...

Ken W. Smith* and Tahseen Rabbani

Nonabelian Orthogonal Building Sets

Extending Orthogonal Building Sets to Nonabelian Groups

DOI ..., Received ...; accepted ...

Abstract: We examine recent construction techniques of Hadamard difference sets in 2-groups, looking for an extension of orthogonal building sets to nonabelian groups.

Keywords: difference sets, Hadamard difference sets, extended building set, nonabelian difference sets

PACS: ...

Communicated by: ...
Dedicated to ...

1 Difference Sets in Hadamard 2-groups

Definition 1.1. *The subset D of a group G of order v is a* **difference set** *with parameters (v, k, λ) if the size of D is k and for all nonidentity elements g in G, the equation $d_1 d_2^{-1} = g$ has exactly λ solutions (d_1, d_2), $d_1, d_2 \in D$.*

In this paper, we focus on difference sets with parameters $(2^{2d+2}, 2^{2d+1} \pm 2^d, 2^{2d} \pm 2^d)$ existing in 2-groups. Difference sets with parameters $(4N^2, 2N^2 \pm N, N^2 \pm N)$ are often called "Hadamard" difference sets because of their connections with Hadamard matrices of order $4N^2$. Many of the concepts in this paper are an extension of those appearing in [5] and [4].

The recent conclusion of a search for difference sets in groups of order 256, [4], included a generalization of covering extended building sets to the concept of orthogonal building sets (OBS) in abelian 2-groups. In this paper we seek

***Corresponding author: Ken W. Smith,** Sam Houston State University, Huntsville TX, kenwsmith54@gmail.com
Tahseen Rabbani, University of Maryland, trabbani@math.umd.edu

generalizations of orthogonal building sets to nonabelian groups, building on the concepts from that paper.

1.1 Recent contributions to difference sets in 2-groups

In 1990, as part of the Director's Summer Program at the National Security Agency (NSA), a small team of undergraduate students, working under the direction of John Dillon, used the software package *CAYLEY* to complete a survey of groups of order 64, identifying those groups which had a $(64, 28, 12)$ difference set. Ken Smith, beginning a sabbatical year at the NSA, was also involved in this project. By August of 1990 it had been determined that 259 of the 267 groups of order 64 had difference sets. Those eight groups that did not have a difference set were ruled out by a result of Turyn and Dillon ([12], [6]) that prohibited difference sets in a group of order 2^{2d+2} if the group had a cyclic or dihedral image of order 2^{d+3}.

In our search for difference sets in 2-groups, the next larger sets of groups to examine were the 56,092 groups of order 256. At that time, those groups were stored in a sequence of *CAYLEY* libraries and any serious investigation into those groups appeared to be beyond the computer capabilities of that time.

In August 2012, Dillon communicated that most of the groups of order 256 had a difference set, with the status open for only 724 groups. In 2013, Taylor Applebaum[1], then at the University of Richmond, successfully constructed a difference set in 643 groups containing a normal subgroup isomorphic to $C_4 \times C_4 \times C_2$ (of a possible 649). After that, a team of students, John Clikeman, Gavin McGrew, and Tahseen Rabbani, led by Jim Davis, successfully constructed a difference set in the remaining six groups with such a normal subgroup. This construction technique, using the concept of extended building sets from [5], left 75 groups still in doubt. Difference sets in those remaining groups were then found using a variety of ad-hoc techniques.

(The number of groups of order 1024 is 49,487,365,422. At this time there is no convenient library of these groups.)

1.2 Extended building sets

We review a few essential concepts relating to the extended building set construction. Let G be a finite group and S a subset of G. We identify S with the

1 now at Google

formal sum of its elements, so that $S := \sum_{s \in S} s$; this identification of a set with a group ring element is common in the study of difference sets.

If ϕ is an irreducible representation of G and $A = \sum_g a_g\ g$ an element in the group ring $\mathbb{C}[G]$, then $\phi(A) := \sum_g a_g \phi(g)$. We write $\mathrm{Irrep}(G)$ for the set of irreducible representations of G. If G is abelian then $\mathrm{Irrep}(G) = G^*$, the set of characters of G.

Definition 1.2. *A subset S of G has **modulus** m with respect to the character χ if $|\chi(S)| = m$.*

Definition 1.3. *The* **support** *of $A = \sum_g a_g\ g$ is the set of group elements g such that $a_g \neq 0$. The* **dual support** *of A is the set of irreducible representations ϕ such that $\phi(A) \neq 0$.*

Definition 1.4. *Elements $A, B \in \mathbb{C}[G]$ are* **orthogonal** *if their product is zero.*

There is a classical lemma relating difference sets to the modulus.

Lemma 1.5. *Let D be a k-element subset of an abelian group G of order v. D is a (v, k, λ) difference set in G if and only if D has modulus $\sqrt{k - \lambda}$ over all non-principal characters.*

Definition 1.6. *A subset B of G is a **building block** with modulus m if for every non-principal character χ on G, $\chi(B) = 0$ or m.*

Definition 1.7. *Let $a, t \in \mathbb{N}$, $m \in \mathbb{R}$. An $(a, m, t, \pm)$ **extended building set** (EBS) on a group G relative to a subgroup U is a set of t building blocks $\{B_1, B_2, \ldots, B_t\}$ with modulus m, such that $t-1$ blocks contain exactly a elements and one contains $a \pm m$ elements, determined by the fourth parameter, and such that for any non-principal character χ on U,*

1. *If χ is principal on U, there is only one B_i such that $\chi(B_i) \neq 0$, for $1 \leq i \leq t$.*
2. *If χ is non-principal on U, then $\forall i, \chi(B_i) = 0$.*

If, for every non-principal character of G, only one block has a nonzero character sum, then we call the EBS covering, abbreviated cov EBS.

Theorem 1.8. *Let G be a finite abelian group containing K as a subgroup with index t. For any $(a, m, t, \pm)$ cov EBS in K, there is a $(t|K|, at \pm m, at \pm m - m^2, m^2)$ difference set in G.*

Example 1.9. *In an abelian group of order 256, the above theorem tells us that one may lift a $(16, 8, 8, -)$ cov EBS in a subgroup isomorphic to $C_4^2 \times C_2$ up to a*

difference set in G. With presentation

$$K = C_4^2 \times C_2 = \langle x, y, z \mid x^4 = y^4 = z^2 = [x, y] = [x, z] = [y, z] = 1 \rangle,$$

the $(16, 8, 8, -)$ *cov EBS, written as elements of a group ring, are:*

$$\begin{aligned}
B_1 &= \langle x^2, y\rangle + x\langle x^2 z, y\rangle = [(1 + x^2) + x(1 + x^2 z)](1 + y)(1 + y^2)\\
B_2 &= \langle x^2, yz\rangle + x\langle x^2 z, yz\rangle = [(1 + x^2) + x(1 + x^2 z)](1 + yz)(1 + y^2)\\
B_3 &= \langle x, y^2 z\rangle + y\langle xy^2, y^2 z\rangle = [(1 + x) + y(1 + xy^2)](1 + y^2 z)(1 + x^2)\\
B_4 &= \langle xy, y^2 z\rangle + y\langle xy^3, y^2 z\rangle = (1 + x)(1 + y)(1 + y^2 z)(1 + x^2 y^2)\\
B_5 &= \langle x, z\rangle + y\langle xy^2, z\rangle = [(1 + x) + y(1 + xy^2)](1 + x^2)(1 + z)\\
B_6 &= \langle x^2, y^2, z\rangle = (1 + x^2)(1 + y^2)(1 + z)\\
B_7 &= \langle y, z\rangle + x\langle x^2 y, z\rangle = [(1 + y) + x(1 + x^2 y)](1 + y^2)(1 + z)\\
B_8 &= \langle xy, z\rangle + x\langle x^3 y, z\rangle = (1 + x)(1 + y)(1 + x^2 y^2)(1 + z)
\end{aligned}$$

Any character of K, other than the trivial representation, maps exactly one of these sets to a nonzero complex number of modulus 8. These blocks are then subsequently translated by the coset representatives of G/K. If G is abelian, this construction is guaranteed to produce a $(256, 120, 56)$ *difference set. Furthermore, it should be evident that the ordering of the coset representatives is irrelevant if G is abelian.*

For nonabelian groups with a normal $C_4^2 \times C_2$, Applebaum conjectured there should be some ordering of the coset representatives (8!= 4320 possible) which would result in a difference set in the 649 open groups with such a normal subgroup. This was eventually verified, programmatically with *GAP* [8], using the EBS above, by the end of 2013.

1.3 OBS, the ± 1 version of EBS

We generalize covering EBS in two steps. First, the "Hadamard" parameters $(4N^2, 2N^2 \pm N, N^2 \pm N)$ allow us to replace group ring elements with coefficients from $\{0, 1\}$ with group ring elements whose coefficients are from $\{1, -1\}$. In this case, the difference set D is replaced by a ± 1 version, $D^* := G - 2D$, so that $D^* D^{*(-1)} = 2^{2d+2}$.

An orthogonal building set (OBS) is then a set of group ring elements $\{B_i\}$ whose coefficients are from $\{-1, 0, 1\}$, with the property that for *every* character $\chi \in G^*$, $\chi(B_i)$ has modulus 2^{d+1} or 0 and each character is zero on all but one element of the building set.

For example, replacing B_i by $B_i^* := K - 2B_i$, we have a set $\{B_i^*\}$ such that each character maps exactly one of the B_i to a complex number of modulus 16 and maps all others to zero. The trivial character is now no different that any other character – this is the advantage of the ± 1 viewpoint – in our case, above, the trivial character maps B_6^* to 16 and maps the seven other B_i^* to zero. Here are the ± 1 versions of the earlier blocks.

$$\begin{aligned}
B_1^* &= -(1+x+x^2+x^3z)(1+y)(1+y^2)(1-z)\\
B_2^* &= -(1+x+x^2+x^3z)(1-y)(1+y^2)(1-z)\\
B_3^* &= -(1+x+y+xyz)(1-y^2)(1+x^2)(1-z)\\
B_4^* &= -(1+x)(1+y)(1-y^2)(1-x^2)(1-z)\\
B_5^* &= -(1+x+y+xy^3)(1+x^2)(1-y^2)(1+z)\\
B_6^* &= -(1-x-y-xy)(1+x^2)(1+y^2)(1+z)\\
B_7^* &= -(1+x+y+x^3y)(1-x^2)(1+y^2)(1+z)\\
B_8^* &= (1+x)(1+y)(1-x^2)(1-y^2)(1+z)
\end{aligned}$$

For future reference, we note that each of these is a multiple of a group ring idempotent, specifically,

$$\begin{aligned}
e_1 &:= \frac{1}{8}(1+y)(1+y^2)(1-z),\ e_2 := \frac{1}{8}(1-y)(1+y^2)(1-z),\\
e_3 &:= \frac{1}{8}(1-y^2)(1+x^2)(1-z),\ e_4 := \frac{1}{8}(1-y^2)(1-x^2)(1-z),\\
e_5 &:= \frac{1}{8}(1+x^2)(1-y^2)(1+z),\ e_6 := \frac{1}{8}(1+x^2)(1+y^2)(1+z),\\
e_7 &:= \frac{1}{8}(1-x^2)(1+y^2)(1+z),\ e_8 := \frac{1}{8}(1-x^2)(1-y^2)(1+z)
\end{aligned}$$

1.4 The result of Drisko

The construction of OBS in abelian groups is a powerful concept, especially if we link it to a result on transversals of an elementary difference set.

Let $E \cong C_2^r$ be an elementary abelian group of order 2^r, rank r. Suppose

$$E \trianglelefteq K \trianglelefteq G$$

and that K has a covering EBS consisting of 2^r building blocks. If the property $\chi(B_i) \neq 0$ gives a bijection between the building blocks B_i and the characters χ of E then a result of [7] (see also Theorem 1.7 in [4]) assures us that G has a difference set. In most of the examples in [4], K is an abelian group.

Example 1.10. *The extended building set in the first section,* $\{B_1, B_2, ..., B_8\}$, *used by Applebaum and others to find difference sets in groups of order 256, can be replaced by the following:*

$$\begin{aligned}
B_1^* &:= (1+x^2)(1+y^2)(1+z)(1-x-y-xy)\\
B_2^* &:= (1+x^2)(1+y^2)(1-z)(1-x-y-xy)\\
B_3^* &:= (1+x^2)(1-y^2)(1+z)(1-x-y-xy)\\
B_4^* &:= (1+x^2)(1-y^2)(1-z)(1-x-y-xy)\\
B_5^* &:= (1-x^2)(1+y^2)(1+z)(1-x-y-xy)\\
B_6^* &:= (1-x^2)(1+y^2)(1-z)(1-x-y-xy)\\
B_7^* &:= (1-x^2)(1-y^2)(1+z)(1-x)(1-y)\\
B_8^* &:= (1-x^2)(1-y^2)(1-z)(1-x)(1-y)
\end{aligned}$$

This set has the advantage that these blocks are multiples of the idempotents

$$\frac{1}{8}(1 \pm x^2)(1 \pm y^2)(1 \pm z)$$

existing in the group ring of the elementary abelian group $E = \langle x^2, y^2, z\rangle$. Then any group of order 256, with $K \cong C_4^2 \times C_2$ a normal subgroup, has a difference set. This saves us from the computer search of Applebaum and others.

Of the 14 groups of order 16, 12 have a difference set. Ten of these groups have difference sets constructed from an OBS in $C_2 \times C_2$. The other two groups with difference sets require a different construction.

Of the 267 groups of order 64, 259 have a difference set. 176 of these groups have difference sets constructed from an OBS in $C_2 \times C_2 \times C_2$ and 130 of these groups have difference sets constructed from an OBS in $C_4 \times C_4$, leaving 22 groups with difference sets *not* constructible by OBS.

Of the 56,092 groups of order 256, 56,049 have a difference set. 42,268 of these groups have difference sets constructed from an OBS in $C_2 \times C_2 \times C_2 \times C_2$ and 49,165 of these groups have difference sets constructed from an OBS in $C_4 \times C_4 \times C_2$, 684 of these groups have difference sets constructed from an OBS in $C_8 \times C_8$ giving a union of 54633 groups, leaving 1416.

The percentages of groups given by OBS is 83%, 91.5% and 97.5%, leaving 1416 groups with difference sets *not* constructible by OBS.

We summarize this in two tables.

Table 1: Success rate of abelian OBS in groups of order 64.

Technique	# groups of order 64	%
OBS in C_2^3	176	65.9%
OBS in $C_4 \times C_4$	130	48.7%
ALL OBS in abelian groups	237	88.8%
other construction required	22	8.2%
Turyn/Dillon bound	8	3.0%

Table 2: Success rate of abelian OBS in groups of order 256

Technique	# groups of order 256	%
OBS in C_2^4	42268	75.35%
OBS in $C_4 \times C_4 \times C_2$	49165	87.65%
OBS in $C_8 \times C_8$	684	2.52 %
ALL OBS in abelian groups	54633	97.40 %
other construction required	1416	2.52%
Turyn/Dillon bound	43	0.08%

2 Nonabelian OBS

Since the existence of OBS in abelian groups is so powerful, need we restrict OBS to abelian groups? Our second step in generalizing extended building sets is to create OBS in nonabelian groups.

Example 2.1. *Let* $Q = \langle x, y : x^4 = y^4 = 1, xyx^{-1} = y^{-1}, x^2 = y^2 \rangle$ *be the quaternion group of order eight. Then the set*

$$\{(1 - x - y - xy)(1 + x^2), (1 - x - y - xy)(1 - x^2)\}$$

acts as an OBS of two sets, with $E = \langle x^2 \rangle$*. Any group of order 16 with normal subgroup isomorphic to* Q *has a* $(16, 6, 2)$ *difference set.*

Example 2.2. *Let* $C_4 \rtimes_{-1} C_4 = \langle x, y : x^4 = y^4 = 1; yxy^{-1} = x^{-1} \rangle$ *be a group of order 16 (with* Q *as an obvious quotient group.) Then the set*

$$\{(1 - x - y - xy)(1 + x^2)(1 + y^2), (1 - x - y - xy)(1 + x^2)(1 - y^2),$$

$$[(1 + x) + y(1 - x)](1 - x^2)(1 + y^2), (1 + x)(1 + y)(1 - x^2)(1 - y^2)\}$$

acts as an OBS of four sets with $E = \langle x^2, y^2 \rangle$. *Any group of order 64 with normal subgroup isomorphic to* $C_4 \rtimes_{-1} C_4$ *has a* $(64, 28, 12)$ *difference set.*

The two examples, above, provide difference sets in groups of order 16 and 64, respectively, that are *not* given by abelian OBS.

2.1 Characters and idempotents

The definition of building blocks and extended building sets in abelian groups depends on interplay between subsets of an abelian group and sets of characters of that group. We may generalize those definitions to nonabelian groups by focusing on idempotents, associating a set of characters (or a set of irreducible representations) with a unique idempotent. Good references for group representations, characters and their associated idempotents include [9], chapter 3, [3], chapter 5, and the excellent small monograph [10].

Definition 2.3. *An element* e *of a ring is an* **idempotent** *if* $e^2 = e$. *An element is* **central** *if it commutes with all elements of the ring. The* **center** *of a ring is the set of all central elements.*

The center of a matrix ring over a field is the set of scalar matrices. This means that the only *central* idempotent of a matrix ring is the identity matrix. Since the group ring $\mathbb{C}[G]$ of a finite group G over the complex numbers is isomorphic to the direct sums of the irreducible representations then, given any irreducible representation ϕ, there exists a unique element e_ϕ of the group ring $\mathbb{C}[G]$ such that

$$\phi(e_\phi) = \phi(1) \text{ and if } \phi' \in \mathrm{Irrep}(G), \phi' \neq \phi, \text{ then } \phi'(e_\phi) = 0.$$

Since, for any $\phi' \in \mathrm{Irrep}(G)$, $\phi'(e^2) = \phi'(e)\phi'(e)$, then e_ϕ is an idempotent in $\mathbb{C}[G]$. The element e_ϕ is *the* central idempotent corresponding to the representation ϕ.

Given a subset $S \subseteq \mathrm{Irrep}(G)$, we may define

$$e_S := \sum_{\sigma \in S} e_\sigma.$$

The element e_S is an idempotent and is the *unique* element of $\mathbb{C}[G]$ such that $\sigma(e_S) = \sigma(1)$ if and only if $\sigma \in S$.

The lattice of subsets of $\mathrm{Irrep}(G)$ gives rise to a lattice of central idempotents of $\mathbb{C}[G]$: If S, T are subsets of $\mathrm{Irrep}(G)$ then

$$e_{S \cap T} = e_S \cdot e_T$$

and if S, T are disjoints subsets of $\mathrm{Irrep}(G)$ then

$$e_{S\cup T} = e_S + e_T.$$

If S is a subset of $\mathrm{Irrep}(G)$ and S^C is the complement of S in $\mathrm{Irrep}(G)$ then

$$e_{S^C} = 1 - e_S.$$

This lattice of idempotents corresponds with the lattice of subsets of irreducible representations. In particular, if G is an abelian group, any set of characters of G is associated with a unique idempotent and we may replace our emphasis on characters with a corresponding emphasis on idempotents. (The idempotents given by this lattice are all *central* in $\mathbb{C}[G]$. If G is a nonabelian group then there will be idempotents that are not central.)

If χ is a linear representation of G then the idempotent e_χ is equal to

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

(Note the need for the conjugate map.) Equating functions with group ring elements allows one to then write

$$\overline{\chi} = |G| e_\chi.$$

Definition 2.4. *A set $\{e_1, e_2, ..., e_\ell\}$ of idempotents of $\mathbb{C}[G]$ is* **complete** *(or covering) if the idempotents are pairwise orthogonal and sum to 1.*

If a set of *central* idempotents is complete then the sets of irreducible representations corresponding the idempotents form a partition of the set of all irreducible representations.

Idempotents provide an equivalent definition of building blocks:

Lemma 2.5. *Let G be an abelian group. An element $B \in \mathbb{Z}[G]$ with coefficients from $\{-1, 0, 1\}$ is a building block of length m if and only if there is a nonzero idempotent e such that*

$$Be = B \text{ and } BB^{(-1)}e = m^2 \cdot e.$$

Proof. A building block of modulus m in an abelian group is a set B with the property that $|\chi(B)| = m$ for some characters χ and is equal to zero for all others. Let S be the dual support of B. Then, for $\chi \in S$,

$$|\chi(B)| = m \iff \chi(B)\overline{\chi(B)} = m^2 \iff \chi(B)\chi(B^{(-1)}) = m^2 \iff \chi(BB^{(-1)}) = m^2\chi(1)$$

Let e be the idempotent associated with the set S of characters. Then

$$Be_S \text{ and } BB^{(-1)}e_S = m^2 e_S.$$

On the other hand, if B has the property that there exists an idempotent e such that $Be = B$ and $BB^{(-1)}e = m^2 e$ then let S be the set of all characters ϕ such that $\phi(e) = 1$. If $\phi \in S$ then

$$\phi(B)\overline{\phi(B)} = \phi(BB^{(-1)}) = m^2$$

and so $|\phi(B)| = m$. If $\phi \notin S$, then since $\phi(e) = 0$ we have

$$\phi(B) = \phi(Be) = \phi(B)\phi(e) = \phi(B) \cdot 0 = 0.$$

□ □

Lemma 2.6. *If G is abelian then $A, B \in \mathbb{C}[G]$ are orthogonal if and only if their dual supports are disjoint.*

Proof. Since each element in $\mathbb{C}[G]$ is determined by its image under the irreducible representations then

$$AB = 0 \iff \forall \chi \in G^*, \chi(AB) = 0.$$

But since G is abelian, χ is a homomorphism and so $\chi(AB) = \chi(A)\chi(B)$. Since χ maps group ring elements into the complex numbers then $\chi(A)\chi(B) = 0$ implies that either $\chi(A) = 0$ or $\chi(B) = 0$, so χ is *not* in the dual support of either A or B. Therefore $AB = 0$ implies that the intersection of the dual supports of A and B are disjoint. Conversely, if the dual supports of A and B are disjoint then for any $\chi \in G^*$, $\chi(A) = 0$ or $\chi(B) = 0$ and so $\chi(AB) = 0$. Since this is true for *all* $\chi \in G^*$ then $AB = 0$. □

2.2 Building Blocks in Nonabelian Groups

Let G be a finite group, possibly nonabelian. We make the following definitions:

Definition 2.7. *An element $B \in \mathbb{Z}[G]$ with coefficients from $\{-1, 0, 1\}$ is a* **building block** *of length m with respect to the nonzero idempotent e if*

$$eB = B \text{ and } BB^{(-1)} = m^2 \cdot e.$$

Fixing the positive real number m, a **building set** *in G is a collection $\{B_1, B_2, ..., B_\ell\}$ of mutually orthogonal building blocks of length m.*

Definition 2.8. *A building set* $\{B_1, B_2, ..., B_\ell\}$ *comes with an associated set of idempotents,* $\{e_1, e_2, ..., e_\ell\}$. *A building set is* **covering** *if the associated idempotents form a covering set of idempotents.*

Lemma 2.9. *Suppose* B_1, B_2 *are building blocks of length* m *in a finite group* G *and suppose the associated idempotents* e_1, e_2 *are central. Then* B_1, B_2 *are orthogonal if and only if their dual supports are disjoint.*

Proof. Suppose the dual supports of B_1, B_2 are disjoint. Then for any representation $\phi \in \mathrm{Irrep(G)}$, either $\phi(B_1) = 0$ or $\phi(B_2) = 0$. Therefore $\phi(B_1 B_2) = 0$. Since this is true for all irreducible representations then $B_1 B_2 = 0$.

On the other hand, suppose $B_1 B_2 = 0$ but there is an irreducible representation ϕ in the intersection of the dual supports of B_1, B_2. Let e be the idempotent associated with ϕ. Then $B_1 B_1^{(-1)} e = m^2 e = B_2 B_2^{(-1)}$ and so

$$(B_1 B_2)(B_1 B_2)^{(-1)} e = B_1 (B_2 B_2^{(-1)}) B_1^{(-1)} e = B_1 (B_2 B_2^{(-1)} e) B_1^{(-1)}$$

$$= B_1 (m^2 e) B_1^{(-1)} = m^2 e B_1 B_1^{(-1)} = m^4 e$$

contradicting the claim that $B_1 B_2 = 0$. □ □

Example 2.10. *The idempotents corresponding to the extended building set in example 1.9, were given immediately after that example. That set of idempotents,* $\{e_1, ..., e_8\}$, *is* complete, *as the sum of the eight idempotents is* 1. *In making this correspondence of idempotents with characters, we assign the trivial character to the sixth building block, the one "short" block in the list, a set of size 8, not 16.*

2.3 Families of (a, m, t) OBS

We define an (a, m, t) OBS and a product construction.

Definition 2.11. *An* (a, m, t) **orthogonal building set** *(OBS) in a group* K *is a set* $\{B_1, B_2, ..., B_t\}$ *of* t *mutually orthogonal elements of* $\mathbb{Z}[G]$ *with coefficients from* $\{-1, 0, 1\}$ *such that each element* B_i *has support of size* a *and modulus* m *with respect to an idempotent* e_i. *The OBS is* **covering** *if the set* $\{e_1, e_2, ..., e_t\}$ *of associated idempotents is complete. The OBS is* **elementary** *if the order of* K *is equal to* a *and the idempotents are idempotents of a central elementary subgroup* E.

Example 2.12. *The two subsets of the quaternion group given in example 2.1 form an* $(8, 4, 2)$ *OBS while those in example 2.2 form a* $(16, 8, 4)$ *OBS.*

A difference set in a group of order 2^{2d+2} gives, trivially, a $(2^{2d+2}, 2^{d+1}, 1)$ OBS. In order to construct a difference set in a group of order 2^{2d+2}, we seek OBS with parameters $(2^{2d+2-r}, 2^{d+1}, 2^r)$.

Lemma 2.13. *(Product construction) If $\mathcal{B}_1 = \{B_{1,1}, ...B_{1,i}, ...B_{1,t_1}\}$ is an (a_1, m_1, t_1) OBS in K_1 and $\mathcal{B}_2 = \{B_{2,1}, ...B_{2,i}, ...B_{2,t_2}\}$ is an (a_2, m_2, t_2) OBS in K_2 then $\mathcal{B}_1 \times \mathcal{B}_2 = \{B_{1,i} \times B_{2,j} : 1 \le i \le t_1, 1 \le j \le t_2\}$ is an (a_1a_2, m_1m_2, t_1t_2) OBS in $K_1 \times K_2$.*

The set of associated idempotents for $\mathcal{B}_1 \times \mathcal{B}_2$ is the direct product of the idempotents associated with $\mathcal{B}_1$ and $\mathcal{B}_2$.

Let $\mathcal{H}(a, m, t)$ represent the set of (isomorphism classes of) groups of order a with an elementary (a, m, t) OBS.

For example: $\mathcal{H}(2, 2, 2) = \{C_2\}$. $\mathcal{H}(4, 4, 4) = \{C_2^2\}$. $\mathcal{H}(4, 2, 1) = \{C_4, C_2^2\}$. $\mathcal{H}'(8, 4, 2) = (\mathcal{H}(4, 2, 1) \times \mathcal{H}(2, 2, 2)) \cup \{Q_4\} = \{C_4 \times C_2, C_2^3, Q_4\}$.

Since the direct product of the set $\mathcal{H}(a_1, m_1, t_1)$ and $\mathcal{H}(a_2, m_2, t_2)$ is a subset of $\mathcal{H}(a_1a_2, m_1m_2, t_1t_2)$, we might seek groups with a "primitive" OBS, one not created by a product. (See examples 2.1 and 2.2.)

It is likely that there are more examples of covering building sets in nonabelian groups of order 16. But it turns out that a "near miss" in $C_8 \times C_2$ will create OBS in important groups of order 32.

2.4 Golay-like pairs of building sets

Some groups of order 64, with difference sets, do not appear to allow a covering building set from normal subgroups of order 16. But there are variations on the covering building set construction that are significant.

Example 2.14. *The group $H = C_8 \times C_2$ does not have a covering building set of four building blocks of length eight. But it has an interesting "near miss". Consider the following four blocks in $H = C_8 \times C_2 = \langle x, y : x^8 = y^2 = [x, y] = 1\rangle$.*

$$B_0 := (1 - x^4)(1 + x^2y)(1 - x - y - xy)$$

$$B_1 := (1 + x^4)(1 + y)(1 - x - x^2 - x^3)$$

$$B_2 := (1 - x^4)(1 - x^2y)(1 - x - y - xy)$$

$$B_3 := (1 + x^4)(1 - y)(1 - x - x^2 - x^3)$$

The elements B_1 and B_3 are mutually orthogonal building blocks of length eight, with respect to the idempotents $\frac{(1+x^4)(1\pm y)}{4}$. Indeed, all pairs of blocks are mutually orthogonal except *the pair B_0, B_2. Noting that $x^8 = 1, y^2 = 1$, we can*

compute

$$B_0 B_0^{(-1)} = 16(1 - x^4) = B_2 B_2^{(-1)}$$

and

$$B_0 B_2^{(-1)} = 8x^2(1 - x^4) = -B_2 B_0^{(-1)}$$

These relations imply that with appropriate care for elements g_i, the set $D = \sum g_i B_i$ will be a difference set.

The group $H = C_8 \times C_2$ only has three involutions, x^4, y and $x^4 y$. The involution x^4 is the only involution which is itself a square and so it is fixed by all automorphisms. Thus, if G is a larger group with H as a normal subgroup, then the idempotents $\frac{1-x^4}{2}$, $\frac{(1+x^4)(1-y)}{4}$ and $\frac{(1+x^4)(1+y)}{4}$ are all fixed by conjugation by elements of G.

Let G be a group of order 64 with H as a normal subgroup. Let $g_0 = 1, g_1, g_2, g_3$ be a left transversal of H in G. Set

$$D := \sum_j g_j B_j.$$

Then

$$DD^{(-1)} = 64 + 8x^2(1 - x^4)g_2^{-1} - 8g_2 x^2(1 - x^4))$$

We have a difference set if and only if

$$8x^2(1 - x^4)g_2^{-1} - 8g_2 x^2(1 - x^4) = 0.$$

Now $8(1 - x^4)$ is in the center of the group ring and can be effectively ignored. So we require the group element $x^2 g_2^{-1}$ to be equal to $g_2 x^2$. When this is true, the set $\{B_0 + g_2 B_2, B_1 + g_2 B_3\}$ is a $(32, 8, 2)$ OBS in a group $H' = \langle g_2, x, y\rangle$ of order 32. Any group of order 64 containing the subgroup H' then has a difference set of the form $D = B_0 + g_2 B_2 + g'(B_1 + g_2 B_3)$ where $g' \notin H'$.

There are eight groups of order 32 containing a normal copy of $H = C_8 \times C_2$ and an element $g \notin H$ such that $x^2 g^{-1} = g x^2$. There are 118 groups of order 64 with a subgroup of order 32 isomorphic to one of these eight. So these 118 groups have a difference set constructible in this manner. Included in this list are 13 groups not covered by the earlier abelian or nonabelian OBS.

This reduces the open groups to SmallGroup(64, cn) where $cn \in \{42, 46, 48, 49, 51\}$. These remaining five groups all have $C_8 \times C_2$ as a normal subgroup but the "building block" structure appears to be more complicated. In these groups a more subtle argument, probably using the inner automorphisms of the group of order 64 acting on $C_2 \times C_8$, will be necessary.

Example 2.15. *Let* $M_{64} := \langle x, y : x^{32} = y^2 = 1, yxy^{-1} = x^{17}\rangle$*, the modular group of order 64. The element* x^{16} *is a central involution (indeed the center of* G *is* $\langle x^2\rangle$*) and* $\langle x^{16}, y\rangle$ *is a subgroup isomorphic to* C_2^2*. However,* y *is not central. Consider the follow four blocks:*

1. $B_{++} := [(1 + x^8) + g_1(1 - x^8)](1 + x^{16})(1 + y)$
2. $B_{++} := [(1 + x^8) + g_2(1 - x^8)](1 + x^{16})(1 - y)$
3. $B_{-+} := [(1 + x^8) + g_3(1 - x^8)](1 - x^{16})(1 + y)$
4. $B_{--} := [(1 + x^8) + g_4(1 - x^8)](1 - x^{16})(1 - y)$

Observe that

$$B_{++}B_{++}^{(-1)}(e_{++}) = 16(1+x^{16})(1+y) \text{ and } B_{+-}B_{+-}^{(-1)}(e_{+-}) = 16(1+x^{16})(1-y)$$

so the sets B_{++} *and* B_{+-} *are orthogonal buidling blocks. However, the other two sets do not work quite as nicely, due to the fact that* y *is not in the center of* G*. But one can tinker with the values of the group elements* g_i *and, just as in the* $C_8 \times C_2$ *example, create complementary building sets The first difference set found in this group (*Δ *in [11]) has form (as a* ± 1 *DS)*

$$\Delta^* = A(1 + x^{16}) + B(1 - x^{16})$$

where

$$A = x^3[(1 + y) - x^2(1 - y)](1 + x^8) + x^4[(1 + y) + x^4(1 - y)](1 - x^8)$$

and

$$B = x^{-2}(1 + x)(1 - y)(1 + x^8) - x(1 - x)(1 + y)(1 - x^8).$$

2.5 Final thoughts

One might wonder if identification of OBS in various nonabelian groups is sufficient to construct difference sets in *all* groups that have them. However, there are two groups of order 64 with the property that *all* normal subgroups in those groups also occur in groups that do *not* have differences sets. (One of these two groups is M_{64}, above.) In groups of order 256, there are ten groups with difference sets, yet all their normal subgroups are normal subgroups of groups that do *not* have difference sets. (One of these ten groups is the "most difficult" group of order 256, the group $C_{64} \rtimes_{47} C_4$; see [13] for a construction.) Thus the OBS construction cannot work directly in those groups. However, in these groups, we often found a "near miss" as described above in $C_8 \times C_2$; we found four sets where one pair were orthogonal building sets and the other pair were complementary, not quite building sets of the same modulus, but offsetting each other in just the right way.

On the other hand, *every* difference set in 2-groups has *some* further connection to OBS:

Theorem 2.16. *Suppose D is a ± 1 difference set in a 2-group G. Let g be a central involution in G. Then there are group ring element $A, B \in \mathbb{Z}[G]$ such that*

$$D = A(1+g) + B(1-g).$$

The set $\{A(1+g), B(1-g)\}$ is then a $(2^{2d+1}, 2^{d+1}, 2)$ OBS in this group of order 2^{2d+2}.

2.6 Summary

It is possible that all the groups with difference sets can be explained in three waves of construction:

1. Use OBS in abelian groups and selected nonabelian groups to dispatch most ($> 99\%$) of the groups.
2. Use OBS in selected nonabelian groups to dispatch most of the remaining groups.
3. Use complementary paired OBS (as above in examples 2.14 and 2.15) to complete construction of difference sets in the final more difficult groups.

All difference sets can be constructed from building blocks, in *some* way, but it is not clear if there is a recursive process that covers every case. The most difficult groups appear to have a cyclic center, preventing a convenient elementary abelian subgroup.

The use of *nonabelian* groups for the construction of difference sets is important. Although large families of difference sets can be constructed from building blocks in abelian groups, this does not cover all groups and if we are to prove the overall conjecture, we *must* develop a theory of nonabelian building blocks.

In drafting this attempt at a general theory of covering building sets, a number of questions occur. (Any of these might be a good place to start an undergraduate research project or a masters thesis.)

1. Explain the difference sets occurring in the five "difficult" groups of order 64. Is there an elegant explanation using the normal subgroup $C_8 \times C_2$?
2. Identify OBS in groups of order 16 and 32. (Must we always require that the idempotents come from a central elementary abelian subgroup E?)
3. Lift the OBS and near-OBS in groups of order 16 to OBS in groups of order 32.

4. Construct the difference sets in the "difficult" groups of order 256, those that do not have a convenient OBS. Can we generalize this construction to *families* of groups with cyclic centers?

Acknowledgment: ...
Funding for finite fields conference?

References

[1] T. Applebaum, *Difference Sets in Non-Abelian 2-Groups*, Honors Thesis, University of Richmond, 2013.
[2] C. Bhattacharya, and K.W. Smith, *Factoring (16, 6, 2) Hadamard Difference Sets*, Electr. J. Comb.. 15, 2008.
[3] C. W. Curtis & I. Reiner, Representation Theory of Finite Groups and Associative Algebras
[4] Davis, Jedwab, et. al. *Constructions of difference sets in nonabelian 2-groups*, submitted, 2019.
[5] J. Davis and J. Jedwab, *A unifying construction for Difference Sets*. J. Comb. Th. (Ser. A), vol. 80, No. 1, 13-78, October 1997.
[6] J.F. Dillon, *Variations on a scheme of McFarland for noncyclic difference sets*, J. Comb. Th. (Ser. A), vol. 40, 9-21, 1985.
[7] A. Drisko, *Transversals in row-Latin rectangles*, J. Comb. Th. (Ser. A), vol. 84, 181-195, 1998.
[8] The GAP Group, GAP - Groups, Algorithms, and Programming, Version 4.9.1, 2018.
[9] D. Gorenstein, Finite Groups, AMS Chelsea Publishing, 2nd ed., 1980.
[10] W. Ledermann, Introduction to Group Characters, Cambridge University Press, 1977.
[11] R.A. Liebler and K.W. Smith, *On difference sets in certain 2-groups*, Coding Theory, Design Theory, Group Theory, eds. D. Jungnickel, S. Vanstone, 195-212, Wiley, NY, 1993.
[12] R. Turyn, *Character sums and difference sets*. Pacific J. Math., vol. 15, 319-346, 1965.
[13] W. Yolland, *Existence of a difference set in the last group of order 256*, summer research report, Simon Fraser University, 2016.