4-1-2013

Difference sets in non-abelian groups of order 256

Taylor Applebaum

Difference Sets in Non-Abelian Groups of Order 256

Taylor Applebaum

Honors Thesis*

Department of Mathematics & Computer Science

University of Richmond

*Under the direction of Dr. James A. Davis

The signatures below, by the thesis advisor, the departmental reader, and the honors coordinator for mathematics, certify that this thesis, prepared by Taylor Applebaum, has been approved, as to style and content.

(Dr. James Davis, thesis advisor)

(Dr. Della Dumbaugh, departmental reader)

(Dr. Lester Caudill, honors coordinator)

Abstract

This paper considers the problem of determining which of the 56092 groups of order 256 contain $(256, 120, 56, 64)$ difference sets. John Dillon at the National Security Agency communicated 724 groups which were still open as of August 2012. In this paper, we present a construction method for groups containing a normal subgroup isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2$. This construction method was able to produce difference sets in 643 of the 649 unsolved groups with the correct normal subgroup. These constructions elimated approximately 90% of the open cases, leaving 81 remaining unsolved groups.

Contents

1 Introduction **1**

2 Building Sets **6**

3 Non-Abelian Groups **18**

4 GAP **22**

5 Results **34**

6 Addendum **37**

1 Introduction

A (v, k, λ, n) *difference set in G* is defined as a k-element subset of a finite multiplicative group G of order v such that the "differences" $\{d_1 d_2^{-1} | d_1, d_2 \in D, d_1 \neq d_2\}$ form a multiset that contains each nonidentity element of G precisely λ times. The fourth parameter n is the value $k - \lambda$. For example, consider $\mathbb{Z}_7 =< x | x^7 = 1 >$. Then the set $D = \{x, x^2, x^4\}$ is a $(7, 3, 1, 2)$ difference set since $x = x^2x^{-1}, x^2 = x^4(x^2)^{-1}, x^3 = x^4x^{-1}, x^4 = x(x^4)^{-1}, x^5 = x^2(x^4)^{-1}, x^6 = x(x^2)^{-1}$. In a similar manner, it can be verified that $\{y, x, xy, xy^2, x^2y, x^3y^3\}$ is a $(16, 6, 2, 4)$ difference set in the group $\mathbb{Z}_4^2 =< x, y | x^2 = y^2 = 1 >$.

Applications of difference sets can be found in both theoretical and applied contexts. For example, there is a natural connection between the study of difference sets and design theory since a (v, k, λ, n) difference set is equal to a $(v, k, \lambda, n)-$design with a regular automorphism group G. Difference sets are also extremely useful in the field of cryptography, the mathematical study of methods of secure commucation of information in the presence of adversaries.

Much work on difference sets is being done at the National Security Agency (NSA) under Dr. John Dillon. Specifically, Dr. Dillon has been working to exhaustively determine which of the 56092 nonisomorphic groups of order 256 contain $(256, 120, 56, 64)-$ difference sets. [3] This project has been underway since the 1990s. Its completion has the capability to serve as a model for analogous projects in other large 2-groups.

At the beginning of this work, we contacted Dr. Dillon and recieved the status of the project: Of the 56092 nonisomorphic groups of order 256, the existence or nonexistence of a $(256, 120, 56, 64)$ difference set was unknown in 724 of those groups. Thus, in the broadest sense, the goal of this work is to contribute to Dr. Dillon's project by finding difference sets in some subset of those 724 groups.

We will use character theory as a tool for determining whether a subset of a group is a difference set. We define a *character* of an abelian group G to be a homomorphism $\chi : G \to \mathbb{C}$, where the image of

G is a cyclic multiplicative group of complex roots of unity of order n generated by $\omega = e^{\frac{2\pi i}{n}}$. The set of all characters of a group G, denoted G^* forms a group under pointwise multiplication that is isomorphic to G. (We are exclusively concerned with finite groups, particularly those of order 256.) The identity of G^* is the *principal character* on G, denoted χ_0, which is the character that maps every element of G to $1_{\mathbb{C}}$. Accordingly, the remaining elements of G^* are *nonprincipal* characters on G. That is, they do not map all elements of G to 1.

Example 1. *Let $G = \mathbb{Z}_4^2 =< (1,0),(0,1) >$ and define a character χ by $\chi(1,0) = i, \chi(0,1) = -1$. The character χ is a nonprincipal character on G.*

The following concept of character sums is central to our method of determining whether a set of G is a difference set: Let S be a subset of G (it is possible that S is a multiset). The *character sum* of S for a particular character χ, denoted $\chi(S)$ is the sum of the image of each element of S under χ. That is, $\chi(S) = \sum_{s \in S} \chi(s)$. The following properties of character sums will be useful in our work:

Lemma 2. *If χ_0 is the principal character on a group G, then $\chi_0(G) = |G|$.*

Proof: The following computation proves the lemma: $\chi_0(G) = \sum_{g \in G} \chi_0(g) = \sum_{g \in G} 1 = |G|$. □

Lemma 3. *If A is a multiset of elements of a group G such that $A = cG$ (A contains each element of G precisely c times), then $\chi(A) = 0$ for every character χ nonprincipal on G.*

Proof: Let χ be a character nonprincipal on a group $G = \{g_1, g_2, \ldots, g_v\}$. We will first show that $\chi(G) = 0$. To see this let $g_k \in G$ satisfy $\chi(g_k) \neq 1$. By cancellation, if $i \neq j$ then $g_k g_i \neq g_k g_j$. Thus, the set $\{g_k g_1, g_k g_2, \ldots, g_k g_v\}$ contains v distinct elements in G. It follows that $G = \{g_1, g_2, ...g_v\} = \{g_k g_1, g_k g_2, \ldots, g_k g_v\}$. Now, by the structure preserving properties of homomorphisms we get $\chi(g_k)\chi(G) = \chi(g_k)\{\chi(g_1) + \ldots + \chi(g_v)\} = \chi(g_k)\chi(g_1) + \ldots + \chi(g_k)\chi(g_1) = \chi(g_k g_1) + \ldots + \chi(g_k g_v) = \chi(G)$. Thus $\chi(g_k)\chi(G) = \chi(G)$. Since we assumed that $\chi(g_k) \neq 1$, it follows that $\chi(G) = 0$.

Now, $\chi(A) = \chi(cG) = \underbrace{\chi(G) + \chi(G) + \ldots + \chi(G)}_{c \text{ times}} = 0 + 0 + \ldots + 0 = 0.$ □

The following example illustrates the first two lemmas.

Example 4. *Let $G = \mathbb{Z}_8$, the cyclic group of order 8 under addition. Written additively, $G =< 1 >$. Let χ_0 denote the principal character on G. By definition, $\chi_0(g) = 1$ for all $g \in G$. Thus, we get $\chi(G) = 1 + ... + 1 = 8 = |G|$, as claimed. Now for a more interesting example: Define χ_1 by $\chi_1(1) = i$. (Since $\chi_1(1) \neq 1$, χ_1 is nonprincipal on G.) This forces $\chi_1(2) = -1, \chi_1(3) = -i, \chi_1(4) = 1, \chi_1(5) = i, \chi_1(6) = -1, \chi_1(7) = -i$. ($\chi_1(0) = 1$ since the identity of G must be mapped to the identity of C.) Now $\chi_1(G) = \chi_1(0)+\chi_1(1)+\chi_1(2)+\chi_1(3)+\chi_1(4)+\chi_1(5)+\chi_1(6)+\chi_1(7) = 1+i+-1+-i+1+i+-1+-i = 0$. Also note that if we take the character sum over $5\mathbb{Z}_8$, the multiset that contains each element of $\mathbb{Z}_8$ 5 times, we simply get $\chi_1(5\mathbb{Z}_8) = \chi_1(\mathbb{Z}_8) + \chi_1(\mathbb{Z}_8) + \chi_1(\mathbb{Z}_8) + \chi_1(\mathbb{Z}_8) + \chi_1(\mathbb{Z}_8) = 5\chi_1(\mathbb{Z}_8) = 5(1 + i + -1 + -i + 1 + i + -1 + -i) = 5(0) = 0$.*

I claim that this property of Lemma 2 is bidirectional. However, before we can show this, we must first consider the following:

Lemma 5. *Let $g \in G$. The sum over all the characters $\chi(g)$ is $|G|$ if $g = e$ and 0 otherwise. That is,* $\sum_{\chi \in G^*} \chi(g) = \begin{cases} |G| & \text{for} \quad g = e \\ 0 & \text{for} \quad g \neq e \end{cases}$.

Proof: In the case that $g = e$, $\chi(g) = 1$ for all possible characters χ on G by the properties of homomorphisms. Thus, each element of G^* contributes 1 to the sum $\sum_{\chi \in G^*} \chi(G)$. It follows that $\sum_{\chi \in G^*} \chi(G) = |G^*|$. Since $G \approx G^*$, $\sum_{\chi \in G^*} \chi(G) = |G|$. Now, let's consider the case in which $g \neq e$. There exists a $\chi_k \in G^* = \{\chi_1, \chi_2, \ldots, \chi_v\}$ such that $\chi_k(g) \neq 1$. By cancellation, if $i \neq j$ then $\chi_k\chi_i \neq \chi_k\chi_j$. Thus, the set $\{\chi_k\chi_1, \chi_k\chi_2, \ldots, \chi_k\chi_v\}$ contains v distinct elements in G^*. It follows that $G^* = \{\chi_1, \chi_2, \ldots, \chi_v\} = \{\chi_k\chi_1, \chi_k\chi_2, \ldots, \chi_k\chi_v\}$. We get that $\sum_{\chi \in G^*} \chi(g) = \chi_1(g)+\chi_2(g)+\ldots+\chi_v(g) = \chi_k(g)\chi_1(g)+\chi_k(g)\chi_2(g)+\ldots+\chi_k(g)\chi_v(g) = \chi_k(g)[\chi_1(g)+\chi_2(g)+\ldots+\chi_v(g)] = \chi_k(g)\sum_{\chi \in G^*} \chi(g)$. Since $\sum_{\chi \in G^*} \chi(g) = \chi_k(g)\sum_{\chi \in G^*} \chi(g)$ and $\chi_k(g) \neq 1$, it follows that $\sum_{\chi \in G^*} \chi(g) = 0$. □

Now we are prepared to prove the converse of Lemma 3:

Lemma 6. *If for every character χ nonprincipal on a group G, $\chi(A) = 0$ then $A = cG$ for some constant c.*

Proof: Suppose that A is a multiset of elements from a group G such that $\chi(A) = 0$ for all non-principal χ in G^*. If $G = g_1, g_2, ...g_v$, then let c_i denote the number of times the element g_i appears in A. For example, if $c_2 = 5$ then there are 5 copies of g_2 in A. We wish to show that $c_i = c$ for $i = 1, ..., v$ and some constant c. That is, each element of G appears the same number of times in A. Now, let $g_m \in G$. We want to determine the value of c_m. In the following calculations, $g_m^{-1}A = \{g_m^{-1}a | a \in A\}$. Now, $|A| = |g_m^{-1}A| = \chi_0(g_m^{-1}A) = \sum_{\chi \in G^*} \chi(g_m^{-1}A)$ (the assumption $\chi(A) = 0$ for every nonprincipal character χ implies that $\chi(g_m^{-1}A) = \chi(g_m^{-1})\chi(A) = 0$ for every nonprincipal character χ). Now $\sum_{\chi \in G^*} \chi(g_m^{-1}A) = \sum_{\chi \in G^*} \sum_{i=1,...,v} c_i \chi(g_m^{-1}g_i) = \sum_{i=1,...,v} c_i \sum_{\chi \in G^*} \chi(g_m^{-1}g_i)$. By Lemma 5, $\sum_{\chi \in G^*} \chi(g_m^{-1}g_i)$ is nonzero only when $g_m^{-1}g_i = e$, or equivalently when $g_i = g_m$. Thus, $\sum_{i=1,...,v} c_i \sum_{\chi \in G^*} \chi(g_m^{-1}g_i) = c_m \sum_{\chi \in G^*} \chi(e) = c_m|G|$. We are left with $|A| = c_m|G|$, or equivalently $c_m = \frac{|A|}{|G|}$. Thus, each element of G appears $c = \frac{|A|}{|G|}$ times in A. □

The property that for a χ nonprincipal on G, $\chi(cG) = 0$ (Lemma 3) will be extremely useful to us. We wish to determine an analogous property for when we have a χ nonprincipal on a group G but principal on a subgroup U of G. We will achieve this with the following theorem:

Theorem 7. *If χ is a character nonprincipal on a group G but principal on a subgroup U of G, there exists a character ψ induced by χ that is nonprincipal on G/U.*

Proof: Suppose χ is a character nonprincipal on a group G but principal on a subgroup U of G. Now define a mapping $\psi : G/U \to C$ by $\psi(gU) = \chi(g)$. To see that ψ is a homomorphism, let $g_1U, g_2U \in G/U$ and observe $\psi(g_1Ug_2U) = \psi(g_1g_2U) = \chi(g_1g_2) = \chi(g_1)\chi(g_2) = \psi(g_1U)\psi(g_2U)$. Also, ψ is well-defined: If $g_1U = g_2U$, then $g_1 = g_2u$ for some $u \in U$. (Since $g_1U = g_2U$, $g_1g_2^{-1}U = U$. Thus $g_1g_2^{-1}e = u$ for some $u \in U$, and we get $g_1 = g_2u$.) So $\psi(g_1U) = \chi(g_1) = \chi(g_2u) = \chi(g_2)\chi(u) = \chi(g_2)(1) = \psi(g_2U)$. Since χ is nonprincipal on G, there exists a $g \in G$ such that $\chi(g) \neq 1$. So if we take $\psi(gU) = \chi(g) \neq 1$. Thus, ψ is nonprincipal on G/U. □

We now have at our disposal the following property: If we have a G, U and χ with the theorem assumptions as properties, and we let ψ be our induced character, then $\psi(cG/U) = 0$ for some

constant c. The following is an example of this property:

Example 8. *As in Example 3, we will use $G = \mathbb{Z}_8$, the cyclic group of order 8 under addition and the character defined by $\chi(1) = i$, which forces $\chi(2) = -1, \chi(3) = -i, \chi(4) = 1, \chi(5) = i, \chi(6) = -1, \chi(7) = -i$. χ is nonprincipal on G but is principal on $U =< 4 >$. Thus, we know there is an induced nonprincipal character ψ on G/U defined by $\psi(gU) = \chi(g)$. To see that it is nonprincipal on G/U, notice $\psi(2U) = \chi(2) = -1 \neq 1$. Futhermore, $\psi(\mathbb{Z}_8/ < 4 >) = 0$.*

From now on, we will say that a character sum on some subset S has modulus m if $|\chi(S)| = m$. We will now employ this definition to connect character theory and difference sets:

Lemma 9. *A subset D of an abelian group G, such that $|D| = k$ and $|G| = v$ is a (v, k, λ, n) difference set in G if and only if the character sum over D has modulus $\sqrt{n}$, that is $|\chi(D)| = \sqrt{n}$, for all nonprincipal characters χ of G.*

Proof: First, suppose that D is a (v, k, λ, n) difference set in G and let $\chi \in G^*$. Now, let $D^{(-1)} = \{d^{-1} | d \in D\}$. Additionally, let $\overline{\chi(D)} = \{\overline{\chi(d)} | d \in D\}$, where $\overline{\chi(d)}$ is the complex conjugate of $\chi(d)$. I claim that $\chi(D^{(-1)}) = \overline{\chi(D)}$. It suffices to show that for $d \in D$, $\chi(d^{-1}) = \overline{\chi(d)}$. By the properties of homomorphisms, $\chi(d^{-1}) = (\chi(d))^{-1}$. Now, since $\chi(d)$ is simply a root of unity, $\chi(d) = a + bi$ for some $a, b \in \mathbb{R}$ such that $a^2 + b^2 = 1$. Now consider $\chi(d)\overline{\chi(d)} = (a + bi)(a - bi) = a^2 + b^2 = 1$. Thus, $(\chi(d))^{-1} = \overline{\chi(d)}$. It follows that $\chi(D^{(-1)}) = \overline{\chi(D)}$. Now, $|\chi(D)|^2 = \chi(D)\overline{\chi(D)} = \chi(D)\chi(D^{(-1)}) = \chi(D)\overline{\chi(D)} = \chi(DD^{(-1)}) = \chi(\lambda(G/e) + ke) = \chi(\lambda G + (k - \lambda)e) = \chi(\lambda G) + \chi((k - \lambda)e) = 0 + (k - \lambda)\chi(e) = k - \lambda = n$. It follows that $|\chi(D)| = \sqrt{n}$.

Now to see the converse, suppose that D is a subset of G such that $|\chi(D)| = \sqrt{n}$. This implies that $n = |\chi(D)|^2 = \chi(D)\overline{\chi(D)} = \chi(D)\chi(D^{(-1)}) = \chi(DD^{(-1)})$. Equivalently, $\chi(DD^{(-1)}) - n = \chi(DD^{(-1)}) - \chi(ne) = \chi(DD^{(-1)} - ne) = 0$. From Lemma 6, we know this implies $DD^{(-1)} - ne = cG$ or $DD^{(-1)} = cG + ne$ for some constant c. We can write $cG + ne = cG/\{e\} + (c + n)e$. The set $DD^{(-1)} = \{d_i d_j^{-1} | d_i, d_j \in D\}$ contains precisely $|D| = k$ copies of e. ($d_i d_j^{-1} = e$ only when $i = j$. This occurs for $i = 1, \ldots, |D|$.) This implies the following equality: $k = c + n$ or $c = k - n = \lambda$. Combining these results, we get $DD^{(-1)} = \lambda G/\{e\} + ke$. By definition, D is a (v, k, λ, n) difference

set in G. □

2 Building Sets

In order to apply character theory to our construction of difference sets, we must introduce the concept of building sets. The material in the section on building sets is based on previous work done by Davis and Jedwab. [1]

Before we are able to define building sets, we must first define a building block:

Definition. *A building block in a group G with modulus m to be a subset B of G such that all non-principal character sums over the subset have modulus either 0 or m. That is, for every χ nonprincipal on G, $|\chi(B)| = 0$ or m.*

Example 10. *Consider kU, a coset of a subgroup U of G with coset representative k. Note that a nonprincipal character χ of G is either nonprincipal on U or principal on U. We will first consider the nonprincipal characters of G that are also nonprincipal on $U = \{u_1, u_2, \ldots, u_n\}$. We now compute the character sum of kU, taking advantage of the structure preserving properties of homomorphisms: $\chi(kU) = \chi(ku_1)+\chi(ku_2)+\ldots+\chi(ku_n) = \chi(k)\chi(u_1)+\chi(k)\chi(u_2)+\ldots+\chi(k)\chi(u_n) = \chi(k)(\chi(u_1)+\chi(u_2)+\ldots+\chi(u_n)) = \chi(k)\chi(U) = \chi(k)(0) = 0$. ($\chi(U) = 0$ since χ is nonprincipal on U.) Thus, $|\chi(kU)| = |0| = 0$. Second, we consider a character χ that is nonprincipal on G but principal on U. Following the same calculations as before, we get $|\chi(kU)| = |\chi(k)\chi(U)| = |\chi(k)||\chi(U)| = |\chi(k)||U| = |U|$. (Since χ is principal on U, $|\chi(U)| = |U|$ and since $\chi(k)$ is just a root of unity $|\chi(k)| = 1$. Thus, all characters on kU have either modulus 0 or $|U|$, and by definition, kU is a building block of G with modulus $|U|$.*

We will now consider building blocks in a larger context:

Definition. *For positive integers a, t, a (a,m,t) building set (BS) on a group G relative to a subgroup U is a set of t building blocks $\{B_1, B_2, \ldots, B_t\}$ in G with modulus m (not necessarily an integer), where*

each block contains a elements such that for every nonprincipal character χ of G, the following two properties hold:

1. *if χ is nonprincipal on U, precisely one building block has nonzero character sum*
2. *if χ is principal on U, no building block has nonzero character sum*

Example 11. *To illustrate an example of a building set, we will introduce hyperplanes. A hyperplane U of an n-dimensional space V is an (n-1)-dimensional subspace of V. Consider $G \approx \mathbb{Z}_2^2$. This is a 2-dimensional vectorspace over $\mathbb{Z}_2$, and we can write $G = \{(a_1, a_2) | a_i \in \mathbb{Z}_2\}$. The three hyperplanes can be represented as follows: $H_0 =< (1,0) >, H_1 =< (0,1) >, H_2 =< (1,1) >$. I claim that the set $\{H_2, H_3\}$ forms a $(2,2,2)$ building set relative to $U = H_1$. First note that H_2, H_3 are both building blocks with modulus 2. (Since H_1, H_2 are just subgroups, if χ is principal on H_i, then $|\chi(H_i)| = 2$ and if χ is nonprincipal on H_i, then $|\chi(H_i)| = 0$). Now, let χ be a character nonprincipal on G. Since the maximum order of $g \in G$ is 2, χ must be a $2-to-1$ mapping onto $C = \{\pm 1\}$. Since the three hyperplanes are the only subgroups of G of order 2, one, say H_i, must be the kernel of χ. Thus, χ is principal on H_i and nonprincipal on the the remaining 2 hyperplanes. If $i \neq 1$, then χ is nonprincpal on $U = H_1$. Then the block H_i has a nonzero character sum ($\chi(H_i) = |H_i| = 2$). The second block has a character sum of 0 since χ is nonprincipal on it. If $i = 1$, then χ is principal on $U = H_1$ and nonprincipal on H_2, H_3. Thus, both blocks have character sum zero. By definition, $\{H_2, H_3\}$ is a $(2,2,2)$ building set relative to $U = H_1$.*

We now define a variation on a building set:

Definition. *For integers $a \geq 0, m \geq 1$ and $h \geq 1$, a (a, m, h, $\pm$) extended building set (EBS) on a group G with respect to a subgroup U is a collection of h building blocks in G with modulus m, of which $h-1$ contain a elements and one contains $a \pm m$ elements ($+$ or $-$ determined by the fourth parameter of the EBS), such that for every nonprincipal character χ of G, the following two properties hold:*

1. *if χ is principal on U, precisely one building block has nonzero character sum*

2. *if χ is nonprincipal on U, no building block has nonzero character sum*

Note that unlike in the definition of a building set, the value of m must be an integer, because the size of one of the blocks is $a \pm m$. Also, the two enumerated conditions in the building set and extended building set are somewhat reversed. To illustrate this, let $\{B_1, B_2, \ldots, B_n\}$ be a building set on some group G relative to a subgroup U, let $\{D_1, D_2, \ldots, D_m\}$ be an extended building set with respect to U, and let χ be a character nonprincipal on G. If χ is nonprincipal on U then precisely one B_i has a nonzero character sum and no D_j has a nonzero character sum. If χ is principal on U then precisely one D_i has a nonzero character sum and no B_j has a nonzero character sum. This reciprocal-like property will be useful to us.

In the case that for each nonprincipal character on G, precisely one building block has nonzero character sum, we will call the EBS *covering*.

Example 12. *We will again use hyperplanes to illustrate an example. Suppose that we have $G \approx \mathbb{Z}_2^3$. This can be thought of as a 3-dimensional vectorspace over $\mathbb{Z}_2$, and we can write $G = \{(a_1, a_2, a_3) | a_i \in \mathbb{Z}_2\}$. The 7 hyperplanes can be represented as follows:*

- $H_2 =< (0,1,0), (0,0,1) >$
- $H_3 =< (1,0,0), (0,0,1) >$
- $H_4 =< (1,0,0), (0,1,0) >$
- $H_5 =< (1,1,0), (0,0,1) >$
- $H_6 =< (1,0,1), (0,1,0) >$
- $H_7 =< (0,1,1), (1,0,0) >$
- $H_8 =< (1,1,0), (0,1,1) >$

Now consider a character χ nonprincipal on G. Since the maximum order of $g \in G$ is 2, the order of $\chi(g)$ is at most 2. This requires χ to be a $4-to-1$ mapping onto $C = \{\pm 1\}$, and thus χ has

a kernel of size 4*. Since the seven hyperplanes are the only subgroups of* G *of order 4, one, say* H_i*, must be the kernel of* χ*. Thus,* χ *is principal on* H_i *and nonprincipal on the the remaining 6 hyperplanes. Viewing these hyperplanes as subgroups (and hence groups), from a previous result, we know* $\chi(H_i) = 4, \chi(H_j) = 0, j \neq i$*. By definition,* $\{H_1, H_2, H_3, H_4, H_5, H_6, H_7, H_8\}$ *forms a* $(4, 4, 8, -)$ *covering EBS on G, where* H_1 *is the empty set with* $4 - 4 = 0$ *elements.*

We will finally establish the connection between building sets and difference sets in the following theorem:

Theorem 13. *A* $(a, m, 1, \pm)$ *covering EBS on a group G is equivalent to a* $(|G|, a \pm m, a \pm m - m^2, m^2)$ *difference set in* G*.*

Proof: Suppose we have a $(a, m, 1, \pm)$ covering EBS on a group G. Recall that this is a collection of 1 building block(s) in G with modulus m of which 0 contains a elements and one contain $a \pm m$ elements. Let D denote this block. Now, since the EBS is covering, we know that for each nonprincipal character on G, precisely one building block has a nonzero character sum. Since D is the only block and has modulus m, this implies that for all nonprincipal characters χ on G, $|\chi(D)| = m$. By Lemma 9, D is a $(|G|, a \pm m, a \pm m - m^2, m^2)$ difference set in G. □

We are now prepared to establish a broader result:

Theorem 14. *Given a* $(a, m, h, \pm)$ *covering EBS on a group G, there exists a* $(h|G|, ah \pm m, ah \pm m - m^2, m^2)$ *difference set in any abelian group* G' *containing* G *as a subgroup of index* h*.*

Proof: In order to apply Theorem 13, we must show that we can use a $(a, m, h, \pm)$ covering EBS on a group G to obtain a $(ah, m, 1, \pm)$ covering EBS on G' relative to G. To see this, let $\{B_1, B_2, \ldots, B_h\}$ be our $(a, m, h, \pm)$ covering EBS on a group G, where B_1 is the block containing $a \pm m$ elements. Let $g'_1, g'_2, \ldots, g'_h$ be the coset representatives of G in G'. Now define $D = \bigcup_{i=1,\ldots,h} g'_i B_i$. Let χ be a character nonprincipal on G'. There are two cases to consider: 1) χ is principal on G and 2) χ is nonprincipal on G. In the first case, we compute $\chi(D) = \sum_{i=1,\ldots,h} \chi(g'_i B_i) = \sum_{i=1,\ldots,h} \chi(g'_i)\chi(B_i) =$

$\sum_{i=1,\ldots,h} \chi(g_i')|B_i|$ (since $B_i \subset G$ and χ is principal on G) = $(a \pm m)\chi(g_1') + a\sum_{i=2,\ldots,h} \chi(g_i') = a\sum_{i=1,\ldots,h} \chi(g_i') \pm m\chi(g_1')$. Now, recall that since χ is nonprincipal on G' and principal on G, there is an induced nonprincipal character $\psi : G'/G \to \mathbb{C}$ defined by $\psi(g_i'G) = \chi(g_i')$. Thus, $\sum_{i=1,\ldots,h} \chi(g_i') = \sum_{i=1,\ldots,h} \psi(g_i'G) = \psi(G'/G) = 0$ (a nonprincipal character on a group has a character sum 0 over that group). Thus, $\chi(D) = a\sum_{i=1,\ldots,h} \chi(g_i') \pm m\chi(g_1') = \pm m\chi(g_1')$, and so $|\chi(D)| = |\pm m\chi(g_1')| = |\pm m||\chi(g_1')| = m$. In the case the χ is nonprincipal on G we consider $\chi(D)$. Since the blocks B_i form a covering EBS and χ is nonprincipal on G, precisely one block, say B_j has a nonzero character sum under χ and $|\chi(B_j)| = m$. Thus $\chi(D) = \chi(g_1'B_1) + \chi(g_2'B_2) + \ldots + \chi(g_h'B_h) = \chi(g_1')\chi(B_1) + \chi(g_2')\chi(B_2) + \ldots + \chi(g_h')\chi(B_h)$ collapses to $\chi(D) = \chi(g_j')\chi(B_j)$. Since $\chi(g_j')$ is simply a root of unity, $|\chi(g_j')| = 1$, and it follows that $|\chi(D)| = |\chi(B_j)| = m$. For every nonprincipal character χ of G', exactly one buiding block (in this case, the only building block) has nonzero character sum. It follows immediately that D is a $(h|G|, ah \pm m, ah \pm m - m^2, m^2)$ difference set in G'. □

Example 15. *To see an application of Theorem 13, we will produce a* $(256, 120, 56)$ *difference set in a abelian group* G *of order 256 containing a subgroup* $U \approx \mathbb{Z}_2^4$*. We will again turn to hyperplanes as a starting point. By now it should be apparent that the construction of building sets and extended building sets out of hyperplanes seems to be the default example. This is not a coincidence. Hyperplanes prove to be rather useful in these constructions because a hyperplane* H *of size* n *is a building block with modulus* n *with the rather handy property that it is also a subgroup (and thus a group). Thus, given a character* χ*,* $\chi(H) = 0$ *if* χ *is nonprincipal on* H *and* $\chi(H) = n$ *if* χ *is principal on* H*. Now, returning to the task at hand, we use the 15 hyperplanes of U , denoted* $H_2, ..., H_{16}$*, and the empty set denoted* H_1 *as the blocks in a* $(8, 8, 16, -)$ *covering EBS* $\{H_1, H_2, \ldots, H_{16}\}$*, where the 16th block is the empty set with* $16 - 16 = 0$ *elements. To see that the hyperplanes form a covering EBS, it suffices to note that the kernel of* χ *must be precisely one hyperplane. This argument is identical to that of Example 12. Let* $g_1, g_2, \ldots, g_{16}$ *represent the coset representataives from the elements in* G/U*. Now, by Theorem 14* $D = \bigcup_{i=1}^{16} g_i H_i$ *is a* $(256, 120, 56)$ *difference set in a* G*. This particular use of hyperplanes to construct difference sets was developed by McFarland and modified by Dillon. [4] [2]*

Our conclusion that a $(a, m, h, \pm)$ covering EBS on a group G can be used to obtain a $(ah, m, 1, \pm)$ covering EBS in a group G' containing G as a subgroup of index h can be generalized as follows:

Theorem 16. *A $(a, m, h, \pm)$ covering EBS on an abelian group G guarantees a $(as, m, h/s, \pm)$ covering EBS in an abelian group G' containing G as a subgroup of index s.*

Accordingly, the argument used to show this will be a generalization of the one just completed.

Proof: Let $\{B_1, B_2, \ldots, B_h\}$ be our $(a, m, h, \pm)$ covering EBS on G, where B_1 is the building block containing $a \pm m$ elements. Now suppose G' is an abelian group that contains G as a subgroup of index s, and let $g'_1, g'_2, \ldots, g'_s$ be the coset representatives of G in G'. Define the following subset of G': $D_j = \bigcup_{i=1}^{s} g'_i B_{i+(j-1)s}$ for $j = 1, 2, \ldots, h/s$. Let χ be a character nonprincipal on G'. Now χ is either principal or nonprincipal on G. We will first consider the case that χ is principal on G and compute $\chi(D_j) = \sum_{i=1}^{s} \chi(g'_i B_{i+(j-1)s}) = \sum_{i=1}^{s} \chi(g'_i)|B_{i+(j-1)s)}| = \chi(g'_1)|B_{1+(j-1)s)}| + \sum_{i=2}^{s} \chi(g'_i)|B_{i+(j-1)s)}| = \chi(g'_1)(|B_{1+(j-1)s}| - a) + a\sum_{i=1}^{s} \chi(g'_i)$. By Theorem 7, since χ is nonprincial on G' and principal on G, there is a nonprincipal character induced by χ on G/G'. This implies $\sum_{i=1}^{s} \chi(g'_i) = 0$. So we get $\chi(D_j) = \chi(g'_1)(|B_{1+(j-1)s)}| - a)$, and $|\chi(D_j)| = |(|B_{1+(j-1)s)}| - a)|$. Recall that $|B_1| = a - m$ and $|B_i| = m$ for $i \neq 1$. Thus, $|\chi(D_j)|$ is equal to m for $j = 1$ and 0 for $j > 1$. Now suppose that χ is nonprincipal on G. Then by the definition of a covering EBS, $\chi(B_k)$ is nonzero for precisely one value of k. The block D_i are define so that B_k appears in D_i for one particular i. Thus $\chi(D_i)$ is nonzero for this particular i, and zero for all others. By definition, $\{D_1, D_2, \ldots, D_{h/s}\}$ is a $(as, m, h/s, \pm)$ covering EBS in a group G' □

Example 17. *As an illustrative example, we will use the $(4, 4, 8, -)$ covering EBS in $G = \mathbb{Z}_2^3$ from Example 12 to construct a $(8, 4, 4, -)$ covering EBS in $G' = \mathbb{Z}_4 \times \mathbb{Z}_2^2$. Recall that $(4, 4, 8, -)$ covering EBS on G consisted of the empty block, B_1, and the 7 hyperplanes of G, $B_i, i = 2, \ldots, 8$. Notice that $G'/G = \{(0, 0, 0) + G, (1, 0, 0) + G\}$. Now we construct D_i according to the construction method given above: $D_1 = B_1 \bigcup (1, 0, 0) + B_5, D_2 = B_2 \bigcup (1, 0, 0) + B_6, D_3 = B_3 \bigcup (1, 0, 0) + B_7$, and $D_4 = B_4 \bigcup (1, 0, 0) + B_8$. (The presence of the coset representative $(0, 0, 0)$ is implicit when it is the coset representative attached to the blocks $B_i, i = 1, 2, 3, 4$). The previous argument tells us that $\{D_1, D_2, D_3, D_4\}$ is a*

$(8,4,4,-)$ *covering EBS in* $G' = \mathbb{Z}_4 \times \mathbb{Z}_2^2$.

Now, with the previous theorems and examples in mind, our goal will be to construct a $(16,8,8,-)$ covering EBS in the group $H = \mathbb{Z}_4^2 \times \mathbb{Z}_2$. By Theorem 14, this covering EBS will be used to construct a $(256,120,56)$ difference set in any abelian group G which contains H as a subgroup of index 8. We will proceed in a recursive manner, first showing that a $(16,8,4,-)$ EBS on H with respect to $U =< (0,2,0) >$ and a $(16,8,4)$ building set on H relative to U can be used to construct our $(16,8,8,-)$ covering EBS. Then we will take the steps necesary to obtain a $(16,8,4,-)$ EBS on H with respect to U and a $(16,8,4)$ building set on H relative to U.

Suppose we have a $(16,8,4,-)$ EBS $\{C_1, C_2, C_3, C_4\}$ on H with respect to U and a $(16,8,4)$ building set on H, denote it $\{C_5, C_6, C_7, C_8\}$, relative to U. Suppose we have a χ nonprincipal on G and principal on H. Then by the definition of an EBS, exactly one of $\{C_1, C_2, C_3, C_4\}$ has a nonzero character sum, and by the definition of a building set none of $\{C_5, C_6, C_7, C_8\}$ has a nonzero character sum. Now suppose χ is nonprincipal on H. By the definition of an EBS, none of $\{C_1, C_2, C_3, C_4\}$ has a nonzero character sum, and by the definition of a building set, precisely one of $\{C_5, C_6, C_7, C_8\}$ has a nonzero character sum. In either case, for a character χ nonprincipal on G, precisely one $\{C_1, C_2, \ldots, C_8\}$ has a nonzero character sum. By definition, this is a $(16,8,8,-)$ covering EBS on H.

We will first obtain our $(16,8,4,-)$ EBS on H with respect to U. I claim that the existence of $(8,4,4,-)$ covering EBS on H/U implies the existence of a $(16,8,4,-)$ EBS on H relative to U. To see this suppose we have an $(8,4,4,-)$ covering EBS on H/U where $U =< (0,2,0) >$. Let $\{B_1', B_2', B_3', B_4'\}$ be our $(8,4,4,-)$ covering EBS on H/U, where B_1' is our block containing $8-4=4$ elements. Define $B_i = \{h \in H | hU \in B_i'\}$. That is, B_i is the pre-image of B_i' in the mapping $\phi : H \to H/U$ defined by $\phi(h) = hU$ for $h \in H$. For example if $B_2' = \{h_1U, h_2U, \ldots, h_8U\}$, then $B_2 = h_1U \bigcup h_2U \bigcup \ldots \bigcup h_8U$. Thus, $|B_i| = |U||B_i'| = 2|B_i'|$. Concretely, $|B_1| = 8$ and $|B_2| = |B_3| = |B_4| = 16$. Now, let χ be a character nonprincipal on H, and consider $\chi(B_i) = \sum_{h_jU \in B_i'} \chi(h_jU)$. As always, we must consider whether χ is principal on U. If χ is nonprincipal on U, we know that $\chi(h_jU) = \chi(h_j)\chi(U) = \chi(h_j)(0) = 0$. Thus $|\chi(h_jU)| = 0$ for all j, and $\chi(B_i) = 0$ for all i.

If χ is principal on U, we will again employ our induced nonprincipal character on G/H, where $\psi : H/U \to \mathbb{C}$ is defined by $\psi(hU) = \chi(h)$. Now, by the definition of a covering EBS, $\psi(B'_k)$ is nonzero for precisely one B'_k and $|\psi(B'_k)| = 4$. We now compute $\chi(B_i) = \sum_{h_jU \in B'_i} \chi(h_jU) = \sum_{h_jU \in B'_i} \chi(h_j)|U| = |U| \sum_{h_jU \in B'_i} \psi(h_jU) = |U|\psi(B'_i) = 2\psi(B'_i)$. Thus, $\chi(B_i)$ is nonzero only when $i = k$ and $|\chi(B_k)| = |2||\psi(B'_k)| = 8$. By definition, $\{B_1, B_2, B_3, B_4\}$ is a $(16, 8, 4, -)$ EBS on H relative to U.

We will now give an example of this construction. Our most recent example left us with a $(8, 4, 4, -)$ covering EBS D_1, D_2, D_3, D_4 in $G' = \mathbb{Z}_4 \times \mathbb{Z}_2^2$. We defined $D_1 = B_1 \bigcup (1, 0, 0) + B_5$, $D_2 = B_2 \bigcup (1, 0, 0) + B_6$, $D_3 = B_3 \bigcup (1, 0, 0) + B_7$, and $D_4 = B_4 \bigcup (1, 0, 0) + B_8$ where B_1 is the empty block, and $B_i, i = 2, \ldots 8$ are the 7 hyperplanes of $G = \mathbb{Z}_2^3$ inside of G'. Explicitly:

- $D_1 = \{\emptyset \bigcup (1, 0, 0) + < (2, 1, 0), (0, 0, 1) >\} =$
  $\{(1, 0, 0), (3, 1, 0), (1, 0, 1), (3, 1, 1)\}$
- $D_2 =< (0, 1, 0), (0, 0, 1) > \bigcup (1, 0, 0) + < (2, 0, 1), (0, 1, 0) >=$
  $\{(0, 0, 0), (0, 1, 0), (0, 0, 1), (0, 1, 1), (1, 0, 0), (3, 0, 1), (1, 1, 0), (3, 1, 1)\}$
- $D_3 =< (2, 0, 0), (0, 0, 1) > \bigcup (1, 0, 0) + < (0, 1, 1), (2, 0, 0) >=$
  $\{(0, 0, 0), (2, 0, 0), (0, 0, 1), (2, 0, 1), (1, 0, 0), (1, 1, 1), (3, 0, 0), (3, 1, 1)\}$
- $D_4 =< (2, 0, 0), (0, 1, 0) > \bigcup (1, 0, 0) + < (2, 1, 0), (0, 1, 1) >=$
  $\{(0, 0, 0), (2, 0, 0), (0, 1, 0), (2, 1, 0), (1, 0, 0), (3, 1, 0), (1, 1, 1), (3, 0, 1)\}$

Now, we will use this $(8, 4, 4, -)$ covering EBS in $H/U \approx \mathbb{Z}_4 \times \mathbb{Z}_2^2$ to construct a $(16, 8, 4, -)$ EBS on $H = \mathbb{Z}_4^2 \times \mathbb{Z}_2$ relative to $U =< (0, 2, 0) >$ according to the method above. Note that to remain consistent with the notation from the previous example, the notation in this construction differs from that in the argument above. Here D_i is used in place of B'_i and C_i is used in place of B_i.

- $C_1 = \bigcup_{d \in D_1} d + U = \{(1, 0, 0), (1, 2, 0), (3, 1, 0), (3, 3, 0), (1, 0, 1), (1, 2, 1), (3, 1, 1), (3, 3, 1)\}$
- $C_2 = \bigcup_{d \in D_2} d + U = \{(0, 0, 0), (0, 2, 0), (0, 1, 0), (0, 3, 0), (0, 0, 1), (0, 2, 1), (0, 1, 1), (0, 3, 1),$
  $(1, 0, 0), (1, 2, 0), (3, 0, 1), (3, 2, 1), (1, 1, 0), (1, 3, 0), (3, 1, 1), (3, 3, 1)\}$

- $C_3 = \bigcup_{d \in D_3} d + U = \{(0,0,0),(0,2,0),(2,0,0),(2,2,0),(0,0,1),(0,2,1),(2,0,1),(2,2,1),$ $(1,0,0),(1,2,0),(1,1,1),(1,3,1),(3,0,0),(3,2,0),(3,1,1),(3,3,1)\}$
- $C_4 = \bigcup_{d \in D_4} d + U = \{(0,0,0),(0,2,0),(2,0,0),(2,2,0),(0,1,0),(0,3,0),(2,1,0),(2,3,0),$ $(1,0,0),(1,2,0),(3,1,0),(3,3,0),(1,1,1),(1,3,1),(3,0,1),(3,2,1)\}$

We will now construct our $(16,8,4)$ building set on H relative to U. To facilitate our construction we will introduce a new notation. We will write $H =< X, Y, z | X^4 = Y^4 = z^2 = 1 >$ and $U =< Y^2 >$. This construction process will follow a similar building up pattern as the construction of our $(16,8,4,-)$EBS. We will use the $(2,2,2)$ BS constructed in Example 11 as our starting point. Using our new notation, if we let $G_1 =< x, y | x^2 = y^2 = 1 > \approx \mathbb{Z}_2 \times \mathbb{Z}_2$ we have a $(2,2,2)$ building set on G_1 relative to $< y >$ composed of the blocks:

- $B_1 =< x >$
- $B_2 =< xy >$

Now, let $G_2 =< x, Y | x^2 = Y^4 = 1 >$. We can use our building set on G_1 to construct a $(4,2,1)$ building set on G_2 relative to $< Y^2 >$ consisting of the block:

- $< x > \bigcup Y < xY^2 >$

The following theorem justifies the claim:

Theorem 18. *Given a (a,m,h) BS on a group G relative to a subgroup U, there exists a $(ah,m,1)$ BS on a group G' relative to U, where G' is any group containing G as a subgroup of index h.*

Proof: Suppose G' is a group containing G as a subgroup of index h, and let $\{B_1, B_2, \ldots, B_h\}$ be a (a,m,h) BS on G relative to a subgroup U. Let $g'_1, g'_2, \ldots, g'_h \in G'$ be the coset representatives of G in G'. Now define as subset of G' $B = \bigcup_{i=1}^{h} g'_i B_i$. I claim that $\{B\}$ is our $(ah,m,1)$ in G'. To see this, let χ be a nonprincipal character of G'. Now compute $\chi(\bigcup_{i=1}^{h} g'_i B_i) = \sum_{i=1}^{h} \chi(g'_i B_i) =$

$\sum_{i=1}^{h} \chi(g_i')\chi(B_i)$. We must consider the value of $\chi(B)$ in the following three cases: 1) χ is nonprincipal on G' and principal on G 2) χ is nonprincipal on G (and hence nonprincipal on G') and principal on U and 3) χ is nonprincipal on U. Suppose χ is nonprincipal on G' and principal on G (case 1). Now, $\chi(B) = \sum_{i=1}^{h} \chi(g_i')\chi(B_i) = \sum_{i=1}^{h} \chi(g_i')|B_i| = \sum_{i=1}^{h} \chi(g_i')|B_i| = a\sum_{i=1}^{h} \chi(g_i') = a\psi(G/U)$, where ψ is the character nonprincipal on G/U guaranteed by Theorem 7. We have that $\chi(B) = a\psi(G/U) = a(0) = 0$. Now, suppose that χ is nonprincipal on G and principal on U (case 2). By the definition of a building set, since χ is principal on U, $\chi(B_i) = 0$ for all i. Now we compute $\chi(B) = \sum_{i=1}^{h} \chi(g_i')\chi(B_i) = \sum_{i=1}^{h} \chi(g_i')(0) = 0$. Finally, suppose that χ is nonprincipal on U (case 3). Then by the definition of building set, $\chi(B_i)$ has non-zero character sum for precisely one value of i, say when $i = j$. Now $\chi(B) = \sum_{i=1}^{h} \chi(g_i')\chi(B_i) = \chi(g_j')\chi(B_j) \neq 0$. In summary, when χ is nonprincipal on U (case 3), precisely one building block (in this case, the only block B) has nonzero character sum. When χ is principal on U (cases 1 and 2), no building block has nonzero character sum. Thus $\{B\}$ satisfies the definition of a $(ah, m, 1)$ building set in G'. □

So, we now have a $(4, 2, 1)$ building set on G_2 relative to $< Y^2 >$. There are two steps remaining in our construction of a $(16, 8, 4)$ building set. The first step is to use our $(4, 2, 1)$ building set on G_2 relative to $< Y^2 >$ to construct a $(8, 4, 2)$ building set on $G_3 =< X, Y | X^4 = Y^4 = 1 >$ relative to $< Y^2 >$. The second and final step will be to use our $(8, 4, 2)$ building set on G_3 from step one to construct a $(16, 8, 4)$ building set on $H =< X, Y, z | X^4 = Y^4 = z^2 = 1 >$ relative to $U =< Y^2 >$. These two steps are based on the same argument and construction method, which is presented in the following proof:

Theorem 19. *Let G be a group of order $4a$ for some $a \in \mathbb{Z}^+$ containing a subgroup $Q \approx \mathbb{Z}_2^2$. Let H_0, H_1, H_2 be the subgroups of G of order 2 corresponding to hyperplanes viewed as subgroups of Q. Given a $(a, \sqrt{at}, t)$ BS on G/H_i relative to Q/H_i for $i = 1, 2$, there exists a $(2a, 2\sqrt{at}, 2t)$ BS on G relative to H_0.*

Proof: Suppose we have a group G of order $4a$ with a subgroup $Q \approx \mathbb{Z}_2^2$, and let H_0, H_1, H_2 be the subgroups of G of order 2 corresponding to hyperplanes viewed as subgroups of Q. Let

$\{B'_{11}, B'_{12}, \ldots, B'_{1t}\}$ be a $(a, \sqrt{at}, t)$ BS on G/H_1 relative to Q/H_1 and $\{B'_{21}, B'_{22}, \ldots, B'_{2t}\}$ be a $(a, \sqrt{at}, t)$ BS on G/H_2 relative to Q/H_2. Define $B_{1j} = \{g \in G | gH_1 \in B'_{1j}\}$ and $B_{2j} = \{g \in G | gH_2 \in B'_{2j}\}$. Thus, B_{ij} is the union of $|B'_{ij}| = a$ distinct cosets of H_i for $i = 1, 2$, which implies that $|B_{ij}| = 2a$. Let χ be a character nonprincipal on G, and compute $\chi(B_{ij})$ for $i = 1, 2$ and $j = 1, \ldots, t$: $\chi(B_{ij}) = \begin{cases} 0 & \text{if } \chi \text{ nonprincipal on } H_i \\ 2\psi(B'_{ij}) & \text{if } \chi \text{ principal on } H_i \end{cases}$, where ψ is the nonprincipal character induced by χ on G/H_i. Applying the definition of a building set, for $i = 1, 2$, if χ is nonprincipal on Q/H_i, then $\psi(B'_{ij})$ is nonzero with modulus $\sqrt{at}$ for one value of j, and if χ is principal on Q/H_i then $\psi(B'_{ij}) = 0$ for all j.

We have three cases to consider: 1) χ is principal on H_k for either $k = 1$ or $k = 2$ and nonprincipal on $H_i, i \neq k$ 2) χ is principal on H_0 and nonprincipal on H_1, H_2, and 3) χ is nonprincipal on Q.

We now consider the first case. Suppose χ is principal on H_k for either $k = 1$ or $k = 2$ and nonprincipal on $H_i, i \neq k$. Then $\chi(B_{ij}) = 0$ for $i \neq k$ and $\chi(B_{ij}) = 2\psi(B'_{ij})$ for $i = k$. Since χ is nonprincipal on H_k, χ is nonprincipal on Q and thus ψ is nonprincipal on Q/H_k. Therefore, $\psi(B'_{kj})$ is nonzero with modulus $\sqrt{at}$ for a particular j. Now, consider the second case: χ is principal on H_0 and nonprincipal on H_1, H_2. For $i = 1, 2$, $\chi(B_{ij}) = 0$. Finally, consider the third case, when χ is nonprincipal on Q. This implies that χ is principal on H_0, H_1, and H_2. Thus, $\chi(B_{ij}) = 2\psi(B'_{ij})$ for $i = 1, 2$. By definition, ψ is principal on Q/H_i. This implies $\psi(B'_{ij}) = 0$ for all i, j. Thus, by definition, the set $\{B_{ij} | i = 1, 2, j = 1, \ldots, t\}$ is a $(2a, 2\sqrt{at}, 2t)$ BS on G relative to H_0. □

Now we can apply this result to construct a $(8, 4, 2)$ building set on $G_3 =< X, Y | X^4 = Y^4 = 1 >$ relative to $< Y^2 >$. Let $Q =< X^2, Y^2 >$ where the hyperplanes of Q are $H_0 =< Y^2 >, H_1 =< X^2 >, H_2 =< X^2Y^2 >$. Since $G_3/H_i \approx G_2$ with $Q/H_i \approx < Y^2 >$ for $i = 1, 2$, we can use our $(4, 2, 1)$ building set on G_2 to construct $(8, 4, 2)$ building set on G_3 consisting of the following blocks:

- $< X > \bigcup Y < XY^2 >$
- $< XY > \bigcup Y < XY^3 >$

In the same manner, we can construct a $(16, 8, 4)$ building set on $H =< X, Y, z | X^4 = Y^4 = z^2 = 1 >$ relative to $U =< Y^2 >$ using our $(8, 4, 2)$ building set on G_3. To satisfy the assumptions of Theorem 19, we let $Q =< Y^2, z >$, where the hyperplanes of Q are $H_0 =< Y^2 >, H_1 =< z >, H_2 =< Y^2 z >$. Our resulting building set on H consists of the following blocks:

- $< X > \bigcup Y < XY^2 > \bigcup z < X > \bigcup Yz < XY^2 >$
- $< XY > \bigcup Y < XY^3 > \bigcup z < XY > \bigcup Yz < XY^3 >$
- $< X > \bigcup Y < XY^2 > \bigcup Y^2 z < X > \bigcup Y^3 z < XY^2 >$
- $< XY > \bigcup Y < XY^3 > \bigcup Y^2 z < XY > \bigcup Y^3 z < XY^3 >$

Using the same notation as our EBS, we write our $(16, 8, 4)$ building set on $H =< X, Y, z | X^4 = Y^4 = z^2 = 1 >$ additively in the following manner:

- $C_5 = \{(0,0,0), (1,0,0), (2,0,0), (3,0,0), (0,1,0), (1,3,0), (2,1,0), (3,3,0), (0,0,1), (1,0,1), (2,0,1), (3,0,1), (0,1,1), (1,3,1), (2,1,1), (3,3,1)\}$
- $C_6 = \{(0,0,0), (1,0,0), (2,0,0), (3,0,0), (0,1,0), (1,3,0), (2,1,0), (3,3,0), (0,2,1), (1,2,1), (2,2,1), (3,2,1), (0,3,1), (1,1,1), (2,3,1), (3,1,1)\}$
- $C_7 = \{(0,0,0), (1,1,0), (2,2,0), (3,3,0), (0,1,0), (1,0,0), (2,3,0), (3,2,0), (0,0,1), (1,1,1), (2,2,1), (3,3,1), (0,1,1), (1,0,1), (2,3,1), (3,2,1)\}$
- $C_8 = \{(0,0,0), (1,1,0), (2,2,0), (3,3,0), (0,1,0), (1,0,0), (2,3,0), (3,2,0), (0,2,1), (1,3,1), (2,0,1), (3,1,1), (0,3,1), (1,2,1), (2,1,1), (3,0,1)\}$

We now combine our $(16, 8, 4, -)$ EBS on $H = \mathbb{Z}_4^2 \times \mathbb{Z}_2$ with our $(16, 8, 4)$ building set on $H =< X, Y, z | X^4 = Y^4 = z^2 = 1 >$ to obtain our $(16, 8, 8, -)$ covering EBS on H relative to $U =< Y^2 >$ (or written additively $U =< (0, 2, 0) >$), consisting of the following blocks:

- $C_1 = \{(1,0,0), (1,2,0), (3,1,0), (3,3,0), (1,0,1), (1,2,1), (3,1,1), (3,3,1)\}$

- $C_2 = \{(0,0,0),(0,2,0),(0,1,0),(0,3,0),(0,0,1),(0,2,1),(0,1,1),(0,3,1),(1,0,0),(1,2,0),$ $(3,0,1),(3,2,1),(1,1,0),(1,3,0),(3,1,1),(3,3,1)\}$
- $C_3 = \{(0,0,0),(0,2,0),(2,0,0),(2,2,0),(0,0,1),(0,2,1),(2,0,1),(2,2,1),(1,0,0),(1,2,0),$ $(1,1,1),(1,3,1),(3,0,0),(3,2,0),(3,1,1),(3,3,1)\}$
- $C_4 = \{(0,0,0),(0,2,0),(2,0,0),(2,2,0),(0,1,0),(0,3,0),(2,1,0),(2,3,0),(1,0,0),(1,2,0),$ $(3,1,0),(3,3,0),(1,1,1),(1,3,1),(3,0,1),(3,2,1)\}$
- $C_5 = \{(0,0,0),(1,0,0),(2,0,0),(3,0,0),(0,1,0),(1,3,0),(2,1,0),(3,3,0),(0,0,1),(1,0,1),$ $(2,0,1),(3,0,1),(0,1,1),(1,3,1),(2,1,1),(3,3,1)\}$
- $C_6 = \{(0,0,0),(1,0,0),(2,0,0),(3,0,0),(0,1,0),(1,3,0),(2,1,0),(3,3,0),(0,2,1),(1,2,1),$ $(2,2,1),(3,2,1),(0,3,1),(1,1,1),(2,3,1),(3,1,1)\}$
- $C_7 = \{(0,0,0),(1,1,0),(2,2,0),(3,3,0),(0,1,0),(1,0,0),(2,3,0),(3,2,0),(0,0,1),(1,1,1),$ $(2,2,1),(3,3,1),(0,1,1),(1,0,1),(2,3,1),(3,2,1)\}$
- $C_8 = \{(0,0,0),(1,1,0),(2,2,0),(3,3,0),(0,1,0),(1,0,0),(2,3,0),(3,2,0),(0,2,1),(1,3,1),$ $(2,0,1),(3,1,1),(0,3,1),(1,2,1),(2,1,1),(3,0,1)\}$

3 Non-Abelian Groups

Now that we have our $(16,8,8,-)$ covering EBS $\{C_1, C_2, \ldots, C_8\}$ in $H = \mathbb{Z}_4^2 \times \mathbb{Z}_2$, where we denote the building blocks $C_1, C_2, \ldots, C_8$, we know precisely how to obtain a $(256,120,56)$ difference set in any abelian group G that contains H has a subgroup: we simply attach the 8 distinct coset representatives g_i from the elements in G/H to the blocks C_i and take the union of all $g_i C_i$. (From now on, when we say we attach a coset representative to a block we mean that we take the product of the coset representative with each element in the block.) However, the assumption that G is abelian is severely limiting. Furthermore, whether or not G is abelian is not relevent in our construction of the $(16,8,8,-)$ covering EBS in H. (Since $H = \mathbb{Z}_4^2 \times \mathbb{Z}_2$, H is abelian even if G is not.) Here we will compare the case that G is abelian with the case the G is non-abelian.

Let G be a group (not necessarily abelian) with normal subgroup $H \approx \mathbb{Z}_4^2 \times \mathbb{Z}_2$, and let g_i be the coset representatives from the elements in the factor group G/H. As before, define $D = \bigcup_{i=1}^{8} g_i C_i$. Consider what happens when we compute the set $DD^{(-1)} = \{d_i d_j^{-1} | d_i, d_j \in D\}$: $DD^{(-1)} = \{g_1 C_1 \bigcup g_2 C_2 \bigcup \dots g_8 C_8\}\{C_1^{(-1)} g_1^{-1} \bigcup C_2^{(-1)} g_2^{-1} \bigcup \dots C_8^{(-1)} g_8^{-1}\} = \bigcup g_i C_i C_j^{(-1)} g_j^{-1}$ for $i = 1, \dots, 8$ and $j = 1, \dots, 8$. We will consider $C_i C_j^{(-1)}$ in two cases: first, when $i \neq j$ and second, when $i = j$. Suppose $i \neq j$. Since $C_1, C_2, \dots, C_8$ is a covering EBS, $\chi(C_k)$ has nonzero sum for exactly one value of k. Consider $\chi(C_i C_j^{(-1)}) = \chi(C_i)\chi(C_j^{(-1)}) = \chi(C_i)\overline{\chi(C_j)}$. If $i = k$, then $\chi(C_j) = 0$ (and $\overline{\chi(C_j)} = 0$). Likewise, If $j = k$ then $\chi(C_i) = 0$. In either case, $\chi(C_i C_j^{(-1)}) = \chi(C_i)\overline{\chi(C_j)} = 0$. It follows that $C_i C_j^{(-1)} = k_1 H$ for some constant k_1. Now, we will add the coset representatives: $g_i C_i C_j^{(-1)} g_j^{-1} = g_i k_1 H g_j^{-1} = k_1 g_i H g_j^{-1} = k_1 g_i g_j^{-1} H$ since H is normal in G. Thus, $\bigcup g_i C_i C_j^{(-1)} g_j^{-1}$ for $i = 1, \dots, 8$ and $j = 1, \dots, 8, i \neq j$ contributes the same elements to the set $DD^{(}-1)$ in the case that G is abelian or non-abelian.

Now suppose $i = j$ and consider $C_i C_j^{(-1)} = C_i C_i^{(-1)}$. We cannot definitively determine the elements of $C_i C_i^{(-1)}$ since C_i will have a nonzero character sum for some but not all characters nonprincipal H. However, we can glean useful information when considering the union of all $C_i C_i^{(-1)}$. Let χ be a character nonprincipal on H. Then precisely one block, say C_k, has a nonzero character sum. So, $\chi(\bigcup_{i=1}^{8} C_i C_i^{(-1)}) = \sum_{i=1}^{8} \chi(C_i C_i^{(-1)}) = \sum_{i=1}^{8} \chi(C_i)\chi(C_i^{(-1)}) = \sum_{i=1}^{8} \chi(C_i)\overline{\chi(C_i)} = \sum_{i=1}^{8} |\chi(C_i)|^2 = |\chi(C_k)|^2 = m^2$. This implies that $\chi(\bigcup_{i=1}^{8} C_i C_i^{(-1)}) - m^2 = \chi(\bigcup_{i=1}^{8} C_i C_i^{(-1)}) - \chi(m^2 e) = \chi(\bigcup_{i=1}^{8} C_i C_i^{(-1)} - (m^2 e)) = 0$. Thus, $\bigcup_{i=1}^{8} C_i C_i^{(-1)} - (m^2 e) = k_2 H$ for some constant k_2. Equivalently, $\bigcup_{i=1}^{8} C_i C_i^{(-1)} = k_2 H + m^2 e$ Now, we will again add the coset representatives. Notice that in the abelian case $\bigcup_{i=1}^{8} g_i C_i C_i^{(-1)} g_i^{-1} = \bigcup_{i=1}^{8} g_i g_i^{-1} C_i C_i^{(-1)} = \bigcup_{i=1}^{8} g_i g_i^{-1} C_i C_i^{(-1)} = \bigcup_{i=1}^{8} C_i C_i^{(-1)} = c_2 H + m^2 e$. Thus, to obtain a difference set in a non-abelian G, coset representatives g_i must be chosen so that $\bigcup_{i=1}^{8} g_i C_i C_i^{(-1)} g_i^{-1} = c_2 H + m^2 e$. The value of k_2 can be calculated as follows: We know that $|\bigcup_{i=1}^{8} g_i C_i C_i^{(-1)} g_i^{-1}| = |k_2 H + m^2 e|$. Thus, $7 * 16^2 + 8 * 8 = |H| k_2 + m^2 = 32 k_2 + m^2$. We also know that the identity element must show up $|\bigcup_{i=1}^{8} C_i| = \sum_i = 1^8 |C_i| = 7 * 16 + (16 - 8) = 120$ times. It follows that $k_2 + m^2 = 120$. Solving this system of equations for k_2 we get $k_2 = 56$. Since $\lambda = 56$ in a $(256, 120, 56, 64)$-difference set, $i \neq j$ $g_i B_i B_j^{(-1)} g_j^{-1} = g_i c H g_j^{-1} = k_1 g_i H g_j^{-1} = k_1 g_i g_j^{-1} H$ must contain the elements of the nontrivial

cosets of H 56 times and it follows that $k_1 = 56$.

To better understand the role of the coset representative g_i in the conjugation of $B_i B_i^{(-1)}$, we have computed the sets $B_i B_i^{(-1)}$ for $i = 1, \ldots, 8$, shown below. The "coefficient" of each element of H tells us how many times that element appears in the multiset $B_i B_i^{(-1)}$. (We have omitted the identity element.) For example, `8 (0,0,1)` in the block of elements below `B1` tells us that $(0, 0, 1) \in H$ appears in $B_1 B_1^{(-1)}$ 8 times.

```
B1:
8 (0,0,1),  0 (0,1,0),  0 (0,1,1),  8 (0,2,0),  8 (0,2,1),  0 (0,3,0),  0 (0,3,1),
0 (1,0,0),  0 (1,0,1),  0 (1,1,0),  0 (1,1,1),  0 (1,2,0),  0 (1,2,1),  0 (1,3,0),
0 (1,3,1),  0 (2,0,0),  0 (2,0,1),  8 (2,1,0),  8 (2,1,1),  0 (2,2,0),  0 (2,2,1),
8 (2,3,0),  8 (2,3,1),  0 (3,0,0),  0 (3,0,1),  0 (3,1,0),  0 (3,1,1),  0 (3,2,0),
0 (3,2,1),  0 (3,3,0),  0 (3,3,1)
B2:
8 (0,0,1), 16 (0,1,0),  8 (0,1,1), 16 (0,2,0),  8 (0,2,1), 16 (0,3,0),  8 (0,3,1),
8 (1,0,0),  8 (1,0,1),  8 (1,1,0),  8 (1,1,1),  8 (1,2,0),  8 (1,2,1),  8 (1,3,0),
8 (1,3,1),  0 (2,0,0),  8 (2,0,1),  0 (2,1,0),  8 (2,1,1),  0 (2,2,0),  8 (2,2,1),
0 (2,3,0),  8 (2,3,1),  8 (3,0,0),  8 (3,0,1),  8 (3,1,0),  8 (3,1,1),  8 (3,2,0),
8 (3,2,1),  8 (3,3,0),  8 (3,3,1)
B3:
8 (0,0,1),  0 (0,1,0),  8 (0,1,1), 16 (0,2,0),  8 (0,2,1),  0 (0,3,0),  8 (0,3,1),
8 (1,0,0),  8 (1,0,1),  8 (1,1,0),  8 (1,1,1),  8 (1,2,0),  8 (1,2,1),  8 (1,3,0),
8 (1,3,1), 16 (2,0,0),  8 (2,0,1),  0 (2,1,0),  8 (2,1,1), 16 (2,2,0),  8 (2,2,1),
0 (2,3,0),  8 (2,3,1),  8 (3,0,0),  8 (3,0,1),  8 (3,1,0),  8 (3,1,1),  8 (3,2,0),
8 (3,2,1),  8 (3,3,0),  8 (3,3,1)
B4:
0 (0,0,1),  8 (0,1,0),  8 (0,1,1), 16 (0,2,0),  0 (0,2,1),  8 (0,3,0),  8 (0,3,1),
8 (1,0,0),  8 (1,0,1),  8 (1,1,0),  8 (1,1,1),  8 (1,2,0),  8 (1,2,1),  8 (1,3,0),
8 (1,3,1),  8 (2,0,0),  8 (2,0,1), 16 (2,1,0),  0 (2,1,1),  8 (2,2,0),  8 (2,2,1),
16 (2,3,0),  0 (2,3,1),  8 (3,0,0),  8 (3,0,1),  8 (3,1,0),  8 (3,1,1),  8 (3,2,0),
8 (3,2,1),  8 (3,3,0),  8 (3,3,1)
B5:
16 (0,0,1), 8 (0,1,0),  8 (0,1,1),  0 (0,2,0),  0 (0,2,1),  8 (0,3,0),  8 (0,3,1),
8 (1,0,0),  8 (1,0,1),  8 (1,1,0),  8 (1,1,1),  8 (1,2,0),  8 (1,2,1),  8 (1,3,0),
8 (1,3,1), 16 (2,0,0), 16 (2,0,1),  8 (2,1,0),  8 (2,1,1),  0 (2,2,0),  0 (2,2,1),
8 (2,3,0),  8 (2,3,1),  8 (3,0,0),  8 (3,0,1),  8 (3,1,0),  8 (3,1,1),  8 (3,2,0),
8 (3,2,1),  8 (3,3,0),  8 (3,3,1)
B6:
0 (0,0,1),  8 (0,1,0),  8 (0,1,1),  0 (0,2,0), 16 (0,2,1),  8 (0,3,0),  8 (0,3,1),
8 (1,0,0),  8 (1,0,1),  8 (1,1,0),  8 (1,1,1),  8 (1,2,0),  8 (1,2,1),  8 (1,3,0),
```

```
8 (1,3,1), 16 (2,0,0),  0 (2,0,1),  8 (2,1,0),  8 (2,1,1),  0 (2,2,0), 16 (2,2,1),
8 (2,3,0),  8 (2,3,1),  8 (3,0,0),  8 (3,0,1),  8 (3,1,0),  8 (3,1,1),  8 (3,2,0),
8 (3,2,1),  8 (3,3,0),  8 (3,3,1)
B7:
16 (0,0,1), 8 (0,1,0),  8 (0,1,1),  0 (0,2,0),  0 (0,2,1),  8 (0,3,0),  8 (0,3,1),
8 (1,0,0),  8 (1,0,1),  8 (1,1,0),  8 (1,1,1),  8 (1,2,0),  8 (1,2,1),  8 (1,3,0),
8 (1,3,1),  0 (2,0,0),  0 (2,0,1),  8 (2,1,0),  8 (2,1,1), 16 (2,2,0), 16 (2,2,1),
8 (2,3,0),  8 (2,3,1),  8 (3,0,0),  8 (3,0,1),  8 (3,1,0),  8 (3,1,1),  8 (3,2,0),
8 (3,2,1),  8 (3,3,0),  8 (3,3,1)
B8:
0 (0,0,1),  8 (0,1,0),  8 (0,1,1),  0 (0,2,0), 16 (0,2,1),  8 (0,3,0),  8 (0,3,1),
8 (1,0,0),  8 (1,0,1),  8 (1,1,0),  8 (1,1,1),  8 (1,2,0),  8 (1,2,1),  8 (1,3,0),
8 (1,3,1),  0 (2,0,0), 16 (2,0,1),  8 (2,1,0),  8 (2,1,1), 16 (2,2,0),  0 (2,2,1),
8 (2,3,0),  8 (2,3,1),  8 (3,0,0),  8 (3,0,1),  8 (3,1,0),  8 (3,1,1),  8 (3,2,0),
8 (3,2,1),  8 (3,3,0),  8 (3,3,1)
```

Note that any nonidentity element $(a_1, a_2, a_3) \in H$ appears 56 times in $\bigcup_{i=1,\ldots,8} B_i B_i^{(-1)}$. For example element $(3, 3, 0)$ appears 8 times in each $B_i B_i^{(-1)}$ for $i = 2, \ldots, 8$. Thus, in order to satisfy $\bigcup_{i=1}^{8} g_i C_i C_i^{(-1)} g_i^{-1} = 56H + m^2 e$, coset representatives g_i must maintain the property that each element of H appears 56 times. For example, any method of attaching coset representatives to blocks in a way that caused a permuation of the blocks would satisfy this. That is, the choice of coset representatives g_i such that $g_i B_i B_i^{(-1)} g_i^- 1 = B_j$ is a one-to-one and onto mapping from $B_1, \ldots, B_j$ to itself. Thus, the way we attach coset representatives to the blocks cannot be arbitrary. However, we expect that some permutation of the coset representatives attached to our blocks will satisfy the necessary property: $\bigcup_{i=1}^{8} g_i C_i C_i^{(-1)} g_i^{-1} = 56H + m^2 e$.

Thus, our hypothesis is as follows: Given a group G with a normal subgroup $H \approx \mathbb{Z}_4^2 \times \mathbb{Z}_2$, we can construct a $(256, 120, 56)$ difference set in G by simply attaching some permutation of the coset representatives from the elements in G/H to the blocks composing our $(16, 8, 8, -)$ covering EBS in H. (This is analogous to the process of constructing a $(128, 8, 1, -)$ covering EBS in G).

4 GAP

We used the GAP software (version 4.63) in order to automate the process for checking for difference sets. GAP, short for Groups, Algorithms, Programming, provides a system for computational discrete algebra along with a programming language. The GAP library contains implementations of many algebraic algorithms and also large data libraries of algebraic objects, including the 56092 groups of order 256.

Before delving into the code written to check for difference sets, we will first give an overview of some of the GAP syntax and structures that will be used repetitively.

The following syntax is used to define a function:

```
MyFunction:=function(formalparameter1, formalparameter2, ..., formalparametern)
//function definition
end;
```

Here, a function with function name `MyFunction` is declared and expects n arguments at runtime. Note that GAP does not require that the type of the formal parameter(s) be specified in a function definition. However, the function can only be called with an argument whose type is supported by the function definition. For example, the operations applied to `formalparameter1` in the function definition must be defined for the type of variable passed in as the first argument at runtime. Note that a function can require zero formal parameters. The entirety of the function definition must be contained within the signature (the first line) and the terminating `end;` command. Then to use the function, simply make the command `MyFunction (argument1, argument2, ..., argumentn);`, where `argument1, argument2, ..., argumentn` correspond to the formal parameters in the function definition.

Within each function, local variables (any variables to be used within the scope of the function) must be the first line of the method definition: `local var1, var2, ... , varn;`

In GAP, the list data structure can be used to store a collection of objects in a particular order, much like the array data structure in many other programming languages. Each element has a particular index, called its position, where the first element has position 1. A list can be defined as follows: `ourlist:=[element1, element2,...,elementn];`

A `for` loop can efficiently loop over a list and perform some operation on each element of the list in order of increasing position. The following syntax accomplishes this:

`for i in listName do someCode; od;`
This line loops over the entire list `listName` and at each iteration temporarily assigns the variable name `i` to the current element. The action to be performed to `i` at each iteration is specified between `do` and `od;`. (`someCode` is used to show the location.)

An `if` statement can be used to perform some operation depending on the condition. The following syntax is used to achieve this: `if condition then someCode;` If the `condition` is true, then `someCode` executes. Otherwise, it is skipped.

Note that there are many functions built into the GAP library. In the method `NormalSubgroupCheck` displayed below, the following built in functions are used: `SmallGroup(), NormalSubgroups(), StructureDescription()` and `Add()`. The GAP documentation specifies the type and number of arguments required and the return type of each function. For example, the `SmallGroup()` function expects two integer arguments `i` and `j` and returns the group of size `i` and of index `j` from the GAP libraries.

Now, we will take a closer look at the GAP code used to automate the construction method outlined above.

We received a list of group indices from Dr. Dillon of the groups of order 256 in which the existence of a difference set was unknown. (The index of a group is simply a reference to the particular group in the GAP library.) This list contained 724 groups of order 256. Recall, our construction method to determine a difference set in a group G requires that G contain a normal subgroup $H \approx \mathbb{Z}_4^2 \times \mathbb{Z}_2$.

Thus, we first determined which of the 724 groups contained the necessary H. The following function achieves this result:

```
NormalSubgroupCheck:=function(groups)

local normal, j, dsIndices, i, G;
dsIndices:=[];

for j in groups do
         G:=SmallGroup(256, j);
         normal:=NormalSubgroups(G);
         for i in normal do
                  if StructureDescription(i)="C4 x C4 x C2" then
                           Add(dsIndices, j);
                           break;
                  fi;
         od;
od;
return dsIndices;
end;
```

The function defined above is named `NormalSubgroupCheck` and expects a single argument at runtime that will take on the variable name `groups`. We have written the function to accomodate the `groups` parameter as a list of integers, in particular, the list of integers containing the indices of the 724 groups in which the existence of a difference set is unknown.

The `NormalSubgroupCheck` function declares `normal, j, dsIndices, i,`and `G` as variables local to the function. We set the variable `dsIndices` equal to an empty list that will eventually contain the indices of the groups with the desired normal subgroup.

The for-loop iterates through `groups` (assumed to be a list of integers), and for each index, temporarily stored in the variable `j`, we set the variable `G` equal to the the group of order 256 with index `j`. We then assign the variable `normal` to the list of the normal subgroups of `G`. The inner for-loop iterates through the the list `normal`, and each element of `normal` (the normal subgroups of `G`) is temporarily stored in the variable `i`. If the subgroup stored in `i` has structure description "C4 x C4 x C2" (i.e. is isomorphic to $\mathbb{Z}_4^2 \times \mathbb{Z}_2$), we add `j`, the current index of the group stored

in G, to the list dsIndices. Upon completion of the function call, the variable dsIndices contains the indices from the list passed in as a parameter that correspond to groups containing a normal $\mathbb{Z}_4^2 \times \mathbb{Z}_2$ subgroup. This list is returned by the function.

Thus, if the variable list stores the list of indices provided by Dr. Dillion, the function call NormalSubgroupCheck(list) returns the list of the indices in list that correspond to the groups containing a $\mathbb{Z}_4^2 \times \mathbb{Z}_2$ normal subgroup. Of the 724 groups in which the existence of the difference set was unknown, 649 contain a $\mathbb{Z}_4^2 \times \mathbb{Z}_2$ normal subgroup .

Once we had determined the list of indices of groups that contained the necessary $\mathbb{Z}_4^2 \times \mathbb{Z}_2$ subgroup, the following code automated the construction method outlined above. We will walk through the code, and preface each block of code with a description of its functionality and purpose.

The code below defines the function GetDifferenceSet and declares the local parameters. These are all of the parameters to be used throughout the function, and their purpose will be explained when they are used. The variable success is set to an empty list, and this will be used to store the indices corresponding to groups containing a difference set built by our construction method. The function will ultimately return success. The list variable, here shown in abbreivated form, is the list of indices returned by the NormalSubgroupCheck function. That is, it is a list of 649 indices corresponding to the groups out of the original 724 that contain the desired $\mathbb{Z}_4^2 \times \mathbb{Z}_2$ normal subgroup.

```
GetDifferenceSet:=function()
local E, i, j, k, c1c2, c1c2c3, N, r1, r2, r3, r4, r5, r6, r7, r8, cosets,
D1, D2, D3, D4, D5, D6, D7, D8, X, Y, z, l, NS, groupElts, v, m, p, q,t, i
ndex, count, current, currentPerm, DSCheck, a, b, c, d,e, temp, dsfound,
cosetReps, list, w, G, attempts, success;

success:=[];
list:=[ 2, 3, 6, 7,..., 51711];
```

The remainder of the function, excluding the return statement, is included in the for loop which begins in the code below. The loop iterates through each index in list, temporarily stored in w.

The four variables instantiated are variables that are reset each time we consider a new index `w` in `list`. The variable `currentPerm` is a list used to store a permuation of the integers 1 through 8. The functionality of the variable is that it enables us to systematically assign the 8 coset representatives from the factor group G/H to our 8 blocks. Each integer will correspond to a particular coset representative, and a permuation of these integers (in list form) will correspond to a particular assignment of the coset representatives to our blocks. The `dsfound` is a boolean variable that represents whether or not a difference set has been found for the current group. It is instantiated to false and is set to true when a difference set is confirmed. The variable `G` is set to the group in the GAP library of size 256 corresponding to index `w`. The variable `NS` is set equal to a list of the normal subgroups of the group G.

```
for w in list do
        currentPerm:=[1, 2, 3, 4, 5, 6, 7, 8];
        dsfound:=false;
        G:=SmallGroup(256, w);
        NS:=NormalSubgroups(G);
```

The purpose of the code below is to find the normal subgroup of the group `G` that is isomorphic to $\mathbb{Z}_4^2 \times \mathbb{Z}_2$. Since we are only considering the indices that were returned by the `NormalSubgroupCheck()` function, we know that each index in `list` corresponds to a group with the desired normal subgroup. The code iterates through each normal subgroup `l` of `G` stored in the list `NS`, and checks whether it is isomorphic to $\mathbb{Z}_4^2 \times \mathbb{Z}_2$. The first normal subgroup to satisfy this condition is stored in the variable `N` and then we break out of the loop.

```
for l in NS do
        if StructureDescription(l)="C4 x C4 x C2" then
                N:=l;
                break;
        fi;
od;
```

Next, we find the generators of the normal subgroup `N`. We set the variable `E` equal to a list of the elements of `G` in `N`. If we define `N` $\approx < X, Y, z | X, Y \in \mathbb{Z}_4, z \in \mathbb{Z}_2 >$, the three `for` loops below find

X, Y and z and we call them `X, Y` and `z`. Because GAP does not store group generators in the way that we would expect algebraically, we have to look through `E` and find the elements with the desired properties. Thus, we look for two elements of order 4 and one element of order 2 that generate a subgroup isomorphic to $\mathbb{Z}_4^2 \times \mathbb{Z}_2$.

The first `for` loop iterates through each element `i` of `E` and sets the variable `X` equal to the first element of order 4. Now in the second `for` loop we again iterate through the elements `j` of `E`. If `j` is an element of order 4, we set `c1c2` equal to the subgroup generated by `X` and `j`. If the number of elements in `c1c2` is 16, then we know that `c1c2` $\approx \mathbb{Z}_4^2$, we set our second generator `Y` equal to `j` and break out of the loop. In the third `for` loop we iterate through the elements `k` of `E`. If `k` is an element of order 2, we set `c1c2c3` equal to the subgroup generated by `X, Y` and `k`. If the number of elements in `c1c2c3` is 32, then we know that `c1c2c3` $\approx \mathbb{Z}_4^2 \times \mathbb{Z}_2$, and we set our third generator `z` equal to `k` and break out of the loop. At this point, the variables `X, Y` and `z` are equal to the generators of `N`.

```
E:=Elements(N);
for i in E do
        if Order(i)=4 then
                X:=i;
                break;
        fi;
od;


for j in E do
        if Order(j)= 4 then
                c1c2:=Subgroup(N, [X,j]);

                if Size(Elements(c1c2))=16 then
                        Y:=j;
                        break;

                fi;
        fi;
od;

for k in E do
        if Order(k) = 2 then
```

```
                c1c2c3:=Subgroup(N, [X,Y,k]);
                if Size(Elements(c1c2c3)) = 32 then
                        z:= k;
                        break;
                fi;
        fi;
od;
```

Now, we want to find coset representatives for the elements in the factor group G/H. To do this, we assign the variable `cosets` equal to the two dimensional list returned by the function call `CosetDecomposition(G,N)`. The function returns a list of the cosets of `N` in `G`, where each coset is represented as a list of elements of `G` in that coset. The syntax `cosets[i][j]` refers to the `j`th element in the `i`th coset of `N`. Now we arbitrarily choose the first element from each of the 8 cosets as our coset representatatives and assign them to the variables `r1` through `r8`. We store the coset representatives in a list called `cosetReps`.

```
cosets:=CosetDecomposition(G,N);

r1:=cosets[1][1];
r2:=cosets[2][1];
r3:=cosets[3][1];
r4:=cosets[4][1];
r5:=cosets[5][1];
r6:=cosets[6][1];
r7:=cosets[7][1];
r8:=cosets[8][1];

cosetReps:=[r1,r2,r3,r4,r5,r6,r7,r8];
```

We are now prepared to construct our blocks in GAP. In terms of our generators $X, Y,$ and z, represented by `X, Y` and `z`, our blocks are as follows:

- $d_1 =< X^2, Y > \bigcup X < X^2 z, Y >$
- $d_2 =< X^2, Yz > \bigcup X < X^2 z, Yz >$
- $d_3 =< X, Y^2 z > \bigcup Y < XY^2, Y^2 z >$

- $d_4 =< XY, Y^2z > \bigcup Y < XY^3, Y^2z >$
- $d_5 =< X, z > \bigcup Y < XY^2, z >$
- $d_6 =< X^2, Y^2, z >$
- $d_7 =< Y, z > \bigcup X < X^2Y, z >$
- $d_8 =< XY, z > \bigcup X < X^3Y, z >$

Note that these blocks are a slight variation on the blocks constructed earlier in this paper.

The code below constructs these blocks stored as lists of elements named `d1` through `d8`. We will walk through the construction of `d1` using our generators and GAP methods, and from this the construction of the remaining blocks should be clear. First, we declare `d1` to be an empty list. Now let's look at the following nested function calls: `Append(D1, Elements(Subgroup(G, [X^2, Y])));` . The function call `Subgroup(G, [X^2, Y])` returns the subgroup of `G` generated by `X^2` and `Y` . `Elements(Subgroup(G, [X^2, Y])` returns a list of elements of this subgroup, and finally `Append(D1, Elements(Subgroup(G, [X^2, Y])));` adds each of the elements in this list to `d1`.

There is one slight difference that requires explanation with the following function call:

```
Append(D1, Elements(RightCoset(Subgroup(G, [X^2*z, Y]),X)));
```

`Subgroup(G, [X^2*z, Y])` returns the subgroup of `G` generated by `X^2*z` and `Y`.
Now `RightCoset(Subgroup(G, [X^2*z, Y]),X))` returns the right coset of the subgroup using `X` as the coset representative.

```
d1:=[];
Append(d1, Elements(Subgroup(G, [X^2, Y])));
Append(d1, Elements(RightCoset(Subgroup(G, [X^2*z, Y]),X)));
```

```
d2:= [];
```

```
Append(d2, Elements(Subgroup(G, [X^2, Y*z])));
Append(d2, Elements(RightCoset(Subgroup(G, [X^2*z, Y*z]),X)));


d3:=[];
Append(d3, Elements(Subgroup(G, [X, Y^2*z])));
Append(d3, Elements(RightCoset(Subgroup(G, [X*Y^2, Y^2*z]),Y)));


d4:=[];
Append(d4, Elements(Subgroup(G, [X*Y, Y^2*z])));
Append(d4, Elements(RightCoset(Subgroup(G, [X*Y^3, Y^2*z]),Y)));


d5:= [];
Append(d5, Elements(Subgroup(G, [X, z])));
Append(d5, Elements(RightCoset(Subgroup(G, [X*Y^2, z]),Y)));

d6:=[];
Append(d6, Elements(Subgroup(G, [X^2, Y^2,z])));

d7:=[];
Append(d7, Elements(Subgroup(G, [Y, z])));
Append(d7, Elements(RightCoset(Subgroup(G, [X^2*Y, z]),X)));

d8:=[];
Append(d8, Elements(Subgroup(G, [X*Y,z])));
Append(d8, Elements(RightCoset(Subgroup(G, [X^3*Y, z]),X)));
```

Now that we have our blocks constructed, we are ready to assign coset representatives. Recall that `cosetReps` is a list containing the 8 coset representatives obtained by forming the factor group G/H and that `currentPerm` is a list that is a permutation of the integers 1 through 8. There are $8! = 40320$ possible permutations. To know when have exhausted them all, we use the variable `attempts` to keep track of how many of the permutations we have tried thus far. We begin by initializing `attempts` to 0. We now begin a `while` loop that continues iterating while the boolean variable `dsfound` is false. We then attach the coset representatives determined by the current permutation to each of our 8 blocks. To see how this is done, we will look at the first line of code `D1:= cosetReps[currentPerm[1]]*d1;` This simply takes the coset representative at position `currentPerm[1]` (the integer in the first position in the `currentPerm` list) and attaches it to

block d1. The constructions of D2 through D8 (the blocks d2 through d8 with coset representatives attached) are done in the same way. Blocks D2 through D8 are then appended to the list D1. By the end of the code below, the variable D1 contains all of the elements in the blocks with the permutation of coset representatives determined by the variable currentPerm.

```
attempts:=0;
while dsfound=false do
        D1:= cosetReps[currentPerm[1]]*D1;
        D2:= cosetReps[currentPerm[2]]*D2;
        D3:= cosetReps[currentPerm[3]]*D3;
        D4:=cosetReps[currentPerm[4]]*D4;
        D5:=cosetReps[currentPerm[5]]*D5;
        D6:=cosetReps[currentPerm[6]]*D6;
        D7:=cosetReps[currentPerm[7]]*D7;
        D8:=cosetReps[currentPerm[8]]*D8;

        Append(D1, D2);
        Append(D1, D3);
        Append(D1, D4);
        Append(D1, D5);
        Append(D1, D6);
        Append(D1, D7);
        Append(D1, D8);
```

Now, D1 contains a tentative difference set constructed by our construction method. It is possible that G is not abelian and consequently D1 is not necessarily a difference set. The purpose of the code below is to check whether or not the elements of D1 form a $(256, 120, 56)$ difference set in G. First, we set the variable groupElts equal to a list of elements of G. We initialize the variable count to a list of size 256 with the value of 0 at each position. The list is shown in abbreviated form. This list will be used to keep track of the number of times that each element in G appears in the set $DD^{(-1)}$, where here we are using the variable D1 to represent D. The two nested for loops iterate through the elements p of D1 and q of D1 and stores the value p^q(-1) in the variable current. We then determine the element of G to which p^q(-1) corresponds: we set the variable index equal to the position of the element in the list groupElts that current matches. We increment the count of that particular element by incrementing the integer at the corresponding position in the list count. Thus, at the end of the block of code below, the integer at position i in the list count corresponds

to the number of times that the ith element of G appears in the set $DD^{(-1)}$.

```
groupElts:=Elements(G);

count:=[0,...0];

for p in D1 do
        for q in D1 do
                current:= p*q^(-1);
                index:= Position(groupElts, current);
                count[index]:=count[index]+1;
        od;
od;
```

If $DD^{(-1)}$ is a difference set, each element of G will show up in $DD^{(-1)}$ precisely 56 times, excluding the identity element (in position 1 of the list G) which will appear $|D| = 120$ times. Thus, we will consider D1 a difference if the value 56 is stored at each position 2 through 256 of the list count after the code above is completed. The boolean variable DSCheck will be used to determine if the set D1 corresponds to a difference set and is initialized to true. The for loop below assigns the variable t to the integers 2 through 256 and if the value at position t of count is not 56 the boolean variable DSCheck is set to false, and we break out of the loop. This implies that using the permutation of cosetReps corresponding to currentPerm to attach coset representatives to our blocks does not result in a difference set. If after the for loop the value of DSCheck remains true, each nonidentity element of G showed up in $DD^{(-1)}$ precisely 56 times. Thus, we have a difference set. The purpose of the if statement is to set the boolean variable dsfound to true and add w, the index of the current group G to the list success when a difference set is found.

```
DSCheck:=true;
for t in [2..256] do
        if count[t]<>56 then
                DSCheck:=false;
                break;
        fi;
od;

if DSCheck=true then
        dsfound:=true;
```

```
Add(success, w);
fi;
```

If we exhaust all $8!$ permutations of our 8 coset representatives, then the current group `G` does not have a difference set using our construction method. If this is the case, we set the boolean variables `DSCheck` and `dsfound` both equal to true. The assignment `DSCheck = true` prevents the next permutation from being generated in the next block of code, while the assignment `dsfound = true` allows us to break out of the outer `for` loop that checks each possible assignment of coset representatives to the blocks of the current group. In this case, the index of `G` is not added to the list `success`.

```
if attempts>40318 then
        DSCheck:=true;
        dsfound:=true;
fi;
```

Now, as long as we have not exhausted all permutations of our coset representatives, we want to check if using the next permuation generated to assign coset representatives to our blocks results in a difference set. If the current permutation did not result in a difference set, the value of the variable `DSCheck` is false, and the body of the `if` statement below is executed. We first increment the variable `attempts`. The remainder of the body generates the subsequent permutation. We will not walk through the algorithm used to generate the next permutation since it is not relevent to our problem. However, permutations of the integers in `currentPerm` will be generated systematically from `[1, 2, 3, 4, 5, 6, 7, 8]` to `[8, 7, 6, 5, 4, 3, 2, 1]`. A smaller example illustrates the algorithm at work. The permutations of the elements in the list [1, 2, 3] are generated in the following order: `[ 1, 3, 2 ], [ 2, 1, 3 ], [ 2, 3, 1 ], [ 3, 1, 2 ], [ 3, 2, 1 ]`.

```
if DSCheck=false then
        attempts:=attempts+1;

        a:= 9;
        b:= a-2;
        while currentPerm[b]>currentPerm[b+1] do
```

```
                b:=b-1;
        od;

        c:= a-1;
         while currentPerm[b]>currentPerm[c] do
                c:=c-1;
        od;

        temp:= currentPerm[b];
        currentPerm[b]:=currentPerm[c];
        currentPerm[c]:=temp;

        d:= a-1;
        e:= b+1;

        while d>e do
                temp:= currentPerm[d];
                currentPerm[d]:=currentPerm[e];
                currentPerm[e]:=temp;
                d:=d-1;
                e:=e+1;
        od;
        fi;
od;

od;
```

At this point, the variable `success` contains the indices of the groups with difference sets produced by our construction method. The list is returned by the function.

```
return success;
end;
```

5 Results

Of the 649 groups that contained the normal $\mathbb{Z}_4^2 \times \mathbb{Z}_2$ normal subgroup, our GAP program generated difference sets in 643. (The indices corresponding to these groups are given in 6 Addendum.) Thus, we were able to produce difference sets in approximately 90% of the groups of order 256 where

the existence of a difference set was unknown.

We will look explicitly at the 6 groups of order 256 containing a $\mathbb{Z}_4^2 \times \mathbb{Z}_2$ normal subgroup for which our construction method did not produce difference sets. The indices of these groups are: 98, 99, 114, 115, 6453, 6528. Recall that for a non-Abelian group of order 256 with a the necessary normal subgroup, we had to assign coset representatives to the blocks D_1 through D_8 so that $\bigcup_{i=1}^{8} g_i B_i B_i^{(-1)} g_i^{-1} = 32H + m^2 e$. Thus, our results show that for the 6 groups whose indices are given above, we were not able to choose coset representatives that satisfy this property.

We speculated that we may be able to determine why we were unable to produce difference sets the 6 groups by looking more closely at their subgroup structure. Recall that all of the 649 groups whose indices were returned by the `NormalSubgroupCheck()` function have a normal $\mathbb{Z}_4^2 \times \mathbb{Z}_2$ subgroup. GAP stores elements in terms of the GAP generators of the group. However, GAP generators are not necessarily the same as the generators we would intuitively expect. Each group of order 256 has 8 generators, regardless of the group structure. For example, even the cyclic group of order 256, $\mathbb{Z}_{256}$, has 8 generators and not just the single generator typically seen in group theory. The generators of each group of order 256 are denoted `f1` through `f8`. For the 6 groups of interest, we printed the elements (in terms of the GAP generators) of the normal subgroup that was used by our program to build our 8 blocks. From now on we will say that two groups have identical normal subgroups if the elements of the subgroups are the same in terms of the GAP generators for that group. The groups corresponding to indices 98, 99, 114, and 115 had the following identical normal subgroups:

```
[ <identity> of ..., f5, f6, f7, f8, f3*f4, f5*f6, f5*f7, f5*f8, f6*f7, f6*f8,
 f7*f8, f3*f4*f5, f3*f4*f6, f3*f4*f7, f3*f4*f8, f5*f6*f7, f5*f6*f8, f5*f7*f8,
f6*f7*f8, f3*f4*f5*f6, f3*f4*f5*f7, f3*f4*f5*f8, f3*f4*f6*f7, f3*f4*f6*f8,
f3*f4*f7*f8, f5*f6*f7*f8, f3*f4*f5*f6*f7, f3*f4*f5*f6*f8, f3*f4*f5*f7*f8,
f3*f4*f6*f7*f8, f3*f4*f5*f6*f7*f8 ]
```

We will call this particular normal subgroup N_1. The groups corresponding to indices 6453 and 6528 had the following identical normal subgroup:

```
[ <identity> of ..., f4, f5, f7, f8, f1*f6, f4*f5, f4*f7, f4*f8, f5*f7, f5*f8,
f7*f8, f1*f4*f6, f1*f5*f6, f1*f6*f7, f1*f6*f8, f4*f5*f7, f4*f5*f8, f4*f7*f8,
 f5*f7*f8, f1*f4*f5*f6, f1*f4*f6*f7, f1*f4*f6*f8, f1*f5*f6*f7, f1*f5*f6*f8,
f1*f6*f7*f8, f4*f5*f7*f8, f1*f4*f5*f6*f7, f1*f4*f5*f6*f8, f1*f4*f6*f7*f8,
f1*f5*f6*f7*f8, f1*f4*f5*f6*f7*f8 ]
```

We will call this particular normal subgroup N_2.

We looked at the structure in terms of GAP generators of the 643 groups in which our construction method successfully found difference sets. Difference sets were successfully built out of the N_1 normal subgroup for two of the groups (corresponding to indices 108 and 109). The normal subgroup N_2 was not used to build difference sets in any of the groups.

Since N_2 was not used for any successful difference set construction, there may be something intrinscially different about the normal subgroup in the way that it interacts with other group elements so that the property $\bigcup_{i=1}^{8} g_i B_i B_i^{(-1)} g_i^{-1} = 32H + m^2 e$ cannot be satisfied. Out of all of the distinct (containing different elements in terms of GAP group generators) normal subgroups used to successfully build difference sets for the 643 groups, N_1 showed up the fewest number of times. Thus, it may be the case that our desired property is difficult to satisfy based on the structure of N_1. Since we are not sure how the GAP generators are determined, it is difficult to form any further hypotheses based on these observations.

These observations give rise to possible extensions of this work. Our hypothesis that some permutation of coset representatives attached to our blocks from the $(16, 8, 8, -)$ covering EBS did not give any indication of how to choose the correct permutation. This gave rise to the brute force approach implemented in GAP of exhaustively attaching each permuation of coset representatives to our blocks until a difference set was found. Since our construction method did not produce difference sets for all 649 groups, it is clear that our construction method of a difference set in a group G of order 256 requires a stronger condition than that G contains a $\mathbb{Z}_4^2 \times \mathbb{Z}_2$ normal subgroup. We may be able to determine what this condition is by closely examining the 6 groups for which our construction method did not produce difference sets. Our final observation that these 6 groups contained "different" normal subgroups in terms of GAP generators may be a feasible initial

approach to this problem.

6 Addendum

The following is a list of the indices of the 643 groups for which our construction method produced a difference set:

```
2, 3, 6, 7, 10, 11, 15, 18, 19, 28, 29, 30, 31, 36, 37, 38, 44, 48, 50, 51, 53, 54,
68, 69, 70, 71, 76, 77, 79, 90, 93, 94, 95, 96, 97, 100, 103, 104, 105, 106, 107, 108,
109, 112, 113, 118, 123, 135, 152, 154, 185, 186, 194, 199, 200, 207, 208, 211, 212,
226, 232, 233, 234, 236, 272, 274, 277, 279, 281, 283, 285, 286, 288, 291, 311, 340,
341, 342, 343, 344, 345, 346, 347, 350, 354, 355, 356, 357, 358, 359, 360, 361, 362,
364, 392, 393, 401, 403, 404, 405, 417, 424, 425, 428, 429, 556, 573, 590, 607, 624,
638, 645, 648, 651, 654, 660, 665, 668, 671, 674, 680, 685, 688, 691, 694, 700, 705,
708, 711, 714, 720, 727, 728, 732, 780, 781, 786, 787, 791, 796, 803, 815, 816, 820,
1119, 1120, 1121, 1122, 1123, 1124, 1754, 1755, 1756, 1757, 1762, 1763, 1772, 1773,
1774, 1775, 1776, 1777, 1786, 1787, 1788, 1789, 1790, 2521, 2522, 2523, 2524, 2525,
2526, 2527, 2528, 2854, 2855, 2859, 2860, 2863, 2864, 2879, 2880, 2881, 2882, 2885,
2887, 2888, 2889, 2890, 2892, 2894, 2895, 3339, 3342, 3348, 3564, 3565, 3566, 3567,
3568, 3569, 3570, 3573, 3574, 3603, 3604, 3607, 3609, 3610, 3613, 3637, 3638, 3639,
3640, 3641, 3642, 3643, 3644, 3645, 3646, 3659, 3660, 3661, 3665, 3666, 3671, 3675,
3676, 3677, 4402, 4555, 4559, 4728, 4769, 4823, 4870, 5008, 5009, 5013, 5017, 5019,
5022, 5024, 5879, 5880, 5882, 5883, 5884, 5885, 6097, 6100, 6101, 6118, 6291, 6468,
6470, 6493, 6514, 6525, 6526, 6527, 6529, 6530, 6531, 6627, 6628, 14660, 14661, 14662,
14663, 14664, 14665, 14666, 14667, 15287, 15288, 15289, 15290, 15291, 15292, 15293,
15294, 15361, 15362, 15363, 15364, 15365, 15366, 15367, 15368, 15369, 15370, 15371,
15372, 16241, 16242, 16243, 16244, 16245, 16246, 16247, 16248, 16249, 16250, 16251,
16252, 16253, 16254, 16255, 16256, 16357, 16358, 16359, 16360, 16361, 16362, 16824,
16828, 16831, 19445, 19447, 19502, 19503, 19504, 19505, 19510, 19511, 19512, 19513,
19852, 19853, 19854, 19855, 19856, 19857, 19858, 19859, 19868, 19869, 19870, 19871,
19872, 19873, 19874, 19875, 20123, 20124, 20127, 20128, 20138, 20141, 20142, 20145,
20978, 20979, 20980, 20981, 20982, 20983, 20984, 20985, 20986, 20987, 20988, 20989,
20990, 20991, 20992, 20993, 20994, 20995, 20996, 20997, 21001, 21002, 21005, 21009,
21010, 21017, 21019, 21020, 21022, 21025, 21026, 21029, 21031, 21032, 21034, 21037,
21039, 21040, 21043, 21044, 21046, 21049, 21778, 21780, 21786, 21788, 21793, 21795,
21815, 21816, 21817, 21818, 21819, 21820, 21821, 21822, 21823, 21824, 21825, 21826,
21827, 21828, 22168, 22171, 22172, 22173, 22174, 22176, 22198, 22202, 22209, 22215,
22218, 22219, 22267, 22273, 22279, 22282, 22283, 22302, 22304, 22306, 22309, 22312,
22314, 22315, 22348, 22504, 22511, 22517, 22518, 23059, 23085, 23086, 23087, 23091,
23092, 23141, 23142, 23149, 23151, 23206, 23212, 23219, 23223, 23295, 23296, 23299,
23300, 23337, 23364, 23367, 23369, 23371, 23372, 23374, 23377, 23378, 23380, 23383,
```

```
25127, 25129, 25131, 25133, 25143, 25145, 25147, 25149, 25225, 25229, 25241, 25245,
25298, 25299, 25300, 25301, 25302, 25303, 25304, 25305, 25306, 25307, 25308, 25309,
25310, 25311, 25312, 25313, 25314, 25315, 25316, 25317, 25318, 25319, 25320, 25321,
25322, 25323, 25324, 25325, 25326, 25327, 25328, 25329, 25362, 25363, 25366, 25367,
25372, 25373, 25376, 25377, 25378, 25379, 25382, 25383, 25388, 25389, 25392, 25393,
25460, 25461, 25462, 25463, 25472, 25473, 25474, 25475, 25476, 25477, 25478, 25479,
25488, 25489, 25490, 25491, 25492, 25493, 25494, 25495, 25496, 25497, 25498, 25499,
25500, 25501, 25502, 25503, 25504, 25505, 25506, 25507, 25508, 25509, 25510, 25511,
25512, 25517, 25521, 25524, 25525, 25529, 25784, 25802, 25815, 25819, 25824, 25829,
25836, 25837, 25838, 25839, 25840, 25841, 25842, 25843, 25844, 25845, 25846, 25847,
25852, 25855, 26244, 26245, 26246, 26247, 26248, 26249, 26250, 26251, 26252, 26254,
26257, 26260, 26263, 26272, 26279, 26283, 26287, 29689, 30601, 34774, 35277, 36732,
37660, 37725, 38211, 39141, 39145, 39148, 39163, 39169, 39179, 39230, 39912, 40328,
43419, 44299, 45293, 45984, 46024, 46109, 46119, 46144, 46145, 46722, 51465, 51483,
51711
```

The following 6 indices correspond to groups with a normal subgroup isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2$ for which our construction method was unable to produce a difference set:

```
98, 99, 114, 115, 6453, 6528
```

The following 81 indices correspond to the remaining open cases (including the 6 groups with the normal subgroup isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2$ for which we were unable to produce a difference set). The structure description given by GAP of the corresponding group is also provided.

```
98:  ((C8 x C2) :  C8) :  C2
99:  (C2 x Q16) :  C8
114:  (C8 :  C4) :  C8
115:  (C8 :  C4) :  C8
321:  C32 :  C8
323:  ((C32 x C2) :  C2) :  C2
351:  (C8 x C2) .  ((C4 x C2) :  C2) = (C4 x C2) .  (C16 x C2)
353:  C8 .  (((C4 x C2) :  C2) :  C2) = (C2 x C2 x C2) .  (C16 x C2)
367:  (C32 x C4) :  C2
368:  (C32 :  C4) :  C2
369:  (C32 x C4) :  C2
370:  (C16 .  D8 = C4 .  (C16 x C2)) :  C2
372:  Q32 :  C8
373:  (C16 :  C8) :  C2
374:  Q32 :  C8
375:  (C32 x C4) :  C2
376:  (C32 :  C4) :  C2
```

```
379:  C2 .  ((C16 :  C4) :  C2) = C16 .  (C8 x C2)
380:  Q8 :  C32
381:  (C8 x C2) .  ((C4 x C2) :  C2) = (C4 x C2) .  (C16 x C2)
408:  ((C32 x C2) :  C2) :  C2
409:  (C2 x C2) .  ((C16 x C2) :  C2) = (C16 x C2) .  (C4 x C2)
433:  (C2 x C2) .  ((C16 x C2) :  C2) = (C16 x C2) .  (C4 x C2)
434:  (C4 :  C32) :  C2
435:  (C8 .  D16 = C8 .  (C8 x C2)) :  C2
436:  (C16 .  D8 = C4 .  (C16 x C2)) :  C2
437:  C2 .  ((C4 :  C16) :  C2) = (C16 x C2) .  (C4 x C2)
439:  (C2 x C2) .  ((C16 x C2) :  C2) = (C16 x C2) .  (C4 x C2)
440:  (C2 x C2) .  ((C16 x C2) :  C2) = (C16 x C2) .  (C4 x C2)
442 :  C2 .  ((C2 x C2) .  ((C8 x C2) :  C2) = (C8 x C2) .  (C4 x C2)) = (C16 x C2)
.   (C4 x C2)
445:  C32 :  C8
449:  C32 :  C8
450:  C8 .  D32 = C16 .  (C8 x C2)
451:  C32 :  C8
452:  C4 .  (C16 :  C4) = C16 .  (C8 x C2)
501:  (C64 :  C2) :  C2
509:  (C2 .  ((((C4 x C2) :  C2) :  C2) :  C2) = (C4 x C4) .  (C4 x C2)) :  C2
514:  C2 .  (((C8 :  C4) :  C2) :  C2) = ((C2 x C2) .  (C2 x C2 x C2)) .  (C4 x C2)
522:  C2 .  ((C8 x C4) :  C4) = (C8 x C4) .  (C4 x C2)
532:  C32 .  D8 = C4 .  (C32 x C2)
536:  C64 :  C4
5331:  ((C16 x C4) :  C2) :  C2
5421:  ((C4 :  C16) :  C2) :  C2
5422:  ((C2 x C2) .  ((C8 x C2) :  C2) = (C8 x C2) .  (C4 x C2)) :  C2
5423:  ((C2 x C2) .  ((C8 x C2) :  C2) = (C8 x C2) .  (C4 x C2)) :  C2
5427:  (C16 x Q8) :  C2
5430:  ((C4 :  C16) :  C2) :  C2
6453 :  (C2 x C2) .  ((((C4 x C2) :  C2) :  C2) :  C2) = (C2 x C2 x Q8) .  (C2 x C2
x C2 )
6528:  C4 .  ((C8 x C4) :  C2) = (C8 x C2 x C2) .  (C2 x C2 x C2)
6532:  C4 .  ((C8 :  C4) :  C2) = (C8 x C2 x C2) .  (C2 x C2 x C2)
6533 :  C2 .  ((C2 x C2 x C2) .  (C2 x D8) = (C4 x C2 x C2) .  (C2 x C2 x C2)) = (C8
x C2 x C2) .  (C2 x C2 x C2)
6620:  C2 x (C32 :  C4)
6629:  (C32 x C4) :  C2
6631:  (C16 .  D8 = C4 .  (C16 x C2)) :  C2
6639:  C4 x Q64
6641:  Q64 :  C4
6642:  (C4 x D32) :  C2
6647:  C32 x Q8
6648:  C32 :  Q8
```

```
6674:  (C2 x QD64) :  C2
6676:  C4 :  Q64
6678:  (C2 x Q64) :  C2
6693:  (C32 :  C4) :  C2
6696:  (C2 x C2) .  (C2 x D32) = (C16 x C2) .  (C2 x C2 x C2)
6700:  (C2 x (C16 :  C4)) :  C2
6701:  ((C32 x C2) :  C2) :  C2
6704:  (C32 :  C4) :  C2
6709:  (C32 x C4) :  C2
6711:  (C32 :  C4) :  C2
6712:  (C2 x C2) .  (C2 x D32) = (C16 x C2) .  (C2 x C2 x C2)
6714:  C4 :  Q64
6715:  (C32 x C4) :  C2
6716:  (C32 x C4) :  C2
6717:  (C2 x QD64) :  C2
6718:  (C2 x Q64) :  C2
6720:  (C2 x C2) .  (C2 x D32) = (C16 x C2) .  (C2 x C2 x C2)
6721:  C32 :  Q8
6724:  C2 x (C64 :  C2)
23224:  (C2 .  ((C2 x (C4 :  C4)) :  C2) = (C4 x C2 x C2) .  (C2 x C2 x C2)) :  C2
23225:  (((C8 x C2) :  C4) :  C2) :  C2
```

References

[1] J.A. Davis, J. Jedwab, A unifying construction for difference sets, *J. Combin. Theory Ser. A* **13** (1997), 80-1.

[2] J.F. Dillion, Variations on a scheme of McFarland for noncylic difference sets, *J. Combin. Theory Ser. A* **40** (1985), 9-21.

[3] J.F. Dillon, Personal correspondence.

[4] R. L. McFarland, A family of difference sets in non-cyclic groups, *J. Combin. Theory Ser. A* **15** (1973), 1-10.