Kragujevac Journal of Mathematics
Volume 35 Number 3 (2011), Pages 479–492.

DO (1276, 51, 2) DIFFERENCE SETS EXIST?

ADEGOKE S. A. OSIFODUNRIN

Abstract. It is known that the $(v, k, 2)$ symmetric designs otherwise called biplanes exist for some integer values $k < 16$. Based on the relationship between symmetric designs and difference sets, we investigate the existence of (1276, 51, 2) difference sets. Some authors have established the non existence of abelian (1276, 51, 2) difference sets. Using representation and algebraic number theories, we show that this difference sets do not exist in most groups of order 1276.

1. Introduction

Suppose that G is a multiplicative group of order v and D is k-subset of G with $k < v$. Then D is a (v, k, λ) difference set if every non-identity element of G can be reproduced exactly 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 $n := k - \lambda$ characterizes D and is called the order of the difference set. Usually, we say that D is abelian (resp. non-abelian or cyclic) difference set if the underlying group G is abelian (resp. non-abelian or cyclic).

A (v, b, r, k, λ) design is an incidence structure consisting of points $\mathcal{P}$, $|\mathcal{P}| = v$ and blocks $\mathcal{B}$, $|\mathcal{B}| = b$ in which distinct points of $\mathcal{P}$ are arranged such that each block is incident with k points, each point is incident with r distinct blocks and every pair of points is incident with λ blocks. In this case, $v > 1$, b are positive integers and r, k, λ are non negative integers. A symmetric design is basically a (v, b, r, k, λ) design in which $b = v$ and $r = k$. The relationship between symmetric designs and difference sets is that a symmetric design admitting a group G as a regular automorphism group

Key words and phrases. Representation, idempotents, difference sets, biplanes.
2010 *Mathematics Subject Classification.* Primary: 05B10, Secondary: 05B20.
Received: August 3, 2010.
Revised: July 21, 2011.

is isomorphic to the development of the difference set (Theorem 4.2, [9]). This means that the existence of difference sets implies the existence of symmetric designs with same parameters. However, the existence of symmetric designs does not necessarily imply that the corresponding difference sets exist [3].

Symmetric designs with $\lambda = 1$ (symmetric 1-designs) are known as projective planes while symmetric designs with $\lambda = 2$ (symmetric 2-designs) are known as biplanes. Projective planes are known to exist for every prime power [6]. Since there are infinite number of projective planes, many researchers wonder whether the same is true of biplanes. To date, biplanes exist only for $(v, k, 2)$ with $k = 3, 4, 5, 6, 9, 11$ and 13. Daniel Hughes and L. J. Dickey [4] showed with the aid of computer that there are no other biplanes in Singer groups with $n = k - 2 \leq 5000$. Contracted multiplier test [7] was used to show that (1276, 51, 2) difference set does not exist in C_{1276} while Kopilovich [8] showed that $(C_2)^2 \times C_{11} \times C_{29}$ does not admit this difference set. There are 11 groups of order 1276 out of which 2 are abelian. Our focus is on the non-abelian groups of order 1276 but the approach incorporates all groups of this order. In this paper, G is a group of order 1276 and N is a normal subgroup of G of an appropriate order. To achieve our objective, we compute difference set images in factor groups of orders 2, 4, 44, 58 and 116. The main result of this paper is

Theorem 1.1. *There are no* $(1276, 51, 2)$ *difference sets except possibly in* $C_{11} \times (C_{29} \rtimes C_4)$ *or* $C_{319} \rtimes C_4$.

Section 2 reproduces the basic results in representation and algebraic number theories required for this work while in Sections 3 and 4, we prove the main theorem by showing that some factor groups of G do not admit the difference sets.

2. Preliminary results

Let $\mathbb{Z}$ and $\mathbb{C}$ be the ring of integers and field of complex numbers respectively. 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

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

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 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 $S = \{1, \zeta_{m'}, \zeta_{m'}^2, \ldots, \zeta_{m'}^{\phi(m')-1}\}$. 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

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

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, $A = \sum_{\chi \in G^*} \chi(A) e_\chi$.

Suppose that χ is a non-trivial 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 can be shown that algebraic conjugacy is an equivalence relation. 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 field over $\mathbb{Q}$, then **central rational idempotents** in $\mathbb{Q}[G]$ are obtained by summing over the equivalence classes $X_i = \{\chi_i : \chi_i \sim \chi_j\}$ on the e_χ's under the action of the Galois group of $K_{m'}$ over $\mathbb{Q}$. That is,

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

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 $\chi_i(x) = \zeta^i_{p^m}, i = 0, \dots, p^m - 1$, 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 theorem is usually employed in the search of difference sets [12].

Theorem 2.1. *Let G be an abelian group and $G^*/\sim$ be the set of equivalence classes of characters. Suppose that $\{\chi_o, \chi_1, \dots, \chi_s\}$ is a system of distinct representatives for the equivalence classes of $G^*/\sim$. Then for $A \in \mathbb{Z}[G]$, we have*

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

where α_i is any χ_i-alias for A.

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

Dillon [1] 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 2.2 (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 2.1. *If the cyclic group Z_{2m} does not contain a (nontrivial) difference set, then neither does the dihedral group of order $2m$.*

Suppose that $\psi : G \longrightarrow G/N$ is a homomorphism, then we can extend ψ, by linearity, to the corresponding group rings. Given that D is a (v, k, λ) difference set in G, a group of order v and H is a homomorphic image of G with kernel N. Then the difference set image in H (also called the contraction of D with respect to the kernel N) is the multi-set $D/N = \psi(D) = \{dN : d \in D\}$. Furthermore, if $T^* = \{1, t_1, \ldots, t_h\}$ is a left transversal of N in G, then $\hat{D} = \sum_{t_j \in T^*} d_j t_j N$, where the integer $d_j = |D \cap t_j N|$ is called 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 $m_i \geq 0$.

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 2.1. *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*

(a) $\hat{D}\hat{D}^{(-1)} = n \cdot 1_{G/N} + |N|\lambda(G/N)$

(b) $\sum d_i^2 = n + |N|\lambda$

(c) $\chi(\hat{D})\overline{\chi(\hat{D})} = n \cdot I_d$*, where χ is a non-trivial representation of G/N of degree d and I_d is the $d \times d$ identity matrix.*

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

Lemma 2.2. *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 next lemma is a necessary condition (but not sufficient) for the existence of difference set image in G/N.

Lemma 2.3 (The Variance Technique)**.** *Suppose that D is a (v, k, λ) difference set in a group G of order v and H is a factor group of G with kernel N. Let $\hat{D}$ be the difference set image in H and T^* be a left transversal of N in G such that $\{d_i\}$ is a* *sequence of intersection numbers and* $\{m_i\}$*, where* m_i *is the number of times* d_i *equals* i*. Then*

$$\sum_{i=0}^{|N|} m_i = |H|; \quad \sum_{i=0}^{|N|} i m_i = k \quad \text{and} \quad \sum_{i=0}^{|N|} i(i-1)m_i = \lambda(|N|-1) \tag{2.6}$$

The method used in this paper is known as representation theoretic method made popular by Leibler ([12]). Some authors like Iiams [5] and Smith [16] have used this method in search of difference sets. This approach entails the computation of $\Omega_{G/N}$, the set of difference set images in the factor group of G of least order. We garner information about D as we gradually increase the size of the factor group. If at a point the distribution list $\Omega_{G/N}$ is empty, then the group G with factor group G/N does not admit (v, k, λ) difference sets. We use Lemmas 2.1, 2.2 and the difference set equation (2.5) to obtain $\Omega_{G/N}$.

We need the aliases in order to successfully obtain the difference set images. 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 2.1, $\chi(\hat{D})\overline{\chi(\hat{D})} = n$. 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. Thus, $\chi(\hat{D})\overline{\chi(\hat{D})} = n$ 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 $\mathbb{Z}[\zeta_{m'}]$. If $\delta := \chi(\hat{D})$, then by (2.5), 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 $(\delta)(\bar{\delta}) = (n)$. To achieve this,

(a) we must look for all principal ideals $\pi \in \mathbb{Z}[\zeta_m]$ such that $\pi\bar{\pi} = (n)$
(b) for each such ideals, we find a representative element, say δ with $\delta\bar{\delta} = n$ and
(c) 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. We use a theorem due to Kronecker [14, 15] that 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 $\delta' = \delta u$[13], 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 $\{\pm\alpha g^j : j = 0, 1, \ldots, m-1\}$.

We use the following result 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 (p) in the cyclotomic integer ring $\mathbb{Z}[\zeta_{m'}]$ is $\frac{\phi(m')}{d}$, where ϕ is the Euler ϕ-function, i.e. $\phi(m') = |\mathbb{Z}^*_{m'}|$ [10]. For instance, the ideal generated by 7 has four factors in $\mathbb{Z}[\zeta_{m'}], m' = 29, 58$ while the ideal generated by 7 is prime in $\mathbb{Z}[\zeta_{2^s}], s = 1, 2$. 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 $(1 - \zeta_{2^s}) = \overline{(1 - \zeta_{2^s})}$ in $\mathbb{Z}[\zeta_{2^s}]$.

According to Turyn [18], 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 $p^i \equiv -1 \pmod{m'}$. 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, $7^5 \equiv -1 \pmod{m'}$, where $m' = 11, 22, 44, 88$ and $7 \equiv -1 \pmod{m'}$, where $m' = 2, 4$. Thus, $\langle 7 \rangle$ is fixed by conjugation in $\mathbb{Z}[\zeta_{m'}]$. In this paper, we shall use the phrase $\underline{m \text{ factors trivially in } \mathbb{Z}[\zeta_{m'}]}$ if the ideal generated by m is prime(or ramifies) in $\mathbb{Z}[\zeta_{m'}]$ or m is self conjugate modulo m'. In this case if $\hat{D}$ is the difference set image of order $n = m^2$ in H, where H is a group with exponent m' and χ is a non-trivial representation of H then $\chi(\hat{D}) = m\zeta^i_{m'}$, $\zeta_{m'}$ is the m'-th root of unity [15].

As stated earlier, the ideal generated by 7 has four factors in $\mathbb{Z}[\zeta_{m'}]$, where $m' = 29, 58$. Since $\mathbb{Z}[\zeta_{58}] = \mathbb{Z}[-\zeta_{29}] = \mathbb{Z}[\zeta_{29}]$, we focus on $\mathbb{Z}[\zeta_{29}]$ [15]. Suppose $\sigma \in Gal(\mathbb{Q}(\zeta_{29})/\mathbb{Q})$, where $\sigma(\zeta_{29}) = \zeta_{29}^7$. This automorphism split the basis elements of $\mathbb{Q}(\zeta_{29})$ into four orbits as $A := \zeta_{29} + \zeta_{29}^7 + \zeta_{29}^{20} + \zeta_{29}^{24} + \zeta_{29}^{23} + \zeta_{29}^{16} + \zeta_{29}^{25}$, $B := \zeta_{29}^2 + \zeta_{29}^{14} + \zeta_{29}^{11} + \zeta_{29}^{19} + \zeta_{29}^{17} + \zeta_{29}^{3} + \zeta_{29}^{21}$, $\overline{A}$ and $\overline{B}$. It is easy to see that $(7) = (1 + A)(1 + B)(1 + \overline{A})(1 + \overline{B})$. Put $\pi_1 = (1 + A)$ and $\pi_2 = (1 + B)$. Let $\delta_1 = 1 + A$ and $\delta_2 = 1 + B$ be representatives of these ideals. Then the solutions to $\delta\bar{\delta} = 7^2$ are, $\delta_1\delta_2\bar{\delta}_1\bar{\delta}_2 = 7$, $\delta_1^2\delta_2^2$, $\bar{\delta}_1^2\bar{\delta}_2^2$, $\delta_1^2\delta_2\bar{\delta}_2$, $\delta_1^2\bar{\delta}_2^2$, $\delta_1\bar{\delta}_1\bar{\delta}_2^2$, $\delta_1\delta_2^2\bar{\delta}_1$, $\delta_2\bar{\delta}_1^2\bar{\delta}_2$ or $\delta_2^2\bar{\delta}_1^2$. A Galois automorphism breaks this solution set into three classes: $\delta_1\delta_2\bar{\delta}_1\bar{\delta}_2 = 7$; $\delta_1^2\delta_2^2$, $\delta_2^2\bar{\delta}_1^2$, $\delta_1^2\bar{\delta}_2^2$, $\bar{\delta}_1^2\bar{\delta}_2^2$; and $\delta_1\bar{\delta}_1\bar{\delta}_2^2$,

$\delta_1\delta_2^2\bar{\delta}_1$, $\delta_2\bar{\delta}_1^2\bar{\delta}_2$, $\delta_1^2\delta_2\bar{\delta}_2$. Since we want the solutions to equivalence, we pick one algebraic number from each class and hence, $\delta = 7$, $\delta_1^2\delta_2\bar{\delta}_2 = 1 + 2\zeta_{29} + 3\zeta_{29}^2 + 3\zeta_{29}^3 + 2\zeta_{29}^7 + 3\zeta_{29}^{11} + 3\zeta_{29}^{14} + 2\zeta_{29}^{16} + 3\zeta_{29}^{17} + 3\zeta_{29}^{19} + 2\zeta_{29}^{20} + 3\zeta_{29}^{21} + 2\zeta_{29}^{23} + 2\zeta_{29}^{24} + 2\zeta_{29}^{25}$ or $\delta_1^2\delta_2^2 = 1+3\zeta_{29}+2\zeta_{29}^4+2\zeta_{29}^5+2\zeta_{29}^6+3\zeta_{29}^7+2\zeta_{29}^9+2\zeta_{29}^{13}+3\zeta_{29}^{16}+3\zeta_{29}^{20}+2\zeta_{29}^{22}+3\zeta_{29}^{23}+3\zeta_{29}^{24}+3\zeta_{29}^{25}+2\zeta_{29}^{28}$. Based on the above information, if $\hat{D}$ is a (1276, 51, 2) difference set in C_{29}, then the possible alias, α in the rational idempotent decomposition of $\hat{D}$ is one of the two forms:

(a) $\alpha = \pm 7x^r$,

(b) $\alpha = \pm(1+3x+2x^4+2x^5+2x^6+3x^7+2x^9+2x^{13}+3x^{16}+3x^{20}+2x^{22}+3x^{23}+3x^{24}+3x^{25}+2x^{28})x^{s'}$ or $\pm(1+2x+3x^2+3x^3+2x^7+3x^{11}+3x^{14}+2x^{16}+3x^{17}+3x^{19}+2x^{20}+3x^{21}+2x^{23}+2x^{24}+2x^{25})x^t$, x is a generator of C_{29} and $r, s', t = 0, \dots, 28$.

On the other hand, if $\hat{D}$ is a (1276, 51, 2) difference set in $C_{m'}, m' = 11, 22, 44$, then the possible alias, α in the rational idempotent decomposition of $\hat{D}$ is $\alpha = \pm 7x^r$. The above discussion is fundamental to the choices of aliases in the later sections.

We now look at norm and trace of algebraic numbers in cyclotomic field, $\mathbb{Q}(\zeta_m)$ where $m > 2$. If m is an odd prime say p, then the minimum polynomial of ζ_p, over $\mathbb{Q}$ is $f(t) = t^{p-1} + t^{p-2} + \cdots + t + 1$ and $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$ ([17], page 64). The minimum polynomial of $\zeta_p^i \neq 1, 1 \leq i \leq p-1$ is also $f(t)$ as ζ_p^i is a p^{th} root of unity and consequently, $f(t) = \prod_{i=1}^{p-1}(t - \zeta_p^i)$ and ζ_p^i are the conjugates of ζ_p. The functions $\sigma_i : \mathbb{Q}(\zeta_p) \to \mathbb{C}$ defined by $\sigma_i(\zeta_p) = \zeta_p^i$ are monomorphisms and for any arbitrary element $\beta = \sum_{j=0}^{p-2} \alpha_j \zeta_p^j \in \mathbb{Q}(\zeta_p)$, $\sigma_i(\sum_{j=0}^{p-2} \alpha_j \zeta_p^j) = \sum_{j=0}^{p-2} \alpha_j \sigma_i(\zeta_p^j) = \sum_{j=0}^{p-2} \alpha_j \zeta_p^{ij}, \alpha_j \in \mathbb{Q}$. We now give the definition of norm and trace of an element β.

Definition 2.1. Based on the preamble above, the norm and trace of β are respectively,

$$N(\beta) = \prod_{i=1}^{p-1} \sigma_i(\beta) \quad \text{and} \quad T(\beta) = \sum_{i=1}^{p-1} \sigma_i(\beta). \tag{2.7}$$

Example 2.1. Suppose that $p = 5$ and $\zeta_5 = e^{\frac{2\pi i}{5}}$ with $\beta = 5+2\zeta_5+2\zeta_5^2$, then the length of β is $\sigma_1(\beta)\sigma_4(\beta) = \beta\bar{\beta} = 33 + 14\zeta_5 + 10\zeta_5^2 + 10\zeta_5^3 + 14\zeta_5^4 = 21 + 2\sqrt{5}$, since $\zeta_5 + \zeta_5^4 = \frac{-1+\sqrt{5}}{2}$. Thus, $N(\beta) = (21 + 2\sqrt{5})(21 - 2\sqrt{5}) = 421$. Also, $T(\beta) = \sum_{i=1}^{4} \sigma_i(\beta) = 16$ as $\sum_{i=0}^{4} \zeta^i = 0$.

Finally, suppose that H is a group of order $2h$ with a central involution z. We take $T = \{t_i : i = 1, \dots, h\}$ to be the transversal of $\langle z\rangle$ in H so that every element in H is viewed as $t_i z^j, 0 \le i \le h, j = 0, 1$. 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 $\mathbb{Z}[T]$. Using the two representations of subgroup $\langle z\rangle$ and Frobenius reciprocity theorem [11], we may write any element X of the group ring $\mathbb{Z}[H]$ in the form

$$X = X\left(\frac{1+z}{2}\right) + X\left(\frac{1-z}{2}\right). \tag{2.8}$$

Furthermore, 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

$$X = A\left(\frac{\langle z\rangle}{2}\right) + B\left(\frac{2-\langle z\rangle}{2}\right), \tag{2.9}$$

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 $A \equiv B \pmod 2$. 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 $\langle z\rangle$ [3]. In particular, it can be shown that if K is a subgroup of a group H such that

$$H \cong K \times \langle z\rangle, \tag{2.10}$$

then the difference set image in H is

$$\hat{D} = A\left(\frac{\langle z\rangle}{2}\right) + gB\left(\frac{2-\langle z\rangle}{2}\right), \tag{2.11}$$

where $g \in H$, A is a difference set in K, $\alpha = \frac{k+\sqrt{n}}{|K|}$ or $\alpha = \frac{k-\sqrt{n}}{|K|}$, $B = A - \alpha K$ and k is the size of the difference set. (2.11) is true as long as $|K| \mid (k+\sqrt{n})$ or $|K| \mid (k-\sqrt{n})$.

In the next two sections, we analyze the (1276, 51, 2) difference set images in factor groups of orders 44, 58 and 116.

3. Difference set images in 2-groups

We compute difference set images in $G/N \cong H$, where H is a group of order $2^m, m = 1, 2$.

3.1. **The C_2 image.** Suppose $H = C_2 = \langle x : x^2 = 1\rangle$ and $\hat{D} = \sum d_j x^j$, $j = 0, 1$ is the difference set image in H. We view this group ring element as a 1×2 array with columns indexed by powers of x. The characters of H are of the form $\chi_j(x) = (-1)^j$, $j = 0, 1$. By applying the map $x \mapsto 1$ on $\hat{D}$, we get $d_0 + d_1 = 51$. Also the map $x \mapsto -1$ on $\hat{D}$ yields $d_0 - d_1 = \pm 7$. We translate $\hat{D}$, if necessary, to obtain $d_0 - d_1 = 7$. By solving the system of equations $d_0 + d_1 = 51$ and $d_0 - d_1 = 7$, the unique element in Ω_{C_2} is $A = 29 + 22x$.

We now obtain difference set images in groups of order 4.

3.2. **The Group 4 images.** Suppose $H \cong C_4 = \langle x : x^4 = 1\rangle$ and the difference set in H is $\hat{D} = \sum_{j=0}^{3} d_j x^j$. This group ring element is viewed as a 1×4 array with columns indexed by powers of x. The characters of H are of the form $\chi_j(x) = i^j$, where $j = 0, 1, 2, 3$ and i is the fourth root of unity. The rational idempotents are: $[e_{\chi_0}] = \frac{1}{4}\langle x\rangle$; $[e_{\chi_1}] = \frac{1}{4}(2\langle x^2\rangle - \langle x\rangle)$; $[e_{\chi_2}] = \frac{1}{2}(2 - \langle x^2\rangle)$. Out of these 3 rational idempotents, only $[e_{\chi_1}]$ does not have $\langle x^2\rangle$ in its kernel. The linear combination of those idempotents having $\langle x^2\rangle$ in their kernel is $A\frac{\langle x^2\rangle}{2}$, where A is the difference set image in C_2. Thus, the difference set image is

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

where $\alpha_{\chi_1} = \pm 7x^s, s = 0, 1, 2, 3$. By translating, if necessary, the unique element of Ω_{C_4}, up to equivalence, is $A_1 = 7 + 11\langle x\rangle$. Similarly, if $H \cong C_2 \times C_2 = \langle x, y : x^2 = y^2 = [x, y] = 1\rangle$, then the difference set image is $7 + 11(1 + x)(1 + y)$.

4. Difference set images in groups of order 44, 58 and a group of order 116

4.1. Difference set images in groups of order 44.

4.1.1. *The C_{11} image.* Suppose that $G/N \cong C_{11} = \langle x : x^{11} = 1\rangle$ and $\hat{D} = \sum_{i=0}^{10} d_i x^i$ is the difference image in G/N. Using the fact that if χ is a non trivial character of G/N, then $\chi(\hat{D}) = \pm 7\zeta_{11}^i, i = 0, \ldots, 10$, up to equivalence, $A = 7 + 4\langle x\rangle$ is the only difference set image in G/N.

4.1.2. *The C_{22} and D_{11} images.* Suppose that $G/N \cong C_{22} = \langle x, y : x^{11} = y^2 = 1 = [x, y]\rangle$ and $\hat{D} = \sum_{i=0}^{10}\sum_{j=0}^{1} d_{ij} x^i y^j$ is the difference image in G/N. Using (2.11) with $K = C_{11}$, $\alpha = 4$ and $|K| = 11$ we obtain, up to equivalence, $A_1 = 7 + 2\langle x\rangle\langle y\rangle$ as the only difference set image in G/N.The Dillon dihedral technique can be used to show that A_1 is also the only difference set image in $G/N \cong D_{11} = \langle x, y : x^{11} = y^2 = 1, yxy = x^{-1}\rangle$.

4.1.3. *The $C_{22} \times C_2$, C_{44} and D_{22} images.* It is easy to show that if $G/N \cong C_{44} = \langle x : x^{44} = 1\rangle$, then the difference set image is $A_2 = 7 + \langle x\rangle$. Also, if $G/N \cong D_{22} = \langle x, y : x^{22} = y^2 = 1, yxy = x^{-1}\rangle$ the difference set image is $A_3 = 7 + \langle x\rangle\langle y\rangle$. Finally, if $G/N \cong C_{22} \times C_2 = \langle x, y, z : x^{11} = y^2 = z^2 = 1 = [x, y] = [y, z] = [x, z]\rangle$ then the difference set image is $A_4 = 7 + \langle x\rangle\langle y\rangle\langle z\rangle$.

4.2. **The C_{29} image.** Suppose that $G/N \cong C_{29} = \langle x : x^{29} = 1\rangle$ and $\hat{D} = \sum_{i=0}^{28} d_i x^i$ is the difference image in G/N. The characters of C_{29} are of the form $\chi_s(x) = \zeta^s$, $s = 0, \dots, 28$, where ζ_{29} is the twenty-ninth root of unity. Thus, the two rational idempotents of G/N are:

$$[e_{\chi_0}] = \frac{1}{29}\langle x\rangle \quad \text{and} \quad [e_{\chi_1}] = \frac{1}{29}(29 - \langle x\rangle)$$

and the difference set equation is

$$\hat{D} = \alpha_{\chi_0}[e_{\chi_0}] \pm \alpha_{\chi_1}[e_{\chi_1}] \tag{4.1}$$

with $\alpha_{\chi_0} \in \mathbb{Z}$, $\alpha_{\chi_1} \in \mathbb{Z}[\zeta_{29}]$. As χ_0 is the trivial character, then $\chi_0(\hat{D}) = \alpha_{\chi_0} = 51$ and $\alpha_{\chi_1} \in \{\pm 7x^s, \pm(1 + 3x + 2x^4 + 2x^5 + 2x^6 + 3x^7 + 2x^9 + 2x^{13} + 3x^{16} + 3x^{20} + 2x^{22} + 3x^{23} + 3x^{24} + 3x^{25} + 2x^{28})x^{s'}, \pm(1 + 2x + 3x^2 + 3x^3 + 2x^7 + 3x^{11} + 3x^{14} + 2x^{16} + 3x^{17} + 3x^{19} + 2x^{20} + 3x^{21} + 2x^{23} + 2x^{24} + 2x^{25})x^{s''})\}$, $s, s', s'' = 0, \dots, 28$. We replace $\hat{D}$ by $\hat{D}\zeta_{29}^s$ or $\hat{D}x$, if necessary to obtain α_{χ_1} to be $a_1 = 7$, $a_2 = 1 + 3x + 2x^4 + 2x^5 + 2x^6 + 3x^7 + 2x^9 + 2x^{13} + 3x^{16} + 3x^{20} + 2x^{22} + 3x^{23} + 3x^{24} + 3x^{25} + 2x^{28}$ or $a_3 = 1 + 2x + 3x^2 + 3x^3 + 2x^7 + 3x^{11} + 3x^{14} + 2x^{16} + 3x^{17} + 3x^{19} + 2x^{20} + 3x^{21} + 2x^{23} + 2x^{24} + 2x^{25}$. Thus, the difference set equation becomes

$$\hat{D} = \frac{51}{29}\langle x\rangle \pm \frac{a_i}{29}(29 - \langle x\rangle), i = 1, 2, 3, \tag{4.2}$$

where $\frac{a_1}{29}(29 - \langle x\rangle) = \frac{7}{29}(29 - \langle x\rangle)$, $\frac{a_2}{29}(29 - \langle x\rangle) = \frac{1}{29}(-7 + 51x - 36x^2 - 36x^3 + 22x^4 + 22x^5 + 22x^6 + 51x^7 - 36x^8 + 22x^9 - 36x^{10} - 3x^{11} - 36x^{12} + 22x^{13} - 36x^{14} - 36x^{15} + 51x^{16} - 36x^{17} - 36x^{18} - 36x^{19} + 51x^{20} - 36x^{21} + 22x^{22} + 51x^{23} + 51x^{24} + 51x^{25} - 36x^{26} - 36x^{27} + 22x^{28}$ and $\frac{a_3}{29}(29 - \langle x\rangle) = \frac{1}{29}(-7 + 22x + 51x^2 + 51x^3 - 36x^4 - 36x^5 - 36x^6 + 22x^7 - 36x^8 - 36x^9 - 36x^{10} + 51x^{11} - 36x^{12} - 36x^{13} + 51x^{14} - 36x^{15} + 22x^{16} + 51x^{17} - 36x^{18} + 51x^{19} + 22x^{20} + 51x^{21} - 36x^{22} + 22x^{23} + 22x^{24} + 22x^{25} - 36x^{26} - 36x^{27} - 36x^{28}$.

Thus, the solutions to (4.2) are:

(a) $E_1 = -7 + 2\langle x\rangle$, which is not viable since intersection number must be non negative integer

(b) $E_2 = 2 + 3x^2 + 3x^3 + x^4 + x^5 + x^6 + 3x^8 + x^9 + 3x^{10} + 3x^{11} + 3x^{12} + x^{13} + 3x^{14} + 3x^{15} + 3x^{17} + 3x^{18} + 3x^{19} + 3x^{21} + x^{22} + 3x^{26} + 3x^{27} + x^{28}$

(c) $E_3 = 2 + x + 3x^4 + 3x^5 + 3x^6 + x^7 + 3x^8 + 3x^9 + 3x^{10} + 3x^{12} + 3x^{13} + 3x^{15} + x^{16} + 3x^{18} + x^{20} + 3x^{22} + x^{23} + x^{24} + x^{25} + 3x^{26} + 3x^{27} + 3x^{28}$.

Only E_2 and E_3 are elements of $\Omega_{C_{29}}$.

4.3. **Groups of order 58.** Let N be an appropriate normal subgroup of G such that $G/N \cong C_{58} = \langle x, y : x^{29} = y^2 = 1 = [x, y]\rangle = C_{29} \times \langle y\rangle$. We view the difference set image in G/N as $\hat{D} = \sum_{i=0}^{28}\sum_{j=0}^{1} d_{ij}x^iy^j$. This group is of the form (2.10). Take $K = C_{29}$, $\alpha = 2$ and $k = 51$. Then (2.11) becomes $\hat{D} = E_i\left(\frac{1+y}{2}\right) + B_jg\left(\frac{1-y}{2}\right), i = 2, 3$ where $g \in G/N$, E_i is a viable difference set image in C_{29} and $B_j = E_j - 2K, j = 1, 2, 3$. We look at two situations. In the first instance, $\hat{D} = E_i\left(\frac{1+y}{2}\right) + B_1g\left(\frac{1-y}{2}\right)$ has no integer solution because of the number of fractions in $E_i\left(\frac{1+y}{2}\right)$ exceeds those of $B_1g\left(\frac{1-y}{2}\right)$. Hence, $E_i\left(\frac{1+y}{2}\right)$ and $B_1g\left(\frac{1-y}{2}\right)$ are not compatible to produce integer solutions. Secondly, $\hat{D} = E_i\left(\frac{1+y}{2}\right) + B_jg\left(\frac{1-y}{2}\right), i, j = 2, 3$ has integer solutions but some entries are negative. Thus, $\Omega_{C_{58}}$ is empty. The Dillon dihedral trick shows that D_{29} does not admit (1276, 51, 2) difference sets.

At this stage, we have ruled out the existence of (1276, 51, 2) difference sets in all groups of order 1276 except $C_{11} \times (C_{29} \rtimes C_4)$ or $C_{319} \rtimes C_4$ with GAP[2] library numbers [1276, 5] and [1276, 6] respectively. These two surviving groups have F_{116} as a factor group. We now explore the difference set images in this group.

4.4. **The group** $F_{116} = C_{29} \rtimes C_4$**.** Suppose that $G/N \cong C_{17} \rtimes C_4 = \langle x, y : x^{29} = y^4 = 1, yxy^{-1} = x^{17}\rangle$. This group is the third group in the GAP[2] list of groups of order 116. We express the difference set image in G/N, if it exists, as $\hat{D} = \sum_{s=0}^{28}\sum_{t=0}^{3} d_{s,t}x^sy^t$. This difference set image is viewed as a 4×29 matrix with the columns indexed by the powers of x and rows by powers of y. Since $(G/N)/\langle x\rangle \cong C_4$, the map $x \mapsto 1$ give rise to a system of equations

$$\sum_{s=0}^{28} d_{s0} = a_0, \qquad \sum_{s=0}^{28} d_{s1} = a_1, \qquad \sum_{s=0}^{28} d_{s2} = a_2, \qquad \sum_{s=0}^{28} d_{s3} = a_3, \tag{4.3}$$

where $(a_{1t}) = A_1$ is a 1×4 matrix and the difference set image in C_4. The group G/N has seven equivalent degree four representations. One of them (ζ is the twenty-ninth root of unity) is

$$\chi : x \mapsto \begin{pmatrix} \zeta & 0 & 0 & 0 \\ 0 & \zeta^{17} & 0 & 0 \\ 0 & 0 & \zeta^{28} & 0 \\ 0 & 0 & 0 & \zeta^{12} \end{pmatrix}, \quad y \mapsto \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

By applying this representation to $\hat{D}$, we get

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

where $A = \sum_{s=0}^{28} d_{s0}\zeta^s$, $B = \sum_{s=0}^{28} d_{s1}\zeta^s$, $C = \sum_{s=0}^{28} d_{s2}\zeta^s$, $D = \sum_{s=0}^{28} d_{s3}\zeta^s$ and $\sigma(\zeta) = \zeta^{17}$. By solving $\chi(\hat{D})\overline{\chi(\hat{D})} = 49I_4$, where I_4 is a 4×4 identity matrix, we get 16 equations which are equivalent to the following system:

$$A\bar{A} + B\bar{B} + C\bar{C} + D\bar{D} = 49 \tag{4.4}$$

$$AC = -BD \tag{4.5}$$

The coset bound of difference set image in G/N is 11 and using the variance trick equations, the possible distributions of this difference set image are $0^{69}1^{46}5^1$, $0^{71}1^{42}2^13^14^1$, $0^{72}1^{39}2^44^1$, $0^{72}1^{40}2^13^3$, $0^{73}1^{37}2^43^2$, $0^{74}1^{34}2^73^1$, $0^{75}1^{31}2^{10}$. The distribution $0^{69}1^{46}5^1$ means that the intersection number 0 occurs 69 times, intersection number 1 occurs 46 times while intersection number 5 occurs only once. Without loss of generality, we take

$$\sum_{s=0}^{28} d_{s0} = 18, \qquad \sum_{s=0}^{28} d_{s1} = 11, \qquad \sum_{s=0}^{28} d_{s2} = 11, \qquad \sum_{s=0}^{28} d_{s3} = 11, \tag{4.6}$$

One way to decide the existence or otherwise of the difference set image in G/N is to use the multiplicative property of norm of algebraic integers on (4.5). Consequently, if $AC = -BD$, then $N(A)N(C) = N(B)N(D)$. We need the converse of this statement. If p is any prime such that $p \mid N(A)N(C)$, then $p \mid N(A)$ or $p \mid N(C)$. Thus, $p \mid N(B)$ or $p \mid N(D)$. The objective is to combine this information with each of the seven possible distributions of the difference set image in G/N to either construct difference set images or show that none exists. For instance, take the distribution $0^{69}1^{46}5^1$. The intersection number 5 is unique and without loss of generality, set $d_{00} = 5$. Then $d_{st} = 0$ or 1 for $s \neq 0$ and $t \neq 0$. Thus, $A = 5 + \sum_{s=1}^{28} d_{s0}\zeta^s$ and $\sum_{s=1}^{28} d_{s0} = 13$. Notice that in this case, all the algebraic numbers B, C and D are like. However, there are

2^{28} possible values of $N(A)$ and 2^{29} values of $N(B)$, $N(C)$ or $N(D)$. This remaining part is inconclusive, requires more work and we hope to report on it soon.

Acknowledgement: The comment of the anonymous referee is appreciated.

References

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

[2] *GAP-Groups, Algorithms and Programming, Version 4. 4. 6* (2006) Retrieved on Jan. 2, 2006 from http://www.gap.gap-system.org

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

[4] D. R. Hughes, *On biplanes and semibiplanes*, Combin. Math, Proceedings of Australian Conference of Combinatorial Maths. **686** (1978), 55–58.

[5] J. E. Iiams, *Lander's tables are complete*, Difference sets, Sequeneces and their Correlation properties, Klumer Academic Publishers (1999), 239–257.

[6] Y. J. Ionin and M. S. Shrikhande, *Combinatorics of Symmetric Designs*, New Mathematical Monographs, Cambridge University Press, UK, 2006.

[7] *La Jolla Cyclic Difference Set Repository.* Retrieved on July 30 2010 from: http://www.ccrwest.org/diffsets.html

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

[9] E. Lander, *Symmetric Design: An Algebraic Approach*, London Math. Soc. Lecture Note Series 74, Cambridge Univ. Press, 1983.

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

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

[12] R. Liebler, *The inversion formula*, J. Combin. Math. and Combin. Computing **13** (1993), 143–160.

[13] S. L. Ma, *Planar functions, relative difference sets and character theory*, J. of Algebra **185** (1996), 342–356.

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

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

[16] K. W. Smith, *Non-abelian Hadamard difference sets*, J. Comb. Theory A (1995), 144–156.

[17] I. Stewart and D. Tall, *Algebraic Number Theory and Fermat's Last Theorem*, A. K. Peters Publishers (3rd ed) 2002.

[18] R. Turyn, *Character sums and difference set*, Pacific J. Math. **15** (1965), 319–346.

Department of Mathematics, Faculty of Science,
University of Lagos, Akoka,
Lagos State-Nigeria
E-mail address: asaosifodunrin@yahoo.com