Journal of the Nigerian Mathematical Society — Vol. 35, pp. 339-368, 2016

IN SEARCH OF SPORADIC (280, 63,14) DIFFERENCE SETS

A. S. A. Osifodunrin

ABSTRACT. In the book titled "Symmetric design: an algebraic approach", Eric Lander gave a wonderful exposition of difference sets and listed some abelian (v, k, λ) difference set parameters that were open for small values of k. One of such parameter sets is (280, 63, 14). Lander[1] and Kopilovich [2] showed that there are no (280, 63, 14) difference sets in the three abelian groups of order 280. Using restrictions imposed by the underlying subgroups of group of order 280, representation theory and factorization of cyclotomic rings, we conclude that these difference sets may only exist in five of the thirty-seven non-abelian groups of order 280.

Keywords and phrases: Representation, group theory, difference set, cyclotomic ring
2010 Mathematical Subject Classification: 05B10

1. Introduction

Suppose that G is a multiplicative group of order v. A non-trivial (v, k, λ) difference set D is a subset of G consisting of k elements, where $1 < k < v - 1$ in which every non-identity element of G can be replicated precisely λ times by the multi-set $\{d_1 d_2^{-1} : d_1, d_2 \in D, d_1 \neq d_2\}$. The natural number $n := k - \lambda$ is known as the order of the difference set. The group type determines the kind of difference set. For instance, if G is abelian (resp. non-abelian or cyclic), then D is abelian (resp. non-abelian or cyclic) difference set. Difference sets are closely associated to other fields of study and a motivating factor for studying difference sets is the pleasure derived in combining of various techniques from algebraic number theory, representation theory, geometry, algebra and combinatorics to tackle difference set problems [3].

There is a nice relationship between symmetric designs and difference sets. A symmetric design admitting a sharply transitive automorphism group G, is isomorphic to the development of a difference set in G (Theorem 4.2 [1]). To the best of our knowledge, there is no (280, 63, 14) symmetric design and this parameter set does not belong to any

Received by the editors July 20, 2015; Accepted: July 07, 2016

known family. There are forty groups of order 280 out of which three are abelian. However, Lander[1] and Kopilovich [2] showed that these three abelian groups do not admit (280, 63, 14) difference sets. Our focus in this paper is on the remaining thirty seven non-abelian groups but our approach incorporates both abelian and non abelian groups. The search for (280, 63, 14) difference sets yields the following main result of this paper.

Theorem 1.1. *Suppose that G is a group of order 280 with a normal subgroup N such that $G/N \cong (C_2)^2 \times C_5$, D_{10}, C_{56}, D_{28}, $C_{28} \times C_2$, $Frob(20) \times C_2$, C_{70} or D_{35}, then G does not admit(280, 63, 14) difference set.*

Section 2 discusses relevant basic results while in sections 3, 4 and 5, we establish the main theorem by illustrating that some factor groups of G of orders 20, 40, 56 and 70 do not not admit (280, 63, 14) difference sets.

2. Preliminary

We look at basic information required to analyze this problem.

2.1. **Difference sets.** Let $\mathbb{Z}$ be the ring of integers and and $\mathbb{C}$ be the field of complex numbers. Suppose that G is a group of order v and D is a (v, k, λ) difference set in a group G. We sometimes view the elements of D as members of the group ring $\mathbb{Z}[G]$, which is a subring of the group algebra $\mathbb{C}[G]$. Thus, D represents both subset of G and element $\sum_{g \in D} g$ of $\mathbb{Z}[G]$. The sum of inverses of elements of D is $D^{(-1)} = \sum_{g \in D} g^{-1}$. Consequently, D is a difference set if and only if

$$DD^{(-1)} = n + \lambda G \text{ and } DG = kG. \tag{2.1}$$

If g is a non identity element of G, then the left and right translates of D, gD and Dg respectively are also difference sets. Furthermore, if α is an automorphism of G, then $D^{\alpha} := \{\alpha(d) : d \in D\}$ is also a difference set. Let $X, Y \in \mathbb{Z}[G]$. These two elements are equivalent if there is a group element g and automorphism α such that $X = g\alpha(Y)$. For each $g \in G$, if we take the left translates(or right translates) of D as blocks, then the resulting structure is called the development of D, $Dev(D)$ and G is the automorphism group of $Dev(D)$.

Difference sets are often used in the construction of symmetric design in that symmetric design admitting a sharply transitive automorphism group G, is isomorphic to the development of a difference set in G (Theorem 4.2 [1]). It is also known that the existence of symmetric designs does not necessarily imply that the corresponding difference sets exists(See [4, 5, 6]).

Given that D is a difference set in a group G of order v and N is a normal subgroup of G. Suppose that $\psi : G \longrightarrow G/N$ is a homomorphism and $T^* = \{1, t_1, \ldots, t_h\}$ is a left transversal of N in G. We can extend ψ by linearity, to the corresponding group rings. Thus, the difference set image in G/N (also known as the contraction of D with respect to the kernel N) is the multi-set $D/N = \psi(D) = \{dN : d \in D\}$. We write $\psi(D) = \sum_{t_j \in G} d_j t_j N$, where the integer $d_j = |D \cap t_j N|$ is known as the **intersection number** of D with respect to N. In this work, we shall always use the notation $\hat{D}$ for $\psi(D)$ and denote the number of times d_i equals i by $m_i \geq 0$. The symbol $\Omega_{G/N}$ represents the set of inequivalent difference set images in G/N. Also, the phrase **group** $|G/N|$ stands for groups of order $|G/N|$. The following lemma is a necessary condition (but not sufficient) for the existence of difference set image in G/N. It describes the distribution of the intersection numbers of difference set image in G/N.

Lemma 2.1. *(The Variance Technique). Suppose that G is a group of order v and N is a normal subgroup of G. Let D be a difference set in G and its image in G/N be $\hat{D}$. Suppose that T^* is a left transversal of N in G such that $\{d_i\}$ is a sequence of intersection numbers and $\{m_i\}$, where m_i the number of times d_i equals i. Then*

$$\sum_{i=0}^{|N|} m_i = |G/N|, \tag{2.2}$$

$$\sum_{i=0}^{|N|} i m_i = k, \tag{2.3}$$

$$\sum_{i=0}^{|N|} i(i-1) m_i = \lambda(|N| - 1). \tag{2.4}$$

2.2. **A little about representation and algebraic number theories.** A $\mathbb{C}$- representation of G is a homomorphism, $\chi : G \to GL(d, \mathbb{C})$, where $GL(d, \mathbb{C})$ is the group of invertible $d \times d$ matrices over $\mathbb{C}$. The positive integer d is the degree of χ. A linear representation(character) is a representation of degree one. The set of all linear representations of G is denoted by G^*. G^* is an abelian group under multiplication and if G' is the derived group of G, then G^* is isomorphic to G/G'. A representation is said to be non trivial if there exist $x \in G$ such that $\chi(x) \neq I_d$, where I_d is the $d \times d$ identity matrix and d is the degree of the representation. The least positive integer m' is the exponent of the group G if $g^{m'} = 1$ for all $g \in G$. If $\zeta_{m'} := e^{\frac{2\pi}{m'} i}$ is a primitive m'-th root of unity, then $K_{m'} := \mathbb{Q}(\zeta_{m'})$ (known as the splitting field of G) is the cyclotomic extension of the field of rational numbers, $\mathbb{Q}$. Without loss of generality, we may replace $\mathbb{C}$ by the field $K_{m'}$. This field is a Galois extension of degree $\phi(m')$, where ϕ is the Euler function. If G is a cyclic group, then a basis for $K_{m'}$ over $\mathbb{Q}$ is $S = \{1, \zeta_{m'}, \zeta_{m'}^2, \dots, \zeta_{m'}^{\phi(m')-1}\}$. S is also the integral basis for $\mathbb{Z}[\zeta_{m'}]$. With this background and for any abelian group G, we define the central primitive idempotents in $\mathbb{C}[G]$ as

$$e_{\chi_i} = \frac{\chi_i(1)}{|G|} \sum_{g \in G} \chi_i(g) g^{-1} = \frac{1}{|G|} \sum_{g \in G} \overline{\chi_i(g)} g, \tag{2.5}$$

where χ_i is an irreducible character of G. The set $\{e_{\chi_i} : \chi_i \in G^*\}$ is a basis for $\mathbb{C}[G]$. Notice that $\sum e_\chi = 1$ and every element $A \in \mathbb{C}[G]$ can be expressed uniquely by its image under the character $\chi \in G^*$, where G is an abelian group. That is, $A = \sum_{\chi \in G^*} \chi(A) e_\chi$.

If χ is a representation of G and σ is a Galois automorphism of K_m fixing $\mathbb{Q}$. For any $g \in G$, σ acts on the entries of the matrix $\chi(g)$ in the natural way and the function $\sigma(\chi)$ is also a group representation. In this case, χ and $\sigma(\chi)$ are algebraically conjugate. It is easy to see that algebraic conjugacy is an equivalence relation. We say that two difference sets D and D' are equivalent if there exist a group element g and automorphism σ such that $D = g\sigma(D')$.

This brings us to an instrument, called an alias that is an interface between the values of group rings and combinatorial analysis. Aliases are members of group ring. They enable us to transfer information from $\mathbb{C}[G]$ to group algebra $\mathbb{Q}[G]$ and then to $\mathbb{Z}[G]$. Let G be an abelian group and $\Omega = \{\chi_1, \chi_2, \cdots, \chi_h\}$ be the set of characters of G. The element $\beta \in \mathbb{Z}[G]$ is known as Ω**-alias** if for $A \in \mathbb{Z}[G]$ and all $\chi_i \in \Omega$, $\chi_i(A) = \chi_i(\beta)$. Since $A = \sum_{\chi \in G^*} \chi(A) e_\chi$, we can replace the occurrence of $\chi(A)$, which is a complex number by Ω-alias, β, an element of $\mathbb{Z}[G]$. Furthermore, two characters of G are algebraic conjugate if and only if they have the same kernel and we denote the set of equivalence classes of G^* by $G^*/\sim$. Primitive idempotents give rise to rational idempotents as follows: If $K_{m'}$ is the Galois over $\mathbb{Q}$, then **central rational idempotents** in $\mathbb{Q}[G]$ are obtained by summing over the equivalence classes $X_i = \{e_{\chi_i} | \chi_i \sim \chi_j\} \in G^*/\sim$ on the e_χ's under the action of the Galois group of $K_{m'}$ over $\mathbb{Q}$. That is,

$$[e_{\chi_i}] = \sum_{e_{\chi_j} \in X_i} e_{\chi_j}, i = 1, \dots, s.$$

In particular, if G is a cyclic group of the form $C_{p^m} = \langle x : x^{p^m} = 1 \rangle$ (p is prime) whose characters are of the form $\chi_i(x) = \zeta_{p^m}^i, i = 0, \dots, p^m - 1$, then the rational idempotents are:

$$[e_{\chi_0}] = \frac{1}{p^m} \langle x \rangle, \tag{2.6}$$

and $0 \le j \le m-1$

$$[e_{\chi_{p^j}}] = \frac{1}{p^{j+1}} \left(p \langle x^{p^{m-j}} \rangle - \langle x^{p^{m-j-1}} \rangle \right). \tag{2.7}$$

The following is the general formula employed in the search of difference set [7].

Theorem 2.2. *Let G be an abelian group and $G^*/\sim$ be the set of equivalence classes of characters. Suppose that $\{\chi_o, \chi_1, \ldots, \chi_s\}$ is a system of distinct representatives for the equivalence classes of $G^*/\sim$. Then for $A \in \mathbb{Z}[G]$, we have*

$$A = \sum_{i=o}^{s} \alpha_i [e_{\chi_i}], \tag{2.8}$$

where α_i is any χ_i-alias for A.

Equation (2.8) is known as **the rational idempotent decomposition** of A. Suppose that χ is any non-trivial representation of degree d and $\chi(\hat{D}) \in \mathbb{Z}[\zeta]$, where ζ is the primitive root of unity. Suppose that $x \in G$ is a non identity element. Then, $\chi(xG) = \chi(x)\chi(G) = \chi(G)$. This shows that $(\chi(x)-1)\chi(G) = 0$. Since x is not an identity element, $(\chi(x)-1) \neq 0$ and $\chi(G) = 0$ ($\mathbb{Z}[\zeta]$ is an integral domain). Consequently, $\chi(D)\overline{\chi(D)} = n \cdot I_d + \lambda\chi(G) = n \cdot I_d$, where I_d is the $d \times d$ identity matrix. The following lemma extends this property to $\hat{D}$.

Lemma 2.3. *Let D be a difference set in a group G and N be a normal subgroup of G. Suppose that $\psi : G \longrightarrow G/N$ is a natural epimorphism. Then*

(1) $\hat{D}\hat{D}^{(-1)} = n \cdot 1_{G/N} + |N|\lambda(G/N)$
(2) $\sum d_i^2 = n + |N|\lambda$
(3) $\chi(\hat{D})\overline{\chi(\hat{D})} = n \cdot I_d$, where χ is a non-trivial representation of G/N of degree d and I_d is a d-squared identity matrix.

The character value of $\chi(\hat{D})$ is given by the following lemma.

Lemma 2.4. *Suppose that G is group of order v with normal subgroup N such that G/N is abelian. If $\hat{D} \in \mathbb{Z}[G/N]$ and $\chi \in (G/N)^*$, then*

$$|\chi(\hat{D})| = \begin{cases} k, & \text{if } \chi \text{ is a principal character of } G/N \\ \sqrt{k-\lambda}, & \text{otherwise.} \end{cases}$$

The method used in this paper is known as representation theoretic method made popular by Leibler(of blessed memory) [7]. Some authors like Iiams[8] and Smith [9] have used this method in search of difference sets. This approach entails obtaining comprehensive lists $\Omega_{G/N}$, of difference set image distribution in factor groups of G. We first find the difference set image in factor group of least order. We garner more information about D as we gradually increase the size of the factor group and compute $\Omega_{G/N}$. If at a point the distribution list $\Omega_{G/N}$ is empty, then it follows that any group G having G/N as a factor group does not admit (v, k, λ) difference sets. We use lemmas 2.3, 2.4 and the difference set equation (2.8) to $\Omega_{G/N}$.

To successfully obtain the difference set images, we need the aliases. Suppose that G/N is an abelian factor group of exponent m' and $\hat{D}$ is a difference set image in G/N. If χ is not a principal character of G/N, then by Lemma 2.3, $\chi(\hat{D})\overline{\chi(\hat{D})} = n$. The determination of the alias requires the knowledge of how the ideal generated by $\chi(\hat{D})$ factors in cyclotomic ring $\mathbb{Z}[\zeta_{m'}]$, where $\zeta_{m'}$ is the m'-th root of unity. Notice that $\chi(\hat{D})\overline{\chi(\hat{D})} = n$ is an algebraic equation in $\mathbb{Z}[\zeta_{m'}]$ and $\chi(\hat{D})$ is an algebraic number of length $\sqrt{n}$. The image of $\mathbb{Z}[G/N]$ is $\mathbb{Z}[\zeta_{m'}]$. For the purpose of this paper, $n = 7^2$ and we require how the ideal generated by 7 factors in $\mathbb{Z}[\zeta_{m'}]$, $m' = 2$, 4, 5, 8, 10, 14, 20, 28, 56 and 70. If $\delta := \chi(\hat{D})$, then by (2.8), we seek a group ring, $\mathbb{Z}[G/N]$ element say α such that $\chi(\alpha) = \delta$. The task of solving the algebraic equation $\delta\bar{\delta} = n$ is sometimes made easier if we consider the factorization of principal ideals $\langle\delta\rangle\langle\bar{\delta}\rangle = \langle n\rangle$. To achieve this,

(1) we must look for all principal ideals $\pi \in \mathbb{Z}[\zeta_m]$ such that $\pi\bar{\pi} = \langle n\rangle$
(2) for each such ideals, we find a representative element, say δ with $\delta\bar{\delta} = n$ and
(3) for each δ, we find an alias $\alpha \in \mathbb{Z}[G/N]$ such that $\chi(\alpha) = \delta$.

Using algebraic number theory, we can easily construct the ideal π. The daunting task is to find an appropriate element $\delta \in \pi$. Suppose we are able to find $\delta = \sum_{i=0}^{\phi(m')-1} d_i\zeta_{m'}^i \in \mathbb{Z}[\zeta_{m'}]$ such that $\delta\bar{\delta} = n$, where ϕ is the Euler ϕ-function. A theorem due to Kronecker [10, 11] states that any algebraic integer all whose conjugates have absolute value 1 must be a root of unity. If there is any other solution to the algebraic equation, then it must be of the form $\delta' = \delta u$[12], where $u = \pm\zeta_{m'}^j$ is a unit. To construct alias from this information, we choose a group element g that is mapped to ζ_m and set $\alpha := \sum_{i=0}^{\phi(m')-1} d_i g^i$ such that $\chi(\alpha) = \delta$. Hence, the set of complete aliases is $\{\pm\alpha g^j : j = 0, 1, \ldots, m' - 1\}$.

The following result is used to determine the number of factors of an ideal in a ring: Suppose p is any prime and m' is an integer such that $\gcd(p, m') = 1$. Suppose that d is the order of p in the multiplicative group $\mathbb{Z}_{m'}^*$ of the modular number ring $\mathbb{Z}_{m'}$. Then the number of prime ideal factors of the principal ideal $\langle p\rangle$ in the cyclotomic integer ring $\mathbb{Z}[\zeta_{m'}]$ is $\frac{\phi(m')}{d}$, where ϕ is the Euler ϕ-function, i.e. $\phi(m') = |\mathbb{Z}_{m'}^*|$ [13]. For instance, the ideal generated by 2 has two factors in $\mathbb{Z}[\zeta_7]$, the ideal generated by 7 has two factors in $\mathbb{Z}[\zeta_{20}]$, while the ideal generated by 7 has four factors in $\mathbb{Z}[\zeta_{40}]$. On the other hand, since 2^s is a power of 2, then the ideal generated by 2 is said to completely ramifies as power of $\langle 1 - \zeta_{2^s}\rangle = \overline{\langle 1 - \zeta_{2^s}\rangle}$ in $\mathbb{Z}[\zeta_{2^s}]$. The ideal generated by 7 ramifies in the cyclotomic ring $\mathbb{Z}[\zeta_{m'}]$, $m' = 7, 14, 28, 35, 70$.

According to Turyn [14], an integer n is said to be semi-primitive modulo m' if for every prime factor p of n, there is an integer i such that $p^i \equiv -1 \mod m'$. In this case, -1 belongs to the multiplicative group generated by p. Furthermore, n is self conjugate modulo m' if every prime divisor of n is semi primitive modulo m'_p, m'_p is the largest divisor of m' relatively prime to p. This means that every prime ideals over n in $\mathbb{Z}[\zeta_{m'}]$ are fixed by complex conjugation. For instance, $7^2 \equiv -1 \pmod{m'}$, where $m' = 2, 5, 10, 50$ and $7 \equiv -1 \pmod{m'}$, $m' = 2, 4, 8$. Thus, $\langle 7 \rangle$ is fixed by conjugation in $\mathbb{Z}[\zeta_{m'}]$, $m' = 2, 4, 5, 8, 10, 50$. In this paper, we shall use the phase m **factors trivially** in $\mathbb{Z}[\zeta_{m'}]$ if the ideal generated by m is prime (or ramifies) in $\mathbb{Z}[\zeta_{m'}]$ or m is self conjugate modulo m'. Since $7 \equiv -1 \pmod 8$, the ideal generated by 7 also factors trivially in the ring $\mathbb{Z}[\zeta_{56}]$. In summary, if $\hat{D}$ is the difference set image of order 7^2 in the cyclic factor group G/N, a group with exponent m', where $m' = 2, 4, 5, 8, 10, 14, 28, 35, 56, 70$ and χ is a non trivial representation of G/N, then $\chi(\hat{D}) = \pm 7\zeta_{m'}^i$, $\zeta_{m'}$ is the m'-th root of unity [11].

Furthermore, the ideal generated by 7 has two factors in $\mathbb{Z}[\zeta_{20}]$. Suppose $\sigma \in Gal(\mathbb{Q}(\zeta_{20})/\mathbb{Q})$, where $\sigma(\zeta_{20}) = \zeta_{20}^7$. This automorphism split the basis elements of $\mathbb{Q}(\zeta_{20})$ into two orbits as $\zeta_{20} + \zeta_{20}^7 + \zeta_{20}^9 + \zeta_{20}^3$ and $\zeta_{20}^{11} + \zeta_{20}^{17} + \zeta_{16}^{19} + \zeta_{16}^{13}$. Take $\theta = \zeta_{20} + \zeta_{20}^7 + \zeta_{20}^9 + \zeta_{20}^3$. It follows that $\overline{\theta} = -\theta$ and $\theta\overline{\theta} = -\theta^2 = 5$. This implies that $\theta = i\sqrt{5}$, where i is the fourth root of unity. Thus, $\delta \in \mathbb{Z}[\theta]$, whose basis elements are $\{1, \theta\}$. Consequently, we need $a, b \in \mathbb{Z}$ with $\delta = a + b\theta$ such that $\delta\overline{\delta} = 49$. This condition generates the equation $a^2 - 5b^2 = 49$. The solutions to this equation are $(a, b) = (\pm 7, 0)$ and $(\pm 2, \pm 3)$. Hence, $\delta = \pm 7$, $\pm(2 + 3\theta)$ or $\pm(2 + 3\overline{\theta})$. Consequently, if $\hat{D}$ is a (280, 63, 14) difference set image in $C_{m'}$ and χ is any non-trivial character of $C_{m'}$ such that $\chi(\hat{D})\overline{\chi(\hat{D})} = 49$. Then $\chi(D)$ is $\pm 7\zeta_{20}^j$, $(2 + 3(\zeta_{20} + \zeta_{20}^3 + \zeta_{20}^7 + \zeta_{20}^9)\zeta_{20}^j$ or $(-2 + 3(\zeta_{20} + \zeta_{20}^3 + \zeta_{20}^7 + \zeta_{20}^9)\zeta_{20}^j$, $j = 0, \ldots, 19$.

Based on the above information, we now state the aliases that will be used later. If $\hat{D}$ is a (280, 63, 14) difference set in $C_{m'}$, where $m' = 2, 4, 5, 8, 10, 14, 28, 35, 70$, then the possible alias α in the rational idempotent decomposition of $\hat{D}$ is $\pm 7x^r$, where x is the generator of $C_{m'}$ and $r = 0, 1, \ldots, m' - 1$. On the other hand, if $\hat{D}$ is a (280, 63, 14) difference set in C_{20}, then the possible alias α in the rational idempotent decomposition of $\hat{D}$ is one of the two forms

- $\pm 7x^r$, x is a generator of C_{20}
- $\pm(2 + 3(x + x^3 + x^7 + x^9))g$ or $\pm(-2 + 3(x + x^3 + x^7 + x^9))g$, x is a generator of C_{20} and $g \in C_{20}$ and $r = 0, \ldots, 19$.

2.3. **Characteristics of difference set images in subgroup of a group.** In this subsection, we use the attributes of subgroups of a group to obtain information about the difference set image in the factor groups. Dillon [15] proved the following results which will be used to obtain difference set images in dihedral group of a certain order if the difference images in the cyclic group of same order are known.

Theorem 2.5 (Dillon Dihedral Trick)**.** *Let H be an abelian group and let G be the generalized dihedral extension of H. That is, $G = \langle Q, H : Q^2 = 1, QhQ = h^{-1}, \forall h \in H\rangle$. If G contains a difference set, then so does every abelian group which contains H as a subgroup of index 2.*

Corollary 2.6. *If the cyclic group Z_{2m} does not contain a (nontrivial) difference set, then neither does the dihedral group of order $2m$.*

Finally, we look at subgroup properties of a group that can aid the construction of difference set image. For the convenience of the reader, we reproduce the idea of Gjoneski, Osifodunrin and Smith[4] with some additions. Suppose that H is a group of order $2h$ with a central involution z. We take $T = \{t_i : i = 1, \ldots, h\}$ to be the transversal of $\langle z\rangle$ in H so that every element in H is viewed as $t_i z^j, 0 \leq i \leq h, j = 0, 1$. Denote the set of all integral combinations, $\sum_{i=1}^{h} a_i t_i$ of elements of $T, a_i \in \mathbb{Z}$ by $\mathbb{Z}[T]$. The subgroup $\langle z\rangle$ has two irreducible representations: $z \mapsto 1$ or $z \mapsto -1$. Let φ_0 be the representation induced on H by the trivial representation $z \mapsto 1$ and φ_1 be the representation induced on H by the non trivial representation $z \mapsto -1$. Using the Frobenius reciprocity theorem [16], every irreducible representation of H is a constituent of φ_0 or φ_1. Thus, we may write any element X of the group ring $\mathbb{Z}[H]$ in the form

$$X = X\left(\frac{1+z}{2}\right) + X\left(\frac{1-z}{2}\right). \tag{2.9}$$

Let A be the group ring element created by replacing every occurrence of z in X by 1. Also, let B be the group ring element created by replacing every occurrence of z in H by -1. Then

$$X = A\left(\frac{\langle z\rangle}{2}\right) + B\left(\frac{2 - \langle z\rangle}{2}\right), \tag{2.10}$$

where $A = \sum_{i=1}^{h} a_i t_i$ and $B = \sum_{j=1}^{h} b_j t_j, a_i, b_j \in \mathbb{Z}$. As $X \in \mathbb{Z}[H]$, A and B are both in $\mathbb{Z}[T]$ and $A \equiv B \mod 2$. We may equate A with the homomorphic image of X in $G/\langle z\rangle$. Consequently, if X is a difference set, then the coefficients of t_i in the expression for A will be intersection number of X in the coset $\langle z\rangle$. In particular, if K is a subgroup of H such that

$$H \cong K \times \langle z\rangle, \tag{2.11}$$

then we may assume that A and B are in the group ring $\mathbb{Z}[K]$ and $BB^{(-1)} = (k - \lambda) \cdot 1$. The search for the homomorphic image A in K gives considerable information about the element B. We describe B in terms of A as follows: If the structure of a group H is like (2.11), then the characters of the group are induced by those of K and $\langle z\rangle$. Let $\varphi_{0,0}$ be the characters of H induced by both trivial characters of K and $\langle z\rangle$; $\varphi_{1,s}$, induced by non-trivial characters of K and $\langle z\rangle$; $\varphi_{1,0}$, induced by trivial character of K and non-trivial character of $\langle z\rangle$ while $\varphi_{0,s}$, is the character induced by non-trivial characters of K and trivial character of $\langle z\rangle$. Suppose that A is a difference set image in K. Then by Lemma 2.4,

$$\varphi_{0,0}(A) = k, |\varphi_{0,s}(A)| = \sqrt{n}, |\varphi_{1,0}(B)| = \sqrt{n}, |\varphi_{1,s}(B)| = \sqrt{n}. \quad (2.12)$$

The identity element of $\mathbb{Z}[K]$ is K and since A is a rational idempotent, it is of the form $\frac{Y}{|K|}, Y \in \mathbb{Z}[K]$. We subtract $k+\sqrt{n}$ or $k-\sqrt{n}$ multiples of $\frac{K}{|K|}$ from both sides of $\varphi_{0,0}(A) = k$ to get $|\varphi_{0,0}(A - (\frac{k+\sqrt{n}}{|K|})K)| = \sqrt{n}$ or $|\varphi_{0,0}(A - (\frac{k-\sqrt{n}}{|K|})K)| = \sqrt{n}$. Set $\alpha = \frac{k+\sqrt{n}}{|K|}$ or $\alpha = \frac{k-\sqrt{n}}{|K|}$ and $B = A - \alpha K$, k is the size of difference set. The entries of A are non-negative integers and if $|K|$ divides $k+\sqrt{n}$ or $k-\sqrt{n}$, then $BB^{(-1)} = (k-\lambda)\cdot 1$ and

$$\hat{D} = A\left(\frac{\langle z\rangle}{2}\right) + gB\left(\frac{2-\langle z\rangle}{2}\right), \quad (2.13)$$

$g \in H$. (2.13) can be used to determine the existence or otherwise of difference set image in H. However, this approach fails to yield a definite result if $|K| \nmid (k+\sqrt{n})$ and $|K| \nmid (k-\sqrt{n})$. To buttress the point being made here, consider the parameter set (70, 24, 8) in the group $C_{70} \cong C_{35} \times C_2$. Take $K = C_{35}$. This shows that $|K| = 35$ and 35 does not divide (24 + 4) or (24 - 4). It is known that the group C_{70} does not admit this difference set([1], Table 6-1). On the other hand, consider (320, 88, 24) difference set in the group $H = (C_2)^6 \times C_5$. Take $K = (C_2)^5 \times C_5$ and $|K| = 160$. Also 160 does not divide (88 + 8) or (88 - 8). Davis and Jedwab[17] constructed (320, 88, 24) difference set in H.

The process of obtaining difference set in any group G starts with the computation of difference set images in G/N, where N is an appropriate normal subgroup. In the next two sections, we shall analyze the non-existence of difference set images in factor groups of orders 20, 40, 56 and 70.

3. Difference set images in some factor groups of orders 8, 20 and 40

3.1. **The Group 8 images.** We first obtain (280, 63, 14) difference set images in groups of order 8.

3.1.1. *The C_2 image.* Suppose that $G/N \cong C_2 = \langle x : x^2 = 1\rangle$ and $\hat{D} = d_0 + d_1x$ is the (280, 63, 14) difference set image in G/N. The characters of G/N are of the form $\chi_j(x) = (-1)^j$, $j = 0, 1$. By applying $x \mapsto 1$ to $\hat{D}$, we get $d_0 + d_1 = 63$ while $x \mapsto -1$ on $\hat{D}$ yields $d_0 - d_1 = 7$ or -7. We translate $\hat{D}$ if necessary to get $d_0 - d_1 = 7$. By solving the system $d_0 + d_1 = 63$ and $d_0 - d_1 = 7$, up to equivalence, the difference set image is $A = 35 + 28x$.

3.1.2. *The C_4 image.* Suppose that $G/N \cong C_4 = \langle x : x^4 = 1\rangle$ and $\hat{D} = \sum_{s=0}^{3} d_s x^s$ is the (280, 63, 14) difference set image in G/N. We view this group ring element as a 1×4 matrix with columns indexed by powers of x. Using (2.6) and (2.7), the rational idempotents of G/N are $[e_{\chi_0}] = \frac{1}{4}\langle x\rangle$, $[e_{\chi_2}] = \frac{1}{4}(2\langle x^2\rangle - \langle x\rangle)$ and $[e_{\chi_1}] = \frac{1}{2}(2 - \langle x^2\rangle)$. The first two rational idempotents have $\langle x^2\rangle$ in their kernel and the linear combination of these idempotents is written as $\alpha_{\chi_0}[e_{\chi_0}] + \alpha_{\chi_2}[e_{\chi_2}] = A\frac{\langle x^2\rangle}{2}$, where A is the difference set image in C_2. The difference set image is $\hat{D} = \sum_{j=0}^{2} \alpha_{\chi_j}[e_{\chi_j}] = A\frac{\langle x^2\rangle}{2} + \alpha_{\chi_1}[e_{\chi_1}]$. As $\chi_1(\hat{D})(\overline{\chi_1(\hat{D})}) = 49 = (7)(7)$, $\alpha_{\chi_1} = \pm 7x^s$ and the difference set image is

$$\hat{D} = A\frac{\langle x^2\rangle}{2} \pm 7x^s[e_{\chi_1}], \tag{3.1}$$

$s = 0, 1, 2, 3$. By translating, if necessary, the distribution scheme, Ω_{C_4} for C_4 (up to translation) consists of only $A_1 = 7 + 14\langle x\rangle$.

3.1.3. *The $C_2 \times C_2$ image.* Using (2.13) with $\alpha = 28$, $K = C_2$ and $|K| = 2$, the difference set image in $C_2 \times C_2 = \langle x, y : x^2 = y^2 = 1 = [x, y]\rangle$ is $A_2 = 7 + 14(1 + x)(1 + y)$.

3.1.4. *The C_8 images.* Suppose that $G/N \cong C_8 = \langle x : x^8 = 1\rangle$ and $\hat{D} = \sum_{s=0}^{7} d_s x^s$ is the (280, 63, 14) difference set image in G/N. We view this group ring element as a 1×8 matrix with columns indexed by powers of x. Using (2.6) and (2.7), the rational idempotents of C_8 are $[e_{\chi_0}] = \frac{1}{8}\langle x\rangle$, $[e_{\chi_1}] = \frac{1}{2}(2 - \langle x^4\rangle)$, $[e_{\chi_4}] = \frac{1}{4}(2\langle x^4\rangle - \langle x^2\rangle$ and $[e_{\chi_2}] = \frac{1}{8}(2\langle x^2\rangle - \langle x\rangle)$. The difference set image is $\hat{D} = \sum_{j=0,1,2,4} \alpha_{\chi_j}[e_{\chi_j}]$. The linear combination of the rational idempotents having $\langle x^4\rangle$ in their kernel is $\frac{A_1}{2}\langle x^4\rangle = \alpha_1[e_{\chi_0}] + \alpha_2[e_{\chi_2}] + \alpha_3[e_{\chi_4}]$, where α_j is an appropriate alias and A_1 is the only difference image in C_4. Thus, the difference set image becomes

$$\hat{D} = \frac{A_1}{2}\langle x^4\rangle + \pm 7x^s[e_{\chi_1}]. \tag{3.2}$$

Up to translation, the only element in Ω_{C_8} is $A' = 7 + 7\langle x\rangle$.

3.1.5. *The D_4 image.* Suppose that $G/N \cong D_4 = \langle x, y : x^4 = y^2 = 1, yxy = x^{-1}\rangle$. Let $\hat{D} = \sum_{t=0}^{1}\sum_{s=0}^{3} d_{st}x^s y^t$ be the difference set image in G/N. Using Dillon Dihedral trick, it can be shown that $B_1' = 7 + 7\langle x\rangle\langle y\rangle$ is the only element of Ω_{D_4} up to equivalence.

3.1.6. *The $C_4 \times C_2$ image.* Consider $G/N \cong C_4 \times C_2 = \langle x, y : x^4 = y^2 = 1 = [x, y]\rangle$. We view the difference set image $\hat{D} = \sum_{i=0}^{3}\sum_{j=0}^{1} d_{ij}x^i y^j$ in $C_4 \times C_2$ as a 2×4 array with columns indexed by powers of x and rows indexed by powers of y. Using (2.13) with $\alpha = 14$, $|K| = 4$, and $B_j = A_1 - 14K$, where $A_1 \in \Omega_{C_4}$, $B_2' = 7 + 7\langle x\rangle\langle y\rangle$ is the only viable difference set image in $C_4 \times C_2$ up to equivalence.

3.1.7. *The* $(C_2)^3$ *image.* Suppose that $G/N \cong (C_2)^3 = \langle a, b, c : a^2 = b^2 = c^2 = 1 = [a, b] = [b, c] = [a, c]\rangle$. Take $K = (C_2)^2$, $|K| = 4$, and $B_j = A - 14K$, where $A \in \Omega_{C_2 \times C_2}$. By (2.13), $B'_3 = 7 + 7(1 + a)(1 + b)(1 + c)$ is the only viable difference set image in $(C_2)^3$ up to equivalence.

3.1.8. *The* Q_4 *image.* Consider $G/N \cong Q_4 = \langle x, y : x^4 = 1, xy = yx^{-1}, x^2 = y^2\rangle$. The derived subgroup of G/N is isomorphic to $\langle x^2\rangle$. Let the difference set image in G/N be $\hat{D} = \sum_{t=0}^{1}\sum_{s=0}^{3} d_{st}x^s y^t$. We view this object as a 2×4 matrix with rows indexed by powers of y and columns indexed by powers of x. Since $Q_4/\langle x^2\rangle \cong C_2 \times C_2$, G/N has four characters. By applying these four characters to $\hat{D}$, we get $A^* = \frac{1}{2}\begin{bmatrix} 21 & 14 & 21 & 14 \\ 14 & 14 & 14 & 14 \end{bmatrix}$. The Only degree two representation of G/N is

$$\chi : x \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad y \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

In non abelian group like this, the idempotents are obtained by applying the diagonal entries of χ to $\hat{D}$. Thus, the idempotents are:

$f = \frac{1}{4}\begin{bmatrix} 1 & -i & -1 & i \\ 0 & 0 & 0 & 0 \end{bmatrix}, \bar{f} = \frac{1}{4}\begin{bmatrix} 1 & i & -1 & -i \\ 0 & 0 & 0 & 0 \end{bmatrix}$

$f_y = \frac{1}{4}\begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & -i & -1 & i \end{bmatrix}, \bar{f}_y = \frac{1}{4}\begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & i & -1 & -i \end{bmatrix}.$

Therefore, the two rational idempotents (from χ) are:

$[f] = f + \bar{f} = \frac{1}{4}\begin{bmatrix} 2 & 0 & -2 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$ and $[f_y] = f_y + \bar{f}_y = \frac{1}{4}\begin{bmatrix} 0 & 0 & 0 & 0 \\ 2 & 0 & -2 & 0 \end{bmatrix}.$

Consequently, the difference set equation is

$$\hat{D} = A^* + \alpha_1[f] + \alpha_2[f_y], \tag{3.3}$$

where $\alpha_j, j = 1, 2$ is an alias. To find the aliases, α_j, we apply χ to $\hat{D}$ and hence,

$$\chi(\hat{D}) = \begin{pmatrix} z & w \\ \overline{w} & \overline{z} \end{pmatrix},$$

where $z = (d_{00} - d_{20}) + (d_{10} - d_{30})i$ and $w = (d_{01} - d_{21}) + (d_{11} - d_{31})i$, $w, z \in \mathbb{Z}[i]$. Thus,

$$\chi(\hat{D})\overline{(\chi\hat{D})} = \begin{pmatrix} z\overline{z} + w\overline{w} & 0 \\ 0 & z\overline{z} + w\overline{w} \end{pmatrix} = 49I_2,$$

and $z\overline{z} + w\overline{w} = 49$. By expanding this equation, we get,

$$(d_{00} - d_{20})^2 + (d_{10} - d_{30})^2 + (d_{01} - d_{21})^2 + (d_{11} - d_{31})^2 = 49 \tag{3.4}$$

Up to permutations, the set of all possible values satisfying (3.4) are listed in Table 1.

Our next task is to find all sets of equivalent solutions to 3.4. The following facts assist with this objective:

TABLE 1. possible coefficients

S/N	$d_{00} - d_{20}$	$d_{10} - d_{30}$	$d_{01} - d_{21}$	$d_{11} - d_{31}$
i.	± 7	0	0	0
ii.	$\pm$ 6	± 3	± 2	0
iii.	± 5	± 4	± 2	± 2
iv.	± 4	± 4	± 4	± 1

(1) $\{1, i\}$ is a basis of $\mathbb{Z}[i]$ and if necessary, we can replace either z or w with zi^k or wi^j or their conjugates, where i, is the fourth root of unity
(2) in (3.3), observe that 2 entries of A^* are congruent to $1 \mod 2$ while 6 entries are congruent to zero modulo $\mod 2$.
(3) The sum of the last two terms in (3.3), must have property 2 also

Hence, up to negatives and permutations, we consider only the coefficients in Table 2. Therefore, we choose aliases according to values in

TABLE 2. possible coefficients

S/N	$d_{00} - d_{20}$	$d_{10} - d_{30}$	$d_{01} - d_{21}$	$d_{11} - d_{31}$
i.	7	0	0	0
ii.	3	6	2	0
iii.	3	2	6	0
iv.	3	0	6	2
v.	1	4	4	4
vi.	5	4	2	2
vii.	5	2	4	2

table 2. Up to equivalence, the following are the elements of Ω_{Q_4}:

- $F_1 = 7+7\langle x\rangle\langle y\rangle$, $F_2 = 12+10x+9x^2+4x^3+8y+7xy+6x^2y+7x^3y$
- $F_3 = 12 + 8x + 9x^2 + 6x^3 + 10y + 7xy + 4x^2y + 7x^3y$, $F_4 = 12 + 7x + 9x^2 + 7x^3 + 10y + 8xy + 4x^2y + 6x^3y$
- $F_5 = 11 + 9x + 10x^2 + 5x^3 + 9y + 9xy + 5x^2y + 5x^3y$, $F_6 = 13 + 9x + 8x^2 + 5x^3 + 8y + 8xy + 6x^2y + 6x^3y$
- $F_7 = 13 + 8x + 8x^2 + 6x^3 + 9y + 8xy + 5x^2y + 6x^3y$.

3.2. **Difference set images in factor groups of order 20.** In this section, we show that some factor groups of order 20 and 40 do not admit (280, 63, 14) difference sets. First, we give the difference set images in factor groups of orders 5 and 10.

3.3. **The C_5 image.** Suppose that $G/N \cong C_5 = \langle x : x^5 = 1\rangle$. Then the difference set image is $A' = -7 + 14\langle x\rangle$.

3.4. **The C_{10} and D_5 images.** Suppose that $G/N \cong C_{10} = \langle x, y : x^5 = y^2 = [x, y] = 1\rangle$. Since $C_{10} \cong C_5 \times C_2$, we can use (2.13) with $\alpha = 14$, $|K| = 5$, and $B_j = A' - 14K$, where A' is the C_5 image. Thus, the difference set image is $E = -7 + 7\langle x\rangle\langle y\rangle$. We can also show using Dillon trick that E is the only difference set image in $G/N \cong D_5 = \langle x, y : x^5 = y^2 = yxyx = 1\rangle$.

3.5. **There are no $C_{10} \times C_2$ and D_{10} images.** Suppose that N is a normal subgroups of G such that $G/N \cong C_{10} \times C_2$ or $D_{10} \cong D_5 \times C_2$. These groups are of the form $K \times C_2$, $K = C_{10}$ or D_5. Let z be the generator of C_2. Take $\alpha = 7$, $|K| = 10$, and $B = E - 7K$, where $E \in \Omega_{D_5}$ or $E \in \Omega_{C_{10}}$. Then, by (2.13)

$$\hat{D} = E\left(\frac{\langle z\rangle}{2}\right) + gB\left(\frac{2 - \langle z\rangle}{2}\right), \tag{3.5}$$

$g \in D_{10}$ or $g \in C_{10} \times C_2$. Notice that $E\left(\frac{\langle z\rangle}{2}\right)$ consists of 2 integers and 18 fractions while $B\left(\frac{2-\langle z\rangle}{2}\right)$ consists of 18 integers and 2 fractions. These observations show that the two terms on the right hand of (3.5) are not compatible to produce integer solutions. Hence, $(C_2)^2 \times C_5$ and D_{10} do not admit (280, 63, 14) difference sets.

3.6. **The C_{20} image.** Consider $G/N \cong C_{20} = \langle x, y : x^5 = y^4 = 1 = [x, y]\rangle$. Let $\hat{D} = \sum_{t=0}^{3}\sum_{s=0}^{4} x^s y^t$ be the difference set in G/N. We view $\hat{D}$ as a 4×5 matrix with the columns indexed by the powers of x and rows indexed by powers of y. This group has 6 rational idempotents out of which four have $\langle y^2\rangle$ in their kernel. The linear combination of these four rational idempotents is $\sum_{j=0,1}\sum_{k=0,2} \alpha_{\chi_{(j,k)}}[e_{\chi_{(j,k)}}] = \frac{E}{2}\langle y^2\rangle$, where E is the difference set image in C_{10} and $\alpha_{\chi_{(j,k)}}$ is an alias. The remaining two rational idempotents are: $[e_{\chi_{(0,1)}}] = \frac{1}{10}\langle x\rangle(1 - y^2)$ and $[e_{\chi_{(1,1)}}] = \frac{1}{10}(5 - \langle x\rangle)(1 - y^2)$. Thus, the difference set image in C_{20} is

$$\hat{D} = \frac{E}{2}\langle y^2\rangle + \alpha_{\chi_{(0,1)}}[e_{\chi_{(0,1)}}] + \alpha_{\chi_{(1,1)}}[e_{\chi_{(1,1)}}], \tag{3.6}$$

where $\alpha_{\chi_{(1,1)}} \in \{\pm 7(xy)^{p_1}, (2 + 3(x + x^3 + x^7 + x^9))(xy)^{p_2}, (-2 + 3(x + x^3 + x^7 + x^9))(xy)^{p_3}\}$ and $\alpha_{\chi_{(0,1)}} \in \{\pm 7(xy)^{p_4}\}$, $p_1, p_2, p_3, p_4 = 0, \ldots, 19$. Put

$B_1 = (2+3(xy+(xy)^3+(xy)^7+(xy)^9)[e_{\chi_{(1,1)}}] = \frac{1}{10}\big((10-2\langle x\rangle)+15(x-x^2-x^3+x^4)-(10-2\langle x\rangle)-15(x-x^2-x^3+x^4)\big)$, $B_2 = (-2+3(xy+(xy)^3+(xy)^7+(xy)^9)[e_{\chi_{(1,1)}}] = \frac{1}{10}\big(-(10-2\langle x\rangle)+15(x-x^2-x^3+x^4)-(10-2\langle x\rangle)-15(x-x^2-x^3+x^4)\big)$, $B_3 = 7[e_{\chi_{(1,1)}}] = \frac{7}{10}\big((5-\langle x\rangle)-(5-\langle x\rangle)\big)$, and $C = 7[e_{\chi(0,1)}] = \frac{7}{10}\langle x\rangle(1-y^2)$. Then (3.6) becomes

$$\hat{D} = \frac{E}{2}\langle y^2\rangle \pm x^t y^s B_l \pm y^j C, t = 0, \cdots, 4; s, j = 0, 1, 2, 3; l = 1, 2, 3 \quad (3.7)$$

Observe that 18 entries of $\frac{E}{2}\langle y^2\rangle$ are congruent to $10 \mod 20$ while the remaining entries are congruent to $0 \mod 20$. This condition implies that solution exist if 18 entries of $\pm x^t y^s B_l \pm y^j C$ are congruent to $10 \mod 20$ while the remaining entries are congruent to $0 \mod 20$. Thus, (3.7) has solutions if and only if $t = 0$, $l = 1$ and $s = j$. Up to equivalence, the unique difference set image is $E' = 2x + 5x^2 + 5x^3 + 2x^4 + (5 + 4x + 4x^2 + 4x^3 + 4x^4)y + (5x + 2x^2 + 2x^3 + 5x^4)y^2 + (2 + 3x + 3x^2 + 3x^3 + 3x^4)y^3$.

3.7. **The $Frob(20)$ images.** Suppose that $G/N \cong Frob(20) = C_5 \rtimes C_4 = \langle x, y : x^5 = y^4 = 1, yx = x^2y\rangle$, the Frobenius group of order 20. The Frobenius groups are finite groups with non trivial normal subgroup N' (known as Frobenius kernel) and a non trivial subgroup K', called Frobenius complement such that for each $t \in Frob(20)/N'$ there is a unique $s \in N'$ with $t \in sK's^{-1}$ and $\gcd(|N|, |K'|) = 1$. The derived group of $Frob(20)$ is a Sylow 5-subgroup, $\langle x\rangle$ and $Frob(20)/\langle x\rangle \cong C_4$. The center of this group is $C(Frob(20)) = \{1\}$. Now let $\hat{D} = \sum_{k=0}^{3}\sum_{j=0}^{4} d_{jk}x^j y^k$ be the difference set image in $Frob(20)$. Since $Frob(20)/\langle x\rangle \cong C_4$, $Frob(20)$ has four characters. These characters are of the form $\chi_j(x) = 1$ and $\chi_j(y) = i^j, j = 0, \ldots, 3$. Also, $Frob(20)$ has a degree four representation induced by the faithful characters of $\langle x\rangle$. This representation is:

$$\chi' : x \mapsto \begin{pmatrix} \zeta_5 & 0 & 0 & 0 \\ 0 & \zeta_5^2 & 0 & 0 \\ 0 & 0 & \zeta_5^4 & 0 \\ 0 & 0 & 0 & \zeta_5^3 \end{pmatrix}, \quad y \mapsto \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

and ζ_5 is the fifth root of unity.

Unlike the usual case, we avoid carrying out our computation in $\mathbb{Q}(\zeta)$, the minimal splitting field of χ', by creating integral representations which are not unitary but equivalent to χ'. The Frobenius complement $\langle y\rangle$ is a Sylow 2-subgroup of $Frob(20)$. Let $\{1, x, x^2, x^3, x^4\}$ be a left transversal of Sylow 2-subgroup of $Frob(20)$. We induce the trivial representation of this Sylow 2-subgroup to get integral-valued representation. This representation is equivalent to $\chi_0' \oplus \chi'$ and defined explicitly

as: $$\chi : x \mapsto \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}, \quad y \mapsto \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}.$$

This is also known as permutation representation of $Frob(20)$.

3.7.1. *The background work.* Let I denote a 5 by 5 identity matrix and J denote the corresponding all one matrix. Suppose that a $(280, 63, 14)$ difference set D exists in group G. Then by (2.1),

$$DD^{(-1)} = 49 \cdot 1_G + 14 \cdot G. \tag{3.8}$$

Thus, the image of this difference set in $Frob(20)$ satisfies

$$\begin{aligned} \chi(\hat{D})\overline{\chi(\hat{D})} &= 49 \cdot I + 14\chi(G) \\ &= 49 \cdot I + 14 \cdot 14 \cdot \chi(Frob(20)) \\ &= 49 \cdot I + 784 \cdot J, \end{aligned} \tag{3.9}$$

where, $\chi(Frob(20)) = 4J$, $\chi(\hat{D})J = 63J$ and $\chi(G) \neq 0$ since this representation has the trivial representation in it's constituent. Set $M = \chi(\hat{D}) - aJ$. As (3.9) does not satisfy orthogonality relations (Chapter 2 [16]), we need to find the value of a such that $(\chi(\hat{D}) - aJ)(\overline{\chi(\hat{D}) - aJ}) = 49 \cdot I + \mu J$ and μ is as small as possible. To achieve this, we multiply out the left hand side of the last equation, to get $\chi(\hat{D})\overline{\chi(\hat{D})} - a\chi(\hat{D})J - aJ\overline{\chi(\hat{D})} - a^2J^2 = 49 \cdot I + (784 - 126a + 5a^2)J$. Since we need μ as small as possible, we choose $\mu = 0$, so that $784 - 126a + 5a^2 = 0$. Using the quadratic formula, we get $a = \frac{126 \pm 14}{10}$. But a has to be an integer, so we choose $a = 14$. Thus, $(\chi(\hat{D}) - 10J)(\overline{\chi(\hat{D}) - 14J}) = 49 \cdot I$ with $M = \chi(\hat{D}) - 14J$. By implication of the above, $MJ = \chi(\hat{D})J - 14J^2 = -7J$. But $MM^t = 49 \cdot I$ implies $(\frac{1}{7}M)(\frac{1}{7}M^t) = I$, which means $\frac{1}{7}M$ and $\frac{1}{7}M^t$ are inverses of each other. Using the fact that A and B are inverses if and only if $AB = I$ and $BA = I$ then $M^tM = 49 \cdot I$. This indicates that the columns of M also preserve the properties of the rows and $JM = -7J$. In order to get more information about M,
let $\vec{a} = \begin{pmatrix} x_0 & x_1 & x_2 & x_3 & x_4 \end{pmatrix}$ be a row(column) vector in M. Thus, the above conditions indicate that inner product of this row(column) by itself, is $\vec{a} \cdot \vec{a} = x_0^2 + x_1^2 + x_2^2 + x_3^2 + x_4^2 = 49$ and row(column)sum, $\sum x_i = -7$. A careful consideration of the constraints shows that the row(column) of M will be generated by vectors (up to permutation) $\vec{a}_1 = \begin{pmatrix} -7 & 0 & 0 & 0 & 0 \end{pmatrix}$, $\vec{a}_2 = \begin{pmatrix} -6 & -3 & 2 & 0 & 0 \end{pmatrix}$,
$\vec{a}_3 = \begin{pmatrix} -6 & -2 & -2 & 2 & 1 \end{pmatrix}$, $\vec{a}_4 = \begin{pmatrix} -4 & -4 & -3 & 2 & 2 \end{pmatrix}$ and $\vec{a}_5 = \begin{pmatrix} -4 & 4 & -3 & -2 & -2 \end{pmatrix}$. Since there are five distinct vectors, there are $2^5 - 1 = 31$ ways to choose these vectors to construct M. Thus,

Lemma 3.1. *Let M be a 5 by 5 matrix with integer entries such that $MJ = -7J$, $JM = -7J$ and $MM^t = 49 \cdot I_5$. Then up to permutation of rows and columns, M is one of the following: $M_1 = -7I_5$,*

$$M_2 = \begin{bmatrix} -7 & 0 & 0 & 0 & 0 \\ 0 & -7 & 0 & 0 & 0 \\ 0 & 0 & -3 & 2 & -6 \\ 0 & 0 & -6 & -3 & 2 \\ 0 & 0 & 2 & -6 & -3 \end{bmatrix}, M_3 = \begin{bmatrix} 1 & -6 & -2 & 2 & -2 \\ -6 & 1 & -2 & 2 & -2 \\ -2 & -2 & -3 & -4 & 4 \\ 2 & 2 & -4 & -3 & -4 \\ -2 & -2 & 4 & -4 & -3 \end{bmatrix}$$

Proof. We split the five vectors into two categories. Category A consists of $\vec{a}_1$ and $\vec{a}_2$ while category B contains the remaining vectors. Notice that for $\vec{a} \in A$ and $\vec{b} \in B$, $\vec{a} \cdot \vec{b} \neq \vec{0}$ up to permutation of entries. As the vectors in these categories are not orthogonal, it implies that any combination of at least one vector from each of the categories will not yield a viable matrix M. Due to the composition of these vectors, $\vec{a}_1$ is the only vector that can produce a viable matrix M by itself. Thus, out of all the 31 combinations, only the following could generate a viable M: $\vec{a}_1$ only, $\vec{a}_1$ and $\vec{a}_2$ only, $\vec{a}_3$ and $\vec{a}_4$ only, $\vec{a}_3$ and $\vec{a}_5$ only, $\vec{a}_4$ and $\vec{a}_5$ only and $\vec{a}_3$, $\vec{a}_4$ and $\vec{a}_5$ only. It turns out that $\vec{a}_1$ only yields M_1, $\vec{a}_1$ and $\vec{a}_2$ only generate M_2, $\vec{a}_3$, $\vec{a}_4$ and $\vec{a}_5$ only yield M_3 while others could not produce any viable matrix. □

Now, we have good information about M and of course, $\chi(\hat{D})$. Thus, $\chi(\hat{D}) = M_i + 14J$, where $i = 1, 2, 3$.

3.7.2. *The search for difference set images in $Frob(20)$.* We now describe the technique for finding the intersection numbers in $Frob(20)$. $Frob(20)$ could be viewed in many ways but the representation χ suggests that we think of this group as a permutation group, $\langle\alpha, \beta\rangle$ with $\alpha = (\ 0\ \ 1\ \ 2\ \ 3\ \ 4\ )$, $\beta = (\ 1\ \ 2\ \ 4\ \ 3\ )$. We can now view this group as a subgroup of symmetric group of degree five, S_5 [9]. In this situation, χ represents each of the elements of $Frob(20)$ as 5×5 permutation matrices in four parallel (non horizontal nor vertical) classes $W = \langle\alpha\rangle$, $W\beta$, $W\beta^2$, $W\beta^3$. These parallel classes have slopes 1, 2, 4 and 3 respectively in the affine plane with 30 lines, 25 points, 6 parallel classes, 5 points on each line and 6 lines on a point. This characterization of elements of $\langle\alpha, \beta\rangle$ as permutation matrices can easily be extended to the permutations of S_5 acting naturally on the set $\{0, 1, 2, 3, 4\}$[9]. In view of the problem at hand, we consider a left transversal of this subgroup, $\langle\alpha, \beta\rangle$ of S_5: $T = \{\pi_0 = 1, \pi_1 = (01), \pi_2 = (234), \pi_3 = (01)(234), \pi_4 = (243), \pi_5 = (01)(243)\}$. The advantages of choosing this transversal in S_5 are:

- $T_s = T_s^{-1}$
- Most of the permutation matrices of elements of T commute with M_j, $j = 1, 2, 3$

Therefore, a matrix equivalent to $\chi(\hat{D})$ (under the row and column permutations) has the form $\chi(\pi_k)\chi(g\hat{D}h)\chi(\pi_l)$, where $g, h \in Frob(20)$ and

$\pi_k, \pi_l \in T$. With this correspondence,

$$\chi(g\hat{D}h) = \chi(\pi_k)(M_i)\chi(\pi_l). \tag{3.10}$$

We know that if σ is an automorphism of a group G then $g\hat{D}^\sigma$ is an equivalent difference set of $\hat{D}$ for $g \in G$. But conjugation is an automorphism, thus $\hat{D}$ is a difference set if and only if $g\hat{D}h$ is a difference set. Therefore, we assume, without loss of generality that the difference set image is of the form

$$\chi(\hat{D}) = \chi(\pi_k)(M_i)\chi(\pi_l), i = 1, 2, 3, \tag{3.11}$$

where $\chi(\pi_l)$ is a permutation matrix corresponding to π_l, a representative of coset of $\langle \alpha, \beta \rangle$. This shows that, for each i, (3.11) has 36 choices of matrices for $\chi(\hat{D})$ and we attempt to reduce these possibilities as far as we can. Notice that the matrix $M_1 = 7I$, a scalar matrix, is at the center of the $\mathbb{Z}Sym(5)$ so it commutes with all the permutation matrices. Thus, the difference set image is transformed as $\chi(\hat{D}) = 14J + M_1\chi(\pi_l)$, $l = 0, 1, 2, 3, 4, 5$; where $\chi(\pi_l)$ is a permutation matrix corresponding to $\pi_l \in T_1$, a representative of coset of $\langle \alpha, \beta \rangle$. To obtain the coset representative that commutes with M_2, we partition M_2 along the columns/rows that have similar entries. Thus,

$$M_2 = \left[\begin{array}{cc|ccc} -7 & 0 & 0 & 0 & 0 \\ 0 & -7 & 0 & 0 & 0 \\ \hline 0 & 0 & -3 & 2 & -6 \\ 0 & 0 & -6 & -3 & 2 \\ 0 & 0 & 2 & -6 & -3 \end{array}\right]$$

This partition suggests that we can permute rows (columns) 0 and 1 or rows (columns) 2, 3, and 4. So, we consider $S_{\{0,1\}} \times S_{\{2,3,4\}}$. This gives information about the permutation matrices of elements of the subgroup of S_5 that commute with M_2. Consequently, the permutation matrices of (1), (01), (234), (01)(234), (243) and (01)(243) commute with M_2. Therefore, the 36 choices of matrices reduce to $\chi(\hat{D}) = 10J + \chi(\pi_k)(M_2)\chi(\pi_l), \quad l = 0, \dots, 5$. Notice that the structure of entries of matrix M_3 is similar to those of M_2 and hence, the permutation matrices of (1), (01)(24), (24) and (01) commute with M_3. Furthermore, (1) and (01)(24) are in the same coset and (01) and (24) are in the same coset of $Frob(20)$. In this case, we have to multiply on the left by permutation matrices of elements in T that do not commute with M_3. Thus, the 36 choices of matrices reduced to $\chi(\hat{D}) = 10J + \chi(\pi_k)(M_3)\chi(\pi_l), k = 2, 3, 4, 5; \quad l = 0, \dots, 5$. We worked through the $6 + 6 + 30 = 42$ matrices by computing the respective line sums for the four out of the six equivalence classes (the other two are assigned zero value). Thus, only $M_2\chi(\pi_5)$, $\chi(\pi_2)M_3\chi(\pi_5)$, $M_3\chi(\pi_1)$, $\chi(\pi_3)M_3\chi(\pi_4)$, $\chi(\pi_4)M_3\chi(\pi_3)$, $\chi(\pi_5)M_3\chi(\pi_2)$ and their transposes have desirable pattern and could potentially yield images.

The question now is how do we construct the corresponding element in $\mathbb{Z}[Frob(20)]$ for any choice of $\chi(\hat{D})$? To answer this question, notice that the rows and columns of the representation χ are indexed by $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ with the coordinates of the 5×5 matrix viewed as points of the affine plane $AG(2, 5)$. For instance, the $\chi(\alpha)$ is the characteristic function of the line $y = x + 1$ while $\chi(\beta)$ is the characteristic function of the line $y = 2x$. In general, $\chi(\alpha^s\beta^t)$ is the characteristic function of the line $y = 2^t x + s$ in $AG(2, 5)$ and is an injection from the 20 members of $Frob(20)$ into the 30 lines of $AG(2, 5)$ missing the horizontal and vertical lines. By this correspondence, each member of $\mathbb{Z}[Frob(20)]$ is associated with a member of the collection of functions from the 30 lines of $AG(2, 5)$ to $\mathbb{Z}$ which assign zero to the horizontal and vertical lines. Thus, the (y, x) coordinates of $\chi(\hat{D}) = \hat{\alpha}_g(\sum_{g\in Frob(20)} \alpha_g g)$ is the sum of the α_g for all lines g on the point (y, x). Next, we give some vital definitions:

Define f to be a function from the lines of an affine plane of order q into the integers $\mathbb{Z}$ and another function $\hat{f}$ on the points and lines by $\hat{f}(p) := \sum_{L \; on \; p} f(L)$ and $\hat{f}(L) := \sum_{p\in L} \hat{f}(p)$, respectively. Furthermore we extend f to parallel classes of the plane by defining $f(\Pi_j) := \sum_{L\in\Pi_j} f(L)$, where Π_j is a parallel class with slope j and L is a line in it. Thus, for any fixed line L in a parallel class Π_j, $\hat{f}(L) = \sum_{p \, \in \, L} \sum_{L' \; on \; p} f(L') = q \cdot f(L) - f(\Pi_j) + \sum_{all \quad lines \; L'} f(L')$. With $k = \sum_{all \, lines \; L'} f(L')$, we can find $f(L)$ using the formula

$$f(L) = \frac{\hat{f}(L) - k + f(\Pi_j)}{q}, \tag{3.12}$$

if $\hat{f}(L)$ and $f(\Pi_j)$ are known.

In considering our specific case, the members of $Frob(20)$ are the non vertical nor horizontal lines and the six parallel classes are the four cosets of $W = \langle\alpha\rangle$ along with the 5-rows and 5-columns of the matrix. The size of our difference set is 63 and thus, $k = \sum_{all \, lines \; L'} f(L') = 57$, $f(\Pi) = \{21, 14, 14, 14\}$ and the order of the plane is $q = 5$. Thus, for any point p with coordinates (y, x) in the affine plane the $\hat{f}(p)$ is the (y, x) coordinate of the matrix $\chi(\hat{D}_i)$, $i = 1, \cdots, 5$ while $\hat{f}(L)$ is the sum of the coordinates corresponding to the points of L. Therefore,

$$f(L) = \frac{\hat{f}(L) - 63 + f(\Pi_j)}{5} = \frac{\hat{f}(L) + f(\Pi_j) - 3}{5} - 12. \tag{3.13}$$

Furthermore, since $f(L)$ is the cardinality of the intersection of $\hat{D}$ and any coset of N, the proposed intersection numbers must be non-negative integers not greater than 14, then $(\hat{f}(L) + f(\Pi_j) - 3) \equiv 0 \pmod 5$ and $60 \leq \hat{f}(L) + f(\Pi_j) - 3 \leq 130$. This constraint severely restricts the possible values of $f(L)$ and the 42 choices of matrices reduced to six (as stated earlier) since the lines L of the affine plane such that $f(L)$

TABLE 3. Values of $\hat{f}(L)$

Slope 1	Slope 3	Slope 4	Slope 2
52	74	69	64
57	64	64	74
72	64	64	59
67	59	69	64
67	54	49	54

TABLE 4. Values of $f(L)$

Slope 1	Slope 3	Slope 4	Slope 2
2	5	4	3
3	3	3	5
6	3	3	2
5	2	4	3
5	1	0	1

is negative integer or fraction is discarded. Consequently, the matrices $M_2\chi(\pi_5)$, $\chi(\pi_2)M_3\chi(\pi_5)$, $M_3\chi(\pi_1)$, $\chi(\pi_3)M_3\chi(\pi_4)$, $\chi(\pi_4)M_3\chi(\pi_3)$, $\chi(\pi_5)M_3\chi(\pi_2)$ and their transposes can generates difference set images in $Frob(20)$. Now take $M_2\chi(\pi_5)$ and

$$\chi(\hat{D}) = 14J + M_2\chi(\pi_5) = \begin{bmatrix} 14 & 7 & 14 & 14 & \underline{14} \\ \underline{7} & 14 & 14 & 14 & 14 \\ 14 & \underline{14} & 8 & 11 & 16 \\ 14 & 14 & \underline{16} & 8 & 11 \\ 14 & 14 & 11 & \underline{16} & 8 \end{bmatrix}$$

The values of $\hat{f}(L)$ (sum of weights on a line) are given in Table 3 according to the parallel classes.

For instance, for line $y = x + 1$ of slope 1, the weights associated with points on this line are 17, 10, 8, 8 and 10, these are the underlined values in $\chi(\hat{D})$. In this case, $\hat{f}(L) = 7 + 14 + 16 + 16 + 14 = 67$(This is the bolded value in Table 3). To use (3.13), we choose $f(\Pi_j) = 21$ and $f(L) = 5$, this is the bolded value in A_1. By repeating this procedure several times, we get the image of $Frob(20)$ corresponding to $M_2\chi(\pi_5)$ as $A_1 = 2 + 3x + 6x^2 + 5x^3 + \mathbf{5}x^4 + (5 + 3x + 3x^2 + 2x^3 + x^4)y + (4 + 3x + 3x^2 + 4x^3)y^2 + (3 + 5x + 2x^2 + 3x^3 + x^4)y^3$.

The other images are $A_2 = 2x + 5x^2 + 5x^3 + 2x^4 + (3 + 2x + 3x^2 + 3x^3 + 3x^4)y + (2 + 5x + 5x^2 + 2x^3 + 7x^4)y^2 + (3 + 3x + 3x^2 + 2x^3 + 3x^4)y^3$, $A_3 = 1 + 2x + 2x^2 + 5x^3 + 4x^4 + (1 + 5x + 3x^2 + 3x^3 + 2x^4)y + (3 + 4x + 4x^2 + 3x^3 + 7x^4)y^2 + (3 + x + 3x^2 + 5x^3 + 2x^4)y^3$ and $A_4 = 1 + 4x +$

$5x^2+2x^3+2x^4+(3+5x+x^2+2x^3+3x^4)y+(3+4x+4x^2+3x^3+7x^4)y^2+(1+3x+2x^2+5x^3+3x^4)y^3$.

3.8. **There are no $Frob(20)\times C_2$ images.** Suppose that there is a normal subgroup of G such that $G/N \cong Frob(20)\times C_2 = \langle x,y,z : x^5=y^4=z^2=1, yx=x^2y, xz=zx, yz=zy\rangle$. The derived group of G/N is isomorphic to $\langle x\rangle$ and $(Frob(20)\times C_2)/\langle x\rangle \cong C_4\times C_2$. Also, $(Frob(20)\times C_2)/\langle z\rangle \cong Frob(20)$. Let $\hat{D}=\sum_{k=0}^{4}\sum_{j=0}^{1}\sum_{i=0}^{3} d_{ijk}x^iy^jz^k$ be the difference set image in $Frob(20)\times C_2$. By applying the eight characters of $Frob(20)\times C_2$ to $\hat{D}$, we get the following equations:

$$\begin{aligned}
&\sum_{i=0}^{4} d_{i00}=c_{00},\quad \sum_{i=0}^{4} d_{i10}=c_{10},\quad \sum_{i=0}^{4} d_{i20}=c_{20},\quad \sum_{i=0}^{4} d_{i30}=c_{30} \\
&\sum_{i=0}^{4} d_{i01}=c_{01},\quad \sum_{i=0}^{4} d_{i11}=c_{11},\quad \sum_{i=0}^{4} d_{i21}=c_{21},\quad \sum_{i=0}^{4} d_{i31}=c_{31}.
\end{aligned} \tag{3.14}$$

where the 2×4 matrix (c_{ij}) is an image set in $\Omega_{C_4\times C_2}$. Also, using the map $z\mapsto 1$ we get 20 more linear equations

$$\begin{aligned}
&d_{i00}+d_{i01}=b_{i0}, \qquad d_{i10}+d_{i11}=b_{i1} \\
&d_{i20}+d_{i21}=b_{i2}, \qquad d_{i30}+d_{i31}=b_{i3}, \qquad i=0,\dots,4,
\end{aligned} \tag{3.15}$$

where the 4×5 matrix (b_{ij}) is the unique element of $\Omega_{Frob(20)}$. The last representation of $Frob(20)\times C_2$ is:

$$\chi : x\mapsto \begin{pmatrix} \zeta & 0 & 0 & 0 \\ 0 & \zeta^2 & 0 & 0 \\ 0 & 0 & \zeta^4 & 0 \\ 0 & 0 & 0 & \zeta^3 \end{pmatrix}, y\mapsto \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}, z\mapsto \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix},$$

ζ is the fifth root of unity. By applying this representation to $\hat{D}$, we get

$$\chi(\hat{D}) = \begin{pmatrix} A & B & C & D \\ \sigma(D) & \sigma(A) & \sigma(B) & \sigma(C) \\ \bar{C} & \bar{D} & \bar{A} & \bar{B} \\ \overline{\sigma(B)} & \overline{\sigma(C)} & \overline{\sigma(D)} & \overline{\sigma(A)} \end{pmatrix},$$

where $A=\sum_{s=0}^{4} a_s\zeta^s$, $B=\sum_{s=0}^{4} b_s\zeta^s$, $C=\sum_{s=0}^{4} c_s\zeta^s$, $D=\sum_{s=0}^{4} d_s\zeta^s$, $a_s=d_{s00}-d_{s01}$, $b_s=d_{s10}-d_{s11}$, $c_s=d_{s20}-d_{s21}$, $d_s=d_{s30}-d_{s31}$ and $\sigma(\zeta)=\zeta^2$.

By solving $\chi(\hat{D})\overline{\chi(\hat{D})}=49$, we get 16 equations which are equivalent to the following system: -

$$A\bar{A}+B\bar{B}+C\bar{C}+D\bar{D}=49 \tag{3.16}$$

$$AC+BD=0 \tag{3.17}$$

$$A\overline{\sigma(D)}+B\overline{\sigma(A)}+C\overline{\sigma(B)}+D\overline{\sigma(C)}=0 \tag{3.18}$$

$$A\overline{\sigma(B)}+B\overline{\sigma(C)}+C\overline{\sigma(D)}+D\overline{\sigma(A)}=0 \tag{3.19}$$

Conditions (3.16)-(3.19) generate 14 more linear equations. We now use computer to search of possible values of d_{ijk} by combining these 14 linear equations with (3.14) and (3.15). In order to have an exhaustive search, we fix the values of b_{ij} from the $Frob(20)$ image and allow c_{sk} in (3.14) to vary. This search yielded no result. Consequently, there is no difference set image in $Frob(20) \times C_2$.

4. Difference set images in factor groups of orders 28 and 56

In this section, we show that G that satisfies $G/N \cong C_{56}$, $C_{28} \times C_2$, $Q_{14} \times C_2$ or D_{28} do not admit (280, 63, 14) difference sets. We also give information about G in which $G/N \cong Q_{28}$.

4.1. **The C_7 Images.** Suppose that $G/N \cong C_7 = \langle x : x^7 = 1\rangle$. Since the ideal generated by 7 factors trivially in the cyclotomic ring, the difference set images are $-7 + 10\langle x\rangle$ and $7 + 8\langle x\rangle$, up to equivalence.

4.2. **The C_{14} and D_7 Images.** Suppose that $G/N \cong C_{14} = \langle x, y : x^7 = y^2 = [x, y] = 1\rangle$. Using (2.13) with $\alpha = 8$ or 10, $|K| = 7$, the difference set images up to equivalence are, $A_1 = 7 + 4\langle x\rangle\langle y\rangle$ and $A_2 = 7 + 3\langle x\rangle + 5\langle y\rangle$. The other solutions are $A_3 = -7 + 5\langle x\rangle\langle y\rangle$ and $A_4 = -7 + 6\langle x\rangle + 4\langle y\rangle$ but they are not considered images because of negative number. By Dillon trick, one can show that A_1 and A_2 are also $D_7 = \langle x, y : x^7 = y^2 = 1, yxy = x^{-1}\rangle$ images. Next, we construct the difference set images in $G/N \cong C_{28}$, D_{14}, $C_{14} \times C_2$ and $C_7 \rtimes C_4$.

4.3. **The C_{28}, D_{14} and $C_{14} \times C_2$ Images.** The construction of the difference set images in factor groups of order 28 involves information from C_{14} and D_7 images.

4.3.1. *The C_{28} and D_{14}.* Consider $G/N \cong C_{28} = \langle x, y : x^7 = y^4 = 1 = [x, y]\rangle$ and let $\hat{D} = \sum_{t=0}^{3}\sum_{s=0}^{7} x^s y^t$ be the difference set in this group. We view $\hat{D}$ as a 4×7 matrix with the columns indexed by the powers of x and rows indexed by powers of y. This group has 6 rational idempotents just like the $G/N \cong C_{20}$ case. Using the same approach therefore, the difference set images, up to equivalence, are $E_1 = 7 + 2\langle x\rangle\langle y\rangle$, $E_2 = 7 + (1 + 2y + 3y^2 + 2y^3)\langle x\rangle$ and $E_3 = 7 + (1 + 3y + 2y^2 + 2y^3)\langle x\rangle$.

Now suppose that $G/N \cong D_{14} = \langle\theta, y : \theta^{14} = y^2 = 1, y\theta y = \theta^{-1}\rangle$ and the difference set image is $\hat{D} = \sum_{s=0}^{14}\sum_{t=0}^{1} d_{st}\theta^s y^t$. We view this group ring element as a 2×14 matrix. In order to take advantage of the Dillon Dihedral trick, we need the difference set images in C_{28}. We now view C_{28} as $C_{28} = \langle z : z^{28} = 1\rangle$. Set $\theta = z^2$ and $y = z$ in C_{28}. This transformation enables us to rewrite each of the three difference set images as 2×14 matrix, E'_j. For instance, take $E_2 \in \Omega_{C_{28}}$. This image is transformed as $E'_2 = (8 + 3\theta + \theta^2 + 3\theta^3 + \theta^4 + 3\theta^5 + \theta^6 + 3\theta^7 + \theta^8 + 3\theta^9 + \theta^{10} + 3\theta^{11} + \theta^{12} + 3\theta^{13}) + 2(1 + \theta + \theta^2 + \theta^3 + \theta^4 + \theta^5 + \theta^6 +$

$\theta^7+\theta^8+\theta^9+\theta^{10}+\theta^{11}+\theta^{12}+\theta^{13})y$. The factor group G/N has three equivalent degree two representations. One of them is:

$$\chi:\theta\mapsto\begin{pmatrix}\zeta_{14} & 0\\ 0 & \zeta_{14}^{13}\end{pmatrix},\quad y\mapsto\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$$

We now apply this degree two representation to the transformed image $E'_j, j=1,2,3$ and verify whether or not $\chi(E'_j)\overline{\chi(E'_j)}=49I_2$. In the case of E'_2, $\chi(E'_2)=\begin{pmatrix}\beta & \alpha\\ \bar{\alpha} & \bar{\beta}\end{pmatrix}$, where $\alpha=5+2\theta\neq 0$, $\theta=\zeta_{14}+\zeta_{14}^3+\zeta_{14}^5-\zeta_{14}^2-\zeta_{14}^4-\zeta_{14}^6$ and $\beta=0$. It turns out that $\alpha=\bar{\alpha}$ and $\theta^2=6-5\theta$. The requirement $\chi(E'_2)\overline{\chi(E'_2)}=49I_2$ implies that $\alpha\bar{\alpha}+\beta\bar{\beta}=49$.Thus, $\alpha\bar{\alpha}+\beta\bar{\beta}=(5+2\theta)(5+2\bar{\theta})=49$. It is easy to verify that $E'_j, j=1,3$ also satisfies the above condition. Consequently, $E'_j, j=1,2,3$ is a difference set image in D_{14}.

4.3.2. *The $C_{14}\times C_2$ images.* Suppose that $G/N\cong C_{14}\times C_2=\langle x,y: x^7=y^2=[x,y]=1\rangle\times\langle z:z^2=1\rangle$. This group is of the form (2.11) and using (2.13) we get

$$\hat{D}=A_i\left(\frac{\langle z\rangle}{2}\right)+gB_j\left(\frac{2-\langle z\rangle}{2}\right), g\in C_{14}\times C_2, \tag{4.1}$$

where $K=C_{14}$, $|K|=14$, $\alpha=4$, $B_j=A_j-4K$, $i=1,2, j=1,2,3,4$. Note that A_i and $A_j, i=j=1,2$ are difference set images in C_{14} while $A_j, j=3,4$ is other solution. Thus, the difference set images are $\bar{E}_1=7+\langle x\rangle\langle y\rangle\langle z\rangle$, $\bar{E}_2=7+\langle x\rangle+3\langle x\rangle y+2\langle x\rangle\langle y\rangle z$ and $\bar{E}_3=7+\langle x\rangle+2\langle x\rangle y+2\langle x\rangle\langle y\rangle z+\langle x\rangle z$.

Remark 1. The computation of difference set distribution in factor groups of 28 will aid us to find the difference set images in $G/N\cong C_7\rtimes C_4$. Notice that all the four groups of order 28 have a factor group that is isomorphic to D_7 or C_{14}. Recall that there are two types of difference set images in D_7 or C_{14}, up to equivalence. The distribution of these difference set images are 11^14^{13}, $3^65^710^1$, where distribution 11^14^{13} means that the intersection number 4 appears thirteen times and the intersection number 11 appears once. The coset bound for difference set images in factor group G/N of order 28 is 10. This means that intersection numbers of difference set images in these groups satisfy $0\le d_{s,t}\le 10$. Furthermore, the size of the kernel of homomorphism between groups of order 14 and groups of order 28 is 2. This means that each intersection number of the difference set image in groups of order 14 will split into two in the difference set image in groups of order 28. Based on the difference set images in groups of order 14, we look at two cases:
Case 1: The distribution 11^14^{13}:
11 split as (10, 1), (9, 2), (8, 3), (7, 4), (6, 5) and 4 split as (4, 0), (3, 1) or (2, 2): We consider five subcases:
Subcase 1a: Suppose 11 split as (10, 1) and 4 split as (4, 0), (3, 1) or (2,

2). Let $0 \leq \alpha_i \leq 13, i = 1, 2, 3$ be the number of intersection number 4 that split as (2, 2), (3, 1) and (4, 0) respectively. Using the symbols of variance technique (Lemma 2.1), $m_0 = m_4 = \alpha_3, m_1 = \alpha_2 + 1, m_2 = 2\alpha_1$, $m_3 = \alpha_2$, $m_{10} = 1$, $m_5 = m_6 = m_7 = m_8 = m_9 = 0$. The variance technique equations (2.2) - (2.4) become:

$$\sum_{i=1}^{3} \alpha_i = 13, \tag{4.2}$$

$$2\alpha_1 + 3\alpha_2 + 6\alpha_3 = 18, \tag{4.3}$$

In all the cases, (2.3) is redundant. From (4.2), the sum of three positive integers is odd. This implies that either one or all the numbers are odd. Thus, by (4.3), α_2 is even. We eliminate α_2 by adding -2 times (4.2) to (4.3). This operation yields $\alpha_2 + 4\alpha_3 = -8$. Since the sum of positive numbers cannot be negative, this option yields no distribution.
Subcase 1b: Suppose 11 split as (9, 2) and 4 split as (4, 0), (3, 1) or (2, 2). Let $0 \leq \alpha_i \leq 13, i = 1, 2, 3$ be the number of intersection number 4 that split as (2, 2), (3, 1) and (4, 0) respectively. Using the symbols Lemma 2.1, $m_0 = m_4 = \alpha_3, m_1 = \alpha_2, m_2 = 2\alpha_1 + 1$, $m_3 = \alpha_2$, $m_9 = 1$, $m_5 = m_6 = m_7 = m_8 = m_{10} = 0$. The variance technique equations (2.2) - (2.4) become:

$$\sum_{i=1}^{3} \alpha_i = 13, \tag{4.4}$$

$$2\alpha_1 + 3\alpha_2 + 6\alpha_3 = 26, \tag{4.5}$$

We again eliminate α_2 by adding -2 times (4.2) to (4.3). This operation yields $\alpha_2 + 4\alpha_3 = 0$. Consequently, $\alpha_2 = \alpha_3 = 0$. The subcase yields a unique distribution $9^1 2^{27}$. A similar approach shows that:
Subcase 1c: If 11 split as (8, 3) and 4 split as (4, 0), (3, 1) or (2, 2), then the distributions are (i) $1^6 2^{14} 3^7 8^1$ and (ii) $0^1 1^2 2^{20} 3^3 4^1 8^1$.
Subcase 1d: If 11 split as (7, 4) and 4 split as (4, 0), (3, 1) or (2, 2), then the distributions are $1^{10} 2^6 3^{10} 4^1 7^1$, $0^1 1^6 2^{12} 3^6 4^2 7^1$ and $0^2 1^2 2^{18} 3^2 4^3 7^1$.
Subcase 1e: If 11 split as (6, 5) and and 4 split as (4, 0), (3, 1) or (2, 2), then the distributions are $1^{12} 2^2 3^{12} 5^1 6^1$, $0^2 1^4 2^{14} 3^4 4^2 5^1 6^1$, $0^1 1^8 2^8 3^8 4^1 5^1 6^1$ and $0^3 2^{20} 4^3 5^1 6^1$.
Case 2: The distribution $10^1 5^7 3^6$: There are six subcases.
Subcase 2a: If 10 split as (10, 0), 5 split as (5, 0), (4, 1) or (3, 2) and 3 split as (3, 0) or (2, 1), then there are no distributions. Subcase 2b: If 10 split as (9, 1), 5 split as (5, 0), (4, 1) or (3, 2) and 3 split as (3, 0) or (2, 1), then there are no distributions. Subcase 2c: If 10 split as (8, 2), 5 split as (5, 0), (4, 1) or (3, 2) and 3 split as (3, 0) or (2, 1), then the unique distribution is $1^6 2^{14} 3^7 8^1$.
Subcase 2d: If 10 split as (7, 3), 5 split as (5, 0), (4, 1) or (3, 2) and 3 split as (3, 0) or (2, 1), then there are no distributions.

Subcase 2e: If 10 split as (6, 4), 5 split as (5, 0), (4, 1) or (3, 2) and 3 split as (3, 0) or (2, 1), then the distributions are $1^{10}2^93^34^56^1$, $0^11^72^{11}3^54^25^16^1$, $0^11^82^93^54^46^1$, $0^21^52^{11}3^74^15^16^1$, $0^21^62^93^74^36^1$, $0^31^42^93^94^26^1$ and $0^41^22^9\ 3^{11}4^16^1$.
Subcase 2f: If 10 split as (5, 5), 5 split as (5, 0), (4, 1) or (3, 2) and 3 split as (3, 0) or (2, 1), then there are no distributions.
All together, there are eighteen possible distributions for the difference set images in G/N.

4.3.3. *The $Q_{28} \cong C_7 \rtimes C_4$ images.* Consider $G/N \cong C_7 \rtimes C_4 = \langle x, y : x^7 = y^4 = 1, yxy^{-1} = x^6\rangle$. The derived subgroup of G/N is isomorphic to $\langle x\rangle$ and the center of G/N is $C(G/N) \cong \langle y^2\rangle$. Suppose that the difference set image in G/N is $\hat{D} = \sum_{s=0}^{6}\sum_{t=0}^{3} d_{s,t}x^sy^t$. We view $\hat{D}$ as a 4×7 matrix with the columns indexed by the powers of x and rows by powers of y. Since $(G/N)/\langle y^2\rangle \cong D_7$, the information about the difference set image in D_7 and the map $y^2 \mapsto 1$ yield the following system of equations:

$$d_{s0} + d_{s2} = f_{s0}, \qquad d_{s1} + d_{s3} = f_{s1} \qquad s = 0, \ldots, 6 \tag{4.6}$$

where 2×7 matrix (f_{st}) is a difference set image set in D_7. Also, $H/\langle x\rangle \cong C_4$ and the map $x \mapsto 1$ produce four more equations:

$$\sum_{s=0}^{6} d_{s0} = c_0, \quad \sum_{s=0}^{6} d_{s1} = c_2, \quad \sum_{s=0}^{6} d_{s2} = c_2, \quad \sum_{s=0}^{6} d_{s3} = c_3, \tag{4.7}$$

where the 1×4 matrix (c_t), is the unique difference set image in C_4. We have considered all the lifted representations of H from normal subgroups. The group H has three other equivalent degree two representations. One of them is

$$\chi : x \mapsto \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}, \quad y \mapsto \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},$$

where ζ and i are the seventh and fourth roots of unity respectively. By applying this representation to $\hat{D}$, we get $\chi(\hat{D}) = \begin{pmatrix} a & bi \\ \bar{b}i & \bar{a} \end{pmatrix}$, where $a = \sum_{s=0}^{6}(d_{s0} - d_{s2})\zeta^s$, $b = \sum_{s=0}^{6}(d_{s1} - d_{s3})\zeta^s$, and $a, b \in \mathbb{Z}[\zeta]$. Furthermore,

$$\chi(\hat{D})\overline{\chi(\hat{D})} = \begin{pmatrix} a\bar{a} + b\bar{b} & 0 \\ 0 & a\bar{a} + b\bar{b} \end{pmatrix}.$$

But as we require $\chi(\hat{D})\overline{\chi(\hat{D})} = 49I_2$, where I_2 is a 2×2 matrix, then

$$a\bar{a} + b\bar{b} = 49. \tag{4.8}$$

We now garner information about the algebraic numbers a and b. But first, we rewrite (4.6) as

$$d_{s2} = f_{s0} - d_{s0}, \qquad d_{s3} = f_{s1} - d_{s1} \qquad s = 0, \ldots, 6 \tag{4.9}$$

and substitute in a and b to get

$$A := 2\sum_{s=0}^{6} d_{s0}\zeta^s - \sum_{s=0}^{6} f_{s0}\zeta^s, \quad B := 2\sum_{s=0}^{6} d_{s1}\zeta^s - \sum_{s=0}^{6} f_{s1}\zeta^s$$

and $A, B \in \mathbb{Z}[\zeta]$. Since f_{s0} and $f_{s1}, s = 0, \ldots, 6$ are known, it turns out that for the two D_7 images, $A = 2\sum_{s=0}^{6} d_{s0}\zeta^s - 7$ and $B = 2\sum_{s=0}^{6} d_{s1}\zeta^s$. Thus, (4.8) becomes

$$\frac{1}{7}\big(A_1\bar{A}_1 + B_1\bar{B}_1\big) = \frac{1}{2}\big(A_1 + \bar{A}_1\big), \tag{4.10}$$

with $A_1 = \sum_{s=0}^{6} d_{s0}\zeta^s$ and $B_1 = \sum_{s=0}^{6} d_{s1}\zeta^s$. The right hand sides of (4.10) implies

- d_{00} is any integer between 0 and 10
- $d_{s0} + d_{7-s,0} \equiv 0 \mod 2, s = 1, \ldots, 6$
- d_{s0} and $d_{7-s,0}$ are either both even integers or both odd integers
- the sum $\sum_{s=1}^{6} d_{s0}$ is even
- based on (4.6), it follows that $\sum_{s=1}^{6} d_{s2}$ is also even.

With the above stipulations, we can show that subcases 2c and 2e cannot generate difference set image. We look at subcase 2e.

Without loss of generality we choose $d_{00} = 6$ and consequently, $d_{02} = 4$. We apply an automorphism, if necessary, so that

$$\sum_{s=0}^{6} d_{s0} = 21, \quad \sum_{s=0}^{6} d_{s1} = 14, \quad \sum_{s=0}^{6} d_{s2} = 14, \quad \sum_{s=0}^{6} d_{s3} = 14. \tag{4.11}$$

As $\sum_{s=1}^{6} d_{s0}$ is even, then $d_{00} + \sum_{s=1}^{6} d_{s0}$ is also even this contradicts the fact that $\sum_{s=0}^{6} d_{s0} = 21$. The subcase 1b and 1c(i) produced images $E_1 = 7+2\langle x\rangle\langle y\rangle$ and $E_2 = 7+(1+2y+3y^2+2y^3)\langle x\rangle$ respectively. Finally, for subcases 1c, 1d and 1e, we need the following: As $a, b \in \mathbb{Z}[\zeta]$, (4.8) has solutions in the quadratic sub ring of $\mathbb{Z}[\zeta]$ whose integral basis are $\{1, \zeta^2 + \zeta^5, \zeta^3 + \zeta^4\}$. Consequently, (4.8) yields three more equations

$$\sum_{s=0}^{6} a_s^2 + \sum_{s=0}^{6} b_s^2 - \sum_{s=0}^{6} a_s a_{s+1} - \sum_{s=0}^{6} b_s b_{s+1} = 49 \tag{4.12}$$

$$\sum_{s=0}^{6} a_{s+2}a_s + \sum_{s=0}^{6} b_{s+2}b_s - \sum_{s=0}^{6} a_s a_{s+1} - \sum_{s=0}^{6} b_s b_{s+1} = 0 \tag{4.13}$$

$$\sum_{s=0}^{6} a_{s+3}a_s + \sum_{s=0}^{6} b_{s+3}b_s - \sum_{s=0}^{6} a_s a_{s+1} - \sum_{s=0}^{6} b_s b_{s+1} = 0 \tag{4.14}$$

The subscripts of (4.12), (4.13), (4.14) are congruent to 0 modulo 7, $a_s = d_{s0} - d_{s2}$ and $b_s = d_{s1} - d_{s3}, s = 0, \ldots, 6$. To find the other images, we need to combine conditions generated by (4.10) with (4.6) and (4.11) - (4.14).

4.4. There are no C_{56}, $C_{28}\times C_2$ and D_{28} Images.

4.4.1. *The C_{56} and D_{28} Cases.* The factor group $G/N \cong C_{56} = \langle x, y : x^7 = y^8 = 1 = [x, y]\rangle$ has eight rational idempotents. Six of these idempotents have $\langle y^4\rangle$ in their kernel and the linear combination of these idempotents is $\sum_{j=0,1}\sum_{k=0,2,4}\alpha_{\chi_{(j,k)}}[e_{\chi_{(j,k)}}] = \frac{E_i}{2}\langle y^2\rangle$, where E_i is a difference set image in C_{28} and $\alpha_{\chi_{(j,k)}}$ is an alias. The remaining two rational idempotents are:

$$[e_{\chi_{(0,1)}}] = \frac{1}{14}\langle x\rangle(1-y^4) \quad \text{and} \quad [e_{\chi_{(1,1)}}] = \frac{1}{14}(7-\langle x\rangle)(1-y^4).$$

Thus, the difference set image in C_{56} will be obtained by the equation

$$\hat{D} = \frac{E_i}{2}\langle y^4\rangle + \alpha_{\chi_{(0,1)}}[e_{\chi_{(0,1)}}] + \alpha_{\chi_{(1,1)}}[e_{\chi_{(1,1)}}] \tag{4.15}$$

with $\alpha_{\chi_{(0,1)}}, \alpha_{\chi_{(1,1)}} \in \{\pm 7x^sy^t\}$ and $s = 0, \ldots, 6; t = 0, \ldots, 7$. Up to equivalence, the solutions to (4.15) are: $7+\langle x\rangle\langle y\rangle$, $8+\langle x\rangle\langle y\rangle+\langle x\rangle(-1+y^4)$ and $9+\langle x\rangle\langle y\rangle+3y-3y^3-2y^4-3y^5+3y^7$. None of these solutions is a difference set image because at least one number is outside the coset bound [0, 5]. Consequently, the Dillon technique shows that there are no (280, 63, 14) difference set images in $G/N \cong D_{28} = \langle x, y : x^{28} = y^2 = 1, yxy = x^{-1}\rangle$.

4.4.2. *The $C_{28}\times C_2$ Case.* Suppose that $G/N \cong C_{28}\times C_2 = \langle x, y : x^7 = y^4 = [x, y] = 1\rangle \times \langle z : z^2 = 1\rangle$. This group is of the form (2.11) and using (2.13) we get

$$\hat{D} = E_j\left(\frac{\langle z\rangle}{2}\right) + gB_j\left(\frac{2-\langle z\rangle}{2}\right), g \in C_{28}\times C_2 \tag{4.16}$$

with $K = C_{28}$, $|K| = 28$, $\alpha = 2$, $B_j = E_j - 2K$, $j = 1, 2, 3$ and E_j is a difference set image in C_{28}. After considering all possible combinations, there is no feasible difference set image.

Remark 2. In order to effectively obtain difference set images in any factor group of order 56, we need the possible distributions. By Variance technique, the feasible distributions of difference set images in any factor group of order 56 is $0^a1^b2^c3^d4^e5^f$, where the values of a, b, c, d, e, f are respectively, 6 45 2 0 1 2; 6 46 0 0 3 1; 7 43 2 2 0 2; 7 44 0 2 2 1; 8 40 5 1 0 2; 8 41 3 1 2 1; 8 42 0 4 1 1; 8 42 1 1 4 0; 9 37 8 0 0 2; 9 38 6 0 2 1; 9 39 3 3 1 1; 9 39 4 0 4 0; 9 40 0 6 0 1; 9 40 1 3 3 0; 10 36 6 2 1 1; 10 37 3 5 0 1; 10 37 4 2 3 0; 10 38 1 5 2 0; 11 33 9 1 1 1; 11 34 6 4 0 1; 11 34 7 1 3 0; 11 35 4 4 2 0; 11 36 1 7 1 0; 12 30 12 0 1 1; 12 31 9 3 0 1; 12 31 10 0 3 0; 12 32 7 3 2 0; 12 33 4 6 1 0; 12 34 1 9 0 0; 13 28 12 2 0 1; 13 29 10 2 2 0; 13 30 7 5 1 0; 13 31 4 8 0 0; 14 25 15 1 0 1; 14 26 13 1 2 0; 14 27 10 4 1 0; 14 28 7 7 0 0; 15 22 18 0 0 1; 15 23 16 0 2 0; 15 24 13 3 1 0; 15 25 10 6 0 0; 16 21 16 2 1 0; 16 22 13 5 0 0; 17 18 19 1 1 0; 17 19 16 4 0 0; 18 15 22 0 1 0; 18 16 19 3 0 0; 19 13 22 2 0 0; 20 10 25 1 0 0; 21 7 28 0 0 0;

4.5. **The $C_7 \rtimes C_8$ Images.** Suppose $G/N \cong C_7 \rtimes C_8 = H = \langle x^7 = y^8 = 1, yxy^{-1} = x^{-1}\rangle$. The center of this group is $C(H) = \{1, y^2, y^4, y^6\} \cong C_4$. Thus, $H/\langle y^4\rangle \cong Q_{28}$, $H/C(H) \cong D_7$ and $H/\langle x\rangle \cong C_8$. Suppose that $\hat{D} = \sum_{s=0}^{6}\sum_{t=0}^{7} d_{st}x^s y^t$ is the difference set image in this group. By applying the map $y^4 \mapsto 1$ to $\hat{D}$, we get the difference set image in Q_{28} and consequently, the system of equations

$$\begin{aligned} &d_{s0} + d_{s4} = f_{s0}, \qquad && d_{s1} + d_{s5} = f_{s1} && \\ &d_{s2} + d_{s6} = f_{s2}, \qquad && d_{s3} + d_{s7} = f_{s3} \qquad && s = 0, \dots, 6, \end{aligned} \tag{4.17}$$

where 4×7 matrix (f_{st}) is a difference set image set in Q_{14}. Also, the map $x \mapsto 1$ on $\hat{D}$ yields

$$\begin{aligned} &\sum_{s=0}^{6} d_{s0} = c_0, \quad \sum_{s=0}^{6} d_{s1} = c_2, \quad \sum_{s=0}^{6} d_{s2} = c_2, \quad \sum_{s=0}^{6} d_{s3} = c_3 \\ &\sum_{s=0}^{6} d_{s4} = c_4, \quad \sum_{s=0}^{6} d_{s5} = c_5, \quad \sum_{s=0}^{6} d_{s6} = c_6, \quad \sum_{s=0}^{6} d_{s7} = c_7, \end{aligned} \tag{4.18}$$

where the 1×8 matrix (c_t), is the unique difference set image in C_8. One of the remaining six equivalent degree two representations of H is

$$\chi : y \mapsto \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}, \quad x \mapsto \begin{pmatrix} 0 & \tau \\ \tau & 0 \end{pmatrix},$$

where ζ and τ are the seventh and eighth roots of unity respectively. By applying this representation to $\hat{D}$, we get

$$\chi(\hat{D}) = \begin{pmatrix} a_0 + b_0\tau^2 & a_1\tau + b_1\tau^3 \\ \bar{a}_1\tau + \bar{b}_1\tau^3 & \bar{a}_0 + \bar{b}_0\tau^2 \end{pmatrix},$$

where $a_0 = \sum_{s=0}^{6}(d_{s0} - d_{s4})\zeta^s$,$b_0 = \sum_{s=0}^{6}(d_{s2} - d_{s6})\zeta^s$,
$a_1 = \sum_{s=0}^{6}(d_{s1} - d_{s5})\zeta^s$, $b_1 = \sum_{s=0}^{6}(d_{s3} - d_{s7})\zeta^s$, and $a_0, a_1, b_0, b_1 \in \mathbb{Z}[\zeta]$. Furthermore,

$$\chi(\hat{D})\overline{\chi(\hat{D})} = \begin{pmatrix} a_{11} & a_{12} \\ \bar{a}_{12} & a_{22} \end{pmatrix},$$

with $a_{11} = a_0\bar{a}_0 - a_0\bar{b}_0\tau^2 + \bar{a}_0 b_0\tau^2 + b_0\bar{b}_0 + a_1\bar{a}_1 - a_1\bar{b}_1\tau^2 + \bar{a}_1 b_1\tau^2 + b_1\bar{b}_1$,$a_{22} = a_0\bar{a}_0 + a_0\bar{b}_0\tau^2 - \bar{a}_0 b_0\tau^2 + b_0\bar{b}_0 + a_1\bar{a}_1 + a_1\bar{b}_1\tau^2 - \bar{a}_1 b_1\tau^2 + b_1\bar{b}_1$ and $a_{12} = -a_0a_1\tau^3 - a_0b_1\tau + b_0a_1\tau - b_0b_1\tau^3 + a_1a_0\tau - a_1b_0\tau^3 + a_0b_1\tau^3 + b_0b_1\tau$. The requirement $\chi(\hat{D})\overline{\chi(\hat{D})} = 49I_2$, implies

$$a_0\bar{a}_0 + b_0\bar{b}_0 + a_1\bar{a}_1 + b_1\bar{b}_1 = 49 \tag{4.19}$$

$$\bar{a}_0 b_0 + \bar{a}_1 b_1 - a_0\bar{b}_0 - a_0\bar{b}_0 = 0 \tag{4.20}$$

$$(a_0 + b_0)(a_1 + b_1) - 2a_0b_1 = 0 \tag{4.21}$$

The existence or otherwise of the difference set image in H will be decided by remark 2 and solving (4.17), (4.18), (4.19), (4.20) and (4.21) simultaneously.

4.6. **The $(C_2)^3 \rtimes C_7$ Images.** Suppose $G/N \cong Frob(56)$, the Frobenius group of order 56 and $Frob(56) = ((C_2)^3 \rtimes C_7) = \langle a, b, c, x : a^2 = b^2 = c^2 = x^5 = 1, xbx^{-1} = a, xbx^{-1} = b, xbx^{-1} = bc, ab = ba, ac = ca, bc = cb\rangle$. The derived subgroup of this group is isomorphic to the elementary abelian group $H' = \langle a, b, c : a^2 = b^2 = c^2 = 1 = [a, b] = [b, c] = [a, c]\rangle$ of order 8. Suppose that

$$\hat{D} = \sum_{\vec{v}\in H', 0\leq j\leq 6} d_{\vec{v},j} g_{\vec{v}} x^j,\ g_{\vec{v}} = a^{v_1} b^{v_2} c^{v_3},\ 0 \leq v_1, v_2, v_3 \leq 1$$

is the difference set image in $Frob(56)$. This group ring element may also be viewed as a 8×7 matrix with the rows indexed by elements of H' and columns indexed by powers of x. Thus, we write $\hat{D} = \sum_{j=0}^{6} \hat{D}_j x^j$ with $\hat{D}_j = (d_{\vec{v},j}) \in \mathbb{Z}[H']$, the $(j + 1)^{th}$ column of $\hat{D}$, $j = 0, \ldots, 6$ and $\hat{D}_j$ is a 8×1 matrix. As a linear representation will have the derived (commutator) group in its kernel and in this case, $Frob(56)/H' \cong C_7$, therefore, H has seven characters, defined as

$$\chi_t(a) = \chi_t(b) = \chi_t(c) = 1, \chi_t(x) = \zeta^t,\ t = 0, \ldots, 6;$$

ζ is the seventh root of unity and χ_0 is the trivial character. Furthermore, using the presentation of $Frob(56)$, there are two conjugate classes in H'. These conjugate classes produced the orbits:

$$1, \text{the identity}$$

$$a \to cb \to ba \to acb \to ca \to c \to b \to a.$$

These orbits are used to define the non linear representations of H by inducing the non-trivial characters of H'. Suppose that $T = \{1, x, x^2, x^3, x^4, x^5, x^6\}$ is a left transversal of H' in $Frob(56)$. Then, the representation of $Frob(56)$ induced by the non-trivial of characters of H' is:

$$\psi : x \mapsto A_0, a \mapsto A_1, b \mapsto A_2, c \mapsto A_3,$$

where

$$A_0 = \begin{bmatrix} 0&1&0&0&0&0&0\\ 0&0&1&0&0&0&0\\ 0&0&0&1&0&0&0\\ 0&0&0&0&1&0&0\\ 0&0&0&0&0&1&0\\ 0&0&0&0&0&0&1\\ 1&0&0&0&0&0&0 \end{bmatrix}, A_1 = \begin{bmatrix} 1&0&0&0&0&0&0\\ 0&-1&0&0&0&0&0\\ 0&0&1&0&0&0&0\\ 0&0&0&-1&0&0&0\\ 0&0&0&0&-1&0&0\\ 0&0&0&0&0&-1&0\\ 0&0&0&0&0&0&1 \end{bmatrix},$$

$$A_2 = \begin{bmatrix} 1&0&0&0&0&0&0\\ 0&-1&0&0&0&0&0\\ 0&0&-1&0&0&0&0\\ 0&0&0&-1&0&0&0\\ 0&0&0&0&1&0&0\\ 0&0&0&0&0&1&0\\ 0&0&0&0&1&0&-1 \end{bmatrix}, A_3 = \begin{bmatrix} -1&0&0&0&0&0&0\\ 0&1&0&0&0&0&0\\ 0&0&-1&0&0&0&0\\ 0&0&0&-1&0&0&0\\ 0&0&0&0&-1&0&0\\ 0&0&0&0&0&1&0\\ 0&0&0&0&0&0&1 \end{bmatrix}.$$

Furthermore, by inducing the trivial representation of H', we get:

$$\chi : x \mapsto A_0, \quad a, b, c \mapsto I_7.$$

As $Frob(56)/H' \cong C_7$, χ is the direct sum of $\chi_t, t = 0, \dots, 6$ and has the trivial representation in its constituent. However, if $\delta = \sum_{t=0}^{6} a_t x^t H' \in \mathbb{Z}[Frob(56)/H']$, then it's translate is $xH'\delta = \sum_{t=0}^{6} a_t x^{t+1} H'$. This shows that translation of δ results in linear shift of coefficients. Thus, $\chi(\hat{D})$ is a circulant matrix and hence, using the C_7 images, we get $\chi(\hat{D}) = 10J_7 - 7I_7$ or $\chi(\hat{D}) = 8J_7 + 7I_7$. Furthermore, $\chi(\hat{D})J_7 = 63J_7$, $\chi(Frob(56)) = 8J_7$ and $\chi(\hat{D})\chi(\hat{D})^{(-1)} = 49I_5 + 14 \cdot 8 \cdot 5J_5 = 49I_7 + 560J_7$. The representation ψ is irreducible and does not have the trivial representation in its constituent, then $\psi(\hat{D}) \cdot \psi(\hat{D})^{(-1)} = 49 \cdot I_7$. Just like in the $Frob(20)$ case, the rows and columns of $\psi(\hat{D})$ have the same property. Also, the entries of $\psi(\hat{D})$ are real and hence the characters of $\psi(\hat{D})$ are real valued (but the converse in not necessarily true). Consequently,

(1) any two distinct rows of $\psi(\hat{D})$ are orthogonal
(2) the inner product of any row of $\psi(\hat{D})$ by itself is 49
(3) $\psi(\hat{D})J = J\psi(\hat{D}) = \pm 7J$

The above information along with remark 2 will be helpful in deciding the existence or otherwise of (280, 63, 14) difference set image in this group.

5. Difference set images in some factor groups of order 70

5.1. **The C_{35} images.** Suppose that $G/N \cong C_{35} = \langle x, y : x^7 = y^5 = 1 = [x, y] \rangle$. As the ideal generated by 7 factors trivially in the ring $\mathbb{Z}[\zeta_{35}]$, the alias is of the form $\pm 7\zeta_{35}^{j}, j = 0, \dots, 34$. Thus, the difference set images are $F_1 = 7 + 2\langle x \rangle(y + y^2 + y^3 + y^4)$ and $F_2 = 7y + (1 + y)\langle x \rangle + 2\langle x \rangle(y^2 + y^3 + y^4)$. The other solutions that are not images are $F_3 = -7 + 2\langle x \rangle\langle y \rangle$ and $F_4 = -7y + (1 + 3y)\langle x \rangle + 2\langle x \rangle(y^2 + y^3 + y^4)$.

5.2. **There are no $C_{70} \cong C_{35} \times C_2$ images.** Suppose that $G/N \cong C_{35} \times C_2 = \langle x, y : x^7 = y^5 = [x, y] = 1 \rangle \times \langle z : z^2 = 1 \rangle$. As this group is of the form (2.11), we use (2.13) to get

$$\hat{D} = F_i \left(\frac{\langle z \rangle}{2} \right) + gB_j \left(\frac{2 - \langle z \rangle}{2} \right), g \in C_{35} \times C_2 \tag{5.1}$$

where $K = C_{35}$, $|K| = 35$, $\alpha = 2$, $B_j = F_j - 2K$, $i = 1, 2, j = 1, 2, 3, 4$. Note that F_i and F_j are difference set images in C_{35} for $i = j = 1, 2$ while F_j is other solution, $j = 3, 4$. The solutions to (5.1) are $7 - \langle x \rangle + \langle x \rangle(y + y^2 + y^3 + y^4) + \langle x \rangle\langle y \rangle z$, $7 + \langle x \rangle(y + y^2 + y^3 + y^4)\langle z \rangle$ and $7 + \langle x \rangle(y + y^2 + y^3) + \langle x \rangle\langle y \rangle z$. However, none of these solutions is a difference set image because either one of the entries is negative or one intersection number exceeds coset bound of 4. Dillon trick also implies that there are no difference set images in D_{35}.

6. CONCLUDING REMARKS

The existence or otherwise of (280, 63, 14) difference sets is almost decided. Our search reveals that, out of the forty groups of order 280, only three with GAP location numbers [18] $(280, cn)$, where $cn = 2, 6, 33$ could possibly admit this difference sets. To finish up, one needs to start by finding the complete difference set images in $G/N \cong Q_{28}$, $G/N \cong C_7 \rtimes C_8$ and $G/N \cong (C_2)^3 \rtimes C_7$ if they exist. Thereafter, one can either construct (280, 63, 14) difference sets or show that such construction is impossible.

ACKNOWLEDGEMENTS

The author would like to thank the anonymous referee

REFERENCES

[1] E. Lander, *Symmetric design: an algebraic approach,* London Math. Soc. Lecture Note Series 74, Cambridge Univ. Press, 1983.

[2] L. E. Kopilovich,*Difference sets in non cyclic abelian groups* Cybernetics **2** (25) 153-157, 1996.

[3] D. Jungnickel, A. Pott, and K. W. Smith, *Difference sets, The CRC Handbook of Combinatorial Designs* , Preprint, C.J. Colbourn and J.H. Dinitz (eds.), CRC Press, 2005.

[4] O. Gjoneski, A. S. A. Osifodunrin and K. W. Smith, *Non existence of (176, 50, 14) and (704, 38, 2) difference sets*, to appear.

[5] A. S. Osifodunrin and K. W. Smith *On the existence of (160, 54, 18) difference sets*, to appear.

[6] A. S. A. Osifodunrin, *Investigation of Difference Sets With Order 36*, Ph.D dissertation, Central Michigan University, Mount Pleasant, MI, U.S.A, 2008.

[7] Robert liebler, *The Inversion Formula,* J. Combin. Math. and Combin. Computing, **13** 143-160, 1993.

[8] J. E.IiAMS,*Lander's Tables are complete ,Difference sets, sequences and their correlation properties*, Kluwer Aca.Publis. 239-257, 1999.

[9] K. W. Smith, *Non-Abelian Difference sets* J.Comb.Theory A 144-156, 1993.

[10] A. Pott, *Finite Geometry and Character Theory,* Springer-Verlag Publishers, 1995.

[11] B. Schmidt, *Cyclotomic Integers and Finite Geometry*, Jour. of Ame. Math. Soc. **4** (12) 929-952, 1999.

[12] S. L. Ma, *Planar functions, relative difference sets and character theory*, J. of Algebra, **185** 342-356, 1996.

[13] S. Lang, *Algebraic number theory*, Addison-Wesley, Reading, MA, 1970.

[14] R. Turyn, *Character sums and difference set,* Pacific J. Math. **15** 319-346, 1965.

[15] J. Dillon, *Variations on a scheme of McFarland for noncyclic difference sets*, J. Comb. Theory A **40** 9-21, 1985.

[16] W. Ledermann, *Introduction to Group Characters*, Cambridge Univ. Press, Cambridge, 1977.

[17] J. A. Davis and J. Jedwab, *A unifying construction for difference sets,* J. Combin. Theory A, N.**1** (80) 13-78, 1997.

[18] The GAP Group, *GAP-Groups, Algorithms and Programming, Version 4. 4. 6* (retrieved from http://www.gap.gap-system.org in 2006).

DEPARTMENT OF MATHEMATICS,FACULTY OF SCIENCE, UNIVERSITY OF LAGOS, LAGOS, NIGERIA

E-mail address: asaosifodunrin@yahoo.com