lambda(G - U)$ in

$\mathbb{Z}[G]$, where by an abuse of notation we identify the sets $R, R^{(-1)}, G$ with the respective group ring elements $R = \sum_{r \in R} r$, $R^{(-1)} = \sum_{r \in R} r^{-1}$, $G = \sum_{g \in G} g$, and 1_G is the identity of G . If R is a (m, u, k, λ) RDS in G relative to U and W is a normal subgroup of U of order w then the *contraction of R with respect to W* (namely, the image of R under the quotient mapping from G to G/W) is a $(m, u/w, k, \lambda w)$ RDS in G/W relative to U/W [11].

Most computations in this paper involve character theory. In the case where the group G is abelian, a *character* of G is a homomorphism from G to the multiplicative group of complex roots of unity. Under pointwise multiplication the set G^* of characters of G forms a group isomorphic to G . The identity of this group is the *principal character* that maps every element of G to 1. The *character sum* of a character χ over the group ring element C is $\chi(C) = \sum_{c \in C} \chi(c)$. It is well-known that the character sum $\chi(C)$ is 0 for all nonprincipal characters χ of G if and only if C is a multiple of G (regarded as a group ring element). Given a character χ of G and a subgroup H of G , we shall say that χ is *principal on H* (or *nonprincipal on H*) when the restriction of χ to H is principal (or nonprincipal) respectively.

The use of character sums to study difference sets in abelian groups was introduced by Turyn [12] and subsequently extended to RDSs. The fundamental result is:

Lemma 1.1

- (i) *The k -element subset R of an abelian group G of order mu containing a subgroup U of order u is a (m, u, k, λ) RDS in G relative to U if and only if for every nonprincipal character χ of G*

$$|\chi(R)| = \begin{cases} \sqrt{k} & \text{if } \chi \text{ nonprincipal on } U \\ \sqrt{k - u\lambda} & \text{if } \chi \text{ principal on } U. \end{cases}$$

- (ii) *The k -element subset D of an abelian group G of order v is a (v, k, λ, n) -difference set in G if and only if $|\chi(D)| = \sqrt{n}$ for every nonprincipal character χ of G .*

Lemma 1.1 (i) indicates the general strategy adopted here for constructing RDSs, namely to choose a group subset for which all nonprincipal character sums have the correct modulus. In these computations, we will require two useful facts about character

sums. The first fact follows from the character sum property mentioned above. It is that the character sum over a subgroup H is 0 if the character is nonprincipal on H , and the character sum is the order of H if the character is principal on H . The second fact is that for p prime, the kernel of a nonprincipal character of an elementary abelian p -group is an affine hyperplane. (For such a group, the affine hyperplanes are the subgroups of codimension p .) This is because the character is a homomorphism onto the p^{th} roots of unity, so the order of the kernel is the order of the group divided by p . The character is principal on this subgroup of codimension p and is nonprincipal on any other subgroup of codimension p (any other hyperplane). Therefore a nonprincipal character of an elementary abelian p -group has character sum 0 over every hyperplane but one, over which its character sum is the order of the hyperplane. We shall use hyperplanes of elementary abelian p -groups as part of our first construction.

2 Two examples

In this section we introduce the main concepts used in the RDS constructions by means of two examples. Our strategy is to build the RDS a piece at a time and then show that the character sums meet the appropriate conditions.

2.1 Example 1: $(392, 8, 392, 49)$ RDS in $Z_7^2 \times Z_4^3$ relative to Z_2^3

We will build this RDS by starting with the group $Z_7 \times Z_2^3 \cong \langle u \mid u^7 = 1 \rangle \times \langle x, y, z \mid x^2 = y^2 = z^2 = 1 \rangle$. We will view the subgroup $\langle u \rangle$ as being isomorphic to the multiplicative group of $\text{GF}(8)$, generated by a primitive element α satisfying $\alpha^3 = \alpha + 1$, and the subgroup $\langle x, y, z \rangle$ as being isomorphic to the additive group of $\text{GF}(8)$. We define an isomorphism from the additive group of $\text{GF}(8)$ to $\langle x, y, z \rangle$ by $1 \mapsto x, \alpha \mapsto y$, and $\alpha^2 \mapsto z$. The subgroup Z_2^3 has seven subgroups isomorphic to Z_2^2 . These subgroups are hyperplanes of the affine geometry of dimension 3 over $\text{GF}(2)$, and because the characteristic of the field is 2 we can consider these sets as projective hyperplanes simply by deleting the identity element. Thus, if $\{1, x, y, xy\}$ is a typical hyperplane in the affine geometry, then $\{x, y, xy\}$ is the corresponding hyperplane in the projective geometry. In multiplicative

notation, the elements of this projective hyperplane are $\{1, u, u^3\}$ (where 1 is now the identity of the group Z_7 rather than of the group Z_2^3). Viewed in this way, the projective hyperplane is a $(7, 3, 1, 2)$ Singer difference set in Z_7 , and every other projective hyperplane is a translate in Z_7 of this one [8]. Thus the list of projective hyperplanes is $\{1, u, u^3\}$, $\{u, u^2, u^4\}$, $\{u^2, u^3, u^5\}$, $\{u^3, u^4, u^6\}$, $\{u^4, u^5, 1\}$, $\{u^5, u^6, u\}$ and $\{u^6, 1, u^2\}$. Each of these projective hyperplanes corresponds to exactly one affine hyperplane in Z_2^3 , as described. We will use this connection between the affine hyperplanes and the projective hyperplanes later.

We now define the set $S = \{(1, x), (u, y), (u^2, z), (u^3, xy), (u^4, yz), (u^5, xyz), (u^6, xz)\} \subset Z_7 \times Z_2^3$. Note that the first component of a member of S is in $\langle u \rangle$ and the second component is in $\langle x, y, z \rangle$. For each member of S , both components represent the same nonzero element of $\text{GF}(8)$ under the given isomorphism from the additive group of $\text{GF}(8)$ to $\langle x, y, z \rangle$.

Let χ be a character of $Z_7 \times Z_2^3$, so that $\chi(S) = \chi(x) + \chi(u)\chi(y) + \chi(u^2)\chi(z) + \chi(u^3)\chi(xy) + \chi(u^4)\chi(yz) + \chi(u^5)\chi(xyz) + \chi(u^6)\chi(xz)$. Consider the effect of the restriction of χ to Z_2^3 , and suppose firstly that χ is nonprincipal on Z_2^3 . Then half the elements of Z_2^3 will be mapped to $+1$ and the other half will be mapped to -1 , since the character sum on Z_2^3 is 0. The four elements that get mapped to $+1$ form an affine hyperplane, and after deletion of the identity element we find that the three elements of the projective hyperplane are mapped to $+1$ and the other four nonidentity elements of the group are mapped to -1 . Therefore if $\chi(u) = 1$, then there are three terms equal to $+1$ and four terms equal to -1 , so $\chi(S) = -1$. Furthermore if $\chi(u) \neq 1$, then each term of $\chi(S)$ is plus or minus a seventh root of unity. The three terms whose character values are positive seventh roots of unity form a projective hyperplane of Z_7 . The sum of the four terms which are negative seventh roots of unity is equal to the sum of the three terms which are positive seventh roots of unity (because the total sum of all of the positive seventh roots of unity is 0). Therefore the character sum $\chi(S)$ in this case is twice the sum of the three terms which correspond to the projective hyperplane. Since this projective hyperplane is a $(7, 3, 1, 2)$ -difference set, by Lemma 1.1 (ii) we have $|\chi(S)| = 2\sqrt{2}$.

Suppose instead that χ is principal on Z_2^3 . Then if $\chi(u) = 1$ then $\chi(S) = |S| = 7$,

whereas if $\chi(u) \neq 1$ then we have a sum of all the seventh roots of unity, so that $\chi(S) = 0$. This completes the character sum calculations on S .

We next embed S in the larger group $Z_7^2 \times Z_2^3 \cong \langle u, v \mid u^7 = v^7 = 1 \rangle \times \langle x, y, z \mid x^2 = y^2 = z^2 = 1 \rangle$ as follows. The group Z_7^2 contains eight distinct subgroups of order 7 (equivalently, eight affine hyperplanes). Call these hyperplanes K_j for $1 \leq j \leq 8$, and note that each quotient group $(Z_7^2/K_j) \times Z_2^3$ is isomorphic to $Z_7 \times Z_2^3$. Therefore each quotient group contains a subset S_j of the form described above which can be “lifted” to a set $S'_j = \{g \in Z_7^2 \times Z_2^3 \mid gK_j \in S_j\}$, the pre-image of S_j under the quotient mapping from $Z_7^2 \times Z_2^3$ to $(Z_7^2/K_j) \times Z_2^3$. This gives eight subsets S'_j , each containing 49 elements. For example, if $K_1 = \langle v \rangle$, then $S'_1 = x\langle v \rangle \cup uy\langle v \rangle \cup u^2z\langle v \rangle \cup u^3xy\langle v \rangle \cup u^4yz\langle v \rangle \cup u^5xyz\langle v \rangle \cup u^6xz\langle v \rangle$.

Finally, we embed the S'_j in the larger group $Z_7^2 \times Z_4^3 \cong \langle u, v \mid u^7 = v^7 = 1 \rangle \times \langle a, b, c \mid a^4 = b^4 = c^4 = 1 \rangle$ by means of the injective homomorphism ϕ from Z_2^3 to Z_4^3 which maps x to a^2 , y to b^2 , and z to c^2 . For example, $\phi(S'_1) = a^2\langle v \rangle \cup ub^2\langle v \rangle \cup u^2c^2\langle v \rangle \cup u^3a^2b^2\langle v \rangle \cup u^4b^2c^2\langle v \rangle \cup u^5a^2b^2c^2\langle v \rangle \cup u^6a^2c^2\langle v \rangle$. We know [6] that the group $\langle a, b, c \rangle$ contains an $(8, 8, 8, 1)$ RDS relative to $\langle a^2, b^2, c^2 \rangle$, say $\{r_1, r_2, \dots, r_8\} = \{1, a, b, c, ab^3c^2, a^2b^3c^3, a^3b^3c, ab^2c\}$. We claim the set $R = \cup_{j=1}^8 r_j \phi(S'_j)$ is a $(392, 8, 392, 49)$ RDS in $Z_7^2 \times Z_4^3$ relative to Z_2^3 . We shall prove this by combining the character computations for the set S given above with Lemma 1.1 (i) applied to the $(8, 8, 8, 1)$ RDS. Let χ be a character of $Z_7^2 \times Z_4^3$, and suppose firstly that χ is nonprincipal on Z_7^2 . Then χ will be principal on one of the affine hyperplanes of Z_7^2 and nonprincipal on all the other seven hyperplanes. Consequently the character sum over seven of the S'_j will be 0. For the remaining S'_j , χ induces a character ψ on $(Z_7^2/K_j) \times Z_4^3$ which is nonprincipal on $Z_7^2/K_j \cong Z_7$, and the sum of χ over S'_j is seven times the sum of ψ over S_j . If ψ is principal on Z_2^3 (the forbidden subgroup), then the sum over S_j will be 0, yielding a total sum of 0. If ψ is nonprincipal on Z_2^3 , then the sum over S_j has modulus $2\sqrt{2}$, and when we multiply this by 7 we get a character sum of modulus $\sqrt{392} = 14\sqrt{2}$.

Suppose instead that χ is principal on Z_7^2 . In this case χ induces a character ψ on each quotient group $(Z_7^2/K_j) \times Z_4^3$, which is principal on Z_7^2/K_j . For each j , the sum of χ over S'_j is again seven times the sum of ψ over S_j . If ψ is nonprincipal on Z_2^3 then the sum over S_j in the quotient group is -1 in each case, so we get a sum of -7 for each S'_j . We

now take the sum over the r_j , which has modulus $2\sqrt{2}$ because the r_j form a $(8, 8, 8, 1)$ RDS. The total sum therefore has modulus $14\sqrt{2}$, as desired. If ψ is principal on Z_2^3 then the sum of χ over S'_j is 49 in each case, and since the r_j form a RDS we obtain a total sum of 0. Therefore by Lemma 1.1 (i) we have established that this example is a RDS. Note that the construction uses affine hyperplanes in two different affine spaces as well as projective hyperplanes.

A useful modification of the construction involves taking the contraction of the set S by a subgroup, in other words the image of S under the mapping from the group to the quotient group. For example, consider contraction by the subgroup $\langle y, z \rangle$. The contraction of S still has seven elements but is contained in a group isomorphic to $Z_7 \times Z_2$. The contraction of S has the same character sums as S , based on whether the character is principal or nonprincipal on the Sylow 7-subgroup and the Sylow 2-subgroup. The eight affine hyperplanes of Z_7^2 provide eight quotient groups of $Z_7^2 \times Z_2$ isomorphic to $Z_7 \times Z_2$ from which we can define sets S'_j based on the contracted sets S_j . We can then use any $(8, 2, 8, 4)$ RDS to provide the coefficients of the S'_j , where the forbidden subgroup (isomorphic to Z_2) corresponds to the Sylow 2-subgroup of the group on which the contracted set S is defined. Since any group of order 16 and exponent at most 8 contains a $(8, 2, 8, 4)$ RDS relative to any subgroup of order 2, provided the forbidden subgroup is contained in a subgroup isomorphic to Z_4 [9], we can therefore construct a $(392, 2, 392, 196)$ RDS in the group $Z_7^2 \times Z_8 \times Z_2$ relative to a subgroup isomorphic to Z_2 , for example. Note that this RDS could not be constructed directly as a contraction of a $(392, 8, 392, 49)$ RDS in $Z_7^2 \times Z_4^3$ relative to Z_2^3 , which demonstrates the advantage of contracting the set S as described prior to attaching the RDS $\{r_j\}$.

2.2 Example 2: $(48, 3, 48, 16)$ RDS in $Z_4^2 \times Z_3^2$ relative to Z_3

We begin this example by listing the six cyclic subgroups of $\langle x, y \mid x^4 = y^4 = 1 \rangle \cong Z_4^2$ of order 4. These subgroups can be written as $\langle x \rangle$, $\langle xy^2 \rangle$, $\langle y \rangle$, $\langle x^2y \rangle$, $\langle xy \rangle$, and $\langle x^3y \rangle$. Any character of Z_4^2 of order 4 is principal on one of these subgroups and nonprincipal on the rest. (These six subgroups are the kernels of the characters of order 4, and are analogous to affine hyperplanes.) Furthermore, a character of order 2 on $\langle x, y \rangle$ is principal

on two of the subgroups and nonprincipal on the other four. We therefore form these subgroups into three pairs depending on their behaviour on the characters of order 2, to give the pairs: $\langle x \rangle, \langle xy^2 \rangle$; $\langle y \rangle, \langle x^2y \rangle$; and $\langle xy \rangle, \langle x^3y \rangle$. We will also use a $(3, 3, 3, 1)$ RDS in $\langle g, h \rangle \cong Z_3^2$ relative to $\langle h \rangle \cong Z_3$, for example $\{h^2, g, g^2\}$.

We now demonstrate by means of Lemma 1.1 (i) that the set represented by the group ring element $\langle x \rangle(h + h^2y^2) + \langle xy^2 \rangle(h^2y + y^3) + \langle y \rangle(g + gh^2x^2) + \langle x^2y \rangle(ghx + gx^3) + \langle xy \rangle(g^2 + g^2h^2x^2) + \langle x^3y \rangle(g^2hx + g^2x^3)$ is a $(48, 3, 48, 16)$ RDS in $\langle x, y, g, h \rangle \cong Z_4^2 \times Z_3^2$ relative to $\langle h \rangle \cong Z_3$. Suppose firstly that χ is a character of order 4 on $\langle x, y \rangle$. In this case, the character sum is 0 over five of the six terms above, and 4 times the character sum of the coefficient of the other term. If χ is principal on $\langle h \rangle$ then in each case the character sum of the coefficient is a multiple of $(1 - 1) = 0$, giving a total character sum of 0. If χ is nonprincipal on $\langle h \rangle$ then in each case the character sum of the coefficient is the difference of two distinct third roots of unity, giving a total character sum of modulus $4\sqrt{3}$.

Next suppose that χ has order 2 on $\langle x, y \rangle$. Then the kernel of χ contains one pair of subgroups, and χ sums to 0 over the other four subgroups. For the subgroup pair that does not get eliminated, the character sum is 4 times the character sum of the coefficients. If χ is principal on $\langle h \rangle$ then in each case the character sum of the coefficient is a multiple of $(2 - 2) = 0$, giving a total character sum of 0. If χ is nonprincipal on $\langle h \rangle$ then in each case the character sum of the coefficient is again the difference of two distinct third roots of unity, giving a total character sum of modulus $4\sqrt{3}$.

Finally, suppose that χ is principal on $\langle x, y \rangle$. If χ is nonprincipal on $\langle h \rangle$ then the character sum is equal to four times the sum over the elements $\{h^2, g, g^2\}$ (using the fact that $\chi(h)$ is a primitive third root of unity to remove multiples of $\{1, h, h^2\}$). Since $\{h^2, g, g^2\}$ a $(3, 3, 3, 1)$ RDS in $\langle g, h \rangle$ relative to $\langle h \rangle$ and χ is nonprincipal on $\langle h \rangle$, by Lemma 1.1 (i) the total character sum has modulus $4\sqrt{3}$. If χ is principal on $\langle h \rangle$ and nonprincipal on $\langle g \rangle$ then the character sum is 16 times the character sum over the elements $\{1, g, g^2\}$, which is 0. We have therefore established that this example is a RDS.

3 Construction 1: u a power of 2

This construction generalises Example 1. Let d be a positive integer and let α generate the cyclic multiplicative group of the finite field $\text{GF}(2^{d+1})$. Considering $\text{GF}(2^{d+1})$ as a vector space of dimension $d + 1$ over $\text{GF}(2)$, there are $2^{d+1} - 1$ subspaces of dimension 1. These can be written $\langle 1 \rangle, \langle \alpha \rangle, \langle \alpha^2 \rangle, \dots, \langle \alpha^{2^{d+1}-2} \rangle$. The affine hyperplanes of this vector space, namely the subspaces of dimension d , can be written $\langle 1, \alpha, \alpha^2, \dots, \alpha^{d-1} \rangle, \langle \alpha, \alpha^2, \alpha^3, \dots, \alpha^d \rangle, \dots, \langle \alpha^{2^{d+1}-2}, 1, \alpha, \dots, \alpha^{d-2} \rangle$. We can view these as projective hyperplanes by deleting the identity element from each set. Each projective hyperplane is a translate of a $(2^{d+1} - 1, 2^d - 1, 2^{d-1} - 1, 2^{d-1})$ Singer difference set in $Z_{2^{d+1}-1}$ (see Lander [8] for further discussion of the projective geometry $\text{PG}(d, 2)$ and its regular cyclic automorphism group).

Let S be the subset $\{(\alpha^i, \alpha^i) \mid i = 0, 1, \dots, 2^{d+1} - 2\}$ of $Z_{2^{d+1}-1} \times Z_2^{d+1}$, where we regard the first component of a member of S as an element of the cyclic multiplicative group of $\text{GF}(2^{d+1})$ and the second component as an element of the additive group of $\text{GF}(2^{d+1})$. We get the following character sums over S .

Lemma 3.1 *Let S be the subset of $G = Z_{2^{d+1}-1} \times Z_2^{d+1}$ defined above and let χ be a character of G . Then*

$$\chi(S) = \begin{cases} -1 & \text{if } \chi \text{ is principal on } Z_{2^{d+1}-1} \text{ and nonprincipal on } Z_2^{d+1} \\ 0 & \text{if } \chi \text{ is nonprincipal on } Z_{2^{d+1}-1} \text{ and principal on } Z_2^{d+1} \\ 2^{d+1} - 1 & \text{if } \chi \text{ is principal on } G \end{cases}$$

and $|\chi(S)| = \sqrt{2^{d+1}}$ if χ is nonprincipal on $Z_{2^{d+1}-1}$ and nonprincipal on Z_2^{d+1} .

Proof: The value of χ applied to an ordered pair belonging to S is the product of the character values of the components. Consider the restriction of χ to the group Z_2^{d+1} , which maps each element of Z_2^{d+1} either to $+1$ or -1 . Suppose firstly χ is nonprincipal on Z_2^{d+1} . The kernel of the restriction of χ to this group is an affine hyperplane H . The character sum over S therefore contains a $+1$ contribution from each element of the projective hyperplane $H \setminus \{0\}$ and a -1 contribution from each element of $Z_{2^{d+1}-1} \setminus$

$(H \setminus \{0\})$. Since the projective hyperplane $H \setminus \{0\}$ can be viewed as a translate gD of a $(2^{d+1} - 1, 2^d - 1, 2^{d-1} - 1, 2^{d-1})$ -difference set D in $Z_{2^{d+1}-1}$, we have

$$\chi(S) = (+1)\chi(gD) + (-1)\chi(Z_{2^{d+1}-1} \setminus gD).$$

If χ is principal on $Z_{2^{d+1}-1}$ then $\chi(gD) = 2^d - 1$ and $\chi(Z_{2^{d+1}-1} \setminus gD) = 2^d$, so that $\chi(S) = -1$. If χ is nonprincipal on $Z_{2^{d+1}-1}$ then $\chi(S) = (+1)\chi(gD) + (-1)(-\chi(gD)) = 2\chi(gD)$. Since D is a difference set, Lemma 1.1 (ii) then implies that $|\chi(S)| = 2\sqrt{2^{d-1}} = \sqrt{2^{d+1}}$.

Suppose instead that χ is principal on Z_2^{d+1} . If χ is principal on $Z_{2^{d+1}-1}$ then $\chi(S) = |S| = 2^{d+1} - 1$, whereas if χ is nonprincipal on $Z_{2^{d+1}-1}$ then $\chi(S) = \sum_{i=0}^{2^{d+1}-2} \chi(\alpha^i) = \chi(\langle \alpha \rangle) = 0$ (since $\langle \alpha \rangle \cong Z_{2^{d+1}-1}$). \square

The set S satisfies the group ring equation $SS^{(-1)} = 2^{d+1}1_G + G - Z_{2^{d+1}-1} - Z_2^{d+1}$ in $Z[G]$, where $G = Z_{2^{d+1}-1} \times Z_2^{d+1}$, and so is an example of a *direct product difference set* as introduced by Ganley [5]. Pott [10] used direct product difference sets to show that the order of a projective plane must be a prime power if the plane has a certain type of quasiregular collineation group and the order is not a square.

Let J be any subgroup of G of order 2^i . A character ψ of G/J defines a character χ of G via $\chi(g) = \psi(gJ)$. If \bar{S} is the image of S in the quotient group G/J then $\chi(S) = \psi(\bar{S})$. The next result then follows directly from Lemma 3.1.

Lemma 3.2 *Let \bar{S} be the image of the subset S under any quotient mapping from $Z_{2^{d+1}-1} \times Z_2^{d+1}$ to $G \cong Z_{2^{d+1}-1} \times Z_2^{d+1-i}$, where $0 \leq i \leq d$. Let ψ be a character of G . Then*

$$\psi(\bar{S}) = \begin{cases} -1 & \text{if } \psi \text{ is principal on } Z_{2^{d+1}-1} \text{ and nonprincipal on } Z_2^{d+1-i} \\ 0 & \text{if } \psi \text{ is nonprincipal on } Z_{2^{d+1}-1} \text{ and principal on } Z_2^{d+1-i} \\ 2^{d+1} - 1 & \text{if } \psi \text{ is principal on } G \end{cases}$$

and $|\psi(\bar{S})| = \sqrt{2^{d+1}}$ if ψ is nonprincipal on $Z_{2^{d+1}-1}$ and nonprincipal on Z_2^{d+1-i} .

Suppose now that $2^{d+1} - 1$ is prime (and therefore a Mersenne prime). This implies that $d + 1$ is prime, so we will use the notation p for the prime $d + 1$. Since $2^p - 1$ is prime, $Z_{2^p-1}^2$ contains 2^p subgroups of order $2^p - 1$ (these are the affine hyperplanes of

$Z_{2^p-1}^2$, and they correspond to the kernels of the nonprincipal characters of $Z_{2^p-1}^2$); call these subgroups K_1, \dots, K_{2^p} . Let U be isomorphic to Z_2^{p-i} , so that the quotient group $(Z_{2^p-1}^2/K_j) \times U$ is isomorphic to $Z_{2^p-1} \times Z_2^{p-i}$. We define the set \overline{S}_j to be the subset of $(Z_{2^p-1}^2/K_j) \times U$ which corresponds to \overline{S} in the group $Z_{2^p-1} \times Z_2^{p-i}$ (as specified in Lemma 3.2), for $j = 1, \dots, 2^p$. We then define the set $S'_j = \{g \in Z_{2^p-1}^2 \times U \mid gK_j \in \overline{S}_j\}$. Note that $|S'_j| = |K_j||S| = (2^p - 1)^2$.

We wish to combine cosets of the S'_j in the group $Z_{2^p-1}^2 \times A$, where A is any abelian group of order 2^{2p-i} containing a $(2^p, 2^{p-i}, 2^p, 2^i)$ RDS relative to an elementary abelian subgroup U . There are many constructions of such RDSs; see Pott [11] and Davis and Jedwab [4]. Write the RDS in A relative to U as $\{r_1, r_2, \dots, r_{2^p}\}$. Since, by the definition of RDS, no two distinct elements r_j belong to the same coset of U , the set $\cup_{j=1}^{2^p} r_j S'_j$ contains $2^p(2^p - 1)^2$ distinct elements. We now show that this set is a RDS in $Z_{2^p-1}^2 \times A$ relative to U .

Theorem 3.3 *Let $2^p - 1$ be prime and let i satisfy $0 \leq i \leq p - 1$. Suppose that the abelian group A contains a $(2^p, 2^{p-i}, 2^p, 2^i)$ semi-regular RDS $\{r_j\}$ relative to an elementary abelian subgroup U . Let S'_j be as defined above, for $j = 1, 2, \dots, 2^p$. Then the set $\cup_{j=1}^{2^p} r_j S'_j$ is a $(2^p(2^p - 1)^2, 2^{p-i}, 2^p(2^p - 1)^2, 2^i(2^p - 1)^2)$ semi-regular RDS in $Z_{2^p-1}^2 \times A$ relative to U .*

Proof:

Let χ be a character on $Z_{2^p-1}^2 \times A$ and set $E = \cup_{j=1}^{2^p} r_j S'_j$. We break the proof up into four cases.

Case 1: Suppose that χ is nonprincipal on $Z_{2^p-1}^2$ and is nonprincipal on U . Then χ is principal on one of the K_j and nonprincipal on all the others, so χ sums to 0 on all of the S'_j except one, say S'_k . This implies that $|\chi(E)| = |\chi(r_k S'_k)| = |\chi(S'_k)| = (2^p - 1)|\psi(\overline{S}_k)|$, where ψ is the character induced by χ on $(Z_{2^p-1}^2/K_k) \times U$. Since ψ is nonprincipal on $Z_{2^p-1}^2/K_k \cong Z_{2^p-1}$ and is nonprincipal on U , we have that $|\psi(\overline{S}_k)| = \sqrt{2^p}$ from Lemma 3.2. Thus, $|\chi(E)| = (2^p - 1)\sqrt{2^p}$.

Case 2: Suppose that χ is nonprincipal on $Z_{2^p-1}^2$ and is principal on U . As in Case 1,

$|\chi(E)| = (2^p - 1)|\psi(\overline{S}_k)|$ for some k , where ψ is again nonprincipal on $Z_{2^{p-1}}^2/K_k \cong Z_{2^{p-1}}$ but is now principal on U . By Lemma 3.2, $\psi(\overline{S}_k) = 0$, so $\chi(E) = 0$.

Case 3: Suppose that χ is principal on $Z_{2^{p-1}}^2$ and is nonprincipal on U . Then, for each j , $\chi(S'_j) = (2^p - 1)\psi(\overline{S}_j)$, where ψ is the character induced by χ on $(Z_{2^{p-1}}^2/K_j) \times U$. Since ψ is principal on $Z_{2^{p-1}}^2/K_j \cong Z_{2^{p-1}}$ and nonprincipal on U , by Lemma 3.2 $\psi(\overline{S}_j) = -1$. Therefore $\chi(E) = -(2^p - 1)\sum_{j=1}^{2^p} \chi(r_j)$. Since the $\{r_j\}$ form a RDS and χ is nonprincipal on U , by Lemma 1.1 (i) we obtain $|\chi(E)| = (2^p - 1)\sqrt{2^p}$.

Case 4: Suppose that χ is principal on $Z_{2^{p-1}}^2$ and is principal on U but is nonprincipal on A . As in Case 3, for each j we have $\chi(S'_j) = (2^p - 1)\psi(\overline{S}_j)$, where ψ is again principal on $Z_{2^{p-1}}^2/K_j \cong Z_{2^{p-1}}$ but is now principal on U . Then Lemma 3.2 gives $\chi(S'_j) = (2^p - 1)^2$ and Lemma 1.1 (i) gives $\chi(E) = (2^p - 1)^2 \sum_{j=1}^{2^p} \chi(r_j) = 0$.

The result follows from Lemma 1.1 (i). \square

As well as making use of the affine hyperplanes of $Z_{2^{p-1}}^2$, the construction of Theorem 3.3 combines two objects with simple character properties, namely a $(2^p - 1, 2^{p-1} - 1, 2^{p-2} - 1, 2^{p-2})$ Singer difference set (used to construct the set S in Lemma 3.1) and a $(2^p, 2^{p-i}, 2^p, 2^i)$ RDS. A similar construction was given by Davis and Jedwab [2], in which the favourable character properties of two difference sets were combined to form divisible difference sets.

Note that the RDSs of Theorem 3.3 occur in groups whose order is not a prime power, and that the forbidden subgroup U has order 2^{p-i} . By the proof of Lemma 7.4 of [4], when p is odd it is necessary that the subgroup U be contained in a subgroup of A isomorphic to Z_4^{p-i} . There are many suitable groups A and U for use in Theorem 3.3. In particular, there exists a $(2^p, 2^p, 2^p, 1)$ semi-regular RDS in Z_4^p for all p [6], which under contraction itself yields a $(2^p, 2^{p-i}, 2^p, 2^i)$ semi-regular RDS in $Z_4^{p-i} \times Z_2^i$ relative to the subgroup Z_2^{p-i} of Z_4^{p-i} , where $0 \leq i \leq p - 1$:

Corollary 3.4 *Let $2^p - 1$ be prime. For each i satisfying $0 \leq i \leq p - 1$, there exists a $(2^p(2^p - 1)^2, 2^{p-i}, 2^p(2^p - 1)^2, 2^i(2^p - 1)^2)$ semi-regular RDS in $Z_{2^{p-1}}^2 \times Z_4^{p-i} \times Z_2^i$ relative to the subgroup Z_2^{p-i} of Z_4^{p-i} .*

In the uncontracted case $i = 0$, Corollary 3.4 provides the following small examples: a $(4 \cdot 3^2, 4, 4 \cdot 3^2, 3^2)$ RDS in $Z_3^2 \times Z_4^2$ relative to Z_2^2 , a $(8 \cdot 7^2, 8, 8 \cdot 7^2, 7^2)$ RDS in $Z_7^2 \times Z_4^3$ relative to Z_2^3 , a $(32 \cdot 31^2, 32, 32 \cdot 31^2, 31^2)$ RDS in $Z_{31}^2 \times Z_4^5$ relative to Z_2^5 , and a $(128 \cdot 127^2, 128, 128 \cdot 127^2, 127^2)$ RDS in $Z_{127}^2 \times Z_4^7$ relative to Z_2^7 .

In the contracted case $i > 0$, Corollary 3.4 provides further examples such as a $(8 \cdot 7^2, 2, 8 \cdot 7^2, 4 \cdot 7^2)$ RDS in $Z_7^2 \times Z_4 \times Z_2^2$ relative to the subgroup Z_2 of Z_4 (using $p = 3, i = 2$). However by direct reference to Theorem 3.3, and using examples for the RDS $\{r_j\}$ found in [4], we obtain RDSs which do not arise from Corollary 3.4, including: a $(8 \cdot 7^2, 2, 8 \cdot 7^2, 4 \cdot 7^2)$ RDS in $Z_7^2 \times Z_8 \times Z_2$ relative to Z_2 (using $p = 3, i = 2$), a $(32 \cdot 31^2, 2, 32 \cdot 31^2, 16 \cdot 31^2)$ RDS in $Z_{31}^2 \times Z_{16} \times Z_4$ relative to Z_2 (using $p = 5, i = 4$), and a $(128 \cdot 127^2, 4, 128 \cdot 127^2, 32 \cdot 127^2)$ RDS in $Z_{127}^2 \times Z_{16} \times Z_4^2 \times Z_2$ relative to Z_2^2 (using $p = 7, i = 5$). (In each of these examples, the forbidden subgroup $U \cong Z_2^{p-i}$ must be contained within a subgroup of A isomorphic to Z_4^{p-i} .)

We can extend Theorem 3.3 by using the recursive construction for RDSs found in [4]. Following [4], define a *building block in an abelian group G with modulus m* to be a subset of G such that all nonprincipal character sums over the subset have modulus either 0 or m . A (a, m, t) *building set (BS) on an abelian group G relative to a subgroup U* is defined as a collection of t building blocks in G with modulus m , each containing a elements, such that for every nonprincipal character χ of G

- (i) exactly one building block has nonzero character sum if χ is nonprincipal on U and
- (ii) no building block has nonzero character sum if χ is principal on U .

For $a > 1$, a $(a, \sqrt{a}, 1)$ BS on a group G relative to a subgroup U of order u is equivalent to a $(a, u, a, a/u)$ semi-regular RDS in G relative to U . If the group G has a subgroup isomorphic to $Z_2^{2^r}$, then we can associate that subgroup with the additive structure of $\text{GF}(2^r)^2$. Once this association is established, we can make the additional link between the affine hyperplanes of $\text{GF}(2^r)^2$ and subgroups of $Z_2^{2^r}$ of order 2^r . One of the hyperplanes (say H_0) will be the forbidden subgroup, and we consider the quotient groups G/H_i , where H_i are the other hyperplanes. If there exists a (a, \sqrt{at}, t) BS on each quotient group G/H_i relative to $Z_2^{2^r}/H_i$ then there exists a $(2^r a, 2^r \sqrt{at}, 2^r t)$ BS on G relative to

H_0 (see [4] for full details). Thus, given an example of a BS relative to an elementary abelian subgroup, we can recursively construct a family of BSs in larger groups, and these new BSs can be used to construct RDSs using the following result [4]:

Theorem 3.5 *Suppose there exists a (a, \sqrt{at}, t) BS on an abelian group G relative to a subgroup U of order u , where $at > 1$. Then there exists a $(at, u, at, at/u)$ semi-regular RDS in G' relative to U , where G' is any abelian group containing G as a subgroup of index t .*

To illustrate the use of the recursive construction, we shall restrict attention to the RDSs of Corollary 3.4. More general results can be obtained from the larger set of RDSs available directly from Theorem 3.3. Now Corollary 7.9 of [4] demonstrates the recursive construction of BSs, starting from a $(2^{r+i}, 2^r, 2^{r+i}, 2^i)$ RDS in $Z_4^r \times Z_2^i$ relative to the subgroup Z_2^r of Z_4^r . A similar method can be used to construct the BSs of the following corollary, starting from the $(2^{r+i}(2^{r+i} - 1)^2, 2^r, 2^{r+i}(2^{r+i} - 1)^2, 2^i(2^{r+i} - 1)^2)$ semi-regular RDS in $Z_{2^{r+i-1}}^2 \times Z_4^r \times Z_2^i$, relative to the subgroup Z_2^r of Z_4^r , given by Corollary 3.4 (setting $p = r + i$). As indicated by Theorem 7.11 of [4], the recursion will affect only the Sylow 2-subgroup of the group to give an analogous result to Corollary 7.9 of [4]:

Corollary 3.6 *Let $2^{r+i} - 1$ be prime, where $r \geq 1$ and $i \geq 0$ are integer. For each d and c satisfying $2 \leq c \leq d$, there exists a*

$$(2^{(d+c-2)r+i}(2^{r+i} - 1)^2, 2^{((2d-1)r+i)/2}(2^{r+i} - 1), 2^{(d-c+1)r})$$

BS on $Z_{2^{r+i-1}}^2 \times G_{d,c}$, where $G_{d,c}$ is any abelian group of order $2^{(d+c-1)r+i}$ and exponent at most 2^c , relative to any subgroup $U_{d,c} \cong Z_2^r$, where $U_{d,c}$ is contained in a subgroup of $G_{d,c}$ isomorphic to Z_4^r and where all of the following hold:

- (i) *For $c = d$, $G_{d,c}/U_{d,c}$ contains a subgroup of index $2^{\min\{r,i\}}$ and exponent at most 2^{d-1} .*
- (ii) *For $i < r$ and $d > 2$ and $c = d - 1$, $G_{d,c}/U_{d,c}$ contains a subgroup of index 2^{r+i} and exponent at most 2^{d-2} .*
- (iii) *For $i > r$ and c in the range $\max\{1, \frac{(d-2)r+i}{i}\} < c \leq d$, $\text{rank}(G_{d,c}/U_{d,c}) \geq r + i$.*

Using Theorem 3.5 we can deduce the existence of many RDSs from Corollary 3.6 (in a similar manner to Theorem 8.4 of [4]). We shall give two such examples, based on the extreme cases $i = 0$ and $i = p - 1$ of Corollary 3.6, where we consider $r + i = p$ to be a fixed prime.

Corollary 3.7 *Let $2^p - 1$ be prime. For each $d \geq 3$, there exists a*

$$(2^{(2d-1)p}(2^p - 1)^2, 2^p, 2^{(2d-1)p}(2^p - 1)^2, 2^{(2d-2)p}(2^p - 1)^2)$$

semi-regular RDS in $Z_{2^{2p-1}}^2 \times Z_{2^d}^{2p}$ relative to any subgroup isomorphic to Z_2^p .

Proof: Take $c = d - 1$, $i = 0$ and $G_{d,c} = Z_{2^{d-1}}^{2r}$ in Corollary 3.6 and set $r = p$. Apply Theorem 3.5. \square

Corollary 3.7 demonstrates that the group order can grow without bound while the rank of the Sylow 2-subgroup remains fixed at $2p$.

Corollary 3.8 *Let $2^p - 1$ be prime. For each $d \geq 2$, there exists a*

$$(2^{2d+p-2}(2^p - 1)^2, 2, 2^{2d+p-2}(2^p - 1)^2, 2^{2d+p-3}(2^p - 1)^2)$$

semi-regular RDS in $Z_{2^{2p-1}}^2 \times Z_{2^{d+1}} \times Z_{2^d} \times Z_2^{p-2}$ relative to $U \cong Z_2$, where U is contained within either of the direct factors $Z_{2^{d+1}}$ and Z_{2^d} .

Proof: Take $c = d$, $r = 1$ and $G_{d,c} = Z_{2^d}^2 \times Z_2^{i-1}$ in Corollary 3.6, with $U_{d,c} \cong Z_2$ a subgroup of $Z_{2^d}^2$, and set $i + 1 = p$. Apply Theorem 3.5. \square

Corollary 3.8 provides new values of λ for which $(2\lambda, 2, 2\lambda, \lambda)$ semi-regular RDSs exist. All previously known examples had $\lambda = v$ or $\lambda = 2v$, where $v = 4N^2$ is the order of an abelian group known to contain a Hadamard difference set with parameter N (see Corollaries 6.7 and 8.1 of [4]). For example, taking $p = 3$, there exists a $(2^{2d+1} \cdot 49, 2, 2^{2d+1} \cdot 49, 2^{2d} \cdot 49)$ semi-regular RDS in $Z_7^2 \times Z_{2^{d+1}} \times Z_{2^d} \times Z_2$ for each $d \geq 2$, whereas no Hadamard difference set with parameter $N = 2^{d-1} \cdot 7$ is known to exist.

Finally, we show how the following product construction for RDSs [11] can be applied to allow the combination of two or more of the examples above to provide further new RDSs.

Theorem 3.9 *Let G be a group of order uaa' containing a normal subgroup U of order u . Let H and H' be subgroups of G of order ua and ua' satisfying $H \cap H' = U$. If H contains a $(a, u, a, a/u)$ RDS relative to U and H' contains a $(a', u, a', a'/u)$ RDS relative to U , then G contains a $(aa', u, aa', aa'/u)$ RDS relative to U .*

For example, take $p = 2$, $i = 0$ in Corollary 3.4 to provide a $(4 \cdot 9, 4, 4 \cdot 9, 9)$ RDS in $H = \langle w_1, w_2, x_1, x_2 \mid w_1^3 = w_2^3 = x_1^4 = x_2^4 = 1 \rangle \cong \mathbb{Z}_3^2 \times \mathbb{Z}_4^2$ relative to $U = \langle x_1^2, x_2^2 \rangle \cong \mathbb{Z}_2^2$. Then take $p = 3$, $i = 1$ in Corollary 3.4 to provide a $(8 \cdot 49, 4, 8 \cdot 49, 2 \cdot 49)$ RDS in $H' = \langle v_1, v_2, x_1 t_1, x_2 t_2, t_3 \mid v_1^7 = v_2^7 = x_1^4 = x_2^4 = t_1^2 = t_2^2 = t_3^2 = 1 \rangle \cong \mathbb{Z}_7^2 \times \mathbb{Z}_4^2 \times \mathbb{Z}_2$ relative to $U = \langle x_1^2, x_2^2 \rangle \cong \mathbb{Z}_2^2$. The group $G = \langle w_1, w_2, v_1, v_2, x_1, x_2, t_1, t_2, t_3 \mid w_1^3 = w_2^3 = v_1^7 = v_2^7 = x_1^4 = x_2^4 = t_1^2 = t_2^2 = t_3^2 = 1 \rangle \cong \mathbb{Z}_3^2 \times \mathbb{Z}_7^2 \times \mathbb{Z}_4^2 \times \mathbb{Z}_2^3$ contains H and H' as subgroups of order $4 \cdot 4 \cdot 9$ and $4 \cdot 8 \cdot 49$ respectively, and $H \cap H' = U$. Therefore by Theorem 3.9, G contains a $(32 \cdot 9 \cdot 49, 4, 32 \cdot 9 \cdot 49, 8 \cdot 9 \cdot 49)$ RDS relative to U . Note that the order of G is divisible by three distinct primes.

More generally, let $2^{p_j} - 1$ be prime for $0 \leq j \leq t$, where $p_j \geq p_0$ for each j . For each j , substitution of $i = p_j - p_0$ in Corollary 3.4 gives a $(2^{p_j}(2^{p_j} - 1)^2, 2^{p_0}, 2^{p_j}(2^{p_j} - 1)^2, 2^{p_j - p_0}(2^{p_j} - 1)^2)$ semi-regular RDS in $G_j = \mathbb{Z}_{2^{2^{p_j}-1}}^2 \times \mathbb{Z}_4^{p_0} \times \mathbb{Z}_2^{p_j - p_0}$ relative to the subgroup $\mathbb{Z}_2^{p_0}$ of $\mathbb{Z}_4^{p_0}$. Following the above example, we can identify each group G_j with a subgroup of a larger group and apply Theorem 3.9 inductively to obtain:

Corollary 3.10 *Let $2^{p_j} - 1$ be prime for $0 \leq j \leq t$, where $p_j \geq p_0$ for each j , and set $T = \sum_{j=1}^t p_j$. There exists a*

$$(2^{p_0+T} \prod_{j=0}^t (2^{p_j} - 1)^2, 2^{p_0}, 2^{p_0+T} \prod_{j=0}^t (2^{p_j} - 1)^2, 2^T \prod_{j=0}^t (2^{p_j} - 1)^2)$$

semi-regular RDS in $\mathbb{Z}_{2^{2^{p_0}-1}}^2 \times \mathbb{Z}_{2^{2^{p_1}-1}}^2 \cdots \times \mathbb{Z}_{2^{2^{p_t}-1}}^2 \times \mathbb{Z}_4^{p_0} \times \mathbb{Z}_2^T$ relative to the subgroup $U \cong \mathbb{Z}_2^{p_0}$ contained within the direct factor $\mathbb{Z}_4^{p_0}$.

There are many other ways in which we can generate further families of RDSs based on Theorem 3.3 by combinations of the three techniques illustrated here: contraction of the forbidden subgroup, recursion on the Sylow 2-subgroup, and the use of the product construction. In particular, note that by contraction of the forbidden subgroup for the

RDSs of Corollary 3.10 we can obtain further examples of $(2\lambda, 2, 2\lambda, \lambda)$ RDSs for new values of λ .

4 Construction 2: $u = 3$

In this section we construct RDSs in the group $G = \langle x, y, g, h \mid x^{2^a} = y^{2^a} = g^3 = h^3 = 1 \rangle \cong \mathbb{Z}_{2^a}^2 \times \mathbb{Z}_3^2$ relative to $\langle h \rangle \cong \mathbb{Z}_3$. We will make use of cosets of all of the cyclic subgroups of order 2^a . There are $2^a + 2^{a-1}$ such distinct cyclic subgroups, which can be written in the form $\langle xy^{2^j} \rangle$, $\langle x^{2^j}y \rangle$ and $\langle x^{2^{j+1}}y \rangle$, where $0 \leq j \leq 2^{a-1} - 1$. These cyclic subgroups are precisely the kernels of the characters of order 2^a on the Sylow 2-subgroup of G . Each such character is therefore principal on one of these subgroups and is nonprincipal on any other. Furthermore, for any character of order less than 2^a on the Sylow 2-subgroup of G , the cyclic subgroups of order 2^a contained in the kernel of the character all have only one of the three forms given above. We remark that the construction presented here is similar to the construction of Hadamard difference sets in [1] which used the cyclic subgroups of $\mathbb{Z}_{3^a}^2$. In this paper the roles of the primes 2 and 3 are the reverse of that in [1].

Theorem 4.1 *Let $G = \langle x, y, g, h \mid x^{2^a} = y^{2^a} = g^3 = h^3 = 1 \rangle \cong \mathbb{Z}_{2^a}^2 \times \mathbb{Z}_3^2$, where $a \geq 1$. The set represented by the group ring element*

$$\begin{aligned} F = & \sum_{j=0}^{2^{a-1}-1} [\langle xy^{2^j} \rangle (h^{j+1}y^j + h^{j+2}y^{2^{a-1}+j}) \\ & + \langle x^{2^j}y \rangle (gh^jx^j + gh^{j+2}x^{2^{a-1}+j}) \\ & + \langle x^{2^{j+1}}y \rangle (g^2h^jx^j + g^2h^{j+2}x^{2^{a-1}+j})] \end{aligned}$$

is a $(2^{2a}3, 3, 2^{2a}3, 2^{2a})$ RDS in G relative to $\langle h \rangle \cong \mathbb{Z}_3$.

Proof: We break the proof up into the following six cases, then apply Lemma 1.1 (i).

Case 1: Suppose that χ is nonprincipal on $\langle x^{2^{a-1}}, y^{2^{a-1}} \rangle$ and nonprincipal on $\langle h \rangle$. In this case, the kernel of χ restricted to $\langle x, y \rangle$ is one of the cyclic subgroups of order 2^a used to define F , and χ will sum to 0 over all of the other cyclic subgroups of

order 2^a . Thus, if the kernel is of the form $\langle xy^{2^j} \rangle$, then $|\chi(F)| = 2^a |\chi(h^{j+1}y^j) + \chi(h^{j+2}y^{2^{a-1}+j})| = 2^a |\chi(h^{j+1}) - \chi(h^{j+2})| = 2^a \sqrt{3}$. If the kernel has one of the other two forms $\langle x^{2^j}y \rangle$ or $\langle x^{2^{j+1}}y \rangle$, a similar computation gives a character sum with the same modulus.

Case 2: Suppose that χ is nonprincipal on $\langle x^{2^{a-1}}, y^{2^{a-1}} \rangle$ and principal on $\langle h \rangle$. As in Case 1, if the kernel is of the form $\langle xy^{2^j} \rangle$ then $|\chi(F)| = 2^a |\chi(h^{j+1}y^j) + \chi(h^{j+2}y^{2^{a-1}+j})|$ and since χ is now principal on $\langle h \rangle$, $|\chi(F)| = 2^a |\chi(y^j) - \chi(y^{2^j})| = 0$. The other two forms for the kernel give the same result.

Case 3: Suppose that χ is principal on $\langle x^{2^{a-1}}, y^{2^{a-1}} \rangle$, nonprincipal on $\langle x, y \rangle$, and nonprincipal on $\langle h \rangle$. Suppose that the cyclic subgroups of order 2^a contained in the kernel of χ are all of the form $\langle xy^{2^j} \rangle$; the cases when they are all of the form $\langle x^{2^j}y \rangle$ or all of the form $\langle x^{2^{j+1}}y \rangle$ are similar. Let $J = \{j \mid \chi(xy^{2^j}) = 1, 0 \leq j \leq 2^{a-1} - 1\}$ be the set which indexes the subgroups on which χ is principal. Let j_0 be the least element of J and let 2^b be the order of $\chi(y)$. Then we have $J = \{j_0 + 2^{b-1}k \mid 0 \leq k \leq 2^{a-b} - 1\}$. Now $\chi(xy^{2^j}) = 1$ for some j and χ is nonprincipal on $\langle x, y \rangle$, so $b > 0$. Also χ is principal on $\langle x^{2^{a-1}}, y^{2^{a-1}} \rangle$ and so $b < a$. Therefore

$$\begin{aligned} \chi(F) &= 2^a \sum_{j \in J} (\chi(h^{j+1}y^j) + \chi(h^{j+2}y^{2^{a-1}+j})) \\ &= 2^a (\chi(h) + \chi(h^2)) \sum_{j \in J} \chi(y^j) \chi(h^j) \\ &= -2^a \chi(y^{j_0}) \chi(h^{j_0}) \sum_{k=0}^{2^{a-b}-1} \chi(y^{2^{b-1}k}) \chi(h^{2^{b-1}k}), \end{aligned}$$

so that $|\chi(F)| = 2^a |\sum_{k=0}^{2^{a-b}-1} (-1)^k \chi(h^{2^{b-1}k})|$. Since χ is nonprincipal on $\langle h \rangle$, $\chi(h)$ is a primitive third root of unity and so $\chi(h^{2^{b-1}})$ is also a primitive third root of unity, say η . Then $|\chi(F)| = 2^a |\sum_{k=0}^{2^{a-b}-1} (-1)^k \eta^k| = 2^a |1 - \eta| |\sum_{k=0}^{2^{a-b}-1} (\eta^2)^k|$. Now $|\sum_{k=0}^{2^{a-b}-1} (\eta^2)^k| = 1$ since η^2 is a primitive third root of unity and 3 does not divide 2^{a-b} . Therefore $|\chi(F)| = 2^a \sqrt{3}$.

Case 4: Suppose that χ is principal on $\langle x^{2^{a-1}}, y^{2^{a-1}} \rangle$, nonprincipal on $\langle x, y \rangle$, and principal on $\langle h \rangle$. As in Case 3, using the example of subgroups of the form $\langle xy^{2^j} \rangle$, we

find $|\chi(F)|$ is a multiple of $|\sum_{k=0}^{2^{a-b}-1} (-1)^k \chi(h^{2^{b-1}k})|$. Since χ is now principal on $\langle h \rangle$, $|\chi(F)| = 0$.

Case 5: Suppose that χ is principal on $\langle x, y \rangle$ and nonprincipal on $\langle h \rangle$. Then $\chi(F) = 2^a \sum_{j=0}^{2^{a-1}-1} (\chi(h^{j+1}) + \chi(h^{j+2}) + \chi(gh^j) + \chi(gh^{j+2}) + \chi(g^2h^j) + \chi(g^2h^{j+2}))$, and since $\chi(h)$ is a primitive third root of unity we have $\chi(F) = -2^a (\chi(h^2) + \chi(g) + \chi(g^2)) \sum_{j=0}^{2^{a-1}-1} \chi(h^{j+1})$. Now $\{h^2, g, g^2\}$ is a $(3, 3, 3, 1)$ RDS in $\langle g, h \rangle$ relative to $\langle h \rangle$, so by Lemma 1.1 (i), $|\chi(h^2) + \chi(g) + \chi(g^2)| = \sqrt{3}$. Also $|\sum_{j=0}^{2^{a-1}-1} \chi(h^{j+1})| = 1$ since $\chi(h)$ is a primitive third root of unity and 3 does not divide 2^{a-1} . Therefore $|\chi(F)| = 2^a \sqrt{3}$.

Case 6: Suppose that χ is principal on $\langle x, y \rangle$, principal on $\langle h \rangle$, and nonprincipal on $\langle g \rangle$.

In this case $\chi(F) = 2^a \sum_{j=0}^{2^{a-1}-1} (\chi(1) + \chi(1) + \chi(g) + \chi(g) + \chi(g^2) + \chi(g^2)) = 0$.

□

The construction of Theorem 4.1 combines the cyclic subgroups of $Z_{2^a}^2$ of order 2^a with a $(3, 3, 3, 1)$ RDS in Z_3^2 relative to Z_3 . The smallest examples, all relative to Z_3 , are: a $(4 \cdot 3, 3, 4 \cdot 3, 4)$ RDS in $Z_2^2 \times Z_3^2$, a $(16 \cdot 3, 3, 16 \cdot 3, 16)$ RDS in $Z_4^2 \times Z_3^2$, a $(64 \cdot 3, 3, 64 \cdot 3, 64)$ RDS in $Z_8^2 \times Z_3^2$, and a $(256 \cdot 3, 3, 256 \cdot 3, 256)$ RDS in $Z_{16}^2 \times Z_3^2$.

As in Section 3 we can extend Theorem 4.1 by means of the recursive construction for RDSs given in [4]. Corollary 7.8 of [4] shows how to construct a family of BSs starting from a $(3, 3, 3, 1)$ RDS in Z_3^2 relative to Z_3 . Following the case $c = d$ of this method for the RDSs of Theorem 4.1 we obtain:

Corollary 4.2 *For each $d \geq 1$ and each $a \geq 1$, there exists a $(2^{2a}3^{2d}, 2^a3^{(2d+1)/2}, 3)$ BS on $Z_{2^a}^2 \times S_d$, where S_d is any abelian group of order 3^{2d+1} and exponent at most 3^d , relative to any subgroup $U_d \cong Z_3$, except possibly when $d > 1$ and $S_d \cong U_d \times Z_{3^d}^2$.*

Application of Theorem 3.5 then gives:

Corollary 4.3 *For each $d \geq 1$ and each $a \geq 1$, there exists a $(2^{2a}3^{2d+1}, 3, 2^{2a}3^{2d+1}, 2^{2a}3^{2d})$ semi-regular RDS in $Z_{2^a}^2 \times G_d$, where G_d is any abelian group of order 3^{2d+2} and exponent*

at most 3^{d+1} , relative to any subgroup U_d of order 3, except possibly when $G_d \cong Z_{3^{d+1}}^2$ or when $d > 1$ and $G_d \cong U_d \times Z_{3^{d+1}} \times Z_{3^d}$.

We can also use the RDS product construction (Theorem 3.9) to yield further families of RDSs based on Theorem 4.1. In particular, the Sylow 2-subgroup can have a more general form than $Z_{2^a}^2$. For example, by Corollary 8.2 of [4] there exists a $(3^w, 3, 3^w, 3^{w-1})$ RDS in $Z_3 \times G$, where G is any abelian group of order 3^w and exponent at most $3^{1+\lfloor w/2 \rfloor}$, relative to the direct factor Z_3 , except possibly when $w > 3$ is odd and $G \cong Z_{3^{(w+1)/2}} \times Z_{3^{(w-1)/2}}$. Furthermore, by Theorem 4.1 there exists a $(2^{2a_j} 3, 3, 2^{2a_j} 3, 2^{2a_j})$ RDS in $Z_{2^{a_j}}^2 \times Z_3^2$ relative to Z_3 , where $a_j \geq 1$ for each j . Recursive application of Theorem 3.9 then gives:

Corollary 4.4 *Let $a_j \geq 1$ for $1 \leq j \leq t$ and set $T = \sum_{j=1}^t a_j$. Let G be any abelian group of order 3^w and exponent at most $3^{1+\lfloor w/2 \rfloor}$ except, in the case $w > 3$ odd, $Z_{3^{(w+1)/2}} \times Z_{3^{(w-1)/2}}$. There exists a $(2^{2T} 3^{w+t}, 3, 2^{2T} 3^{w+t}, 2^{2T} 3^{w+t-1})$ semi-regular RDS in*

$$Z_{2^{a_1}}^2 \times Z_{2^{a_2}}^2 \times \cdots \times Z_{2^{a_t}}^2 \times Z_3^{t+1} \times G$$

relative to a subgroup Z_3 contained within the direct factor Z_3^{t+1} .

5 Future directions

The results of this paper show that the existence pattern for semi-regular RDSs is much richer than was previously apparent. As mentioned, we have indicated only some of the parameter sets and groups for which such RDSs can now be obtained by means of contraction, the recursive construction, and the product constructions. There are also generalisations to certain nonabelian groups, as outlined in [4]. We close with some possible future research directions suggested by our results.

1. Can the two RDS constructions of this paper be unified?
2. Which other classes of groups contain semi-regular RDSs whose order is not a prime power?

3. Can these or other RDS examples be used to construct new difference sets? We know [4] that certain BSs can be used to construct difference sets, and that if the parameters of a resulting difference set do not belong to a known family then the BS involved must be defined on a group whose order is not a prime power. This paper contains the first examples of BSs on groups whose order is not a prime power, relative to a subgroup of order greater than 2.
4. Can the RDSs of Corollary 3.8, or similar examples with a forbidden subgroup of order 2, be used in the construction of new Hadamard difference sets according to the methods of [4]? These RDSs are the first examples with parameters $(2\lambda, 2, 2\lambda, \lambda)$ for which λ is neither the order nor twice the order of an abelian group known to contain a Hadamard difference set. For example, is there a Hadamard difference set in $Z_7^2 \times A$ for some abelian 2-group A (which, from [3], must have order at least 256 if $\exp(A) \leq 8$)?
5. Are there other ways to combine difference sets, relative difference sets, direct product difference sets, or divisible difference sets to construct new examples of any of these?

Note added in proof

K.T. Arasu reports [private communication, 1996] that he recently presented (K.T. Arasu and W. de Launey, “Complex Hadamard matrices and relative difference sets”, presentation at Bose Memorial Conference, Fort Collins, Colorado, June 1995) a construction for a $(2^p(2^p - 1)^2, 2, 2^p(2^p - 1)^2, 2^{p-1}(2^p - 1)^2)$ semi-regular RDS in $Z_{2^{p-1}}^2 \times Z_4 \times Z_2^{p-1}$ relative to the subgroup Z_2 of Z_4 , where $2^p - 1$ is prime. This corresponds to the case $i = p - 1$ of Corollary 3.4, in which the forbidden subgroup has order 2.

References

- [1] K.T. Arasu, J.A. Davis, J. Jedwab, and S.K. Sehgal, New constructions of Menon difference sets, *J. Combin. Theory (A)*, Vol. 64 (1993) pp. 329–336.

- [2] J.A. Davis and J. Jedwab, A note on new semi-regular divisible difference sets, *Designs, Codes and Cryptography*, Vol. 3 (1993) pp. 373–381.
- [3] J.A. Davis and J. Jedwab, Nested Hadamard difference sets. Submitted (1996).
- [4] J.A. Davis and J. Jedwab, A unifying construction for difference sets, Technical Report HPL-96-31, Hewlett-Packard Labs., Bristol (February 1996).
- [5] M.J. Ganley, Direct product difference sets, *J. Combin. Theory (A)* Vol. 23 (1977) pp. 321–332.
- [6] D. Jungnickel, On automorphism groups of divisible designs, *Canad. J. Math.* Vol. 34 (1982) pp. 257–297.
- [7] D. Jungnickel, Difference sets, *Contemporary Design Theory: a Collection of Surveys* (J.H. Dinitz and D.R. Stinson, eds.), Wiley, New York (1992) pp. 241–324.
- [8] E.S. Lander, *Symmetric Designs: an Algebraic Approach*, London Mathematical Society Lecture Notes Series 74, Cambridge University Press, Cambridge (1983).
- [9] S.L. Ma and B. Schmidt, On (p^a, p, p^a, p^{a-1}) -relative difference sets, *Designs, Codes and Cryptography* Vol. 6 (1995) pp. 57–71.
- [10] A. Pott, *Finite Geometry and Character Theory*, Lecture Notes in Mathematics 1601, Springer-Verlag, Berlin (1995).
- [11] A. Pott, A survey on relative difference sets, *Groups, Difference Sets and the Monster* (K.T. Arasu et al., eds.), de Gruyter, Berlin-New York (1996) pp. 195–232.
- [12] R.J. Turyn, Character sums and difference sets, *Pacific J. Math.* Vol. 15 (1965) pp. 319–346.