International Journal of Mathematical Analysis and Optimization: Theory and Applications
Vol. 2019, No. 2, pp. 521 - 545

Existence of $(v, k, 2)$ difference sets with $k < 2030$ and $\sqrt{k-2}$ is a natural number

Adegoke Solomon Osifodunrin

Department of Mathematics,
Houston Community College, Houston, Texas 77083 USA
*Corresponding author: asaosifodunrin@yahoo.com, solomon.osifodunrin@hccs.edu

Article Info
Received: June 16 2019 Revised: 1 August 2019
Accepted: 21 September 2019 Available online: 15 October 2019

Abstract

$(v, k, 2)$ symmetric designs(or Biplanes) are known to exist for some integer values $k < 16$. This paper investigates the existence of a class of $(v, k, 2)$ difference sets with $2 \leq \sqrt{k-2} \leq 45$ and $\sqrt{k-2}$ is an integer using variance technique, representation, group and algebraic number Theories. Our results indicate that most of these parameters do not exist.

Keywords: Representation, Biplane, Idempotents, difference Sets, Intersection numbers
MSC2010:05B10

1 Introduction

Let G be a multiplicative group of order v and let D be a k-subset of G with $k < v$. The set D is a (v, k, λ) difference set if every non-identity element of G can be replicated 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). Difference sets are useful in optical alignment, imaging astronomical events, communication sciences like interpreting signals in the presence of noise or constructing error correcting codes and facilitating processes in quantum informatics. Also, it is known that difference sets are closely related to designs since symmetric design admitting a sharply transitive automorphism group G, is isomorphic to the development of a difference set in G (Theorem 4.2 [1]). The study of difference sets is the epitome of elegance of combination of techniques in geometry, combinatorics, group, representation and number theories.

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 [2]. Hence, there are infinite number of projective planes and many

International Journal of Mathematical Analysis and Optimization: Theory and Applications
Vol. 2019, No. 2, pp. 521 - 545

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 [3]. The author assumes that the readers are familiar with Symmetric designs, difference sets and the relationship between them. The readers that are not familiar with these subjects are encouraged to read Lander [1], Beth et al [4], Ionin and Shrikhande [2], or Pott [5].

Baumert's result[6] indicated that there are no other Singer cyclic biplanes for $k \leq 100$ while Hughes and Dickey [3] showed (with the aid of computer) that there are no biplanes for $k \leq 5002$. The implication of these results(based on Lander's Theorem 4.2 [1]) is that the corresponding difference set with the same parameters do not exist but our results are achieved by analytical method. Furthermore, other authors including Gjoneski et al [7], Kopilovich [8], Lander [1], López and Sánchez [9] and Osifodunrin [10, 11, 12], Smith and Borman[13] showed that difference sets with some of these parameters do not exist in some or all groups of appropriate order. On the other hand, it is known that 12 of the 14 groups of order 16 have (16, 6, 2) difference sets and there are three biplanes(up to isomorphism) with these parameters.

In this paper, we consider $(v, k, 2)$ parameter sets in which $k-2 \geq 4$ is a perfect square and $k < 2030$. We combine variance technique(a necessary condition for the existence of (v, k, λ) difference set) with Sylow Theorems, representation and algebraic theories to establish non existence of some difference set parameters and partial results on other parameters. G will represent a group of order v and N, a normal subgroup of G of an appropriate order. The main results of this paper are:

Theorem 1.1. *There are no (56, 11, 2), (154, 18, 2), (352, 27, 2), (704, 38, 2), (2146, 66, 2), (3404, 83, 2), (10586, 146, 2), (14536, 171, 2), (33154, 258, 2), (42196, 291, 2),(65704, 363, 2), (97904, 443, 2), (196252, 627, 2), (463204, 963, 2), (1282402, 1602, 2), (1415404, 1683, 2), (1558496, 1766, 2), (1712176, 1851, 2), (1876954, 1938, 2), (2053352, 2027, 2) difference sets.*

Theorem 1.2. *There are no (1276, 51, 2) difference sets except possibly in* $C_{11} \times (C_{29} \rtimes C_4)$ *or* $C_{319} \rtimes C_4$.

Theorem 1.3. *Suppose that G is a group of order 5152 and N is a normal subgroup of G. Then there are no (5152, 102, 2) difference sets except possibly in G such that* $G/N \cong (C_4 \times (C_2^3 \rtimes C_7))$ *(with GAP location number [224, 173]).*

Theorem 1.4. *Suppose that G is a group of order 7504 and N is a normal subgroup of G. Then G does not admit (7504, 123, 2) difference sets if $G/N \cong H$, where H is any group of order 1876.*

Theorem 1.5. *Suppose that G is a group of order 19504 and N is a normal subgroup of G. Then there are no (19504, 198, 2) difference sets except possibly in G such that $G/N \cong H$, where H is a group of order 848 with GAP location number [848, cn], cn =28, 29, 30, 31, 32, 33, 34, 49.*

Theorem 1.6. *Suppose that G is a group of order 52976 and N is a normal subgroup of G. Then there are no (52976, 326, 2) difference sets if $G/N \cong H$, where H is a group of order 172 or* C_{43}, C_{86},D_{43}, $C_{14} \times C_2 \times C_2$ *or* $D_{14} \times C_2$.

Theorem 1.7. *Suppose that G is a group of order 166754. If there is a normal subgroup, N of G such that G/N is isomorphic to* C_{43}, D_{43} *or* C_{86}, *then G does not admit (166754, 578, 2) difference sets.*

Theorem 1.8. *Suppose that G is a group of order 229504 and N is a normal subgroup of G. Then there are no (229504, 678, 2) difference sets if $G/N \cong H$, where H is* C_{1793}, D_{1793}, C_{3586} *or* $C_{22} \times (C_2)^2$.

Theorem 1.9. *Suppose that G is a group of order 266816 and N is a normal subgroup of G. Then there are no (266816, 731, 2) difference sets if $G/N \cong H$, where H is* C_{379}, C_{758} *or* D_{379} *or any of the four groups of order 1516.*

Theorem 1.10. *Suppose that G is a group of order 308506 and N is a normal subgroup of G. Then there are no (308506, 786, 2) difference sets if $G/N \cong H$, where H is C_{4179}, C_{8338} or D_{4169}.*

Theorem 1.11. *Suppose that G is a group of order 354904 and N is a normal subgroup of G. Then there are no (354904, 843, 2) difference sets if $G/N \cong H$, where H is C_{44}, $C_{22} \times C_2$,D_{22}, D_{74} or $C_{74} \times C_2$ or C_{1488}.*

Theorem 1.12. *Suppose that G is a group of order 594596 and N is a normal subgroup of G. Then there are no (594596, 1091, 2) difference sets if $G/N \cong H$, where H is C_{281}, any group of order 562 or 1124 except Frobenious group of order 1124.*

Theorem 1.13. *Suppose that G is a group of order 939136 and N is a normal subgroup of G. Then there are no (939136, 1371, 2) difference sets if $G/N \cong H$, where H is C_{92}, $C_{46} \times C_2$, $C_{58} \times C_2$, D_{46} or C_{116}.*

Theorem 1.14. *Suppose that G is a group of order 1044736 and N is a normal subgroup of G. Then there are no (1044736, 1446, 2) difference sets if $G/N \cong H$, where H is C_{77}, C_{154}, or D_{77}.*

Theorem 1.15. *Suppose that G is a group of order 1159004 and N is a normal subgroup of G. Then there are no (1159004, 1523, 2) difference sets if $G/N \cong H$, where H is C_{71}, C_{142}, D_{71} or C_{116}.*

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 theorems by showing that some factor groups of G do not admit the difference sets. Section 5 gives an example of work in progress and section 6 is the summary of this work.

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 $\mathbb{C}[G]$[5]. 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

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

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 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' [14]. 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[5]. 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 G. 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 $\mathbb{Z}[G]$[5]. 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 $\mathbb{Q}$[5]. 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 $\chi_i(x) = \zeta^i_{p^m}, i = 0, \ldots, p^m - 1$, then the rational idempotents are

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

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

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

The following theorem is usually employed in the search of difference sets [15].

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

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

where α_i is any χ_i-alias for A.

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

Dillon [16] 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 2.3. *If the cyclic group Z_{2m} does not contain a (nontrivial) difference set, then neither does the dihedral group of order $2m$.*

IJMAO

International Journal of Mathematical Analysis and Optimization: Theory and Applications
Vol. 2019, No. 2, pp. 521 - 545

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 $\hat{D} = \sum_{t_j \in G} d_j t_j N$, where the integer $d_j = |D \cap t_j N|$ is called the **intersection number** of D with respect to N[5]. 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[5]. The following lemma extends this property to $\hat{D}$[5].

Lemma 2.4. *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 the $d \times d$ identity matrix.*

The character value of $\chi(\hat{D})$ is given by the following lemma[5].

Lemma 2.5. *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 2.6. *(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*

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

The method used in this paper is known as representation theoretic method made popular by Leibler ([15]). Some authors like Iiams [?] and Smith [22] 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 2.4, 2.5 and the difference set equation (2.5) to obtain $\Omega_{G/N}$.

International Journal of Mathematical Analysis and Optimization: Theory and Applications
Vol. 2019, No. 2, pp. 521 - 545

2.1 Formation of aliases

In this section, we look at aliases that will be needed to generate respective 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 2.4, $\chi(\hat{D})\overline{\chi(\hat{D})} = n$. 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,

1. we must look for all principal ideals $\pi \in \mathbb{Z}[\zeta_m]$ such that $\pi\bar{\pi} = (n)$
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. We use a theorem due to Kronecker [5, 17] 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 $\delta' = \delta u$[18], 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. $\phi(m') = |\mathbb{Z}^*_{m'}|$ [19]. For instance, the ideal generated by 7 has four factors in $\mathbb{Z}[\zeta_{m'}], m' = 16, 29, 58$ while the ideal generated by 7 is prime in $\mathbb{Z}[\zeta_{2^s}], s = 1, 2, 3$. 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 [20], 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, $a^{105} \equiv -1 \pmod{211}, a = 3, 7$. Thus, $\langle 3\rangle$ or $\langle 7\rangle$ is fixed by conjugation in $\mathbb{Z}[\zeta_{211}]$. The following remark shows a special case of the ideal generated by m^2 that has two factors in $\mathbb{Z}[\zeta_{m'}]$, that is $\langle m^2\rangle = \langle\delta\rangle\langle\bar{\delta}\rangle$, but the algebraic equation $\delta\bar{\delta} = m^2$ has trivial solutions $\delta = \pm m\zeta_{m'}^j$.

Remark 2.7. Take $m = 7$ and $m' = 31$. Let G be a group of order 496 and let N be a normal subgroup of G. In order to find (496, 55, 6) difference sets in $G/N \cong C_{31}$, we need to solve the equation $\delta\bar{\delta} = 7^2$ in the algebraic integers of the cyclotomic field of 31st roots of unity to obtain the aliases. That is, we must find all algebraic integers of length 7 in the ring of algebraic integers of this cyclotomic field. Suppose that ζ_{31} is the primitive 31st root of unity and σ is the Galois automorphism of $\mathbb{Q}(\zeta_{31})$ fixing $\mathbb{Q}$ defined by $\sigma(\zeta_{31}) = \zeta_{31}^7$. We are interested in the factoring of ideal $\langle 7\rangle$ and as $7^{15} \equiv 1 \mod 31$, the order of this map is 15 and it fixes any ideal over $\langle 7\rangle$. The Galois

International Journal of Mathematical Analysis and Optimization: Theory and Applications
Vol. 2019, No. 2, pp. 521 - 545

automorphism of $\mathbb{Q}(\zeta_{31})$ fixing $\mathbb{Q}$ has order 30 and the number of ideals over $\langle 7\rangle$ is exactly $\frac{30}{15}=2$. That is, $\langle 7\rangle=\pi_1\pi_2$. As -1 is not in the subgroup $\langle 7\rangle$ of the group of units $U(31)$, the conjugate map $z\mapsto\bar{z}$ is not in $\langle\sigma\rangle$. Thus, the conjugate map must interchange π_1 and π_2. Consequently, there is a prime ideal π such that $\langle 7\rangle=\pi\bar{\pi}$. Suppose that $\langle\delta\rangle\langle\delta\rangle=\langle 7\rangle^2$. In order to find all solutions to the equation $\delta\bar{\delta}=7^2$, we need to enumerate all possibilities such that $\pi^{2-i}\bar{\pi}^i=7^2$ and $i=0,1$. Consequently, the two possible choices of $\langle\delta\rangle$ are: 1) $\langle\delta\rangle=\langle 7\rangle=\pi\bar{\pi}$, 2) $\langle\delta\rangle=\pi^2$.
Case 1:
Suppose that $\langle\delta\rangle=\langle 7\rangle=\pi\bar{\pi}$, then $\delta=\pm 7u$, where u is a root of unity. Thus, $\delta=\pm 7$ is the solution to equation $\delta\bar{\delta}=7^2$.
Case 2:
Suppose that $\langle\delta\rangle=\pi^2$, where $\langle\delta\rangle=\langle 7\rangle=\pi\bar{\pi}$. You will recall that the ideal $\langle\delta\rangle$ is fixed by σ but there is no reason to believe that same is true of δ. However, we can show that there is another element δ' fixed σ such that by $\langle\delta\rangle=\langle\delta'\rangle$. Since $\langle\delta\rangle$ is fixed by σ then $\sigma(\delta)\in\langle\delta\rangle$. Thus, $\sigma(\delta)=\delta u$, for some unit u. Observe that both $\langle\delta\rangle$ and $\sigma(\delta)$ satisfy $\delta\bar{\delta}=7^2$ and their conjugates have length 7. By a theorem due to Kronecker, $\sigma(\delta)=\pm\zeta^j\delta$, for some j [5, 17]. For now, we ignore the sign and take $\sigma(\delta)=\zeta^j\delta$. Thus, we can solve for s in the equation $\sigma(\zeta^s\delta)=\zeta^s\delta$. It then follows that $\sigma(\zeta^s\delta)=\zeta^{7s+j}\delta$ and consequently, $7s+j\equiv s \mod 31$ or $6s\equiv -j \mod 31$. Notice that the multiplicative inverse of 6 is $-5 \mod 31$ and so $s\equiv 5j \mod 31$. Hence, $\zeta^{5j}\delta$ is also fixed by σ and in the fixed field of σ. However, if $\sigma(\delta)=-\zeta^j\delta$ then $\sigma(\zeta^{5j}\delta)=-\zeta^{5j}\delta$ and so $\sigma^2(\zeta^{5j}\delta)=\zeta^{5j}\delta$. This means that $\zeta^{5j}\delta$ is fixed by σ^2. But $(\sigma^2)^8=\sigma$, which implies that an element fixed by σ^2 is also fixed by σ. As a result of the above, it follows that if $\langle\delta\rangle=\pi^2$, then there is a root of unity u such that $u\delta$ is fixed by σ and thus, in the fixed field of $\langle\sigma\rangle$. But the Galois group $\langle\sigma\rangle$ has index two in the Galois group of $\mathbb{Q}(\zeta_{31})$ fixing $\mathbb{Q}$, consequently, this fixed field is $\mathbb{Q}(\sqrt{-31})$. The ring of algebraic integers in this extension is described as $\{a+b\big(\frac{1+\sqrt{-31}}{2}\big):a,b\in\mathbb{Z}\}$[21]. The norm of the element $a+b\big(\frac{1+\sqrt{-31}}{2}\big)=\frac{(2a+b)+b\sqrt{-31}}{2}$ in this ring of integers is $\frac{(2a+b)^2+31b^2}{4}=\frac{4a^2+4ab+32b^2}{4}=a^2+ab+8b^2$. Since the objects of interest have length 49, the question now is what are the values of integers a and b such that $a^2+ab+8b^2=49$? Clearly, the possible values of b are ±2, ±1 and 0. If $b=\pm 2$, then $a^2-2a-17=0$ or $a^2+2a-17=0$. If $b=\pm1$, then $a^2-a-41=0$ or $a^2+a-41=0$ and If $b=0$, then $a^2=49$. The discriminant of the first four of these quadratic equations is either 72 or 165. Since 72 and 165 are not perfect squares,only $a^2=49$ has integer solutions ±7. This also means that $\delta=\pm 7u$, where u is a root of unity. Thus, we conclude that the only algebraic integers of length 7 are ±7.

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'. 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. The following remarks generate more aliases that will be required to obtain the difference set images in some homomorphic images of G/N.

Remark 2.8. The (1415404, 1683, 2) parameter set:
We show that although the ideal generated by 41 has two factors in the cyclotomic ring $\mathbb{Z}[\zeta_{m'}]$, $m'=431,862$ but the algebraic equation $\delta\bar{\delta}=41^2=1681$ has trivial solution. By Remark 2.7, we need to find solutions to the algebraic equation $\delta\bar{\delta}=1681$ in the cyclotomic ring $\mathbb{Z}[\zeta_{m'}]$, $m'=431,862$. This requires solving $a^2+ab+108b^2=1681$, for $a,b\in\mathbb{Z}$. This equation has rational solutions only if $b=0,1,2,3$. When $b=0$, then $a=\pm41$. On the other hand, when $b=1$, we get $a^2+a+108=1681$ or $a^2+a-1573=0$, which is a quadratic equation in a. The discriminant of this equation is $D=6293$. Since D is not a perfect square, then $a^2+a-1573=0$ has no integer solutions. Similarly, when $b=2$, the discriminant is $D=5000$ and when $b=3$, the discriminant is $D=2845$. As none of these discriminants is a perfect square, the equation $\delta\bar{\delta}=41^2=1681$ has only trivial solutions. The implication of this is that the aliases of the difference set image in factor group of order 431 is of the form $\pm 41x^j$, where x is a generator of factor group of order 431.

International Journal of Mathematical Analysis and Optimization: Theory and Applications
Vol. 2019, No. 2, pp. 521 - 545

Remark 2.9. For (2053352, 2027, 2) case, the order of the difference set parameter is $n = 2025 = 45^2 = 3^4 5^2$. The prime 3 is self conjugate modulo 991 since $3^{165} \equiv -1 \mod 991$ and the ideal generated by 5 has two factors in the cyclotomic ring $\mathbb{Z}[\zeta_{m'}]$, $m' = 991, 1982$. We need to establish that the algebraic equation $\delta\bar{\delta} = 2015$ has trivial solutions. By Remark 2.7, finding solutions to the algebraic equation $\delta\bar{\delta} = 2025$ in the cyclotomic ring $\mathbb{Z}[\zeta_{m'}]$, $m' = 991, 1982$ is equivalent to solving $a^2 + ab + 248b^2 = 2025$ in $\mathbb{Z}$. This equation has rational solutions only if $b = 0, 1, 2$. When $b = 0$, $a = \pm 45$. On the other hand, when $b = 1$, the discriminant of the resulting quadratic equation in a is $D = 7109$ and when $b = 2$, the discriminant is $D = 4136$. As none of these discriminants is a perfect square, the equation $\delta\bar{\delta} = 2025$ has only trivial solutions. This means that the aliases of the difference set image in factor group of order 991 is of the form $\pm 45x^j$, where x is a generator of factor group of order 991. The following result will be useful later.

Lemma 2.10. *If p is a prime such that $p \equiv 1 \mod 4$, then the ideal generated by p has at least two factors in the cyclotomic ring $\mathbb{Z}[\zeta_i]$, where i is the fourth root of unity.*

Proof. Since $p \equiv 1 \mod 4$, then p can be written as sum of squares of two integers say $p = a^2 + b^2$, where $a, b \in \mathbb{Z}$[21]. Take $a + bi \in \mathbb{Z}[\zeta_i]$, then $(a + bi)(a - bi) = a^2 + b^2 = p$. On the other hand, if $b + ai \in \mathbb{Z}[\zeta_i]$, then $(b + ai)(b - ai) = b^2 + a^2 = p$. ☐

Remark 2.11. In the case of (5152, 102, 2) difference sets, the ideal generated by 5 has two factors in $\mathbb{Z}[\zeta_{m'}], m' = 4, 8, 16, 32, 92$. Now we use Lemma 2.10 with $a = 2$ and $b = 1$. The solutions to $\delta\bar{\delta} = 5^2$ are 5, $(2 + i)^2 = 3 + 4i, (2 - i)^2 = 3 - 4i$. Thus the aliases for generating difference set images in $C_{m'}$ are 10, $2(3 + 4y)$, $2(3 - 4y)$, y is an element of order 4 in $C_{m'}$, $m' = 4, 8, 16, 32, 92$.

Also, the ideal generated by 2 has two factors in $\mathbb{Z}[\zeta_{m'}], m' = 7, 14, 28$. In fact $\langle 2\rangle = \langle \zeta_7 + \zeta_7^2 + \zeta_7^4\rangle\langle \zeta_7^3 + \zeta_7^5 + \zeta_7^6\rangle$. This means that the solutions to the algebraic equation $\delta\bar{\delta} = 100$ are $\delta = 10, 5(-1 + \theta), 5(-1 + \bar{\theta})$, $\theta = \zeta_7 + \zeta_7^2 + \zeta_7^4$. For the cases $\mathbb{Z}[\zeta_{m'}], m' = 14, 28$, replace ζ_7 with ζ_{14}^2 and ζ_{28}^4 respectively.

To study (7504, 198,2), we need to know how the ideal generated by 7 factors in $\mathbb{Z}[\zeta_{16}]$. This ideal has four factors in $\mathbb{Z}[\zeta_{16}]$. Suppose $\sigma \in Gal(\mathbb{Q}(\zeta_{16})/\mathbb{Q})$, where $\sigma(\zeta_{16}) = \zeta_{16}^7$. This automorphism split the basis elements of $\mathbb{Q}(\zeta_{16})$ into four orbits as $\zeta_{16} + \zeta_{16}^7$, $\zeta_{16}^3 + \zeta_{16}^5$, $\zeta_{16}^9 + \zeta_{16}^{15}$ and $\zeta_{16}^{11} + \zeta_{16}^{13}$. It is easy to see that $\langle 7\rangle = \langle 1 + \zeta_{16} + \zeta_{16}^7\rangle\langle 1 + \zeta_{16}^3 + \zeta_{16}^5\rangle\langle 1 + \zeta_{16}^9 + \zeta_{16}^{15}\rangle\langle 1 + \zeta_{16}^{11} + \zeta_{16}^{13}\rangle$. Put $\pi_1 = \langle 1 + \zeta_{16} + \zeta_{16}^7\rangle$ and $\pi_2 = \langle 1 + \zeta_{16}^3 + \zeta_{16}^5\rangle$. Let $\delta_1 = 1 + \zeta_{16} + \zeta_{16}^7$ and $\delta_2 = 1 + \zeta_{16}^3 + \zeta_{16}^5$ be a representatives of these ideals. Then the nine solutions to $\delta\bar{\delta} = 7^2$ are $\delta_1\delta_2\bar{\delta}_1\bar{\delta}_2 = 7$, $\delta_1^2\delta_2^2$, $\bar{\delta}_1^2\delta_2^2$, $\delta_1^2\bar{\delta}_2^2$, $\bar{\delta}_1^2\bar{\delta}_2^2$, $\delta_1^2\delta_2\bar{\delta}_2$, $\delta_2^2\delta_1\bar{\delta}_1$, $\bar{\delta}_1^2\delta_2\bar{\delta}_2$ or $\bar{\delta}_2^2\delta_1\bar{\delta}_1$. The Galois automorphism $\sigma(\zeta_{16}) = \zeta_{16}^3$ divides the solution set into three equivalence classes: $\delta_1\delta_2\bar{\delta}_1\bar{\delta}_2 = 7$; $\delta_1^2\delta_2^2$, $\bar{\delta}_1^2\delta_2^2$, $\delta_1^2\bar{\delta}_2^2$, $\bar{\delta}_1^2\bar{\delta}_2^2$; $\delta_1^2\delta_2\bar{\delta}_2$, $\delta_2^2\delta_1\bar{\delta}_1$, $\bar{\delta}_1^2\delta_2\bar{\delta}_2$ or $\bar{\delta}_2^2\delta_1\bar{\delta}_1$. As we need solutions up to equivalence, we pick a representative from each class. Thus, $\delta = 7$, $\delta_1^2\delta_2^2 = -1 + 2\zeta_{16} - 4\zeta_{16}^2 - 2\zeta_{16}^3 - 2\zeta_{16}^5 + 4\zeta_{16}^6 + 2\zeta_{16}^7$ or $\delta_1^2\delta_2\bar{\delta}_2 = -1 + 4\zeta_{16} + 2\zeta_{16}^2 + 2\zeta_{16}^3 + 2\zeta_{16}^5 - 2\zeta_{16}^6 + 4\zeta_{16}^7$.

In the study of (25652, 227, 2) difference sets, we need to know how the ideals generated by 3 and 5 factor in the cyclotomic ring $\mathbb{Z}[\zeta_{m'}], m' = 11, 22, 44$. The ideal generated by 3 has 2 factors in $\mathbb{Z}[\zeta_{m'}], m' = 11, 22, 44$. The ideal generated by 5 has 2 factors in $\mathbb{Z}[\zeta_{m'}], m' = 4, 11, 22, 121, 242$ and four factors in $\mathbb{Z}[\zeta_{44}]$. It can be shown that $\langle 5\rangle = \langle 2 + q\rangle\langle 2 + \bar{q}\rangle$ and $\langle 3\rangle = \langle q\rangle\langle \bar{q}\rangle$ in $\mathbb{Z}[\zeta_{m'}], m' = 11, 22$, $q = \zeta_{11} + \zeta_{11}^3 + \zeta_{11}^4 + \zeta_{11}^5 + \zeta_{11}^9$, $q + \bar{q} = -1$, $q\bar{q} = 3$, $q^2 = -2 + \bar{q}$ and $(\bar{q})^2 = -2 + q$. Thus, in rings $\mathbb{Z}[\zeta_{m'}], m' = 11, 22$, the equation $\delta\bar{\delta} = 225$ has the following solutions:$\delta = 15, 3(1 + 3q), 3(-2 - 3q), (3 + q)(1 + 3q) = -6 + 7q$, $(3 + q)(-2 - 3q) = 3 - 8q$, $(-2 + q)(1 + 3q) = -11 - 8q$, $(-2 + q)(1 + 3q) = 13 + 7q, 5(-3 - q)$ and $5(-2 + q)$. It should be noted that the ideal generated by 3 has 22 factors in $\mathbb{Z}[\zeta_{m'}], m' = 121, 242$ while the ideal generated by 5 has 4 factors in $\mathbb{Z}[\zeta_{44}]$. The above information will be used to obtain difference set images in the factor groups of orders 11 and 22.

International Journal of Mathematical Analysis and
Optimization: Theory and Applications
Vol. 2019, No. 2, pp. 521 - 545

In the case of (52976, 326, 2) difference set parameters, the order is $n = 324 = 2^2 3^4$. Hence we need to know how ideals generated by 2 or 3 factors in the cyclotomic ring $\mathbb{Z}[\zeta_{m'}], m' = 7, 14$. The ideal generated by 3 factors trivially in the cyclotomic ring $\mathbb{Z}[\zeta_{m'}], m' = 7, 14$ while $\langle 2\rangle = \langle \zeta+\zeta^2+\zeta^4\rangle\langle\zeta^3+\zeta^5+\zeta^6\rangle$ in the cyclotomic ring $\mathbb{Z}[\zeta_{m'}], m' = 7, 14$, where ζ is the seventh root of unity. Consequently, the equation $\delta\bar{\delta} = 324$ has the following solutions: $\delta = 18$, $9(\zeta + \zeta^2 + \zeta^4)^2 = 9(-1 + \zeta^3 + \zeta^5 + \zeta^6)$ and $9(\zeta^3 + \zeta^5 + \zeta^6)^2 = 9(-1 + \zeta + \zeta^2 + \zeta^4)$. Furthermore, the ideal generated by 3 has two factors in the cyclotomic ring $\mathbb{Z}[\zeta_{28}]$.

Finally, we look at subgroup properties of a group that can aid the construction of difference set image. It has been established [7, 10, 11, 12] that if K is a subgroup of H such that

$$H \cong K \times \langle z\rangle, z^2 = 1 \tag{2.7}$$

then the difference set image in H can be written as

$$\hat{D} = A\left(\frac{\langle z\rangle}{2}\right) + gB\left(\frac{2-\langle z\rangle}{2}\right), \tag{2.8}$$

$g \in H$, $B = A - \alpha K$, $\alpha = \frac{k+\sqrt{n}}{|K|}$ or $\alpha = \frac{k-\sqrt{n}}{|K|}$ is an integer and k is the size of difference set.

The process of obtaining (v, k, λ) difference set in any group G starts with the computation of difference set images in G/N, where N is an appropriate normal subgroup [22]. These difference set images are constructed by applying various irreducible representations of G/N to solve the equation $\hat{D}\hat{D}^{(-1)} = n + \lambda|N|(G/N)$. We start by finding difference set image in factor group G/N of least order and gradually increase the size of the factor group. In this process, we garner more information about D. If $\hat{D}$ does not exist in G/N, then D does not exist in G. The following remark constructs the difference set image in a group of order p under certain conditions.

Remark 2.12. Suppose G is a group of order v with a normal subgroup N such that $G/N \cong C_p = \langle x : x^p = 1\rangle, p$ is prime. Suppose also that the image of (v, k, λ) difference set, $\hat{D} = \sum_{i=0}^{p-1} d_i x^i$ exists in G/N. We view this image as a $1 \times p$ matrix with the columns indexed by the powers of x.

The characters of C_p are of the form $\chi_i = \zeta_p^i, i = 0, \cdots, p-1$. Using (2.3) and (2.4), the two rational idempotents are:

$$[e_{\chi_0}] = \left(\frac{\langle x\rangle}{p}\right) \quad \text{and} \quad [e_{\chi_1}] = \left(\frac{p-\langle x\rangle}{p}\right).$$

Suppose that $k-\lambda$ is a square and the ideal generated by $\sqrt{k-\lambda}$ factors trivially in the cyclotomic ring $\mathbb{Z}[\zeta_p]$. Then for each non trivial character, $\chi_i, i \neq 0$, $\chi_i(\hat{D}) = \pm(\sqrt{k-\lambda})\zeta_p^{j_i}, j_i = 0, \ldots, p-1$[17]. Thus, the difference set equation is

$$\hat{D} = \sum_{i=0,1} \alpha_{e_{\chi_i}}[e_{\chi_i}], \tag{2.9}$$

where $\alpha_{e_{\chi_i}}$ is an alias. As $\alpha_{e_{\chi_0}} = k$ and based on our hypothesis, $\alpha_{e_{\chi_i}} = \pm(\sqrt{k-\lambda})x^{j_i}$ Hence, the difference set equation becomes $\hat{D} = k[e_{\chi_0}] \pm (\sqrt{k-\lambda})x^{j_i}[e_{\chi_1}], j_i = 0, \ldots, p-1$.

Up to translation, the difference set image(s) is (are)

$$\hat{D} = \frac{1}{p}\left[k \pm \sqrt{k-\lambda}(p-1), k \mp \sqrt{k-\lambda}, \ldots, k \mp \sqrt{k-\lambda}, k \mp \sqrt{k-\lambda}\right] \tag{2.10}$$

In fact, if gcd $(\sqrt{k-\lambda}, p) = 1$, then (2.10) has a unique solution otherwise there are two solutions.

We illustrate the non existence and partial non existence results in the next two sections by looking at some parameter sets.

International Journal of Mathematical Analysis and Optimization: Theory and Applications
Vol. 2019, No. 2, pp. 521 - 545

3 The non-existence results

This section illustrates the method used to establish the non existence of each parameter listed in Theorem 1.1. We look at two cases and assume that G is a group of order v with N, an appropriate normal subgroup. We investigate difference set images in some factor groups G/N.

3.1 The (97904, 443, 2) case

In this case, the order of the group G is $97904 = 2^4 \cdot 29 \cdot 211$. Suppose that N is an appropriate normal subgroup of G. Then by Sylow Theorem, Sylow 29 and Sylow 211 subgroups of G are normal. Thus, we look at the homomorphic images G/N of order $3376 = 2^4 \cdot 211$. Using GAP[23], there are 42 groups of order 3376. Furthermore, the factor groups of order 3376 have Sylow 2 subgroup of order 4 that is normal. Hence, every group of order 3376 has at least one group of order 844 as homomorphic image. Consequently, we investigate the existence or otherwise of difference set images in factor groups of order 844 by stating the following three lemmas.

Lemma 3.1. *We may assume(after translation or applying a group automorphism of G/N, if necessary) that the difference set image in $G/N \cong C_{211} = \langle x | x^{211} = 1\rangle$ is $21 + 2\langle x\rangle$.*

Proof. Use Remark 2.12 and the fact that the ideal generated by 3 and 7 factor trivially in the cyclotomic ring $\mathbb{Z}[\zeta_{211}]$. □

Lemma 3.2. *By using appropriate translation or group automorphism, the difference set image in $G/N \cong C_{422} = \langle x, y | x^{211} = y^2 = [x, y] = 1\rangle$ is $21 + \langle x\rangle\langle y\rangle$.*

Proof. Use equation (2.8) and Lemma 3.1. □

Lemma 3.2 and Dillon Dihedral technique can be used to show that the difference set image in $G/N \cong D_{211} = \langle x, y | x^{211} = y^2 = 1, yxy = x^{-1}\rangle$ is $21 + \langle x\rangle\langle y\rangle$.

Lemma 3.3. *There are no (97904, 443, 2) difference set images in any factor group of order 844.*

Proof. Let H be a factor group of order 844. This proof uses Lemmas 2.6 and 3.2. The distribution of (97904, 443, 2) difference set image in the groups of order 422 is $22^1 1^{421}$. Since there is a normal subgroup N' of H such that H/N' is isomorphic to a group of order 422, we combine this distribution with the variance technique to find the distribution of difference set images in groups of order 844. Using the third equation of Lemma 2.6 and the fact that the coset bound for factor groups of order 844 in G is 116, we get a simplified equation

$$\begin{aligned} m_2 + 3m_3 + 6m_4 + 10m_5 + 15m_6 + 21m_7 + 28m_8 + 36m_9 + 45m_{10} + 55m_{11} \\ +66m_{12} + 78m_{13} + 91m_{14} + 105m_{15} + 120m_{16} + 136m_{17} + 153m_{18} \\ +171m_{19} + 190m_{20} + 210m_{21} + 231m_{22} = 115. \end{aligned} \tag{3.1}$$

However, integer solutions exist if the coefficients of the unknown m_j are not greater than the value on the right hand side of the equal sign (in this case 115). Hence, equation (3.1) reduces to

$$\begin{aligned} m_2 + 3m_3 + 6m_4 + 10m_5 + 15m_6 + 21m_7 + 28m_8 + 36m_9 + 45m_{10} + 55m_{11} \\ +66m_{12} + 78m_{13} + 91m_{14} + 105m_{15} = 115 \end{aligned} \tag{3.2}$$

But the two distinct intersection numbers in the distribution of difference set image of the groups of order 422 are 22 and 1. In order to use these numbers to find the distribution of difference set images in factor groups of order 844, we must recognize that the coset size between these factor groups(order of N') is 2 and as such, each intersection number from the distribution of difference set images in the factor group of order 422 must split into two. Thus, 1 can only split as (1, 0) while 22 will split into one of the following: (22, 0), (21, 1), (20, 2), (19, 3), (18, 4), (17, 5), (16, 6), (15, 7), (14, 8), (13, 9), (12, 10) or (11, 11). Based on the constraint imposed by equation (3.2), 22 cannot split as (22, 0), (21, 1), (20, 2), (19, 3), (18, 4), (17, 5) and (16, 6) because, for each m_j in this equation, j lies between 2 and 15. This simply means that the intersection number "22" must split into two numbers that lie between 2 and 15. But there is only one integer 22 in the distribution of difference set image in the factor group of order 422 that is greater than 1. Consequently, this unique integer 22 can only split as one of the following: (15, 7), (14, 8), (13, 9), (12, 10), or (11, 11). Thus, j must lie between 7 and 15 and (3.2) reduces to

$$21m_7 + 28m_8 + 36m_9 + 45m_{10} + 55m_{11} + 66m_{12} + 78m_{13} + 91m_{14} + 105m_{15} = 115 \tag{3.3}$$

Using the symmetric nature of (3.3) and the way "22" split, the unknown numbers m_j in this equation are paired. That is, if m_j is one of the terms in the equation, so is m_{22-j}. Consequently, (3.3) forced the sum of the coefficients of m_{22-j} and $m_j, j = 7, \ldots, 11$ to be 115 while the other coefficients must be zero. It turns out that there is no j such that the sum of the coefficients of m_{22-j} and m_j equals 115, for $j = 7, \ldots, 11$. For instance, if $m_7 = 1$ and $m_{15} = 1$, then $m_j = 0$ for $j = 8, \ldots, 11$ and $21(1) + 105(1) \neq 115$. This implies that there are no distribution for the difference set images in groups of order 844 and consequently, there are no difference set images in factor groups of order 844. □

Lemma 3.3 implies that there are no difference set images in any of the 42 groups of order 3376. As sylow 29 subgroup is normal in groups of order 97904, there are no (97904, 443, 2) difference sets. The same approach can be used to show that there are no (1415404, 1683, 2) difference sets.

3.2 The (1415404, 1683, 2) case

The order of the group G, in this case, is $v = 1415404 = 2^2 \cdot 431 \cdot 821$. Let N be an appropriate normal subgroup of G. By Sylow Theorem, Sylow 431 and Sylow 821 subgroups of G are normal. We focus on the factor group of order 1724. But we know that if $p \equiv 3 \mod 4$, then there are four groups of order $4p$. Hence, there are four groups of order 1724 and each of these groups has at least one factor group of order $2p = 862$.

Lemma 3.4. *By using appropriate translation or group automorphism, there are no difference set image in* $G/N \cong C_{431} = \langle x | x^{431} = 1 \rangle$.

Proof. The order of this parameter set is $n = k - \lambda = 1681 = 41^2$. Use Remarks 2.12 and 2.8, the set that satisfies all the conditions of being a difference set image in the factor group $G/N \cong C_{431}$ is $4\langle x \rangle - 41$. But the negative intersection number indicates that this set is not admissible as a difference set image. Therefore, there is no difference set image in $G/N \cong C_{431}$.

□

Consequently by Lemma 3.4, there are no difference set images in factor group $G/N \cong C_{862}$. By Dillon technique, there are no difference set images in factor group $G/N \cong D_{431}$. Thus, no factor group of order 1724 admit (1415404,1683, 2) difference set image since any group of order 1724 has least one group of 862 as factor group. Since Sylow 821 subgroups of G are normal, then (841754, 1298, 2) difference set do not exist. This approach can be used to show that (10586, 146, 2),(42196, 291, 2),(65704, 363, 2),(14536, 171, 2),(33154, 258, 2),(196252, 627, 2), (463204, 963, 2), (1282402, 1602, 2), (1558496, 1766, 2), (1712176, 1851, 2),(1876954, 1938, 2) and (2053352, 2027, 2) difference sets do not exist. This completes the proof of Theorem 1.1.

IJMAO

INTERNATIONAL JOURNAL OF MATHEMATICAL ANALYSIS AND OPTIMIZATION: THEORY AND APPLICATIONS
VOL. 2019, NO. 2, PP. 521 - 545

4 Partial non existence results

In this section, we analyze four parameter sets which gives insight into the work done in the other cases in this category. The proof of Theorem 1.2 can be found in [10].

4.1 The (5152, 102, 2) case

In this section, G is a group of order 5152. The order of the difference set is $100 = 2^2 5^2$. To proceed, we must know how the ideals generated by 2 and 5 factor in the respective cyclotomic rings. Consequently, we show that if N is a normal subgroup of G such that G/N is isomorphic to $K \times C_2$, where $K = C_{92}$, $D_{23} \times C_2$ or $C_{46} \times C_2$, then G does not admit (5152, 102, 2) difference sets.

4.1.1 The C_{23} image

Suppose that $G/N \cong C_{23} = \langle x : x^{23} = 1 \rangle$. We know that the ideal generated by 5 or 2 factors trivially in $\mathbb{Z}[\zeta_{23}](5^{11} \equiv -1 \mod 23$ and Remark 2.8). Thus, by Remark 2.12 the difference set image in $G/N \cong C_{23}$, up to equivalence, is $10 + 4\langle x \rangle$.

4.1.2 The C_{46} and D_{23} images

Suppose that $G/N \cong C_{46} = \langle x, y : x^{23} = y^2 = 1 = [x, y] \rangle$. Using (2.8) with $K = C_{23}$, $\alpha = 4$ and $|K| = 23$ we obtain, up to equivalence, $A_1 = 10 + 2\langle x \rangle \langle y \rangle$ 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 $G/N \cong D_{23} = \langle x, y : x^{23} = y^2 = 1, yxy = x^{-1} \rangle$.

4.1.3 The $C_{46} \times C_2$, C_{92} and D_{46} images

We can use equation (2.8) to show that if $G/N \cong D_{46} = \langle x, y : x^{46} = y^2 = 1, yxy = x^{-1} \rangle$, then the difference set image is $A_2 = 10 + \langle x \rangle \langle y \rangle$. Also, if $G/N \cong C_{46} \times C_2 = \langle x, y, z : x^{23} = y^2 = z^2 = 1 = [x, y] = [y, z] = [x, z] \rangle$ then the difference set image is $A_3 = 10 + \langle x \rangle \langle y \rangle \langle z \rangle$. We now work through that of $G/N \cong C_{92} \cong C_{23} \times C_4 = \langle x : x^{23} = y^4 = [x, y] = 1 \rangle$. Suppose that $\hat{D} = \sum_{i=0}^{22} \sum_{j=0}^{3} d_{ij} x^i y^j$ is the difference image in G/N. The group G/N has six rational idempotents out of which four are embedded in $(G/N)/\langle y^2 \rangle \cong C_{46}$. The remaining idempotents are

$$[e_{\chi_{01}}] = \frac{2}{92}\langle x \rangle (1 - y^2) \quad \text{and} \quad [e_{\chi_{11}}] = \frac{2}{92}(23 - \langle x \rangle)(1 - y^2).$$

Thus, the difference set equation is

$$\hat{D} = \frac{46}{92}(A_1)(1 + y^2) \pm \alpha_{\chi_{01}}[e_{\chi_{01}}](xy)^i \pm \alpha_{\chi_{11}}[e_{\chi_{11}}](xy)^j \tag{4.1}$$

where A_1 is the difference set image in $C_{46}, i, j = 0, \ldots, 91$, and $\alpha_{\chi_{01}}, \alpha_{\chi_{11}} \in \{10, 6 + 8y, 6 - 8y\}$. As $46(A_1)(1 + y^2) \equiv 0 \pmod{92}$, the choices of aliases are limited. Up to translation, the three choices are $\alpha_{\chi_{01}} = 10$ and $\alpha_{\chi_{11}} = 10$ or $\alpha_{\chi_{01}} = 6 + 8y$ and $\alpha_{\chi_{11}} = 6 + 8y$ or $\alpha_{\chi_{01}} = 6 - 8y$ and $\alpha_{\chi_{11}} = 6 - 8y$. Consequently, there are many solutions to (4.1) but the only viable difference set image, up to translation, is $A_4 = 10 + \langle x \rangle \langle y \rangle$.

Notice that the distribution of difference set images $A_i, i = 2, 3, 4$ is $11^1 1^{91}$. We will use this information along with variance technique to find the distribution of difference set images in groups of order 184 having $C_{46} \times C_2$, C_{92} or D_{46} as homomorphic image(s). The intersection number 11 can split in one of the following ways: (11, 0), (10, 1), (9, 2), (8, 3), (7, 4) or (6,5). If we only look

IJMAO

INTERNATIONAL JOURNAL OF MATHEMATICAL ANALYSIS AND OPTIMIZATION: THEORY AND APPLICATIONS
VOL. 2019, NO. 2, PP. 521 - 545

at the third equation of Lemma 2.6 and the fact that the coset bound for groups of order 184 in G is 28, we get

$$m_2 + 3m_3 + 6m_4 + 10m_5 + 15m_6 + 21m_7 + 28m_8 + 36m_9 + 45m_{10} + 55m_{11} = 27. \tag{4.2}$$

In this case, the sum of coefficients of m_j and m_{11-j} must be 27. The only pair that satisfies this constraint is m_4 and m_7. Thus, Lemma 2.6 becomes

$$m_0 + m_1 + m_4 + m_7 = 184 \tag{4.3}$$
$$m_1 + 4m_4 + 7m_7 = 102 \tag{4.4}$$
$$6m_4 + 21m_7 = 27. \tag{4.5}$$

Equation (4.5) implies that $m_4 = m_7 = 1$. Substituting $m_4 = m_7 = 1$ in equation (4.4), we get $m_1 = 91$. Finally, equation (4.3) shows that $m_0 = 91$. Hence, the unique distribution of difference set image in factor groups of order 184 is $0^{91}1^{91}4^17^1$. By combining this distribution with (2.8), it can be shown that if $G/N \cong K \times C_2$, where $K = C_{92}$, $D_{23} \times C_2$ or $C_{46} \times C_2$, then G does not admit (5152, 102, 2) difference sets. Next, we show that some groups of order 28 and 32 do not admit (5152, 102, 2) difference sets.

4.1.4 Groups of order 28

4.1.5 The C_7 Image

Suppose that $G/N \cong C_7 = \langle x : x^7 = 1 \rangle$ and $\hat{D} = \sum_{i=0}^{7} d_i x^i$ is the difference image in G/N. We know that the ideal generated by 2 has two factors in $\mathbb{Z}[\zeta_7]$ while the ideal generated by 5 is prime in the same cyclotomic ring. Thus, from Remark 2.11, the solutions to the algebraic equation $\delta\bar{\delta} = 100$ are $\delta = 10, 5(-1+\theta), 5(-1+\bar{\theta})$, $\theta = \zeta_7 + \zeta_7^2 + \zeta_7^4$.

Now, the rational idempotents of C_7 are

$$[e_{\chi_0}] = \frac{1}{7}\langle x \rangle \quad \text{and} \quad [e_{\chi_1}] = \frac{1}{7}(7 - \langle x \rangle)$$

and the difference set equation is

$$\hat{D} = \alpha_{\chi_0}[e_{\chi_0}] \pm \alpha_{\chi_1}[e_{\chi_1}] \tag{4.6}$$

with $\alpha_{\chi_0} = 102$, $\alpha_{\chi_1} \in \{a_1, a_2, a_3\}$, $a_1 = \pm 10x^s$, $a_2 = \pm 5(-1 + x^3 + x^5 + x^6)x^{s'}$ and $a_3 = \pm 5(-1 + x + x^2 + x^4)x^{s''}$, $s, s', s'' = 0, \ldots, 6$. Thus, the difference set equation becomes

$$\hat{D} = \frac{102}{7}\langle x \rangle \pm \frac{a_i}{7}(7 - \langle x \rangle), i = 1, 2, 3. \tag{4.7}$$

Thus, the solutions to (4.7) are:

1. $A_1 = -10 + 16\langle x \rangle$,
2. $A_2 = 21 + 16x + 16x^2 + 11x^3 + 16x^4 + 11x^5 + 11x^6$
3. $A_3 = 21 + 11x + 11x^2 + 16x^3 + 11x^4 + 16x^5 + 16x^6$.

International Journal of Mathematical Analysis and Optimization: Theory and Applications
Vol. 2019, No. 2, pp. 521 - 545

4.1.6 Images of factor groups of order 14

Let N be an appropriate normal subgroup of G such that $G/N \cong C_{14} = \langle x, y : x^7 = y^2 = 1 = [x, y]\rangle \cong C_7 \times \langle y\rangle$. We view the difference set image in G/N as $\hat{D} = \sum_{i=0}^{6}\sum_{j=0}^{1} d_{ij}x^iy^j$. This group is of the form (2.7) and we take $K = C_7$, $\alpha = 16$ and $k = 102$. Then (2.8) becomes $\hat{D} = A_i(\frac{1+y}{2}) + B_jg(\frac{1-y}{2}), i = 1, 2, 3$ where $g \in G/N$, A_i is a difference set image in C_7 and $B_j = A_j - 16K, j = 1, 2, 3$. Up to translation, the difference set images are:

1. $B_1 = 8\langle x\rangle\langle y\rangle - 5 - 5x - 5y + 5xy$,
2. $B_2 = 8\langle x\rangle\langle y\rangle + 5 - 5x^3 - 5x^5 - 5x^6$
3. $B_3 = 8\langle x\rangle\langle y\rangle + 5 - 5x - 5x^2 - 5x^4$.

The Dillon dihedral technique shows that the only difference set images in $D_7 = \langle x, y : x^7 = y^2 = 1, yxy = x^{-1}\rangle$ are B_2 and B_3.

4.1.7 Images of some groups of order 28

Consider $G/N \cong C_{28} = \langle x, y : x^7 = y^4 = 1 = [x, y]\rangle$ and let $\hat{D} = \sum_{t=0}^{3}\sum_{s=0}^{7} x^sy^t$ be the difference set image 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. In section, we are only interested in how ideals generated by 2 and 5 factor in cyclotomic ring $\mathbb{Z}[\zeta_{m'}], m' = 4, 28$ because of our strategy. By Remark 2.11,the solutions to the algebraic equation $\delta\bar{\delta} = 100$ in $\mathbb{Z}[\zeta_4]$ are $\delta = 10, 2(3-4i), 2(3+4i)$ while the solutions in $\mathbb{Z}[\zeta_{28}]$ are $5(-1+\theta), 5(-1+\bar{\theta})$, $\theta = \zeta_7 + \zeta_7^2 + \zeta_7^4$. 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 $\sum_{j=0,1}\sum_{k=0,2}\alpha_{\chi_{(j,k)}}[e_{\chi_{(j,k)}}] = \frac{14B_s}{28}\langle y^2\rangle$, where $B_s, s = 1, 2, 3$ is the difference set image in C_{14} and $\alpha_{\chi_{(j,k)}}$ is an alias. The remaining two rational idempotents are: $[e_{\chi_{(0,1)}}] = \frac{1}{14}\langle x\rangle(1 - y^2)$ and $[e_{\chi_{(1,1)}}] = \frac{1}{14}(7 - \langle x\rangle)(1 - y^2)$. Thus, the difference set image in C_{28} is

$$\hat{D} = \frac{14B_s}{28}\langle y^2\rangle + \alpha_{\chi_{(0,1)}}[e_{\chi_{(0,1)}}] + \alpha_{\chi_{(1,1)}}[e_{\chi_{(1,1)}}], \tag{4.8}$$

where $\alpha_{\chi_{(1,1)}} \in \{\pm 10(xy)^{p_1}, \pm 2(3-4y)(xy)^{p_2}, \pm 2(3+4y)(xy)^{p_3}, \pm(3-4y)(-1+x+x^2+x^4)(xy)^{p_4}, \pm(3+4y)(-1+x+x^2+x^4)(xy)^{p_5}, \pm(3-4y)(-1+x^3+x^5+x^6)(xy)^{p_6}, \pm(3+4y)(-1+x^3+x^5+x^6)(xy)^{p_7}, \pm 5(-1+x^3+x^5+x^6)(xy)^{p_8}, \pm 5(-1+x+x^2+x^4)(xy)^{p_9}, \}$ and $\alpha_{\chi_{(0,1)}} \in \{\pm 10(xy)^{p_{10}}, \pm 2(3-4y)(xy)^{p_{11}}, \pm 2(3+4y)(xy)^{p_{12}}\}$, $p_1, \ldots, p_{12} = 0, \ldots, 27$.

The fact that only four entries of $14B_s\langle y^2\rangle$ are congruent to $0 \mod 28$ reduces the search space severely. Hence, up to equivalence, the difference set images are

1. $E_1 = 5 + 4x + 4x^2 + 3x^3 + 4x^4 + 3x^5 + 3x^6 + (6 + 4x + 4x^2 + 2x^3 + 4x^4 + 2x^5 + 2x^6)y + (8 + 4x + 4x^2 + 4x^4)y^2 + (2 + 4x + 4x^2 + 6x^3 + 4x^4 + 6x^5 + 6x^6)y^3$,
2. $E_2 = 4 + 2x + 2x^2 + 3x^3 + 2x^4 + 3x^5 + 3x^6 + (7 + 3x + 3x^2 + 5x^3 + 3x^4 + 5x^5 + 5x^6)y + (9 + x + x^2 + 5x^3 + x^4 + 5x^5 + 5x^6)y^2 + (1 + 5x + 5x^2 + 3x^3 + 5x^4 + 3x^5 + 3x^6)y^3$,
3. $E_3 = 4 + 3x + 3x^2 + 2x^3 + 3x^4 + 2x^5 + 2x^6 + (1 + 3x + 3x^2 + 5x^3 + 3x^4 + 5x^5 + 5x^6)y + (9 + 5x + 5x^2 + x^3 + 5x^4 + x^5 + x^6)y^2 + (7 + 5x + 5x^2 + 3x^3 + 5x^4 + 3x^5 + 3x^6)y^3$.

The Dillon dihedral technique shows that there no difference set images in $D_{14} = \langle x, y : x^{14} = y^2 = 1, yxy = x^{-1}\rangle$.

The case of $G/N \cong (C_{14} \times C_2) = \langle x, y, z : x^7 = y^2 = z^2 = 1 = [x, y] = [y, z] = [x, z]\rangle = C_{14} \times \langle z\rangle$. will be decided by (2.8) since this group is of the form (2.7). Take $K = C_{14}$, $\alpha = 8$ and $k = 102$.

International Journal of Mathematical Analysis and Optimization: Theory and Applications
Vol. 2019, No. 2, pp. 521 - 545

By considering all possible choices, it turns out that this group does not admit (5152, 102, 2) difference sets. The same argument can be used to confirm the Dillon technique result for D_{14} since $D_{14} \cong D_7 \times C_2$.

Remark 4.1. The Sylow 23 is normal in any group of order 5152 and we look at all homomorphic images of order 224. There are 197 groups of order 224[23]. The fact that there are no (5152, 102, 2) difference set images in $G/N \cong (C_{14} \times C_2)$ or D_{14} eliminates all these groups except for those with the following GAP location number $[224, j], j = 1, 2, 173$. The groups $[224, j], j = 1, 2$ have factor groups that are isomorphic to C_{32}. In the next subsection, we will show that $G/N \cong C_{32}$ does not admit (5152, 102, 2) difference sets.

4.1.8 There are no C_{32} and D_{16}images

4.1.9 The C_2 image

Suppose that $G/N \cong C_2 = \langle x : x^2 = 1\rangle$. Then the difference set image is $10 + 46\langle x\rangle$.

4.1.10 The C_4 image

By using Remark 2.11 and the rational idempotent of $G/N \cong C_4 = \langle x : x^4 = 1\rangle$, it can be shown that the difference set images, up to translation, are:

1. $A_1 = 10 + 23\langle x\rangle$, $A_2 = -10 + 28\langle x\rangle$
2. $A_3 = 31 + 19x + 25x^2 + 27x^3$
3. $A_4 = 32 + 26x + 24x^2 + 20x^3$.

4.1.11 The C_8 image

Given that $G/N \cong C_8 = \langle x : x^8 = 1\rangle$. Using the rational idempotents of C_8 along with Remark 2.11, the difference sets images in C_8 are:

1. $B_1 = -10 + 14\langle x\rangle$, $B_2 = 9 + 9x + 14x^2 + 14x^3 + 9x^4 + 19x^5 + 14x^6 + 14x^7$
2. $B_3 = 11 + 13x + 12x^2 + 5x^3 + 21x^4 + 13x^5 + 12x^6 + 10x^7$
3. $B_4 = 16 + 8x + 12x^2 + 10x^3 + 16x^4 + 18x^5 + 12x^6 + 10x^7$
4. $B_5 = 16 + 13x + 7x^2 + 10x^3 + 16x^4 + 13x^5 + 17x^6 + 10x^7$
5. $B_6 = 16 + 13x + 12x^2 + 5x^3 + 16x^4 + 13x^5 + 12x^6 + 15x^7$
6. $B_7 = 12 + 14x + 10x^2 + 14x^3 + 6x^4 + 14x^5 + 18x^6 + 14x^7$
7. $B_8 = 9 + 17x + 14x^2 + 10x^3 + 9x^4 + 11x^5 + 14x^6 + 18x^7$
8. $B_9 = 13 + 14x + 17x^2 + 14x^3 + 5x^4 + 14x^5 + 11x^6 + 14x^7$
9. $B_{10} = 19 + 13x + 8x^2 + 10x^3 + 13x^4 + 13x^5 + 16x^6 + 10x^7$
10. $B_{11} = 16 + 16x + 12x^2 + 6x^3 + 16x^4 + 10x^5 + 12x^6 + 14x^7$
11. $B_{12} = 20 + 13x + 15x^2 + 10x^3 + 12x^4 + 13x^5 + 9x^6 + 10x^7$
12. $B_{13} = 16 + 17x + 12x^2 + 13x^3 + 16x^4 + 9x^5 + 12x^6 + 7x^7$

International Journal of Mathematical Analysis and Optimization: Theory and Applications
Vol. 2019, No. 2, pp. 521 - 545

4.1.12 The C_{16} image

Consider $G/N \cong C_{16} = \langle x : x^{16} = 1\rangle$. By combining the rational idempotents of C_{16} along with Remark 2.11, the difference sets images in C_{16} are:

1. $E_1 = 2+12x+7x^2+7x^3+7x^4+7x^5+7x^6+7x^7+2x^8+2x^9+7x^{10}+7x^{11}+7x^{12}+7x^{13}+7x^{14}+7x^{15}$
2. $E_2 = 13+4x+6x^2+5x^3+8x^4+9x^5+6x^6+5x^7+3x^8+4x^9+6x^{10}+5x^{11}+8x^{12}+9x^{13}+6x^{14}+5x^{15}$
3. $E_3 = 8+4x+11x^2+5x^3+8x^4+9x^5+6x^6+5x^7+8x^8+4x^9+x^{10}+5x^{11}+8x^{12}+9x^{13}+6x^{14}+5x^{15}$
4. $E_4 = 8+4x+6x^2+10x^3+8x^4+9x^5+6x^6+5x^7+8x^8+4x^9+6x^{10}+8x^{12}+9x^{13}+6x^{14}+5x^{15}$
5. $E_5 = 8+4x+6x^2+5x^3+13x^4+9x^5+6x^6+5x^7+8x^8+4x^9+6x^{10}+5x^{11}+3x^{12}+9x^{13}+6x^{14}+5x^{15}$
6. $E_6 = 8+4x+6x^2+5x^3+8x^4+14x^5+6x^6+5x^7+8x^8+4x^9+6x^{10}+5x^{11}+8x^{12}+4x^{13}+6x^{14}+5x^{15}$
7. $E_7 = 8+4x+6x^2+5x^3+8x^4+9x^5+11x^6+5x^7+8x^8+4x^9+6x^{10}+5x^{11}+8x^{12}+9x^{13}+x^{14}+5x^{15}$
8. $E_8 = 8+4x+6x^2+5x^3+8x^4+9x^5+6x^6+10x^7+8x^8+4x^9+6x^{10}+5x^{11}+8x^{12}+9x^{13}+6x^{14}$
9. $E_9 = 11+7x+5x^2+7x^3+3x^4+7x^5+9x^6+7x^7+x^8+7x^9+5x^{10}+7x^{11}+3x^{12}+7x^{13}+9x^{14}+7x^{15}$
10. $E_{10} = 6+12x+5x^2+7x^3+3x^4+7x^5+9x^6+7x^7+6x^8+2x^9+5x^{10}+7x^{11}+3x^{12}+7x^{13}+9x^{14}+7x^{15}$
11. $E_{11} = 6+7x+10x^2+7x^3+3x^4+7x^5+9x^6+7x^7+6x^8+7x^9+3x^{10}+7x^{11}+3x^{12}+7x^{13}+9x^{14}+7x^{15}$
12. $E_{12} = 6+7x+5x^2+12x^3+3x^4+7x^5+9x^6+7x^7+6x^8+7x^9+6x^{10}+2x^{11}+3x^{12}+7x^{13}+9x^{14}+7x^{15}$
13. $E_{13} = 6+7x+5x^2+7x^3+3x^4+12x^5+9x^6+7x^7+6x^8+7x^9+5x^{10}+7x^{11}+3x^{12}+2x^{13}+9x^{14}+7x^{15}$
14. $E_{14} = 6+7x+5x^2+7x^3+3x^4+7x^5+14x^6+7x^7+6x^8+7x^9+5x^{10}+7x^{11}+3x^{12}+7x^{13}+4x^{14}+7x^{15}$
15. $E_{15} = 6+7x+5x^2+7x^3+3x^4+7x^5+9x^6+12x^7+6x^8+7x^9+5x^{10}+7x^{11}+3x^{12}+7x^{13}+9x^{14}+2x^{15}$
16. $E_{16} = 6+10x+5x^2+7x^3+3x^4+4x^5+9x^6+7x^7+6x^8+4x^9+5x^{10}+7x^{11}+3x^{12}+11x^{13}+9x^{14}+7x^{15}$
17. $E_{17} = 6+7x+8x^2+7x^3+3x^4+7x^5+5x^6+7x^7+6x^8+7x^9+2x^{10}+7x^{11}+3x^{12}+7x^{13}+13x^{14}+7x^{15}$
18. $E_{18} = 6+7x+5x^2+10x^3+3x^4+7x^5+9x^6+3x^7+6x^8+7x^9+5x^{10}+4x^{11}+3x^{12}+7x^{13}+9x^{14}+11x^{15}$
19. $E_{19} = 10+7x+5x^2+7x^3+6x^4+7x^5+9x^6+7x^7+2x^8+7x^9+5x^{10}+7x^{11}+7x^{13}+9x^{14}+7x^{15}$
20. $E_{20} = 6+11x+5x^2+7x^3+3x^4+10x^5+9x^6+7x^7+6x^8+3x^9+5x^{10}+7x^{11}+3x^{12}+4x^{13}+9x^{14}+7x^{15}$
21. $E_{21} = 6+7x+9x^2+7x^3+3x^4+7x^5+12x^6+7x^7+6x^8+7x^9+x^{10}+7x^{11}+3x^{12}+7x^{13}+6x^{14}+7x^{15}$
22. $E_{22} = 6+7x+5x^2+11x^3+3x^4+7x^5+9x^6+10x^7+6x^8+7x^9+5x^{10}+3x^{11}+3x^{12}+7x^{13}+9x^{14}+4x^{15}$
23. $E_{23} = 13+8x+6x^2+3x^3+8x^4+5x^5+6x^6+7x^7+3x^8+8x^9+6x^{10}+3x^{11}+8x^{12}+5x^{13}+6x^{14}+7x^{15}$
24. $E_{24} = 8+13x+6x^2+3x^3+8x^4+5x^5+6x^6+7x^7+8x^8+3x^9+6x^{10}+3x^{11}+8x^{12}+5x^{13}+6x^{14}+7x^{15}$
25. $E_{25} = 8+8x+11x^2+3x^3+8x^4+5x^5+6x^6+7x^7+8x^8+8x^9+x^{10}+3x^{11}+8x^{12}+5x^{13}+6x^{14}+7x^{15}$
26. $E_{26} = 8+8x+6x^2+3x^3+13x^4+5x^5+6x^6+7x^7+8x^8+8x^9+6x^{10}+3x^{11}+3x^{12}+5x^{13}+6x^{14}+7x^{15}$

27. $E_{27} = 8+8x+6x^2+3x^3+8x^4+10x^5+6x^6+7x^7+8x^8+8x^9+6x^{10}+3x^{11}+8x^{12}+6x^{14}+7x^{15}$

28. $E_{28} = 8+8x+6x^2+3x^3+8x^4+5x^5+11x^6+7x^7+8x^8+8x^9+6x^{10}+3x^{11}+8x^{12}+5x^{13}+x^{14}+7x^{15}$

29. $E_{29} = 8+8x+6x^2+3x^3+8x^4+5x^5+6x^6+12x^7+8x^8+8x^9+6x^{10}+3x^{11}+8x^{12}+5x^{13}+6x^{14}+2x^{15}$

30. $E_{30} = 11+8x+6x^2+3x^3+4x^4+5x^5+6x^6+7x^7+5x^8+8x^9+6x^{10}+3x^{11}+12x^{12}+5x^{13}+8x^{14}+7x^{15}$

31. $E_{31} = 8+11x+6x^2+3x^3+8x^4+x^5+6x^6+7x^7+8x^8+5x^9+6x^{10}+3x^{11}+8x^{12}+9x^{13}+6x^{14}+7x^{15}$

32. $E_{32} = 8+8x+9x^2+3x^3+8x^4+5x^5+2x^6+7x^7+8x^8+8x^9+3x^{10}+3x^{11}+8x^{12}+5x^{13}+4x^{14}$

33. $E_{33} = 8+8x+6x^2+6x^3+8x^4+5x^5+6x^6+3x^7+8x^8+8x^9+6x^{10}+8x^{12}+5x^{13}+6x^{14}+11x^{15}$

34. $E_{34} = 12+8x+6x^2+3x^3+11x^4+5x^5+6x^6+7x^7+4x^8+8x^9+6x^{10}+3x^{11}+5x^{12}+5x^{13}+6x^{14}+7x^{15}$

35. $E_{35} = 8+12x+6x^2+3x^3+8x^4+8x^5+6x^6+7x^7+8x^8+4x^9+6x^{10}+3x^{11}+8x^{12}+2x^{13}+6x^{14}+7x^{15}$

36. $E_{36} = 8+8x+10x^2+3x^3+8x^4+5x^5+9x^6+7x^7+8x^8+8x^9+2x^{10}+3x^{11}+8x^{12}+5x^{13}+3x^{14}+7x^{15}$

4.1.13 There are no C_{32} and D_{16} images

Suppose that $G/N \cong C_{32} = \langle x : x^{32} = 1\rangle$ and (5152, 102, 2) difference set image $\hat{D} = \sum_{i=0}^{31} d_i x^i$ exists in G/N. Using (2.3) and (2.4), C_{32} has six rational idempotents and only one of them, $[e_{\chi_1}] = \frac{2-\langle x^{16}\rangle}{2}$ does not have $\langle x^{16}\rangle$ in its kernel. The linear combination of the remaining five rational idempotents which have $\langle x^{16}\rangle$ in their kernel is

$$Y_k = \sum_{j=0,2,4,8,16} \alpha_{e_{\chi_j}}[e_{e_{\chi_j}}] = E_k\left(\frac{\langle x^{16}\rangle}{2}\right),$$

where E_k is a difference set image in C_{16}. Thus, the difference set equation is

$$\hat{D} = E_k\left(\frac{\langle x^{16}\rangle}{2}\right) + \alpha_{e_{\chi_1}}[e_{e_{\chi_1}}], \tag{4.9}$$

where $\alpha_{e_{\chi_1}} \in \{\pm 10x^r, \pm 2(3-4x^8)x^s, \pm 2(3-4x^8)x^t\}, r, s, t = 0, \ldots, 31$. Define $Z_1 = 10 \cdot [e_{\chi_1}] = 5(1-x^{16})$, $Z_2 = 2(3-4x^8)[e_{\chi_1}] = 3-4x^8-3x^{16}+4x^{24}$ and$Z_3 = 2(3+4x^8)[e_{\chi_1}] = 3+4x^8-3x^{16}-4x^{24}$. So (4.9) becomes

$$\hat{D} = Y_k + x^s Z_l, l = 1,2,3; s = 0,\ldots,15; k = 1,\ldots,36 \tag{4.10}$$

As $Z_l \equiv 0 \pmod{32}$, we would expect Y_k to possess the same property. However, none of the Y_k does. This means that (4.10) has no solution. Thus,C_{32} does not admit (5152, 102, 2) difference set. Consequently, by Dillon dihedral trick, so does D_{16}.

Remark 4.2. In addition to Remark 4.1 and the fact that $G/N \cong C_{32}$ does not possess (5152, 102, 2) difference sets, we can now conclude that if (5152, 102, 2) difference sets exist, it must be in groups of order 5152 that have group [224,173] as homomorphic image. This proves Theorem 1.3.

International Journal of Mathematical Analysis and Optimization: Theory and Applications
Vol. 2019, No. 2, pp. 521 - 545

4.2 The (7504, 123,2) case

Let $\hat{D} = \sum_{i=0}^{66} d_i x^i$ be the difference set image in $G/N \cong C_{67} = \langle x : x^{67} = 1\rangle$. The ideal generated by 11 is prime in the cyclotomic ring $\mathbb{Z}[\zeta_{67}]$. By Remark 2.12, $\hat{D} = -11 + 2\langle x\rangle$. Since one of the intersection numbers is negative, there is no difference set image in $G/N \cong C_{67}$. This means that $G/N \cong C_{134}$ does not admit (7504, 123,2) difference sets and the same goes for $G/N \cong D_{67}$ by Dillon dihedral technique. Furthermore, all the nine groups of order 1876 have factor group that is isomorphic to either C_{134} or D_{67}. Hence, all groups of order 1876 do not admit (7504, 123,2) difference sets. Consequently, no group of order 7504 having any one of these groups as homomorphic image admit (7504, 123,2) difference sets. This proves Theorem 1.4.

4.3 The (19504, 198,2) case

In this case, Sylow 23 and Sylow 53 are normal. So, we will look at the factor groups of order 848. The difference set order is $14^2 = 2^2 7^2$ and the ideals generated by 2 and 7 factor trivially in the cyclotomic ring $\mathbb{Z}[\zeta_{m'}], m' = 53, 106$. Thus, by Remark 2.12, there are no difference set images in $G/N \cong C_{53} = \langle x : x^{53} = 1\rangle$(the only solution is $-14 + 4\langle x\rangle$, which is not viable). This implies that there are no difference set images in $G/N \cong C_{106}$ and consequently, in $G/N \cong D_{53}$ by Dillon dihedral technique. But observe that 106 divides 848 and in groups of order 848, Sylow subgroup of order 8 is normal. This implies that groups of order 848 with homomorphic image of order 106 do not admit this difference set. Consequently, all groups of order 848 except those with Gap location number $[848, j], j = 3, 28, 29, 30, 31, 32, 33, 34, 49$ do not admit (19504, 198,2) difference sets.

4.3.1 There are no C_{16} and D_8 images

4.3.2 The C_2 image

If $G/N \cong C_2 = \langle x : x^2 = 1\rangle$, then the difference set image is $14 + 92\langle x\rangle$.

4.3.3 The C_4 and $C_2 \times C_2$ images

Using Remark 2.11 and the rational idempotent of $G/N \cong C_4 = \langle x : x^4 = 1\rangle$, the difference set images, up to translation, are: $A_1 = 14 + 46\langle x\rangle$ and $A_2 = -14 + 53\langle x\rangle$. Similarly, the difference set images in $G/N \cong C_2 \times C_2 = \langle x, y : x^2 = y^2 = [x, y] = 1\rangle$ are $A_3 = 14 + 46\langle x\rangle\langle y\rangle$ and $A_4 = -14 + 53\langle x\rangle\langle y\rangle$.

4.3.4 The C_8 image

Suppose that $G/N \cong C_8 = \langle x : x^8 = 1\rangle$. Using the rational idempotents of C_8 along with Remark 2.11, the difference sets images in C_8 are:

1. $B_1 = 14 + 23\langle x\rangle$, $B_2 = 30 + 30x + 23x^2 + 23x^3 + 30x^4 + 16x^5 + 23x^6 + 23x^7$
2. $B_3 = 30 + 23x + 30x^2 + 23x^3 + 30x^4 + 23x^5 + 16x^6 + 23x^7$
3. $B_4 = 30 + 23x + 23x^2 + 30x^3 + 30x^4 + 23x^5 + 23x^6 + 16x^7$.

By Dillon dihedral technique, the difference set in $D_4 = \langle x, y : x^4 = y^2 = 1, yxy = x^{-1}\rangle$ are

1. $B_5 = 14 + 23\langle x\rangle\langle y\rangle$, $B_6 = 30 + 23x + 30x^2 + 23x^3 + (30 + 23x + 16x^2 + 23x^3)y$
2. $B_7 = 30 + 23x + 30x^2 + 23x^3 + (23 + 30x + 23x^2 + 16x^3)y$
3. $B_8 = 16 + 30x + 30x^2 + 30x^3 + (23 + 23x + 23x^2 + 23x^3)y$.

INTERNATIONAL JOURNAL OF MATHEMATICAL ANALYSIS AND OPTIMIZATION: THEORY AND APPLICATIONS
VOL. 2019, NO. 2, PP. 521 - 545

Using (2.8) with $K = C_4$, $\alpha = 53$ or 46 and $|K| = 4$, the difference set in $G/N \cong C_4 \times C_2 = \langle x, y : x^4 = y^2 = [x, y] = 1\rangle$ are

1. $B_9 = 14 + 23\langle x\rangle\langle y\rangle$, $B_{10} = 30 + 23x + 30x^2 + 23x^3 + (30 + 23x + 16x^2 + 23x^3)y$
2. $B_{11} = 30 + 30x + 23x^2 + 23x^3 + (30 + 16x + 23x^2 + 23x^3)y$
3. $B_{12} = 16 + 30x + 30x^2 + 30x^3 + (23 + 23x + 23x^2 + 23x^3)y$
4. $B_{13} = 23 + 23x + 30x^2 + 30x^3 + (16 + 30x + 23x^2 + 23x^3)y$
5. $B_{14} = 23 + 30x + 23x^2 + 30x^3 + (16 + 23x + 30x^2 + 23x^3)y.$

The difference set images in $G/N \cong (C_2)^3 = \langle x, y, z : x^2 = y^2 = z^2 = [x, y] = [y, z] = [x, z] = 1\rangle$ are similar to those of $C_4 \times C_2$.

4.3.5 The C_{16} image

Consider the group $G/N \cong C_{16} = \langle x : x^{16} = 1\rangle$. Suppose that the difference image in this group is $\hat{D} = \sum_{s=0}^{15} d_s x^s$. We view this element as 1×16 matrix. Using (2.3) and (2.4), the five rational idempotents of C_{16} are:
$[e_{\chi_0}] = \frac{\langle x\rangle}{16}, [e_{\chi_8}] = \frac{2\langle x^2\rangle - \langle x\rangle}{16}, [e_{\chi_4}] = \frac{2\langle x^4\rangle - \langle x^2\rangle}{8}$, $[e_{\chi_1}] = \frac{2 - \langle x^8\rangle}{2}$, and $[e_{\chi_2}] = \frac{2\langle x^8\rangle - \langle x^4\rangle}{4}$. Four of these rational idempotents have $\langle x^8\rangle$ in their kernel and we write their linear combination as

$$Y_j = \sum_{j=0,2,4,8} \alpha_{\chi_j}[e_{\chi_j}] = B_j\left(\frac{\langle x^8\rangle}{2}\right), j = 1, 2, 3, 4$$

where B_j is a difference set image in C_8 and α_{χ_j} is an alias. Hence, the difference set equation is

$$\hat{D} = Y_j + \alpha_{\chi_1}[e_{\chi_1}], \tag{4.11}$$

where $\alpha_{\chi_1} \in \{\pm 14x^s, \pm 2a_1x^u, \pm 2a_2x^t\}$, $a_1 = -1 + 2x - 4x^2 - 2x^3 - 2x^5 + 4x^6 + 2x^7$, $a_2 = -1 + 4x + 2x^2 + 2x^3 + 2x^5 - 2x^6 + 4x^7, s, t = 0, \ldots, 15$. Define $Z_1 = 14 \cdot [e_{\chi_1}] = 7(2 - \langle x^8\rangle)$, $Z_2 = 2a_1[e_{\chi_1}] = (-1 + 2x - 4x^2 - 2x^3 - 2x^5 + 4x^6 + 2x^7)(1 - x^8)$ and $Z_3 = 2a_2[e_{\chi_1}] = (-1 + 4x + 2x^2 + 2x^3 + 2x^5 - 2x^6 + 4x^7)(1 - x^8)$. Rewrite (4.11) as

$$\hat{D} = Y_j \pm x^l Z_k, k = 1, 2, 3; l = 0, \ldots, 15 \tag{4.12}$$

There are fractions in $Y_j, j = 1, 2, 3, 4$ while $Z_l \equiv 0 \pmod{16}$. The incompatibility implies (4.12) has no solution. Thus,C_{16} does not admit (19504, 198, 2) difference set. Consequently, by Dillon dihedral trick, so does D_8. This information eliminates [848, 3]. Thus if (19504, 198, 2) difference set exist, it must be in the groups of order 7504 with factor groups that are isomorphic to $[848, j], j = 28, 29, 30, 31, 32, 33, 34, 49$. This proves Theorem 1.5.

4.4 The (52976, 326,2) case

Let G be a group of order 52978 and N an appropriate normal subgroup of G.The order of this difference set parameter is $324 = 2^2 3^4$. The ideals generated by 2 and 3 factor trivially in the cyclotomic ring $\mathbb{Z}[\zeta_{43}]$ since $2^7 \equiv -1 \mod 43$ and $2^7 \equiv -1 \mod 43$. Let $\hat{D} = \sum_{s=0}^{42} d_s x^s$ be the difference set image in the factor group $G/N \cong C_{43} = \langle x : x^{43} = 1\rangle$. Using Remark 2.11 and the rational idempotent of G/N, it can be shown that up to translation, the only solution is $\hat{D} = -18 + 8\langle x\rangle$. However, the negative number in the distribution implies that there is no admissible difference set image in $G/N \cong C_{43}$. Consequently, there are no difference set images in factor groups $G/N \cong C_{86}$ and $G/N \cong D_{43}$. This also means that there are no difference set images in each of the four factor groups of order 172. Now, we look at difference set images in some factor groups of order 56.

International Journal of Mathematical Analysis and Optimization: Theory and Applications
Vol. 2019, No. 2, pp. 521 - 545

4.4.1 Factor group of order 7

Suppose that $G/N \cong C_7 = \langle x : x^7 = 1\rangle$ and $\hat{D} = \sum_{i=0}^{7} d_i x^i$ is the difference image in G/N. By using the same method as subsection 4.1.5, we can show that the (52976, 326,2) difference set image in the factor group G/N are

1. $A_1 = 18 + 44\langle x\rangle$
2. $A_2 = 35 + 44x + 44x^2 + 53x^3 + 44x^4 + 53x^5 + 53x^6$
3. $A_3 = 35 + 53x + 53x^2 + 44x^3 + 53x^4 + 44x^5 + 44x^6$.

4.4.2 Factor groups of order 14

Suppose that $G/N \cong C_{14} = \langle x, y : x^7 = y^2 = 1 = [x, y]\rangle = C_7 \times \langle y\rangle$. Let $\hat{D} = \sum_{i=0}^{6}\sum_{j=0}^{1} d_{ij} x^i y^j$ be the difference set image in G/N. Then by (2.8), the difference set images in $G/N \cong C_{14}$ are

1. $B_1 = 18 + 22\langle x\rangle\langle y\rangle$
2. $B_2 = 31+31x+22x^2+22x^3+22x^4+22x^5+22x^6+(31+13x+22x^2+22x^3+22x^4+22x^5+22x^6)y$
3. $B_3 = 13 + 22x + 22x^2 + 31x^3 + 22x^4 + 31x^5 + 31x^6 + 22\langle x\rangle y$
4. $B_4 = 13 + 31x + 31x^2 + 22x^3 + 31x^4 + 22x^5 + 22x^6 + 22\langle x\rangle y$

On the other hand, using Dillon trick, only B_1, B_3 and B_4 are difference set images in the factor group $G/N \cong D_7 = \langle x, y : x^7 = y^2 = 1, yxy = x^{-1}\rangle$.

4.4.3 The $C_{14} \times C_2$ images

Using (2.8), the difference set images in $G/N \cong C_{14} \times C_2 = \langle x, y, z : x^7 = y^2 = z^2 = 1 = [x, y] = [x, z] = [z, y]\rangle$ are

1. $D_1 = 18 + 11\langle x\rangle\langle y\rangle\langle z\rangle$
2. $D_2 = 20 + 20x + 11x^2 + 11x^3 + 11x^4 + 11x^5 + 11x^6 + (20 + 2x + 11x^2 + 11x^3 + 11x^4 + 11x^5 + 11x^6)y + 11\langle x\rangle z + 11\langle x\rangle yz$
3. $D_3 = 2 + 11x + 11x^2 + 20x^3 + 11x^4 + 20x^5 + 20x^6 + 11\langle x\rangle y + 11\langle x\rangle z + 11\langle x\rangle yz$
4. $D_4 = 2 + 20x + 20x^2 + 11x^3 + 20x^4 + 11x^5 + 11x^6 + 11\langle x\rangle y + 11\langle x\rangle z + 11\langle x\rangle yz$
5. $D_5 = 20 + 20x + 11x^2 + 11x^3 + 11x^4 + 11x^5 + 11x^6 + (11 + 11x + 11x^2 + 11x^3 + 11x^4 + 11x^5 + 11x^6)y + (20 + 2x + 11x^2 + 11x^3 + 11x^4 + 11x^5 + 11x^6)z + 11\langle x\rangle yz$.

Furthermore, only D_1, D_3, D_4 and D_5 are the difference set images in factor group $D_7 \times C_2 = \langle x, y, z : x^7 = y^2 = z^2 = [x, z] = [z, y] = 1, yxy = x^{-1}\rangle$.

4.4.4 There are no difference set images in some factor groups of order 56

Using (2.8), we can show that there are no difference set images in factor groups $G/N \cong C_{14}\times C_2\times C_2$ and $G/N \cong D_{14} \times C_2$. This proves Theorem 1.6.

An approach similar to the one in this section can be used to establish Theorems 1.7, 1.8 , 1.9 , 1.10 , 1.11 , 1.12 , 1.13, 1.14 and 1.15

International Journal of Mathematical Analysis and Optimization: Theory and Applications
Vol. 2019, No. 2, pp. 521 - 545

5 Work in progress

5.1 The (25652, 227,2) case

This section generates the difference set images in factor groups of order 11 and 22 that will be used to find the corresponding difference sets images in factor groups of order 44.

5.1.1 The C_{11} image

Suppose that $G/N \cong C_{11} = \langle x : x^{11} = 1\rangle$. One can combine the rational idempotents of C_{11} with Remark 2.11 to obtain the following difference sets images in C_{11}:

1. $A_1 = 7 + 22\langle x\rangle$
2. $A_2 = 22 + 16x + 25x^2 + 16x^3 + 16x^4 + 16x^5 + 25x^6 + 25x^7 + 25x^8 + 16x^9 + 25x^{10}$
3. $A_3 = 22 + 25x + 16x^2 + 25x^3 + 25x^4 + 25x^5 + 16x^6 + 16x^7 + 16x^8 + 25x^9 + 16x^{10}$
4. $A_4 = 12 + 25x + 18x^2 + 25x^3 + 25x^4 + 25x^5 + 18x^6 + 18x^7 + 18x^8 + 25x^9 + 18x^{10}$
5. $A_5 = 27 + 16x + 24x^2 + 16x^3 + 16x^4 + 16x^5 + 24x^6 + 24x^7 + 24x^8 + 16x^9 + 24x^{10}$
6. $A_6 = 27 + 24x + 16x^2 + 24x^3 + 24x^4 + 24x^5 + 16x^6 + 16x^7 + 16x^8 + 24x^9 + 16x^{10}$
7. $A_7 = 12 + 18x + 25x^2 + 18x^3 + 18x^4 + 18x^5 + 25x^6 + 25x^7 + 25x^8 + 18x^9 + 25x^{10}$
8. $A_8 = 32 + 22x + 17x^2 + 22x^3 + 22x^4 + 22x^5 + 17x^6 + 17x^7 + 17x^8 + 22x^9 + 17x^{10}$
9. $A_9 = 32 + 17x + 22x^2 + 17x^3 + 17x^4 + 17x^5 + 22x^6 + 22x^7 + 22x^8 + 17x^9 + 22x^{10}$

5.1.2 The C_{22} and D_{11} images

Given that $G/N \cong C_{22} = \langle x, y : x^{11} = y^2 = 1 = [x, y]\rangle$. By using (2.8) with $K = C_{11}$, $\alpha = 22$ and $|K| = 11$ we obtain, up to equivalence, the following difference sets images:

1. $B_1 = 11 + 5x + 14x^2 + 5x^3 + 5x^4 + 5x^5 + 14x^6 + 14x^7 + 14x^8 + 5x^9 + 14x^{10} + 11\langle x\rangle y$
2. $B_2 = 6 + 6x + 14x^2 + 6x^3 + 6x^4 + 6x^5 + 14x^6 + 14x^7 + 14x^8 + 6x^9 + 14x^{10} + (16 + 10x + 11x^2 + 10x^3 + 10x^4 + 10x^5 + 11x^6 + 11x^7 + 11x^8 + 10x^9 + 11x^{10})y$
3. $B_3 = 16 + 8x + 10x^2 + 8x^3 + 8x^4 + 8x^5 + 10x^6 + 10x^7 + 10x^8 + 8x^9 + 10x^{10} + (6 + 8x + 15x^2 + 8x^3 + 8x^4 + 8x^5 + 15x^6 + 15x^7 + 15x^8 + 8x^9 + 15x^{10})y$
4. $B_4 = 6 + 8x + 12x^2 + 8x^3 + 8x^4 + 8x^5 + 12x^6 + 12x^7 + 12x^8 + 8x^9 + 12x^{10} + (1 + 14x + 10x^2 + 14x^3 + 14x^4 + 14x^5 + 10x^6 + 10x^7 + 10x^8 + 14x^9 + 10x^{10})y$
5. $B_5 = 1 + 14x + 7x^2 + 14x^3 + 14x^4 + 14x^5 + 7x^6 + 7x^7 + 7x^8 + 14x^9 + 7x^{10} + 11\langle x\rangle y$
6. $B_6 = 6 + 14x + 6x^2 + 14x^3 + 14x^4 + 14x^5 + 6x^6 + 6x^7 + 6x^8 + 14x^9 + 6x^{10} + (6 + 11x + 12x^2 + 11x^3 + 11x^4 + 11x^5 + 12x^6 + 12x^7 + 12x^8 + 11x^9 + 12x^{10})y$
7. $B_7 = 11 + 10x + 9x^2 + 10x^3 + 10x^4 + 10x^5 + 9x^6 + 9x^7 + 9x^8 + 10x^9 + 9x^{10} + (1 + 15x + 9x^2 + 15x^3 + 15x^4 + 15x^5 + 9x^6 + 9x^7 + 9x^8 + 15x^9 + 9x^{10})y$
8. $B_8 = 16 + 5x + 13x^2 + 5x^3 + 5x^4 + 5x^5 + 13x^6 + 13x^7 + 13x^8 + 5x^9 + 13x^{10} + 11\langle x\rangle y$
9. $B_9 = 7 + 9\langle x\rangle + (11 + 7x + 15x^2 + 7x^3 + 7x^4 + 7x^5 + 15x^6 + 15x^7 + 15x^8 + 7x^9 + 15x^{10})y$

10. $B_{10} = 6+8x+12x^2+8x^3+8x^4+8x^5+12x^6+12x^7+12x^8+8x^9+12x^{10}+(21+8x+12x^2+8x^3+8x^4+8x^5+12x^6+12x^7+12x^8+8x^9+12x^{10})y$

11. $B_{11} = 16+8x+10x^2+8x^3+8x^4+8x^5+10x^6+10x^7+10x^8+8x^9+10x^{10}+(16+14x+7x^2+14x^3+14x^4+14x^5+7x^6+7x^7+7x^8+14x^9+7x^{10})y$

12. $B_{12} = 11+9x+10x^2+9x^3+9x^4+9x^5+10x^6+10x^7+10x^8+9x^9+10x^{10}+(21+13x+7x^2+13x^3+13x^4+13x^5+7x^6+7x^7+7x^8+13x^9+7x^{10})y$

13. $B_{13} = 21+11x+6x^2+11x^3+11x^4+11x^5+6x^6+6x^7+6x^8+11x^9+6x^{10}+11\langle x\rangle y$

By Dillon dihedral technique, only B_1, B_5, B_{11} and B_{13} are difference set images in $G/N \cong D_{11} = \langle x, y : x^{11} = y^2 = 1, yxy = x^{-1}\rangle$.

6 CONCLUDING REMARKS

The variance technique is a necessary condition for the existence of difference set. However, if combined with the difference set images in some factor groups, it is sufficient to determine the non-existence of difference sets. Finally, Table 1 summarizes this paper.

Table 1: Status of $(v, k, 2)$ parameter sets with $n = m^2$ and $m \leq 45$

No.	Parameter	m	Reason
1	(16, 6, 2)	2	exists
2	(56, 11, 2)	3	does not exist, [1]
3	(154, 18, 2)	4	does not exist,[1]
4	(352, 27, 2)	5	does not exist, [13]
5	(704, 38, 2)	6	does not exist,[7]
6	(1276, 51, 2)	7	Thm. 1.2, [10],
7	(2146, 66, 2)	8	does not exist, [11]
8	(3404, 83, 2)	9	does not exist, [11]
9	(5152, 102, 2)	10	Thm. 1.3
10	(7504, 123, 2)	11	Thm. 1.4
11	(10586, 146, 2)	12	does not exist, Thm.1.1
12	(14536, 171, 2)	13	does not exist, Thm.1.1
13	(19504, 198, 2)	14	Thm. 1.5
14	(25652, 227, 2)	15	work in progress
15	(33154, 258, 2)	16	does not exist, Thm.1.1
16	(42196, 291, 2)	17	does not exist, Thm.1.1
17	(52976, 326, 2)	18	Thm. 1.6
18	(65704, 363, 2)	19	does not exist, Thm.1.1
19	(80602, 402, 2)	20	work in progress
20	(97904, 443, 2)	21	does not exist, Thm.1.1
21	(117856, 486, 2)	22	work in progress
22	(140716, 531, 2)	23	work in progress
23	(166754, 578, 2)	24	Thm. 1.7
24	(196252, 627, 2)	25	does not exist, Thm.1.1
25	(229504, 678, 2)	26	Thm. 1.8
26	(266816, 731, 2)	27	Thm. 1.9
27	(308506, 786, 2)	28	Thm. 1.10
28	(354904, 843, 2)	29	Thm. 1.11
29	(406352, 902, 2)	30	work in progress
30	(463204, 963, 2)	31	does not exist, Thm.1.1
31	(525826, 1026, 2)	32	work in progress
32	(594596, 1091, 2)	33	Thm. 1.12
33	(669904, 1158, 2)	34	work in progress
34	(752152, 1227, 2)	35	work in progress
35	(841754, 1298, 2)	36	work in progress
36	(939136, 1371, 2)	37	Thm. 1.13
37	(1044736, 1446, 2)	38	Thm. 1.14
38	(1159004, 1523, 2)	39	Thm. 1.15
39	(1282402, 1602, 2)	40	does not exist, Thm.1.1
40	(1415404, 1683, 2)	41	does not exist, Thm.1.1
41	(1558496, 1766, 2)	42	does not exist, Thm.1.1
42	(1712176, 1851, 2)	43	does not exist, Thm.1.1
43	(1876954, 1938, 2)	44	does not exist, Thm.1.1
44	(2053352, 2027, 2)	45	does not exist, Thm.1.1

References

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

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

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

[4] T. Beth, D. Jungnickel and H. Lenz, *Design theory,* Cambridge University Press, 1999.

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

[6] L. D. Baumert, *Cyclic Difference Sets,* volume 182 of Lecture Notes in Mathematis, Springer-Verlag Publishers, 1971

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

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

[9] A. V. López and M. A. G. Sánchez, *On the existence of abelian difference sets with* $100 < k \leq 150$, J. Combin. Math. and Combin. Computing **23** (1997), 97–112.

[10] A. S. Osifodunrin, *Do (1276, 51, 2) difference sets exist?*, Kragujevac J. Math. Vol. 35, No. 3 (2011), 479-492.

[11] A. S. Osifodunrin, *On the existence of* (v, k, λ) *difference sets with order* $k < 1250$ *and* $k - \lambda$ *is a square*, International Scholarly Research Network, ISRN Algebra, Volume 2012, Article ID 367129, 19 pages.

[12] A. S. Osifodunrin,*On the non-existence of difference sets with perfect square order*, British Journal of Mathematics and Computer Science **18**(2): 1-17, 2016, Article no.BJMCS.9173

[13] K. W. Smith and S. M. Borman, *Investigations in non abelian difference sets of order 25.* Retrieved on June. 20, 2007 from: http://www.cst.cmich.edu/users/smith1kw/

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

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

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

[17] B. Schmidt, *Cyclotomic Integers and Finite Geometry*, Jour. of Ame. Math. Soc., 12, N.**4**, 1999, pp.929-952.

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

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

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

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

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

[23] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.7.4*; 2014,(http://www.gap-system.org).