British Journal of Mathematics & Computer Science
18(2): 1-17, 2016, Article no.BJMCS.9173
ISSN: 2231-0851

SCIENCEDOMAIN *international*
www.sciencedomain.org

On the Non-Existence of Difference Sets with Perfect Square Order

Adegoke S. Osifodunrin[1*]

[1] *Department of Mathematics, Faculty of Science, University of Lagos, Akoka, Lagos, Nigeria.*

Author's contribution

The sole author designed, analyzed and interpreted and prepared the manuscript.

Article Information

DOI: 10.9734/BJMCS/2016/9173
Editor(s):
(1)Qi Wang, The school of mathematics science, Anhui University, Hefei, China.
Reviewers:
(1) Ayad R. Khudair, Science College, Basrah University, Iraq.
(2) Jaykov Foukzon, Israeli Institute of Technology, Israel.
(3) Nasr Anwer Zeyada, Cairo University, Giza, Egypt.
Complete Peer review History: http://www.sciencedomain.org/review-history/15769

Received: 25th January 2014
Accepted: 15th March 2014
Published: 12th August 2016

Original Research Article

Abstract

The existence of Paley-Hadamard $(4t-1, 2t-1, t-1)$ difference sets provides a platform for solving the equation $\delta\bar{\delta} = n$ in the cyclotomic ring $\mathbb{Z}[\zeta_{4t-1}]$, where ζ_{4t-1} is root of unity, $n > 1$ and $t > 1$ are integers. We look at cases where $\langle n\rangle = \langle\delta\rangle\langle\bar{\delta}\rangle$ in $\mathbb{Z}[\zeta_{4t-1}]$ but $\delta\bar{\delta} = n$ has trivial solutions. This criterion is combined with other results to conclude non-existence of some difference set parameters.

Keywords: Factoring; cyclotomic ring; difference sets; sylow theorems; dillon dihedral trick.

1 Introduction

Suppose that G is a multiplicative group of order v. A subset D of G consisting of k elements, where $1 < k < v-1$ is a non trivial (v, k, λ) difference set if every non-identity element can be replicated precisely λ times by the multi-set $\{d_1 d_2^{-1} : d_1, d_2 \in D, d_1 \neq d_2\}$. The natural number $n = k - \lambda$ is known as the order of the difference set. The group structure determines the nature of the difference set. For instance, if the underlying group G is abelian (resp. non abelian or cyclic,

[*] *Corresponding author: E-mail: asaosifodunrin@yahoo.com;*

then D is abelian (resp. non abelian or cyclic) difference set . The study of Difference sets integrates various techniques ranging from algebraic number theory to geometry, algebra and combinatorics [1]. The readers are referred to [2, 3, 4, 5, 6] for more detailed results on difference sets. This paper uses Turyn's self conjugacy approach [7] to study a class of (v, k, λ) difference sets with $n = m^2$ in groups of order $v = (4t - 1)s$, where $s > 1$ and $t > 1$ are positive integers. We use the existence of Paley-Hadamard $(4t - 1, 2t - 1, t - 1)$ difference sets to look for cases where the ideal generated by m^2 has two factors in $\mathbb{Z}[\zeta_{4t-1}]$, 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 $\delta = \pm m\zeta_{4t-1}^{j}$. This assumption along with Dillon dihedral trick [8] and Sylow Theorems provide sufficient information necessary to decide the non-existence of the difference sets in some or all groups of order v. Paley-Hadamard difference sets exist(in abundance) in that they exist whenever $(4t - 1) \equiv 3 \mod 4$ and $4t - 1$ is a prime power[3]. We illustrate with examples where $2 \leq m \leq 45$. This idea is based on the results of [9] and personal communication with Professor Ken W. Smith.

Section 2 gives a brief description of some basic results which include materials from group theory, representation and algebraic number theories. Section 3 lists some difference sets parameters that do not exist and gives examples of partial results of non-existence of difference sets in groups of order v.

2 Preliminaries

2.1 Difference sets

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

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

Suppose that D is a difference set in a group G of order v and N is a normal subgroup of G. Suppose that $\psi : G \longrightarrow G/N$ is a homomorphism. We can extend ψ by linearity, to the corresponding group rings. Thus, the difference set image in G/N is the multi-set $D/N = \psi(D) = \{dN : d \in D\}$. Let $T^* = \{1, t_1, \ldots, t_h\}$ be a left transversal of N in G. We can write $\psi(D) = \sum_{t_j\in T^*} d_j t_j N$, where the integer $d_j = |D \cap t_j N|$ is known as the **intersection number** of D with respect to N. In this work, we shall always use the notation $\hat{D}$ for $\psi(D)$.

2.2 Basic representation and algebraic number theories

A $\mathbb{C}$- representation of G is a homomorphism, $\chi : G \to GL(d, \mathbb{C})$, where $GL(d, \mathbb{C})$ is the group of invertible $d \times d$ matrices over $\mathbb{C}$. The positive integer d is the degree of χ. A linear representation (character) is a representation of degree one. The set of all linear representations of G is denoted by G^*. G^* is an abelian group under multiplication and if G' is the derived group of G, then G^* is isomorphic to G/G'[10]. Define $\zeta_{m'} := e^{\frac{2\pi}{m'}i}$ to be a primitive m'-th root of unity and $K_{m'} := \mathbb{Q}(\zeta_{m'})$ to be the cyclotomic extension of the field of rational numbers, $\mathbb{Q}$, where m' is the exponent of G. Without loss of generality, we may replace $\mathbb{C}$ by the field $K_{m'}$. Thus, the central primitive idempotents in $\mathbb{C}[G]$ is

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

where χ_i is an irreducible character of G[11].

Aliases are members of group ring which 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 $\Omega = \{\chi_1, \chi_2, \ldots, \chi_h\}$, 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 $G^*/\sim$. The **central rational idempotents** in $\mathbb{Q}[G]$ are obtained by summing over the equivalence classes $X_i = \{e_{\chi_i} | \chi_i \sim \chi_j\} \in G^*/\sim$ on the e_χ's under the action of the Galois group of $K_{m'}$ over $\mathbb{Q}$. That is, $[e_{\chi_i}] = \sum_{e_{\chi_j} \in X_i} e_{\chi_j}, i = 1, \ldots, s$. The following is the general formula employed in the search of difference set [12]

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

$$A = \sum_{i=0}^{s} \alpha_i [e_{\chi_i}], \tag{2.3}$$

where α_i is any χ_i-alias for A.

Equation 2.3 is known as **the rational idempotent decomposition** of A.

Suppose that χ is any non-trivial representation of degree d and $\chi(\hat{D}) \in \mathbb{Z}[\zeta]$, where ζ is the primitive root of unity. Suppose that $x \in G$ is a non identity element. Then, $\chi(xG) = \chi(x)\chi(G) = \chi(G)$. This shows that $(\chi(x) - 1)\chi(G) = 0$. Since x is not an identity element, $(\chi(x) - 1) \neq 0$ and $\chi(G) = 0$ ($\mathbb{Z}[\zeta]$ is an integral domain). Consequently, $\chi(D)\overline{\chi(D)} = n \cdot I_d + \lambda\chi(G) = n \cdot I_d$, where I_d is the $d \times d$ identity matrix. Furthermore, if χ is a non-trivial representation of G/N of degree d then $\hat{D}\hat{D}^{(-1)} = n \cdot 1_{G/N} + |N|\lambda(G/N)$ and $\chi(\hat{D})\overline{\chi(\hat{D})} = n \cdot I_d$.

Recall that the ring of integers of the cyclotomic field $\mathbb{Q}[\zeta_{m'}]$ is $\mathbb{Z}[\zeta_{m'}]$. This ring is also an integral domain. Let $p, a, b \in \mathbb{Z}[\zeta_{m'}]$. The number p is irreducible if $p = ab$ implies one of a or b is a unit. The element p is prime if $p|ab$ implies $p|a$ or $p|b$ [13]. A domain is a unique factorization domain (UFD) if factorization into irreducibles is possible and unique. In UFD, the irreducibles are also primes. In order to successfully obtain the difference set images, we need the aliases. Suppose that G/N is an abelian factor group of exponent m' and $\hat{D}$ is a difference set image in G/N. If χ is not a principal character of G/N, then $\chi(\hat{D})\overline{\chi(\hat{D})} = n$ is an algebraic equation in $\mathbb{Z}[\zeta_{m'}]$. 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. If $\delta := \chi(\hat{D})$, then by equation 2.3, we seek $\alpha \in \mathbb{Z}[G/N]$ such that $\chi(\alpha) = \delta$. The task of solving the algebraic equation $\delta\bar{\delta} = n$ is sometimes made easier if we consider the factorization of principal ideals $\langle\delta\rangle\langle\bar{\delta}\rangle = \langle n\rangle$. Suppose we are able to find $\delta = \sum_{i=0}^{\phi(m')-1} d_i\zeta_{m'}^i \in \mathbb{Z}[\zeta_{m'}]$ such that $\delta\bar{\delta} = n$, where ϕ is the Euler ϕ-function. A theorem due to Kronecker [5, 14] states that any algebraic integer all whose conjugates have absolute value 1 must be a root of unity. We use this theorem to characterize the solutions. If there is any other solution to the algebraic equation, then it must be of the form $\delta' = \delta u$ [15], where $u = \pm\zeta_{m'}^j$ is a unit.

The following result is used to determine the number of factors of an ideal in a ring: Suppose p is any prime and m' is an integer such that $\gcd(p, m') = 1$. Suppose that d is the order of p in the multiplicative group $\mathbb{Z}_{m'}^*$ of the modular number ring $\mathbb{Z}_{m'}$. Then the number of prime ideal factors of the principal ideal $\langle p\rangle$ in the cyclotomic integer ring $\mathbb{Z}[\zeta_{m'}]$ is $\frac{\phi(m')}{d}$, where ϕ is the Euler ϕ-function, i.e. $\phi(m') = |\mathbb{Z}_{m'}^*|$ [16]. For instance, the ideal generated by 2 has two factors in $\mathbb{Z}[\zeta_7]$, the ideal generated by 7 has two factors in $\mathbb{Z}[\zeta_{20}]$, while the ideal generated by 3 has four factors in $\mathbb{Z}[\zeta_{40}]$. On the other hand, since 2^s is a power of 2, the ideal generated by 2 is said to completely ramifies as power of $\langle 1-\zeta_{2^s}\rangle = \overline{\langle 1-\zeta_{2^s}\rangle}$ in $\mathbb{Z}[\zeta_{2^s}]$.

According to Turyn [7], 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, where m'_p is the largest divisor of m' relatively prime to p. This means that every prime ideals over n in $\mathbb{Z}[\zeta_{m'}]$ are fixed by complex conjugation. For instance, $7^2 \equiv -1 \pmod{m'}$, where $m' = 2, 5, 10$ and $7 \equiv -1 \pmod{m'}$, $m' = 2, 4, 8$. Thus, $\langle 7\rangle$ is fixed by conjugation in $\mathbb{Z}[\zeta_{m'}]$, $m' = 2, 4, 5, 8, 10, 50$.

Remark 2.2. If $\langle n\rangle = \Pi_{i=1}^{s}\theta_i$ in cyclotomic ring $\mathbb{Z}[\zeta_{m'}]$, where θ_i is an ideal and s is an odd integer, then there is no solution to $\delta\bar{\delta} = n$. To see this, assume that a δ exist such that $\langle\delta\rangle = \Pi_{i=1}^{k}\alpha_i$. Then $\langle n\rangle = \langle\delta\rangle\langle\bar{\delta}\rangle$ has $2k$ factors but $\langle n\rangle$ has odd factors.

Remark 2.3. In order to verify the existence of (v, k, λ) difference set with $n = k - \lambda = m^2$, where $v = (4t-1)s$, and m is a positive integer, we need aliases of difference set images in C_{4t-1}. Suppose that $(4t-1) \equiv 3 \mod 4$ is a prime power, then $(4t-1,\ 2t-1,\ t-1)$ Paley-Hadamard difference set exists. Let p be a prime divisor of m. We assume that at least one of the following is true: $\langle p\rangle$ is prime, ramifies or has two factors in the cyclotomic ring $\mathbb{Z}[\zeta_{4t-1}]$. If $\langle p\rangle$ is prime or ramifies, then we are done. We now look at the case where $\langle p\rangle$ has two factors. However, we claim that the algebraic number p is prime in this ring. Since $(4t-1,\ 2t-1,\ t-1)$ difference sets exists, there exists θ such that $\theta\bar{\theta} = t$ and $\theta + \bar{\theta} = -1$. This implies that $\theta^2 + \theta + t = 0$ and $\theta = \frac{-1\pm\sqrt{-4t+1}}{2}$. Consequently, $\theta \in \mathbb{Z}[\sqrt{-4t+1}]$. Since $-4t+1 \equiv 1 \pmod 4$([13] chapter 3), the elements of the integral basis of $\mathbb{Z}[\sqrt{-4t+1}]$ are 1 and $\frac{1+i\sqrt{4t-1}}{2}$ and we seek $a, b \in \mathbb{Z}$ such that $\delta = \frac{a+bi\sqrt{4t-1}}{2}$ and $\delta\bar{\delta} = \frac{a^2+(4t-1)b^2}{4} = p$. Consequently, we seek $a, b \in \mathbb{Z}$ such that $\frac{a^2+(4t-1)b^2}{4} = m^2$. In this paper, we look at the situation where this equation has trivial solutions $(a, b) = (-2m, 0)$ and $(2m, 0)$ for some m and values of t listed in Table 1[17]. Hence, $\delta = \pm\frac{a}{2} = \pm m$. Since $2(4t-1) \equiv 2 \pmod 4$[14], the above property is also valid in $\mathbb{Z}[\zeta_{8t-2}]$. In general if $q > 2$ is a prime power such that the ideal generated by p has two factors in $\mathbb{Z}[\zeta_{q(4t-1)}]$, then the above property is also extendable to $\mathbb{Z}[\zeta_{q(4t-1)}]$.

There is a more sophisticated way to show the result of Remark 2.3. This will be illustrated with the non existence of (496, 55, 6) difference sets[18]. The author will like to thank Professor Ken W. Smith for his insight.

Remark 2.4. 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 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. 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 filed 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 $\{a + b(\frac{1+\sqrt{-31}}{2}) : a, b \in \mathbb{Z}\}$. The norm of the element $a + b(\frac{1+\sqrt{-31}}{2} = \frac{(2a+b)+b\sqrt{-31}}{2}$ 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 $b = \pm 1$, then $a^2 - a - 41 = 0$ or $a^2 + a - 41 = 0$ and If $b = 0$, then $a^2 = 49$. Out of these five equations, 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 $\mathbb{Z}[\zeta_{m'}]$; m is self conjugate modulo m'; the ideal generated by m has odd factors or the algebraic equation $\delta\bar{\delta} = m^2$ has trivial solution. In summary, suppose that $\hat{D}$ is the difference set image of order $n = m^2$ in the cyclic factor group G/N, where G/N is a group with exponent m'. Suppose that m factors trivially in $\mathbb{Z}[\zeta_{m'}]$ and χ is a non trivial representation of G/N. Then $\chi(\hat{D}) = \pm m\zeta^i_{m'}$, $\zeta_{m'}$ is the m'-th root of unity [14] and the corresponding alias is $\alpha = \pm mx^i$, where x is a generator of the factor group. Thus, by Theorem 2.1, the (v, k, λ) difference set image in $H = C_q = \langle x : x^q = 1\rangle$ is $\alpha H \pm m$, where q is prime and $\alpha = \frac{k+m}{q}$ or $\alpha = \frac{k-m}{q}$.

2.3 Some attributes of difference set images in the subgroup of a group

Dillon [8] 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 2.5. If the cyclic group Z_{2m} does not contain a (nontrivial) difference set, then neither does the dihedral group of order $2m$.

Remark 2.6. Suppose that H is a group of order $2h$ with a central involution z. We take $T = \{t_i : i = 1, \ldots, h\}$ to be the transversal of $\langle z\rangle$ in H so that every element in H is viewed as $t_iz^j, 0 \le i \le h, j = 0, 1$. Denote the set of all integral combinations, $\sum_{i=1}^h a_it_i$ 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

$$X = X\left(\frac{1+z}{2}\right) + X\left(\frac{1-z}{2}\right). \tag{2.4}$$

Table 1. Parameter sets where the equation $\delta\bar{\delta} = n$ has trivial solution

	$(4t-1,\ 2t-1,\ t-1)$	$k-\lambda = t$		$(4t-1,\ 2t-1,\ t-1)$	$k-\lambda = t$
1	(19, 9, 4)	5	16	(151, 75, 37)	38
2	(23, 11, 5)	6	17	(167, 83, 41)	42
3	(31, 15, 7)	8	18	(191, 95, 47)	48
4	(43, 21, 10)	11	19	(199, 97, 49)	50
5	(47, 23, 11)	12	20	(211, 105, 52)	53
6	(59, 29, 14)	15	21	(223, 111, 55)	56
7	(67, 33, 16)	17	22	(331, 165, 82)	83
8	(71, 35, 17)	18	23	(359, 179, 89)	90
9	(79, 39, 19)	20	24	(383, 191, 95)	96
10	(83, 41, 20)	21	25	(439, 219, 109)	110
11	(103, 51, 25)	26	26	(463, 231, 115)	116
12	(107, 53, 26)	27	27	(467, 233, 116)	117
13	(127, 63, 31)	32	28	(563, 281, 140)	141
14	(131, 65, 32)	33	29	(839, 419, 209)	210
15	(139, 69, 34)	35	30	(991, 495, 247)	248

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

$$X = A\bigg(\frac{\langle z\rangle}{2}\bigg) + B\bigg(\frac{2-\langle z\rangle}{2}\bigg), \tag{2.5}$$

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 $\langle z\rangle$[19]. In particular, it can be shown that if K is a subgroup of a group H such that

$$H \cong K \times \langle z\rangle, \tag{2.6}$$

then the difference set image in H is

$$\hat{D} = A\bigg(\frac{\langle z\rangle}{2}\bigg) + gB\bigg(\frac{2-\langle z\rangle}{2}\bigg), \tag{2.7}$$

where $g \in H$, A is a difference set in K, $\alpha = \frac{k+m}{|K|}$ or $\alpha = \frac{k-m}{|K|}$, $B = A - \alpha K$ and k is the size of the difference set. The equation 2.7 is true as long as $|K| \mid (k+m)$ or $|K| \mid (k-m)$ [19].

2.4 Putting some results together

In this paper, we study (v, k, λ) difference sets in which $n = k - \lambda = m^2$ and the ideal generated by m factors trivially in the cyclotomic ring $\mathbb{Z}[\zeta_{m'}]$. That is, if $n = m^2$, then $(n) = (m)(m)$ up to units in $\mathbb{Z}[\zeta_{m'}]$. This method is very useful in the investigation of difference sets in solvable groups. A group G is solvable if the sequence $G \supseteq G' \supseteq G'' \ldots \supseteq \ldots \supseteq G^{(i)} \ldots$ terminates in the identity, $G^{(e)} = 1$, in a finite number of steps, each $G^{(i)}$ is the derived group of the preceding one[10]. Consequently, each i, the factor group $G^{(i)}/G^{(i+1)}$ is Abelian. We refer readers to the extended Sylow theorem in solvable groups ([10], page 141).

The next three criteria enable us to rule out the existence of difference sets.

Criterion 2.7. Suppose that G is a group of order $v = (4t-1)s$, where s and t are integers. Then G does not admit (v, k, λ) if there exists a normal subgroup N of G such that

1. $k - \lambda = m^2$, m is a natural number,
2. $|G/N| = 4t - 1$
3. m factors trivially in the cyclotomic ring $\mathbb{Z}[\zeta_{4t-1}]$, where ζ_{4t-1} is the $(4t-1)$-th root of unity,
4. the difference set solution in G/N is one of the forms $\alpha(G/N)+m$, $\alpha+m > |N|$ or $\alpha(G/N)-m$, $\alpha < m$.

Proof: The non existence of viable difference set image in G/N implies that G does not admit (v, k, λ) difference set $\square$.

In this criterion, we may replace $|G/N| = 4t-1$ with $|G/N| = q(4t-1)$ if $q > 2$ is prime power, $q|s$, $\gcd(4t-1, q) = 1$ and the ideal generated by p has two factors in $\mathbb{Z}[\zeta_{q(4t-1)}]$, where p is a prime divisor of m(See Remark 2.3).

Criterion 2.8. Suppose that G is a group of even order v and H is a factor group of G with $|H| = 2q$, where q is prime. Let g be an element of order 2 in H. Then G does not admit (v, k, λ) if

1. $k - \lambda = m^2$, m is a natural number,
2. m factors trivially in the cyclotomic rings $\mathbb{Z}[\zeta_q]$, where ζ_q is q-th root of unity,
3. the difference set solution in $H/\langle g\rangle$ is one of the forms $\alpha(H/\langle g\rangle) + m$, $\alpha + m > |G/(H/\langle g\rangle)|$ or $\alpha(H/\langle g\rangle) - m$, $\alpha < m$;alternatively, the difference set image in H is one of the forms $\alpha(H) + m$, $\alpha + m > |G/H|$ or $\alpha(H) - m$, $\alpha < m$.

Proof:See [9] $\square$.

Criterion 2.9. Suppose that G is a group of order $v = 2^2 \times q \times s$, where $q \geq 3$ is prime and s is an integer. Suppose that H is a factor group of G of order $2q$. The group G does not admit (v, k, λ) difference set if there exists a normal subgroup N such that $G/N \cong H \times C_2$ and

1. $k - \lambda = m^2$, m is a natural number,
2. every prime divisor m' of m factors trivially in the cyclotomic rings $\mathbb{Z}[\zeta_q]$, where ζ_q is q-th root of unity, $\gcd(m', q) = 1$
3. the difference set solution in H is of the form $\alpha H + m$, and α is an odd integer or
4. the difference set solution in H is of the form $\alpha H - m$, α is an even integer, m is odd an odd integer and $m > \frac{\alpha}{2}$

Proof: See [9] $\square$.

Notice that there are five factor groups of order $2^2 \times q$ if $q \equiv 1 \pmod 4$ and four factor groups if $q \equiv 3 \pmod 4$. Criterion 2.10 rules out the existence of difference set images in $C_q \times C_2 \times C_2$ and $D_{2q} \cong D_q \times C_2$. In addition to conditions of Criterion 2.10, if m factors trivially also in $\mathbb{Z}[\zeta_{2^2 \times q}]$, then three of the four or five factor groups (C_{2q}, $C_q \times C_2 \times C_2$ and D_{2q}) of order $2^2 \times q$ do not admit difference sets.

3 Non-existence of Some Difference Sets Parameters

In this section, we list some parameter sets (both known and new) that do not exist. In each of these cases, G is a group of order v and $\varphi : G \to H$ is a group homomorphism. Suppose that D is a k-subset of G and $n = k - \lambda = m^2$ such that m factors trivially in the cyclotomic ring $\mathbb{Z}[\zeta_{|H|}]$. We use Criteria 2.7., 2.8., 2.9 to rule out the existence of (v, k, λ) difference set. Examples of such parameters are listed in Tables 3 and 5. We also listed partial results in Tables 2,7 and 9. $*$

indicates new results while $**$ indicates $|G/N| = q(4t-1), q > 2$ is prime power. $***$ refers to the result from [18]. GAP[20] was used to determine the number of groups of order v and the number of groups ruled out.

Table 2. Partial results in groups of order v by Criterion 2.7. $C_{|G/N|} = \langle x \rangle$. The symbol ? means the number of groups of order v is unknown

	$(v,\ k,\ \lambda)$	m	p	$\|G/N\|$	No. of groups of order v	No. of groups ruled out	Solutions in G/N
$1^{*,\ **}$	(3726, 150, 6)	12	2, 3	207	?	?	None
2	(13135, 199, 3)	14	2, 7	71	2	1	$-14 + 3\langle x \rangle$
3^{*}	(54003, 403, 3)	20	2, 5	47	?	?	$-20 + 9\langle x \rangle$
4^{*}	(4042, 450, 50)	20	2, 5	47	4	2	$-20 + 10\langle x \rangle$
5^{*}	(65565, 444, 3)	21	3, 5	31	?	?	$-21 + 15\langle x \rangle$
6	(6461, 476, 35)	21	3, 5	71	2	1	$-21 + 7\langle x \rangle$
7^{*}	(3479, 518, 77)	21	3, 5	497	4	2	$21 + \langle x \rangle$
$8^{*,\ **}$	(234741, 485, 1)	22	2, 11	1389	?	?	None
9^{*}	(79255, 630, 5)	25	5	131	?	?	$-25 + 5\langle x \rangle$
10^{*}	(9423, 673, 48)	25	5	493	13	5	$-25 + 2\langle x \rangle$
11^{*}	(77408, 682, 6)	26	2, 13	59	?	?	$-26 + 12\langle x \rangle$
12	(31787, 691, 15)	26	2, 13	239	2	1	$-26 + 3\langle x \rangle$
13	(6015, 776, 100)	26	2, 13	401	2	1	$-26 + 2\langle x \rangle$
14^{*}	(4221, 845, 169)	26	2, 13	67	11	4	$-26 + 13\langle x \rangle$
15^{*}	(266816, 731, 2)	27	3	379	?	?	$-27 + 2\langle x \rangle$
16^{*}	(67805, 737, 8)	27	3	191	7	2	$-27 + 4\langle x \rangle$
17^{*}	(11716, 781, 52)	27	3	101	15	11	$-27 + 8\langle x \rangle$
18^{*}	(8340, 807, 78)	27	3	139	41	29	$-27 + 6\langle x \rangle$
18^{*}	(6111, 846, 117)	27	3	97	11	4	$-27 + 9\langle x \rangle$
19^{*}	(3015, 1233, 504)	27	3	67	4	2	$-27 + 18\langle x \rangle$
$20^{*,**}$	(2961, 1296, 567)	27	3	329	4	2	None
21^{*}	(615441, 785, 1)	28	2, 7	271	5	2	$-28 + 3\langle x \rangle$
22	(69785, 793, 9)	28	2, 7	821	2	1	$-28 + \langle x \rangle$
23^{*}	(52736, 796, 12)	28	2, 7	103	?	?	$-28 + 8\langle x \rangle$
24	(14145, 833, 49)	28	2, 7	41	2	1	$-28 + 21\langle x \rangle$
24^{*}	(12990, 838, 54)	28	2, 7	433	9	8	$-28 + 2\langle x \rangle$
$25^{*,**}$	(3355, 1248, 464)	28	2, 7	305	7	5	$28 + 4\langle x \rangle$
$26^{*,**}$	(142975, 846, 5)	29	29	215	?	?	None
27^{*}	(102609, 848, 7)	29	29	877	?	?	$-29 + \langle x \rangle$
$28^{*,**}$	(8515, 946, 105)	29	29	655	4	1	None

Table 3. Parameter sets that do not exist by Criterion 2.7. $C_{|G/N|} = \langle x \rangle$

	$(v,\ k,\ \lambda)$	m	p	$\lvert G/N \rvert$	No. of groups of order v	Solutions in G/N
1	(115, 19, 3)	4	2	23	1	$-4 + \langle x \rangle$
2	(391, 40, 4)	6	2, 3	23	1	$-6 + 2\langle x \rangle$
3	(885, 52, 3)	7	7	59	1	$-7 + \langle x \rangle$
$4^{*,**}$	(1475, 67, 3)	8	2	295	2	None
5	(345, 129, 48)	9	3	23	1	$-9 + 6\langle x \rangle$
$6^{*,**}$	(2679, 104, 4)	10	2, 5	141	2	None
7^{*}	(2185, 105, 5)	10	2, 5	23	1	$-10 + 5\langle x \rangle$
$8^{*,**}$	(621, 125, 25)	10	2, 5	69	5	None
9^{**}	(483, 241, 120)	11	11	69	1	None
$10^{*,**}$	(2585, 153, 9)	12	2, 3	235	2	None
11	(2171, 155, 11)	12	2, 3	167	1	$-12 + \langle x \rangle$
12	(581, 261, 117)	12	2, 3	83	1	$12 + 3\langle x \rangle$
$13^{*,**}$	(575, 285, 143)	12	2, 3	115	2	None
14	(2323, 216, 20)	14	2, 7	23	1	$-14 + 10\langle x \rangle$
15	(1411, 235, 39)	14	2, 7	83	1	$-14 + 3\langle x \rangle$
$16^{*,**}$	(1179, 248, 52)	14	2, 7	131	2	$-14 + 2\langle x \rangle$
17	(6059, 234, 9)	15	3, 5	83	1	$-15 + 3\langle x \rangle$
18^{*}	(1035, 330, 105)	15	3, 5	69	2	$-15 + 5\langle x \rangle$
19	(913, 400, 175)	15	3, 5	83	1	$-15 + 5\langle x \rangle$
20^{*}	(28325, 292, 3)	17	17	103	4	$-17 + 3\langle x \rangle$
21^{*}	(35535, 327, 3)	18	2, 3	23	2	$-18 + 5\langle x \rangle$
22	(9381, 336, 12)	18	2, 3	59	1	$-18 + 6\langle x \rangle$
23	(6821, 341, 17)	18	2, 3	359	1	$-18 + \langle x \rangle$
24^{*}	(2751, 375, 51)	18	2, 3	131	2	$-18 + 3\langle x \rangle$
25	(2011, 400, 76)	18	2, 3	191	1	$18 + 2\langle x \rangle$
26	(2021, 405, 81)	18	2, 3	47	1	$-18 + 9\langle x \rangle$
27	(9401, 376, 15)	19	19	79	1	$-19 + 5\langle x \rangle$
28	(44045, 364, 3)	19	19	383	1	$-19 + \langle x \rangle$
29^{*}	(2575, 495, 95)	20	2, 5	103	2	$-20 + 5\langle x \rangle$
30	(1645, 685, 285)	20	2, 5	47	1	$-20 + 15\langle x \rangle$
31^{*}	(1611, 736, 336)	20	2, 5	179	2	$20 + 4\langle x \rangle$
32	(39695, 446, 5)	21	3, 5	467	1	$-21 + \langle x \rangle$
33	(25145, 449, 8)	21	3, 5	47	1	$-21 + 10\langle x \rangle$
34	(5573, 481, 40)	21	3, 5	251	1	$-21 + 2\langle x \rangle$
35	(4465, 496, 55)	21	3, 5	47	1	$-21 + 11\langle x \rangle$
36	(1781, 801, 360)	21	3, 5	137	1	$-21 + 6\langle x \rangle$
37	(22231, 495, 11)	22	2, 11	47	1	$-22 + 11\langle x \rangle$
38	(26461, 540, 11)	23	23	563	1	$-23 + \langle x \rangle$
39	(6391, 640, 64)	24	2, 3	83	1	$-24 + 8\langle x \rangle$
40	(153455, 679, 3)	26	2, 13	47	1	$-26 + 15\langle x \rangle$

Table 4. Table 3 continued

	(v, k, λ)	m	p	$\|G/N\|$	No. of groups of order v	Solutions in G/N
41^*	(115431, 680, 4)	26	2, 13	353	2	$-26+2\langle x\rangle$
42	(92617, 681, 5)	26	2, 13	101	1	$-26+7\langle x\rangle$
43	(52061, 685, 9)	26	2, 13	79	1	$-26+9\langle x\rangle$
44^*	(14063, 712, 36)	26	2, 13	41	5	$-26+18\langle x\rangle$
45	(11537, 721, 45)	26	2, 13	83	1	$-26+9\langle x\rangle$
46	(8437, 741, 65)	26	2, 13	59	1	$-26+13\langle x\rangle$
47^*	(7511, 751, 75)	26	2, 13	37	2	$-26+21\langle x\rangle$
48	(3173, 976, 300)	26	2, 13	167	1	$-26+6\langle x\rangle$
$49^{*,**}$	(4067, 856, 180)	26	2, 13	581	2	None
50^*	(42295, 742, 13)	27	3	769	2	$-27+\langle x\rangle$
51^*	(15105, 768, 39)	27	3	53	2	$-27+15\langle x\rangle$
52^*	(6665, 833, 104)	27	3	43	2	$-27+20\langle x\rangle$
53^*	(3471, 1041, 312)	27	3	89	2	$-27+12\langle x\rangle$
$54^{*,**}$	(2915, 1457, 728)	27	3	265	2	None
55^*	(206195, 787, 3)	28	2, 7	163	3	$-28+5\langle x\rangle$
56^*	(103886, 790, 6)	28	2, 7	409	4	$-28+2\langle x\rangle$
57^*	(24331, 811, 27)	28	2, 7	839	1	$-28+\langle x\rangle$
58^*	(16226, 826, 42)	28	2, 7	61	8	$-28+14\langle x\rangle$
59	(14405, 832, 48)	28	2, 7	43	1	$-28+20\langle x\rangle$
60^*	(5975, 928, 144)	28	2, 7	239	2	$-28+4\langle x\rangle$
61	(5891, 931, 147)	28	2, 7	137	1	$-28+7\langle x\rangle$
$62^{*,**}$	(5005, 973, 189)	28	2, 7	65	2	None
63	(4795, 987, 203)	28	2, 7	685	1	None
64	(3401, 1225, 441)	28	2, 7	179	1	$-28+7\langle x\rangle$
65^*	(89995, 849, 8)	29	29	439	2	$-29+2\langle x\rangle$
66^*	(48793, 856, 15)	29	29	59	2	$-29+15\langle x\rangle$
67	(14353, 897, 56)	29	29	463	1	$-29+2\langle x\rangle$
68	(9889, 928, 87)	29	29	341	1	None
69^{**}	(7689, 961, 120)	29	29	699	1	None
70^*	(4485, 1121, 280)	29	29	69	2	None

Table 5. Parameter sets that do not exist by Criterion.2.8. $C_{|H|} = \langle x, y : x^q = y^2 = [x, y]\rangle$

	$(v,\, k,\, \lambda)$	m	p	$\|H\|$	No. of groups of order v	Solutions in H
1^{***}	(496, 55, 6)	7	7	62	42	$-7 + 2\langle x\rangle$ in $H/\langle g\rangle$
2^{*}	(711, 71, 7)	8	2	79	4	$-8 + \langle x\rangle$ in $H/\langle g\rangle$
3^{*}	(430, 78, 14)	8	2	86	4	$-8 + 2\langle x\rangle$ in $H/\langle g\rangle$
4^{*}	(3404, 83, 2)	9	3	46	11	$-9 + 4\langle x\rangle$ in $H/\langle g\rangle$
5^{*}	(1786, 85, 4)	9	3	94	4	$-9 + 2\langle x\rangle$ in $H/\langle g\rangle$
6^{*}	(2668, 127, 6)	11	11	46	11	$-11 + 6\langle x\rangle$ in $H/\langle g\rangle$
7^{*}	(10586, 146, 2)	12	2, 3	158	4	$-12 + 2\langle x\rangle$ in $H/\langle g\rangle$
8^{*}	(1106, 170, 26)	12	2, 3	158	4	$12 + 2\langle x\rangle$ in $H/\langle g\rangle$
9^{*}	(590, 248, 104)	12	2, 3	118	4	$12 + 4\langle x\rangle$ in $H/\langle g\rangle$
10^{*}	(1888, 222, 26)	14	2, 7	118	195	$-14 + 4\langle x\rangle$ in $H/\langle g\rangle$
11^{*}	(1886, 261, 36)	15	3,5	46	4	$-15 + 12\langle x\rangle$ in $H/\langle g\rangle$
12^{*}	(1692, 267, 42)	15	3,5	94	30	$-15 + 6\langle x\rangle$ in $H/\langle g\rangle$
13^{*}	(1222, 297, 72)	15	3,5	94	4	$15 + 3H$
14^{*}	(7050, 266, 10)	16	2	94	26	$-16 + 6\langle x\rangle$ in $H/\langle g\rangle$
15^{*}	(1128, 392, 136)	16	2	94	39	$16 + 4H$
16^{*}	(1770, 610, 210)	20	2, 5	118	8	$20 + 5H$
17^{*}	(2140, 621, 180)	21	3,7	214	11	$-21 + 6\langle x\rangle$ in $H/\langle g\rangle$

Table 6. Table 5 continued: Parameter sets that do not exist by Criterion 2.8. $C_{|H|} = \langle x, y : x^q = y^2 = [x, y]\rangle$

	$(v,\ k,\ \lambda)$	m	p	$\lvert H\rvert$	No. of groups of order v	Solutions in H
18^*	(2068, 637, 196)	21	3,7	94	9	$-21 + 14\langle x\rangle$ in $H/\langle g\rangle$
19^*	(1984, 661, 220)	21	3,7	62	1388	$-21 + 11H$
20^*	(19570, 594, 18)	24	2, 3	206	8	$-24 + 6\langle x\rangle$ in $H/\langle g\rangle$
21^*	(11534, 608, 32)	24	2, 3	158	4	$-24 + 8\langle x\rangle$ in $H/\langle g\rangle$
22^*	(4922, 666, 90)	24	2, 3	214	4	$24 + 3H$
23^*	(2822, 806, 230)	24	2, 3	166	4	$-24 + 10\langle x\rangle$ in $H/\langle g\rangle$
24^*	(2338, 1026, 450)	24	2, 3	167	4	$-24 + 6\langle x\rangle$ in $H/\langle g\rangle$
25^*	(4544, 826, 150)	26	2, 13	71	1387	$-26 + 12\langle x\rangle$ in $H/\langle g\rangle$
26^*	(134140, 733, 4)	27	3	38	?	$-27 + 20H$
27^*	(4556, 911, 182)	27	3	134	11	$-27 + 14\langle x\rangle$ in $H/\langle g\rangle$
28^*	(45430, 798, 14)	28	2, 7	118	24	$-28 + 14\langle x\rangle$ in $H/\langle g\rangle$
29^*	(35690, 802, 18)	28	2, 7	166	8	$-28 + 10\langle x\rangle$ in $H/\langle g\rangle$
30^*	(6566, 910, 126)	28	2, 7	134	10	$-28 + 14\langle x\rangle$ in $H/\langle g\rangle$
31^*	(4626, 1000, 216)	28	2, 7	514	10	$-28 + 4\langle x\rangle$ in $H/\langle g\rangle$
32^*	(3950, 1078, 294)	28	2, 7	158	10	$-28 + 14\langle x\rangle$ in $H/\langle g\rangle$
33^*	(3486, 1190, 406)	28	2, 7	166	10	$28 + 7H$
34^*	(178296, 845, 4)	29	29	184	?	None
35^*	(18544, 883, 42)	29	29	38	?	$-29 + 24H$
36^*	(13516, 901, 60)	29	29	62	11	$-29 + 15H$
37^*	(11844, 911, 70)	29	29	94	111	$-29 + 20H$

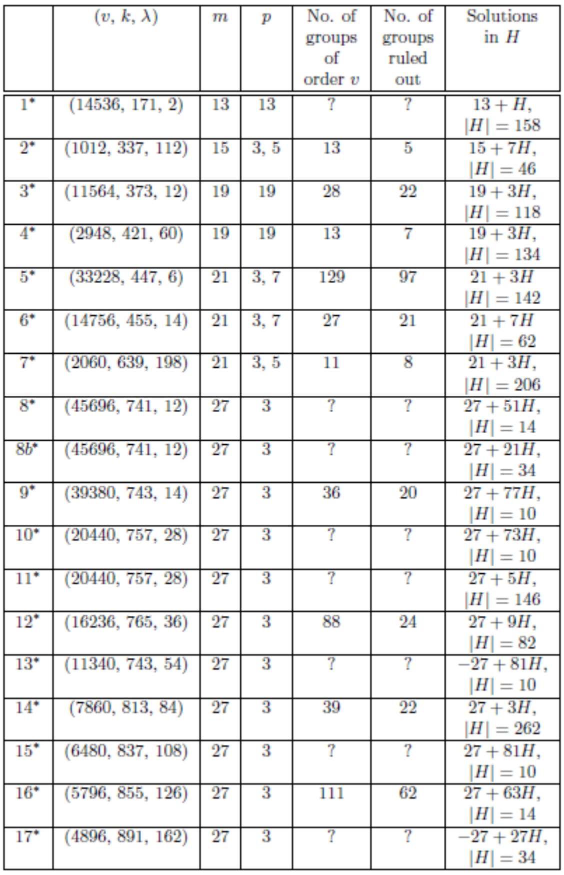
Table 7. Partial results in groups of order v by Criterion 2.8.
$C_{|H|} = \langle x, y : x^q = y^2 = [x, y]\rangle$. **? means the number of groups of order v is unknown**

	(v, k, λ)	m	p	$\|H\|$	No. of groups of order v	No. of groups ruled out	Solutions in H
1^*	(14536, 171, 2)	13	13	46	?	?	$-13 + 8\langle x\rangle$ in $H/\langle g\rangle$
2^*	(5964, 268, 12)	16	2	142	44	34	$-16 + 5\langle x\rangle$ in $H/\langle g\rangle$
3^*	(2718, 286, 30)	16	2	302	16	10	$-16 + 2\langle x\rangle$ in $H/\langle g\rangle$
4^*	(52976, 326, 2)	18	2, 3	86	?	?	$-18 + 8\langle x\rangle$ in $H/\langle g\rangle$
5^*	(3760, 358, 34)	18	2, 3	94	?	?	$-18 + 8\langle x\rangle$ in $H/\langle g\rangle$
6^*	(5336, 485, 44)	21	3, 7	46	?	?	$-21 + 11\langle x\rangle\langle y\rangle$
7^*	(3128, 531, 90)	21	3, 7	46	?	?	$-21 + 12\langle x\rangle\langle y\rangle$
8^*	(2484, 573, 132)	21	3, 7	138	?	?	$21 + 4\langle x\rangle\langle y\rangle$
9^*	(117856, 486, 2)	22	2, 11	254	?	?	$-22 + 4\langle x\rangle$ in $H/\langle g\rangle$
10^*	(6576, 526, 42)	22	2, 11	274	?	?	$-22 + 4\langle x\rangle$ in $H/\langle g\rangle$
11^*	(5372, 656, 80)	24	2, 3	316	11	8	$24 + 2\langle x\rangle\langle y\rangle$
12^*	(98754, 629, 4)	25	5	906	24	12	None
13^*	(33762, 637, 12)	25	5	662	12	8	$-25 + 2\langle x\rangle$ in $H/\langle g\rangle$
14^*	(10528, 726, 50)	26	2, 13	94	?	?	$-26 + 16\langle x\rangle$ in $H/\langle g\rangle$
15^*	(89916, 735, 6)	27	3	254	?	?	$-27 + 6\langle x\rangle$ in $H/\langle g\rangle$
16^*	(30960, 747, 18)	27	3	86	?	?	$-27 + 18\langle x\rangle$ in $H/\langle g\rangle$
17^*	(21896, 755, 26)	27	3	34	?	?	$-27 + 23H$
18^*	(21896, 755, 26)	27	3	46	?	?	$-27 + 17H$
19^*	(14136, 771, 42)	27	3	38	?	?	$-27 + 21H$
20^*	(5016, 885, 156)	27	3	38	?	?	$-27 + 24H$
16^*	(12976, 1275, 546)	27	3	62	?	?	$-27 + 21\langle x\rangle$ in $H/\langle g\rangle$
17^*	(78310, 792, 8)	28	2, 7	82	32	12	$-28 + 20\langle x\rangle$ in $H/\langle g\rangle$
18^*	(18656, 820, 36)	28	2, 7	106	?	?	$-28 + 16\langle x\rangle$ in $H/\langle g\rangle$
19^*	(3526, 1176, 392)	28	2, 7	82 or 86	4	3	None
$20^{*,**}$	(3290, 1288, 504)	28	2, 7	470	8	4	None

Table 8. Table 7 continued.

	(v, k, λ)	m	p	$\|H\|$	No. of groups of order v	No. of groups ruled out	Solutions in H
21^*	(37024, 861, 20)	29	29	178	?	?	$-29 + 10\langle x\rangle$ in $H/\langle g\rangle$
22^*	(26940, 869, 28)	29	29	898	37	27	$-29 + 2\langle x\rangle$ in $H/\langle g\rangle$
23^*	(10176, 925, 84)	29	29	106	?	?	$-29 + 18\langle x\rangle$ in $H/\langle g\rangle$
24^*	(6868, 981, 140)	29	29	202	15	11	$-29 + 10\langle x\rangle$ in $H/\langle g\rangle$
25^*	(3784, 1261, 420)	29	29	86	?	?	$-29 + 15H$

Table 9. Partial results in groups of order v by Criterion 2.9. ? means the number of groups of order v is unknown



	(v, k, λ)	m	p	No. of groups of order v	No. of groups ruled out	Solutions in H
1^*	(14536, 171, 2)	13	13	?	?	$13 + H,$ $\|H\| = 158$
2^*	(1012, 337, 112)	15	3, 5	13	5	$15 + 7H,$ $\|H\| = 46$
3^*	(11564, 373, 12)	19	19	28	22	$19 + 3H,$ $\|H\| = 118$
4^*	(2948, 421, 60)	19	19	13	7	$19 + 3H,$ $\|H\| = 134$
5^*	(33228, 447, 6)	21	3, 7	129	97	$21 + 3H$ $\|H\| = 142$
6^*	(14756, 455, 14)	21	3, 7	27	21	$21 + 7H$ $\|H\| = 62$
7^*	(2060, 639, 198)	21	3, 5	11	8	$21 + 3H,$ $\|H\| = 206$
8^*	(45696, 741, 12)	27	3	?	?	$27 + 51H,$ $\|H\| = 14$
$8b^*$	(45696, 741, 12)	27	3	?	?	$27 + 21H,$ $\|H\| = 34$
9^*	(39380, 743, 14)	27	3	36	20	$27 + 77H,$ $\|H\| = 10$
10^*	(20440, 757, 28)	27	3	?	?	$27 + 73H,$ $\|H\| = 10$
11^*	(20440, 757, 28)	27	3	?	?	$27 + 5H,$ $\|H\| = 146$
12^*	(16236, 765, 36)	27	3	88	24	$27 + 9H,$ $\|H\| = 82$
13^*	(11340, 743, 54)	27	3	?	?	$-27 + 81H,$ $\|H\| = 10$
14^*	(7860, 813, 84)	27	3	39	22	$27 + 3H,$ $\|H\| = 262$
15^*	(6480, 837, 108)	27	3	?	?	$27 + 81H,$ $\|H\| = 10$
16^*	(5796, 855, 126)	27	3	111	62	$27 + 63H,$ $\|H\| = 14$
17^*	(4896, 891, 162)	27	3	?	?	$-27 + 27H,$ $\|H\| = 34$

Table 10. Table 9 continued

	(v, k, λ)	m	p	No. of groups of order v	No. of groups ruled out	Solutions in H
18^*	(3960, 963, 234)	27	3	?	?	$-27 + 99H$, $\|H\| = 10$
19^*	(3816, 981, 252)	27	3	?	?	$27 + 9H$, $\|H\| = 106$
20^*	(3420, 1053, 324)	27	3	144	68	$27 + 27H$, $\|H\| = 38$
21^*	(3280, 1093, 364)	27	3	?	?	$27 + 13H$, $\|H\| = 82$
22^*	(3060, 1197, 468)	27	3	113	50	$27 + 117H$, $\|H\| = 10$
23^*	(3060, 1197, 468)	27	3	113	68	$-27 + 36H$, $\|H\| = 34$
24^*	(3036, 1215, 486)	27	3	34	19	$-27 + 27H$, $\|H\| = 46$
25^*	(119428, 847, 6)	29	29	?	?	$29 + H$, $\|H\| = 818$
26^*	(72336, 851, 10)	29	29	?	?	$29 + 3H$, $\|H\| = 274$
27^*	(52156, 855, 14)	29	29	?	?	$29 + 7H$, $\|H\| = 118$
28^*	(25260, 871, 30)	29	29	71	15	$29 + H$, $\|H\| = 842$
29^*	(18544, 883, 42)	29	29	?	?	$29 + 7H$, $\|H\| = 122$
30^*	(13920, 899, 58)	29	29	?	?	$29 + 87H$, $\|H\| = 10$
31^*	(7888, 957, 116)	29	29	?	?	$-29 + 29H$, $\|H\| = 34$
32^*	(5916, 1015, 174)	29	29	36	21	$29 + 29H$, $\|H\| = 34$
33^*	(5256, 1051, 210)	29	29	?	?	$29 + 7H$, $\|H\| = 146$
34^*	(4408, 1131, 290)	29	29	?	?	$29 + 29H$, $\|H\| = 38$
35^*	(3828, 1247, 406)	29	29	28	15	$29 + 203H$, $\|H\| = 6$
36^*	(3480, 1421, 580)	29	29	?	?	$-29 + 145H$, $\|H\| = 10$

4 Conclusion

This paper shows that Turyn's self conjugacy can be combined with Dillon dihedral trick and Sylow Theorems to establish the non existence of (v, k, λ) difference sets with $n = m^2$ in groups of order $v = (4t - 1)s$, where $m > 1$, $s > 1$ and $t > 1$ are positive integers.

Acknowledgement

The author is grateful to Professor K. W. Smith for his insight and the anonymous referees for the useful suggestions.

Competing Interests

Author has declared that no competing interests exist.

References

[1] Jungnickel D, Pott A, Smith KW. Difference sets. The CRC Handbook of Combinatorial Designs, Preprint, C.J. Colbourn and J.H. Dinitz (Eds.), CRC Press; 2005.

[2] Ionin YJ, Shrikhande MS. Combinatorics of symmetric designs. New Mathematical Monographs, Cambridge University Press, UK; 2006.

[3] Jungnickel D, Pott A. Difference sets: An introduction. Difference Sets, Sequeneces and their Correlation Properties, Klumer Academic Publishers. 1999;259-295.

[4] Lander E. Symmetric design: An algebraic approach. London Math. Soc. Lecture Note Series, Cambridge Univ. Press; 1983.

[5] Pott A. Finite geometry and character theory. Springer-Verlag Publishers; 1995.

[6] Yan T, Xiao G. Divisible difference sets, relative difference sets and sequences with ideal autocorrelation. Information Sciences. 2013;249:143147.

[7] Turyn R. Character sums and difference set. Pacific J. Math. 1965;15:319-346.

[8] Dillon J. Variations on a scheme of McFarland for NonCyclic difference sets. J.Comb.theory A. 1985;40:9-21.

[9] Osifodunrin AS. 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. 2012:19. Article ID 367129.

[10] Hall M, Jr. The theory of groups. Macmillan Company; 1959.

[11] Ledermann W. Introduction to group characters. Cambridge Univ. Press, Cambridge; 1977.

[12] Liebler R. The inversion formula. J. Combin. Math. and Combin. Computing. 1993;13:143-160.

[13] Stewart I, Tall D. Algebraic number theory and fermat's last theorem. A. K. Peters Publishers (3rd ed); 2002.

[14] Schmidt B. Cyclotomic integers and finite geometry. Jour. of Ame. Math. Soc. 1999;12(4):929-952.

[15] Ma SL. Planar functions, relative difference sets and character theory. J. of Algebra. 1996;185: 342-356.

[16] Lang S. Algebraic number theory. Addison-Wesley, Reading, MA; 1970.

[17] Center for communications research. La Jolla Difference Sets Repository. Retrieved on July 21, 2012.
Available:http://www.ccrwest.org/diffsets/diff underscore sets/index.html

[18] Osifodunrin AS. On the existence of non-abelian (210, 77, 28), (336, 135, 54) and (496, 55, 6) difference sets. Discrete Mathematics, Algorithms and Applications. 2011;3(1):121-137.

[19] Osifodunrin AS. On the existence of (400, 57, 8) non-abelian difference sets. Turkish Journal of Mathematics. 2013;37:375-390.

[20] GAP Group. GAP-Groups, Algorithms and Programming, Version 4. 4. 6; 2006. Retrieved on June 20, 2008.
Available:http://www.gap.gap-system.org

Peer-review history:
The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)
http://sciencedomain.org/review-history/15769