Journal of the Nigerian Mathematical Society
Vol. 38, Issue 1, pp. 11-19, 2019


# NON-EXISTENCE OF (155, 56, 20) DIFFERENCE SETS

A. S. A. OSIFODUNRIN[1] AND J. AIZEBEOKHAI

ABSTRACT. It is known that (155, 56, 20) abelian difference set does not exist. Using methods in algebraic number theory and representation theory, we conclude that there are no non-abelian (155, 56, 20) difference sets.

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

## 1. Introduction

Let $D$, the set consisting of $k$ elements, be a subset of a multiplicative group $G$ of order $v$ with $k < v$. If every non-identity element, $g$, of $G$ can be recovered $\lambda$ times by the multi-set $\{g = d_1 d_2^{-1} : d_1, d_2 \in D, d_1 \neq d_2\}$, then $D$ is called a non-trivial $(v, k, \lambda)$ difference set. The natural number $n := k - \lambda$ is known as the order of the difference set. If $G$ is abelian (resp. non abelian or cyclic) then $D$ is known as abelian (resp. non abelian or cyclic) difference set. The parameter set (155, 56, 20) is one of 18 difference set parameters satisfying the algebraic equation $\chi(D)\overline{\chi(D)} = 36$, where $\chi$ is a non trivial representation of $G$[1]. Most of the abelian difference sets in this category have been decided while most of the non-abelian cases remain unsolved. In the case of (155, 56, 20) parameter set, there are two groups of order 155 of which one is abelian. Lander [2](Theorem 4.19) showed that abelian (155, 56, 20) difference set does not exist. This paper explores the possibility of existence of this parameter set in the non abelian group but our method applies to both abelian and non abelian groups. We conclude the following:

**Theorem 1.1.** *There are no (155, 56, 20) difference sets.*

In this paper, $G$ is a group of order 155. In section 2, we state basic results and give a brief description of the method used in this paper. While in sections 3 and 4, we establish the main theorem.

Received by the editors July 23, 2017; Revised December 30, 2018 ; Accepted: January 30, 2019
www.nigerianmathematicalsociety.org; Journal available online at https://ojs.ictp.it/jnms/
[1]Corresponding author

## 2. Preliminary

We start with some background information.

We assume basic knowledge of representation and group theories.

Let $G$ be a group of order $v$ and $D$, a $(v, k, \lambda)$ 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 $\sum_{g\in G} g$ of $\mathbb{Z}[G]$. The sum of inverses of elements of $D$ is $D^{(-1)} = \sum_{g\in G} g^{(-1)}$. Consequently, $D$ is a difference set if and only if

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

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 $\chi$. 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 $G/G'$. The positive integer $m$ is the exponent of the group $G$ if $g^m = 1$ for all $g \in G$. If $\zeta_m := e^{\frac{2\pi i}{m}}$ is a primitive m-th root of unity, then $K_m := \mathbb{Q}(\zeta_m)$ is the cyclotomic extension of the set of rational numbers, $\mathbb{Q}$. Without loss of generality, we may replace $\mathbb{C}$ by the field $K_m$ (known as the splitting field of $G$). This field is a Galois extension of degree $\phi(m)$, ($\phi$ is the Euler function) and a basis for $K_m$ over $\mathbb{Q}$ is $S = \{1, \zeta_m, \zeta_m^2, \ldots, \zeta_m^{\phi(m)-1}\}$. $S$ is also the integral basis for $\mathbb{Z}[\zeta_m]$. Thus, the central primitive idempotents in $\mathbb{C}[G]$ is

$$e_{\chi_i} = \frac{\chi_i(1)}{|G|} \sum_{g\in G} \chi_i(g)g^{-1} = \frac{1}{|G|} \sum_{g\in G} \overline{\chi_i(g)}g \tag{2.2}$$

where $\chi_i$ is an irreducible character of $G$ and $\{e_{\chi_i} : \chi_i \in G^*\}$ is a basis for $\mathbb{C}[G]$.

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 $X_i$ on the $e_\chi$'s under the action of the Galois group of $K_m$ over $\mathbb{Q}$. That is,

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

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 $\chi_i(x) = \zeta_{p^m}^i, i = 0, \ldots, m-1$ then the rational idempotents are

$$[e_{\chi_0}] = \frac{1}{p^m}\langle x\rangle, \tag{2.3}$$

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

$$[e_{\chi_{p^j}}] = \frac{1}{p^{j+1}}\left(p\langle x^{p^{m-j}}\rangle - \langle x^{p^{m-j-1}}\rangle\right). \tag{2.4}$$

The following yields the general formula employed in the search of difference set [3].

**Theorem 2.1.** *Let $G$ be an abelian group and $G^*/\sim$ is the set of equivalence classes of characters. Suppose that $\{\chi_0, \chi_1, \ldots, \chi_s\}$ is a system of distinct representatives for the equivalence classes of $G^*/\sim$.*

*Then for $A \in \mathbb{Z}[G]$, we have*

$$A = \sum_{i=0}^{s} \alpha_i [e_{\chi_i}], \tag{2.5}$$

*where $\alpha_i$ is any $\chi_i$-alias for $A$.*

Equation (2.5) is known as **the rational idempotent decomposition** of $A$.

Now, suppose that $\psi : G \longrightarrow G/N$ is a homomorphism then we can extend $\psi$, by linearity, to the corresponding group rings. Given that $D$ is a $(v, k, \lambda)$ difference set in $G$, a group of order $v$ and $H$ is a homomorphic image of $G$ with kernel $N$. Then the contraction of $D$ with respect to the kernel $N$ is the multi-set $D/N = \psi(D) = \{dN : d \in D\}$ (also called the difference set image in $H$). If $T^* = \{1, t_1, \ldots, t_h\}$ is a left transversal of $N$ in $G$ then we write $\hat{D} = \sum_{t_j \in G} d_j t_j N$ 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 $\psi(D)$, the difference set image in a homomorphic image of $G$ and denote the number of times $d_i$ equals $i$ by $m_i \geq 0$. The following results follow immediately.

**Lemma 2.2.** *Let $D$ be a difference set in a group $G$ and $N$, a normal subgroup of $G$. Suppose that $\psi : G \longrightarrow G/N$ be 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)* $\chi(\hat{D})\overline{\chi(\hat{D})} = n \cdot 1_{G/N}$, *where $\chi$ is a non trivial representation of $G/N$*

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

**Lemma 2.3.** *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*

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

According to Turyn [4], 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 to $p$. This means that every prime ideals over $n$ in $\mathbb{Z}[\zeta_m]$ are fixed by complex conjugation. Consequently, the construction of elements of length $n$ is trivial in $\mathbb{Z}[\zeta_m]$. To successfully obtain the difference set images, we need the aliases. The alias requires the knowledge of how the ideal generated by $\chi(\hat{D})$ factors in the cyclotomic ring $\mathbb{Z}[\zeta_m]$, $\zeta_m$ is the $m^{th}$ root of unity and $m$ is the exponent of $G/N$. For the purpose of this paper, if $\chi$ is not a principal character then $|\chi(\hat{D})| = 6$ and we need to know how the ideal generated by 2 and 3 factor in $\mathbb{Z}[\zeta_m]$, $m = 5, 31$. All the necessary algebraic numbers will be determined by a theorem due to Kronecker that states that any algebraic integer all whose conjugates have absolute value 1 must be a root of unity[5].

## 3. Abelian group of order 155 and it's linear representations

The group $C_{155} = \langle x, y : x^{31} = y^5 = [x, y] = 1\rangle$ has a cyclic homomorphic image of order 31. Let $N$ be the normal subgroup of $G$ of order 5 such that $G/N \cong C_{31}$. So we explore difference set image in the cyclic homomorphic image of order 31.

3.1. **There are no difference set image in $G/N \cong C_{31}$.** The linear representations (characters) of the group $G/N = \langle x : x^{31} = 1\rangle$ are of the form $\chi_j(x) = \zeta_{31}^j$, $j = 0, \ldots, 30$, $\chi_j(y) = 1$. Thus, the rational idempotents are

$$[e_{\chi_0}] = \frac{1}{31}\langle x\rangle \quad \text{and} \quad [e_{\chi_1}] = \frac{1}{31}(31 - \langle x\rangle)$$

with

$$\hat{D} = \alpha_{\chi_0}[e_{\chi_0}] + \alpha_{\chi_1}[e_{\chi_1}](using(2.5)),$$

where $\alpha_{\chi_0} \in \mathbb{Z}^+$, $\alpha_{\chi_1} \in \mathbb{Z}[\zeta_{31}]$. The ideal generated by 3 does not factor in $\mathbb{Z}[\zeta_{31}]$ while that generated by 2 has six factors[5]. Thus, we need principal ideal $\pi$ such that $\pi\bar{\pi} = \langle 2\rangle$ and $\pi$ is a product of three factors. An ideal is principal when the class number is zero. Smith, Franklin and Sam [6] used a software, PARI to show that the class number of each of the six factors of $\langle 2\rangle$ are distinct and lies between 1 and 8. This implies that algebraic number 2 factors trivially in $\mathbb{Z}[\zeta_{31}]$ and consequently, $\alpha_{\chi_1} \in \{\pm 6x^j\}, j = 0, 1, ..., 30$. Hence,

$$\hat{D} = 56[e_{\chi_0}] \pm 6x^j[e_{\chi_1}].$$

As the sum on the right hand side must be divisible by 31, we choose the alias $-6$ with $j = 0$. Thus, $\hat{D} = -6 + 2\langle x\rangle$.

However, the intersection numbers are non-negative, so $\hat{D}$ is not a viable difference set image. Hence, $C_{31}$ has no difference set image. Consequently, the group $C_{155}$ does not admit (155, 56, 20) difference sets.

## 4. Non abelian group of order 155 and it's representations

The non abelian group of order 155 is $G = C_{31} \rtimes C_5 = \langle x, y : x^{31} = y^5 = 1, yxy^{-1} = x^2 \rangle$. The derived(commutator) subgroup of this group is $G' = \langle x \rangle \cong C_{31}$. Since any linear representation will have the derived subgroup $G'$ in it's kernel, it follows that $G/G' \cong \langle y \rangle$, a cyclic group of order 5. This shows that $G$ has five inequivalent linear representations described as follows:

$$\chi_j(x) = 1, \chi_j(y) = \zeta^j, j = 0, \ldots, 4. \tag{4.1}$$

Suppose that $\hat{D} = \sum_{j=0}^{4} d_j y^j$ is the difference set image in group $G/G' \cong C_5 = \langle y : y^5 = 1 \rangle$. This set is viewed as a $1 \times 5$ matrix with columns indexed by powers of $y$. By applying the linear representation (4.1) to $\hat{D}$, we get two rational idempotents:

$$[e_{\chi_0}] = \frac{1}{5}\langle y \rangle \quad \text{and} \quad [e_{\chi_1}] = \frac{(5 - \langle y \rangle)}{5}.$$

Using the above idempotents, the difference set equation is $\hat{D} = \alpha_{e_{\chi_0}}[e_{\chi_0}]$ $+\alpha_{e_{\chi_1}}[e_{\chi_1}]$ where , $\alpha_{e_{\chi_0}} = 56$ and $\alpha_{e_{\chi_1}} = \pm 6y^j$, since ideals generated by 2 and 3 are primes in $\mathbb{Z}(\zeta_5)$. We translate, if necessary, to obtain the unique difference set image in $G/G' \cong C_5$ as $6 + 10\langle y \rangle$.

Now, suppose that difference set exists in $G$. We take this object to be $D = \sum_{i=0}^{30} \sum_{j=0}^{4} d_{i,j} x^i y^j$ and view it as $5 \times 31$ matrix with columns indexed by powers of $x$ and rows indexed by powers of $y$. Furthermore, suppose that $\zeta_{31}$ is the thirty first root of unity and consider the Galois automorphism $\sigma(\zeta_{31}) = \zeta_{31}^2$. This automorphism divides the basis elements of $\mathbb{Z}[C_{31}]$ into seven orbits. These are

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

$$\zeta_{31} \to \zeta_{31}^2 \to \zeta_{31}^4 \to \zeta_{31}^8 \to \zeta_{31}^{16} \to \zeta_{31}$$

$$\zeta_{31}^3 \to \zeta_{31}^6 \to \zeta_{31}^{12} \to \zeta_{31}^{24} \to \zeta_{31}^{17} \to \zeta_{31}^3$$

$$\zeta_{31}^5 \to \zeta_{31}^{10} \to \zeta_{31}^{20} \to \zeta_{31}^9 \to \zeta_{31}^{18} \to \zeta_{31}^5$$

$$\zeta_{31}^7 \to \zeta_{31}^{14} \to \zeta_{31}^{28} \to \zeta_{31}^{25} \to \zeta_{31}^{19} \to \zeta_{31}^7$$

$$\zeta_{31}^{11} \to \zeta_{31}^{22} \to \zeta_{31}^{13} \to \zeta_{31}^{26} \to \zeta_{31}^{21} \to \zeta_{31}^{11}$$

$$\zeta_{31}^{15} \to \zeta_{31}^{30} \to \zeta_{31}^{29} \to \zeta_{31}^{27} \to \zeta_{31}^{23} \to \zeta_{31}^{15}$$

These orbits are used to define the non linear representations of $G$ by inducing the non-trivial characters of $G'$. These correspond to six degree five representations of $G$ but they are all equivalent under a Galois automorphism and one of them is given below:

$$\chi : x \mapsto \begin{bmatrix} \zeta & 0 & 0 & 0 & 0 \\ 0 & \zeta^2 & 0 & 0 & 0 \\ 0 & 0 & \zeta^4 & 0 & 0 \\ 0 & 0 & 0 & \zeta^8 & 0 \\ 0 & 0 & 0 & 0 & \zeta^{16} \end{bmatrix}, \quad y \mapsto \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

As this representation $\chi$ is irreducible and does not have the trivial representation in its constituent, then $\chi(D) \cdot \overline{\chi(D)} = 36 \cdot I_5$. By applying this degree five representation, $\chi$ to $D$ we get

$$\chi(D) = \begin{bmatrix} A & B & C & D & E \\ \sigma(E) & \sigma(A) & \sigma(B) & \sigma(C) & \sigma(D) \\ \sigma^2(D) & \sigma^2(E) & \sigma^2(A) & \sigma^2(B) & \sigma^2(C) \\ \sigma^3(C) & \sigma^3(D) & \sigma^3(E) & \sigma^3(A) & \sigma^3(B) \\ \sigma^4(B) & \sigma^4(C) & \sigma^4(D) & \sigma^4(E) & \sigma^4(A) \end{bmatrix},$$

where $A = d_{0,0} + d_{1,0}\zeta + d_{2,0}\zeta^2 + d_{3,0}\zeta^3 + \cdots + d_{30,0}\zeta^{30}$;
$B = d_{0,1} + d_{1,1}\zeta + d_{2,1}\zeta^2 + d_{3,1}\zeta^3 + \cdots + d_{30,1}\zeta^{30}$;
$C = d_{0,2} + d_{1,2}\zeta + d_{2,2}\zeta^2 + d_{3,2}\zeta^3 + \cdots + d_{30,2}\zeta^{30}$;
$D = d_{0,3} + d_{1,3}\zeta + d_{2,3}\zeta^2 + d_{3,3}\zeta^3 + \cdots + d_{30,3}\zeta^{30}$ and
$E = d_{0,4} + d_{1,4}\zeta + d_{2,4}\zeta^2 + d_{3,4}\zeta^3 + \cdots + d_{30,4}\zeta^{30}$ with $A, B, C, D, E \in \mathbb{Z}[\zeta]$.
Furthermore, as $G/G' \cong C_5$, then

$$\sum_{i=0}^{30} d_{i,0} = 16, \sum_{i=0}^{30} d_{i,1} = 10, \sum_{i=0}^{30} d_{i,2} = 10, 10, \tag{4.2}$$

$$\sum_{i=0}^{30} d_{i,3} = 10, \sum_{i=0}^{30} d_{i,4} = 10, \tag{4.3}$$

$d_{i,j} \in \{0, 1\}, j = 0, 1, 2, 3, 4$. Thus,

$$\chi(D)\overline{\chi(D)} = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} \\ a_{31} & a_{32} & a_{33} & a_{34} & a_{35} \\ a_{41} & a_{42} & a_{43} & a_{44} & a_{45} \\ a_{51} & a_{52} & a_{53} & a_{54} & a_{55} \end{bmatrix}$$

with

$$a_{11} = A\bar{A} + B\bar{B} + C\bar{C} + D\bar{D} + E\bar{E} = 36 \tag{4.4}$$

$$a_{12} = A\overline{\sigma(E)} + B\overline{\sigma(A)} + C\overline{\sigma(B)} + D\overline{\sigma(C)} + E\overline{\sigma(D)} = 0 \tag{4.5}$$

$$a_{13} = A\overline{\sigma^2(D)} + B\overline{\sigma^2(E)} + C\overline{\sigma^2(A)} + D\overline{\sigma^2(B)} + E\overline{\sigma^2(C)} = 0 \quad (4.6)$$

$$a_{14} = A\overline{\sigma^3(C)} + B\overline{\sigma^3(D)} + C\overline{\sigma^3(E)} + D\overline{\sigma^3(A)} + E\overline{\sigma^3(B)} = 0 \quad (4.7)$$

$$a_{15} = A\overline{\sigma^4(B)} + B\overline{\sigma^4(C)} + C\overline{\sigma^4(D)} + D\overline{\sigma^4(E)} + E\overline{\sigma^4(A)} = 0 \quad (4.8)$$

$a_{21} = \sigma(E)\bar{A} + \sigma(A)\bar{B} + \sigma(B)\bar{C} + \sigma(C)\bar{D} + \sigma(D)\bar{E} = 0$
$a_{22} = \sigma(E)\overline{\sigma(E)} + \sigma(A)\overline{\sigma(A)} + \sigma(B)\overline{\sigma(B)} + \sigma(C)\overline{\sigma(C)} + \sigma(D)\overline{\sigma(D)} = 36$
$a_{23} = \sigma(E)\overline{\sigma^2(D)} + \sigma(A)\overline{\sigma^2(E)} + \sigma(B)\overline{\sigma^2(A)} + \sigma(C)\overline{\sigma^2(B)} + \sigma(D)\overline{\sigma^2(C)} = 0$
$a_{24} = \sigma(E)\overline{\sigma^3(C)} + \sigma(A)\overline{\sigma^3(D)} + \sigma(B)\overline{\sigma^3(E)} + \sigma(C)\overline{\sigma^3(A)} + \sigma(D)\overline{\sigma^3(B)} = 0$
$a_{25} = \sigma(E)\overline{\sigma^4(B)} + \sigma(A)\overline{\sigma^4(C)} + \sigma(B)\overline{\sigma^4(D)} + \sigma(C)\overline{\sigma^4(E)} + \sigma(D)\overline{\sigma^4(A)} = 0$
$a_{31} = \sigma^2(D)\bar{A} + \sigma^2(E)\bar{B} + \sigma^2(A)\bar{C} + \sigma^2(B)\bar{D} + \sigma^2(C)\bar{E} = 0$
$a_{32} = \sigma^2(D)\overline{\sigma(E)} + \sigma^2(E)\overline{\sigma(A)} + \sigma^2(A)\overline{\sigma(B)} + \sigma^2(B)\overline{\sigma(C)} + \sigma^2(C)\overline{\sigma(D)} = 0$
$a_{33} = \sigma^2(D)\overline{\sigma^2(D)} + \sigma^2(E)\overline{\sigma^2(E)} + \sigma^2(A)\overline{\sigma^2(A)} + \sigma^2(B)\overline{\sigma^2(B)} + \sigma^2(C)\overline{\sigma^2(C)} = 36$
$a_{34} = \sigma^2(D)\overline{\sigma^3(C)} + \sigma^2(E)\overline{\sigma^3(D)} + \sigma^2(A)\overline{\sigma^3(E)} + \sigma^2(B)\overline{\sigma^3(A)} + \sigma^2(C)\overline{\sigma^3(B)} = 0$
$a_{35} = \sigma^2(D)\overline{\sigma^4(B)} + \sigma^2(E)\overline{\sigma^4(C)} + \sigma^2(A)\overline{\sigma^4(D)} + \sigma^2(B)\overline{\sigma^4(E)} + \sigma^2(C)\overline{\sigma^4(A)} = 0$
$a_{41} = \sigma^3(C)\bar{A} + \sigma^3(D)\bar{B} + \sigma^3(E)\bar{C} + \sigma^3(A)\bar{D} + \sigma^3(B)\bar{E} = 0$
$a_{42} = \sigma^3(C)\overline{\sigma(E)} + \sigma^3(D)\overline{\sigma(A)} + \sigma^3(E)\overline{\sigma(B)} + \sigma^3(A)\overline{\sigma(C)} + \sigma^3(B)\overline{\sigma(D)} = 0$
$a_{43} = \sigma^3(C)\overline{\sigma^2(D)} + \sigma^3(D)\overline{\sigma^2(E)} + \sigma^3(E)\overline{\sigma^2(A)} + \sigma^3(A)\overline{\sigma^2(B)} + \sigma^3(B)\overline{\sigma^2(C)} = 0$
$a_{44} = \sigma^3(C)\overline{\sigma^3(C)} + \sigma^3(D)\overline{\sigma^3(D)} + \sigma^3(E)\overline{\sigma^3(E)} + \sigma^3(A)\overline{\sigma^3(A)} + \sigma^3(B)\overline{\sigma^3(B)} = 36$
$a_{45} = \sigma^3(C)\overline{\sigma^4(B)} + \sigma^3(D)\overline{\sigma^4(C)} + \sigma^3(E)\overline{\sigma^4(D)} + \sigma^3(A)\overline{\sigma^4(E)} + \sigma^3(B)\overline{\sigma^4(A)} = 0$
$a_{51} = \sigma^4(B)\bar{A} + \sigma^4(C)\bar{B} + \sigma^4(D)\bar{E} + \sigma^4(E)\bar{D} + \sigma^4(A)\bar{E} = 0$
$a_{52} = \sigma^4(B)\overline{\sigma(E)} + \sigma^4(C)\overline{\sigma(A)} + \sigma^4(D)\overline{\sigma(B)} + \sigma^4(E)\overline{\sigma(C)} + \sigma^4(A)\overline{\sigma(D)} = 0$
$a_{53} = \sigma^4(B)\overline{\sigma^2(D)} + \sigma^4(C)\overline{\sigma^2(E)} + \sigma^4(D)\overline{\sigma^2(A)} + \sigma^4(E)\overline{\sigma^2(B)} + \sigma^4(A)\overline{\sigma^2(C)} = 0$
$a_{54} = \sigma^4(B)\overline{\sigma^3(C)} + \sigma^4(C)\overline{\sigma^3(D)} + \sigma^4(D)\overline{\sigma^3(E)} + \sigma^4(E)\overline{\sigma^3(A)} + \sigma^4(A)\overline{\sigma^3(B)} = 0$
$a_{55} = \sigma^4(B)\overline{\sigma^4(B)} + \sigma^4(C)\overline{\sigma^4(C)} + \sigma^4(D)\overline{\sigma^4(D)} + \sigma^4(E)\overline{\sigma^4(E)} + \sigma^4(A)\overline{\sigma^4(A)} = 36.$

We need the following lemma to continue.

**Lemma 4.1.** *If $F = \sum_{i=0}^{30} d_{i,j}\zeta^i \in \mathbb{Z}[C_{31}]$ has exactly $m$ coefficients $d_{i,0}$ that are equal to one and other are equal to zero, then the sum of coefficients of $F\overline{F}$ is $m^2$.*

*Proof.* Without loss of generality, we pick any of the coefficients of $F$ say $d_{1,j}$ and assume that $d_{1,j} = 0$. Then for any coefficient $d_{i,j}$ of $\overline{F}$, $(d_{1,j})(d_{i,j}) = 0, i = 0, \ldots, 30$ and $\sum_{i=0}^{30}(d_{1,j})(d_{i,j}) = 0$. On the other hand, suppose that $d_{1,j} = 1$, then for any coefficient $d_{i,j}$ of $\overline{F}$, $(d_{1,j})(d_{i,j}) = 1$ if $d_{i,j} = 1$ and $(d_{1,j})(d_{i,j} = 0$ if $d_{i,j} = 0$. By adding these products together, we get $\sum_{i=0}^{30}(d_{1,j})(d_{i,j}) = m$. As exactly $m$ coefficients of $F$ are equal to one, then there are $m$ such sums and consequently, the sum of coefficients of $F\overline{F}$ is $m^2$ □

Furthermore, since $d_{i,j}$ is either 1 or 0 and the fact that the sum of the coefficients of the algebraic numbers $A$, $B$, $C$, $D$ and $E$ are respectively 16, 10, 10, 10 and 10, by Lemma 4.1, the sum of the coefficients of $A\bar{A}$, $B\bar{B}$, $C\bar{C}$, $D\bar{D}$ and $E\bar{E}$ are $16^2$, $10^2$, $10^2$, $10^2$ and $10^2$ respectively. Consequently, we can write each of these algebraic numbers as follows:

$$A\bar{A} = 16 + \sum_{i=1}^{30} \alpha_i \zeta^i, \quad B\bar{B} = 10 + \sum_{i=1}^{30} \beta_i \zeta^i, \quad C\bar{C} = 10 + \sum_{i=1}^{30} \gamma_i \zeta^i,$$

$$D\bar{D} = 10 + \sum_{i=1}^{30} \delta_i \zeta^i \quad \text{and} \quad E\bar{E} = 10 + \sum_{i=1}^{30} \mu_i \zeta^i$$

with

$$\sum_{i=1}^{30} \alpha_i = 240, \sum_{i=1}^{30} \beta_i = \sum_{i=1}^{30} \gamma_i = \sum_{i=1}^{30} \delta_i = \sum_{i=1}^{30} \mu_i = 90, \tag{4.9}$$

$\alpha_i, \beta_i, \gamma_i, \delta_i, \mu_i \in \mathbb{Z}^+$, the set of non negative integers. Thus,

$$A\bar{A} + B\bar{B} + C\bar{C} + D\bar{D} + E\bar{E} = 36 + 20 + \sum_{i=1}^{30} \alpha_i \zeta^i + \sum_{i=1}^{30} \beta_i \zeta^i + \sum_{i=1}^{30} \gamma_i \zeta^i + \sum_{i=1}^{30} \delta_i \zeta^i + \sum_{i=1}^{30} \mu_i \zeta^i. \tag{4.10}$$

From (4.4), difference set exists if and only if

$$20 + \sum_{i=1}^{30} \alpha_i \zeta^i + \sum_{i=1}^{30} \beta_i \zeta^i + \sum_{i=1}^{30} \gamma_i \zeta^i + \sum_{i=1}^{30} \delta_i \zeta^i + \sum_{i=1}^{30} \mu_i \zeta^i = 0. \tag{4.11}$$

This last equation implies that $20 + \sum_{i=1}^{30}(\alpha_i + \beta_i + \gamma_i + \delta_i + \mu_i)\zeta^i = 0$. By the Kronecker Theorem,

$$\alpha_i + \beta_i + \gamma_i + \delta_i + \mu_i = 20 \tag{4.12}$$

for every $i = 1, \ldots, 30$. This condition gives rise to 30 equations with 150 variables. We obtained all the possible values of $(\alpha_i, \beta_i, \gamma_i, \delta_i, \mu_i)$ (there are 10626 such quintets) such that (4.12) is true. However, a search for viable $A$, $B$, $C$, $D$ and $E$ using equations (4.2), (4.3),(4.4), (4.5), (4.6), (4.7), (4.8), (4.9) and (4.12) produced no solution. Hence, there are no

algebraic numbers $A$, $B$, $C$, $D$ and $E$ such that $A\bar{A}+B\bar{B}+C\bar{C}+D\bar{D}+E\bar{E}=36$.

## 5. CONCLUDING REMARKS

Based on the above, we conclude that there are no (155, 56, 20) difference sets.

## ACKNOWLEDGEMENTS

The authors would like to thank the anonymous referee

## REFERENCES

[1] A. S. A. Osifodunrin, *Investigation of Difference Sets With Order 36*, Ph.D dissertation, Central Michigan University, Mount Pleasant, MI, U.S.A, 2008.
[2] E. Lander, *Symmetric design: an algebraic approach,* London Math. Soc. Lecture Note Series 74, Cambridge Univ. Press, 1983.
[3] Robert liebler, *The Inversion Formula,* J. Combin. Math. and Combin. Computing, **13** 143-160, 1993.
[4] R. Turyn, *Character sums and difference set,* Pacific J. Math. **15** 319-346, 1965.
[5] A. Pott, *Finite Geometry and Character Theory*, Springer-Verlag Publishers, 1995.
[6] B. Franklin and S. Sam, *Non existence of some cyclic difference sets.* Retrieved on Aug.10, 2007 from: http://www.cst.cmich.edu/users/smith1kw/

DEPARTMENT OF MATHEMATICS, HOUSTON COMMUNITY COLLEGE, NORTHLINE CAMPUS, HOUSTON, TEXAS, 77022, USA
*E-mail address*: asaosifodunrin@yahoo.com, solomon.osifodunrin@hccs.edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF LAGOS,AKOKA, LAGOS, NIGERIA
*E-mail addresses*: joshino95@gmail.com