Finding Hadamard Difference Sets

Alec Biehl[1], Kevin Halasz[2], Rachael Keller[3], Maryna Longnickel[4], Dylan Peifer[5], Ken Smith[6], and Jason Steinberg[7]

[1]Wittenberg University
[2]University of Puget Sound
[3]Louisiana State University
[4]California State University East Bay
[5]Carleton College
[6]Sam Houston State University
[7]Princeton University

August 9, 2013

San Diego State University
Funded by NSF Grant 1061366

Contents

1 Introduction

Let S be a set of size k. We define a (v, k, λ)-*symmetric design* to be a subset of the power set $P(S)$ containing v k-sets, which we will call blocks, such that each element of S appears in exactly k blocks, and for any pair of elements $(a, b) \in S$, there are exactly λ blocks containing both a and b. Given a finite group G of order v, a subset $D \subseteq G$ is called a *(v,k,λ)-difference set* if $|D| = k$ and the set $\{d_i d_j^{-1} | d_i, d_j \in D\}$ contains λ copies of each nonidentity element in G. We set the notation $n = k - \lambda$, which is sometimes considered to be a fourth parameter. It is not particularly difficult to see that, if we have a (v, k, λ)-difference set D based upon the group G, then the collection of sets $\{Dg|g \in G\}$ is a symmetric design. We call a difference set a *Hadamard difference set* (HDS) if, for some $m \in \mathbb{N}$, $v = 4m^2$, $k = 2m^2 \pm m$, and $\lambda = m^2 \pm m$. We can also see here that $v = 4n$. The name *Hadamard* is derived from the fact that the $1, -1$-incidence matrix of the associated design of any HDS is a Hadamard matrix. Note that a *Hadamard matrix* is simply an $n \times n$ $\{1, -1\}$ matrix A such that $AA^\intercal = n\mathtt{I}$.

We will start with a basic example, before discussing some basic properties. Let $G \cong C_4 \times C_4 = \langle a, b | a^4 = b^4 = [a, b] = 1\rangle$. Then it easy to check that the set $D = \{a, a^2, a^3, ab, b^2, ab^3\}$ is a $(16, 6, 2)$-Hadamard difference set in G. Given any difference set $D \subseteq G$, the image of D under any automorphism $\alpha \in aut(G)$ is also a difference set. We can also translate a difference set via left or right multiplication while still retaining the fundamental difference set property. This means that, given the difference set $D = \{a, a^2, a^3, ab, b^2, ab^3\}$ in $C_4 \times C_4$, we may conclude that $a^3 D = \{1, a, a^2, b, a^3 b^2, b^3\}$ is also a difference set. Given two difference sets D_1 and D_2 contained in a group G, we say that D_1 and D_2 are *equivalent* if there is some automorphism $\phi \in Aut(G)$ and some element $g \in G$ such that $D_1 = g\phi(D2)$. Hence, just as group theorists are only concerned with characterizing groups up to isomorphism, we are generally concerned only with characterizing Hadamard difference sets up to equivalence (though not always, see Section 2).

We may also view difference sets in the context of a *group ring*. Given a group G and a ring R, the group ring R[G] is the set $\{\sum_{g_i \in G} r_i g_i | r_i \in R\}$, which is a module under the natural definitions of addition and scalar multiplication, and a ring under the natural definition of addition and distributive multiplication. When working with difference sets in a group G, we make repeated use of both $\mathbb{Z}[G]$ and $\mathbb{C}[G]$.

We will abuse notation and use D to refer both to the difference set itself, and to the group ring element $\sum_{d \in D} d \in \mathbb{Z}[G]$. We use similar notation for entire groups, and for elements of $\mathbb{C}[G]$. So, for example $G = \sum_{g \in G} g \in \mathbb{C}[G]$. Furthermore, given a group ring element $F = r_1 g_1 + r_2 g_2 + \ldots + r_v g_v$, we use the symbol $F^{(-1)}$ to denote the element $r_1 g_1^{-1} + r_2 g_2^{-1} + \ldots + r_v g_v^{-1}$. This gives rise to the following lemma.

Lemma 1.0.1. *Given a group G, a set $D \subseteq G$ is a (v, k, λ)-difference set if and only if $DD^{(-1)} = n1_G + \lambda G$.*

Now consider $D^* = G - 2D$, which we call the *associate of D*. We then get the following theorem, which we will utilize heavily below.

Theorem 1.0.2. *Given a group G, a set $D \subseteq G$ is a (v, k, λ)-difference set if and only if $D^* D^{*(-1)} = v1_G$.*

The first part of this research project was to create a list of Hadamard difference sets in all groups of order 64 in which one exists. It is known that 12 of the 14 groups of order 16 and 9 of the 14 groups of order 36 have a Hadamard difference set; see [1] and [2]*** for more details. Several other basic results that we used repeatedly this summer are as follows:

- In any difference set, $(v-1)\lambda = k(k-1)$. This is because each side of this equality just counts the number of nonidentity elements in $DD^{(-1)}$.
- In an abelian group of order 2^{2s+2}, $s \in \mathbb{N}$, there is no difference set if the groups exponent is greater than 2^{s+2}. This result is commonly known as *Turyn's bound*, and is proven in [10].
- If a generalized dihedral group contains a difference set, then any Abelian group containing its underlying Abelian subgroup as a subgroup of index two has a difference set. This result is proven in [3].

Perhaps our most utilized tool this summer was the computer algebra system GAP (Groups, Algorithms, and Programming, gap-system.org). Using GAP, we created various algorithms based on known constructions of difference sets, including the product construction, the spread construction, and the extended-building set construction, all of which we will explain in detail below. We then applied these to 259 groups of order 64 known to contain Hadamard difference sets to find at least one difference set in each group. The list is contained as a supplementary appendix to this paper. Each element of this list contains the GAP ID of the group, the elements that create the difference set, and the method used to find the difference set. In some cases, more "difficult" groups, such as the modular group (see [3], page 83), were outside the domain of the main construction methods, so we searched through other published documents that provided difference sets and translated them into GAP notation. After completing this project, we used observations that we had made along the way to try and form novel conjectures and prove original results concerning Hadamard difference sets. We ended up completing four sub-projects: (1) classifying and beginning to explain how we can transfer difference sets from one group to another using shared GAP indices, (2) analyzing and exploring the details of the Davis-Jedwab construction to offer a new view of extended building sets, (3) studying the optimization of exhaustive searches, (4) using Latin rectangles to create difference sets.

2 Difference Set Transfers

2.1 Voodoo in Groups of Order 64

In our first project we found an explicit difference set in each of the 259 groups of order 64 that admit a difference set. We stored our produced difference sets as group ID numbers and lists of indices using GAP's SmallGroups Library. For example, one entry in our table of difference sets is

[[64, 10], [1, 2, 3, 5, 7, 11, 12, 13, 18, 23, 26, 27, 31, 32, 36, 38, 39, 40, 41, 42, 44, 48, 49, 52, 53, 55, 56, 63]].

The [64, 10] in this entry indicates that the difference set was found in the tenth group of order 64 in GAP's SmallGroups Library, which GAP will return when given the command `SmallGroup(64,10)`. The list [1, 2, . . . , 56, 63] in the entry indicates which specific elements in GAP's ordered list of elements of the group form the found difference set (this list of elements is returned from the command `Elements(SmallGroup(64,10))` in GAP).

These table entries were nothing more than a convenient shorthand, and the lists of indices meant nothing when separated from the context of the group that contained the difference set. However, as we exhausted various constructions for producing difference sets we found that we could sometimes transfer the indices corresponding to a difference set in one group into another group and still have a difference set. For example, the list of indices [1, 2, . . . , 56, 63] given above for a difference set in group 10 in GAP's catalog of order 64 groups is also a difference set in groups 9, 14, 100, 120, 240, and 265. During our first project we used this technique to produce a difference set in four groups that were not covered by our other constructions.

This "voodoo" of transferring difference sets between groups by way of GAP indices is actually somewhat common in groups of order 64. Our table of one difference set in each of the 259 groups of order 64 that have a difference set gives as a total of 259 difference sets in indices (actually, our table already had 11 sets that were repeated twice and one set that occurred four times, but we will pretend that we didn't know this already). Taking these 259 sets of indices and trying each in every group of order 64 gives that each set of indices works in between 1 and 141 different groups, with the number of groups a given set of indices works in having a mean of 55.6 and median of 61. This is very surprising, and indicates that there is some underlying pattern to the way GAP lists elements that preserves difference sets when transferring between groups.

2.2 Voodoo in Groups of Order 16

We would like to understand the source of this voodoo, and perhaps use it to create constructions or prove existence results. To determine where the patterns are, we first want to organize all cases where transferring a difference set in one group to another by way of GAP indices results in a difference set in the new group. This is very difficult to do in groups of order 64 because there are a large number of groups and difference sets, because all difference sets up to equivalence in groups of order 64 have not been found, and because basic computations can take a long time in these groups. For these reasons, we decided to instead focus on groups of order 16. These groups have similar voodoo behavior, are still 2-groups, and are much easier to work with than order 64 groups. We also already know all difference sets up to equivalence in groups of order 16. Note that groups of order 36 also show some definite voodoo behavior (for example, groups 7, 13, and 14 in order 36 all have the same difference sets when viewed as indices), but it is not as pronounced as in order 16 and we decided to avoid it for now.

We already know (and can quickly perform a computer search to find) all difference sets in order 16 groups and the number of difference sets up to equivalence in each group. This is summarized in Table 2.2.1, which lists the 14 groups of order 16 by their ID in GAP, the total number of difference sets in each group, and the number of difference sets up to equivalence.

Table 2.2.1: Difference Sets in Groups of Order 16

IdGroup	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Difference Sets	0	192	192	192	192	64	0	128	256	448	192	704	320	448
Equivalence Classes	0	3	4	3	2	2	0	2	2	2	2	2	2	1

To classify the voodoo we observed, we want to know when transferring a difference set expressed in indices from one group to another results in a difference set. Table 2.2.2 shows all the places transfers can occur in groups of order 16. Each row and column of the table is labeled by GAP's category number for a group of order 16. The number in each entry indicates how many difference sets in the two groups from the associated column and row are the same when expressed as lists of indices in GAP. For example, the table shows that SmallGroup(16,3) and SmallGroup(16,8) share 64 difference sets. For reference, note that difference sets in groups of order 16 are subsets of 6 elements, and that there are then $\binom{16}{6} = 8008$ total subsets of 6 elements that could potentially be a difference set.

Table 2.2.2 clearly shows that transfers are very common in groups of order 16. Other than groups 1 and 7, which have no difference sets, the only time we can transfer no difference sets is

Table 2.2.2: Voodoo in Groups of Order 16

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	192	192	192	64	64	0	64	128	192	192	192	128	192
3	0	192	192	192	64	64	0	64	128	192	192	192	128	192
4	0	192	192	192	64	64	0	64	128	192	192	192	128	192
5	0	64	64	64	192	64	0	0	64	192	64	192	64	192
6	0	64	64	64	64	64	0	0	64	64	64	64	64	64
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	64	64	64	0	0	0	128	128	64	64	64	64	64
9	0	128	128	128	64	64	0	128	256	128	128	128	128	128
10	0	192	192	192	192	64	0	64	128	448	192	448	192	448
11	0	192	192	192	64	64	0	64	128	192	192	192	128	192
12	0	192	192	192	192	64	0	64	128	448	192	704	256	448
13	0	128	128	128	64	64	0	64	128	192	128	256	320	192
14	0	192	192	192	192	64	0	64	128	448	192	448	192	448

between group 8 to group 5 or 6. Also note that transfers do not seem to be randomly distributed. The numbers in the table are all multiples of 64 and show far too much organization to be the result of random chance.

One problem with the above table is it simply contains too much information. In order to better approach the problem we decided to simplify our question of when some difference sets may be transferred between groups to the question of when all difference sets in some group correspond to difference sets in another group by way of GAP indices. This question led us to Figure 2.2.1.

In Figure 2.2.1 groups are represented by their category number in GAP. Groups are placed in a box together if they have the same difference sets when viewed in GAP index form. At the bottom right of each box is the total number of difference sets found in the group or groups. A directed arrow indicates that all difference sets from the starting group are also difference sets in the ending group when viewed as indices in GAP. For example, group 5 contains 192 total difference sets. Every difference set in group 6 can be transferred to a difference set in group 5 by expressing it as indices, and then every difference set in 5 can be transferred to a difference set in group 10 or 14 in the same way. Furthermore, groups 10 and 14 have exactly the same difference sets when their difference sets are viewed as lists of GAP indices.

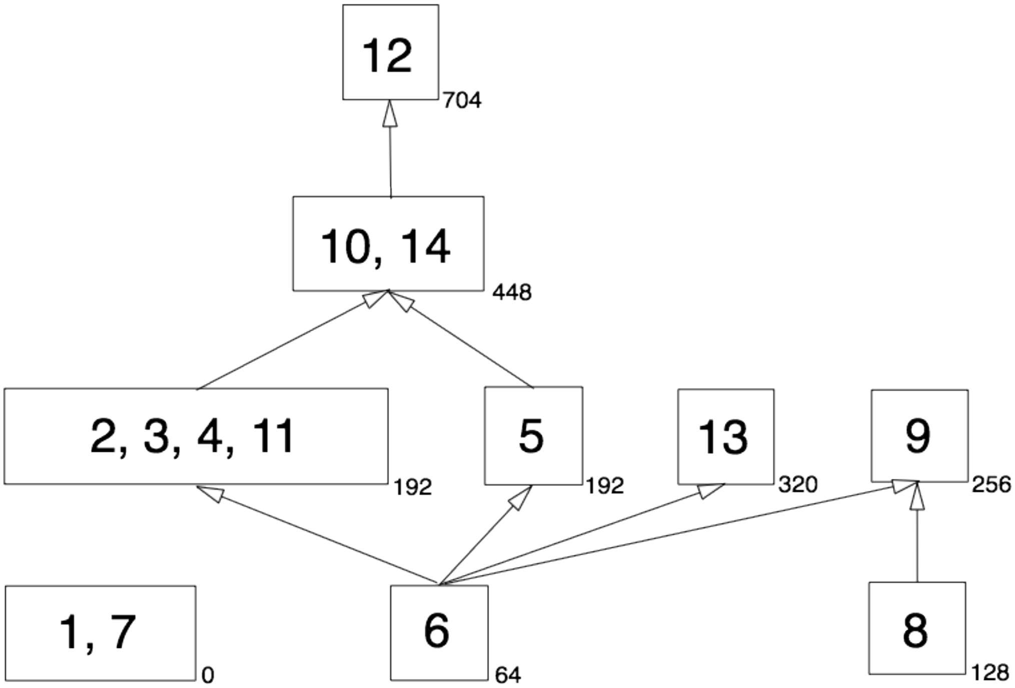
A good deal of voodoo is lost when viewing Figure 2.2.1. For example, Table 2.2.2 shows that group 12 and group 13 share 256 difference sets, but here they appear to be totally separate. Still, the diagram is very useful in organizing and presenting the most surprising examples of voodoo, and it gives us suggestions for where to focus our efforts. The remainder of our work will be aimed at explaining and proving the various relations we can see in Figure 2.2.1.

2.3 Power-Commutator Presentations

A difference set transfer occurs when two groups having the same difference set when expressed as indices in the ordered list of elements GAP provides for each group. To understand transfers we need to know how GAP organizes its ordered list of elements, specifically in groups of order 16 and groups of order 64.

A group is called *polycyclic* if it admits a subnormal series with cyclic factors, i.e. if we can form a chain of subgroups $G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_n = \{1\}$ such that G_1/G_{i+1} is cyclic. It is a

Figure 2.2.1: Voodoo in Groups of Order 16



well-known fact that all p-groups are polycyclic [6], and as it turns out, polycyclic groups always have a very computationally effecient presentation, known as a *PC-presentation.*

GAP stores the groups of order 16 and 64 using a special type of PC-presentation known as a *power-commutator presentation.* There is an immense amount of theory behind how GAP represents p-groups in its SmallGroups database. We refer an interested reader to [6]. We will only present here what is necessary to understand difference set transfers.

A power-commutator presentation of a group G of order p^n is a presentation with generators $g_1, g_2, \ldots, g_n$ and two sets of relations: the power relations

$$g_i^p = \prod_{k>i} g_k^{a_{i,k}},$$

and commutator relations

$$[g_i, g_j] = \prod_{k>\max(i,j)} g_k^{b_{i,j,k}},$$

where $[g_i, g_j] = g_i^{-1} g_j^{-1} g_i g_j$ is the commutator of g_i and g_j and the $a_{i,k}$ and $b_{i,j,k}$ are nonnegative integers less than p. If a group G can be generated by k elements, then $\{g_1, g_2, \ldots, g_k\}$ will generate G. Furthermore, if the size of a minimal generating set for G is k, then all g_i, $i > k$, will be defined by one of the relations, as it will be the sole element in the right hand side's product for either a power relation or a commutator relation on smaller elements of G. Most importantly, 2ith respect to a power-commutator presentation, every element of G can be written in the form $g_1^{c_1} g_2^{c_2} \ldots {g_n}^{c_n}$ where $c_i < p$, which we call the *normal form* of the element.

Every p-group has a power-commutator presentation, but for a given group there can be several different power-commutator presentations. In GAP, the groups of order 16 all have generators f_1, f_2, f_3, f_4 and relations listed in Table 2.3.1.

Table 2.3.1: Power Commutator Presentations in GAP

IdGroup	StructureDescription	f_1^2	f_2^2	f_3^2	f_4^2	$[f_1, f_2]$	$[f_1, f_3]$	$[f_1, f_4]$	$[f_2, f_3]$	$[f_2, f_4]$	$[f_3, f_4]$
1	C_{16}	f_2	f_3	f_4	1	1	1	1	1	1	1
2	$C_4 \times C_4$	f_3	f_4	1	1	1	1	1	1	1	1
3	$(C_4 \times C_2) \rtimes C_2$	f_4	1	1	1	f_3	1	1	1	1	1
4	$C_4 \rtimes C_4$	f_4	f_3	1	1	f_3	1	1	1	1	1
5	$C_8 \times C_2$	f_3	1	f_4	1	1	1	1	1	1	1
6	$C_8 \rtimes C_2$	f_3	1	f_4	1	f_4	1	1	1	1	1
7	D_{16}	1	1	f_4	1	f_3f_4	f_4	1	f_4	1	1
8	QD_{16}	f_4	1	f_4	1	f_3f_4	f_4	1	f_4	1	1
9	Q_{16}	f_4	f_4	f_4	1	f_3f_4	f_4	1	f_4	1	1
10	$C_4 \times C_2 \times C_2$	f_4	1	1	1	1	1	1	1	1	1
11	$C_2 \times D_8$	1	1	1	1	f_4	1	1	1	1	1
12	$C_2 \times Q_8$	f_4	f_4	1	1	f_4	1	1	1	1	1
13	$(C_4 \times C_2) \rtimes C_2$	1	1	f_4	1	f_4	1	1	1	1	1
14	$C_2 \times C_2 \times C_2 \times C_2$	1	1	1	1	1	1	1	1	1	1

Next, as the power-commutator presentation gives a way to write every element in a group of order 16 in the form $f_1^{a_1} f_2^{a_2} f_3^{a_3} f_4^{a_4}$ where $a_i \in \{0, 1\}$, GAP simply writes all elements of the group in this form and orders them lexicographically. This means that the command `Elements(g)` returns the ordered list

$$[1,\ f_1,\ f_2,\ f_3,\ f_4,\ f_1f_2,\ f_1f_3,\ f_1f_4,\ f_2f_3,\ f_2f_4,\ f_3f_4,\ f_1f_2f_3,\ f_1f_2f_4,\ f_1f_3f_4,\ f_2f_3f_4,\ f_1f_2f_3f_4]$$

for every group of order 16. Thus difference sets that have the same indices are really difference sets that are composed of the same words on generators f_1, f_2, f_3, f_4.

2.4 The Spread Construction

If we can determine that all of the difference sets in some collection of groups have some well understood structure, then we should be able to easily explain why difference sets can be transferred between the groups in this collection. We can perform such a procedure in several groups of order 16 using a difference set construction technique known as the spread construction, showing that all difference sets in a given group are what we call difference set of *spread form.* Before we get to these central results, however, we will briefly examine some basic notions concerning the spread construction, and see that we can use it to better understand some of patterns in Table 2.2.1 and Table 2.2.2.

The spread construction was first introduced by McFarland in 1973, before being expanded upon and mathematically justified by J.F. Dillon in [3] and Drisko in [4]. Though the construction can be applied to a wide variety of groups, it only can construct *Hadamard* difference sets in 2-groups, so we will define it only in this restricted case.

Let G be a group of order $4(2^s)^2 = 2^{2s+2}$, for some $s \in \mathbb{N}$. If G has a normal elementary Abelian subgroup E of order 2^{s+1}, then we can employ the spread construction. Note that this means that we can use the spread constructions only on groups containing a normal subgroup isomorphic to C_2^{s+1}. If we treat E as a vector space over $\mathbb{Z}_2$, we can easily see that the hyperplanes of this vector space are exactly the subgroups of index 2 in E. Because a hyperplane of a vector space is made up of all points orthogonal to a given point in that vector space, there are $\frac{2^{s+1}-1}{2-1}$ hyperplanes of E.

So, let $\{H_i | 1 \leq i < 2^{s+1}\}$ be the collection of subgroups of E of order 2^s. Note that if $|G| = 16$, then $\{H_i\}$ is a spread in E. This is the source of the name "spread" construction. We now let $T = \{t_i | \cup_{i=1}^{2^{s+1}} t_i E = G\}$ be a transversal of E in G. It is now possible to (potentially) create a difference set in G by assigning each hyperplane H_i to a coset of E in G. Letting F^* represent the set of all nonidentity elements in some group F, it was shown in [3] that if $\{t_i H_i^* t_i^{-1}\}$ is a 1-design on E^*, then $D = \sum_{i=1}^{2^{s+1}-1} t_i H_i$ is a difference set in G. We call such a D a *difference set of spread form.* Though there many assignments of hyperplanes to cosets that do not meet the sufficient condition for generating a difference set, Art Drisko showed in [4] that there is always some assignment that works when we have a properly sized elementary abelian subgroup.

We should note a couple of things here. First of all, it is important to realize that the orderings t_i and H_i are arbitrary. Therefore, if some assignment of difference sets to cosets does yield a 1-design, we can still try other assignments. Also, note that in each assignment one of the cosets is left empty, as $|\{H_i\}| = |T| - 1$. Finally, if $E \subseteq Z(G)$, the center of G, then any assignment of hyperplanes to cosets will leave $\{t_i H_i^* t_i^{-1}\}$ as a 1-design on E^*.

We now turn to a couple of enumerative results concerning the number of difference sets we can build as spread constructions over a single normal elementary abelian subgroup. Though the first theorem will be general, in the second we will focus on groups of order 16, as it is in these groups that we have our best data on transfers.

Theorem 2.4.1. For a group G of order 2^{2s+2}, the spread construction generates $2^{s+1}!(2^{2^{s+1}-1})$ sets over any subgroup E isomorphic to C_2^{s+1}.

Proof. We start by assigning hyperplanes to cosets. Recalling that one coset must be left empty, we see that we have 2^{s+1} choices for this coset. Then, if we set an arbitrary ordering of the nonempty cosets, any permutation of the $2^{s+1}-1$ hyperplanes represents a different assignment of hyperplanes to cosets, so we have $(2^{s+1}-1)!$ ways of matching the hyperplanes to the remaining cosets. Now, given a mapping of hyperplanes to cosets, we look out how changing coset representatives changes the set we construct. For some t, tH_i is itself a coset of H_i. Inside each coset of E, say gE, we have two cosets of H_i, namely gH_i and geH_i, for some $e \in E$ such that $E \notin H_i$. We then have two choices for where each hyperplane may lie in the coset it has been assigned to. Thus, we must multiply our total count by $2^{2^{s+1}-1}$, to get $2^{s+1}!(2^{2^{s+1}-1})$. □

Corollary 2.4.2. For a group G of order 2^{2s+2}, if there is some $E \subseteq Z(G)$ such that $E \cong C_2^{s+1}$, then G has at least $2^{s+1}!(2^{2^{s+1}-1})$ difference sets when we ignore equivalence classes.

Proof. By the final observation made concerning the spread construction above, every set constructed via a spread construction over E is a difference set, and by Theorem 2.4.1 there are $2^{s+1}!(2^{2^{s+1}-1})$ such sets. □

So, restricting our attention to groups of order 16, we see that each spread construction in a group of order 16 generates $2^{1+1}!(2^{2^{1+1}-1}) = 4!2^3 = 192$ potential difference sets. Furthermore, if a group of order 16 has a subgroup isomorphic to $C_2 \times C_2$ in its center, then it has at least 192 difference sets, ignoring equivalence classes. It should be noted that not all difference sets generated via a spread construction over the same subgroup are equivalent, as we will show below that in several groups with more than one inequivalent difference set, the spread construction generates all of the group's difference sets.

We saw the number 192 come up quite a bit in Table 2.2.1 and Table 2.2.2. We in no way claim to have explained the reason for every occurrence. However, we will show below that the spread construction can be used to generate all difference sets in several groups of order 16, so Theorem

2.4.1 and Corollary 2.4.2 shed some light on why this number occurs so often. Another number that consistently occurs in these two tables is 64. As it turns out, we can explain many of these occurrences via counting spread constructions as well.

Theorem 2.4.3. Let G be a group of order 16 with a normal subgroup E isomorphic to $C_2 \times C_2$. Then a spread construction over E generates at least 64 difference sets.

Proof. Let $\{t_1, t_2, t_3, t_4\}$ be a transversal of E, and let H_1, H_2, H_3 be the order 2 subgroups of E. We know, from [4], that there will always be some assignment of hyperplanes to cosets that yields a difference set. Let $t_1H_1 + t_2H_2 + t_3H_3$ be one such difference set that we know must exist. If the map $H_i \to t_iH_it_i^{-1}$ were not a permutation, then $\{t_iH_i * t_i^{-1}\}$ could not be a 1-design, for it would fail to contain one of the elements of E^*. Therefore, $H_i \to t_iH_it_i^{-1}$ must be a permutation of the H_i. Consider the maps $H_i \to t_jt_iH_it_i^{-1}t_j^{-1}$ for $j \in \{1, 2, 3, 4\}$. As conjugation is an automorphism which maps subgroups to subgroups, these 4 maps are all permutations of the H_i as well. These four maps correspond to four distinct placements of the H_i into cosets of E. Clearly, when $H_i \to t_iH_it_i^{-1}$ is a permutation, then $\{t_iH_i * t_i^{-1}\}$ is a 1-design.

We can do even more by noting that E, as a normal subgroup, must intersect the center of G nontrivially, a standard result which can be proven using the conjugacy class equation. So E must contain some nonidentity element that is in the center of G, and this means one of the H_i is in the center of G. This H_i is fixed under conjugation by any element of G, and thus given any of the four placements into cosets above we can swap this H_i to the unused coset and still preserve the fact that the map is a permutation. This gives a total of $4 \cdot 2 = 8$ placements of the H_i into cosets.

As each H_i is of index 2 in E, there are two choices for how to position each H_i in its coset (see proof of Theorem 2.4.1). Combined, this means there are $8 \cdot 2^3 = 64$ total sets where the map $H_i \to t_iH_it_i^{-1}$ is a permutation of the H_i, and thus each of these 64 sets is a difference set.

□

2.5 Difference Set Transfers via The Spread Construction

Having introduced the spread construction and briefly discussed some immediate enumerative results, we are now ready to use it to explain difference set transfers. This subsection will be focused almost entirely around Theorem 2.5.3, a theorem that requires some substantial machinery, which we will now introduce.

An element $T = \sum_{g \in G} t_g\, g$ in $\mathbb{Z}[G]$ is called a perfect ternary array of energy v, or $PTA(v)$, if $t_g \in \{-1, 0, 1\}$ for all $g \in G$, and $TT^{(-1)} = v1_G$. It then follows that $D \in \mathbb{Z}[G]$, where $|G| = 4m^2$, is a Hadamard difference set if and only if $\hat{D}$ is a $PTA(4m^2)$. It was shown in [1] that the associate of every Hadamard difference set in a group G of order 16 could be represented as the product of two $PTA(4)$s of the form $T = 1 - a - b - ab$, translated on the left by some element of G. It was also shown in [1] that every $PTA(4)$ in the canonical form given above was of one of two types: (1) $T = 1 - a - b - ab$, where a has order 2 and a and b commute, or (2) $T = 1 - a - b - ab$ and $< a, b >$, the group generated by a and b, is isomorphic to the quaternion group. Clearly, the translation of a product of two $PTA(4)$s is the associate of a Hadamard difference set, as, letting T_1, T_2 be $PTA(4)$s, $(gT_1T_2)(gT_1T_2)^{(-1)} = gT_1T_2T_2^{(-1)}T_1^{(-1)}g^{-1} = 4gT_1T_1^{(-1)}g^{-1} = 16gg^{-1} = 16$. This gives us the following theorem.

Theorem 2.5.1. Let G be a group of order 16. $D \in \mathbb{Z}[G]$ is a Hadamard difference set if and only if $\hat{D}$ is the product of two $PTA(4)$s, each of type (1) or type (2), translated on the right by an element of G, i.e. $\hat{D} = gT_1T_2$.

Note that the nonidentity elements in the two factors of a difference set must be unique, as otherwise we would get two identical elements in their product, and would therefore be unable to scale each element of G with either a 1 or a -1 in the 16 element product.

We now must define some basic group theoretic tools, starting with a special subgroup known as the socle. Noting that a subgroup $N \triangleleft G$ is called a *minimal normal subgroup* when there are no groups $H \subset N$ such that $H \triangleleft G$, we define the socle of G, $soc(G)$, to be the group generated by all minimal normal subgroups in G. Clearly, $soc(G)$ is a characteristic subgroup of G, as an automorphism bijectively maps normal subgroups to normal subgroups, and therefore must map minimal normal subgroups to minimal normal subgroups. Therefore, $soc(G) \triangleleft G$. The following lemma is a standard part of literature on p-groups.

Lemma 2.5.2. The socle of a finite p-group G is made up of all elements in $Z(G)$ that have order p.

Proof. Let G act on itself via conjugation. By the orbit stabilizer lemma, the size of each conjugacy class is a power of p. Because the sum of the sizes of the conjugacy classes must equal the size of G, and because the identity is in its own conjugacy class, we must have at least $p-1$ nonidentity elements in their own conjugacy class. So, $Z(G)$ is nontrivial. Similarly, if $N \triangleleft G$ and we let G act on N via conjugation, then there must be at least $p-1$ fixed points in N. So, $N \cap Z(G)$ must be nontrivial. Because every subgroup of the center is normal, any normal subgroup of order greater than p has a proper subgroup that is normal in G. Therefore, the only minimal normal subgroups are the subgroups of $Z(G)$ of order p. □

We now turn to the central theorem of this section.

Theorem 2.5.3. Let G be a group of order 16 that does not contain a subgroup isomorphic to the quaternion group. If the socle of G has order 4, then every difference set in G can be generated via a spread construction over $soc(G)$.

Proof. For convenience, we will denote $soc(G)$ by N. Let $D \subset G$ be a difference set. We know from Theorem 2.5.1 that $D = gT_1T_2$, a translation of the product of two $PTA(4)$s. Because G has no subgroup isomorphic to the quaternion group, these must both be type (1).

We claim that the nonidentity elements of each T_i consist of one element in N and two elements in some coset g_1N. To see this, we first suppose that the designated commuting involution, a, lies outside of N. Because $N \subseteq Z(G)$, a commutes with every element of N, as well as every element of aN. If a were to commute with some element outside of $N \cup aN$, a set of index 2, then, by LaGrange's Theorem, $C_G(a)$ would be the whole group, in which case a would necessarily be in the socle, a clear contradiction. So, we must have $C_G(a) = N \cup aN$. Then, the b chosen so that it commutes with a must be either in N or in aN. In both cases, the product ab will be in the coset we need it to be in, and our claim is proven. If $a \in N$, then b cannot be a member of N, for then their product would be the third nonidentity element of N. We would then not be able to produce a second $PTA(4)$, as the above case (where we show $a \notin N$) shows that any $PTA(4)$ must contain an element of N, and we cannot repeat any elements. Then, we must multiply $b \in bN \neq N$ by $a \in N$, implying that $ab \in bN$, and thereby proving the claim in both cases.

We now will show that the element of T_i that lies in N determines the hyperplane translate formed by the other two nonidentity elements of T_i. Let n_i denote the nonidentity element in $T_i \cap N$. If n_i is the product element ab, where a is the commuting involution, then $b = an_i$, and $\{a, b\} = a\{1, n_i\}$. Alternatively, if T_i is of the form $1 - c - n_i - cn_i$, whether n_i is the designated commuting involution or not, then clearly the two elements in T_i not in the socle form the hyperplane translate $c\{1, n_i\}$.

Because $n_1 \neq n_2$, the hyperplanes $\{1, n_1\}$ and $\{1, n_2\}$ are distinct. Because $N \cong C_2 \times C_2$, $\{n_1, n_2\} = n_1\{1, n_1 n_2\}$, which is a translate of the third hyperplane of N. We also know that the hyperplane translate in T_1 and the hyperplane translate in T_2 must lie in distinct cosets, for otherwise they would have a nonempty intersection. To see this, simply note that in aN, $\{1, n_1\}$ can be sent to $\{a, an_1\}$ or $\{an_2, an_1n_2\}$ and $\{1, n_2\}$ can be sent to $\{a, an_2\}$ or $\{an_1, an_1n_2\}$. So, the elements with negative scalars in T_1T_2, i.e. the difference set generated by these two $PTA(4)$s, will form a set containing a translate of each hyperplane of N, each contained in a unique coset of N. Symbolically, $T_1T_2 = (G \setminus S) - S$, where $S = x(1+n_1) + y(1+n_2) + n_1(1+n_1n_2)$, and $x \notin yN$. Translating T_1T_2 by some element in g, we get $(G \setminus S') - S'$, where $S' = gx(1+n_1) + gy(1+n_2) + gn_1(1+n_1n_2)$, which, because translation permutes cosets, is a difference set of spread form. □

Though this theorem is interesting in its own right, providing insight into the structure of difference sets in groups of order 16, our main motivation for proving and presenting it was to explain the transfers we had observed. Let G_i denote the group with Gap ID $[16, i]$. We prove a quick lemma, before getting to our central result.

Lemma 2.5.4. Given the presentations given for G_2, G_3, G_4, and G_{11} in table 2.3.1, the socle of each of these groups is $\langle f_3, f_4\rangle$.

Proof. We will employ lemma 2.5.2, showing that f_3, f_4, and f_3f_4 are the only central elements of order 2 in each group.

1. It is easy to see that $G_2 = \langle f_1, f_2 | f_1^4 = f_2^4 = [f_1, f_2] = 1\rangle$ only has 3 elements of order 2, namely $f_1^2 = f_3$, $f_2^2 = f_4$, and $f_1^2 f_2^2 = f_3 f_4$. Because G_2 is abelian, all of these elements are in $Z(G_2)$.

2. Looking to the presentation of G_3 in table 2.3.1, it is clear that f_3 and f_4 are both central. Combining this with the fact that $f_2 f_1 = f_1 f_2 f_3$, we see that any element containing an f_1 in its normal form will not commute with f_2, while any element containing an f_2 in its normal form will not commute with f_1. Thus, $Z(G_3) = \langle f_3, f_4\rangle$, and because $|f_3| = |f_4| = 2$, we see that $soc(G_3) = \langle f_3, f_4\rangle$.

3. The argument for G_4 is literally identical to the argument just given for G_3, due to immense similarities in their given PC presentations.

4. We may use a nearly identical argument as above again for G_{11}, with the only difference being that $f_2 f_1 = f_1 f_2 f_4$ instead of $f_1 f_2 f_3$. Clearly, this change does not alter the stated implications.

□

Corollary 2.5.5. Given the presentations in table 2.3.1, let D be a set of words on $\{f_i | 1 \leq i \leq 4\}$. Then, the following are equivalent:

1. D forms a difference set in G_2

2. D forms a difference set in G_3

3. D forms a difference set in G_4

4. D forms a difference set in G_{11}

Proof. By Theorem 2.5.3 and Lemma 2.5.4, every difference set in G_i, where $i \in \{2, 3, 4, 11\}$, is a spread construction over $\langle f_3, f_4 \rangle$. From this, the result follows.

□

Corollary 2.5.5 is certainly the most powerful, and most immediate, result we can derive from Theorem 2.5.3. However, there are a couple more results we can derive from this theorem to further explain difference set transfers. Once again, we start with a lemma.

Lemma 2.5.6. In G_{10}, G_{12}, and G_{14}, $\{f_3, f_4\} \in Z(G)$, and $|f_3| = |f_4| = 2$, while in G_{10} and G_{14} we can say the same for $\{f_2, f_4\}$.

Proof. This result can be easily obtained by examining Table 2.3.1 □

Corollary 2.5.7. When considered as words over $\{f_i | 1 \leq i \leq 4\}$, every difference set in G_2, G_3, G_4, and G_{11} is also a difference set in G_{10}, G_{12}, and G_{14}.

Proof. We know that if some group of order 16 has a subgroup $S \cong C_2 \times C_2$ such that $S \subseteq Z(G)$, then every set constructed via the spread construction over S is a Hadamard difference set. Thus, by Corollary 2.5.7, every spread construction over $\{f_3, f_4\}$ is a difference set in G_{10}, G_{12}, and G_{14}. The result then follows from Corollary 2.5.5. □

We finally prove one last structural lemma, before deriving our final corollary of Theorem 2.5.3.

Lemma 2.5.8. Given the presentation given for G_5 in table 2.3.1, $soc(G_5) = \langle f_2, f_4 \rangle \cong C_2 \times C_2$.

Proof. $G_5 = \langle f_1, f_2 | f_1^8 = f_2^2 = [f_1, f_2] = 1 \rangle$. It is fairly easy to see that there are only 3 elements of order 2 in this group, namely $f_1^4 = f_4, f_2$, and $f_2 f_1^4 = f_2 f_4$, and because G_5 is abelian, these elements are all in $Z(G_5)$. □

Corollary 2.5.9. When considered as words over $\{f_i | 1 \leq i \leq 4\}$, every difference set in G_5 is also a difference set in G_{10} and G_{14}.

Proof. By Theorem 2.5.3 and Lemma 2.5.8, every difference set in G_5 can be constructed via a spread construction over $\langle f_2, f_4 \rangle$. By Lemma 2.5.6, these sets are all difference sets in G_{10} and G_{14} as well. □

2.6 Difference Set Transfers via Quaternion Subgroups

We will continue our slightly sporadic explanation of difference set transfers in groups of order 16 by using Theorem 2.5.1 in a slightly different setting. We will start by introducing a new difference set construction, which we will call the *half quaternion construction.*

Let G be a group such that $|G| = 16$. Suppose further that there is some $H \lhd G$ such that $H \cong Q_8$, the quaternion group. It is traditional to represent the quaternion group as $\langle \hat{\imath}, \hat{\jmath}, \hat{k}, n | \hat{\imath}^4 = \hat{\jmath}^4 = \hat{k}^4 = n^2 = 1, \hat{\imath}n = \hat{\imath}^{-1}, \hat{\jmath}n = \hat{\jmath}^{-1}, \hat{k}n = \hat{k}^{-1}, \hat{\imath}\hat{\jmath} = \hat{k}, \hat{\jmath}\hat{k} = \hat{\imath}, \hat{\imath}\hat{k} = \hat{\jmath}^{-1} \rangle$. If we give such labels to the elements of H, then we can follow one of two procedures to construct a difference set. (i) Select one element from each of the pairs $(\hat{\imath}, \hat{\imath}^{-1})$, $(\hat{\jmath}, \hat{\jmath}^{-1})$, $(\hat{k}, \hat{k}^{-1})$, $(n, 1)$, and place them in a set D, then add to D some element in $g \in G \setminus H$, and finally add the element gn, or (ii) let $g_1 \in G \setminus H$, and select one element from each of the pairs $(g_1\hat{\imath}, g_1\hat{\imath}^{-1})$, $(g_1\hat{\jmath}, g_1\hat{\jmath}^{-1})$, $(g_1\hat{k}, g_1\hat{k}^{-1})$, $(g_1 n, g_1)$, place them in a set D, than add to D some $h \in H$, as well as the element hn. Note that in construction (ii) the property of having one element in each pair does not depend on which coset representative we choose. In both cases, we will call D a *difference set of half quaternion type.* We now justify our calling D a difference set.

Theorem 2.6.1. A set D constructed using either procedure (i) or procedure (ii) is a difference set.

Proof. Let $D = D_1 + D_2$, where D_2 is the last two elements added to D, namely g and gn, for some $g \in G$. Then, $DD^{(-1)} = D_1D_1^{(-1)} + D_1D_2^{(-1)} + D_2D_1^{(-1)} + D_2D_2^{(-1)}$. We will first show that $D_1D_1^{(-1)} + D_2D_2^{(-1)} = 4 + 2H$. Note that, because $n \in Z(H)$ is the only element in H of order 2 in H, n is always fixed under conjugation by some element of G, so $n \in Z(G)$. Then, $D_2D_2^{(-1)} = (g + gn)(g^{-1} + g^{-1}n) = 2 + 2n$. Meanwhile, it is easy to check that if we formed D in procedure (i), then $D_1D_1^{(-1)} = 2 + 2(H \setminus \{n\})$. If we formed D in procedure (ii), however, then $D_1 = g_1D_1'$, where $g_1 \in G \setminus H$ and D_1' is some set formed in the way we would form D_1 in procedure (i). But then $D_1D_1^{(-1)} = g_1(2 + 2(H \setminus \{n\}))g_1^{-1} = 2 + 2(H \setminus \{n\})$.

We now turn to $D_1D_2^{(-1)} + D_2D_1^{(-1)}$. Because multiplying by n sends each element of $H \setminus \{1, n\}$ to its inverse, if D was created using procedure (i) then $D_1g_1^{-1} + D_1ng_1^{-1} = Hg_1^{-1} = g_1^{-1}H$, where $g_1 \in G \setminus H$, while if D was constructed with procedure (ii), we use similar notation as in the previous paragraph to see that $D_1g^{-1} + D_1ng^{-1} = g_1(D_1' + D_1'n)g^{-1} = g_1H$, where $g_1 \in G \setminus H$ and $g \in H$. Similarly, $D_2D_1^{(-1)} = G \setminus H$. But then $DD^{(-1)} = 4 + 2G$.

□

This construction was originally crafted with an eye towards general 2-groups, perhaps generating a difference set in any group with a generalized quaternion subgroup of index 2. Unfortunately, many groups with generalized quaternion subgroups of index 2 do not have difference sets at all, so this generalized construction failed to work out.

However, we are still in a position to use this specific construction to demonstrate the theory behind some more difference set transfers. We will here again be using Theorem 2.5.1 to classify the structure of all difference sets in a group of order 16. Here, we will be considering the modular group of order 16.

Theorem 2.6.2. Every difference set in G_8 is of the half quaternion type.

Proof. Because G_8 has a subgroup isomorphic to the quaternion group, we may here use $PTA(4)$s of either the quaternion type or of the commuting involution type. Because a $PTA(4)$ of the quaternion type must be of the form $1 - a - b - ab$, it can contain either $\hat{\imath}$, $\hat{\jmath}$, and $\hat{k}$, or it can contain two of these three elements multiplied by n, and the other one unaltered. Thus, any two quaternion $PTA(4)$s generated over a single quaternion subgroup must intersect. Because G_8 contains only one subgroup isomorphic to the quaternion group, it cannot contain two $PTA(4)$s of the quaternion type without them intersecting.

When we look at what $PTA(4)$s of the commuting involution type we can form in G_8, we see that we are also very restricted. We can discern from Table 2.3.1 that G_8 contains only 5 elements of order 2, namely f_4, f_2, f_2f_4, f_2f_3, and $f_2f_3f_4$. It is not immediately obvious, but not particularly difficult to use the relations in Table 2.3.1 to see that $C_G(f_2) = C_G(f_2f_4) = \langle f_2, f_4\rangle$ and $C_G(f_2f_3) = C_G(f_2f_3f_4) = \langle f_2f_3, f_4\rangle$. But then we see that each $PTA(4)$ of the commuting involution type must contain f_4, and must be of the form $1 - g - f_4 - gf_4$, for some $g \in G$. So, we cannot have a difference set that is the product of two $PTA(4)$s of the commuting involution type, and we then see that every difference set in G_8 must be the translation of the product of one $PTA(4)$ of each type.

Clearly, the product of one $PTA(4)$ of each type is a difference set of half quaternion type, constructed via procedure (i). But what happens when we multiply this product by some element of G? Recycling notation from the proof of Theorem 2.6.1, we can easily see that multiplying D_1

by any element in H will simply permute the pairs from which each element in D_1 comes, and perhaps switch the element of each pair that is chosen, neither of which will take D_1 out of the proper form. Multiplying D_1 by some element in $G \setminus H$, on the other hand, will simply place the elements into the other coset of H, and we will simply switch from a type (i) half quaternion construction to a type (ii) half quaternion construction. Furthermore, whichever coset D_2 lies in, $g_2\{g, gn\} = \{g_2g, g_2gn\}$, for any $g_2 \in G$, so multiplying D_2 will never take it out of its proper form. Thus, we can conclude that every difference set in G_8 is of half quaternion type. □

Corollary 2.6.3. Every difference set in G_8 is a difference set in G_9.

Proof. We can see from Table 2.3.1 that the one quaternion subgroup of G_8 is $\langle f_1, f_3, f_4\rangle$, while $\langle f_1, f_3, f_4\rangle$ is also a quaternion subgroup in G_9. By Theorem 2.6.1, G_9 contains all possible difference sets of the half quaternion type, generated over the group $\langle f_1, f_3, f_4\rangle$, and then by Theorem 2.6.2, the result follows.

□

2.7 Difference Set Transfers via Basic Algebra

We now turn a more direct proof of one difference set transfer. Although the relevant result will still be a corollary of the theorem whose proof we give in detail, the theorem will be mapping difference sets in one group to those in another, rather than simply classifying the structure of all difference sets in various groups. Letting $r = 2s + 2$, for some natural number s, we will be considering the groups C_2^r, which we will call G, and $C_4 \times C_2^{r-1}$, which we will call H. We will use the standard presentations of these groups, representing G as $\langle g_1, \dots, g_r | \forall i, j \in \{1, \dots, r\} g_i^2 = [g_i, g_j] = 1\rangle$, and representing H as $\langle h_1, \dots, h_{r-1} | h_1^4 = 1, \forall i, j \in \{2, \dots, r-1\} h_i^2 = [h_1, h_i] = [h_i, h_j] = 1\rangle$. We will let $[m]$ denote the set of numbers from 1 to m, i.e. $[m] = \{1, 2, \dots, m\}$.

Set $v = 2^r$, $k = 2^{2s+1} - 2^s$, $\lambda = 2^{2s} - 2^s$, and $n = k - \lambda = 2^{2s}$. Then, let $\alpha : [r] \times [k] \to \{0, 1\}$ be some function that maps ordered pairs of integers to a binary value. We will use α to assign exponents to the generators in G and H. Using α, we can generate two sets, $D_G = \{\gamma_j = g_1^{\alpha(1,j)} g_2^{\alpha(2,j)} \cdots g_r^{\alpha(r,j)} | j \in [k]\}$, and $D_H = \{\eta_j = h_1^{\alpha(1,j)+2\alpha(r,j)} h_2^{\alpha(2,j)} \cdots h_{r-1}^{\alpha(r-1,j)} | j \in [k]\}$. It is worth noting that these two sets are of the correct size to be Hadamard difference sets in a group of order 2^r. We now turn to a theorem that can be applied to infinitely many 2-groups.

Theorem 2.7.1. Given some function α, if D_G is a difference set in G then D_H is a difference set in H.

Proof. Our proof will revolve around the group ring products

$$D_G D_G^{(-1)} = \sum_{i,j=1}^{k} g_1^{\alpha(i,1)+\alpha(j,1)} \cdots g_r^{\alpha(i,r)+\alpha(j,r)} \qquad (1)$$

and

$$D_H D_H^{(-1)} = \sum_{i,j=1}^{k} h_1^{\alpha(i,1)-\alpha(j,1)+2(\alpha(i,r)+\alpha(j,r))} \cdots h_{r-1}^{\alpha(i,r-1)+\alpha(j,r-1)}. \qquad (2)$$

We start by noting that (1) contains every element in the subgroup $S_G = \langle g_2, g_3, \dots g_r\rangle$ exactly λ times if and only if (2) contains every element in $S_H = \langle h_1^2, h_2, \dots, h_{r-1}\rangle$ exactly λ times. This is because the statements (i) $g_2^{e_2} \cdots g_r^{e_r}$ occurs λ times in (1), and (ii) $h_1^{2e_r} h_2^{e_2} \cdots h_{r-1}^{e_{r-1}}$ occurs λ times in (2) are both equivalent to the statement there are exactly λ pairs $(p, q) \in [k] \times [k]$ such that $\alpha(p, i) + \alpha(q, i) = e_i$ for all $i \in [r]$.

We now assume that (1) contains each element of G λ times. So, (1) contains each element of S_G λ times, meaning (2) contains each element of S_H λ times. Furthermore, (1) contains each element of $g_1 S_G$ λ times. Because every element in G has order 2, $\gamma_i \gamma_j^{(-1)} = \gamma_j \gamma_i^{(-1)}$ for all $i, j \in [k]$. Thus, for some $g_1 s \in g_1 S_G$, $P(D_G)$, the power set of D_G, contains $\frac{\lambda}{2}$ unordered pairs (γ_i, γ_j) such that $\gamma_i \gamma_j = \gamma_j \gamma_i = g_1 s$. Similarly, there are $\frac{\lambda}{2}$ unordered pairs in $P(D_G)$ such that the product of the two elements in the pair is $g_1 s g_r$.

If $\gamma_i \gamma_j = g_1 s$, then, without loss of generality, we can assume $\gamma_i = g_1 s_1$ and $\gamma_j = s_2$, where $s_1, s_2 \in S_G$. Remembering our original definitions of γ_i and η_i, this implies that $\eta_i = h_1 t_1$ and $\eta_j = t_2$, where $t_1, t_2 \in S_H$ and for $i \in [r-1]$ the exponent of h_i in $t_1 t_2 = t$ is equal to the expoenent of g_i in s, while the exponent of g_r in s is equal to the expoenent of h_1^2 in t. Therefore, $\eta_i \eta_j^{(-1)} = h_1 t$, while $\eta_j \eta_i^{(-1)} = h_1^3 t$. So, we have both $h_1 t$ and $h_1^3 t$ occuring at least $\frac{\lambda}{2}$ times each in (2), once for each pair (γ_i, γ_j) such that $\gamma_i \gamma_j = g_1 s$. We can follow a similar procedure for each pair (γ_i, γ_j) such that $\gamma_i \gamma_j = g_1 s g_4$, and get $\frac{\lambda}{2}$ copies of $h_1 t h_1^2 = h_1^3 t$ and $\frac{\lambda}{2}$ copies of $h_1 t h_1^2 h_1^2 = h_1 t$. Thus, we have λ copies of $h_1 t$ and λ copies of $h_1^3 t$ in (2), for each $t \in S_H$, meaning D_H is a difference set in H.

□

We believed that we had proven Theorem 2.7.1 as a biconditional, but recently discovered a problem with the second half of our proof. However, based on computational evidence, we have a strong reason to believe that a biconditional still holds in general. Therefore, we will list the second half as a conjecture.

Conjecture 2.7.2. Given some function α, if D_H is a difference set in H then D_G is a difference set in G.

Luckily, most of our observations concern just groups of order 16. When we make the same restriction here, we do indeed have a proof for the biconditional.

Theorem 2.7.3. Let G and H be as defined above, with r set to 4 so that $|G| = |H| = 16$. Then D_G is a difference set in G if and only if D_H is a difference set in H.

Proof. We will recycle notation from the proof of Theorem 2.7.1, while we know from that same theorem that if D_G is a difference set in G, then D_H is a difference set in H. Furthermore, we know that (1) contains every element in the subgroup $S_G = \langle g_2, g_3, \ldots g_r \rangle$ exactly λ times if and only if (2) contains every element in $S_H = \langle h_1^2, h_2, \ldots, h_{r-1} \rangle$ exactly λ times.

Keep in mind here that $k = 6$ and $\lambda = 2$. Now, we suppose that (2) contains every element in H twice. We then know immediately that (1) contains every element in S_G twice, by the result stated at the end of the last paragraph. But we are also supposing that (2) contains every element of $h_1 S_H$ twice. Let $\eta_i \eta_j^{(-1)} = \eta_p \eta_q^{(-1)} = h_1 t$, for some $t \in S_H$. See that then, $\eta_j \eta_i^{(-1)} = \eta_q \eta_p^{(-1)} = (h_1 t)^{-1} = h_1^3 t$. We know by (2) that either (a) $\eta_i = h_1 t_1$ and $\eta_j = t_2$, for $t_1, t_2 \in \langle h_2, h_3 \rangle$, or (b) $\eta_i = t_1$ and $\eta_j = h_1^3 t_2$, for $t_1, t_2 \in \langle h_2, h_3 \rangle$. We can make a similar claim about η_p and η_q.

But suppose both pairs were of form (a), so that $\eta_p = h_1 t_3$ and $\eta_q = t_4$. Then $\eta_i \eta_p^{(-1)} = \eta_j \eta_q^{(-1)}$ implies that $h_1 t_1 t_3 h_1^{-1} = t_2 t_4 = t_4 t_2$, and we have three ways of comibing elements of D_H to make the same element, violating our assumption that D_H was a difference set. Similarly, if both pairs were of form (b) we would be violating our initial assumption. So, one of the pairs must be of form (a) and the other must be of form (b).

By the definition of γ_i and of η_i, we then know that then one of $\gamma_i\gamma_j = \gamma_j\gamma_i$ and $\gamma_p\gamma_q = \gamma_q\gamma_p$ equal to $g_1 s$, and the other is equal to $g_1 s g_4$, where the exponent of h_i in t is equal to the expoenent of g_i in s, for $i \in \{2,3\}$, while the exponent of g_4 in s is equal to the expoenent of h_1^2 in t.

If we repeat this process for each inverse pair of elements in H, we see that (1) contains every element of G exactly twice, so D_G is a difference set.

□

Corollary 2.7.4. When considered as words over $\{f_i | 1 \leq i \leq 4\}$, the difference sets in G_{10} and G_{14} are exactly the same.

Proof. We can see from Table 2.3.1 that in G_{10}, $f_4 = f_1^2$. Then, given our definitions of D_H and D_G above, the result follows from Theorem 2.7.3 □

2.8 Next Steps in Difference Set Transfers

We remain impressed with how pervasive difference set transfers are in 2-groups. Although we were only able to characterize transfers in groups of order 16, we believe that there are fully general results out there to be proven. We spent only about three weeks investigating this phenomenon, so what we have done here is just scratching the surface of what can be done.

We believe that there are likely grand overall theorems that can be used to explain vast swaths of our observations concerning difference set transfers. The study of difference set transfers is just beginning, and if it is given the time and attention that it deserves, there are almost certainly some fascinating and illuminating results to be drawn from it.

3 Extended Building Sets

3.1 Introduction

James A. Davis and Jonathan Jedwab co-authored a paper titled *A Unifying Construction for Difference Sets* that features exactly what its title alludes to: another method for constructing difference sets. Applicable to those of the Hadamard type, Davis and Jedwab create a recursive construction that relies on three major concepts, which we shall now define.

Definition 3.1.1. For a finite multiplicative group G of order $m * u$, where m is the modulus of G and u is the order of $U \trianglelefteq G$, we call R, a k-element subset of G, a (m, u, k, λ) **relative difference set (RDS)** in G relative to U if every element of $G - U$ is contained in $\{r_1 r_2^{-1} \mid r_1, r_2 \in R, r_1 \neq r_2\}$ exactly λ times.

Definition 3.1.2. A building block in a group G with modulus m is a subset of G such that all nonprincipal character sums over the subset have modulus either 0 or m. A collection of t building blocks in G with modulus m, each containing a elements, is known as a (a, m, t) **building set (BS)** on a group G relative to a subgroup U, where for each nonprincipal character of G, either precisely one building block has nonzero character sum or none of the building blocks have nonzero character sum depending on whether the character is nonprincipal or principal on U, respectively.

Definition 3.1.3. Suppose we have a collection of building blocks B_i, $i \in \{1, 2, ..., h\}$, of elements in the group G. Suppose further that $h-1$ blocks have a elements and one block has $a \pm m$ elements, where $\sum_i \mid B_i \mid = (h-1)a + (a \pm m) = ha \pm m$, which must equal $2m^2 \pm m$ (the parameter k for Hadamard difference sets), where $+$ or $-$ must be preserved. The collection of these sets is referred to as a (a, m, h, $\pm$) **extended building set (EBS)** with respect to a subgroup U, where for each nonprincipal character of G, either precisely one building block has nonzero character sum of none of the building blocks have nonzero character sum depending on whether the character is principal or nonprincipal on U, respectively.

The ultimate goal of the Davis-Jedwab construction is to find a *covering* extended building set, which means that the EBS is relative to the trivial subgroup. We now make a critical observation. A difference set, in general, is actually a relative difference set where $U = 1_G$. To give an analogy, a building set is to a relative difference set as a (covering) EBS is to a difference set for a group G. Thus, we have a difference set in G through this relation with the trivial subgroup! This process of creating extended building becomes noticeably more difficult as the size of the group grows; however, the fact that this construction is recursive by nature allows for a covering EBS on G to be "lifted" to another group $G^{'}$ that contains G fairly easily.

One of the primary tools that the authors use in their difference set construction is character theory, as indicated in the above definitions. To be brief, the group of characters of G is isomorphic to G itself and contains all possible homomorphisms (the characters) from G to the complex roots of unity, a multiplicative group. An extended building set contains only one building block with nonzero character sum for every nonprincipal character of G, with the term "nonprincipal" describing characters which do not map every element of G to the identity element, **1**, of the group of complex roots of unity. We would like to note here that Ken Smith provided the covering EBS for $G \cong C_4 \times C_4$ and Jim Davis provided the covering EBS for $G \cong C_8 \times C_8$, likely using these character properties to do so.

Given these, however, we were able to do two things: first, create our own covering EBS for $G \cong C_2 \times C_2$ and for $G \cong C_3 \times C_3$, since these groups are smaller and therefore easier to manipulate to construct building blocks; second, examine these extended buildings sets and find patterns that do not rely on character theory in order to provide new guidelines for creating an covering EBS. This has led to our development of **quasi-difference sets**, which we will explain in detail after the presentation of our results in order to accurately portray the progression of our research. These new sets, which exist in $C_m \times C_m$, are, in a sense, shadows of the Hadamard difference sets found in groups of order $4m^2$ since they uphold similar parameters to those of their larger counterparts. Moreover, quasi-difference sets are distinct from relative difference sets because the latter is a result of building sets while the former is a result of extended building sets. It seems, however, that this new way of looking at the EBS construction is only applicable to groups where $m = 2^n$, $n \in \mathbb{N}$, $n \geq 2$.

We shall cite three important theorems from *Unifying Construction.* The first, appearing as Theorem 2.4 in the paper, makes explicit the "lifting" process utilized in our EBS algorithm. The second theorem, appearing as Theorem 4.3, illustrates the origins of this "lifting" process: finding a building set in the p^r quotient groups and injecting them into G to obtain a building set. The third theorem, appearing as Theorem 3.1.5, bridges these first two theorems. We omit the proofs but encourage readers to find them in [2].

Theorem 3.1.4. Suppose there exists a $(a,\, m,\, h,\, \pm)$ covering EBS on a group G. Then there exists an $(h \mid G \mid, ah \pm m, ah \pm m - m^2, m^2)$-difference set in any group $G^{'}$ containing G as a subgroup of index h.

We note the importance of Theorem 3.1.4. The proof construction proves that shifting any building block B by an element of the group G still results in a building block and, in fact, is another choice for building blocks when making the extended building set.

Theorem 3.1.5. Let G be a group of order $p^{2r}a$ containing a subgroup $Q \cong \mathbb{Z}_p^{2r}$, where p is prime. Let $H_0, ..., H_{p^r}$ be the subgroups of G of order p^r corresponding to hyperplanes when viewed as subgroups of Q. Suppose there exists a $(a, \sqrt{at}, t)$ building set on G/H_i relative to Q/H_i for each $i = 1$, ..., p^r. Then there exists a $(p^r a, p^r\sqrt{at}, p^r t)$ building set on G relative to H_0.

Theorem 3.1.6. Let G be a group of order u^2am containing a subgroup U of order u. Suppose there exists a $(am, m, h, \pm)$ covering EBS on G/U and there exists a (a^2t, at, t) BS on G relative to U, where $um = at$. Then there exists a $(uam, um, h+t, \pm)$ covering EBS on G.

In the context of Hadamard difference sets, Theorem 3.1.4 indicates that any difference set in a group of order $4m^2$, whose parameters could be expressed as indicated in the theorem, originates from an extended building set that covers a group of order m^2, which itself gives a difference set in this smaller group. Davis and Jedwab use character theory to show how a covering EBS for a group G relates to a covering EBS for a group $G^{'}$ containing G as a subgroup with index $h = 4$, thus leading to the utilization of four building blocks in our algorithm. This covering EBS for $G^{'}$ then gives a difference set for that group. The proof of Theorem 3.1.4, meanwhile, shows how the idea of using quotient groups and coset representatives to build difference sets begins with constructing the building sets, which again relate to relative difference sets. The subgroups of Q (and G by extension) correspond to hyperplanes in the Galois field of size p^{2r} under an isomorphism between Q and $GF(p^r)$. Disregarding H_0, the building blocks formed for the quotient groups G/H_i using the generators of G are "lifted" into G to create the building set for this group, with H_0 becoming our U. To create a covering EBS on G, we find a covering EBS for G/U and combine it with the BS we have already constructed on G, as indicated by Theorem 3.1.6.

We will now look at how the EBS construction is implemented using GAP.

3.2 Algorithm

The algorithm we used to create difference sets with the Davis-Jedwab EBS construction technique begins with identifying the GAP index of the group we are going to use as our G from Theorem 3.1.4. We decided to restrict ourselves to looking at $G \cong C_m \times C_m$, where m is a natural number greater than one. Hence our EBS construction will only work in groups that contain a subgroup isomorphic to $C_m \times C_m$.

Next we generated the list of elements of G in GAP and stored it in a variable. Since GAP maintains the same number of generators for each group of equal size (i.e. the number of components in the elementary abelian group), we needed to search for two elements in G that generated the entire group. These were always the second and third elements in the list, which were denoted f1 and f2. With these generators, we were able to construct our extended building sets. Since $G \cong C_m \times C_m$ has order m^2 and we are looking at G in the context of larger groups with order $4m^2$, we will always have four building blocks in our covering EBS, three of size a and one of size $a \pm m$. Each building block is, by design, the union of particular subgroups of G; this is more clear with the examples in the subsequent section.

The set-up is now complete and we may dive into the heart of the code. It begins with a for loop that allows us to search for Hadamard difference sets over all groups of a particular size; this index is represented by the variable *cn*. Within the for loop, we set a variable, which we call *found*, equal to false, the reason being clear later. Then we create a variable to store our groups of size $4m^2$, which correspond to $G^{'}$ in Theorem 3.1.4, as we move through this initial for loop. Now we must find all subgroups of $G^{'}$ isomorphic to G. We accomplish this using the *Filtered* function in GAP, and we store these subgroups in a list, which we call K. After creating another for loop that cycles through these subgroups, we create an if statement that breaks the code if a difference set has been found (this is because we only care about the existence of a difference set rather than finding all inequivalent ones). Again, this will make more sense later. In order for GAP to recognize the subgroups of $G^{'}$ isomorphic to G, we utilized the *IsomorphismGroups* function to create an isomorphism between G and each element of K. We are thus able to use the *RightCosets* function to create a list of coset representatives of the elements of $G^{'}/K$.

With this list of coset representatives, we create yet another for loop that moves through the elements of the permutation group of size four, denoted S_4. This is because the main idea behind this EBS construction is consider all possible permutations of our coset representatives with respect to our four building blocks. In other words, we want to search through the 24 distinct matchings of buildings blocks and coset representatives and find the first one that yields a Hadamard difference set. The first item in this for loop is instantiating our list of elements of our potential difference set, which we designate as empty for now. Then, using a pair of for loops, we essentially inject the elements of our covering EBS into $G^{'}$ by multiplying each building block by one of the coset representatives. These elements are appended to our list of "proposed" difference set elements.

The final step of our algorithm is to call the *DiffsetTest* function that we created, which checks whether or not a given set of element meets the criteria to be a Hadamard difference set. If this returns true, then we set our variable *found* to be true and the for loop which moves through all of our subgroups isomorphic to G breaks. This process continues into the next $G^{'}$ of a given order. It is critical to understand that the building blocks are formed without the influence of $G^{'}$, as indicated by Theorem 3.1.4. This permits the "lifting" process to extend to infinite families of difference sets.

We share our results in the next section, examining the cases of $m = 2$, 3, 4, and 8. Attempts have been made for the cases $m = 5$, 6, and 7, but with no success. Only one difference set has been found in groups of order 100 (see [8]) and, according to [7], only one group of order 196 could possibly have a difference set, which has not been found yet; on the other hand, we are aware that numerous difference sets in groups of order 144 (see [9]) have been found.

3.3 Results

When referring to groups, which appear in the left-hand columns of the tables below, we use the notation (u, v), where u is the size of the groups, and v is the GAP ID. The tables also include the list of GAP indices emitted by our algorithm that make a Hadamard difference set. We will reiterate that we found the extended building sets for the first two groups sizes while we were provided the extended building sets for the last two groups sizes. The EBS algorithm took mere seconds to search for difference sets in groups of order 16 and 36, a couple of minutes for groups of order 64, and roughly five days for groups of order 256 (but, given how we restricted G, it is basically unnecessary to search after a certain GAP index since groups beyond that point definitely do not contain G as a subgroup).

Note that we list the covering extended buildings sets used to find the difference sets. By Theorem 3.4, each building block can, in fact, be acted on by an element in the group and still be a building block, and thus we still have an covering EBS.

- **Groups of order 16:**

  - $G = \mathbf{C_2} \times \mathbf{C_2}$

    1. $B_1 = \langle x, y\rangle$, $B_2 = \langle y\rangle$, $B_3 = \langle x\rangle$, $B_4 = \langle xy\rangle$.
       Emitted HDSs:
       (16,2): [7, 10, 12, 13, 14, 15]
       (16,3): [3, 4, 6, 11, 12, 15]
       (16,4): [7, 10, 12, 13, 14, 15]
       (16,5): [6, 11, 12, 13, 14, 15]
       (16,6): [3, 5, 6, 11, 13, 15]
       (16,10): [6, 11, 12, 13, 14, 15]
       (16,11): [2, 5, 6, 11, 13, 14]
       (16,12): [7, 10, 12, 13, 14, 15]
       (16,13): [2, 5, 6, 11, 13, 14]
       (16,14): [6, 11, 12, 13, 14, 15]

    Hence 10 out of 12 possible groups of order 16, of which there are 14, emit Hadamard difference sets with this method.

- **Groups of order 36:**

  - $G = \mathbf{C_3} \times \mathbf{C_3}$

    1. $B_1 = \langle y\rangle \cup x^2\langle y\rangle$, $B_2 = \langle xy\rangle$, $B_3 = \langle x^2y\rangle$, $B_4 = \langle x\rangle$.
       Emitted HDSs:
       (36,6): [4, 12, 19, 23, 29, 35, 2, 16, 33, 7, 32, 34, 1, 3, 9]
       (36,7): [1, 5, 11, 13, 22, 31, 2, 17, 34, 3, 29, 30, 6, 14, 24]
       (36,8): [1, 4, 9, 12, 19, 29, 2, 15, 32, 5, 30, 31, 8, 16, 25]
       (36,9): [6, 15, 24, 26, 32, 36, 2, 17, 34, 3, 29, 30, 1, 4, 11]
       (36,10): [1, 5, 11, 13, 22, 31, 2, 17, 34, 3, 29, 30, 6, 14, 24]
       (36,12): [3, 10, 19, 21, 29, 35, 2, 17, 34, 6, 32, 33, 1, 4, 11]

(36,13): [1, 5, 11, 13, 22, 31, 2, 17, 34, 3, 29, 30, 6, 14, 24]
(36,14): [1, 5, 11, 13, 22, 31, 2, 17, 34, 3, 29, 30, 6, 14, 24]

2. $B_1 = \langle y\rangle \cup x^2\langle y\rangle$, $B_2 = x\langle xy\rangle$, $B_3 = x^2\langle x^2y\rangle$, $B_4 = \langle x\rangle$.
   Emitted HDSs:
   (36,6): [4, 12, 19, 23, 29, 35, 6, 18, 25, 24, 26, 28, 1, 3, 9]
   (36,7): [1, 5, 11, 13, 22, 31, 7, 18, 27, 19, 20, 21, 6, 14, 24]
   (36,8): [1, 4, 9, 12, 19, 29, 6, 17, 24, 20, 22, 23, 8, 16, 25]
   (36,9): [6, 15, 24, 26, 32, 36, 7, 18, 27, 19, 20, 21, 1, 4, 11]
   (36,10): [1, 5, 11, 13, 22, 31, 7, 18, 27, 19, 20, 21, 6, 14, 24]
   (36,12): [3, 10, 19, 21, 29, 35, 7, 18, 27, 24, 25, 26, 1, 4, 11]
   (36,13): [1, 5, 11, 13, 22, 31, 7, 18, 27, 19, 20, 21, 6, 14, 24]
   (36,14): [1, 5, 11, 13, 22, 31, 7, 18, 27, 19, 20, 21, 6, 14, 24]

Hence 8 out of 9 possible groups of order 36, of which there are 14, emit Hadamard difference sets with this method. We put two constructions to illustrate that different EBSs emit different Hadamard Difference Sets.

- **Groups of order 64:**

  ∗ $G = \mathbf{C_4} \times \mathbf{C_4}$

  1. $B_1 = \langle x^2, y^2\rangle \cup x\langle y\rangle$,
     $B_2 = \langle x^2y\rangle$,
     $B_3 = \langle x\rangle \cup y\langle xy^2\rangle$,
     $B_4 = \langle xy\rangle \cup y\langle xy^3\rangle$.

  Hence 140 out of 259 groups of order 64, of which there are 267, emit Hadamard difference sets with this method, which we will not list for the sake of brevity.

- **Groups of order 256:**

  ∗ $G = \mathbf{C_8} \times \mathbf{C_8}$

  1. $B_1 = \langle x^4, y^2\rangle \cup x^2\langle y\rangle \cup x\langle x^4y\rangle$,
     $B_2 = \langle x^2, y^4\rangle \cup y\langle x^2y^2, y^4\rangle \cup x\langle x^2y\rangle \cup xy\langle x^2y^3\rangle$,
     $B_3 = \langle x\rangle \cup y\langle xy^2\rangle \cup y^2\langle xy^4\rangle \cup y^3\langle xy^6\rangle$,
     $B_4 = \langle xy\rangle \cup y\langle\ xy^3\rangle \cup y^2\langle xy^5\rangle \cup y^3\langle xy^7\rangle$.

  Hence 779 groups of order 256, of which there are 56,092, emit Hadamard difference sets with this method, which we will not list for brevity. We are unsure of the number of groups of this size that do not have an HDS due to known nonexistence results.

One item we would like to make note of is that we do not need to have a covering EBS that contains all of the elements of G; remember this "covering" property is based on character sums. We can observe such a phenomenon with the covering EBS for $C_4 \times C_4$. We also notice that each building block of does **not** have to contain the identity 1_G, as proven by the second covering EBS on groups of order 36. We do believe, though, that the building block with $a \pm m$ elements must contain the identity element in order for this algorithm to produce a difference set. This is because the subgroup H_0 of Q in Theorem 1.2 is our subgroup U used in the definitions given in the beginning of this paper, thus serving as the kernel in the "lifting" process from G/U to G to $G^{'}$. Furthermore, the fact that we were able to find more than one covering EBS in the first place for $C_3 \times C_3$ has led to the following theorem for any abelian group.

Theorem 3.3.1. Given an $(a, m, h, \pm)$ extended building set $\phi = \{B_1, B_2, \dots, B_h\}$ that covers a group G, and, without loss of generality, letting the block B_h be the $a \pm m$ block, containing the identity element. For any $h' \in \{1, 2, \dots, h-1\}$ and any $g \in G$, $\phi' = \{B_1, \dots, g'B_{h'}, \dots, B_h\}$ is also a covering extended building set on G.

This follows from the proof of Lemma 2.3 in [2] with s = 1 and thus forcing the condition that $G^{'}$ is G. We will restate the lemma here.

Lemma 3.3.2. Suppose there exists a $(a,\ m,\ h,\ \pm)$ covering EBS on a group G. Then there exists a $(as,\ m,\ h/s,\ \pm)$ covering EBS on $G^{'}$, where s divides h and $G^{'}$ is any group containing G as a subgroup of index s.

In the proof of this lemma, Davis and Jedwab explicitly shift the elements of the building blocks, which are located in G, via multiplying them by elements of $G^{'}$. They then show that the character properties necessary for a covering EBS still hold after this transformation. Accordingly, Theorem 3.4 indicates that "shifting" a building block within a covering EBS for G will maintain the required properties of a covering EBS. An example of this would be to take the covering EBS for $C_4 \times C_4$ and modifying it in the following manner:

1. $B_1 = \langle x^2,\ y^2 \rangle \cup x\langle y \rangle$
2. $B_2 = \langle x^2 y \rangle$
3. $B_3 = y\langle x \rangle \cup y^2\langle xy^2 \rangle$
4. $B_4 = \langle xy \rangle \cup y\langle xy^3 \rangle$.

It is easy to check that by "shifting" the third building block via left multiplication by y yields a different building block than in the previous example, and the algorithm still emits a Hadamard difference set for all 140 groups it previously worked for.

Another interesting observation we have made is how the value of m influences which groups emit difference sets. To expound, for $m = 2$ and $m = 3$, groups that contained a normal subgroup isomorphic to $C_m \times C_m$ would only emit difference sets. This means that, for instance, group (36,11) in GAP did not emit a difference set because the subgroup isomorphic to $C_m \times C_m$ is **not** normal. For the non-prime values of m that we looked at, there is no such "surface-level" indicator of why certain groups containing $C_m \times C_m$ as a subgroup do not emit difference sets with our algorithm. The groups of order 64 with this phenomenon have indices 25, 28, 45, 102, 124, and 125; those of order 256 have indices 167, 168, 169, 444, 447, 4657, 4658, 5034, 5035, 5298, 5299, 5300, 5352, and 5353. For the most part, these groups appear close together in GAP's ranking system, which suggests some structural similarities that might explain these observations.

The above examples also demonstrate the use of both addition and subtraction in covering EBS parameters. We shall explore this concept in more detail. The nature of the covering EBS over G is that the total number of elements equals the number of elements, k, of the Hadamard difference set in $G^{'}$, as demonstrated in Definition 3.1.3. Thus we have the equation $ha \pm m = 2m^2 \pm m$. Given a particular value of m for $G \cong C_m \times C_m$, we can solve this equation for a (since we know $h = 4$ when aiming to create an HDS) to give us the size of three of the building blocks, with the remaining building block of size $a \pm m$. So, naturally, one is curious as to which operation to choose when forming a covering EBS. Looking at the EBS for $C_2 \times C_2$, it is obvious that three building blocks have size 2 while the fourth has size 4. This sums up to 10 elements, which is the complement to the more standard (16,6,2) difference set. It is known, however, that the complement of a difference set is too a difference set, so as explained earlier, we can find the complement of the complement to obtain the size 6 difference set that corresponds to subtraction as the fourth parameter of our (2,2,4,+) covering EBS (see [10], page 322). We provide an algorithm in the appendix that is an addition to our EBS algorithm and allows for the conversion of an HDS complement into an HDS.

This does not imply that using addition always gives the complement of a Hadamard difference set. For instance, we observe that both covering extended building sets for $C_3 \times C_3$ contain three building blocks of size 3 and another of size 6. This yields an HDS of size 15 using addition as the fourth parameter of our (3,3,4,+) covering EBS. An example of using subtraction is our (8,4,4,-) covering EBS for $C_4 \times C_4$. Hence, in general, the operation chosen in $a \pm m$ to create the hth building block is itself not imperative to successfully finding an HDS in a group; the choice is only a starting point!

3.4 Quasi-difference Sets

The structure of the extended building sets constructed for $C_4 \times C_4$ and $C_8 \times C_8$ have motivated our exploration into a new type of set in these groups. In fact, these sets in the groups $C_m \times C_m$ relate directly to the $(4m^2, 2m^2 \pm m, m^2 \pm m)$ Hadamard difference sets in groups of order $4m^2$, as we shall reveal soon.

Definition 3.4.1. Let G be a group of order v_G, and suppose we want a (v_G, k_G, λ_G) difference set on G. On a group H of order v_H, where for some $z \in \mathbb{N}$, $\frac{v_G}{v_H} = z$, a set $S \subseteq H$ is a $(v_H, k_H, \lambda_G, \delta)$ quasi-difference set relative to a group G, provided H is contained in G, the set SS^{-1} contains $\delta = (v - k)((v - k) - 1)$ non-identity elements exactly $\lambda_G + 1$ times, and all other non-identity elements exactly λ_G times.

Corollary 3.4.2. $\mid SS^{-1} \mid = (k_H - \lambda_G) \mid 1_H \mid + \lambda \mid H \mid + \delta$

Proof.

$$\begin{aligned} \mid SS^{-1} \mid &= \delta(\lambda_G + 1) + (v_H - \delta)\lambda_G + (k_H - \lambda_G) && (3) \\ &= \delta\lambda_G + \delta + \lambda_G v_H - \delta\lambda_G + (k_H - \lambda_G) && (4) \\ &= \delta + \lambda_G \mid H \mid + (k_H - \lambda_G) && (5) \\ \implies \mid SS^{-1} \mid &= (k_H - \lambda) \mid 1_H \mid + \lambda \mid H \mid + \delta && (6) \end{aligned}$$

□

Corollary 3.4.3. If $\lambda_G = k_H - (v_H - k_H)$, then: $(k_H(k_H - 1) - \delta) = (v_H - 1)\lambda_G$

Proof.

$$\begin{aligned} k_H(k_H - 1) - \delta &= k_H(k_H - 1) - (v_H - k)((v - 1) - k_H) && (7) \\ &= k_H(k_H - 1) - (v_H - k_H)(v_H - 1) - k_H(v_H - k_H) && (8) \\ &= k_H(k_H - 1) - (v_H - k_H)(v_H - 1) - k_H(v_H - k_H) && (9) \\ &= k_H^2 - k_H - (v_H - k_H)(v_H - 1) + k_H v - k_H^2 && (10) \\ &= (v_H - 1)k_H - (v_H - k_H)(v_H - 1) && (11) \\ &= (v_H - 1)(k_H - (v_H - hk_H)) && (12) \\ &= (v_H - 1)\lambda_G && (13) \end{aligned}$$

□

We focus our attention on groups of order $4m^2$ and smaller groups H of order m^2, in hopes to further understand the Hadamard Difference Sets.

Theorem 3.4.4. *For a group G of order $4m^2$ and H of order m^2 a set $S \subseteq G$ is a $(m^2, m^2 - \frac{m}{2}, m^2 - m, \frac{m^2}{4} - \frac{m}{2})$ quasi-difference set on H.*

Proof. We check the conditions given by the two corollaries above.

1. $k(k-1) = (v-1)\lambda$, eliminating the elements counted $\lambda + 1$ times, which break the difference set condition.

$$k(k-1) - \left(\frac{m^2}{4} - \frac{m}{2}\right) = (m^2 - \frac{m}{2})(m^2 - \frac{m}{2} - 1) - \left(\frac{m^2}{4} - \frac{m}{2}\right) \tag{14}$$

$$= \left(m^4 - m^3 - \frac{3m^2}{4} + \frac{m}{2}\right) - \left(\frac{m^2}{4} - \frac{m}{2}\right) \tag{15}$$

$$= m^4 - m^3 - m^2 + m \tag{16}$$

$$= \left(m^2 - 1\right)\left(m^2 - m\right) \tag{17}$$

$$= (v-1)\,\lambda \tag{18}$$

$$\implies k(k-1) - \delta = (v-1)\lambda \tag{19}$$

2. The size of the differences of S, $\mid SS^{-1} \mid = (k - \lambda) \mid 1_G \mid + \lambda \mid G \mid + \left(\frac{m^2}{4} - \frac{m}{2}\right)$.

$$\mid SS^{-1} \mid = \left(\frac{3m^2}{4} + \frac{m}{2} - 1\right)\lambda + \left(\frac{m^2}{4} - \frac{m}{2}\right)(\lambda + 1) + \left(m^2 - \frac{m}{2}\right) \tag{20}$$

$$= \frac{3m^2}{4}\lambda + \frac{m}{2}\lambda - \lambda + \frac{m^2}{4}\lambda - \frac{m}{2}\lambda + \frac{m^2}{4} - \frac{m}{2} + m^2 - \frac{m}{2} \tag{21}$$

$$= \left(\frac{3m^2}{4} + \frac{m^2}{4}\right)\lambda + \left(\frac{m}{2} - \frac{m}{2} - 1\right)\lambda + \left(m^2 + \frac{m^2}{4} - m\right) \tag{22}$$

$$= m^2\lambda + \left(-m^2 + m\right) + m^2 + \frac{m^2}{4} - m \tag{23}$$

$$= \lambda\,|G| + \frac{m^2}{4} + \left(\frac{m}{2} - \frac{m}{2}\right) \tag{24}$$

$$= \frac{m}{2} + \lambda\,|G| + \frac{m^2}{4} - \frac{m}{2} \tag{25}$$

$$= (k - \lambda)\,|1_G| + \lambda\,|G| + \left(\frac{m^2}{4} - \frac{m}{2}\right) \tag{26}$$

□

In defining these sets, we borrow the notation for difference sets, setting $v = m^2$, $k = m^2 - \frac{m}{2}$, and $\lambda = m^2 - m$, without meeting the requirements for being a difference set; however, the motivation for this definition lies in its connection to Hadamard Difference Sets. We can lift these sets into groups of order $4m^2$ that contain a group isomorphic to G, and the elements in these sets will, in fact, be a difference set on that group.

Example 3.4.5. Consider $G = C_4 \times C_4$.
The covering EBS is $\phi = \{\{\langle x^2y\rangle\}, \{\langle x\rangle \cup y\langle xy^2\rangle\}, \{\langle xy\rangle \cup y\langle xy^3\rangle\}, \{\langle x^2, y^2\rangle \cup x\langle y\rangle\}\}$. The differences $\phi * \phi^{-1}$on $C_4 \times C_4$ gives the following count matrix, where the nth entry in the matrix refers to the nth element of $C_4 \times C_4$ in GAP:

$$[14\ 12\ 12\ 12\ 12\ 12\ 12\ 13\ 12\ 12\ 12\ 12\ 12\ 13\ 12\ 12]$$

Conjecture 3.4.6. For every $m = 2n$, $n \in \mathbb{Z}$ with $n \geq 2$, there exists an $(m^2, m^2 - \frac{m}{2}, m^2 - m)$-quasi-difference set on $C_m \times C_m$.

Proof. Conjectured outline of process:

Consider $G \cong \langle x, y | x^m = y^m = 1 \rangle$. Take $\frac{m}{4}$ non-identity elements or non-nilpotent elements of G and their inverses; label the set of these elements L. Let $S = G - L$. Since G is symmetric and L is defined as stated above, we know that $S = S^{-1}$. Looking at the group ring structure of difference sets, we have the definition $DD^{-1} = (k - \lambda)1_G + \lambda G$. We can adapt this to our set S to express the differences as $SS^{-1} = S^2$. These differences can be visualized with the Cayley table for G, where the elements of L can be viewed as "holes" in the table.

Group theory allows us to conclude that for any $g_1, g_2 \in G$, there exists an element $h \in G$ such that $h = g_1 g_2$. Hence for any nonidentity $s_1 \in S$, $s_1 S$ is a bijective shift of elements in S by s_1 on G, from which we obtain the elements of L. There are $k = m^2 - \frac{m}{2}$ elements to shift by, where k elements are hit $k - \frac{m}{2}$ times and the remaining elements, naturally in L, are hit $k - \frac{m}{2} + 1$ times. Thus we have $m^2 - \frac{m}{2}$ stages of "shifting" and in each stage $\frac{m}{2}$ elements fall into the "holes." □

For m prime, the quasi-difference sets behave differently, as we have (m, m, 4, +) extended building sets for them. The sets on $C_m \times C_m$ are such that the union is m^2, and the differences thus include each element of $C_m \times C_m$ m times.

Conjecture 3.4.7. For every $m \in \mathbb{N}$, there exists an $(m^2, m^2 - \frac{m}{2}, m^2 - m)$ quasi-difference set on $C_m \times C_m$ lifts to groups G' of order $4m^2$ to serve as elements of the Hadamard Difference Set on the group, provided G' contains a subgroup isomorphic to $C_m \times C_m$.

Although we did not have the time to prove this, evidence strongly suggests that this statement is true, based off of data collected on groups of order 64 and 256 while searching for Hadamard Difference Sets. However, some groups that contain an isomorphic $C_m \times C_m$ do *not* emit a Hadamard Difference Set with this construction, independent of $C_m \times C_m$ being normal.
We believe that the problem of missing some of the groups requires a stronger condition, particularly regarding the order of the generating elements of the subgroup isomorphic to $C_m \times C_m$ and the larger group's generating elements.

3.5 Future Work

Although the preceding conjectures were beyond our scope to prove within the time of the program, we firmly believe that these are true given the evidence we've gathered on $C_4 \times C_4$ and $C_8 \times C_8$ using the Extended Building Sets that Dr. Jim Davis formed. As such, future work would firmly and rigorously prove the purported statements, namely Conjectures 3.4.6 and 3.4.7.

The motivation for quasi-difference sets is in the power of applying this to much higher order groups and in the fact that these sets can be formed on abelian groups. One can lift and inject the sets into non-abelian groups, whether or not the group that the set was found on is normal. In a word, we can use the nice properties of smaller order, abelian, well-understood groups to discover a concrete difference set on a much higher order group, namely, on groups of order $z \,|\, v_H \,|$, where $z = \frac{v_G}{v_H}$. We find quasi-difference sets on smaller groups and lift up to more complicated, less well-understood groups to get difference sets.

4 Finding All (64,28,12)-Difference Sets

4.1 Difference Sets

Definition 4.1.1. A (v, k, λ)-difference set is a set δ of elements of a group G such that $|G| = v$, $|\delta| = k$, and all nonidentity elements $g \in G$ can be represented as $g = d_1 \cdot d_2^{-1}$ for exactly λ ordered pairs (d_1, d_2) of elements of δ.

Two (v, k, λ)-difference sets δ_1 and δ_2 of a group G are considered equivalent iff there exist an element $g_0 \in G$ and an automorphism ψ of G such that $\delta_2 = \{g_0 \cdot \psi(g) \mid g \in G\}$.

A Hadamard difference set is a difference set with the parameters $(4m^2, 2m^2 - m, m^2 - m)$ for some positive integer m.

All inequivalent (16,6,2)-difference sets and (36,15,6)-difference sets are listed in [1] and [5] respectively. This section will go about listing all inequivalent (64,28,12)-difference sets.

In this section we will be working in the group ring $\mathbb{Z}[G]$. By a common abuse of notation, we will denote the element $\sum_{g \in G} g$ by G. Throughout this section, let δ denote a difference set, and $D = \sum_{d \in \delta} d \in \mathbb{Z}[G]$. We will call both δ and D difference sets, but δ will refer to a set, while D will refer to an element of $\mathbb{Z}[G]$.

Definition 4.1.2. Let $S \in \mathbb{Z}[G]$ and $g \in G$. Throughout this section, let S^g denote the coefficient of g in S. That is,

$$S = \sum_{g \in G} S^g \cdot g$$

Inside the group ring, the difference set must satisfy the following equation:

$$DD^{(-1)} = (k - \lambda) \cdot 1_G + \lambda \cdot G,$$

where 1_G refers to the identity element of G, and

$$D^{(-1)} = \sum_{g \in G} S^g \cdot g^{-1}$$

.

We will assume standard results from the theory of representations of finite groups. Most important is the following theorem:

Theorem 4.1.3. If $S_1, S_2 \in \mathbb{Z}[G]$ are such that $\chi(S_1) = \chi(S_2)$ for all irreducible representations χ of G, then $S_1 = S_2$.

Let χ_0 denote the trivial representation from here on, defined by $\chi_0(g) = 1$ for all $g \in G$. Notice that $\chi_0(D) = \sum_{d \in \delta} 1 = |\delta| = \chi_0\left(D^{(-1)}\right)$. The difference set equation, under χ_0, then rearranges to

$$\begin{array}{rcl} |\delta|^2 & = & k - \lambda + \lambda|G| \\ \Longrightarrow k(k-1) & = & \lambda(v-1), \end{array}$$

an auxilliary equation that v, k, λ must always satisfy, and which is automatically satisfied by $v = 4m^2, k = 2m^2 - m$, and $\lambda = m^2 - m$. Throughout this section assume v, k, λ satisfy this condition.

Lemma 4.1.4. For $S \in \mathbb{Z}[G]$ and χ a representation, $\chi\left(S^{(-1)}\right) = \overline{\chi}(S)^{\mathrm{t}}$.

Proof. Immediate from algebraic manipulation. □

We will also need the following result from the theory of representations:

Lemma 4.1.5. For any subgroup $H \subseteq G$ and representation χ of G, we have

$$\chi(H) := \sum_{h\in H} \chi(h) = \begin{cases} |H| & \text{if } \chi(h) = 1 \text{ for all } h \in H \\ 0 & \text{otherwise} \end{cases},$$

from which it is immediate that $\chi(G) = 0$ for all nontrivial irreducible representations χ of G.

Combining theorem 4.1.3 with the above two lemmas yields the defining theoerem for difference sets:

Theorem 4.1.6. Let $S \in \mathbb{Z}[G]$. Then S is a difference set iff

1. $S^g \in \{0, 1\}$ for all $g \in G$,
2. $\chi_0(S) = \sum_{g\in G} S^g = k$, and
3. $\chi(S)\overline{\chi(S)}^{\mathrm{t}} = (k - \lambda)\chi(1_G)$ for all irreducible $\chi \neq \chi_0$.

4.2 Difference Sums

Definition 4.2.1. For $S \in \mathbb{Z}[G]$, we say that S is a (v, k, λ)-*difference sum of magnitude* r if $|G| = v/r$, $S^g \in \{0, 1, ..., r\}$ for all $g \in G$, and $SS^{(-1)} = (k - \lambda) \cdot 1_G + r\lambda \cdot G$.

As in the previous subsection, we have

Theorem 4.2.2. $S \in \mathbb{Z}[G]$ is a difference sum of magnitude r if and only if

1. $S^g \in \{0, 1, ..., r\}$ for all $g \in G$,
2. $\chi_0(S) = \sum_{g\in G} S^g = k$, and
3. $\chi(S)\overline{\chi(S)}^{\mathrm{t}} = (k - \lambda)\chi(1_G)$ for all irreducible $\chi \neq \chi_0$.

A difference set is just a difference sum of magnitude 1. The following shows how a difference sum on a group will induce difference sums on its quotient groups.

Definition 4.2.3. Suppose $S \in \mathbb{Z}[G]$ and K is a normal subgroup of G. Then S induces an element $S_K \in \mathbb{Z}[G/K]$, defined by

$$S_K^{gK} = \sum_{h\in gK} S^h = \sum_{k\in K} S^{gk}$$

for all $gK \in G/K$.

The theory of representations tells us that the irreducible representations of a quotient group are induced by those of the base group:

Lemma 4.2.4. For a normal subgroup K of G, the irreducible representations of G/K are induced by the irreducible representations of G which contain K in the kernel.

From this lemma, we can show the following:

Theorem 4.2.5. Suppose $S \in \mathbb{Z}[G]$ is a difference sum of magnitude r, and K is a normal subgroup of G. Then $S_K \in \mathbb{Z}[G/K]$ is a difference sum of magnitude $r|K|$.

Proof. Since $0 \leq S^g \leq r$ for all $g \in G$ we have

$$0 \leq S^{gK} = \sum_{k \in K} S^{gk} \leq r|K|$$

for all $gK \in G/K$. Furthermore, consider an irreducible representation $\chi \neq \chi_0$ of G/K. From the above lemma, we can consider χ to be a nontrivial irreducible representation of G with $\chi(k) = \chi(1_G)$ for all $k \in K$. Thus

$$\begin{aligned}
\chi(S_K) &= \sum_{gK \in G/K} S^{gK} \chi(gK) \\
&= \sum_{gK \in G/K} \chi(gK) \sum_{k \in K} S^{gk} \\
&= \sum_{gK \in G/K} \sum_{k \in K} S^{gk} \chi(gk) \\
&= \chi(S),
\end{aligned}$$

and so

$$\chi_0(S_K) = \chi_0(S) = k$$

and

$$\chi(S_K)\overline{\chi(S_K)}^t = \chi(S)\overline{\chi(S)}^t = (k - \lambda)\chi(1_G)$$

for all nontrivial irreducible representations χ. Thus S_K is a difference sum of magnitude $r|K|$. □

The following observation will become helpful in the next chapter.

Theorem 4.2.6. If $S \in \mathbb{Z}[G]$ is a (v, k, λ)-difference sum of magnitude r, then

$$\sum_{g \in G} (S^g)^2 = k - \lambda + r\lambda$$

Proof. The coefficient of 1_G in $(k - \lambda) \cdot 1_G + \lambda \cdot G$ is $k - \lambda + r\lambda$, and the coefficient of 1_G in $SS^{(-1)}$ is $\sum_{g \in G} (S^g)^2$. □

If G is a group of size 64, then G is a 2-group, so there exists $K \lhd G$ with $|K| = 2$. If, furthermore, G has a difference set $D \in \mathbb{Z}[G]$, then $D_K \in \mathbb{Z}[G/K]$ is a difference sum of magnitude 2.

On the other hand, suppose we are given a difference sum $S \in \mathbb{Z}[G/K]$ of magnitude 2. Then there are finitely many $T \in \mathbb{Z}[G]$ such that $T_K = S$, and $T^g \in \{0, 1\}$ for all $g \in G$, although not all such T are difference sets. In fact, such a T is a difference set if and only if $\chi(T)\overline{\chi(T)}^t = 16\chi(1_G) + 12\chi(G)$ for all irreducible χ.

Thus if we know all difference sums of magnitude 2 in groups of size 32, we can use this information to find all difference sets in groups of size 64. Similarly we can use a list of all difference sums of magnitude 4 in groups of size 16 to find a list of all difference sums of magnitude 2 in groups of size 32.

Our starting point will be to find all difference sums of magnitude 4 in groups of size 16.

4.3 Difference Sums of Magnitude 4 in Groups of Size 16

Let S be a (64,28,12)-difference sum of magnitude 4 in a group G of size 16, and define $m_i = |\{g \in G \mid S^g = i\}|$ for $i = 0, 1, 2, 3, 4$.

Theorem 4.3.1. There are 9 possible values of $(m_0, m_1, m_2, m_3, m_4)$. They are listed in the table below, along with the number of group ring elements $T \in \mathbb{Z}[G]$ that have $m_i = |\{g \in G \mid T^g = i\}|$.

$(m_0, m_1, m_2, m_3, m_4)$	# group ring elements
$(3, 0, 12, 0, 1)$	$7,280$
$(0, 8, 6, 0, 2)$	$360,360$
$(2, 3, 9, 1, 1)$	$4,804,800$
$(1, 6, 6, 2, 1)$	$20,180,160$
$(3, 1, 9, 3, 0)$	$1,601,600$
$(0, 9, 3, 3, 1)$	$1,601,600$
$(2, 4, 6, 4, 0)$	$25,225,200$
$(1, 7, 3, 5, 0)$	$5,765,760$
$(0, 10, 0, 6, 0)$	$8,008$

Proof. We have the equations

$$\begin{aligned} m_0 + m_1 + m_2 + m_3 + m_4 &= & |G| & \quad = 16 \\ m_1 + 2m_2 + 3m_3 + 4m_4 &= & \textstyle\sum_{g\in G} S^g & \quad = 28 \\ m_1 + 4m_2 + 9m_3 + 16m_4 &= & \textstyle\sum_{g\in G} (S^g)^2 & \quad = 64 \end{aligned}$$

from which we can solve for m_0, m_1, m_2 in terms of m_3 and m_4:

$$\begin{aligned} m_0 &= -m_3 - 3m_4 + 6 \\ m_1 &= 3m_3 + 8m_4 - 8 \\ m_2 &= -3m_3 - 6m_4 + 18. \end{aligned}$$

The equation $m_0 \geq 0$ gives $m_3 + 3m_4 \leq 6$, which limits (m_3, m_4) to $(0, 0)$,$(0, 1)$, $(0, 2)$, $(1, 0)$, $(1, 1)$, $(2, 0)$, $(2, 1)$, $(3, 0)$, $(3, 1)$, $(4, 0)$, $(5, 0)$, or $(6, 0)$. The equaton $m_1 \geq 0$ gives $3m_3 + 8m_4 \geq 8$, which rules out $(m_3, m_4) = (0, 0)$, $(1, 0)$, or $(2, 0)$. This leaves us with the 9 choices shown in the table. The number of group ring elements for a given $(m_0, ..., m_4)$ is found by the combinatorial formula

$$\frac{16!}{m_0!m_1!m_2!m_3!m_4!}.$$

□

From this theorem, we see that, for any G with $|G| = 16$, there are at most 59,554,768 elements of $\mathbb{Z}[G]$ that could be (64,28,12)-difference sums of magnitude 4. For each of the 14 groups of order 16, we can run an exhaustive computer search on each of these 59,554,768 elements T to see whether $\chi(T)\overline{\chi(T)}^{\mathrm{t}} = 16\chi(1_G)$ for all nontrivial irreducible representations of G. T is a difference sum if and only if it has this property. The computer search yields the following number of difference sums in each of the 14 groups of order 16, as ordered by GAP's small group database.

cn (catalogue number)	# difsums in SmallGroup(16,cn)
1	304
2	14448
3	3440
4	10608
5	3440
6	5360
7	304
8	1200
9	27184
10	14448
11	3440
12	33136
13	5360
14	14448

The function AllMag4 takes a group of size 16 and produces all (64,28,12)-difference sums of magnitude 4 in that group, using this method.

4.4 Translational Equivalence

Definition 4.4.1. Two difference sums $S_1, S_2 \in \mathbb{Z}[G]$ are *equivalent* if there exist $g_0 \in G$ and $\phi \in Aut(G)$ such that $S_2 = g_0\phi(S_1)$.

Definition 4.4.2. Two difference sums $S_1, S_2 \in \mathbb{Z}[G]$ are *translationally equivalent*, or *t-equivalent*, if there exists $g_0 \in G$ such that $S_2 = g_0 S_1$.

Notice that our definition of equivalent difference sums corresponds to our definition of equivalent difference sets. That is, two difference sets are equivalent when viewed as difference sets if and only if they are equivalent when viewed as difference sums of magnitude 1.

T-equivalence is stronger than equivalence: t-equivalent difference sums are always equivalent but not vice-versa. As such, a list with at least one representative from each t-equivalence class of difference sums will contain at least one representative from each equivalence class of difference sums.

Lemma 4.4.3. For any $S \in \mathbb{Z}[G]$, we have $(g_0S)^g = S^{g_0^{-1}g}$.

Proof. The coefficient of $g_0^{-1}g$ becomes that of g when translating by g_0 on the left. □

Lemma 4.4.4. For any $K \lhd G$ and $S \in \mathbb{Z}[G]$, we have $(g_0S)_K = (g_0K)S_K$.

Proof.

$$\begin{aligned}
(g_0S)_K^{gK} &= \sum_{k\in K} (g_0S)^{gk} \\
&= \sum_{k\in K} S^{g_0^{-1}gk} \\
&= S_K^{g_0^{-1}gK} \\
&= S_K^{(g_0K)^{-1}(gK)} \\
&= ((g_0K)S_K)^{gK}.
\end{aligned}$$

Thus $(g_0S)_K = (g_0K)S_K$. $\square$

Theorem 4.4.5. Let G be a group and K a normal subgroup. Let $\mathcal{T}$ be a set of (v,k,λ)-difference sums of magnitude $r|K|$ in G/K such that at least one difference sum from each t-equivalence class is contained in T. Define $\mathcal{S} = \{S \in \mathbb{Z}[G] \mid S$ is a (v,k,λ)-difference sum of magnitude r and $S_K \in \mathcal{T}\}$. Then $\mathcal{S}$ contains an element from each t-equivalence class.

Proof. Let $S \in \mathbb{Z}[G]$ be a (v,k,λ)-difference sum of magnitude r. Then $S_K \in \mathbb{Z}[G/K]$ is a (v,k,λ)-difference sum of magnitude $r|K|$, and so S_K is t-equivalent to some $T \in \mathcal{T}$. Thus there exists $gK \in G/K$ such that $T = (gK)S_K$. But then $(gS)_K = (gK)S_K = T \in \mathcal{T}$, so $gS \in \mathcal{S}$. Thus S is t-equivalent to some element of $\mathcal{S}$. $\square$

This theorem tells us that if we take a single representative from each t-equivalence class of difference sums of G/K, then, when we pull back to difference sums of G, we will still get at least one representative from each t-equivalence class of difference sums, and hence from each equivalence class of difference sums. The following theorem tells us that the size of each t-equivalence of difference sums in G is exactly $|G|$.

Theorem 4.4.6. If $S \in \mathbb{Z}[G]$ is a (v,k,λ)-difference sum of magnitude r, then $S = gS$ if and only if $g = 1_G$.

Proof. Suppose $S = gS$. Then

$$\begin{aligned}(k-\lambda)1_G + r\lambda G &= SS^{(-1)}\\ &= gSS^{(-1)}\\ &= g[(k-\lambda)1_G + r\lambda G]\\ &= (k-\lambda)g + r\lambda G.\end{aligned}$$

Thus $g = 1_G$. $\square$

Thus the number of t-inequivalent difference sums of magnitude 4 inside a group of size 16 is 1/16 of the total number of difference sums.

The function TPurge (with the parameter “K” set to equal “Group(Identity(G))”) takes a list of difference sums of a group and returns a list of representatives of the t-equivalence classes of that list.

4.5 Difference Sums of Magnitude 2 in Groups of Size 32

Theorem 4.5.1. Let $S \in \mathbb{Z}[G]$ be a (v,k,λ)-difference sum of magnitude 2. Let $n_i = |\{g \in G \mid S^g = i\}|$ for $i = 0,1,2$. Then

$$(n_0,n_1,n_2) = (\frac{v+\lambda}{2} - k, k-\lambda, \frac{\lambda}{2})$$

Proof. We know that $n_0 + n_1 + n_2 = |G| = v/2$, and that $0 \cdot n_0 + 1 \cdot n_1 + 2 \cdot n_2 = \sum_{g \in G} S^g = k$. Furthermore, from theorem 4.2.6, we have $0^2 \cdot n_0 + 1^2 \cdot n_1 + 2^2 \cdot n_2 = k - \lambda + 2\lambda = k + \lambda$. Solving these three linear equations simultaneously yields the unique solution for (n_0,n_1,n_2) given. $\square$

Corollary 4.5.2. Let G be a group of size 32, and $S \in \mathbb{Z}[G]$ a (64,28,12)-difference sum of magnitude 2. Let $n_i = |\{g \in G \mid S^g = i\}|$ for $i = 0,1,2$. Then $(n_0,n_1,n_2) = (10,16,6)$.

Let G be a group of size 32 and $K = \{1, x\}$ a normal subgroup of size 2. We will now describe the process of finding all (64,28,12)-difference sums $S \in \mathbb{Z}[G]$ of magnitude 2 which induce a given (64,28,12)-difference sum $T \in \mathbb{Z}[G/K]$ of magnitude 4.

Suppose $S_K = T$, with S, T as above, and fix $g \in G$. Then

$$T^{gK} = S_K^{gK} = \sum_{k \in K} S^{gk} = S^g + S^{gx}.$$

We know that $S^g, S^{gx} \in \{0, 1, 2\}$ and $T^{gK} \in \{0, 1, 2, 3, 4\}$ since S, T have magnitudes 2,4 respectively. With these constraints, the value of T^{gK} gives us the following information about S^g and S^{gx}:

$$\begin{aligned}
T^{gK} = 0 \quad &\Longrightarrow \quad S^g = S^{gx} = 0 \\
T^{gK} = 1 \quad &\Longrightarrow \quad \{S^g, S^{gx}\} = \{0, 1\} \\
T^{gK} = 2 \quad &\Longrightarrow \quad \{S^g, S^{gx}\} = \{0, 2\} \text{ or } S^g = S^{gx} = 1 \\
T^{gK} = 3 \quad &\Longrightarrow \quad \{S^g, S^{gx}\} = \{1, 2\} \\
T^{gK} = 4 \quad &\Longrightarrow \quad S^g = S^{gx} = 2
\end{aligned}$$

Theorem 4.5.3. Let $C = \{gK \mid T^{gK} = 2\}$. Define $A := \{gK \in C \mid \{S^g, S^{gx}\} = \{0, 2\}\}$ and $B := \{gK \in C \mid S^g = S^{gx} = 1\}$. Then $C = A \sqcup B$ is a partition of C, and $|A| = \frac{1}{3}|C|$.

Proof. The fact that C partitions into A and B follows from the above discussion. Define $m_i = |\{gK \in G/K \mid T^{gK} = i\}|$ for $i = 0, 1, 2, 3, 4$ and $n_i = |\{g \in G \mid S^g = i\}|$ for $i = 0, 1, 2$. Then, from the proof of theorem 4.3.1, we have

$$|C| = m_2 = -3m_3 - 6m_4 + 18.$$

On the other hand, from the above discussion and corollary 4.5.2, we have

$$6 = n_2 = |A| + m_3 + 2m_4.$$

Thus $|A| = -m_3 - 2m_4 + 6 = \frac{1}{3}|C|$. □

Keep the notation $m_i = |\{gK \in G/K \mid T^{gK} = i\}|$ for $i = 0, 1, 2, 3, 4$. From the above theorem and the discussion leading up to it, we see that we have a choice of two options for (S^g, S^{gx}) when $T^{gK} = 1$ or 3, and $\frac{1}{3}$ of the time when $T^{gK} = 2$. With

$$\binom{m_2}{\frac{1}{3}m_2}$$

choices for which of the m_2 elements of C belong to A, as per theorem 4.5.3, the number of elements $S \in \mathbb{Z}[G]$ which *could* be (64,28,12)-difference sums of magnitude 2 such that $S_K = T$ is given by

$$\binom{m_2}{\frac{1}{3}m_2} \times 2^{m_1 + \frac{1}{3}m_2 + m_3}.$$

This value, for the 9 possible distributions $(m_0, ..., m_4)$ produced by theorem 4.3.1 is given below

$(m_0, m_1, m_2, m_3, m_4)$	potential # of difsums with mag 2
$(3, 0, 12, 0, 1)$	$7,920$
$(0, 8, 6, 0, 2)$	$15,360$
$(2, 3, 9, 1, 1)$	$10,752$
$(1, 6, 6, 2, 1)$	$15,360$
$(3, 1, 9, 3, 0)$	$10,752$
$(0, 9, 3, 3, 1)$	$24,576$
$(2, 4, 6, 4, 0)$	$15,360$
$(1, 7, 3, 5, 0)$	$24,576$
$(0, 10, 0, 6, 0)$	$65,536$

As can be seen, any given (64,28,12)-difference sum of magnitude 4 in a quotient group G/K can yield at most 65,536 (64,28,12)-difference sums of magnitude 2 in G.

Without the restriction imposed by theorem 4.5.3 the number of elements of $\mathbb{Z}[G]$ that would need to be checked would be $3^{m_2} \times 2^{m_1+m_3}$, which, for $(m_0, ..., m_4) = (3, 0, 12, 0, 1)$, would give 531,441 possiblities instead of only 7,920. Thus, in practice, this extra restriction can drastically cut down the size of the search space.

Theorem 4.5.4. Let G be a group and K a normal subgroup. If $S \in \mathbb{Z}[G]$ is such that $0 \leq S^g \leq r$ for all $g \in G$ and $S_K \in \mathbb{Z}[G/K]$ is a (v, k, λ)-difference sum of magnitude $r|K|$, then S is a (v, k, λ)-difference sum of magnitude r if and only if $\chi(S)\overline{\chi(S)}^{t} = (k - \lambda)\chi(1_G)$ for each irreducible representation χ of G such that $K \not\subseteq ker(\chi)$.

Proof. From representation theory, we know that the irreducible representations of G/K are induced by those of G which contain K in the kernel. The theorem then follows immediately from theorem theorem 4.2.2. □

Going back to the setup with $K \lhd G$, $|G| = 32$, $|K| = 2$, we see that if $S \in \mathbb{Z}[G]$ is produced in the manner descibed in this chapter, so that $0 \leq S^g \leq 2$ for each $g \in G$ and so that S_K is a (64,28,12)-difference sum of magnitude 4, then one can determine whether or not S is a (64,28,12)-difference sum of magnitude 2 simply by checking the value of $\chi(S)$ for each irreducible representation χ of G not containing K in its kernel.

The function Mag4toMag2 takes as input a group G of size 32, a normal subgroup K of size 2, and a (64,28,12)-difference sum $T \in \mathbb{Z}[G/K]$ of magnitude 4, and returns all (64,28,12)-difference sums $S \in \mathbb{Z}[G]$ of magnitude 2 such that $S_K = T$. The function AllMag2 iterates this process over all (64,28,12)-difference sums $T \in \mathbb{Z}[G/K]$ of magnitude 4, up to t-equivalence.

4.6 Purging the List of Difference Sums of Magnitude 2 in a Group of Size 32

At this point in the algorithm, we can get a list of all (64,28,12)-difference sums of magnitude 2, up to t-equivalence, in a given group G of size 32. However, each t-equivalence class may have up to 32 duplicates. However, because the difference sums of magnitude 2 were produced from a list of difference sums of magnitude 4 in a quotient group, and this original list did not contain repeats within t-equivalence classes, we actually have more information about our newer list.

Theorem 4.6.1. Let G be a group and K a normal subgroup. Suppose $\mathcal{T}$ is a list of difference sums of magnitude $r|K|$ in $\mathbb{Z}[G/K]$ such that no two elements of $\mathcal{T}$ are t-equivalent. Let $\mathcal{S}$ be the set of difference sums $S \in \mathbb{Z}[G]$ of magnitude r such that $S_K \in \mathcal{T}$. Then, for any $S \in \mathcal{S}$, we have $\{gS \mid g \in G\} \cap \mathcal{S} = \{kS \mid k \in K\}$.

Proof. $\subseteq$: Fix $S \in \mathcal{S}$ and $g \in G$ such that $gS \in \mathcal{S}$. Thus $(gS)_K \in \mathcal{T}$. Then, by lemma 4.4.4, $(gS)_K = (gK)S_K$. Since $S_K \in \mathcal{T}$ and $(gK)S_K$ is t-equivalent to S_K, it must be that $(gK)S_K = S_K$. Thus, by theorem 4.4.6, gK is the identity of G/K, so $g \in K$.

$\supseteq$: Fix $S \in \mathcal{S}$ and $k \in K$. Then clearly $kS \in \{gS \mid g \in G\}$. Furthermore, $(kS)_K = (kK)S_K = S_K \in \mathcal{T}$, so $kS \in \mathcal{S}$. □

Thus, in our setup, when $|G| = 32$ and $|K| = 2$, and we have a difference sum in G, we only have to check for one difference sum in the list that is t-equivalent, rather than 31.

The number of (64,28,12)-difference sums of magnitude 2, up to t-equivalence, in each group of size 32 is shown below. As seen in theorem 4.4.6, the total number of (64,28,12)-difference sums of magnitude 2 is found by multiplying each number in the table by 32.

Remark 4.6.2. *SmallGroup(32,1) is C_{32}, the cyclic group of order 32, and SmallGroup(32,18) is D_{32}, the dihedral group of order 32. Empirically, we have shown that C_{32} and D_{32} do not contain any (64,28,12)-difference sums of magnitude 2. Consequently, any group of size 64 which has a holomorphic image of (i.e. a quotient group isomorphic to) either of these two groups cannot have a difference set. Thus, we have computationally proven Turyn's bound and the dihedral trick (see [2]) for groups of size 64.*

The function TPurge takes a group G, a normal subgroup K, and a list $\mathcal{S}$ of difference sums in G, and return a list of representatives from the t-equivalence classes of the list. It is assumed that the set $\{S_K \mid S \in \mathcal{S}\}$ contains two t-equivalent elements in $\mathbb{Z}[G/K]$, and thus the reduction made in theorem 4.6.1 can be applied.

cn (catalogue number)	# difsums in SmallGroup(32,cn) up to t-equivalence
1	0
2	12180
3	11556
4	19620
5	5620
6	3780
7	4116
8	28596
9	1604
10	9008
11	6020
12	5604
13	5020
14	4236
15	9492
16	708
17	2132
18	0
19	1072
20	5472
21	112020
22	25620
23	58000
24	60148
25	39044
26	94180
27	11572
28	12652
29	43876
30	22264
31	23292
32	65396
33	33528
34	8640
35	91776
36	25620
37	38068
38	31956
39	708
40	7012
41	124164
42	9332
43	4132
44	32836
45	219604
46	25620
47	609428
48	62132
49	10132
50	137492
51	219604

4.7 Difference Sets in Groups of Size 64

Theorem 4.7.1. Let G be a group and K a normal subgroup. If $\phi \in \mathrm{Aut}(G)$ is such that $\phi(K) = K$, then ϕ induces an automorphism ϕ_K on G/K defined by

$$\phi_K(gK) = \phi(g)K.$$

Furthermore, for any $S \in \mathbb{Z}[G]$, we have

$$\phi(S)_K = \phi_K(S_K).$$

Proof. Fix G, K, and ϕ as in the theorem. Define $\phi_K : G/K \to G/K$ by $\phi_K(gK) = \phi(g)K$. If $g_1K = g_2K$, then $g_1^{-1}g_2 \in K$ and hence $\phi(g_1^{-1}g_2) \in K$, so $\phi_K(g_1K) = \phi(g_1)K = \phi(g_1)(\phi(g_1^{-1}g_2)K) = \phi(g_2)K = \phi_K(g_2K)$. Hence ϕ_K is well defined.

For any $g_1, g_2 \in G$, we have $\phi_K(g_1K)\phi_K(g_2K) = (\phi(g_1)K)(\phi(g_2)K) = \phi(g_1)\phi(g_2)K = \phi(g_1g_2)K = \phi_K((g_1K)(g_2K))$, so ϕ_K is a homomorphism. If $\phi_K(gK) = K$, then $\phi(g)K = K \implies \phi(g) \in K$. Observing that ϕ, when restricted to K, is an automorphism of K, we have that $\phi(g) \in K \implies g \in K$. Thus $\phi_K(gK) = K$ if and only if $gK = K$, and so ϕ_K is injective. For surjectivity, observe that $\phi_K(\phi^{-1}(g)K) = gK$. Thus ϕ_K is an automorphism of G/K.

For the last part of the theorem, fix $S \in \mathbb{Z}[G]$. By the same argument as in lemma 4.4.3, we see that $\phi(S)^g = S^{\phi^{-1}(g)}$. Thus

$$\begin{aligned}
\phi(S)_K^{gK} &= \sum_{k\in K} \phi(S)^{gk} \\
&= \sum_{k\in K} S^{\phi^{-1}(g)\phi^{-1}(k)} \\
&= \sum_{k\in K} S^{\phi^{-1}(g)k} \\
&= S_K^{\phi^{-1}(g)K} \\
&= S_K^{\phi_K^{-1}(gK)} \\
&= \phi_K(S_K)
\end{aligned}$$

□

The following analogue to theorem 4.4.5 follows immediately, with precisely the same proof.

Theorem 4.7.2. Let G be a group and K a normal subgroup. Let $\mathcal{T}$ be a set of (v, k, λ)-difference sums of magnitude $r|K|$ in G/K such that for any (v, k, λ)-difference sum $T \in \mathbb{Z}[G/K]$ of magnitude $r|K|$, there exists some $gK \in G/K$ and $\phi \in \mathrm{Aut}(G)$ with $\phi(K) = K$, such that $\phi_K((gK)S_K) \in \mathcal{T}$. Define $\mathcal{S} = \{S \in \mathbb{Z}[G] \mid S \text{ is a } (v, k, \lambda)\text{-difference sum of magnitude } r \text{ and } S_K \in \mathcal{T}\}$. Then $\mathcal{S}$ contains an element from each equivalence class.

This theorem allows one to cut down on the number of difference sums that one has to look at in G/K order to find difference sums in G. It is not possible to apply this method without knowing what G is, i.e. the set $\{\phi_K \mid \phi \in \mathrm{Aut}(G)\}$ may change if G/K is realized as a different quotient group G'/K'. Thus this reduction is applied only in the final step, in which we find difference sets in groups of size 64 from difference sums of magnitude 2 in groups of size 32.

By corollary 4.5.2, each difference sum $T \in \mathbb{Z}[G/K]$ of magnitude 2 has 10 0's, 16 1's, and 6 2's. Thus there are $2^{16} = 65{,}536$ elements $S \in \mathbb{Z}[G]$ with $S_K = T$. As in theorem 4.5.4, we have only to check that $\chi(S)\overline{\chi(S)}^{\mathrm{t}} = 16\chi(1_G)$ for each irreducible representation χ of G which does not contain K in the kernel. Since K is not in the kernel and $|K| = 2$, say $K = \{1_G, x\}$, lemma 4.1.5 tells us that $\chi(x) = -\chi(1_G)$. For each $gK \in G/K$ with $T^{gK} = 2$, we will have $S^g = S^g k = 1$, which will contribute $\chi(g) + \chi(gk) = 0$ to the sum $\chi(S)$ when K is not in the kernel of χ. Thus, for such a χ, we have

$$\chi(S) = \sum_{\{g|S^g = T^{gK} = 1\}} \chi(g),$$

which is the sum over 16 values rather than the naive sum

$$\chi(S) = \sum_{\{g|S^g = 1\}} \chi(g),$$

which is a sum over 28 values.

The function FindDifsets takes a group G of size 64 and a normal subgroup K of size 2, and a difference sum $T \in \mathbb{Z}[G/K]$ of magnitude 2, and finds all difference sets $S \in \mathbb{Z}[G]$ such that $S_K = T$, by cycling through all 65,536 possibilities and then using the method described above to test each one and see if it is a difference set.

The function AllMag1 takes a group G of size 64 and produces a list of difference sets of G, with at least one per equivalence class. The algorithm starts by picking a normal subgroup K of size 2, taking a list of all difference sums of magnitude 2 in G/K, up to t-equivalence, and then further purging this list using theorem 4.7.2. FindDifsets is then applied to the elements of the resulting list of difference sets.

Unfortunately, in practice, AllMag1 will give an error indictating that the allocated memory has been exceeded when G=SmallGroup(64,cn) for cn=260, 262, or 267. This is because these three groups have the largest automorphism groups out of all groups of size 64, and minipulating these automorphism groups requires too much memory.

Finally, the function FinalPurge takes a list of difference sets in a group G of size 64 and removes duplicates within equivalence classes. No “shortcuts” are used in this final step, although conceivably one can be created using information from previous steps in the algorithm.

4.8 Selected Final Results

The following is a table of the number of difference sets in certain groups of size 64, up to equivalence.

cn (catalogue number)	# difsets in SmallGroup(64,cn) up to equivalence
1	0
2	31
3	71
4	468
5	708

cn (catalogue number)	# difsets in SmallGroup(64,cn) up to equivalence
6	584
7	1320
8	616
9	1652
10	300
11	522
12	67
13	688
14	319
15	104
16	104
17	1012
18	652
19	176
20	1944
21	968
22	600
23	882
24	1026
25	1180
26	32
27	24
28	148
29	284
30	338
31	448
32	642
33	962
34	228
35	684
36	306
37	706
38	0
39	440
40	168
41	204
42	60
43	340
44	52
45	136

cn (catalogue number)	# difsets in SmallGroup(64,cn) up to equivalence
46	152
47	0
48	56
49	52
50	0
51	112
52	0
53	0
54	0
58	1936
63	1321
85	721
86	1122
87	944
88	760
89	1162
90	964
91	948
92	422
109	1348
110	656
111	616
112	1186
113	814
114	1044
115	1624
116	1673
117	1007
118	320
119	1639
120	2672
121	1808
129	1314
130	878
131	738
139	751
140	136
141	554
142	998
186	0

5 Latin Rectangles

5.1 Introduction

If R is an $m \times n$ array whose entries are elements of $\{1, 2, ..., k\}$ such that no entry occurs more than once in any row or column, then R is a *latin rectangle* based on k .

$$\begin{array}{cccc}
1 & 2 & 3 & 4 \\
2 & 3 & 4 & 1 \\
3 & 4 & 1 & 2
\end{array}$$

A *row-latin rectangle* is a latin rectangle in which no entry occurs more than once in any row, but columns can have repeating entries.

$$\begin{array}{cccc}
1 & 2 & 4 & 3 \\
2 & 3 & 4 & 1 \\
1 & 2 & 4 & 3 \\
4 & 3 & 2 & 1 \\
4 & 1 & 3 & 2
\end{array}$$

A *partial transversal* of length r is a set of r distinct entries of R, no two from the same row or column.

$$\begin{array}{cccc}
1 & 2 & \underline{4} & 3 \\
2 & 3 & 4 & \underline{1} \\
1 & \underline{2} & 4 & 3 \\
4 & 3 & 2 & 1 \\
2 & 4 & 1 & 3
\end{array}$$

A *transversal* is a partial transversal of length n.

$$\begin{array}{cccc}
\underline{1} & 2 & 4 & 3 \\
2 & 3 & \underline{4} & 1 \\
1 & \underline{2} & 4 & 3 \\
4 & 3 & 2 & 1 \\
2 & 4 & 1 & \underline{3}
\end{array}$$

Suppose group $A = \{a_1, ..., a_m\}$ acts on $X = \{x_1, ..., x_n\}$, $a \in A$ maps $x \in X$ to $x^a \in X$.

Definition 5.1.1. *A complete A-mapping θ is an injection $\theta : X \to A$ such that $\{x^{\theta(x)} : x \in X\} = X$.*

Let R be a row-latin rectangle with entries $R_{a,x} = x_c^{a_r}$.

Theorem 5.1.2. *$\theta : X \to A$ is a complete A-mapping iff $T = \{R_{\theta(x),x} | x \in X\}$ is a transversal in R.* [4]

Proof. Assume θ is a complete A-mapping. Since θ is 1-1, $\theta(x_i) \neq \theta(x_j)$ for $i \neq j$, and $x_i \neq x_j$, $i \neq j$, then no two elements of T would have come from the same row or column.Since by definition

5.1.1 $\{x^{\theta(x)} : x \in X\} = X$, T contains all of X in which each element is distinct. Therefore R has a transversal.

Theorem 5.1.3. *Let p be a prime, A a finite p-group, and X a A-set with $|X| \leq |A|$. Then X has a complete A-mapping. [4]*

5.2 Application to groups of order 2^n

Let G be a group of order $2^{2(s+1)}$, and $E \lhd G$ such that $E = C_2^{s+1}$. Define a quotient goup $Q = G/E$, and a set $H = \{H_i \lhd E, |H_i| = 2^s\}$ such that $Q = \{q_1, ..., q_{2^{s+1}}\}, q_i = g_i E$ and $H = \{H_1, ..., H_{2^{s+1}-1}\}$. Let R be a $|Q| \times |H|$ array whose rows and columns are indexed by the elements of Q and H, respectively, such that $R_{q,H} = H_c^{q_r}$

Theorem 5.2.1. *If there exist elements $g_1, ..., g_r$ in distinct cosets of E in G, and $H_i \mapsto g_i H_i g_i^{-1}$ is a permutation of elements of H, then $D = g_1 H_1 + ... + g_r H_r$ is a difference set of G with parameters [3]*

$$v = 2^{2(s+1)}$$

$$k = 2^s(2^{s+1} - 1)$$

$$\lambda = 2^s(2^s - 1)$$

The quotient group Q acts on H by $H_j^{q_i} = g_i H_j g_i^{-1}$.

By Theorem 5.1.2, R has a transversal $\{R_1, ..., R_{2^{s+1}-1}\}$, $R_i = R_{q^{(i)},H_i}$, where $q^{(i)}, ..., q^{2^{s+1}-1}$ are distinct elements of Q. Then by Theorem 5.2.1 $\bigcup_i g^{(i)} H_i$ is a difference set.

Example. Let $G =< x, y, z | x^4 = y^2 = z^2 = 1, [x, z], [y, z], xyx^{-1} = yz >$ and $E \lhd G$, $E = \{1, y, z, yz\}$. Define $Q = G/E = \{1, x, x^2, x^3\}$, and $H = \{\{1, y\}, \{1, z\}, \{1, yz\}\}$.
We can now construct a row-latin rectangle R as follows

	$\{1, y\}$	$\{1, yz\}$	$\{1, z\}$
1	$\underline{\{1, y\}}$	$\{1, yz\}$	$\{1, z\}$
x	$\{1, yz\}$	$\{1, y\}$	$\underline{\{1, z\}}$
x^2	$\{1, y\}$	$\underline{\{1, yz\}}$	$\{1, z\}$
x^3	$\{1, yz\}$	$\{1, y\}$	$\{1, z\}$

A transversal $T = \{\{1, y\}, \{1, yz\}, \{1, z\}\}$ and difference set, by Theorem 5.2.1, is $D = 1\{1, y\} + x^2\{1, yz\} + x\{1, z\} = \{1, x, y, x^2, xz, x^2yz\}$.

5.3 Algorithm

The algorithm will first check to make sure there exists an elementary abelian soubgroup of G of order $\sqrt{n}$. Once confirmed, the algorithm will begin a series of recursive comparisons.

We begin by fixing one of the columns and a symbol in it, staring with $R_{1,1}$ in the first row and column. Next, we compare each of the symbols in the second column to $R_{1,1}$, omitting the first one since entries in a transversal must all belong to different rows, until we find a distinct symbol $R_{r,2} \neq R_{1,1}$ and fix it as well as the row it is in. Proceeding in this fashion, the algorithm will go through the rest of the columns recursively comparing each of the symbols to the set of the ones we have already found $\{R : R_i \neq R_j, i \neq j\}$ and fixing them if they are not in the set. If after fixing a symbol in the last column we have a set of n distinct entries, then we have a transversal. Otherwise, we will begin the process again, this time by fixing a symbol $R_{2,1}$ in the first column and second row. If we failed to find a transversal by the time both the last symbol in the first column and some symbol in the last column are in the set, we will begin again by fixing a symbol $R_{1,2}$ in the second column and carrying out the algorithm as before, starting with the symbol in the first row and column.

Such procedure randges between $n-1$ comparisons per group before a transversal is found in the best case scenario and $n(2n-1)\binom{2n-2}{2}$ comparisons in the worst.

The results of running the algorithm on groups of size 64 and 256 are in the table below.

Group size	# of groups	Time	Difsets found
64	267	< 1 min	181
256	56092	¡12 hrs	42353

6 Appendix

The following packages are included as sources of the found difference sets by our group. In general, each file is a list of difference sets found on different group sizes; for each group size, we use code to iterate over all groups in GAP for that size and output the resulting difference set (if found). Each output file includes a list showing the GAP ID of a group and the difference set found on that group.

- DifsetMap.txt is a list of difference sets in all groups of order 64 that can have a difference set, and it includes the method used to find the difference set. This file thus includes the solution to the first problem we were tasked with, finding difference sets for each group of order 64.
- 64TransversalResults.txt is the list of difference sets found using the Latin Rectangles method on groups of order 64.
- 256TransversalResults.7z contains the list of difference sets found using the Latin Rectangles method on groups of order 256.
- EBS_Order16_difsets.txt is the list of difference sets found using the Extended Building Set method on groups of order 16.
- EBS_Order36_difsets.txt is the list of difference sets found using the Extended Building Set method on groups of order 36.
- EBS_Order64_difsets.txt is the list of difference sets found using the Extended Building Set method on groups of order 64.
- EBS_Order256_difsets.txt.zip contains a file with the list of difference sets found using the Extended Building Set method on groups of order 256.
- EBS_HDSData is an Excel spreadsheet of the results and characteristics of the results of applying the EBS construction to groups of order 16, 36, 64, and 256.
- HDS_Code.txt is a file containing all of the code written, referenced, and used. The Difference Sums package is contained in that file, but due to the interplay between so many different, large functions and their variables, the given files have also been uploaded separately in case of error.
- DifferenceSumsCode.zip contains the aforementioned Difference Sum package.
- SpreadConstructionGroupsOfSize64.txt contains code that generates a difference set in each group of order 64 that contain a normal elementary Abelian group of order 8 using the spread construction (see section 2.4).

7 Acknowledgments

We would like to thank the National Science Foundation for funding this research and San Diego State University for hosting the program. Thank you to Dr. Ken Smith and Dr. Vadim Ponmarenko for mentoring us, and thanks to all people involved in difference sets. Thank you Dr. Jim Davis for being helpful and responsive. Thanks to our professors at our home institutions that encourage us in Mathematics, and thanks to our fellow REU peers for always motivating us.

References

[1] Chirashree Bhattacharya and Ken W. Smith. Factoring $(16, 6, 2)$ Hadamard difference sets. *Electron. J. Combin.*, 15(1):Research Paper 112, 16, 2008.

[2] James A. Davis and Jonathan Jedwab. A survey of Hadamard difference sets. In *Groups, difference sets, and the Monster (Columbus, OH, 1993)*, volume 4 of *Ohio State Univ. Math. Res. Inst. Publ.*, pages 145–156. de Gruyter, Berlin, 1996.

[3] J. F. Dillon. Variations on a scheme of McFarland for noncyclic difference sets. *J. Combin. Theory Ser. A*, 40(1):9–21, 1985.

[4] Arthur A. Drisko. Transversals in row-Latin rectangles. *J. Combin. Theory Ser. A*, 84(2):181–195, 1998.

[5] Robert E. Kibler. A summary of noncyclic difference sets, $k < 20$. *J. Combinatorial Theory Ser. A*, 25(1):62–67, 1978.

[6] E. A. O'Brien. The p-group generation algorithm. *J. Symbolic Comput.*, 9(5-6):677–698, 1990. Computational group theory, Part 1.

[7] Adegoke S. A. Osifodunrin. On the existence of $(196, 91, 42)$ Hadamard difference sets. *Kragujevac J. Math.*, 34:113–130, 2010.

[8] Ken W. Smith. Non-abelian Hadamard difference sets. *J. Combin. Theory Ser. A*, 70(1):144–156, 1995.

[9] Ken W. Smith and Jordan Webster. Spread construction for (36, 15, 6) hadamard difference sets.

[10] Richard J. Turyn. Character sums and difference sets. *Pacific J. Math.*, 15:319–346, 1965.