

DETERMINING EXISTENCE OF HADAMARD DIFFERENCE SETS IN GROUPS OF ORDER 144

NICOLE KROEGER, NORTH CAROLINA STATE UNIVERSITY
MARCUS MILLER, HARVARD UNIVERSITY
CHRIS MOONEY, TRANSYLVANIA UNIVERSITY
KATHLEEN SHEPARD, GRINNELL COLLEGE
KEN W. SMITH, CENTRAL MICHIGAN UNIVERSITY

ABSTRACT

Finding difference sets and classifying them for all finite groups is a major project of combinatorics. We present the results of our investigation into $(144, 66, 30)$ difference sets and also a powerful new construction that allowed us to classify 37 unresolved cases. This *spread* construction is, roughly, a generalization of the more common product constructions. Out of 197 groups of order 144, we were able to determine existence in 170 of them. If we assume a famous conjecture by Eric Lander stating that a group with a cyclic Sylow-3 subgroup has no difference set, then only 1 group of order 144 remains.

Acknowledgment. This project was supported by NSF-REU grant 05-52594.

CONTENTS

1. INTRODUCTION

1.1. What is a Difference Set. A (v, k, λ) difference set \mathcal{D} is a k -subset of a group G with $|G| = v$, such that the collection of products $d_1 d_2^{-1}$, for $d_1, d_2 \in \mathcal{D}$, contains exactly λ copies of all non-identity elements of G . If we consider the group algebra

$$\mathbb{C}[G] = \left\{ \sum_{g \in G} \alpha_g g \mid \alpha_g \in \mathbb{C} \right\}$$

we may think of the group G as the formal sum of group elements. The difference set then becomes the formal sum of elements in the difference set.

While considering the group algebra seems like a simple change in notation, the shift from group to the group algebra allows us to make some key observations. First, we may redefine a difference set in a more natural way. If $\mathcal{D} = (g_0 + g_1 + \cdots + g_k)$, lets define $\mathcal{D}^{(-1)} = (g_0^{-1} + g_1^{-1} + \cdots + g_k^{-1})$. Taking the product $\mathcal{D}\mathcal{D}^{(-1)}$ we get

$$\begin{aligned} \mathcal{D}\mathcal{D}^{(-1)} &= (g_0 + g_1 + \cdots + g_k)(g_0^{-1} + g_1^{-1} + \cdots + g_k^{-1}) \\ &= (k - \lambda) + \lambda(G). \end{aligned}$$

Using this equation, we can prove some important properties of difference sets.

Proposition 1.1. *If \mathcal{D} is a difference set in G and $g \in G$ then $g\mathcal{D}$ is a difference set.*

Proof. Let \mathcal{D} be a difference set then

$$\mathcal{D}\mathcal{D}^{(-1)} = (k - \lambda) + \lambda(G)$$

We want $g\mathcal{D}$ to be a difference set.

$$g\mathcal{D}(g\mathcal{D})^{(-1)} = (gg_0 + gg_1 + \cdots + gg_k)(g_0^{-1}g^{-1} + g_1^{-1}g^{-1} + \cdots + g_k^{-1}g^{-1})$$

For k products $(gg_i)(g_i^{-1}g)$ we get the identity. We may write the products $(gg_i)(g_k^{-1}g^{-1}) = g(g_i g_k^{-1})g^{-1}$. The products $(g_i g_k^{-1})$ produce each group element λ times, and each of these products is conjugated by g . Thus,

$$g\mathcal{D}(g\mathcal{D})^{(-1)} = (k - \lambda) + \lambda(G).$$

□

Proposition 1.2. *If \mathcal{D} is a difference set in G and σ is an algebra automorphism on $\mathbb{C}[G]$ then $\sigma\mathcal{D}$ is a difference set.*

Proof. Let \mathcal{D} be a difference set then

$$\mathcal{D}\mathcal{D}^{(-1)} = (k - \lambda) + \lambda(G)$$

We want $\sigma\mathcal{D}$ to be a difference set.

$$\sigma\mathcal{D}(\sigma\mathcal{D})^{(-1)} = \sigma(\mathcal{D}\mathcal{D}^{-1}) = \sigma((k - \lambda) + \lambda(G)) = \sigma(k - \lambda) + \lambda\sigma(G) = (k - \lambda) + \lambda(G)$$

□

1.2. Group Representations and Idempotents. It is necessary to develop a method of finding difference sets. One could search for subsets of a group and naïvely multiply the elements to see if they form difference sets, however, it is easy to see that this process becomes absurd as groups become larger. Instead, it is useful to employ some representation theory to make the process easier.

A group representation is a group homomorphism

$$\rho : G \rightarrow \text{Aut}(\mathbb{C}^m) \simeq GL_m(\mathbb{C})$$

We define the degree of a representation as the dimension of the vector space on which the image of ρ acts, or equivalently, $\deg(\rho) = m$. If G is abelian, then we only need to consider the case $m = 1$. We may define another map

$$\chi : G \rightarrow \mathbb{C}$$

$$\chi : g \rightarrow \text{tr}(\rho(g))$$

called the character. *In the case that G is abelian*, we may think of the character map and the representation map as equivalent. For an abelian group, the number of group elements is equal to the number of irreducible characters.

We use representation theory for our analysis in two ways. The first application is to develop idempotents in $\mathbb{C}[G]$, which are indispensable to the analysis of difference sets in abelian groups. An idempotent is an element e in any set with a multiplication such that $e^2 = e$. In $\mathbb{C}[G]$, we define an idempotent $e_{\chi_b} = e_b$ as

$$e_b = \frac{1}{|G|} \sum_{g \in G} \overline{\chi_b(g)} g$$

We may verify that this is an idempotent

$$\begin{aligned} e_b^2 &= e_b e_b = \left(\frac{1}{|G|} \sum_{g \in G} \overline{\chi_b(g)} g \right) \left(\frac{1}{|G|} \sum_{g \in G} \overline{\chi_b(g)} g \right) = \\ &= \frac{1}{|G|^2} \sum_{g \in G} |G| \overline{\chi_b(g)} g = \frac{1}{|G|} \sum_{g \in G} \overline{\chi_b(g)} g \\ &= e_b \end{aligned}$$

Lemma 1.1. *For G abelian, $e_i e_j = e_i \delta_i = e_j \delta_j$*

Proof.

$$\begin{aligned} e_i e_j &= \left(\frac{1}{|G|} \sum_{g \in G} \overline{\chi_i(g)} g \right) \left(\frac{1}{|G|} \sum_{g \in G} \overline{\chi_j(g)} g \right) = \frac{1}{n^2} \sum_{g \in G} |G| \overline{\chi_{i,j}(g)} g = \\ &= \frac{1}{|G|} \sum_{g \in G} (1 + \zeta + \zeta^2 + \dots + \zeta^{|G|-1}) g = 0 \end{aligned}$$

Where we use the result that the product of characters is a character and ζ is some n th root of unity such that divides n the order of the group. \square

Theorem 1.2. *For G abelian, the set of idempotents is a linearly independent set.*

Proof. Suppose

$$a_0 e_0 + a_1 e_1 + \dots + a_{n-1} e_{n-1} = 0$$

Then

$$\begin{aligned} e_i (a_0 e_0 + a_1 e_1 + \dots + a_{|G|-1} e_{|G|-1}) &= a_i e_i = 0 \\ \Rightarrow a_i &= 0. \end{aligned}$$

\square

Idempotents are defined on the characters. We know from earlier that in an abelian group G with order n , there are n characters. Thus we have that the set of idempotents is an independent set of cardinality n . This is equivalent to saying that the set of idempotents forms a basis for the group algebra $\mathbb{C}[G]$ (for G abelian). By changing the basis, we change the question of finding difference sets into a question of linear algebra: Find linear combinations of idempotents that sum to a difference set.

The second function of representation theory is applying the character or representation map to our definition of difference set in the group algebra. If G is an abelian group, then

$$\begin{aligned} \chi(\mathcal{D}\mathcal{D}^{-1}) &= \chi((k - \lambda) + \lambda(G)) \\ \chi\mathcal{D}\chi\mathcal{D}^{-1} &= \chi(k - \lambda) + \lambda\chi(G) \\ z\bar{z} &= (k - \lambda) \end{aligned}$$

Where z is a complex number and $\chi(G) = \rho(G)$ vanishes because, for a fixed ρ ,

$$\sum_{g \in G} \rho g = 0$$

We call an element α in the group ring an alias if $\chi(\alpha) = z$. Aliases serve as coefficients for the idempotents, so this process further narrows down our search for appropriate linear combinations.

For G non-abelian

$$\rho((\mathcal{D}\mathcal{D}^{-1}) = \rho((k - \lambda) + \lambda(G)) =$$

$$\rho(\mathcal{D})\rho(\mathcal{D}^{-1}) = \rho(k - \lambda) + \lambda\rho(G) =$$

$$AA^* = (k - \lambda)I$$

Where A is a complex matrix and A^* is its conjugate transpose.

In G abelian, we may pare down this problem further by reducing the number of idempotents we have to consider. Lets consider $\chi(g) = \zeta_n$, a primitive n th root of unity. If σ is an automorphism, then $\chi(\sigma(g)) = \zeta_n^k$ where ζ_n^k is some primitive n th root of unity. As it turns out, the set of irreducible characters forms a dual group G^* of G such that $G \simeq G^*$. Thus if we consider the isomorphism

$$\varphi : Aut(G) \rightarrow Aut(G^*)$$

we may consider an automorphism σ on G as isomorphic to an automorphism σ^* on G^* . Basically this all means that there is an automorphism

$$\sigma^*(\chi)(g) = \chi(\sigma(g)) = \zeta_n^k$$

Extending these group automorphisms to algebra automorphisms, we may investigate what the automorphisms do to our idempotents.

$$\sigma^*(e_b) = \frac{1}{|G|} \sum_{g \in G} \sigma^*(\overline{\chi_b})(g)g = \frac{1}{|G|} \sum_{g \in G} \overline{(\chi_k)}(g)g = e_k$$

Since these automorphisms permute the images of χ , we see that they can be thought of as field automorphisms of the base field of our group ring $\mathbb{Q}[\zeta_n]$. Galois theory tells us that any element invariant under the group of these automorphisms is an element of the fixed field, which in our case is, \mathbb{Q} . If we sum the idempotents defined on a set K of χ_i such that for all σ^* , $\sigma^*(\chi_i) \in K$, then we will have such an element. Alternatively, we may say that the sum of idempotents algebraically conjugate to one another is fixed under all automorphisms of $\mathbb{Q}[\zeta_n] \Rightarrow$ its coefficients are in the fixed field \mathbb{Q} . It can be shown that the characters with the same kernels will be algebraically conjugate.

By taking these sums, we construct the rational idempotents. Rational idempotents simplify the project even further in two ways. First, they cut down the number of idempotents we have to deal with, since many of them will be summed together. Second, we rid ourselves of complex numbers in our idempotents and allow ourselves to work with computationally convenient rational numbers.

2. SELECTING A PARAMETER SET

When trying to select a parameter set for which to investigate, there were several things that we wanted to take into consideration. First, the parameter sets had to satisfy the equation:

$$\lambda(v - 1) = k(k - 1)$$

Then the parameter set had to meet the Bruck-Ryser-Chowla condition. On top of these basic conditions we were looking for a parameter set that was especially nice where we had (v, k, λ) such that:

- (1) The parameter set has not been exhausted by others already.
- (2) It is manageable to make substantial progress on it in the course of eight weeks
- (3) We want $k - \lambda = m^2$ such that $m \in \mathbb{N}$ so factoring for magnitudes of aliases gave us an easy factoring (m) .

2.1. On Hadamard Difference Sets. We settled on a special group of difference set parameters, the so called Hadamard parameters. These are parameters of the form

$$(4m^2, 2m^2 - m, m^2 - m)$$

Simple algebra shows that these Hadamard parameter sets do indeed meet the desired characteristics that we hoped to show:

$$\lambda(v - 1) = k(k - 1)$$

$$(m^2 - m)(4m^2 - 1) = (2m^2 - m)(2m^2 - m - 1)$$

$$m(m - 1)(2m - 1)(2m + 1) = m(2m - 1)(m - 1)(2m + 1)$$

Also it is evident that $k - \lambda$ is a perfect square:

$$k - \lambda = (2m^2 - m) - (m^2 - m) = 2m^2 - m - m^2 + m = m^2$$

2.2. The Appeal of (144, 66, 30). Hadamard difference sets allow us to use the useful Hadamard transform: $\hat{D} = G - 2D$. Also, Hadamard difference sets have been found by computer up to $m = 5$, but for $m \geq 6$ these same approaches become computationally infeasible, so this is a natural starting place.

Another major appeal of this particular parameter set was the fact that all the difference sets in groups of order 36 had been found which would allow us to construct a lot of difference sets in groups of order 144.

3. METHODS

3.1. (40,13,4) Difference Set. Before beginning the process of classifying (144,66,30) difference sets, we look at the smaller case of (40,13,4) in order to explain some methods we will use in the larger group. This difference set is not a new solution; however, we use new methods to find the difference set. We find a difference set in C_{40} using idempotents and aliases.

3.1.1. *Rational Idempotents.* In C_{40} , the rational idempotents are:

$$\begin{aligned}
[e_{\chi_0}] &= \frac{1}{40} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \\
[e_{\chi_{20}}] &= \frac{1}{40} \begin{bmatrix} 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \end{bmatrix} \\
[e_{\chi_{10}}] &= \frac{1}{40} \begin{bmatrix} 2 & 0 & -2 & 0 & 2 & 0 & -2 & 0 \\ 2 & 0 & -2 & 0 & 2 & 0 & -2 & 0 \\ 2 & 0 & -2 & 0 & 2 & 0 & -2 & 0 \\ 2 & 0 & -2 & 0 & 2 & 0 & -2 & 0 \\ 2 & 0 & -2 & 0 & 2 & 0 & -2 & 0 \end{bmatrix} \\
[e_{\chi_5}] &= \frac{1}{40} \begin{bmatrix} 4 & 0 & 0 & 0 & -4 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & -4 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & -4 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & -4 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & -4 & 0 & 0 & 0 \end{bmatrix} \\
[e_{\chi_8}] &= \frac{1}{40} \begin{bmatrix} 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \end{bmatrix} \\
[e_{\chi_4}] &= \frac{1}{40} \begin{bmatrix} 4 & -4 & 4 & -4 & 4 & -4 & 4 & -4 \\ -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \end{bmatrix} \\
[e_{\chi_2}] &= \frac{1}{40} \begin{bmatrix} 8 & 0 & -8 & 0 & 8 & 0 & -8 & 0 \\ -2 & 0 & 2 & 0 & -2 & 0 & 2 & 0 \\ -2 & 0 & 2 & 0 & -2 & 0 & 2 & 0 \\ -2 & 0 & 2 & 0 & -2 & 0 & 2 & 0 \\ -2 & 0 & 2 & 0 & -2 & 0 & 2 & 0 \end{bmatrix} \\
[e_{\chi_1}] &= \frac{1}{40} \begin{bmatrix} 16 & 0 & 0 & 0 & -16 & 0 & 0 & 0 \\ -4 & 0 & 0 & 0 & 4 & 0 & 0 & 0 \\ -4 & 0 & 0 & 0 & 4 & 0 & 0 & 0 \\ -4 & 0 & 0 & 0 & 4 & 0 & 0 & 0 \\ -4 & 0 & 0 & 0 & 4 & 0 & 0 & 0 \end{bmatrix}
\end{aligned}$$

3.1.2. *Factoring.* For this difference set, we want to factor: $z\bar{z} = k - \lambda = 13 - 4 = 9 = 3 \cdot 3$. However, 3 is prime in all rings that we are dealing with except $\mathbb{Z}[\zeta_{40}]$, $\mathbb{Z}[\zeta_{20}]$, $\mathbb{Z}[\zeta_8]$. These rings correspond to the the idempotents $[e_1], [e_2], [e_5]$.

In these rings, we get the following factoring of 3:

$$\text{In } \mathbb{Z}[\zeta_8]: (1 - \zeta_8 - \zeta_8^3)(1 + \zeta_8 + \zeta_8^3)$$

In $\mathbb{Z}[\zeta_{20}]: (1 + \zeta_{20} + \zeta_{20}^4 + \zeta_{20}^{13})(1 + \zeta_{20}^{19} + \zeta_{20}^{16} + \zeta_{20}^7)$

In $\mathbb{Z}[\zeta_{40}]: 3$ factors into 4 pieces, but we avoid using these factorings.

3.1.3. *Aliases.* Due to the factoring in these rings, we get the following possible aliases for each idempotent:

$[e_{\chi_0}]$	13	where $g \in C_{40}$.
$[e_{\chi_{20}}]$	$3g$	
$[e_{\chi_{10}}]$	$3g$	
$[e_{\chi_5}]$	$3g$ $-1 - 2x - 2x^3$ $-1 + 2x + 2x^3$	
$[e_{\chi_8}]$	$3g$	
$[e_{\chi_4}]$	$3g$	
$[e_{\chi_2}]$	$3g,$ $1 + 2x^5 + 2x^8 + 2x^{12}$ $1 + 2x^8 + 2x^{12} + 2x^{15}$	
$[e_{\chi_1}]$???	

3.1.4. *Homomorphic Images.* In order to simplify our alias-idempotent combinations, we look at different homomorphic images of our idempotents. These images give us information about what aliases must be used and about what idempotents must add together. Looking at homomorphic images also allows us to eliminate factoring in $\mathbb{Z}[\zeta_{40}]$

C_8 image To obtain the C_8 image, we use the mapping: $x^8 \rightarrow 1$. In terms of our idempotents from C_{40} , this means that all the rows are added together. Therefore, we were left with the following idempotents:

$$\begin{aligned}
 [e_{\chi_0}] &= \frac{1}{8} [1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1] \\
 [e_{\chi_{20}}] &= \frac{1}{8} [1 \ -1 \ 1 \ -1 \ 1 \ -1 \ 1 \ -1] \\
 [e_{\chi_{10}}] &= \frac{1}{8} [2 \ 0 \ -2 \ 0 \ 2 \ 0 \ -2 \ 0] \\
 [e_{\chi_5}] &= \frac{1}{8} [4 \ 0 \ 0 \ 0 \ -4 \ 0 \ 0 \ 0]
 \end{aligned}$$

Note that $[e_{\chi_5}]$ is the only idempotent that has an alias other than some shift of 3. Looking at all possible alias idempotent combinations, we determine that the only possible difference set image in this set is:

$$\begin{aligned}
 13[e_{\chi_0}] + 3x[e_{\chi_{20}}] + 3x^2[e_{\chi_{10}}] + (-1 - 2x - x^2)[e_{\chi_5}] = \\
 [\ 0 \ 1 \ 2 \ 1 \ 1 \ 3 \ 2 \ 3]
 \end{aligned}$$

3.1.5. *Information from Other Images.* In addition to the C_8 image, we also consider the C_5 , C_{10} , and C_{20} images of a (40,13,4) difference set. Each of these images gives us new information about the structure of the difference set. From these homomorphic images, we get the following information about a (40, 13, 4) difference set:

0	1	0	1	1	1	0	1	5
0	0	*	0	0	0	*	1	2
0	0	*	0	0	1	*	0	2
0	0	*	0	0	1	*	0	2
0	0	*	0	0	0	*	1	2
0	1	2	1	1	3	2	3	

In this array, the last row gives the row sum and was found from the C_8 image; the last column is the column sum which comes from the C_5 image; the bold numbers

come from the C_{20} image. The spots with * are the elements that we did not know. In order to determine if these elements were included in the difference set, we used all possible combinations and checked to see if they were a difference set or not.

3.1.6. *Difference Set.* The difference set that we found in this group with (40,13,4) parameters is:

$$x^5+x^{13}+x^{15}+x^{20}+x^{22}+x^{25}+x^{26}+x^{31}+x^{34}+x^{35}+x^{37}+x^{38}+x^{39}$$

3.2. **Nonexistence of a C_{16} Image.** Using idempotents, we show that a (144, 66, 30) difference set cannot have a C_{16} homomorphic image. This conclusion allows us to determine the nonexistence of difference sets in 18 groups of order 144.

3.2.1. *Rational Idempotents of C_{16} .* Rational Idempotents of C_{16} :

$$\begin{aligned} [e_{\chi_0}] &= \frac{1}{16} [1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1] \\ [e_{\chi_9}] &= \frac{1}{16} [8 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ -8 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0] \\ [e_{\chi_{18}}] &= \frac{1}{16} [4 \ 0 \ 0 \ 0 \ -4 \ 0 \ 0 \ 0 \ 4 \ 0 \ 0 \ 0 \ -4 \ 0 \ 0 \ 0] \\ [e_{\chi_{36}}] &= \frac{1}{16} [2 \ 0 \ -2 \ 0 \ 2 \ 0 \ -2 \ 0 \ 2 \ 0 \ -2 \ 0 \ 2 \ 0 \ -2 \ 0] \\ [e_{\chi_{72}}] &= \frac{1}{16} [1 \ -1 \ 1 \ -1 \ 1 \ -1 \ 1 \ -1 \ 1 \ -1 \ 1 \ -1 \ 1 \ -1 \ 1 \ -1] \end{aligned}$$

3.2.2. *Aliases.* Since we are using a Hadamard transform, we are trying to factor $z\bar{z} = 144 = 12^2 = (2^2 * 4)^2$. Therefore, the aliases for our idempotents will be some factoring of 12. In the different rings that we are interested in, 2 and 3 are prime except in $\mathbb{Z}[\zeta_{16}]$ and $\mathbb{Z}[\zeta_8]$. In both of these rings, 2 is prime, but 3 factors as: $(1 + \zeta_8 + \zeta_8^3)^2$ or $(1 - \zeta_8 - \zeta_8^3)^2$ from this information, we get the following possible aliases:

For $[e_{\chi_9}]$: $12g$, $-4 + 8x^2 + 8x^6$ or $-4 - 8x^2 - 8x^6$

For $[e_{\chi_{18}}]$: $12g$, $-4 + 8x + 8x^3$, or $-4 - 8x - 8x^3$, where $g \in C_{16}$

Since 2 and 3 are prime in the other rings, the remaining idempotents ($[e_{\chi_0}], [e_{\chi_{36}}], [e_{\chi_{72}}]$) will have aliases of $12g$ for some $g \in C_{16}$.

3.2.3. *Addition of Idempotents.* Since there is a 9 to 1 mapping between C_{144} and C_{16} , a difference set image in C_{16} will have only odd entries between -9 and 9.

Since $[e_{\chi_0}]$ and $[e_{\chi_{72}}]$ both have similar patterns and both have an alias of 12, we can (without loss of generality) add these idempotents together before multiplying by the alias. So we combine these idempotents to get

$$12([e_{\chi_0}] + [e_{\chi_{72}}]) = \frac{3}{2} [1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0 \ 1 \ 0]$$

Then, with these two aliases, we can either add $12[e_{\chi_{36}}]$ or $12x[e_{\chi_{36}}]$. If we add $12[e_{\chi_{36}}]$ to the first two, we get:

$$\frac{3}{4} [3 \ 0 \ 0 \ 0 \ 3 \ 0 \ 0 \ 0 \ 3 \ 0 \ 0 \ 0 \ 3 \ 0 \ 0 \ 0] \quad (1)$$

If we add $12x[e_{\chi_{36}}]$ to the first two, we get:

$$\frac{3}{2} [1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1] \quad (2)$$

Now, we show that no possible combination of (1) or (2) with $[e_{\chi_9}]$ and $[e_{\chi_{18}}]$ will give just odd numbers.

First, we must look at the different possibilities alias-idempotent combinations with these two idempotents.

For $[e_{\chi_9}]$, we get the three possibilities:

$$12[e_{\chi_9}] = [6 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ -6 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0]$$

$$(-4+8x^2+8x^6)[e_{\chi_9}] = [-2 \ 0 \ 4 \ 0 \ 0 \ 0 \ 0 \ 4 \ 0 \ 2 \ 0 \ -4 \ 0 \ 0 \ 0 \ -4 \ 0]$$

$$(-4-8x^2-8x^6)[e_{\chi_9}] = \begin{bmatrix} -2 & 0 & -4 & 0 & 0 & 0 & -4 & 0 & 2 & 0 & 4 & 0 & 0 & 0 & 4 & 0 \end{bmatrix}$$

For $[e_{\chi_{18}}]$, we get the three possibilities:

$$\begin{aligned} 12[e_{\chi_{18}}] &= \begin{bmatrix} 3 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 3 & 0 & 0 & 0 \end{bmatrix} \\ (-4+8x+8x^3)[e_{\chi_{18}}] &= \begin{bmatrix} -12 & 0 & 2 & 0 & 0 & 0 & 4 & 0 & 2 & 0 & -4 & 0 & 0 & 0 & -4 & 0 \end{bmatrix} \\ (-4-8x-8x^3)[e_{\chi_{18}}] &= \begin{bmatrix} -2 & 0 & -4 & 0 & 0 & 0 & -4 & 0 & 2 & 0 & 4 & 0 & 0 & 0 & 4 & 0 \end{bmatrix} \end{aligned}$$

First, consider the case where we have to use (1). Then, we need some combination of

3.2.4. Impact. Since there are no images of difference sets in C_{16} , this means there are also no images (144,60,30) difference sets in any group with a C_{16} image. Therefore, we rule out images in C_{48} and ultimately rule out (144,66,30) difference sets in C_{144} . Also, using Dillon's Dihedral Trick, we can show that there are no Difference sets in any group of order 144 that has an image of D_{16}

3.2.5. Dillon's Dihedral Trick. If there is a difference set with parameters $(4m^2, 2m^2 - m, m^2 - m)$ in a dihedral group, then there is a difference set in the cyclic group.

Proof. Let $G = \langle x, y \mid x^t = 1, y^2 = 1, yxy^{-1} = x^{-1} \rangle \cong D_{16}$

Rewriting this, we get $G = \langle x \rangle + y \langle x \rangle$

Suppose $D \in \mathbb{Z}[G]$ such that $DD^{(-1)} = m^2 \cdot 1_G + \lambda G = m^2 \cdot 1_G + \lambda(\langle x \rangle + y \langle x \rangle)$

Then, $D = A + yB$ where $A, B \in \mathbb{Z}[\langle x \rangle]$

$$\begin{aligned} DD^{(-1)} &= (A + yB)(A + yB)^{-1} \\ &= (A + yB)(A^{-1} + B^{-1}y^{-1}) \\ &= (A + yB)(A^{-1} + B^{-1}y) \\ &= AA^{-1} + AB^{-1}y + yBA^{-1} + yBB^{-1}y \\ &= AA^{-1} + BB^{-1} + 2yBA^{-1} \quad \text{since } yg = g^{-1}y\forall g \in G \\ &= (m^2 + \lambda \langle x \rangle) + \lambda y \langle x \rangle \\ \text{Therefore, } AA^{-1} + BB^{-1} &= m^2 + \lambda \langle x \rangle \\ \text{and } 2yBA^{-1} &= \lambda y \langle x \rangle \text{ or } BA^{-1} = \frac{\lambda}{2} \langle x \rangle \end{aligned}$$

Now, suppose $G_1 = \langle x, y \mid x^t = 1, y^2 = x \rangle = \langle y \mid y^{2t} = 1 \rangle \cong C_{2t}$

$G = \langle x \rangle + y \langle x \rangle$

Given $D_1 \in \mathbb{Z}[G_1]$ then $D_1 = A_1 + yB_1$ where $A_1, B_1 \in G_1$

$$\begin{aligned} \text{Then, } D_1 D_1^{-1} &= (A_1 + yB_1)(A_1^{-1} + B_1^{-1}y^{-1}) \\ &= (A_1 A_1^{-1} + B_1 B_1^{-1}) + A_1 B_1^{-1} y^{-1} + A_1^{-1} B_1 y \end{aligned}$$

If we chose $A_1 = A$ and $B_1 = B$, then

$$\begin{aligned} &= (m^2 + \lambda \langle x \rangle) + \frac{\lambda}{2} \langle x \rangle y^{-1} + \frac{\lambda}{2} \langle x \rangle y \\ &= m^2 + \lambda G_1 \quad \text{since } \langle x \rangle y^{-1} = \langle x \rangle y \end{aligned}$$

Therefore, $A + yB$ is a difference set in C_t . \square

3.2.6. Consequences. Dillon's Dihedral Trick implies that if there is not a difference set in the cyclic group, then the dihedral group also does not have a difference set. Since we did not have and C_{16} images, we were able to rule our any D_{16} images also and were able to show the nonexistence of difference sets in 18 groups.

4. NON-ABELIAN DIFFERENCE SETS

4.1. Product Construction. Here, we will explain a Product Construction which we used to find difference sets in groups.

4.1.1. **Definition.** [?] A **perfect ternary array** of length k^2 in a group G is a group ring element $T = \sum_{g \in G} \alpha_g g$ for $\alpha_g \in \{-1, 0, 1\}$ and $T \cdot T^{-1} = k^2$.

With the following product construction, we can construct Hadamard difference sets using a perfect ternary array of length 4 and previously found (36,15,6) difference sets.

Given a group G and integer group ring $\mathbb{Z}[G]$ define for $a, b \in G$, $T_{a,b} = 1 - a - b - ab$
If either

$$(1) \quad a^2 = 1 \text{ and } ab = ba \quad \text{“Commuting Involution”}$$

or

$$(2) \quad a^4 = b^4 = 1, \quad bab^{-1} = a^{-1}, \quad a^2 = b^2 \quad \text{“Quaternion”}$$

then $T_{a,b} \cdot T_{a,b}^{-1} = 4$, which means $T_{a,b}$ is a perfect ternary array of length 4.

Proof. $T_{a,b} \cdot T_{a,b}^{-1} = 4$ for “commuting involution” and “quaternion”

$$\begin{aligned} T_{a,b} \cdot T_{a,b}^{-1} &= (1 - a - b - ab)(1 - a^{-1} - b^{-1} - b^{-1}a^{-1}) \\ &= 4 - b^{-1} - b^{-1}a^{-1} + ab^{-1} + ab^{-1}a^{-1} - b + ba^{-1} - ab + aba^{-1} \end{aligned}$$

Case 1: Commuting Involution

$$\begin{aligned} &4 - b^{-1} - b^{-1}a^{-1} + ab^{-1} + ab^{-1}a^{-1} - b + ba^{-1} - ab + aba^{-1} \\ &= 4 - b - ab + ab + b - b + ab - ab + b \\ &= 4 = T_{a,b} \cdot T_{a,b}^{-1} \end{aligned}$$

Case 2: Quaternion

$$\begin{aligned} &4 - b^{-1} - b^{-1}a^{-1} + ab^{-1} + ab^{-1}a^{-1} - b + ba^{-1} - ab + aba^{-1} \\ &= 4 - b^{-1} - b^{-1}bab^{-1} + ab^{-1} + ab^{-1}bab^{-1} - b + bbab^{-1} - ab + abbab^{-1} \\ &= 4 = T_{a,b} \cdot T_{a,b}^{-1} \quad \square \end{aligned}$$

4.1.2. *Product Construction.* Let G be a group of order 144 and H be a group of order 36 that contains a (36,15,6) difference set, \hat{D}_1 . If there exists $a, b \in G$ of the “convoluting involution” or “quaternion” types such that

$$G = H \cup Ha \cup Hb \cup Hab,$$

then

$$\hat{D} = \hat{D}_1 \cdot T_{a,b}$$

is a (144,66,30) difference set.

Proof. Show that \hat{D} satisfies the difference set equation

$$\begin{aligned} \hat{D}\hat{D}^{-1} &= (\hat{D}_1 \cdot T_{a,b})(\hat{D}_1 \cdot T_{a,b})^{-1} \\ &= (\hat{D}_1 \cdot T_{a,b})(T_{a,b}^{-1} \cdot \hat{D}_1^{-1}) \\ &= \hat{D}_1(T_{a,b} \cdot T_{a,b}^{-1})\hat{D}_1^{-1} \\ &= \hat{D}_1(4)\hat{D}_1^{-1} \\ &= 4(\hat{D}_1\hat{D}_1^{-1}) \\ &= 4 \cdot 36 = 144 \quad \square \end{aligned}$$

4.1.3. *Consequences.* Using this product construction, we were able to determine the existence of difference sets in 94 groups.

4.2. **Spread Construction.**

4.2.1. *Theorem 1.* Suppose G is a group of order 144 with a subgroup K of order 36 such that

- (1) K has a difference set E with Hadamard transform \hat{E} (so that $\hat{E}\hat{E}^{(-1)} = 36 \cdot 1_K$.)
- (2) K has a left transversal (system of distinct coset representatives) $1, a, b, ab$ in G .
- (3) $T_{a,b}$ is of “commuting involution type” or “quaternion type.”

Then $\hat{D} := T_{a,b} \cdot \hat{E}$ is the Hadamard transform of a $(144, 66, 30)$ difference set in G .

4.2.2. *Proof of Theorem 1, Condition 3.* Let G be a group of order 144 with a non-cyclic subgroup H of order 9.

Assuming that $T_{a,b}$ is of “commuting involution type” or “quaternion type,” we can construct a difference set in G .

In either case, we can order all L_i such that

$$\{L_0, L_1, L_2, L_3\} = \{L_0, aL_1a^{-1}, bL_2b^{-1}, abL_3b^{-1}a^{-1}\}.$$

Because we are taking elements a and b from the Sylow-2 subgroup of our group G of order 144, they will have order equal to 2, 4 or 8.

We represent subgroups $\{L_0, L_1, L_2, L_3\}$ of our cyclic 3 by cyclic 3 subgroup $H = Z_3 \times Z_3$ as $\langle (1, 0) \rangle, \langle (0, 1) \rangle, \langle (1, 1) \rangle$ and $\langle (1, -1) \rangle$, respectively. One way to think about conjugation by elements a and b is left multiplication of the generator of the subgroup by an element of $GL(2, 3)$. We can denote these conjugations as σ_a, σ_b and σ_{ab} , and represent the generators of the subgroups as column vectors $\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, and $\begin{pmatrix} 1 \\ -1 \end{pmatrix}$.

Case 1: Elements a and b satisfy commuting involution type: $a^2 = 1$ and $ab = ba$. We have five choices for a . By choosing $\sigma_a = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, we see that it will commute with all other elements within the Sylow-2 subgroup and fix all L_i . Choose b to be any element of order 2 or 4.

The four choices for σ_b with order 2 include $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$.

The first two choices for σ_b with 0 on the main diagonals will permute (L_0, L_1) but fix L_2 and L_3 . The second two cases, where σ_b is a diagonal matrix, will permute (L_2, L_3) but fix L_0 and L_1 . For either of these choices for σ_b with the general form $(L_h, L_i)(L_j)(L_k)$ we can choose the following:

$$\{L_h, \sigma_a(L_i), \sigma_b(L_j), \sigma_{ab}(L_k)\}$$

which is equal to

$$\{L_h, L_i, L_j, L_k\}.$$

When σ_b has order 4, it permutes L 's in the following general form: $(L_h, L_i)(L_j, L_k)$. When such a σ_b is paired with σ_a that fixes L , we can choose the following:

$$\{L_i, \sigma_a(L_h), \sigma_b(L_j), \sigma_{ab}(L_k)\}$$

which is equal to

$$\{L_i, L_h, L_k, L_j\}.$$

There are also several cases where σ_a fails to commute with all other elements in the group but will commute with a select few elements of order 2, allowing limited choices for σ_b .

We first consider the case where $\sigma_a = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. In order to satisfy our commutativity relations $ab = ba$, we need to find a matrix σ_b such that

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \sigma_b = \sigma_b \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

This condition forces σ_b to be a diagonal matrix.

The only matrix σ_b in $GL(2, 3)$ that satisfies this relation and has not already been accounted for in previous cases is $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$. Note that $\sigma_b = (-1)\sigma_a$. Thus when considering group action of σ_a on the set $\{L_0, L_1, L_2, L_3\}$, we automatically account for σ_b as well since scalar multiplication fixes the vector.

Both σ_a and σ_b have the following form: $(L_0)(L_1)(L_2, L_3)$. We also know that, given our choices for σ_a and σ_b , $\sigma_{ab} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, which we have already shown fixes the set. We can choose

$$\{L_0, \sigma_a(L_2), \sigma_b(L_3), \sigma_{ab}(L_1)\}$$

which is equal to

$$\{L_0, L_3, L_2, L_1\}.$$

We use a similar argument for the case $\sigma_a = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. We need to choose σ_b such that

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \sigma_b = \sigma_b \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

This condition implies that σ_b must have both sets of diagonal and off-diagonal entries equal.

There are 2 non-trivial matrices in $GL(2, 3)$ that satisfy this property: $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$

and $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. However, we have already described the first case, so we need only to investigate the second. Once again, $\sigma_b = (-1)\sigma_a$, so σ_b will perform the same permutation as σ_a . Both will take the following form: $(L_0, L_1)(L_2)(L_3)$ Again, $\sigma_{ab} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. We can choose

$$\{L_2, \sigma_a(L_1), \sigma_b(L_0), \sigma_{ab}(L_3)\}$$

which is equal to

$$\{L_2, L_0, L_1, L_3\}.$$

Thus we have considered all choices for a and b that satisfy “commuting involution” type and each case satisfies

$$\{L_0, L_1, L_2, L_3\} = \{L_0, aL_1a^{-1}, bL_2b^{-1}, abL_3b^{-1}a^{-1}\}.$$

Case 2: Elements a and b satisfy quaternion type: $a^4 = b^4 = 1$, $a^2 = b^2$ and $aba^{-1} = b^{-1}$. Any elements that satisfy this type lie in the subgroup of $GL(2, 3)$ that is isomorphic to the quaternion group.

In general, if we have σ_a and σ_b that satisfy the quaternion type, they will each permute L 's in two 2-cycles. In addition, σ_a and σ_b will permute different pairings of L 's.

$$\text{If } \sigma_a = (L_i, L_j)(L_k, L_h) \text{ and } \sigma_b = (L_i, L_k)(L_j, L_h), \text{ then } \sigma_{ab} = (L_i, L_h)(L_j, L_k).$$

We can choose

$$\{L_i, \sigma_a(L_k), \sigma_b(L_h), \sigma_{ab}(L_j)\}$$

which is equal to

$$\{L_i, L_h, L_j, L_k\}$$

There are six choices for σ_a and σ_b ; each permutes in two 2-cycles. There are three different possible permutations, each occurs twice. By choosing elements a and b that satisfy the quaternion type, we ignore the case where $\sigma_a = \sigma_b$ because, of our six choices for σ , the only way to get the same permutation is when we choose elements a and b so $b = a^{-1}$. This violates our initial set of assumptions. Thus we have considered all choices for a and b that satisfy “quaternion” type and each case satisfies

$$\{L_0, L_1, L_2, L_3\} = \{L_0, aL_1a^{-1}, bL_2b^{-1}, abL_3b^{-1}a^{-1}\}.$$

Therefore, in all groups with either of these conditions met, we will be able to construct a difference set using this spread construction.

5. RESOLVING EXISTENCE OF DIFFERENCE SETS IN THE GROUPS OF ORDER 144

Using the methods explained previously, we now categorize all the groups of order 144 in which we either found a difference set or proved that the group cannot contain a difference set.

5.1. Product Construction Says Yes in 94 Groups. The $T_{a,b}$ product construction described in section 4.1 can also be broken into smaller pieces which is what we used. A direct product construction is a more specific example of the product construction and finds 17 difference sets. There is also a more specific construction with a product of a Hadamard 36 difference set and a group of order 4 which accounts for 45 difference sets. The remaining 32 can be found using $T_{a,b}$; 10 of which is a “Quaternion” type and 22 where a is a ‘Commuting Involution.’

The following table describes which groups each of these product constructions finds difference sets in. The sets are the i 's which represent the category number in GAP, that is 'SmallGroup(144, i)'¹.

Method of Construction	D.S. in Group $(144, i) \forall i$
$H_{36} \times H_4$	76, 92, 101, 132, 143, 155, 159, 166 169, 176, 178, 191, 192, 193, 195, 195, 197
$H_{36} \bar{H}_4$	63, 64, 65, 66, 67, 77, 78, 79, 84, 93 94, 95, 100, 102, 103, 115, 116, 120 123, 126, 129, 133, 136, 144, 145, 146 149, 150, 151, 153, 154, 160, 162, 167 170, 172, 177, 179, 183, 184, 186, 188 189, 190, 194
$T_{a,b} \bar{H}_{36}$ a is Quaternion Type	74, 90, 104, 134, 152, 158, 168, 180, 185, 187
$T_{a,b} \bar{H}_{36}$ a is Commuting Involution	52, 53, 69, 85, 130, 137, 138, 139, 140 141, 142, 147, 148, 161, 163, 164, 165 171, 173, 174, 175 181

5.2. Homomorphic Images Rule Out 39 More Groups. If a group contains a difference set, then any homomorphic image of that group will contain an image of the difference set. We investigate the contrapositive of this statement. If a homomorphic image of a group can be shown that it cannot contain a difference set, then any group that has that homomorphic image cannot contain a difference set.

We have ruled out the possibility for difference sets to exist in any group with images of $C_{16} \Rightarrow D_{16}$ ², $C_{36} \times C_2 \Rightarrow D_{36} \times C_2$, and $C_{18} \times C_2 \times C_2$. That eliminates the possibility of difference sets in 18, 5, 11, and 5 groups of order 144 respectively. The following table describes which groups have the specified image and thus do not have a difference set.

Homomorphic Image	Group $(144, i) \forall i$ with Particular Image
C_{16} or D_{16}	1, 2, 8, 16, 25, 28, 29, 30, 51, 56, 57 72, 80, 88, 96, 106, 114, 117
$C_{36} \times C_2$	20, 21, 22, 23, 24
$D_{36} \times C_2$	37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 112
$C_{18} \times C_2 \times C_2$	47, 48, 49, 50, 113

5.3. 64 Remain: Separating the Sheep from the Goats. Lander's conjecture³ tells us that there will be no difference set in 26 of the remaining 64 groups. While this is obviously a conjecture, it is a strong enough conjecture to make us focus on the other 38 groups for which it seems likely that we will find a difference set instead of looking where we expect not to find any. This is where the new spread construction plays a large part. It creates difference sets in 37 of the 38

¹If one wanted to investigate the structure of these various groups, I recommend using the 'StructureDescription(g)' command, where $g := \text{SmallGroup}(144, i)$. This will give you an idea of which group is which in GAP.

²See Section 3.2 for an example of how this was done for C_{16} . The others were done with similar techniques.

³citation of Lander

remaining groups. If we assume Lander's conjecture to be true, we have successfully categorized every group but 1 into 2 sets; those with difference sets and those without. It will take time to verify Lander's conjecture, and unfortunately we are out of it; however, this part of the project should be finished by computer in the coming weeks. As of now, here is the table showing where the remaining 68 groups fall.

Lander, Spread, Other	Group $(144, i) \forall i$
Lander Conjectures says no difference set	3, 4, 5, 6, 7, 9, 10, 11, 12, 13, 14 15, 17, 18, 19, 26, 27, 31, 32, 33, 34 35, 36, 109, 110, 111
Successful Spread Construction	54, 55, 58, 59, 60, 61, 62, 70, 71, 73 75, 81, 82, 83, 86, 87, 89, 91, 97, 98, 99 105, 107, 108, 118, 119, 121, 122, 124, 125 127, 128, 131, 135, 156, 157, 182
Still Unknown	68

6. CONCLUSION

At this point we have officially resolved the question of existence of difference sets in 170 of the 197 groups of order 144. After that there are essentially two cases, either of which are quite good.

Case 1: Lander's conjecture holds true in groups of order 144. Then we finished the summer resolving existence of difference sets in all but 1 group of order 144; namely, `SmallGroup(144,68)`.

(Case 2): Lander's conjecture fails in at least one group of order 144 and we find a difference set. This would mean we found a counterexample and thus disproved Lander's conjecture.

The investigation of existence in these remaining 26 Lander's conjecture groups is being carried on as this paper is being written. Hopefully these groups as well as `SmallGroup(144,68)` will be resolved in the near future; however, the REU ends July 27 and the work will have to be continued by Dr. Smith and the two graduate students who have been assisting us over the summer.

7. ACKNOWLEDGEMENT

This research was done with the funding from an NSF grant at Central Michigan University. We would like to thank Ken Smith for his support during this program. We would also like to thank Ryan Kaliszawski and Jordan Webster for their assistance.

APPENDIX A. DIFFERENCE SETS FROM SPREAD CONSTRUCTION

Note: We found difference sets in 37 groups using this construction. [144,68] was the only possible group that did not yield a difference set by this construction.

The following list includes the catalogue number for each group and the list of which elements are included in the difference set using GAP notation.

144,54 [1, 3, 6, 10, 11, 12, 13, 14, 17, 18, 21, 22, 25, 28, 29, 30, 31, 34, 35, 36, 37, 46, 47, 48, 51, 52, 55, 57, 59, 61, 62, 65, 67, 76, 81, 82, 85, 86,87, 88, 89, 92, 95, 97, 98, 99, 100, 102, 104, 105, 106, 107, 108, 110,114, 115, 119, 120, 123, 126, 127, 128, 135, 141, 142, 143]

144,55 [1, 3, 6, 9, 12, 13, 14, 16, 17, 18, 19, 21, 22, 26, 27, 28, 29, 33, 35, 36, 37, 41, 44, 47, 48, 49, 51, 52, 55, 56, 60, 62, 69, 70, 71, 72, 76, 80, 88, 89, 92, 93, 94, 97, 99, 100, 104, 105, 106, 107, 108, 110, 117, 118, 119, 120, 123, 124, 125, 129, 130, 132, 135, 140, 141, 143]

144,58 [1, 3, 4, 6, 8, 9, 11, 12, 16, 19, 20, 22, 25, 26, 29, 32, 33, 34, 36, 37, 39, 41, 44, 46, 49, 50, 51, 55, 61, 66, 68, 69, 70, 71, 72, 74, 76, 77, 79, 80, 84, 85, 88, 89, 111, 112, 113, 114, 115, 117, 118, 120, 122, 124, 125,126, 127, 128, 129, 130, 131, 132, 135, 136, 137, 144]

144,59 [1, 3, 4, 6, 8, 9, 11, 12, 13, 14, 19, 20, 22, 28, 29, 32, 33, 34, 36, 37, 43, 46, 49, 50, 51, 55, 57, 59, 62, 66, 68, 69, 70, 71, 72, 84, 85, 88, 89,92, 94, 95, 97, 98, 110, 112, 113, 114, 115, 116, 117, 118, 120, 123, 124,125, 126, 127, 129, 130, 131,132,137,140,141, 143]

144,60 [1, 3, 4, 6, 8, 10, 11, 12, 13, 14, 19, 21, 22, 26, 28, 29, 30, 31, 34, 36, 37, 43, 45, 49, 51, 52, 57, 59, 62, 65, 66, 67, 69, 71, 72, 79, 83, 84, 88, 89, 92, 94, 95, 98, 112, 113, 116, 117, 118, 120, 122, 123, 124, 125, 129, 130, 131, 132, 133, 134, 136, 137, 138, 139, 140, 144]

144,61 [1, 3, 6, 10, 11, 12, 13, 14, 17, 18, 21, 22, 25, 28, 29, 30, 31, 34, 35, 36, 37, 43, 46, 47, 48, 51, 52, 55, 57, 59, 61, 62, 65, 67, 79, 85, 86, 87,88, 89, 92, 95, 97, 98, 99, 100, 102, 104, 105, 106, 107, 108, 112, 113, 116, 119, 120, 123, 126, 127, 128, 133, 134, 136, 141, 142]

144,62 [1, 2, 3, 4, 6, 13, 14, 20, 21, 22, 25, 27, 28, 29, 31, 33, 35, 37, 41, 46, 48, 50, 52, 55, 58, 60, 61, 62, 66, 67, 69, 70, 74, 80, 81, 82, 84, 85, 88, 89, 92, 96, 97, 102, 104, 105, 106, 107, 108, 111, 112,113, 117, 118, 119, 123, 124, 125, 126, 127, 128, 131, 132, 137, 141, 142]

144,70 [1, 3, 4, 9, 11, 12, 14, 15, 17, 18, 21, 23, 26, 28, 29, 30, 32, 33, 34,36,41, 45, 49, 50, 52, 54, 58, 59, 60, 61, 62, 63, 71, 75, 77, 79,84,85,88,89, 90, 93, 96, 97, 98, 99, 100, 102, 103, 104, 105, 106,107,111,113,115, 118, 119, 123, 124, 127, 128, 134, 140, 142,143]

144,71 [1, 3, 4, 5, 8, 9, 10, 12, 14, 15, 17, 19, 22, 28, 29, 31, 33, 35, 36, 40, 41, 46, 50, 52, 53, 59, 60, 61, 62, 64, 65, 67, 68, 69, 72, 85, 87, 89, 90, 95, 96, 98,

99, 100, 110, 111, 112, 113, 114, 115, 117, 119, 120, 122, 123, 126, 127, 128, 129, 130, 131, 132, 137, 139, 140, 143]

144,73 [1, 3, 4, 9, 11, 12, 14, 15, 17, 18, 21, 23, 26, 28, 29, 30, 32, 33, 34, 36, 40, 41, 45, 49, 50, 52, 54, 58, 59, 60, 61, 62, 63, 71, 78, 84, 85, 88, 89, 90, 93, 96, 97, 98, 99, 100, 102, 103, 104, 105, 106, 107, 110, 112, 114, 118, 119, 123, 124, 127, 128, 133, 135, 136, 140, 142]

144,75 [1, 2, 4, 10, 11, 13, 15, 16, 17, 18, 21, 22, 23, 26, 28, 32, 33, 34, 37, 38, 41, 44, 45, 49, 50, 53, 54, 58, 59, 61, 62, 68, 70, 71, 73, 75, 77, 78, 79, 80, 85, 89, 93, 96, 97, 100, 104, 108, 110, 114, 116, 117, 118, 119, 120, 122, 123, 124, 126, 127, 131, 134, 135, 138, 140, 141]

144,81 [1, 3, 4, 5, 8, 9, 11, 12, 15, 16, 17, 22, 23, 26, 27, 29, 30, 33, 34, 36, 42, 43, 44, 48, 50, 53, 54, 58, 59, 63, 65, 67, 68, 69, 71, 77, 80, 81, 82, 83, 85, 87, 89, 96, 110, 113, 114, 116, 117, 119, 120, 122, 124, 126, 129, 130, 131, 132, 133, 134, 136, 137, 138, 140, 141, 143]

144,82 [1, 3, 4, 5, 8, 9, 10, 12, 16, 17, 19, 22, 26, 27, 29, 31, 33, 35, 36, 41, 42, 43, 44, 46, 50, 52, 53, 58, 59, 64, 65, 67, 68, 69, 72, 77, 78, 80, 81, 82, 85, 87, 89, 90, 110, 111, 114, 115, 116, 117, 119, 120, 122, 123, 124, 125, 126, 127, 129, 130, 131, 132, 134, 135, 137, 144]

144,83 [1, 2, 4, 10, 11, 13, 15, 16, 17, 18, 21, 22, 23, 26, 28, 32, 33, 34, 37, 38, 41, 44, 45, 49, 50, 53, 54, 58, 59, 61, 62, 68, 70, 71, 73, 75, 77, 78, 79, 80, 85, 89, 93, 96, 97, 100, 104, 108, 110, 114, 116, 117, 118, 119, 120, 122, 123, 124, 126, 127, 131, 134, 135, 138, 140, 141]

144,86 [1, 3, 6, 10, 11, 12, 13, 14, 17, 18, 19, 21, 22, 25, 28, 29, 30, 34, 36, 37, 39, 43, 47, 48, 49, 51, 52, 55, 59, 61, 62, 64, 65, 66, 69, 71, 72, 74, 77, 79, 88, 89, 97, 98, 99, 100, 103, 104, 105, 111, 116, 117, 118, 119, 120, 124, 125, 126, 127, 128, 131, 132, 136, 138, 139, 141]

144,87 [1, 3, 4, 6, 9, 11, 12, 13, 14, 16, 20, 21, 22, 25, 26, 28, 29, 32, 34, 36, 37, 44, 46, 50, 51, 52, 61, 62, 64, 66, 68, 69, 71, 72, 74, 76, 79, 84, 85, 86, 87, 92, 99, 100, 103, 106, 107, 111, 117, 118, 120, 122, 123, 124, 125, 126, 127, 128, 131, 132, 135, 136, 137, 138, 139, 144]

144,89 [1, 3, 6, 10, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 25, 28, 29, 30, 34, 36, 37, 41, 44, 47, 48, 49, 51, 52, 55, 59, 61, 62, 64, 65, 66, 69, 71, 72, 76, 80, 88, 89, 97, 98, 99, 100, 103, 104, 105, 110, 117, 118, 119, 120, 124, 125, 126, 127, 128, 131, 132, 135, 138, 139, 141, 143]

144,91 [1, 2, 6, 9, 10, 14, 15, 16, 17, 18, 19, 21, 22, 25, 28, 29, 31, 35, 37, 38, 42, 44, 47, 48, 49, 51, 52, 55, 59, 61, 62, 64, 67, 69, 74, 75, 76, 79, 81, 82, 88, 89, 97, 98, 99, 100, 103, 108, 111, 112, 113, 117, 118, 119, 120, 124, 125, 126, 127, 128, 132, 135, 136, 138, 139, 141]

144,97 [1, 3, 6, 10, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 25, 28, 29, 30, 34, 36, 37, 41, 44, 47, 48, 49, 51, 52, 55, 59, 61, 62, 64, 65, 66, 69, 71, 72, 76, 80, 88, 89, 97, 98, 99, 100, 103, 104, 105, 110, 117, 118, 119, 120, 124, 125, 126, 127, 128, 131, 132, 135, 138, 139, 141, 143]

144,98 [1, 3, 4, 6, 8, 9, 11, 12, 20, 21, 22, 25, 26, 29, 32, 34, 36, 37, 39, 41, 46, 50, 51, 52, 55, 57, 59, 61, 64, 66, 68, 69, 71, 72, 76, 77, 79, 80, 81, 82, 84, 85, 86, 87, 95, 98, 103, 106, 107, 112, 113, 114, 115, 117, 118, 120, 122, 128, 131, 132, 133, 134, 135, 136, 137, 144]

144,99 [1, 3, 6, 10, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 25, 28, 29, 30, 34, 36, 37, 41, 44, 47, 48, 49, 51, 52, 55, 59, 61, 62, 64, 65, 66, 69, 71, 72, 76, 80, 88, 89, 97, 98, 99, 100, 103, 104, 105, 110, 117, 118, 119, 120, 124, 125, 126, 127, 128, 131, 132, 135, 138, 139, 141, 143]

144,105 [1, 2, 4, 11, 12, 13, 14, 16, 17, 19, 22, 23, 24, 26, 27, 30, 34, 36, 37, 39, 41, 44, 46, 49, 50, 52, 53, 56, 59, 61, 62, 68, 70, 72, 73, 74, 76, 77, 78, 82, 85, 88, 91, 94, 96, 99, 101, 108, 110, 113, 116, 117, 118, 119, 120, 121, 122, 123, 125, 126, 130, 133, 134, 139, 140, 141]

144,107 [1, 3, 4, 9, 10, 12, 14, 15, 16, 17, 19, 22, 23, 24, 26, 27, 29, 31, 33, 36, 41, 43, 44, 46, 49, 50, 52, 53, 56, 59, 61, 62, 63, 64, 66, 67, 68, 72, 77, 81, 85, 88, 91, 94, 96, 99, 102, 105, 108, 115, 117, 118, 119, 120, 121, 122, 123, 125, 126, 129, 130, 133, 139, 140, 141, 143]

144,108 [1, 3, 4, 9, 10, 12, 14, 15, 16, 17, 19, 22, 23, 24, 26, 27, 29, 31, 33, 36, 41, 43, 44, 46, 49, 50, 52, 53, 56, 59, 61, 62, 63, 64, 66, 67, 68, 72, 77, 81, 85, 88, 91, 94, 96, 99, 102, 105, 108, 115, 117, 118, 119, 120, 121, 122, 123, 125, 126, 129, 130, 133, 139, 140, 141, 143]

144,118 [1, 3, 4, 6, 8, 9, 11, 12, 16, 19, 20, 22, 25, 26, 29, 32, 33, 34, 36, 37, 39, 41, 44, 46, 49, 50, 51, 55, 61, 66, 68, 69, 70, 71, 72, 74, 76, 77, 79, 80, 84, 85, 88, 89, 111, 112, 113, 114, 115, 117, 118, 120, 122, 124, 125, 126, 127, 128, 129, 130, 131, 132, 135, 136, 137, 144]

144,119 [1, 3, 6, 10, 11, 12, 13, 14, 17, 18, 21, 22, 25, 28, 29, 30, 31, 34, 35, 36, 37, 43, 46, 47, 48, 51, 52, 55, 57, 59, 61, 62, 65, 67, 79, 85, 86, 87, 88, 89, 92, 95, 97, 98, 99, 100, 102, 104, 105, 106, 107, 108, 112, 113, 116, 119, 120, 123, 126, 127, 128, 133, 134, 136, 141, 142]

144,121 [1, 3, 5, 6, 8, 9, 10, 11, 13, 17, 19, 20, 25, 26, 29, 30, 33, 34, 35, 36, 40, 43, 44, 48, 49, 51, 52, 53, 54, 58, 68, 72, 75, 76, 80, 81, 82, 84, 87, 88, 89, 90, 91, 92, 93, 94, 98, 100, 101, 102, 103, 109, 110, 111, 113, 116, 119, 120, 122, 128, 130, 133, 136, 139, 141, 144]

144,122 [1, 3, 5, 6, 8, 9, 10, 11, 13, 17, 19, 20, 25, 29, 30, 33, 34, 35, 36, 40, 43, 44, 48, 49, 51, 52, 53, 54, 55, 58, 59, 60, 61, 62, 68, 72, 75, 76, 80, 81, 82, 84, 87, 88, 89, 90, 99, 109, 110, 111, 113, 116, 119, 120, 121, 123, 124, 125, 126, 129,

131, 133, 136, 138, 140, 142]

144,124 [1, 3, 5, 6, 8, 9, 10, 11, 13, 17, 21, 25, 29, 30, 31, 32, 34, 35, 36, 40, 43, 44, 50, 51, 52, 53, 54, 55, 58, 59, 60, 61, 62, 66, 67, 69, 72, 74, 75, 80, 81, 84, 87, 88, 89, 94, 100, 105, 109, 110, 111, 112, 113, 114, 116, 117, 118, 119, 121, 123, 131, 133, 136, 137, 138, 140]

144,125 [1, 3, 5, 6, 8, 9, 10, 11, 13, 17, 21, 25, 29, 30, 31, 32, 34, 35, 36, 40, 43, 44, 50, 51, 52, 53, 54, 55, 58, 59, 60, 61, 62, 66, 67, 69, 72, 74, 75, 80, 81, 84, 87, 88, 89, 94, 100, 105, 109, 110, 111, 112, 113, 114, 116, 117, 118, 119, 121, 123, 131, 133, 136, 137, 138, 140]

144,127 [1, 3, 4, 5, 8, 9, 10, 11, 13, 17, 19, 21, 25, 28, 29, 30, 32, 34, 35, 36, 40, 44, 47, 48, 49, 50, 51, 52, 53, 58, 60, 67, 72, 74, 79, 83, 84, 86, 87, 88, 89, 90, 92, 96, 97, 98, 102, 103, 104, 111, 114, 115, 117, 118, 120, 125, 126, 130, 134, 136, 137, 138, 139, 140, 142, 143]

144,128 [1, 3, 4, 5, 8, 9, 10, 11, 13, 17, 19, 21, 25, 29, 30, 32, 34, 35, 36, 40, 44, 47, 48, 49, 50, 51, 52, 53, 57, 58, 62, 64, 65, 67, 72, 74, 79, 83, 84, 86, 87, 88, 89, 90, 94, 100, 101, 111, 114, 115, 117, 118, 120, 121, 123, 124, 127, 128, 129, 131, 134, 136, 137, 141, 143, 144]

144,131 [1, 4, 6, 8, 9, 12, 14, 15, 16, 19, 21, 22, 25, 26, 29, 31, 33, 35, 36, 37, 38, 39, 42, 43, 44, 45, 49, 51, 52, 55, 64, 67, 69, 70, 71, 72, 75, 77, 83, 84, 88, 89, 94, 99, 100, 103, 106, 107, 108, 110, 112, 113, 114, 115, 116, 117, 118, 120, 122, 126, 127, 132, 137, 140, 143, 144]

144,135 [1, 2, 6, 9, 10, 14, 15, 16, 17, 18, 19, 21, 22, 25, 28, 29, 31, 35, 37, 38, 42, 44, 47, 48, 49, 51, 52, 55, 59, 61, 62, 64, 67, 69, 74, 75, 76, 79, 81, 82, 88, 89, 97, 98, 99, 100, 103, 108, 111, 112, 113, 117, 118, 119, 120, 124, 125, 126, 127, 128, 132, 135, 136, 138, 139, 141]

144,156 [1, 3, 5, 6, 8, 9, 13, 17, 21, 23, 24, 25, 29, 30, 31, 32, 34, 35, 36, 40, 42, 43, 44, 50, 51, 52, 53, 54, 55, 58, 59, 60, 61, 62, 66, 67, 72, 75, 80, 83, 87, 88, 89, 92, 94, 99, 100, 101, 108, 109, 110, 111, 114, 117, 121, 122, 123, 124, 125, 128, 130, 132, 133, 138, 141, 142]

144,157 [1, 3, 5, 6, 8, 9, 10, 11, 13, 17, 21, 25, 29, 30, 31, 32, 34, 35, 36, 40, 42, 44, 50, 51, 52, 53, 54, 55, 58, 59, 60, 62, 66, 67, 72, 74, 75, 80, 81, 85, 87, 88, 89, 94, 100, 103, 108, 110, 111, 112, 113, 114, 116, 117, 118, 119, 122, 123, 131, 132, 134, 136, 137, 139, 143, 144]

144,182 [1, 2, 4, 6, 9, 10, 13, 15, 16, 20, 21, 22, 25, 26, 28, 29, 33, 35, 37, 40, 42, 44, 46, 50, 51, 52, 61, 62, 64, 66, 70, 74, 76, 78, 79, 81, 82, 84, 85, 86, 87, 92, 99, 100, 103, 108, 111, 114, 115, 117, 118, 120, 122, 123, 124, 125, 126, 127, 128, 131, 135, 136, 137, 138, 139, 144]

REFERENCES

- [1] K.T. Arasu, J. Dillon, Perfect Ternary Arrays, in Sequences and their Correlation Properties, edited by Pott, Kumar, Helleseth, Jungnickel, NATO Science Series, C 542, 1-16, 1999.
- [2] The GAP Group, Gap Groups, Algorithms, and Programming, Version 4.4, 2006. (<http://www.gap-system.org>)