7-1997

Using the Simplex Code to Construct Relative Difference Sets in 2-groups

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

Surinder K. Sehgal

Designs, Codes and Cryptography, 11, 267–277 (1997)

Using the Simplex Code to Construct Relative Difference Sets in 2-groups

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

SURINDER K. SEHGAL
Ohio State University, Columbus, OH 43210

Communicated by: D. Jungnickel

Received July 8, 1994; Revised February 9, 1995; Accepted July 1, 1996

Abstract. Relative Difference Sets with the parameters $(2^a, 2^b, 2^a, 2^{a-b})$ have been constructed many ways (see [2], [3], [5], [6], and [7] for examples). This paper modifies an example found in [1] to construct a family of relative difference sets in 2-groups that gives examples for $b = 2$ and $b = 3$ that have a lower rank than previous examples. The Simplex code is used in the construction.

Keywords: Simplex code; relative difference sets; 2-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 $k = n\lambda$; in particular, we will be using the parameters $(2^a, 2^b, 2^a, 2^{a-b})$. In a recent survey of RDS, Pott says "It is, in my opinion, one of the most interesting questions about relative difference sets to find all possible groups G which contain such difference sets (referring to (p^a, p^b, p^a, p^{a-b})) ..." [7]. These were first studied by Elliot and Butson [3]. More recently, Jungnickel [5] has constructed RDS with these parameters for all possibilities of a and b. The (abelian) groups he used were $Z_4^b \times Z_2^{a-b}$ (he also has some nonabelian examples). In [2], the author used techniques from difference sets to find many more groups that have a RDS; these examples were mainly when a is even. This paper modifies a construction found in [1] to construct examples. The current state of knowledge about RDS with these parameters is summarized as follows (see [7] for more details).

THEOREM 1.1 *Let G be an abelian group of order 2^{2a+b}. If $b = 1$, then G has a $(2^{2a}, 2, 2^{2a}, 2^{2a-1})$ RDS relative to any subgroup of order 2 if and only if $\exp(G) \leq 2^{a+1}$ [6]. If $b > 1$, then G has a $(2^{2a}, 2^b, 2^{2a}, 2^{2a-b})$ RDS if G has rank at least $a + b$ (and the*

* This work is partially supported by a University of Richmond summer grant.

RDS is relative to an elementary abelian subgroup) [2]. Also, a necessary condition for a RDS with these parameters to exist is $\exp(G) \leq 2^{2a}$ *and* $\exp(G) \leq 2^a \exp(N)$ *[8].*

Thus, the $b = 1$ existence question has been completely answered (for $p = 2$). In solving that problem, Ma and Schmidt [6] state that the case with $b > 1$ is "much more difficult". We focus on that case in that paper, and we provide new constructions for two cases.

It is helpful to consider the group ring ZG when working with RDS. If we write the subset A of G as $A = \sum_{a \in A} a$, and $A^{(-1)} = \sum_{a \in A} a^{-1}$, then the definition of RDS implies that D is a RDS iff $DD^{(-1)} = k + \lambda(G - N)$. When the group G is abelian, then a character of G is a homomorphism from G to the complex numbers. We can extend this character (homomorphism) linearly to the group ring. If we use the basic fact that the character sum over a group will be 0 if the character is nonprincipal (nontrivial) on the group, then there are 3 possible character sums. Moreover, the standard inversion theory arguments show that if we have a set that has all of the correct character sums, then the set must be a RDS. This tool is summarized in the following well-known lemma (see [9]).

LEMMA 1.1 *Let G be an abelian group. A subset D is a (m, n, k, λ) RDS relative to a subgroup N if and only if (i) every character that is nonprincipal on N has a character sum of modulus $\sqrt{k}$ (ii) every character that is principal on N but nonprincipal on G has a character sum of modulus $\sqrt{k - n\lambda}$ (iii) The size of the set D is k.*

In order to construct the RDS in the next section, we will need some basic information about the Simplex code (actually the extended Simplex code). One way to define this code is as the dual of the binary Hamming code. The parity check matrix for the Hamming code will have r rows, and there will be $2^r - 1$ columns: each column will be a distinct nonzero binary r-tuple. We will extend this matrix by one further column of all zeros (for convenience, put the column of zeros as the first column and call it column 0). The Simplex code is the code C generated by the row space. The weight enumerator of this code is $W_C(z) = 1 + (2^r - 1)z^{2^{r-1}}$; in other words, all of the nonzero codewords have weight 2^{r-1} (see [4]). We need a few other basic facts about this code, which we include in the following lemma.

LEMMA 1.2 *Any r linearly independent codewords $\alpha_1, \alpha_2, \ldots, \alpha_r$ from C will generate the Simplex code. If we put these codewords into a matrix with α_i being the i^{th} row, then the columns of this matrix will be distinct, and every possible r-tuple of 0s and 1s will appear as a column. Any two distinct $r - 1$ dimensional spaces H_1 and H_2 will have the property they they intersect in a $r - 2$ dimensional space, so their union will not be the whole code.*

Proof. The first property is basic linear algebra. The second part is true because of the connection to the Hamming code. If we drop the all 0 column, the matrix formed by the α_i is the parity check matrix for a code. Since the Hamming code has minimum distance 3, no two columns of the parity check matrix can be the same (otherwise, there would be a word of weight 2). The all 0 column will be distinct from any of the other columns. Since there are 2^r distinct columns and there are 2^r distinct r-tuples, it is clear that every r-tuple appears as a column exactly once. Finally, the last part about the $r - 1$ dimensional spaces

is basic linear algebra of hyperplanes along with a counting argument of elements of the code. ■

The code will be used to determine how to modify a basic group ring element so the character sums of the combinations will all be correct.

2. The $b = 2$ Case

In this section, we consider RDS with the parameters $(2^{2r+4}, 4, 2^{2r+4}, 2^{2r+2})$. From the results mentioned in the introduction, these will exist in any group whose rank is at least $r + 4$. To do this, use the technique found in [2] to construct a $(2^{2r+4}, 2^{r+2}, 2^{2r+4}, 2^{r+2})$ RDS in a group with rank $2r + 4$ relative to any elementary abelian subgroup of order 2^{r+2}. A result mentioned in [5] implies that we will still have a RDS when we consider the image of the RDS under the natural map from G to G/H, where H is any subgroup of the forbidden subgroup N. Thus, if we contract the group with the $(2^{2r+4}, 2^{r+2}, 2^{2r+4}, 2^{r+2})$ RDS by an elementary abelian subgroup of order 2^r, the image of the RDS will be a $(2^{2r+4}, 4, 2^{2r+4}, 2^{2r+2})$ RDS in a group with rank at least $r + 4$. We will construct a RDS with these parameters in any abelian group with rank at least $r + 3$ and that contains a subgroup isomorphic to $Z_4 \times Z_4$. Note that any abelian group with rank exactly $r + 3$ that meets the exponent bound of 2^{r+3} (when $\exp(N) = 2$) will have a subgroup isomorphic to $Z_4 \times Z_4$.

Suppose G is an abelian group of order 2^{2r+6} with a subgroup H isomorphic to $Z_4^2 \times Z_2^{r+1}$. Let H be generated by $x, y, z, w_1, \ldots, w_r$, where $x^4 = y^4 = z^2 = w_1^2 = \cdots = w_r^2 = 1$. The forbidden subgroup for the construction will be $\langle x^2, y^2 \rangle$. The basic building block of our RDS is the following group ring element:

$$D_0 = (1 + x)(1 + y)(1 + xyz)(1 + w_1)(1 + w_2) \cdots (1 + w_r)$$

We have the following character theory sum on this basic block.

LEMMA 2.1 *Let χ be a nonprincipal character on H. Then $\chi(D_0) = 2^{r+2}$ or 0 if χ is a character of order 4, and $\chi(D_0) = 0$ if χ is a character of order 2.*

Proof. If χ is a character of order 4, then χ will have sum $(1 \pm \sqrt{-1})$ on two of the three terms $(1 + x)$, $(1 + y)$, $(1 + xyz)$. Since the modulus of $(1 \pm \sqrt{-1})$ is $\sqrt{2}$, the two of these multiplied together will have modulus 2. There are $r + 1$ other terms, and all of these terms will have character sum (1 ± 1). If any of the terms is (1-1), then $\chi(D_0) = 0$, but if all of these terms are (1+1), then $\chi(D_0) = 2^{r+2}$. If χ is a character of order 2, then at least one of the terms in D_0 will have a character sum of (1-1), and so $\chi(D_0) = 0$. ■

This result gives a clue as to why we will need the Simplex code to help us construct the code. We will eventually want the character sum of the RDS to be 2^{r+2} for *every* character of order 4. The D_0 that we have defined above is only nonzero for those characters that have (1+1) as a character sum for all of the terms that are not $(1 \pm \sqrt{-1})$. We will need a

lot of other blocks that are modifications of this basic block that will contribute the correct character sum for some of the characters of order 4 and will have a character sum of 0 on all of the rest. The Simplex code will tell us how to make the modifications.

Let $\alpha_1, \alpha_2, \ldots, \alpha_{r+1}$ be a basis for the Simplex code C of dimension $r+1$ as defined in the introduction. We want to choose another basis for C, say $\beta_1, \beta_2, \ldots, \beta_r$, in a careful way. We first choose $\beta_2 \notin \langle \alpha_2 \rangle$. We next choose $\beta_3 \notin \langle \alpha_3, \alpha_2 + \beta_2 \rangle \cup \langle \beta_2 \rangle$. The next choice is $\beta_4 \notin \langle \alpha_4, \alpha_2 + \beta_2, \alpha_3 + \beta_3 \rangle \cup \langle \beta_2, \beta_3 \rangle$; this process is continued until we choose $\beta_{r+1} \notin \langle \alpha_{r+1}, \alpha_2 + \beta_2, \alpha_3 + \beta_3, \ldots, \alpha_r + \beta_r \rangle \cup \langle \beta_2, \beta_3, \ldots, \beta_r \rangle$. Finally, we choose $\beta_1 \notin \langle \beta_2, \beta_3, \ldots, \beta_{r+1} \rangle$. These choices accomplish two things at once: first, the β_i are linearly independent and therefore are a basis for C. Second, the $\alpha_2 + \beta_2, \alpha_3 + \beta_3, \ldots, \alpha_{r+1} + \beta_{r+1}$ are linearly independent, and we can pick one more linearly independent codeword γ_1 so that $\gamma_1, \alpha_2 + \beta_2, \alpha_3 + \beta_3, \ldots, \alpha_{r+1} + \beta_{r+1}$ is also a basis for C.

We are now in a position to define all of the other blocks. We will use the notation $\alpha_{i,j}$ to refer to the j^{th} component of α_i (and similarly for the $\beta_{i,j}$ and $\gamma_{i,j}$). With that notation, the following are all of the other blocks of the RDS.

$$\begin{aligned} D_j \;=\; & (1 + xy^{2\alpha_{1,j}})(1 + x^{2\beta_{1,j}} y)(1 + x^{1+2\gamma_{1,j}} yz)(1 + x^{2\beta_{2,j}} y^{2\alpha_{2,j}} w_1) \\ & (1 + x^{2\beta_{3,j}} y^{2\alpha_{3,j}} w_2) \cdots (1 + x^{2\beta_{r+1,j}} y^{2\alpha_{r+1,j}} w_r) \end{aligned}$$

Note that these blocks are indexed by the columns of the matrices of the basis vectors; since there are 2^{r+1} columns, we will have a total of 2^{r+1} blocks (including D_0: note that D_0 comes from the all 0 column). Each of these blocks is a subset of H, and there are $2^{2r+6}/2^{r+5} = 2^{r+1}$ distinct cosets of H in G. If we label the coset representatives $\{g_0, g_1, \ldots, g_{2^{r+1}-1}\}$, then define $D = \cup_{j=0}^{2^{r+1}-1} g_j D_j$. The next theorem claims that this is the RDS we have been looking for.

THEOREM 2.1 *The set D defined above is a $(2^{2r+4}, 4, 2^{2r+4}, 2^{2r+2})$ RDS in any abelian group with rank at least $r+3$ and $Z_4 \times Z_4$ as a subgroup (N is the subgroup $Z_2 \times Z_2$ inside $Z_4 \times Z_4$).*

Proof. We need to show that for any character that is nonprincipal on $N = \langle x^2, y^2 \rangle$, the character sum is 2^{r+2}. Consider the case when $\chi|_H$ (the character restricted to the subgroup H) sends the generator x to $\pm\sqrt{-1}$ and all the other generators to ± 1. In this case, the terms $(1 + xy^{2\alpha_{1,j}})$ and $(1 + x^{1+2\gamma_{1,j}} yz)$ both go to $(1 \pm \sqrt{-1})$ in all the blocks. The other terms will all go to (1 ± 1), and we want exactly one block to have all of its terms go to (1 + 1). If we look at where the $(r+1)$-tuple $(y, w_1, w_2, \ldots, w_r)$ gets sent, each component will be sent to ± 1. We want to choose the column j' so that $\beta_{i,j'} = 1$ when the i^{th} component is -1 and $\beta_{i,j'} = 0$ when the i^{th} component is +1 (we know that we can do this because every possible $r+1$-tuple shows up exactly one time as a column of the β_i matrix). The reason for this is we will multiply the -1 character value in the i^{th} component by $\chi(x^{2\beta_{i,j'}})$, and this is -1 if $\beta_{i,j'} = 1$. The $D_{j'}$ associated to the j'^{th} column will have a character sum of modulus 2^{r+2}. All of the other D_j will have at least one term of (1-1), so the sum over those will be 0. Similar arguments will handle the characters that send y to $\pm\sqrt{-1}$ and everything else to ± 1 (this will use the αs instead of the βs) and the characters that send both x and y to $\pm\sqrt{-1}$ and everything else to ± 1 (this will use the γ_1 and the $\alpha_i + \beta_i$s). The key to all of these working is that each possible column will show up in the appropriate

matrix exactly one time, and that is true of the Simplex code. Thus, every character that is nonprincipal on the subgroup $\langle x^2, y^2\rangle$ has a character sum of modulus 2^{r+2}.

There are still a few characters that we need to check to show that this is an RDS. We need to check all characters of order 2 on H. Characters of order 2 have to send the generators x and y to ± 1, so all of the terms x^2 and y^2 that we introduced in the D_j have no effect on the character sum. Thus, the character sum for these characters of order 2 on H have exactly the same character sum as D_0 for all j. We showed in Lemma 2.1 that characters of order 2 on H have a 0 character sum on D_0, so this is true for all the D_j and thus the sum over all of D is 0. If the character χ is principal on H but nonprincipal on G, then $\chi(D_j) = 2^{r+3}$ (that is the size of the D_j). The sum over D is $\chi(D) = \sum \chi(g_i)\chi(D_i) = 2^{r+3}\sum \chi(g_i) = 0$. Finally, the principal character on G counts the number of elements in this subset, and that number is $2^{r+1} \cdot 2^{r+3} = 2^{2r+4} = k$ (the first term in the product is the number of distinct blocks, and the second term is the size of each block). Since all of the character sums are what we want them to be, the inversion formula says that this subset is a RDS with the proper parameters in any group of rank at least $r + 3$ and that has a subgroup Z_4^2. ■

Example 2.1: Consider the case when $r = 3$. Let $\alpha_1 = 0000000011111111, \alpha_2 = 0000111100001111, \alpha_3 = 0011001100110011$, and $\alpha_4 = 0101010101010101$ (this is the case where the parity check matrix for the Hamming code is a binary counter). We can then choose $\beta_2 = 0000000011111111, \beta_3 = 0000111100001111, \beta_4 = 0011001100110011$, and $\beta_1 = 0101010101010101$. The final matrix will be $\alpha_2+\beta_2 = 0000111111110000, \alpha_3+\beta_3 = 0011110000111100, \alpha_4 + \beta_4 = 0110011001100110$, and $\gamma_1 = 0000000011111111$. The following are the blocks of the RDS:

$$D_0 = (1 + x)(1 + y)(1 + xyz)(1 + w_1)(1 + w_2)(1 + w_3);$$

$$D_1 = (1 + x)(1 + x^2y)(1 + xyz)(1 + w_1)(1 + w_2)(1 + y^2w_3);$$

$$D_2 = (1 + x)(1 + y)(1 + xyz)(1 + w_1)(1 + y^2w_2)(1 + x^2w_3);$$

$$D_3 = (1 + x)(1 + x^2y)(1 + xyz)(1 + w_1)(1 + y^2w_2)(1 + x^2y^2w_3);$$

$$D_4 = (1 + x)(1 + y)(1 + xyz)(1 + y^2w_1)(1 + x^2w_2)(1 + w_3);$$

$$D_5 = (1 + x)(1 + x^2y)(1 + xyz)(1 + y^2w_1)(1 + x^2w_2)(1 + y^2w_3);$$

$$D_6 = (1 + x)(1 + y)(1 + xyz)(1 + y^2w_1)(1 + x^2y^2w_2)(1 + x^2w_3);$$

$$D_7 = (1 + x)(1 + x^2y)(1 + xyz)(1 + y^2w_1)(1 + x^2y^2w_2)(1 + x^2y^2w_3);$$

$$D_8 = (1 + xy^2)(1 + y)(1 + x^3yz)(1 + x^2w_1)(1 + w_2)(1 + w_3);$$

$$D_9 = (1 + xy^2)(1 + x^2y)(1 + x^3yz)(1 + x^2w_1)(1 + w_2)(1 + y^2w_3);$$

$$D_{10} = (1 + xy^2)(1 + y)(1 + x^3yz)(1 + x^2w_1)(1 + y^2w_2)(1 + x^2w_3);$$

$$D_{11} = (1 + xy^2)(1 + x^2y)(1 + x^3yz)(1 + x^2w_1)(1 + y^2w_2)(1 + x^2y^2w_3);$$

$$D_{12} = (1 + xy^2)(1 + y)(1 + x^3yz)(1 + x^2y^2w_1)(1 + x^2w_2)(1 + w_3);$$

$$D_{13} = (1 + xy^2)(1 + x^2y)(1 + x^3yz)(1 + x^2y^2w_1)(1 + x^2w_2)(1 + y^2w_3);$$

$$D_{14} = (1 + xy^2)(1 + y)(1 + x^3yz)(1 + x^2y^2w_1)(1 + x^2y^2w_2)(1 + x^2w_3);$$

$$D_{15} = (1 + xy^2)(1 + x^2y)(1 + x^3yz)(1 + x^2y^2w_1)(1 + x^2y^2w_2)(1 + x^2y^2w_3)$$

In the group $Z_{64} \times Z_4 \times Z_2^4$, if g is an element of order 64 so that $g^{16} = x$, then the RDS is $D = \cup_{i=0}^{15} g^i D_i$. This is an RDS in a group of rank 6, and the best that could be done with previous constructions was rank 7 (start with a $(1024, 32, 1024, 32)$ RDS in a group of rank 10 and mod out the forbidden subgroup by a subgroup of order 8). The exponent of the group we have chosen is as big as the exponent bound allows; any other group of order 4096, rank 6, and exponent less than 64 will have a RDS by using these basic blocks. □

3. The $b = 3$ Case

We will use the same basic pattern as in the last section. We first define a basic building block for a $(2^{2r+10}, 8, 2^{2r+10}, 2^{2r+7})$ RDS. This basic block will be a subset of a subgroup isomorphic to $H = Z_4^3 \times Z_2^{r+4}$, where $x^4 = y^4 = z^4 = w^2 = u^2 = v^2 = t^2 = s_1^2 = \cdots = s_r^2 = 1$ (note that the forbidden subgroup in this case will be $\langle x^2, y^2, z^2 \rangle$).

$$\begin{aligned} D_0 \;=\; & (1 + x)(1 + y)(1 + z)(1 + xyw)(1 + xzu)(1 + yzv) \\ & (1 + xyzt)(1 + s_1)(1 + s_2) \cdots (1 + s_r) \end{aligned}$$

LEMMA 3.1 *Any character of order* 4 *on* H *will have character sum of modulus* 2^{r+5} *or* 0 *on* D_0. *Any character of order* 2 *on* H *will have character sum of* 0 *on* D_0.

The reason for this is the same as for Lemma 2.1, but in this case for every character of order 4 there will be 4 terms of the form $(1 \pm \sqrt{-1})$.

We need to determine where to modify this basic block to get the character sums to work out correctly. The Simplex code is used here to determine the pattern for the x^2, y^2, and z^2. We will only do the case where $r > 1$ here: the $r = 0$ and $r = 1$ cases will be explained in the example following the theorem. Choose a basis $\alpha_1, \alpha_2, \ldots, \alpha_{r+3}$ for the code C of dimension $r + 3$. We will use the α_i to determine which of the blocks to put the x^2 in for the terms (in order) $(1 + y)$, $(1 + z)$, $(1 + yzv)$, $(1 + s_1), \ldots, (1 + s_r)$. For the next phase we will use the basis $\alpha_4 + \alpha_{r+3}, \alpha_1, \alpha_2, \ldots, \alpha_{r+2}$ to determine which of the blocks to put the y^2 in for the terms (in order) $(1 + x)$, $(1 + z)$, $(1 + xzu)$, $(1 + s_1), \ldots, (1 + s_r)$. To determine where to put the z^2, we use the basis $\alpha_2, \alpha_3, \ldots, \alpha_{r+3}, \alpha_1 + \alpha_{r+2} + \alpha_{r+3}$ for the terms (in order) $(1 + x)$, $(1 + y)$, $(1 + xyw)$, $(1 + s_1), \ldots, (1 + s_r)$. Those three patterns will make the blocks work for the characters that are of order 4 on (respectively) just x, just y, and just z. Once these three are established, most of the rest of the bases that are required are combinations of these basic three ordered bases.

The following tables show how to fill out the rest of the bases. In the "how chosen" column of the table, most of the vectors are forced on us by choices made in previous bases (those are indicated by "from ... bases for ..."). There are two choices in the first table,

two choices in the second table, and one choice in the third table. These choices are made with two goals: first, they have to complete a basis for the vector space so that the characters listed at the top of the table will have the proper character sum. Second, they have to be chosen so that the combination with a vector from another table will be the appropriate vector in a later table. The last table does not have any choices because all of the vectors are simply combinations of previously chosen vectors, and we had to make those choices so that the last table would be a basis.

When x and y are sent to $\pm\sqrt{-1}$

Term	vector	how chosen
$(1+z)$	$\alpha_1+\alpha_2$	from first and second bases for $(1+z)$
$(1+xyw)$	α_1	chosen to avoid basis vectors, other $(1+xyw)$ term (use y^2)
$(1+xyzt)$	α_3	chosen to avoid basis vectors (use y^2)
$(1+s_1)$	$\alpha_3+\alpha_4$	from first and second bases for $(1+s_1)$
$(1+s_2)$	$\alpha_4+\alpha_5$	from first and second bases for $(1+s_2)$
$\vdots$	$\vdots$	$\vdots$
$(1+s_r)$	$\alpha_{r+2}+\alpha_{r+3}$	from first and second bases for $(1+s_r)$

When x and z are sent to $\pm\sqrt{-1}$

Term	vector	how chosen
$(1+y)$	$\alpha_1+\alpha_3$	from first and third bases for $(1+y)$
$(1+xzu)$	α_1	chosen to avoid basis vectors, other $(1+xzu)$ term (use z^2)
$(1+xyzt)$	α_2 if r is odd $\alpha_2+\alpha_3$ if r is even	chosen to avoid basis vectors (use z^2)
$(1+s_1)$	$\alpha_4+\alpha_5$	from first and third bases for $(1+s_1)$
$(1+s_2)$	$\alpha_5+\alpha_6$	from first and third bases for $(1+s_2)$
$\vdots$	$\vdots$	$\vdots$
$(1+s_{r-1})$	$\alpha_{r+2}+\alpha_{r+3}$	from first and third bases for $(1+s_{r-1})$
$(1+s_r)$	$\alpha_{r+2}+\alpha_1$	from first and third bases for $(1+s_r)$

When y and z are sent to $\pm\sqrt{-1}$

Term	vector	how chosen
$(1+x)$	$\alpha_2+\alpha_4+\alpha_{r+3}$	from second and third bases for $(1+x)$
$(1+yzv)$	α_1	chosen to avoid basis vectors, other $(1+yzv)$ term (use z^2)
$(1+xyzt)$	$\alpha_2+\alpha_3$ if r is odd α_2 if r is even	from fourth and fifth bases for $(1+xyzt)$
$(1+s_1)$	$\alpha_3+\alpha_5$	from second and third bases for $(1+s_1)$
$(1+s_2)$	$\alpha_4+\alpha_6$	from second and third bases for $(1+s_2)$
$\vdots$	$\vdots$	$\vdots$
$(1+s_{r-1})$	$\alpha_{r+1}+\alpha_{r+3}$	from first and third bases for $(1+s_{r-1})$
$(1+s_r)$	$\alpha_{r+3}+\alpha_1$	from second and third bases for $(1+s_r)$

When x, y, and z are sent to $\pm\sqrt{-1}$

Term	vector	how chosen
$(1+xyw)$	$\alpha_1+\alpha_4$	from third and fourth bases for $(1+xyw)$
$(1+xzu)$	$\alpha_1+\alpha_2$	from second and fifth bases for $(1+xzu)$
$(1+yzv)$	$\alpha_1+\alpha_3$	from first and sixth bases for $(1+yzv)$
$(1+s_1)$	$\alpha_3+\alpha_4+\alpha_5$	from first, second, and third bases for $(1+s_1)$
$(1+s_2)$	$\alpha_4+\alpha_5+\alpha_6$	from first, second, and third bases for $(1+s_2)$
$\vdots$	$\vdots$	$\vdots$
$(1+s_{r-1})$	$\alpha_{r+1}+\alpha_{r+2}+\alpha_{r+3}$	from first, second, and third bases for $(1+s_{r-1})$
$(1+s_r)$	α_1	from first, second, and third bases for $(1+s_r)$

We will use these ordered bases for the Simplex code in the same way we did before to define the rest of the blocks of the RDS. The D_j will have x^2, y^2, and z^2 in the blocks where the appropriate basis vector has a 1 in the j^{th} position, and they will not appear if there is a 0 in the j^{th} position. If G is any abelian group of order 2^{2r+13} with H as a subgroup, then there are $2^{2r+13}/2^{r+10} = 2^{r+3}$ cosets of H in G. If $\{g_0, g_1, \ldots, g_{2^{r+3}-1}\}$ is a set of coset representatives, the $D = \cup g_j D_j$ is the RDS.

THEOREM 3.1 *Let G be any abelian group of order 2^{2r+13} ($r > 1$) of rank at least $r+7$ and a subgroup isomorphic to Z_4^3. Then the set D defined above is a $(2^{2r+10}, 8, 2^{2r+10}, 2^{2r+7})$ RDS in G relative to the subgroup $Z_2 \times Z_2 \times Z_2$ contained in $Z_4 \times Z_4 \times Z_4$.*

The proof of this is similar to (but more complicated than) the proof of the theorem in the previous section. It relies on the fact that the seven sets of codewords chosen above are linearly independent. This would imply that they form a basis for the code, and when they are put into the matrix form every possible column will show up exactly one time. If this is true, then every character of order 4 will have a character sum of modulus 2^{r+5} for exactly one of the D_j and will sum to 0 on all the other blocks. The other characters will work out the same as they did on D_0, and the inversion formula will finish the proof. The rank of the group here is one less than what was previously possible (start with a $(2^{2r+10}, 2^{r+5}, 2^{2r+10}, 2^{2r+5})$ RDS in a group with rank 2^{2r+10} and mod out the forbidden subgroup by a group of order 2^{r+2} yielding rank $r+8$).

Example 3.1: Consider the case when $r = 1$. Let $\alpha_1 = 0000000011111111, \alpha_2 = 0000111100001111, \alpha_3 = 0011001100110011$, and $\alpha_4 = 0101010101010101$ as in Example 2.1. The pattern of ordered bases that we will use for the 7 different types of characters of order 4 are as follows: $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$; $\{\alpha_4, \alpha_1, \alpha_2, \alpha_3\}$; $\{\alpha_2, \alpha_3, \alpha_4, \alpha_1\}$; $\{\alpha_1+\alpha_2, \alpha_1, \alpha_3, \alpha_3+\alpha_4\}$; $\{\alpha_1+\alpha_3, \alpha_1, \alpha_2, \alpha_1+\alpha_4\}$; $\{\alpha_2+\alpha_4, \alpha_1, \alpha_2+\alpha_3, \alpha_1+\alpha_3\}$; $\{\alpha_1+\alpha_4, \alpha_1+\alpha_2, \alpha_1+\alpha_3, \alpha_1+\alpha_3+\alpha_4\}$. The blocks are as follows:

$$\begin{aligned} D_0 &= (1+x)(1+y)(1+z)(1+xyw)(1+xzu)(1+yzv) \\ &\quad (1+xyzt)(1+s_1); \\ D_1 &= (1+xy^2)(1+y)(1+z)(1+xyz^2w)(1+xzu)(1+yzv) \\ &\quad (1+xyzt)(1+x^2s_1); \end{aligned}$$

$$
\begin{aligned}
D_2 &= (1+x)(1+yz^2)(1+z)(1+xyw)(1+xzu)(1+x^2yzv)\\
&\quad (1+xy^3zt)(1+y^2s_1);\\
D_3 &= (1+xy^2)(1+yz^2)(1+z)(1+xyz^2w)(1+xzu)(1+x^2yzv)\\
&\quad (1+xy^3zt)(1+x^2y^2s_1);\\
D_4 &= (1+xz^2)(1+y)(1+x^2z)(1+xyw)(1+xy^2zu)(1+yzv)\\
&\quad (1+xyz^3t)(1+s_1);\\
D_5 &= (1+xy^2z^2)(1+y)(1+x^2z)(1+xyz^2w)(1+xy^2zu)\\
&\quad (1+yzv)(1+xyz^3t)(1+x^2s_1);\\
D_6 &= (1+xz^2)(1+yz^2)(1+x^2z)(1+xyw)(1+xy^2zu)\\
&\quad (1+x^2yzv)(1+xy^3z^3t)(1+y^2s_1);\\
D_7 &= (1+xy^2z^2)(1+yz^2)(1+x^2z)(1+xyz^2w)(1+xy^2zu)\\
&\quad (1+x^2yzv)(1+xy^3z^3t)(1+x^2y^2s_1);\\
D_8 &= (1+x)(1+x^2y)(1+y^2z)(1+xy^3w)(1+xz^3u)\\
&\quad (1+yz^3v)(1+xyzt)(1+z^2s_1);\\
D_9 &= (1+xy^2)(1+x^2y)(1+y^2z)(1+xy^3z^2w)(1+xz^3u)\\
&\quad (1+yz^3v)(1+xyzt)(1+x^2z^2s_1);\\
D_{10} &= (1+x)(1+x^2yz^2)(1+y^2z)(1+xy^3w)(1+xz^3u)\\
&\quad (1+x^2yz^3v)(1+xy^3zt)(1+y^2z^2s_1);\\
D_{11} &= (1+xy^2)(1+x^2yz^2)(1+y^2z)(1+xy^3z^2w)(1+xz^3u)\\
&\quad (1+x^2yz^3v)(1+xy^3zt)(1+x^2y^2z^2s_1);\\
D_{12} &= (1+xz^2)(1+x^2y)(1+x^2y^2z)(1+xy^3w)(1+xy^2z^3u)\\
&\quad (1+yz^3v)(1+xyz^3t)(1+z^2s_1);\\
D_{13} &= (1+xy^2z^2)(1+x^2y)(1+x^2y^2z)(1+xy^3z^2w)(1+xy^2z^3u)\\
&\quad (1+yz^3v)(1+xyz^3t)(1+x^2z^2s_1);\\
D_{14} &= (1+xz^2)(1+x^2yz^2)(1+x^2y^2z)(1+xy^3w)(1+xy^2z^3u)\\
&\quad (1+x^2yz^3v)(1+xy^3z^3t)(1+y^2z^2s_1);\\
D_{15} &= (1+xy^2z^2)(1+x^2yz^2)(1+x^2y^2z)(1+xy^3z^2w)(1+xy^2z^3u)\\
&\quad (1+x^2yz^3v)(1+xy^3z^3t)(1+x^2y^2z^2s_1)
\end{aligned}
$$

If we consider the group $Z_{64} \times Z_4^2 \times Z_2^5$, if g is an element of order 64 so that $g^{16} = x$, then the RDS is $D = \cup_{i=0}^{15} g^i D_i$. This has rank 8, and the best that could be done before was 9. As before, there are a lot of other abelian groups of rank 8 that will have RDSs based on this construction. □

There is a similar construction for the $r = 0$ case. The only difference is the ordered sets of vectors with 3 elements must be chosen so that they are linearly independent.

It is worth making several notes about this construction.

1. The involutions u, v, w and t are needed here in order to make sure that the basic block

does not have any coefficients other than 0 or 1. If there were coefficients of higher orders, then this would be a RDS with repeated elements, which we are not allowed to do. The same thing was true in the $b = 2$ case, and in general we will need $2^b - b - 1$ involutions when there are b distinct generators of order 4.

2. There are other ways to choose the seven bases that are required to make this construction work. The difficult part of making the choices is that each stage has implications on later bases. For example, when we chose α_1 as the codeword associated to $(1+y)$ in the first basis (for characters that just send x to $\pm\sqrt{-1}$) and α_2 as the codeword associated to $(1+y)$ in the second basis (for characters that just send z to $\pm\sqrt{-1}$), that forced $\alpha_1+\alpha_2$ to be the codeword associated to $(1+y)$ in the fourth basis (for characters that send x and z to $\pm\sqrt{-1}$). The reason this is forced on us is that α_1 determines where to put x^2, α_2 determines where to put z^2. Once these are placed, when just one of x^2 and z^2 appears in a term, the character χ that sends both x and z to $\pm\sqrt{-1}$ will multiply the y term by -1; if neither x^2 nor z^2 appear or both, then the y term will not be affected. This situation is best described by adding the two codewords: when one component has a 0 and the other has a 1, the sum is 1 (corresponding to multiplying by -1) and when both components have either 0s or 1s, the sum is 0 (corresponding to multiplying by +1). There are many dependence relationships like this.

3. We will need to use the notation $a_1, \ldots, a_{r+3}$ for the first basis, $b_1, \ldots, b_{r+3}$ for the second basis, up through $g_1, \ldots, g_{r+3}$ for the seventh basis. With this notation, the most difficult of the choices to make are the following:

a. The codeword d_2 must be chosen so that it is not in the hyperplane $\langle d_1, d_4, \ldots, d_{r+3}, c_3\rangle$ (those are all predetermined, and d_2 cannot be dependent on any of the d_is). Also, d_2 cannot be in the coset $c_3 + \langle a_4 + b_4 + c_4, \ldots, a_{r+3} + b_{r+3} + c_{r+3}\rangle$. There are elements left to choose from by Lemma 1.1. The codeword e_2 has a similar restriction.

b. The codeword e_3 must be chosen so that it is not in the hyperplane $\langle e_1, e_2, e_4, \ldots, e_{r+3}\rangle$. It must also avoid $d_3 + \langle b_1 + c_1, b_4 + c_4, \ldots, b_{r+3} + c_{r+3}\rangle$ so that $f_3 = d_3 + e_3$ will be linearly independent of the other f_i.

c. The codeword f_2 must avoid the hyperplane $\langle f_1, f_3, \ldots, f_{r+3}\rangle$ and the coset $a_3 + \langle c_3 + d_2, b_3 + e_2, a_4 + b_4 + c_4, \ldots, a_{r+3} + b_{r+3} + c_{r+3}\rangle$. Since both of these are hyperplanes, we need to know that they are not the same hyperplane. This can be done if we make a good choice of e_2. This choice is the reason that we did not write the basis in the most general way possible. Lemma 1.1 helps with making the choices.

4. This idea can be generalized to higher order forbidden subgroups. For example, if we want to do this for a forbidden subgroup that is elementary abelian of order 16, we need to use a basic block with 15 elements in it which include all possible elements of order 4. The subgroup H will be $Z_4^4 \times Z_2^{r+11}$, and the parameters will be $(2^{2r+22}, 16, 2^{2r+22}, 2^{2r+18})$ for abelian groups of rank $r+15$. This rank can be obtained through previously mentioned methods (start with a $(2^{2r+22}, 2^{r+11}, 2^{2r+22}, 2^{r+11})$ and contract by a subgroup of order 2^{r+7} yielding a group of rank $2r+22-(r+7) = r+15$).

References

1. K. T. Arasu and S. Sehgal, Some new difference sets, *J. Comb. Th., Ser. A*, Vol. 69 (1995), pp. 170–172.
2. J. A. Davis, Construction of relative difference sets in p-groups, *Discrete Mathematics*, Vol. 103, (1992) pp. 7–15.
3. J. E. H. Elliot and A. T. Butson, Relative difference sets, *Illinois J. Math*, Vol 10, (1966) pp. 517–531.
4. R. Hill, A first course in coding theory, in *Oxford Applied Mathematics and Computing Science Series*, Oxford University Press, New York (1993).
5. D. Jungnickel, On automorphism groups of divisible designs, *Can. J. Math*, Vol. 34, (1982) pp. 257–297.
6. 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. 57–72.
7. A. Pott, A survey on relative difference sets. In K. T. Arasu et al., editors, *Groups, Difference Sets, and the Monster*, pp. 195–232, de Gruyter, Berlin-New York, 1996.
8. A. Pott, On the structure of abelian groups admitting divisible difference sets, *J. Comb. Th., Ser. A*, Vol. 65, (1994) pp. 202–213.
9. R. J. Turyn, Character sums and difference sets, *Pacific J. Math.*, Vol 15, (1965) pp. 319–346.