Arab J Math (2013) 2:103–114
DOI 10.1007/s40065-012-0055-9

RESEARCH ARTICLE

Jordan D. Webster

Reversible difference sets with rational idempotents

Received: 28 March 2012 / Accepted: 8 October 2012 / Published online: 26 October 2012

Abstract Reversible difference sets have been studied extensively by many people. Dillon showed that reversible difference sets existed in groups $(C_{2^r})^2$ and C_4. Davis and Polhill showed the existence of DRAD difference sets in the groups $(C_{2^r})^2$ for $r \geq 2$ and also for the group C_4. This paper gives a construction technique utilizing character values, rational idempotents, and tiles to produce both reversible and DRAD Hadamard difference sets in the group $C_{2^r} \times C_{2^r}$ for $r \geq 2$ and in C_4. We also show necessary conditions for both reversible and DRAD difference sets in abelian 2-groups.

Mathematics Subject Classification 05B10

الملخص

تمت دراسة مجموعات الفرْق القابلة للعكس بشكل مكثف من قبل العديد من الباحثين. بيَّن دِلون أن مجموعات الفرْق القابلة للعكس موجودة للزمر $(C_{2^r})^2$ وَ C_4. أثبت ديفيدز وَبولهل وجود مجموعات فرْق DRAD في الزمر $(C_{2^r})^2$ حيث $r \geq 2$ وكذلك للزمرة C_4. تعطي هذه الورقة تقنية بناء تستخدم قيم السمة، والجامدات النسبية، ووحدات البناء لإنتاج كل من مجموعات فرْق هدامارد قابلة للعكس وَ DRAD في الزمر $C_{2^r} \times C_{2^r}$ حيث $r \geq 2$ وفي C_4. نثبت أيضاً شروطاً ضرورية لكل من مجموعات فرْق قابلة للعكس وَ DRAD في زمر-2 الأبيلية.

1 Introduction

Let G be a group of order v written multiplicatively and let D be a k-subset of G. We say that D is a (v, k, λ) *difference set* in G if each nonidentity element of G appears exactly λ times in the multiset $\{d_1 d_2^{-1} : d_1, d_2 \in D\}$. A Hadamard (or Menon) difference set is a difference set with parameters $(4m^2, 2m^2 - m, m^2 - m)$ for some $m \in \mathbb{N}$.

We work in the group ring $\mathbb{C}[G]$. This is the ring of all formal sums $\sum_{g \in G} a_g g$ where each $a_g \in \mathbb{C}$. The a_g's are known as the coefficients of the group elements. Addition in this group ring is done linearly and multiplication happens both in $\mathbb{C}$ and by the operation of the group. The support of a group ring element is the set of group elements with nonzero coefficients. We say that a group ring element X has been shifted by g if it is multiplied by g. This is due to the shift in support of the elements X and gX. For more on group rings and their applications to difference sets see [9], [12], or [13].

Let $S = \{s_1, s_2, \ldots, s_n\}$ be a multiset containing elements of G. We write $S = \sum_{k=1}^{n} s_k$ to be the group ring element associated with the multiset S. This abuses the notation of S, but allows one to use these objects interchangeably and think of a set (or multiset) as an element of the group ring. Another convenient notation

J. D. Webster (✉)
Mid Michigan Community College Harrison, Harrison, MI, USA
E-mail: jdwebster@midmich.edu

is the notation of $S^{(-1)}$. As a set, this corresponds to the set of all group elements whose inverses are in S. This notation may be generalized to all elements of the group ring $\mathbb{C}[G]$. If $A = \sum_{g\in G} a_g g$, then define $A^{(-1)} = \sum_{g\in G} a_g g^{-1}$. In particular $D^{(-1)} = \sum_{d\in D} d^{-1}$.

When working with Hadamard difference sets, we can use the "Hadamard difference set transform." If D is a (v, k, λ) difference set, then the group ring element $\widehat{D} = G - 2D$ is the Hadamard difference set transform of D. The existence of the Hadamard difference set transform of a difference set is equivalent to the existence of the difference set itself. In this paper, we work exclusively with the Hadamard difference set transforms of difference sets. For this reason, in the remainder of the paper we use the terminology "difference set" for $\widehat{D} = G - 2D$, and use the terminology "(0,1)-difference set" to describe D. We note here that $\widehat{D}^{(-1)} = \widehat{D^{(-1)}}$.

Theorem 1.1 *Let G be a group of order $4m^2$ and let $\widehat{D}$ be a group ring element of $\mathbb{C}[G]$. The group ring element $\widehat{D}$ is a $(4m^2, 2m^2 - m, m^2 - m)$ difference set if and only if $\widehat{D}\widehat{D}^{(-1)} = 4m^2$ and $\widehat{D}$ has coefficients of ± 1.*

This theorem is a corollary of Turyn's classical theorem in [15]. The theorem does not work if the order of G is not a square.

A difference set $\widehat{D}$ is said to be reversible if $\widehat{D}^{(-1)} = \widehat{D}$. More generally, a group ring element X is reversible if $X^{(-1)} = X$. Reversible difference sets have been extensively studied due to their connection with multipliers. Dillon's construction in [5] gave reversible difference sets in $(C_{2^r})^2$ for $r \geq 1$. For more information on reversible difference sets see [8].

DRAD difference sets are a more recent idea. The term DRAD comes from their connection to doubly regular asymmetric digraphs as shown in [7]. These difference sets also can create nonsymmetric imprimitive association schemes as seen in [3]. The difference set $\widehat{D}$ is a DRAD difference set in a group, G, of order $4m^2$ if $\widehat{D} + \widehat{D}^{(-1)} = 2N$ where N is a subgroup of order $2m$. The subgroup N is called the forbidden subgroup of $\widehat{D}$ and is forced to have size $2m$. The (0,1) difference set D, is DRAD if $D \cap D^{(-1)} = \emptyset$, $D \cap N = \emptyset$, and $D + D^{(-1)} + N = G$. Davis and Polhill showed how to create DRAD difference sets in the groups C_4 and $(C_{2^r})^2$ for $r \geq 2$ [3]. They also showed that direct products of groups with DRAD and reversible difference sets contained DRAD difference sets.

We say that a group ring element X is *skew-symmetric* if $X^{(-1)} = -X$. DRAD difference sets can be thought of as a combination of a skew-symmetric element $\widehat{D} - N$ added to a subgroup N of order $2m$. Since N is a subgroup, it is reversible.

2 Characters and idempotents

A character of a group is a homomorphism from the group to the set of complex numbers. One can consult [6] and [10] for information on characters. Let χ be a character on G. The character $\chi : G \to \mathbb{C}$ is a group homomorphism, but we also let χ represent the $\mathbb{C}$-algebra homomorphism given by extending the group homomorphism linearly on $\mathbb{C}[G]$, $\chi(\sum_{g\in G} a_g g) = \sum_{g\in G} a_g \chi(g)$. This allows us to talk about characters of the group ring $\mathbb{C}[G]$.

Denote G^* as the set of all characters of G. If G is abelian, G^* is the *dual group* of G. The dual group forms a group under multiplication ($\chi\phi(g) = \chi(g)\phi(g)$), and is isomorphic to G when G is abelian. The identity element of the dual group is the character that maps every element of the group to the identity. This character is known as the *principal character*. All other characters are nonprincipal.

The use of characters applied to difference sets was first shown to be useful in [14]. Many others have used character theory to advance their research in the area of difference sets. One of the critical facts comes in the following theorem. This theorem is a corollary of Turyn's original statement.

Theorem 2.1 *Let G be an abelian group of order $4m^2$. A group ring element $\widehat{D}$ with coefficients of ± 1, is a $(4m^2, 2m^2 - m, m^2 - m)$ difference set in G if and only if*

$$\chi(\widehat{D})\chi(\widehat{D}^{(-1)}) = 4m^2$$

for each character $\chi \in G^*$.

As a consequence of the above theorem, $\chi(\widehat{D})$ is a complex number which has modulus $2m$ for each character $\chi \in G^*$. Moreover, $\chi(\widehat{D}^{(-1)}) = \chi(\widehat{D})^{-1}$ is the complex conjugate of $\chi(\widehat{D})$. This includes all nonprincipal characters and the principal character. We extensively make use of this fact to construct our difference sets.

From the definitions of reversible and DRAD difference sets, we immediately have two corollaries of this theorem.

Corollary 2.2 *Let $\widehat{D}$ be a difference set in an abelian group of order $4m^2$. The difference set $\widehat{D}$ is a reversible difference set if and only if $\chi(\widehat{D}) = \pm 2m$ for each $\chi \in G^*$.*

Corollary 2.3 *Let $\widehat{D}$ be a difference set in an abelian group of order $4m^2$. The difference set $\widehat{D}$ is a DRAD difference set with forbidden subgroup N if and only if $\chi(\widehat{D}) = \pm 2mi$ for every nonprincipal character on N and $\chi(\widehat{D}) = 2m$ for every principal character on N.*

Proof We know that for all difference sets $\chi(\widehat{D})\chi(\widehat{D}^{(-1)}) = 4m^2$. By the definition of DRAD difference sets $\widehat{D}^{(-1)} = 2N - \widehat{D}$ so we must have $\chi(\widehat{D})\chi(-\widehat{D} + 2N) = 4m^2$. If χ is nonprincipal on N then $\chi(N) = 0$ and we have $-\chi(\widehat{D})\chi(\widehat{D}) = 4m^2$. This means that $\chi(\widehat{D}) = \pm 2mi$.

If χ is principal on N, then $\chi(N) = 2m$. This means that the equation $-\chi(\widehat{D})\chi(\widehat{D}) + 2\chi(\widehat{D})\chi(N) = 4m^2$ becomes $-\chi(\widehat{D})^2 + 4m\chi(\widehat{D}) = 4m^2$. Solving the equation for $\chi(\widehat{D})$ forces $\chi(\widehat{D}) = 2m$. □

In this paper, we use characters to form a new basis for the group ring $\mathbb{C}[G]$. The standard basis of $\mathbb{C}[G]$ is the set $\{g : g \in G\}$. This is not the only basis for $\mathbb{C}[G]$. If G is abelian, then the following elements of $\mathbb{C}[G]$ form a basis:

$$e_\chi = \frac{1}{|G|}\sum_{g \in G} \chi(g)g^{-1} = \frac{1}{|G|}\sum_{g \in G} \overline{\chi(g)}g.$$

The elements e_χ are *primitive idempotents* of the group ring $\mathbb{C}[G]$. These are explained in detail in [4]. One important fact is that if χ and χ' are two characters of an abelian group G, then $\chi(e_{\chi'}) = \delta_{\chi\chi'}$ where $\delta_{\chi\chi'}$ represents the Kronecker delta function. The orthonormality gives that $\{e_\chi : \chi \in G^*\}$ is an orthonormal basis for $\mathbb{C}[G]$ when G is abelian.

Each group ring element has a unique representation as a linear combination of basis elements. If $X \in \mathbb{C}[G]$, then we wish to obtain the coefficients of the basis elements. Write $X \in \mathbb{C}[G]$ as $X = \sum_{\chi \in G^*} x_\chi e_\chi$. If we apply a character χ' to both sides of the equation $X = \sum_{\chi \in G^*} x_\chi e_\chi$, we find that $\chi'(X) = \chi'(x_\chi)$. So each element of the group ring may be uniquely written as

$$X = \sum_{\chi \in G^*} \chi(X)e_\chi.$$

Due to the uniqueness of coefficients on the basis elements, we must have that if $\chi(X) = \chi(Y)$ for every character $\chi \in G^*$, then $X = Y$. The $\chi(X)$ are all complex numbers, but we may wish to use group ring elements as coefficients rather than complex numbers. We do not need to limit ourselves to using $\chi(X)$ as the coefficient of e_χ. As shown in [4], if $A_\chi \in \mathbb{Z}[G]$ with $\chi(A_\chi) = \chi(X)$, then we may use $\chi(X)$ and A_χ interchangeably in the sum $X = \sum_{\chi \in G^*} \chi(X)e_\chi$.

The element A_χ is known as a χ-alias for the element X, but a χ-alias may not be unique. There may be many group ring elements which can be χ-aliases for X. In this paper, we will require aliases be from $\mathbb{Z}[G]$. We say that a χ-alias, A, has modulus n if $|\chi(A)| = n$. Let G be an abelian group of order $4m^2$. If $\widehat{D}$ is a group ring element with coefficients of ± 1, and $\widehat{D} = \sum_{\chi \in G^*} A_\chi e_\chi$ where $|\chi(A_\chi)| = 2m$, then $\widehat{D}$ is a difference set in G.

If we further require that $\chi(A_\chi) = \pm 2m$ for each character in G^*, then we know that $\widehat{D}$ is reversible. If we require that $\chi(A_\chi) = \pm 2mi$ for each nonprincipal character on a subgroup N of order $2m$, and require that each principal character on N has $\chi(A_\chi) = 2m$, then $\widehat{D}$ is a DRAD difference set with forbidden subgroup N.

3 Rational idempotents

The idempotents e_χ often have complex numbers as coefficients on group elements. The difference set $\widehat{D}$ has ± 1 as coefficients of group elements. If we let our aliases be from $\mathbb{Z}[G]$, they also have coefficients in $\mathbb{Z}$. In this section, we show how we may combine idempotents to obtain elements with rational coefficients.

Characters send group elements to roots of unity. We denote roots of unity by $\zeta_n = e^{\frac{2\pi i}{n}}$. This implies that every character sends elements of the group ring $\mathbb{Z}[G]$ to elements of a ring $\mathbb{Z}[\zeta_m]$ for some $m \in \mathbb{N}$. This is a ring inside the field $\mathbb{Q}(\zeta_m)$. Due to the Galois theory of this field, if our aliases are from $\mathbb{Z}[G]$, then we can assume that primitive idempotents whose characters have the same kernel also have the same aliases. Therefore, we add together primitive idempotents whose characters have the same kernel.

We denote $[e_\chi]$ (or $[\chi]$) as the sum of all primitive idempotents whose characters have the same kernel as χ. The group ring element $[e_\chi]$ is an idempotent by the orthogonality relations of the primitive idempotents. By the Galois theory, this idempotent must have rational coefficients on group elements. Thus, $[e_\chi]$ is known as a *rational idempotent*.

If χ_1 and χ_2 have the same kernel, then it is clear that $[e_{\chi_1}] = [e_{\chi_2}]$. While the number of primitive idempotents in the basis of $\mathbb{C}[G]$ is the size of the group G, the number of rational idempotents is the number of distinct kernels of the characters in G^*. Let the equivalence class of χ be $(\chi/\sim)$ and let the set of all equivalence classes be $(G^*/\sim)$. By Theorem 2.1, we have the following theorem.

Theorem 3.1 *Let G be an abelian group of order $4m^2$. If $\widehat{D} = \sum_{(\chi/\sim)\in(G^*/\sim)} Y_\chi[e_\chi]$ has group element coefficients of 1 and -1 and also has the property that $|\chi(Y_\chi)| = 2m$ for all $\chi \in G^*$, then $\widehat{D}$ is a difference set in G.*

If we further make $\chi(Y_\chi) = \pm 2m$ for every Y_χ, then $\widehat{D}$ is reversible. To ensure a DRAD difference set, we require $\chi(Y_\chi) = \pm 2mi$ for all nontrivial characters on a subgroup N of order $2m$ and $\chi(Y_\chi) = \pm 2m$ for all trivial characters on N. One may check that these requirements are both necessary and sufficient for DRAD and reversible sets in abelian groups of order $4m^2$.

4 Tiles

We keep track of the character values of an object by keeping track of the aliases on the rational idempotents. Define the *dual support* of a group ring element to be the set of characters which are nonzero on that element. The dual support of a difference set covers the dual group. Also the support of a difference set covers the group since the coefficient on each group element is ± 1. We wish to simultaneously know the dual support and the support of a group ring element. Furthermore, since every coefficient of a difference set is ± 1, we wish to make objects with coefficients of 1, 0, and -1.

Definition 4.1 Let G be an abelian group of order $4m^2$. An element $T \in \mathbb{Z}[G]$ is a *tile* of G if the coefficients of T are 1, 0, and -1 and for any character $\chi \in G^*$, either $\chi(T) = 0$ or $|\chi(T)| = 2m$.

Any Hadamard difference set is itself a tile with support equal to G and dual support equal to G^*. Any subgroup H of order $2m$ in an abelian group G of order $4m^2$ is a tile of G. The dual support of H is the set of characters that are principal on H. The tiles that we concern ourselves with are those created with rational idempotents. Any group ring element which is a sum of rational idempotents with aliases of modulus $2m$ with coefficients in the set $\{1, 0, -1\}$ is a tile.

If T is a tile of G and g is an element of G, then $-T$ and gT are also tiles of G. Sums of tiles with distinct supports and made with different rational idempotents are tiles. We create tiles using rational idempotents with aliases of modulus $2m$ and add them together so that the total support is the entire group. If this is the case, then we have created a difference set.

This definition of tiles is similar to the definition of building blocks given in [2]. The similarities are that they are specific group ring elements with specific character values. However, there are some differences. Most notably, we wish to add tiles in order to cover every element of G with coefficients of ± 1. Building blocks do not cover G when added to create (0, 1)-difference sets. Also, if we keep track of aliases on the rational idempotents made to create a tile, we do not need to check character values after we have made the difference set. This means that if we have tiles made from rational idempotents with the correct aliases and we add them to create an element which covers G, then we have a difference set. When using building blocks, one must continually check that character values are correct. So the advantage of using rational idempotents to make tiles is that after we get tiles, we only need to check that they have the correct support.

Tiles are group ring elements so tiles can be reversible or skew-symmetric. A DRAD difference set is a sum of a skew-symmetric tile $\widehat{D} - N$ with a reversible tile N. A reversible difference set is itself a reversible tile. The sum of reversible tiles with disjoint support is reversible and the sum of the skew-symmetric tiles with disjoint support is skew-symmetric.

5 The idempotents in $C_{2^r} \times C_{2^r}$

We now build the notation used in the rest of the paper. Denote the direct product of two cyclic groups of order 2^r by $C_{2^r} \times C_{2^r} = (C_{2^r})^2 = \langle x, y : x^{2^r} = y^{2^r} = [x, y] = 1\rangle$. For the remainder of this paper, we assume we are in this group for some $r \in \mathbb{N}$. The character and rational idempotent notation is the following:

- $\chi_{i,j}$ represents the character which maps x to $\zeta_{2^r}^i$ and y to $\zeta_{2^r}^j$.
- With each character $\chi_{i,j}$ we associate the idempotent $e_{i,j}$.
- The rational idempotent $[i, j]$ is the rational idempotent containing idempotent $e_{i,j}$.

We may assume that any $\chi_{i,j}$ alias for $\widehat{D}$ must be $2^r g$ for some $g \in G$. We wish to build reversible tiles and skew-symmetric tiles. This requires that $\chi_{i,j}(g) = \pm 1$ for reversible tiles or $\chi_{i,j}(g) = \pm i$ for skew-symmetric tiles if $2^r g$ is the alias on the rational idempotent $[i, j]$.

The rational idempotent associated with character χ may be written as $c(1-g)(\ker(\chi))$ where $c \in \mathbb{Q}$ and $g^2 \in \ker(\chi)$ but $g \notin \ker(\chi)$. Since each alias is of the form $2^r g$, we write rational idempotents having already been multiplied by 2^r. All rational idempotents fall into one of the following situations.

$$\text{The trivial rational idempotent is } 2^r[2^r, 2^r] = \frac{1}{2^r}(\langle x\rangle\langle y\rangle)$$

$$\text{For } r \geq i \geq 1 \text{ and } 1 \leq n \leq 2^i,\ 2^r[2^{r-i}, n2^{r-i}] = \frac{1}{2^{r-i+1}}(1 - x^{2^{i-1}})(\langle x^{-n}y\rangle\langle x^{2^i}\rangle)$$

$$\text{For } r \geq i \geq 1 \text{ and } 1 \leq n \leq 2^i,\ 2^r[n2^{r-i}, 2^{r-i}] = \frac{1}{2^{r-i+1}}(1 - y^{2^{i-1}})(\langle xy^{-n}\rangle\langle y^{2^i}\rangle)$$

We will add rational idempotents with aliases in such a way as to create irreducible tiles. These tiles are then added together to create first order tiles and these are added to create supertiles. Irreducible tiles, first order tiles and supertiles are tiles and their distinction is used to better keep track of supports. The supertiles satisfy the following.

- For $0 \leq k \leq \frac{r}{2} - 1$, S_k is created from idempotents $[i2^k, j2^k]$ so that at least one of i or j is odd. The support of S_k is the set $\langle x^{2^k}\rangle\langle y^{2^k}\rangle - \langle x^{2^{k+1}}\rangle\langle y^{2^{k+1}}\rangle$.
- If r is even, $S_{\frac{r}{2}}$ is created from rational idempotents of the form $[2^{\frac{r}{2}}i, 2^{\frac{r}{2}}j]$ such that $i, j \in \mathbb{Z}$. $S_{\frac{r}{2}}$ has support of $\langle x^{2^{\frac{r}{2}}}\rangle\langle y^{2^{\frac{r}{2}}}\rangle$.
- If r is odd, $S_{\frac{r-1}{2}}$ is created from rational idempotents of the form $[2^{\frac{r-1}{2}}i, 2^{\frac{r-1}{2}}j]$ such that $i, j \in \mathbb{Z}$. $S_{\frac{r-1}{2}}$ has support of $\langle x^{2^{\frac{r-1}{2}}}\rangle\langle y^{2^{\frac{r-1}{2}}}\rangle$.

If we have reversible tiles of this form, then we may take $\sum S_k$ to be the reversible difference set. While the construction of the last supertile varies slightly depending on whether r is even or odd, the constructions for the other supertiles do not depend on the parity of r.

To build the supertiles, we categorize rational idempotents by the orders of $\chi(x)$ and $\chi(y)$ in $\mathbb{C}$. We use the rational idempotents of the form $[n2^k, m2^k]$ where at least one of n or m is odd to create the supertile S_k for $0 \leq k \leq \frac{r-2}{2}$. Each S_k with $k \leq \frac{r}{2} - 1$ is created from three first order tiles. These are made by subdividing these rational idempotents of the form $[n2^k, m2^k]$ where at least one of n or m is odd into three forms.

The first form is $[2^k, m2^k]$ where m is odd. These rational idempotents create the reversible first order tile $F_{1,k}$ with support being the set $x^{2^k}y^{2^k}\langle x^{2^{k+1}}\rangle\langle y^{2^{k+1}}\rangle$.

The second form is $[2^k, m2^k]$ where m is even. These rational idempotents create the reversible first order tile $F_{2,k}$ with support being the set $y^{2^k}\langle x^{2^{k+1}}\rangle\langle y^{2^{k+1}}\rangle$.

The third form is $[m2^k, 2^k]$ where m is even. These rational idempotents create the reversible first order tile $F_{3,k}$ with support being the set $x^{2^k}\langle x^{2^{k+1}}\rangle\langle y^{2^{k+1}}\rangle$.

We categorize the rational idempotents in the above way for $k \leq \frac{r}{2} - 1$. The last supertiles are created from the rational idempotents not used in creating the other supertiles.

6 Example

To show how to accomplish the building of the difference sets in various groups, we start with an example from the group $C_4 \times C_4 = \langle x, y : x^4 = y^4 = [x, y] = 1\rangle$. This is the above group with $r = 2$. We begin by listing the rational idempotents of the group. Each has been multiplied by four for convenience.

$$4[0,0] = \frac{1}{4}\langle x\rangle\langle y\rangle,$$
$$4[0,2] = \frac{1}{4}(1-y)\langle x\rangle\langle y^2\rangle,\quad 4[2,2] = \frac{1}{4}(1-x)\langle x^2\rangle\langle xy\rangle,\quad 4[2,0] = \frac{1}{4}(1-x)\langle x^2\rangle\langle y\rangle,$$
$$4[0,1] = \frac{1}{2}(1-y^2)\langle x\rangle,\quad 4[1,1] = \frac{1}{2}(1-x^2)\langle xy^3\rangle,\quad 4[1,0] = \frac{1}{2}(1-x^2)\langle y\rangle,$$
$$4[2,1] = \frac{1}{2}(1-x)\langle xy^2\rangle,\quad 4[1,3] = \frac{1}{2}(1-x^2)\langle xy\rangle,\quad 4[1,2] = \frac{1}{2}(1-y)\langle yx^2\rangle$$

These rational idempotents will be combined in such a way as to make reversible tiles. The first tile is the supertile $S_1 = 4([0,0]+[0,2]+[2,0]+[2,2]) = \langle x^2\rangle\langle y^2\rangle$.

This reversible tile is made from the rational idempotents which do not send any element of the group to a primitive fourth root of unity. The other tiles are made from rational idempotents which send an element of the group to a primitive fourth root of unity. These rational idempotents create reversible first order tiles, $F_{1,0}$, $F_{2,0}$, and $F_{3,0}$ as follows.

$$F_{1,0} = 4x([0,1]+[2,1]) = x(1-y^2)\langle x^2\rangle$$
$$F_{2,0} = 4y([1,0]+[1,2]) = y(1-x^2)\langle y^2\rangle$$
$$F_{3,0} = 4xy([1,1]+[1,3]) = xy(1-x^2)(1-y^2)$$

Adding these three first order tiles creates the reversible supertile S_0. This supertile has support of $\langle x\rangle\langle y\rangle - \langle x^2\rangle\langle y^2\rangle$. When we let $\widehat{D} = S_0 + S_1$, we have created a reversible difference set in $C_4 \times C_4$.

When we change from reversible to DRAD difference sets, we leave S_1 as it is and multiply the reversible tiles $F_{1,0}$, $F_{2,0}$, and $F_{3,0}$ by appropriate group elements. Specifically we create the following three skew-symmetric tiles.

$$yF_{1,0} = 4xy([0,1]+[2,1]) = xy(1-y^2)\langle x^2\rangle$$
$$xyF_{2,0} = 4xy^2([1,0]+[1,2]) = x(1-x^2)\langle y^2\rangle$$
$$xF_{3,0} = F_{3,0} = 4x^2y([1,1]+[1,3]) = y(x^2-1)(1-y^2)$$

Adding these three skew-symmetric tiles creates the skew-symmetric tile S_1' with support equal to $\langle x\rangle\langle y\rangle - \langle x^2\rangle\langle y^2\rangle$. Letting $\widehat{D} = S_0 + S_1'$ gives us that $\widehat{D}$ is a DRAD difference set with forbidden subgroup $N = S_0 = \langle x^2\rangle\langle y^2\rangle$.

7 The supertile S_k for $k \le \frac{r}{2} - 1$

We assume again that we are in the general group $C_{2^r} \times C_{2^r}$ for arbitrary $r \in \mathbb{Z}$. In this section, we create S_k by creating each of the three first order tiles for $k \le \frac{r}{2} - 1$. We start by creating $F_{1,k}$.

There are a total of 2^{r-k-2} rational idempotents of the form $[2^k, n2^k]$ where n is odd. Recall that $2^r[2^k, n2^k] = \frac{1}{2^{k+1}}(1 - y^{2^{r-k-1}})(\langle x^{-n}y\rangle\langle y^{2^{r-k}}\rangle)$. The irreducible tiles are sums of 2^{k+1} rational idempotents. They are the following:

For $1 \le i \le 2^{r-2-2k}$,
$$T_i = 2^r x^{-(2i-1)2^k} y^{2^k} \sum_n [2^k, n2^k] \quad \text{where } n \equiv 2i-1 \bmod 2^{r-2k-1}.$$
$$T_i = x^{-(2i-1)2^k} y^{2^k}(1 - y^{2^{r-k-1}})(\langle x^{-(2i-1)2^{k+1}} y^{2^{k+1}}\rangle).$$

Lemma 7.1 *Each T_i is a reversible tile.*

Proof It is clear that each T_i is a tile since it is a sum of rational idempotents with alias $2^r g$ for some $g \in G$ and it has group ring coefficients in the set $\{1, 0, -1\}$. We only need to show that $2^r x^{-(2i-1)*2^k} y^{2^k}$ is a reversible alias for any rational idempotent in the sum $\sum_n [2^k, n2^k]$ where $n \equiv 2i-1 \bmod 2^{r-2k-1}$. This is true if $\chi_{2^k,n2^k}$ sends the alias to $\pm 2^r$ for any $n \equiv (2i-1) \bmod 2^{r-2k-1}$.

$$\chi_{2^k,n2^k}(2^r x^{-(2i-1)2^k} y^{2^k}) = 2^r \zeta_{2^r}^{-(2i-1)2^{2k}} \zeta_{2^r}^{n2^{2k}} = 2^r \zeta_{2^r}^{(n-2i+1)2^{2k}}.$$

The equivalence of n means that $n = (2i-1) + c2^{r-2k-1}$ for some $c \in \mathbb{Z}$. Therefore, we have $\chi_{2^k,n2^k}(2^r x^{-(2i-1)2^k} y^{2^k}) = 2^r \zeta_{2^r}^{(n-2i+1)2^{2k}} = 2^r \zeta_{2^r}^{(c2^{r-2k-1})2^{2k}} = \pm 2^r$.

This shows that each T_i is a reversible tile. □

Lemma 7.2 *T_i and T_j have disjoint support for $i \neq j$.*

Proof Assume that the support of tiles T_i and T_j have nonempty intersection. The support of T_i is $x^{-(2i-1)2^k} y^{2^k} (\langle x^{-(2i-1)2^{k+1}} y^{2^{k+1}} \rangle \langle y^{2^{r-k-1}} \rangle)$ and the support of T_j is $x^{-(2j-1)2^k} y^{2^k} (\langle x^{-(2j-1)2^{k+1}} y^{2^{k+1}} \rangle \langle y^{2^{r-k-1}} \rangle)$.

If these two sets are equal, then there exist integers m_1, m_2, and m_3 so that $x^{-(2i-1)2^k} y^{2^k} (x^{-(2i-1)2^{k+1}} y^{2^{k+1}})^{m_1} = x^{-(2j-1)2^k} y^{2^k} (x^{-(2j-1)2^{k+1}} y^{2^{k+1}})^{m_2} (y^{2^{r-k-1}})^{m_3}$.

We may assume that (WLOG) $m_1 \geq m_2$. This equivalence implies that $x^{(-2i+2j)2^k} (x^{(m_1(-2i+1)-m_2(-2j+1))2^{k+1}} y^{(m_1-m_2)2^{k+1}-m_3 2^{r-k-1}}) = 1$.

Examining the exponent of y gives us that $m_1 \equiv m_2 \bmod 2^{r-2k-2}$.

The exponent on x is $(j - i - 2im_1 + m_1 + 2jm_2 - m_2)2^{k+1} = (j - i - 2im_2 - 2i(m_1 - m_2) + 2jm_2 + m_1 - m_2)2^{k+1} = (2m_2 + 1)(j - i)2^{k+1} - (2i + 1)(m_1 - m_2)2^{k+1}$. Since this exponent must be a multiple of 2^r, since $m_1 \equiv m_2 \bmod 2^{r-2k-2}$, and since both $(2i + 1)$ and $(2m_2 + 1)$ are odd, we must have that $i \equiv j \bmod 2^{r-2k-2}$. Therefore, T_i and T_j have distinct support. □

Theorem 7.3 *$F_{1,k} = \sum_{i=1}^{2^{r-2-2k}} T_i$ is a reversible tile with support equal to the set $x^{2^k} y^{2^k} \langle x^{2^{k+1}} \rangle \langle y^{2^{k+1}} \rangle$.*

Proof It is clear that each tile T_i has support in the set $x^{2^k} y^{2^k} \langle x^{2^{k+1}} \rangle \langle y^{2^{k+1}} \rangle$ and support size of 2^r. The support size of $x^{2^k} y^{2^k} \langle x^{2^{k+1}} \rangle \langle y^{2^{k+1}} \rangle$ is $2^{2r-2k-2}$. By Lemmas 7.1 and 7.2, $F_{1,k}$ is the sum of 2^{r-2k-2} reversible tiles each with support size of 2^r and having disjoint support. Therefore, we must have that $F_{1,k}$ is a reversible tile with support equal to the set $x^{2^k} y^{2^k} \langle x^{2^{k+1}} \rangle \langle y^{2^{k+1}} \rangle$. □

Notice that $F_{1,k}$ was created with rational idempotents of the form $[2^k, n2^k]$ where n is odd. If we take the construction above, substitute the rational idempotents by $[2^k, (n+1)2^k]$, and multiply each rational idempotent by x^{-2^k}, then we have created $F_{2,k}$. This first order tile was created by rational idempotents $[2^k, m2^k]$ where m is even, is reversible, and has support of $y^{2^k} \langle x^{2^{k+1}} \rangle \langle y^{2^{k+1}} \rangle$. If we switch the roles of x and y in creating $F_{2,k}$, then we create reversible $F_{3,k}$ from rational idempotents $[m2^k, 2^k]$ where m is even and which has support $y^{2^k} \langle x^{2^{k+1}} \rangle \langle y^{2^{k+1}} \rangle$.

Due to the above arguments, $S_k = F_{1,k} + F_{2,k} + F_{3,k}$ is a reversible tile with support equal to the set $\langle x^{2^k} \rangle \langle y^{2^k} \rangle - \langle x^{2^{k+1}} \rangle \langle y^{2^{k+1}} \rangle$ for $0 \leq k \leq \frac{r}{2} - 1$.

8 Last supertile

The formulation of the last supertile depends on the parity of r. We first go through the case when r is even.

Since r is even, we have $\frac{r}{2}$ is an integer and we have created $\frac{r}{2}$ supertiles $S_0, \ldots, S_{\frac{r}{2}-1}$. Notice that these supertiles were formed with the rational idempotents $[i, j]$ so that $2^{\frac{r}{2}}$ does not divide both i and j.

When r is even, we simply add all the rational idempotents which have not been already used in creating the other S_k and multiply each by an alias of 2^r to create $S_{\frac{r}{2}}$. Specifically, let $S_{\frac{r}{2}} = 2^r \sum_{i,j \in \mathbb{Z}} [i2^{\frac{r}{2}}, j2^{\frac{r}{2}}]$.

Therefore, we have $S_{\frac{r}{2}} = \langle x^{2^{\frac{r}{2}}} \rangle \langle y^{2^{\frac{r}{2}}} \rangle$. This is clearly a reversible tile with support $\langle x^{2^{\frac{r}{2}}} \rangle \langle y^{2^{\frac{r}{2}}} \rangle$.

Theorem 8.1 *$\widehat{D_1} = \sum_{k=0}^{\frac{r}{2}} S_k$ is a reversible difference set in $C_{2^r} \times C_{2^r}$ when r is even.*

It suffices to say that each S_k is a reversible tile with support disjoint from the other $S_{k'}$ and the support of $\widehat{D}$ is $(C_{2^r})^2$. This construction satisfies the case when r is even.

The case where r is odd is more complex. We create $S_{\frac{r-1}{2}}$ by combining two irreducible tiles. We use idempotents of the form $[i2^{\frac{r-1}{2}}, j2^{\frac{r-1}{2}}]$ where i and j are in $\mathbb{Z}$. For convenience we separate the rational idempotents into four categories. The following table states the four categories of rational idempotents, the aliases for the four categories, the sum of all idempotents with the alias of each category, and the notation for the tile the category is in.

Rational idempotents	Alias	Sum	Tile used in
$[i2^{\frac{r-1}{2}}, j2^{\frac{r-1}{2}}]$: both i and j even	2^r	$\frac{1}{2}(1-x^{2^{\frac{r-1}{2}}})\langle x^{2^{\frac{r+1}{2}}}\rangle(1-y^{2^{\frac{r-1}{2}}})\langle y^{2^{\frac{r+1}{2}}}\rangle$	T_1^*
$[i2^{\frac{r-1}{2}}, j2^{\frac{r-1}{2}}]$: both i and j odd	2^r	$\frac{1}{2}\langle x^{2^{\frac{r-1}{2}}}\rangle\langle y^{2^{\frac{r-1}{2}}}\rangle$	T_1^*
$[i2^{\frac{r-1}{2}}, j2^{\frac{r-1}{2}}]$: i even and j odd	$2^r x^{2^{\frac{r-1}{2}}}$	$\frac{1}{2}\langle x^{2^{\frac{r-1}{2}}}\rangle(1-y^{2^{\frac{r-1}{2}}})\langle y^{2^{\frac{r+1}{2}}}\rangle$	T_2^*
$[i2^{\frac{r-1}{2}}, j2^{\frac{r-1}{2}}]$: i odd and j even	$2^r x^{2^{\frac{r-1}{2}}}$	$\frac{1}{2}(1-x^{2^{\frac{r-1}{2}}})\langle x^{2^{\frac{r+1}{2}}}\rangle\langle y^{2^{\frac{r-1}{2}}}\rangle$	T_2^*

The tiles are the following:

$$T_1^* = \langle x^{2^{\frac{r-1}{2}}} y^{2^{\frac{r-1}{2}}}\rangle\langle x^{2^{\frac{r+1}{2}}}\rangle$$
$$T_2^* = x^{2^{\frac{r-1}{2}}}\left(2\langle x^{2^{\frac{r-3}{2}}} y^{2^{\frac{r-3}{2}}}\rangle - \langle x^{2^{\frac{r-1}{2}}} y^{2^{\frac{r-1}{2}}}\rangle\right)\left(\langle x^{2^{\frac{r+1}{2}}}\rangle\right)$$

It should be quite obvious that T_1^* and T_2^* are reversible irreducible tiles and that the supertile $S_{\frac{r-1}{2}} = T_1^* + T_2^*$ is a reversible tile with support equal to the set $\langle x^{2^{\frac{r-1}{2}}}\rangle\langle y^{2^{\frac{r-1}{2}}}\rangle$.

Theorem 8.2 *$\widehat{D_1} = \sum_{k=0}^{\frac{r-1}{2}} S_k$ is a reversible difference set in $C_{2^r} \times C_{2^r}$ when r is odd.*

This construction satisfies the case when r is odd. Therefore, we have shown that reversible Hadamard difference sets exist in groups of the form $(C_{2^r})^2$ for any r.

9 DRAD Hadamard difference set in $(C_{2^r})^2$

We create a DRAD difference set in the group $(C_{2^r})^2$ with tiles for $r \geq 2$. We assume from this point on that $r \geq 2$. We utilize the work we have already done to find the DRAD difference set in $C_{2^r} \times C_{2^r}$.

In this group, an alias on a rational idempotent is skew-symmetric if it is mapped to $\pm 2^r i$ under the corresponding character. Since all tiles in the previous sections were reversible (had alias mapped to $\pm 2^r$), we simply need to multiply tiles already created by a group element which is mapped to $\pm i$ in order to have skew-symmetric tiles. For all but the last k, we make each reversible supertile S_k into a skew-symmetric supertile S'_k which has support equal to the support of S_k. Again the construction of the final tiles depends on the parity of r.

Recall $S_k = F_{1,k} + F_{2,k} + F_{3,k}$ for $k \leq \frac{r}{2} - 1$.

Lemma 9.1 *For $0 \leq k \leq \frac{r-1}{2} - 1$, $y^{2^{r-2+k}} F_{1,k}$ is a skew-symmetric tile, $x^{2^{r-2-k}} F_{2,k}$ is a skew-symmetric tile, and $x^{2^{r-2-k}} y^{2^{r-2-k}} F_{3,k}$ is a skew-symmetric tile.*

Proof We only need to check that each of these of $y^{2^{r-2+k}}$, $x^{2^{r-2+k}}$, and $x^{2^{r-2+k}} y^{2^{r-2+k}}$ are sent to $\pm i$ for each rational idempotent in the corresponding first order tile.

The tile $F_{1,k}$ is created with rational idempotents of the form $[2^k, n2^k]$ where n is odd. So $y^{2^{r-2-k}}$ is sent to $\zeta_{2^r}^{n2^k 2^{r-2-k}} = \zeta_{2^r}^{n2^{r-2}} = \zeta_4^n = \pm i$.

The proof for the other two first order tiles is similar. □

Proposition 9.2 *Let* $S'_k = y^{2^{r-2+k}} F_{1,k} + x^{2^{r-2-k}} F_{2,k} + x^{2^{r-2-k}} y^{2^{r-2-k}} F_{3,k}$. *Then for* $0 \leq k \leq \frac{r-2}{2}$, S'_k *is a skew-symmetric tile with support equal to*

$$\langle x^{2^k} \rangle \langle y^{2^k} \rangle - \langle x^{2^{k+1}} \rangle \langle y^{2^{k+1}} \rangle.$$

Proof From the previous proposition, we know that each of $y^{2^{r-2+k}} F_{1,k}, x^{2^{r-2-k}} F_{2,k}, x^{2^{r-2-k}} y^{2^{r-2-k}} F_{3,k}$ are skew-symmetric tiles. It suffices then to show the support of each $y^{2^{r-2+k}} F_{1,k}, x^{2^{r-2-k}} F_{2,k}$, and $x^{2^{r-2-k}} y^{2^{r-2-k}} F_{3,k}$.

We utilize a table to show how supports of the tiles are arranged. The original first order tiles, the original support, the new first order tile, and the new supports are listed both when $k = \frac{r-2}{2}$ and when $k \leq \frac{r-3}{2}$.

For $k \leq \frac{r-3}{2}$

Original first order tile	Original support	New first order tile	New support
$F_{1,k}$	$x^{2^k} y^{2^k} \langle x^{2^{k+1}} \rangle \langle y^{2^{k+1}} \rangle$	$y^{2^{r-2+k}} F_{1,k}$	$x^{2^k} y^{2^k} \langle x^{2^{k+1}} \rangle \langle y^{2^{k+1}} \rangle$
$F_{2,k}$	$y^{2^k} \langle x^{2^{k+1}} \rangle \langle y^{2^{k+1}} \rangle$	$x^{2^{r-2+k}} F_{2,k}$	$y^{2^k} \langle x^{2^{k+1}} \rangle \langle y^{2^{k+1}} \rangle$
$F_{3,k}$	$x^{2^k} \langle x^{2^{k+1}} \rangle \langle y^{2^{k+1}} \rangle$	$x^{2^{r-2-k}} y^{2^{r-2-k}} F_{3,k}$	$x^{2^k} \langle x^{2^{k+1}} \rangle \langle y^{2^{k+1}} \rangle$

For $k = \frac{r-2}{2}$

Original first order tile	Original support	New first order tile	New support
$F_{1,k}$	$x^{2^k} y^{2^k} \langle x^{2^{k+1}} \rangle \langle y^{2^{k+1}} \rangle$	$y^{2^{r-2+k}} F_{1,k}$	$x^{2^k} \langle x^{2^{k+1}} \rangle \langle y^{2^{k+1}} \rangle$
$F_{2,k}$	$y^{2^k} \langle x^{2^{k+1}} \rangle \langle y^{2^{k+1}} \rangle$	$x^{2^{r-2+k}} F_{2,k}$	$x^{2^k} y^{2^k} \langle x^{2^{k+1}} \rangle \langle y^{2^{k+1}} \rangle$
$F_{3,k}$	$x^{2^k} \langle x^{2^{k+1}} \rangle \langle y^{2^{k+1}} \rangle$	$x^{2^{r-2-k}} y^{2^{r-2-k}} F_{3,k}$	$y^{2^k} \langle x^{2^{k+1}} \rangle \langle y^{2^{k+1}} \rangle$

This shows that S'_k has support equal to $\langle x^{2^k} \rangle \langle y^{2^k} \rangle - \langle x^{2^{k+1}} \rangle \langle y^{2^{k+1}} \rangle$ in all cases when $k \leq \frac{r-2}{2}$. □

We have successfully created skew-symmetric tiles S'_k for $k \leq \frac{r-2}{2}$. Now we create the last few tiles. For the even case, the creation of the last tile is previously done for us. We keep the supertile $S_{\frac{r}{2}}$ as the last tile when r is even.

Theorem 9.3 *If r is even, then* $\widehat{D} = S_{\frac{r}{2}} + \sum_{k=0}^{\frac{r-2}{2}} S'_k$ *is a DRAD difference set in* $(C_{2^r})^2$ *with forbidden subgroup equal to* $\langle x^{2^{\frac{r}{2}}} \rangle \langle y^{2^{\frac{r}{2}}} \rangle$.

Proof We have created skew-symmetric supertiles S'_k with support equal to $\langle x^{2^k} \rangle \langle y^{2^k} \rangle - \langle x^{2^{k+1}} \rangle \langle y^{2^{k+1}} \rangle$ for $k \leq \frac{r-2}{2}$ and have the reversible supertile $S_{\frac{r}{2}} = \langle x^{2^{\frac{r}{2}}} \rangle \langle y^{2^{\frac{r}{2}}} \rangle$. Therefore, it is clear that $\widehat{D}$ is a DRAD difference set with forbidden subgroup $N = \langle x^{2^{\frac{r}{2}}} \rangle \langle y^{2^{\frac{r}{2}}} \rangle$. □

Now we create the DRAD difference set when r is odd and at least 3. This case is more complex. From earlier, we created a reversible supertile $S_{\frac{r-1}{2}}$ with shifts of the two reversible tiles

$$T_1^* = \langle x^{2^{\frac{r-1}{2}}} y^{2^{\frac{r-1}{2}}} \rangle \langle x^{2^{\frac{r+1}{2}}} \rangle$$
$$T_2^* = \left(2\langle x^{2^{\frac{r-3}{2}}} y^{2^{\frac{r-3}{2}}} \rangle - \langle x^{2^{\frac{r-1}{2}}} y^{2^{\frac{r-1}{2}}} \rangle \right) \left(\langle x^{2^{\frac{r+1}{2}}} \rangle \right)$$

Even though we have created a skew-symmetric supertile $S'_{\frac{r-3}{2}}$, we do not wish to use it in this form. We wish to interchange part of the support with support of T_2^*. We must deconstruct $F_{1,\frac{r-3}{2}}$ to accomplish this.

We added shifts of irreducible tiles in order to create $F_{1,\frac{r-3}{2}}$. These irreducible tiles were the following reversible tiles (previously they had different aliases):

$$T_1 = 2^r \sum_{n\equiv 1 \mod 4} \left[2^{\frac{r-3}{2}}, n2^{\frac{r-3}{2}}\right].$$

$$T_1 = (1 - y^{2^{\frac{r+1}{2}}})(\langle x^{-2^{\frac{r-1}{2}}} y^{2^{\frac{r-1}{2}}}\rangle\langle y^{2^{\frac{r+3}{2}}}\rangle).$$

$$T_2 = 2^r \sum_{n\equiv 3 \mod 4} \left[2^{\frac{r-3}{2}}, n2^{\frac{r-3}{2}}\right].$$

$$T_2 = (1 - y^{2^{\frac{r+1}{2}}})(\langle x^{2^{\frac{r-1}{2}}} y^{2^{\frac{r-1}{2}}}\rangle\langle y^{2^{\frac{r+3}{2}}}\rangle).$$

Notice that supports of T_2^*, T_1, and T_2 are all equal to $(\langle x^{2^{\frac{r-1}{2}}} y^{2^{\frac{r-1}{2}}}\rangle)(\langle y^{2^{\frac{r+1}{2}}}\rangle)$.

Proposition 9.4 *Denote* $S''_{\frac{r-3}{2}} = x^{2^{\frac{r-1}{2}}} F_{2,k} + x^{2^{\frac{r-1}{2}}} y^{2^{\frac{r-1}{2}}} F_{3,k} + x^{-2^{\frac{r-3}{2}}} y^{2^{\frac{r-3}{2}}} T_2^* + x^{2^{\frac{r-3}{2}}} y^{2^{\frac{r-3}{2}}} T_1 + x^{2^{\frac{r-1}{2}}} T_2$. *If r is odd and at least three, then $S''_{\frac{r-3}{2}}$ is a skew-symmetric tile with support equal to the set* $\langle x^{2^{\frac{r-3}{2}}}\rangle\langle y^{2^{\frac{r-3}{2}}}\rangle - \langle x^{2^{\frac{r-1}{2}}} y^{2^{\frac{r-1}{2}}}\rangle\langle x^{2^{\frac{r+1}{2}}}\rangle$.

Proof This proposition is true if each alias on the rational idempotent associated with character χ has $\chi(a_\chi) = \pm 2^r i$ and if the sum has correct support. One can easily check that all aliases have correct character values. We show support in the following table.

Original tile	Original support	New tile	New support
T_2^*	$x^{2^{\frac{r-3}{2}}}\langle x^{2^{\frac{r-1}{2}}} y^{2^{\frac{r-1}{2}}}\rangle\langle y^{2^{\frac{r+1}{2}}}\rangle$	$x^{-2^{\frac{r-3}{2}}} y^{2^{\frac{r-3}{2}}} T_2^*$	$y^{2^{\frac{r-3}{2}}}\langle x^{2^{\frac{r-1}{2}}} y^{2^{\frac{r-1}{2}}}\rangle\langle y^{2^{\frac{r+1}{2}}}\rangle$
T_1	$\langle x^{2^{\frac{r-1}{2}}} y^{2^{\frac{r-1}{2}}}\rangle\langle y^{2^{\frac{r+1}{2}}}\rangle$	$x^{2^{\frac{r-3}{2}}} y^{2^{\frac{r-3}{2}}} T_1$	$x^{2^{\frac{r-3}{2}}} y^{2^{\frac{r-3}{2}}}\langle x^{2^{\frac{r-1}{2}}} y^{2^{\frac{r-1}{2}}}\rangle\langle y^{2^{\frac{r+1}{2}}}\rangle$
T_2	$\langle x^{2^{\frac{r-1}{2}}} y^{2^{\frac{r-1}{2}}}\rangle\langle y^{2^{\frac{r+1}{2}}}\rangle$	$x^{2^{\frac{r-1}{2}}} T_2$	$x^{2^{\frac{r-1}{2}}}\langle x^{2^{\frac{r-1}{2}}} y^{2^{\frac{r-1}{2}}}\rangle\langle y^{2^{\frac{r+1}{2}}}\rangle$
$F_{2,\frac{r-3}{2}}$	$y^{2^{\frac{r-3}{2}}}\langle x^{2^{\frac{r-1}{2}}}\rangle\langle y^{2^{\frac{r-1}{2}}}\rangle$	$x^{2^{\frac{r-1}{2}}} F_{2,\frac{r-3}{2}}$	$y^{2^{\frac{r-3}{2}}}\langle x^{2^{\frac{r-1}{2}}}\rangle\langle y^{2^{\frac{r-1}{2}}}\rangle$
$F_{3,\frac{r-3}{2}}$	$x^{2^{\frac{r-3}{2}}}\langle x^{2^{\frac{r-1}{2}}}\rangle\langle y^{2^{\frac{r-1}{2}}}\rangle$	$x^{2^{\frac{r-1}{2}}} y^{2^{\frac{r-1}{2}}} F_{3,\frac{r-3}{2}}$	$x^{2^{\frac{r-3}{2}}}\langle x^{2^{\frac{r-1}{2}}}\rangle\langle y^{2^{\frac{r-1}{2}}}\rangle$

This table shows that we have the correct support for $S''_{\frac{r-3}{2}}$. □

Theorem 9.5 *If $r \geq 3$ is odd then $\widehat{D} = T_1^* + S''_{\frac{r-3}{2}} + \sum_{k=0}^{\frac{r-5}{2}} S'_k$ is a DRAD Hadamard difference set in $(C_{2^r})^2$ with forbidden subgroup* $\langle x^{2^{\frac{r-1}{2}}} y^{2^{\frac{r-1}{2}}}\rangle\langle x^{2^{\frac{r+1}{2}}}\rangle$.

The proof follows by the constructions of the supertiles. Therefore, a DRAD Hadamard difference set $\widehat{D}$ exists in $(C_{2^r})^2$ for any $r \geq 2$. We show how to create DRAD difference sets in direct products of these groups in the next section.

10 Product constructions using tiles

We have utilized tiles to keep track or both the support and dual support of groups. Tiles have nice properties when we take the direct product of two groups. If T_1 and T_2 are tiles in groups G and H of order $4m_1$ and $4m_2$, then $T_1 * T_2$ is a tile in the direct product $G \times H$. This follows from the definition of tiles and knowledge of characters acting on direct products of groups. As in Menon's product construction [11], reversibility is preserved when multiplying tiles. Also, if T_1 is reversible and T_2 is skew-symmetric then $T_1 * T_2$ is skew-symmetric.

Since a reversible difference set itself is a reversible tile, the direct products of two groups containing reversible difference sets is reversible. This result has been long established [11].

Theorem 10.1 *Let G and H be groups of order $4m_1$ and $4m_2$, respectively. If G has DRAD and reversible difference sets and H also has DRAD and reversible difference sets, then $G \times H$ has a DRAD difference set.*

Proof Let $\widehat{D_1}$ be a DRAD difference set in G with forbidden subgroup N_1 and let $\widehat{R_1}$ be a reversible difference set in G. Similarly let $\widehat{D_2}$ be a DRAD difference set with forbidden subgroup N_2 in H.

Define $\widehat{D} = N_1N_2 + \widehat{R_1}(\widehat{D_2} - N_2) + \widehat{N_2}(\widehat{D_1} - N_1)$. I claim that $\widehat{D}$ is a DRAD difference set with forbidden subgroup N_1N_2. Note that N_1, N_2, and $\widehat{R_1}$ are all reversible tiles and $\widehat{D_1} - N_1$ and $\widehat{D_2} - N_2$ are skew-symmetric tiles in the original groups G and H. From earlier results, N_1N_2 is a reversible tile (in fact a subgroup) in $G \times H$ and $\widehat{R_1}(\widehat{D_2} - N_2)$ and $\widehat{N_2}(\widehat{D_1} - N_1)$ are skew-symmetric tiles in $G \times H$. One can easily check that these tiles have disjoint support and their added support is the group $G \times H$. Therefore, $\widehat{D}$ is a DRAD difference set in $G \times H$. □

By the above theorem and the constructions of the reversible and DRAD difference sets in the previous sections, we are able to make a DRAD difference set in any group of the form $(C_{2^{r_1}} \times C_{2^{r_2}} \times \cdots \times C_{2^{r_n}})^2$ where each $r_i \geq 2$. One can easily check that in the group $C_4 = \langle x : x^4 = 1\rangle$, the group ring element $\widehat{D} = 1 - x + x^2 + x^3$ is a DRAD difference set and the element $\widehat{D'} = -1 + x + x^2 + x^3$ is a reversible difference set. This means that DRAD difference sets also exist in groups of the form $(C_{2^{r_1}} \times C_{2^{r_2}} \times \cdots \times C_{2^{r_n}})^2 \times C_4$ where each $r_i \geq 2$. This is the same result obtained by Davis and Polhill [3] using Galois rings and their own product construction. These are the first groups known to contain DRAD difference sets.

11 Nonexistence

We have created both DRAD and reversible difference sets in infinitely many groups. There are many known results on nonexistence of many types of difference sets in groups as well [8]. We provide two new nonexistence results concerning reversible and DRAD difference sets here. The first result explains why we require $r \geq 2$ when creating the DRAD difference set in $(C_{2^r})^2$.

Proposition 11.1 *Let G be a group of order $4m^2$. If $G = C_q \times H$ where q is not divisible by four, then G does not contain a DRAD difference set.*

Proof If a DRAD difference set, $\widehat{D}$, existed in G with forbidden subgroup N, then there must be some characters which act trivially on H but not on C_q or N. These characters must map group ring elements of $\mathbb{Z}[C_q]$ to $2m\zeta_4 = 2mi$. This cannot happen since characters must send group elements of C_q to either 1 or a complex number of order dividing q. Their sums with integer coefficients cannot add to $\pm i$. □

The second nonexistence result gives necessary conditions for both reversible and DRAD difference sets in abelian 2-groups. If G is an abelian 2-group, then we may write G as $C_{2^{k_0}} \times C_{2^{k_1}} \times \cdots \times C_{2^{k_n}} = C_{2^{k_0}} \times H$ where $k_0 \geq k_1 \geq \cdots \geq k_n$. Also, we may set the generators of $C_{2^{k_0}}, C_{2^{k_1}}, \ldots, C_{2^{k_n}}$ to be $x, y_1, \ldots, y_n$.

Proposition 11.2 *With the notation above, if we have $k_0 > k_1$ and $k_0 \geq 3$, then G does not contain a reversible difference set and does not contain a DRAD difference set.*

Proof With the notation as above, assume $k_0 > k_1$. The number of primitive idempotents sending x to a primitive 2^{k_0} root of unity is exactly the same as the number sending x to a nonprimitive root of unity. This is due to there being equal numbers of odd powers and even powers of $\zeta_{2^{k_0}}$.

To have a reversible difference set, aliases must be sent to $\pm 2^r$. If j_0 were odd, then $x^{j_0}y_1^{j_1}\cdots y_n^{j_n}$ would be sent to a primitive 2^{k_0} root of unity for any character sending x to a primitive 2^{k_0} root of unity. This forces aliases of rational idempotents sending x to a primitive 2^{k_0} to be $2^r x^{j_0}y_1^{j_1}\cdots y_n^{j_n}$ where j_0 is even. Therefore the idempotents sending x to a primitive 2^{k_0} root of unity along with each alias must combine to form a tile which has support $\langle x^2\rangle \times H$. Idempotents sending x to a primitive root of unity also have the property that g and $gx^{2^{k_0-1}}$ have opposite coefficients. So sums of these idempotents with aliases have the same property. In particular, this forces $x^{2^{k_0-2}}$ and $x^{3*2^{k_0-2}}$ to have opposite coefficients in the difference set. This contradicts reversibility.

To create a DRAD difference set, we need aliases which are sent to $\pm 2^r$ or $\pm 2^r i$. This also forces the idempotents sending x to a primitive 2^{k_0} root of unity along with each alias to combine to form a tile which has support $\langle x^2\rangle \times H$. This means that the identity element, 1, and $x^{2^{k_0-1}}$ have opposite coefficients. This forces either the identity or $x^{2^{k_0-1}}$ to be outside of the forbidden subgroup. To be DRAD elements of order two must be in the forbidden subgroup. This contradicts being DRAD. □

Although this paper has ruled out existence of DRAD difference sets in many groups, there are many groups where DRAD difference sets may be possible. In abelian 2-groups, we have given necessary conditions for reversibility and DRAD. An immediate question that arises is if these necessary conditions are also sufficient. Furthermore, in known cases DRAD difference sets always exist in groups where reversible difference sets also exist. However, reversible difference sets exist in many groups where DRAD difference sets cannot [1]. This author conjectures that if a DRAD difference set exists in an abelian group, then a reversible difference set also exists in that group. We would like to see if the techniques of this paper would apply to other groups.

Acknowledgments This work was done as partial fulfillment of a Ph.D. at Central Michigan University under the guidance of Ken W. Smith. The author is extremely grateful for the help and support of both Ken W. Smith and Central Michigan University.

References

1. Davis, J.; Jebwab, J.: A survey of Hadamard difference sets. In: Arasu, K.T.; Dillon, J.; Harada, K.; Sehgal, S.K.; Solomon, R. (eds.) Groups, Difference Sets and the Monster, pp. 145–156. deGruyter Verlag, Berlin-New York (1996)
2. Davis, J.; Jedwab, J.: A unifying construction for difference sets. J. Comb. Theory Ser. A **80**(1), 13–78 (1997)
3. Davis, J.A.; Polhill, J.B.: Difference set constructions of DRAD's and association schemes. J. Combin. Theory Ser. A. **117**, 598–605 (2010)
4. Davis, J.A.; Smith, K.W.: Rational idempotents in the integral group ring and their applications (2007, preprint)
5. Dillon, J.: Difference sets in 2-groups. In: Finite Geometric and Combinatorial Designs: Proceedings of the AMS, pp. 65–72 (1990)
6. Dummit, D.S.; Foote, R.M.: Abstract Algebra. Prentice Hall, Englewood Cliffs (1991)
7. Ito, N.: Automorphism groups of DRAD's. In: Cheng, K.N.; Leong, Y.K. (eds.) Group Theory: Proceedings of the Singapore Group Theory Conference. de Gruyter (1987)
8. Jungnickel, D.; Pott, A.; Smith, K.: Difference sets, Chap. 18. In: Colburn, C.J.; Dinitz, J.H. (eds.) CRC Handbook of Combinatorial Designs, 2nd edn. CRC Press, Boca Raton (2007)
9. Lander, E.S.: Symmetric Designs: An Algebraic Approach. London Mathematical Society Lecture Note Series, vol. 74. Cambridge University Press, Cambridge (1983)
10. Lederman, W.: Introduction to Group Characters. Cambridge University Press, Cambridge (1977)
11. Menon, P.K.: On difference sets whose parameters satisfy a certain relation. Proc. Am. Math. Soc. **13**, 739–745 (1962)
12. Milies, S.K.; Sehgal, C.P.: An Introduction to Group Rings. Kluwer Academic Publishers, Boston (2002)
13. Schmidt, B.: Lecture Notes in Mathematics: Characters and Cyclotomic Fields in Finite Geometry. Springer, New York (2002)
14. Turyn, R.J.: Character sums and difference sets. Pac. J. Math. **15**, 319–346 (1965)
15. Turyn, R.J.: A special class of Williamson matrices and difference sets. J. Combin. Theory Ser. A **36**, 111–115 (1984)