MATHEMATICAL COMMUNICATIONS
Math. Commun. **17**(2012), 469–488

On non-existence of some difference sets

Adegoke Solomon Osifodunrin[1,*]

[1] *Division of Mathematics and Sciences, Livingstone College, Salisbury, North Carolina 28 144, USA*

Received December 28, 2010; accepted December 22, 2011

Abstract. Eric Lander conjectured that if G is an abelian group of order v containing a difference set of order n and p is a prime dividing v and n, then the Sylow p-subgroup of G cannot be cyclic. This paper verifies a version of this conjecture for $k < 6500$. A special case of this version is the non-existence of Menon-Hadamard-McFarland difference sets in 2-groups. We also give an algorithm that easily verifies this version of Lander's conjecture and show that some groups do not admit (288, 42, 6) difference sets.

AMS subject classifications: 05B10

Key words: representation, idempotents, Menon-Hadamard-McFarland difference sets, intersection numbers

1. Introduction

We assume that the reader is familiar with the basic information on difference sets [11] and symmetric designs [3, 9]. Ryser conjectured that if D is a (v, k, λ) difference set in a cyclic group G, then $\gcd(v, n) = 1$, while Lander conjectured that if D is a (v, k, λ) difference set in an abelian group G with a cyclic Sylow p-subgroup, then p does not divide $\gcd(v, n)$. Lander's conjecture was an improvement of that of Ryser. Many authors proved some versions of these conjectures but no conclusive general result is known. It has been established that both conjectures are true for $\lambda = 1$ and the case $\lambda = 2$ for abelian difference sets was verified by Dickey and Hughes [7] with $k \leq 5000$ using computer. Also, Arasu [1, 2] validated Lander's conjecture for $\lambda = 3$ and $k \leq 500$ using various non-existence results. Turyn [19] proved a special case of Ryser's conjecture where self conjugacy holds. The most significant progress on these conjectures was made by Leung et al. [14] and they showed that both conjectures are true when n is a power of a prime greater than 3.

Furthermore, Lander [11] proved that 12 of the 14 abelian groups of order 288 do not admit (288, 42, 6) difference sets while Iiams [8] demonstrated that this difference set does not exist in the remaining two abelian groups. This paper studies the non-existence of (v, k, λ) difference sets in which n is a perfect square and G is a group of order v. We start by using difference set basic equation $\lambda(v-1) = r(k-1)$ to find potential (v, k, λ) tuples and use the fact that if v is even, then $n = k - \lambda$ is a perfect square to prune the list for $k < 6500$. Thereafter, we use

*Corresponding author. *Email address:* `Asa_osifodunrin@yahoo.com` (A. S. Osifodunrin)

representation and factorization in cyclotomic rings to show that cyclic Sylow 2-factor group of G does not admit respective difference sets. The Dillon technique shows that the corresponding dihedral factor group behaves similarly. The tuples with these properties appear in Tables 3 - 10. Also, we show that 170 of 1045 groups of order 288 do not admit (288, 42, 6) difference sets. In this paper, we verify the following version of Lander's conjecture combined with Dillon's result.

Conjecture 1. *Let G be a group of order $v = 2^s a$, where $s \geq 4$, $\gcd(2, a) = 1$ and a is a positive integer. Suppose $n = k - \lambda = 2^{2r} b^{2t}$, $\gcd(2, b) = 1, r, t \geq 1$. If there exists a normal subgroup N of G such that G/N is isomorphic to C_{2^s} or $D_{2^{s-1}}$, then G does not admit a (v, k, λ) difference set.*

We also establish the following:

Theorem 1. *Suppose that G is a group of order 288. If there exists a normal subgroup N of G such that G/N is isomorphic to one of C_{32}, D_{16}, $D_8 \times C_2$, $(C_4 \times C_2) \rtimes C_4$, $(C_4)^2 \times C_2$, $D_4 \times (C_2)^2$, $((C_4 \times C_2) \rtimes C_2) \rtimes C_2$([32, 22]), $((C_4 \times C_2) \rtimes C_2) \rtimes C_2$([32, 48]), $(C_4 \times (C_2)^3$, $(C_2)^5$, $(C_2)^4 \rtimes C_2$ or $(C_4 \times C_4) \rtimes C_2$, then G does not admit a $(288, 42, 6)$ difference set.*

[$|G/N|$, cn] means the GAP [5] library number of group G/N. Section 2 discusses basic results while Section 3 provides an algorithm that verifies Conjecture 1 in Sylow 2-cyclic factor groups. In Section 4, we provide a detailed example that demonstrates Conjecture 1 and show that certain groups do not admit (288, 42, 6) difference sets. The last section enumerates parameter sets that satisfy the conjecture along with those that do not.

2. Preliminaries

Difference sets are closely related to symmetric designs and difference sets as follows ([11, Theorem 4.2])

Lemma 1. *Suppose that D is a (v, k, λ) difference set in a group G, then the $Dev(D)$ is a (v, k, λ) symmetric design and G acts as a regular automorphism group of this design.*

This lemma simply means that difference sets can be used to construct symmetric designs. However, the converse is not necessarily true (see [6]).
Let G be a group and N a normal subgroup of G. If D is a (v, k, λ) difference set in G, then the difference set image in G/N (also known as the contraction of D with respect to the kernel N) is the multi-set $D/N = \psi(D) = \{dN : d \in D\}$. Let $T^* = \{1, t_1, \ldots, t_h\}$ be a left transversal of N in G. We can write $\hat{D} = \sum_{t_i \in T^*} d_i t_i N$, where the integer $d_i = |D \cap t_i N|$ is known as the **intersection number** of D with respect to N. In this work, we shall always use the notation $\hat{D}$ for $\psi(D)$ and denote the number of times d_i equals i by $m_i \geq 0$. We now state another necessary but not sufficient condition for the existence of difference sets.

Lemma 2 (Variance trick)**.** *Suppose that D is a (v, k, λ) difference in a group G of order v and N is a normal subgroup of G. Suppose also that $\hat{D}$ is the difference set* *image in G/N and T^* is a left transversal of N in G such that $\{d_i\}$ is a sequence of intersection numbers and $\{m_i\}$, where m_i is the number of times d_i equal to i. Then*

$$\sum_{i=0}^{|N|} m_i = |G/N|, \sum_{i=0}^{|N|} im_i = k, \sum_{i=0}^{|N|} i(i-1)m_i = \lambda(|N|-1). \tag{1}$$

Notice that the bound for each intersection number is $0 \leq d_i \leq \min(|N|, |\hat{D}|)$.

Readers are referred to [12, 13, 16, 18] for basic information on character and representation theories and algebraic number theory. The following results characterize the algebraic number $\chi(\hat{D})$.

Lemma 3. *Let D be a difference set in a group G and N a normal subgroup of G. Suppose that $\psi : G \longrightarrow G/N$ is a natural epimorphism and $n = k - \lambda$. 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 an identity matrix of order d.*

We now state the general formula employed in the search of the difference set in abelian groups [15].

Theorem 2. *Let G be an abelian group and $G^*/\sim$ 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*

$$A = \sum_{i=0}^{s} \alpha_i [e_{\chi_i}], \tag{2}$$

where α_i is any χ_i-alias for A.

Equation (2) is known as **the rational idempotent decomposition** of A.

There are many ways to study difference sets. We adopt the representation theoretic method [15, 17], which entails getting information about the putative difference set D in a group G, by first obtaining comprehensive list $\Omega_{G/N}$ of difference set images in factor group G/N of least size. 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 this signifies non-existence. The following result is credited to Kronecker [18].

Theorem 3 (Kronecker)**.** *Let α be an algebraic integer in $\mathbb{Q}(\zeta)$ where ζ is some root of unity. If α and all its algebraic conjugates have modulus one, then α is a root of unity.*

Aliases are needed for the construction of 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 3, $\chi(\hat{D})\overline{\chi(\hat{D})} = n$, where $\chi(\hat{D})$ is an algebraic number of length $\sqrt{n}$. 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. If $\delta := \chi(\hat{D})$, then by (2) we seek a group ring, $\mathbb{Z}[G/N]$ element say α such that $\chi(\alpha) = \delta$. The task of solving the algebraic equation $\delta\bar{\delta} = n$ is sometimes made easier if we consider the factorization of principal ideals $(\delta)(\bar{\delta}) = (n)$. To achieve this,

a) we must look for all principal ideals $\pi \in \mathbb{Z}[\zeta_{m'}]$ such that $\pi\bar{\pi} = (n)$,

b) for each such ideal, we find a representative element, say δ with $\delta\bar{\delta} = n$, and

c) for each δ we find an alias $\alpha \in \mathbb{Z}[G/N]$ such that $\chi(\alpha) = \delta$.

Using algebraic number theory, we can easily construct the ideal π. The daunting task is to find an appropriate element $\delta \in \pi$. Suppose we are able to find $\delta = \sum_{i=0}^{\phi(m')-1} d_i\zeta_{m'}^i \in \mathbb{Z}[\zeta_{m'}]$ such that $\delta\bar{\delta} = n$, where ϕ is the Euler ϕ-function. By Kronecker's Theorem if there is any other solution to the algebraic equation, then it must be of the form $\delta' = \delta u$ [16], 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 $\zeta_{m'}$ 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. $\phi(m') = |\mathbb{Z}_{m'}^*|$ [12]. For instance, the ideal generated by 2 has two factors in $\mathbb{Z}[\zeta_7]$, the ideal generated by 3 is prime in $\mathbb{Z}[\zeta_{2^s}], s \le 2$ while the ideal generated by 3 has two factors in $\mathbb{Z}[\zeta_{2^s}], s \ge 3$. On the other hand, since 2^s is a power of 2, the ideal generated by 2 is said to completely ramify as power of $(1 - \zeta_{2^s}) = \overline{(1 - \zeta_{2^s})}$ in $\mathbb{Z}[\zeta_{2^s}]$.

According to Turyn [19], an integer n is said to be semi-primitive modulo m' if for every prime factor p of n, there is an integer i such that $p^i \equiv -1 \pmod{m'}$. In this case, -1 belongs to the multiplicative group generated by p. Furthermore, n is self conjugate modulo m' if every prime divisor of n is semi primitive modulo ${m'}_p$, ${m'}_p$ is the largest divisor of m' relatively prime to p. This means that every prime ideal over n in $\mathbb{Z}[\zeta_{m'}]$ is fixed by complex conjugation. For instance, $a^8 \equiv -1 \pmod{m'}$, where $a = 3, 7, 11$ and $m' = 17, 34$. Also, $2^4 \equiv -1 \pmod{17}$ and $7 \equiv -1 \pmod 8$. Thus, $\langle a \rangle$ is fixed by conjugation in $\mathbb{Z}[\zeta_{m'}]$. In this paper, we shall use the phrase 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 G/N, a group with exponent m' and χ is a non trivial representation of G/N, then $\chi(\hat{D}) = m\zeta_{m'}^i$, $\zeta_{m'}$ is the m'-th root of unity.

For (288, 42, 6) difference sets, $n = k - \lambda = 36 = 2^2 3^2$ and we look at factor groups of order $m' = 2^s, s = 1, \ldots, 5$. The ideal $(36) = (2)^2(3)^2$ and we need the factoring of (2) and (3) in the cyclotomic ring $\mathbb{Z}[\zeta_{2^s}]$. The ideal generated by 2 factors trivially in $\mathbb{Z}[\zeta_{2^s}]$, the ideal generated by 3 is prime in $\mathbb{Z}[\zeta_{2^s}], s \le 2$ while (3) has two factors in the same cyclotomic ring for $s > 2$. Consequently, every alias of the difference set is a multiple of 2 in the factor group of order 2^s. Now, we need δ such that $\delta\bar{\delta} = 3^2$ in the cyclotomic field $\mathbb{Q}[\zeta_{2^s}]$, where $s = 3, 4, 5$. (3) has two factors in each of these cyclotomic fields and we consider $\mathbb{Q}[\zeta_8]$. Suppose $\sigma \in \mathbb{Q}[\zeta_8]$, where $\sigma(\zeta_8) = \zeta_8^3$. This Galois automorphism splits the integral basis of $\mathbb{Q}[\zeta_8]$ into two orbits as (ζ_8, ζ_8^3), (ζ_8^5, ζ_8^7). It can be verified that $(3) = (1+\zeta_8+\zeta_8^3)(1+\zeta_8^5+\zeta_8^7)$. Put $\pi = (1 + \zeta_8 + \zeta_8^3)$ and let $\delta_1 = 1 + \zeta_8 + \zeta_8^3$ be a representative of this ideal. The solutions to the algebraic equation $\delta\bar{\delta} = 3^2$ are: $\delta_1\bar{\delta}_1 = 3^2$, δ_1^2 or $\bar{\delta_1}^2$. This shows that $\delta = 9$, $-1 + 2\zeta_8 + 2\zeta_8^3$ or $-1 - 2\zeta_8 - 2\zeta_8^3$. In general, if $m' = 2^s$, where $s \geq 3$, then $(3) = (1+\zeta_{m'}^{2^{s-3}}+\zeta_{m'}^{3\cdot 2^{s-3}})(1-\zeta_{m'}^{2^{s-3}}-\zeta_{m'}^{3\cdot 2^{s-3}})$. In summary, if $\hat{D}$ is a difference set image in $C_{m'}$, a factor group of any group of order 288 and χ is a non trivial representation of $C_{m'}$ such that $\chi(\hat{D})\overline{\chi(\hat{D})} = 2^2 3^2$. Then using Theorem 3, $\chi(\hat{D})$ is

a) $\pm 6\zeta_{m'}^j$ if $m' = 2, 4$, and $j = 0, \ldots, m' - 1$.

b) one of $\pm 6\zeta_{m'}^t, \pm 2(-1+2\zeta_{m'}^{2^{s-3}}+2\zeta_{m'}^{3\cdot 2^{s-3}})\zeta_{m'}^u, \pm 2(-1-2\zeta_{m'}^{2^{s-3}}-2\zeta_{m'}^{3\cdot 2^{s-3}})\zeta_{m'}^r$, if $m' = 2^s, s \geq 3$ and $r, t, u = 0, \ldots, m' - 1$.

Consequently, the possible aliases α in the rational idempotent decomposition of $\hat{D}$ is

1) $\pm 6x^j$ if $m' = 2, 4$, and $j = 0, \ldots, m' - 1, x$ is a generator of $C_{m'}$.

2) one of $\pm 6x^t, \pm 2(-1 + 2x^{2^{s-3}} + 2x^{3\cdot 2^{s-3}})x^u, \pm 2(-1 - 2x^{2^{s-3}} - 2x^{3\cdot 2^{s-3}})x^r$, if $m' = 2^s, s \geq 3$, and $r, t, u = 0, \ldots, m' - 1, x$ is a generator of C_{2^s}.

2.1. Useful results about difference sets in subgroups of a group

The Dillon result below provides a nice way to obtain difference set images in a dihedral group if the difference set images in the corresponding cyclic group of the same order are known.

Theorem 4 (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 1. *If the cyclic group C_{2m} does not contain a (nontrivial) difference set, then neither does the dihedral group of order $2m$.*

The next result describes geometrically how properties of factor group of a group can be lifted, under certain conditions, to the group itself [17].

Theorem 5. *Let D be a (v, k, λ) difference set in group G with a factor group H. Suppose that q is a prime such that $q^s \mid |H|$ and $E \subset C(H)$ is an elementary abelian subgroup of order q^r, $r \leq s$. Suppose also that $E_1, E_2, \ldots, E_t$, where $t = q^{r-d}(\frac{q^r-1}{q-1})$ are the subgroups of E and their cosets, each of order $q^d, d < r$, $\hat{D}$ and $\hat{\hat{D}}_i$ are the corresponding difference set images in H and H/E_i respectively. Suppose there exists an integer a and prime p with $p \mid (k - \lambda)$ such that for each i, $\hat{\hat{D}}_i \equiv a(H/E_i)$ mod p, then there exist an integer k' such that $\hat{D} \equiv a(k')^{-1}H \mod p$.*

It turns out that $k' = q^d$. We will use this result to determine the non-existence of (288, 42, 6) difference set images in some groups of order 32 with $q = 2$, $p = 11$, $k' = 2$, $r = 2$ and $d = 1$. In this paper, we work with (4, 6, 3, 2, 1) design.

Finally, suppose that H is a group of order $2h$ with a central involution z. We take $T = \{t_i : i = 1, \ldots, h\}$ to be the transversal of $\langle z \rangle$ in H so that every element in H is viewed as $t_i z^j, 0 \leq i \leq h, j = 0, 1$. Denote the set of all integral combinations, $\sum_{i=1}^{h} a_i t_i$ of elements of $T, a_i \in \mathbb{Z}$ by $\mathbb{Z}[T]$. Using the two representations of subgroup $\langle z \rangle$ and Frobenius reciprocity theorem [13], we may write any element X of the group ring $\mathbb{Z}[H]$ in the form

$$X = X\left(\frac{1+z}{2}\right) + X\left(\frac{1-z}{2}\right). \tag{3}$$

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

$$X = A\left(\frac{\langle z \rangle}{2}\right) + B\left(\frac{2 - \langle z \rangle}{2}\right), \tag{4}$$

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

$$H \cong K \times \langle z \rangle, \tag{5}$$

then the difference set image in H is

$$\hat{D} = A\left(\frac{\langle z \rangle}{2}\right) + gB\left(\frac{2 - \langle z \rangle}{2}\right), \tag{6}$$

where $g \in H$, A is a difference set in K, $\alpha = \frac{k+\sqrt{n}}{|K|}$ or $\alpha = \frac{k-\sqrt{n}}{|K|}$, $B = A - \alpha K$ and k is the size of the difference set. (6) is true as long as $|K| \mid (k+\sqrt{n})$ or $|K| \mid (k-\sqrt{n})$.

3. The non-existence result and algorithm

3.1. A version of Turyn's and Dillon's results

Turyn's bound [10] states that an abelian group G of order 2^{2u+2} contains a Hadamard difference set if and only if the exponent of G is at most 2^{u+2}. A particular case of Conjecture 1 yields a version of Turyn's and Dillon's results:

Lemma 4. *If $s = 2u+2$ and $p = 1$ in Conjecture 1, then there is no $(2^{2u+2}, 2^u(2^{u+1}-1), 2^u(2^u-1))$ difference set in $C_{2^{2u+2}}$ and $D_{2^{2u+1}}$, u is a natural number.*

3.2. The algorithm: A quadruple summary of the non-existence result

This construction hinges on the splitting of intersection numbers of a (v, k, λ) difference set image in the cyclic factor group of order 2^j, as j increases from 1 to $s-1$, where $v = 2^s a$. The process involves four important intersection numbers of the difference set image in a factor group of order 2^j. Since G is a group of order $v = 2^s a$, let N be a subgroup of order a such that $G/N \cong C_{2^s}$. Let g be the unique element of G/N of order 2 and x the generator of $H = G/\langle g, N\rangle$. Thus by (4), we can write the difference set image in G/N as

$$\hat{D} = A\frac{(1+g)}{2} + B\frac{(1-g)}{2}, \tag{7}$$

where $A = \sum_{i=0}^{|H|-1} t_i x^i$ and t_i is the intersection number of a difference set image in $G/\langle g, N\rangle$, which is isomorphic to $C_{2^{s-1}}$. As $\sqrt{n} = 2^r q^t$, the ideal generated by 2 factors trivially in the cyclotomic ring $Z[\zeta]$, where ζ is the $(2^s)^{th}$ root of unity and presumably q may factor in this cyclotomic ring. Consequently, B is just a translate of 2, say $B = 2g^*$ for some $g^* \in G$. This stipulation forces $A \equiv 0 \pmod 2$. The steps below show that intersection numbers of a difference set image in $H \cong C_{2^{s-1}}$ are not all even integers.

Step 1: Obtain the difference set image in $G/N \cong C_2 = \langle y : y^2 = 1\rangle$. Suppose that $\hat{D} = d_0 + d_1 y$ is the (v, k, λ) difference set image in C_2. The characters of G/N are of the form $\chi_j(y) = (-1)^j$, $j = 0, 1$. By applying $y \mapsto 1$ to $\hat{D}$, we get $d_0 + d_1 = k$ while $y \mapsto -1$ on $\hat{D}$ yields $d_0 - d_1 = \sqrt{n}$ or $-\sqrt{n}$. The solution to this system of equations is one of $d_0 = \frac{k+\sqrt{n}}{2}$ and $d_1 = \frac{k-\sqrt{n}}{2}$ or $d_1 = \frac{k+\sqrt{n}}{2}$ and $d_0 = \frac{k-\sqrt{n}}{2}$.

Step 2: We translate if necessary to ensure that $d_0 > d_1$ and set $d_0 = \frac{k+\sqrt{n}}{2}$ and $d_1 = \frac{k-\sqrt{n}}{2}$. The first number of the quadruple is obtained by dividing d_0 by 2 and adding $\frac{\sqrt{n}}{2}$; the second is obtained by dividing d_0 by 2; for the next number, divide d_1 by 2 and the last number is obtained by dividing d_1 by 2 and subtracting $\frac{\sqrt{n}}{2}$. This process generates the quadruple $\left[\frac{d_0+\sqrt{n}}{2}, \frac{d_0}{2}, \frac{d_1}{2}, \frac{d_1-\sqrt{n}}{2}\right]$.

Step 3: Divide the first coordinate of the quadruplet in step 2 by 2 and add $\frac{\sqrt{n}}{2}$; divide the second coordinate by 2; divide the third coordinate by 2; and finally, divide the fourth coordinate by 2 and subtract $\frac{\sqrt{n}}{2}$. This process generates the quadruple $\left[\frac{d_0+3\sqrt{n}}{4}, \frac{d_0}{4}, \frac{d_1}{4}, \frac{d_1-3\sqrt{n}}{4}\right]$.

Step $j, j \geq 2$: Continue with the iteration to get the j-th quadruplet

$$\left[\frac{d_0 + (2^{j-1}-1)\sqrt{n}}{2^{j-1}}, \frac{d_0}{2^{j-1}}, \frac{d_1}{2^{j-1}}, \frac{d_1 - (2^{j-1}-1)\sqrt{n}}{2^{j-1}}\right].$$

The process terminates at the step $j = s-1$, when the entries are either fractions or odd numbers. At this stage, there is at least one odd number in each set of intersection numbers in the factor group $C_{2^{s-1}}$. Consequently, by parity (7) has no integer solutions and C_{2^s} does not admit a difference set. The Dillon dihedral technique shows that $D_{2^{s-1}}$ does not either. We illustrate the above algorithm with an example.

Example 1. *Consider a (1024, 496, 240) parameter set. In this case,* $n = 256$, $d_0 = \frac{496+\sqrt{n}}{2} = 256$ *and* $d_1 = k - d_0 = 240$ *and* $\frac{\sqrt{n}}{2} = 8$.

Step 1: [256, 240]

Step 2: [136, 128, 120, 112]

Step 3: [76, 64, 60, 48]

Step 4: [46, 32, 30, 16]

Step 5: [31, 16, 15, 0]

Step 6: [, 8, *, *]*

Step 7: [, 4, *, *]*

Step 8: [, 2, *, *]*

Step 9: [, 1, *, *],*

*where * is a place holder for fractions or negative integers. The process terminates at step 9 and there must be at least one odd intersection number in each set of difference set images of* C_{512}. *This shows that* C_{1024} *and* D_{512} *do not admit a (1024, 496, 240) difference set.*

4. Non-existence of (288, 42, 6) difference sets in some groups

We show that if G is a group of order 288 and N is an appropriate normal subgroup of G such that $G/N \cong H$, where H is one of the identified groups of order 32, then G does not admit (288, 42, 6) difference sets. Part of the work in this section provides an example that illustrates the non-existence of (v, k, λ) in groups that are isomorphic to C_{32} or D_{16}.

4.1. The C_2 image

Suppose $G/N \cong C_2 = \langle x : x^2 = 1\rangle$ and $\hat{D} = \sum_{j=0}^{1} d_j x^j$ is the difference set image in G/N. Then the unique element of Ω_{C_2} is $A = 24 + 18x$.

4.2. Images on groups of order 4

We obtain the (288, 42, 6) difference sets images in the two groups of order 4.

4.2.1. The C_4 images

Suppose $G/N \cong C_4 = \langle x : x^4 = 1\rangle$ and the difference set image in G/N is $\hat{D} = \sum_{j=0}^{3} d_j x^j$. We view this group ring element as a 1×4 matrix with columns indexed by powers of x. The rational idempotents of G/N are $[e_{\chi_0}] = \frac{1}{4}\langle x\rangle$; $[e_{\chi_2}] = \frac{1}{4}(2\langle x^2\rangle - \langle x\rangle)$; $[e_{\chi_1}] = \frac{1}{2}(2 - \langle x^2\rangle)$. The first two rational idempotents have $\langle x^2\rangle$ in their kernel and the linear combination of these idempotents is written as $\alpha_{\chi_0}[e_{\chi_0}]+\alpha_{\chi_2}[e_{\chi_2}] = A\frac{\langle x^2\rangle}{2}$, where A is the difference set image in C_2. As $\chi_1(\hat{D})(\overline{\chi_1(\hat{D})}) = 36 = (6)(6)$, the difference set image is

$$\hat{D} = A\frac{\langle x^2\rangle}{2} \pm 6x^j[e_{\chi_1}], \tag{8}$$

$j = 0, 1, 2, 3$. By translating if necessary, the distribution scheme, Ω_{C_4} for C_4 (up to translation) consists of $A_1 = -6 + 12\langle x\rangle$ and $A_2 = 6 + 9\langle x\rangle$.

4.2.2. The $(C_2)^2$ images

It can be shown that if $G/N \cong (C_2)^2 = \langle x, y : x^2 = y^2 = [x, y] = 1\rangle$ and the difference set image in G/N is $\hat{D} = \sum_{s,t=0}^{1} d_{st}x^s y^t$, then the elements of $\Omega_{(C_2)^2}$, up to translation, are $12\langle x\rangle\langle y\rangle - 6$ and $9\langle x\rangle\langle y\rangle + 6$.

4.3. Images of groups of order 8

We obtain the (288, 42, 6) difference set images in four of the five groups of order 8.

4.3.1. The C_8 images

Suppose $G/N \cong C_8 = \langle x : x^8 = 1\rangle$ and $\hat{D} = \sum_{j=0}^{7} d_j x^j$ is the (288, 42, 6) difference set image in G/N. We view this group ring element as a 1×8 matrix with columns indexed by powers of x. The characters of G/N are of the form $\chi_j(x) = \zeta^j$, $j = 0, \cdots, 7$, where ζ is the eighth root of unity. The four rational idempotents of G/N are: $[e_{\chi_0}] = \frac{1}{8}\langle x\rangle$, $[e_{\chi_4}] = \frac{1}{8}(2\langle x^2\rangle - \langle x\rangle)$, $[e_{\chi_2}] = \frac{1}{4}(2\langle x^4\rangle - \langle x^2\rangle)$, and $[e_{\chi_1}] = \frac{1}{2}(2 - \langle x^4\rangle)$.
The linear combination of the three rational idempotents which have $\langle x^4\rangle$ in their kernel is written as $\sum_{j=0,2,4}\alpha_{\chi_j}[e_{\chi_j}] = \frac{A_k}{2}\langle x^4\rangle$, where $A_k, k = 1, 2$ is a difference set in C_4.

Thus, the difference set image in C_8 is

$$\hat{D} = \frac{A_k}{2}\langle x^4\rangle + \alpha_{\chi_1}[e_{\chi_1}], \tag{9}$$

where $\alpha_{\chi_1} \in \{\pm 6x^s, \pm 2(-1 - 2x - 2x^3)x^t, \pm 2(-1 + 2x + 2x^3)x^u\}, s, t, u = 0, \ldots, 7$. If D is a solution (9) so does gD for an group element $g \in G/N$. Hence, we use only the first two aliases. Define:

$Z_1 = 6[e_{\chi_1}] = 3(1 - x^4)$, $Z_2 = 2(-1 + 2x + 2x^3)[e_{\chi_1}] = (-1 + 2x + 2x^3)(1 - x^4)$. Thus, (9) becomes $\hat{D} = \frac{A_k}{2}\langle x^4\rangle \pm x^j Z_l, j = 0, 1, 2, 3, l, k = 1, 2$. The fact that $8Z_l \equiv 0 \mod 8$ forces $k = 1$. Up to equivalence, the elements of Ω_{C_8} are

$$\begin{aligned}
B_1 =& -6 + 6\langle x\rangle,\\
B_2 =& 3\langle x\rangle + 3x(2 + x + x^2 + x^5 + x^6)\\
B_3 =& 3\langle x\rangle + 3x(1 + 2x + x^2 + x^4 + x^6)\\
B_4 =& 2 + 8x + 6x^2 + 8x^3 + 4x^4 + 4x^5 + 6x^6 + 4x^7
\end{aligned}$$

$$B_5 = 1 + 5x + 8x^2 + 6x^3 + 5x^4 + 7x^5 + 4x^6 + 6x^7$$
$$B_6 = 3 + 4x + 5x^2 + 8x^3 + 3x^4 + 8x^5 + 7x^6 + 4x^7$$

4.3.2. The D_4 images

We use the Dillon dihedral technique trick to obtain the difference set image in $G/N \cong D_4 = \langle \theta, y : \theta^4 = y^2 = 1, y\theta y = \theta^{-1}\theta \rangle$. Take $\hat{D} = \sum_{s=0}^{3}\sum_{t=0}^{1} d_{st}\theta^s y^t$ to the (288, 42, 6) difference set image in G/N. We view this group ring element as a 2×4 matrix with columns indexed by powers of θ and rows indexed by y. To use the $C_8 = \langle x : x^8 = 1 \rangle$ difference set images, set $\theta = x^2$ and $y = x$. This transformation enables us to view each $B_j, j = 1, \dots, 6$ as a 2×4 matrix. For instance, B_2 becomes $B_2' = 3 + 6\theta + 3\theta^2 + 6\theta^3 + (9 + 6\theta + 3\theta^2 + 6\theta^3)y$.

Furthermore, $G/N \cong D_4$ has one degree two representation and four characters. The degree two representation is

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

where i is the fourth root of unity. We apply this representation to each transformed difference set image $B_j', j = 1, \dots, 6$ and verify whether or not $\chi(B_j')\overline{\chi(B_j')} = 36I_2, I_2$ is a 2×2 identity matrix. For example,

$$\chi(B_2') = \begin{pmatrix} 3 + 6i + 3i^2 + 6i^3 & 9 + 6i + 3i^2 + 6i^3 \\ 9 + 6i^3 + 3i^2 + 6i & 3 + 6i^3 + 3i^2 + 6i \end{pmatrix} = \begin{pmatrix} 0 & 6 \\ 6 & 0 \end{pmatrix}.$$

Notice that $\chi(B_2')\overline{\chi(B_2')} = 36I_2$. Hence, the elements of Ω_{D_4} are $B_1' = -6 + 6\langle\theta\rangle\langle y\rangle$, $B_2' = -3(1 + \theta^2) + 6\langle\theta\rangle\langle y\rangle + 3(1 - \theta^2)y$ and $B_3' = 3\theta + 3\langle\theta\rangle + 6\langle\theta\rangle y$.

4.3.3. The $C_4 \times C_2$ images

Consider $G/N \cong C_4 \times C_2 = \langle x, y : x^4 = y^2 = 1 = [x, y]\rangle$. Let $\hat{D} = \sum_{s=0}^{3}\sum_{t=0}^{1} d_{st}x^s y^t$ be the (288, 42, 6) difference set image in G/N. We view this group ring element as a 2×4 matrix with columns indexed by powers of x and rows indexed by y. As G/N is of the form (5), $\alpha = 12$ or 9. Wlog, take $\alpha = 12$, $K = C_4$ and $B_s = A_s - 12K$, where $A_s, s = 1, 2$ is an element of Ω_{C_4}. Then by (6), the difference set image is

$$\hat{D} = A_s\left(\frac{\langle y\rangle}{2}\right) + gB_s\left(\frac{2 - \langle y\rangle}{2}\right), \tag{10}$$

$g \in C_4 \times C_2$, $B_1 = 3 - 3y$ and $B_2 = \frac{1}{2}(6 - 3\langle x\rangle)(1 - y)$. Up to equivalence, the difference set image in $C_4 \times C_2$ are $B_4' = -6 + 6\langle x\rangle\langle y\rangle$, $B_5' = 6 + 6\langle x\rangle\langle y\rangle - 3\langle x\rangle$, $B_6' = 3 + 3x + 6x^2 + 6x^3 + (3 + 9x + 6x^2 + 6x^3)y$ and $B_7' = 6 + 6x + 3x^2 + 3x^3 + (9 + 3x + 6x^2 + 6x^3)y$.

4.3.4. The $(C_2)^3$ images

Consider $G/N \cong (C_2)^3 = \langle x, y, z : x^2 = y^2 = z^2 = 1 = [x, y] = [x, z] = [z, y]\rangle$. The (288, 42, 6) difference set image in this group are $B_8' = -6 + 6(1 + x)(1 + y)(1 + z)$, $B_9' = 3 + 6(1 + x)(1 + y)(1 + z) - 3(x + y + xz)$.

4.4. Images on some groups of order 16

We obtain the (288, 42, 6) difference set images in some groups of order 16.

4.4.1. The C_{16} image

Suppose that $G/N \cong C_{16} = \langle x : x^{16} = 1\rangle$ and the difference set in G/N is $\hat{D} = \sum_{j=0}^{15} d_j x^j$. Out of the five rational idempotents of G/N, only $[e_{\chi_1}] = \frac{2-\langle x^8\rangle}{2}$ do not have $\langle x^8\rangle$ in its kernel. The linear combination of rational idempotents having $\langle x^8\rangle$ in their kernel is written as $\sum_{j=0,2,4,8} \alpha_{e_{\chi_j}}[e_{e_{\chi_j}}] = B_j\left(\frac{\langle x^8\rangle}{2}\right)$, where B_j is a difference set image in C_8.

Thus, the difference set image in G/N is

$$\hat{D} = B_j\left(\frac{\langle x^8\rangle}{2}\right) + \alpha_{e_{\chi_1}}[e_{e_{\chi_1}}], \tag{11}$$

where $\alpha_{e_{\chi_1}} \in \{\pm 6x^u, \pm 2(-1+2x^2+2x^6)x^t, \pm 2(-1-2x^2-2x^6)x^r\}$, $r, t, u = 0, \ldots, 15$. Define $Z_1 = 6 \cdot [e_{\chi_1}] = 3(1-x^8)$ and $Z_2 = 2(-1+2x^2+2x^6)[e_{\chi_1}] = -1+2x^2+2x^6+x^8-2x^{10}-2x^{14}$. We now rewrite (11) as $\hat{D} = B_j\left(\frac{\langle x^8\rangle}{2}\right) + x^l Z_k, k = 1, 2; l = 0, \cdots, 15; j = 1, \ldots, 6$. Since $16Z_k \equiv 0 \mod 16$, a solution exists if and only if $16B_j\left(\frac{\langle x^8\rangle}{2}\right) \equiv 0 \mod 16$. This condition is satisfied by $B_j, j = 1, 4$. Up to equivalence, the C_{16} images are:

$$
\begin{aligned}
F_1 =& 6x+3x^2+3x^3+3x^4+3x^5+3x^6+3x^7+3x^{10}+3x^{11}+3x^{12}+3x^{13}+3x^{14}+3x^{15}\\
F_2 =& 1+7x+3x^2+4x^3+2x^4+2x^5+3x^6+2x^7+x^8+x^9+3x^{10}+4x^{11}+2x^{12}+2x^{13}\\
&+3x^{14}+2x^{15}\\
F_3 =& 1+4x+6x^2+4x^3+2x^4+2x^5+3x^6+2x^7+x^8+4x^9+4x^{11}+2x^{12}+2x^{13}+3x^{14}\\
&+x^{15}\\
F_4 =& 2x+3x^2+5x^3+3x^4+3x^5+3x^6+5x^7+4x^9+3x^{10}+x^{11}+3x^{12}+3x^{13}+3x^{14}+x^{15}\\
F_5 =& x+3x^2+3x^4+5x^5+3x^6+3x^7+5x^9+3x^{10}+4x^{11}+3x^{12}+x^{13}+3x^{14}+3x^{15}\\
F_6 =& 4x+5x^2+4x^3+2x^4+2x^5+5x^6+2x^7+2x^8+4x^9+x^{10}+4x^{11}+2x^{12}+2x^{13}\\
&+x^{14}+2x^{15}\\
F_7 =& 1+3x+3x^2+6x^3+2x^4+2x^5+3x^6+4x^7+x^8+5x^9+3x^{10}+2x^{11}+2x^{12}+2x^{13}+3x^{14}\\
F_8 =& 1+4x+x^2+4x^3+x^4+2x^5+5x^6+2x^7+x^8+4x^9+5x^{10}+4x^{11}+3x^{12}+2x^{13}+x^{14}\\
&+2x^{15}\\
F_9 =& 1+4x+3x^2+2x^3+2x^4+x^5+3x^6+4x^7+x^8+4x^9+3x^{10}+6x^{11}+2x^{12}+3x^{13}+3x^{14}
\end{aligned}
$$

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

4.4.2. The D_8 image

Consider the factor group $G/N \cong D_8 = \langle x, y : x^8 = y^2 = 1, yxy = x^{-1}\rangle$ and let $\hat{D} = \sum_{s=0}^{7}\sum_{t=0}^{1} d_{st}x^s y^t$ be its difference set image. By the Dillon technique and up to equivalence, $\hat{D}$ is one of the following:

$$\begin{aligned}
F_1' =&(3x + 3x^2 + 3x^3 + 3x^5 + 3x^6 + 3x^7)\\
&+ (6 + 3x + 3x^2 + 3x^3 + 3x^4 + 3x^5 + 3x^6 + 3x^7)y\\
F_2' =&(3x + 3x^2 + 3x^3 + 3x^5 + 3x^6 + 3x^7)\\
&+ (2 + 5x + 3x^2 + 5x^3 + 4x^4 + x^5 + 3x^6 + x^7)y\\
F_3' =&(3x + 3x^2 + 3x^3 + 3x^5 + 3x^6 + 3x^7)\\
&+ (1 + 2x + 5x^2 + 3x^3 + 5x^4 + 4x^5 + x^6 + 3x^7)y\\
F_4' =&(3x + 3x^2 + 3x^3 + 3x^5 + 3x^6 + 3x^7)\\
&+ (3 + x + 2x^2 + 5x^3 + 3x^4 + 5x^5 + 4x^6 + x^7)y\\
F_5' =&(x + 2x^2 + 5x^3 + 5x^5 + 4x^6 + x^7)\\
&+ (3 + 3x + 3x^2 + 3x^3 + 3x^4 + 3x^5 + 3x^6 + 3x^7)y\\
F_6' =&(3x + 6x^2 + 3x^3 + 3x^5 + 3x^7) + (3 + 3x + 3x^2 + 3x^3 + 3x^4 + 3x^5 + 3x^6 + 3x^7)y\\
F_7' =&(6x + 3x^2 + 3x^3 + 3x^6 + 3x^7) + (3 + 3x + 3x^2 + 3x^3 + 3x^4 + 3x^5 + 3x^6 + 3x^7)y
\end{aligned}$$

Notice that the D_8 difference set images are either of the form $0^3 3^{12} 6^1$ or $0^2 1^2 2^1 3^8 4^1 5^2$. The notation $0^3 3^{12} 6^1$ means the intersection number 0 occurs three times, intersection number 3 occurs twelve times while intersection number 6 occurs once. This information will be used to show that $G/N \cong D_8 \times C_2$ does not admit (288, 42, 6) difference sets.

4.4.3. The $(C_4 \times C_2) \rtimes C_2$ images

Consider $G/N \cong (C_4 \times C_2) \rtimes C_2 = \langle x, y, z : x^4 = y^2 = z^2 = 1 = [x, y] = [x, z], yz = zx^2y\rangle$ with GAP[5] location number [16, 13]. The derived subgroup of G/N is $(G/N)' = \{1, x^2\}$ and the center of G/N, $C(G/N) = \langle x\rangle \cong C_4$. Suppose that the difference set image in G/N is $\hat{D} = \sum_{i=0}^{3}\sum_{i=0}^{1}\sum_{i=0}^{1} d_{ijk}x^i y^j z^k$. We view this group ring element in array form as:

$$\hat{D} = \begin{bmatrix} d_{000} & d_{100} & d_{200} & d_{300} & d_{010} & d_{110} & d_{210} & d_{310} \\ d_{001} & d_{101} & d_{201} & d_{301} & d_{011} & d_{111} & d_{211} & d_{311} \end{bmatrix}.$$

Since $(G/N)/(G/N)' \cong (C_2)^3 = \langle x, y, z : x^2 = y^2 = z^2 = [x, y] = [y, z] = [x, z]\rangle$, the projection map $x^2 \mapsto 1$ produces the following system of equations:

$$\sum_{s,t=0}^{1}(d_{s,t0} + d_{s+2,t0}) = c_{st0}, \sum_{s,t=0}^{1}(d_{s,t1} + d_{s+2,t1}) = c_{st1}, \tag{12}$$

where the array $(c_{000}, c_{100}, c_{010}, c_{110}, c_{001}, c_{101}, c_{011}, c_{111})$ is a difference set image in $(C_2)^3$. Furthermore, the degree two representation of G/N is:

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

where i is the fourth root of unity. The image of $\hat{D}$ under this representation is $\chi(\hat{D}) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, with

$$\begin{aligned} a &= (a_0 + a_2) + (a_1 + a_3)i, \\ b &= (b_0 + b_2) + (b_1 + b_3)i, \\ c &= (b_0 - b_2) + (b_1 - b_3)i, \\ d &= (a_0 - a_2) + (a_1 - a_3)i, \end{aligned}$$

where

$$\begin{aligned} &a_0 = d_{000} - d_{200}, \quad a_1 = d_{100} - d_{300}, \quad a_2 = d_{001} - d_{201}, \quad a_3 = d_{101} - d_{301}, \\ &b_0 = d_{010} - d_{210}, \quad b_1 = d_{110} - d_{310}, \quad b_2 = d_{011} - d_{211}, \quad b_3 = d_{111} - d_{311}. \end{aligned}$$

Hence, $\chi(\hat{D})\overline{\chi(\hat{D})} = \begin{pmatrix} a\bar{a} + b\bar{b} & a\bar{c} + b\bar{d} \\ c\bar{a} + d\bar{b} & c\bar{c} + d\bar{d} \end{pmatrix}$, where

$$\begin{aligned} a\bar{a} + b\bar{b} &= a_0^2 + a_2^2 + 2a_0a_2 + a_1^2 + a_3^2 + 2a_1a_3 + b_0^2 + b_2^2 + 2b_0b_2 + b_1^2 + b_3^2 + 2b_1b_3, \\ c\bar{c} + d\bar{d} &= a_0^2 + a_2^2 - 2a_0a_2 + a_1^2 + a_3^2 - 2a_1a_3 + b_0^2 + b_2^2 - 2b_0b_2 + b_1^2 + b_3^2 - 2b_1b_3, \\ a\bar{c} + b\bar{d} &= 2(a_0b_0 - a_2b_2 + a_1b_1 - a_3b_3 - a_2b_1i + a_3b_0i - a_1b_2i + a_0b_3i), \\ c\bar{a} + d\bar{b} &= 2(a_0b_0 - a_2b_2 + a_1b_1 - a_3b_3 - a_2b_1i - a_0b_3i + a_1b_2i - a_3b_0i). \end{aligned}$$

As we require $\chi(\hat{D})\overline{\chi(\hat{D})} = 36I_2$, where I_2 is a 2×2 identity matrix, it follows that

$$a\bar{a} + b\bar{b} = 36, \quad c\bar{c} + d\bar{d} = 36, \quad c\bar{a} + d\bar{b} = 0, \quad c\bar{a} + d\bar{b} = 0.$$

The sum of equations $a\bar{a} + b\bar{b} = 36$ and $c\bar{c} + d\bar{d} = 36$ yields

$$a_0^2 + a_2^2 + a_1^2 + a_3^2 + b_0^2 + b_2^2 + b_1^2 + b_3^2 = 36 \tag{13}$$

$$a_0a_2 + a_1a_3 + b_0b_2 + b_1b_3 = 0, \tag{14}$$

while $c\bar{a} + d\bar{b} = 0$ or $c\bar{a} + d\bar{b} = 0$ implies

$$a_0b_0 - a_2b_2 + a_1b_1 - a_3b_3 = 0 \tag{15}$$

$$-a_2b_1 - a_0b_3 + a_1b_2 - a_3b_0 = 0. \tag{16}$$

The solution set of (13) is some permutation of the entries of the row 1 through 6 of the following tables:

1	±6	0	0	0	0	0	0	0
2	±5	±3	±2	±1	0	0	0	0
3	±4	±4	±2	0	0	0	0	0

,

4	±4	±4	±1	±1	±1	±1	0	0
5	±3	±3	±3	±3	0	0	0	0
6	±3	±3	±2	±2	±2	±2	±1	±1

There are 1248 possible solutions to (13)-(16). To get difference set images, we need to solve (12)-(16). Recall that (13) involves the array $(c_{000}, c_{100}, c_{010}, c_{110}, c_{001}, c_{101}, c_{011}, c_{111})$, which is a difference set image in $(C_2)^3$. The difference set images in $(C_2)^3$ are either of the form $0^1 6^7$ in which all intersection numbers are even or $3^3 6^4 9^1$ in which half of the intersection numbers are even and the rest are odd integers. Due to the nature of (13) and (14), only solutions arising from rows 1 and 3 of the above tables are comparable with $0^1 6^7$ while the rest are compatible with $3^3 6^4 9^1$. Interestingly, it turns out that any putative difference set image in G/N has one of the distributions $0^3 3^{12} 6^1$, $0^2 1^2 2^1 3^8 4^1 5^2$ or $0^1 1^2 2^3 3^9 7^1$. This is the only vital information required to establish the non-existence of difference set images in $((C_4 \times C_2) \rtimes C_2) \times C_2[32, 48]$.

4.4.4. The structure of difference set images in some groups of order 16

Suppose that G/N is isomorphic to some groups of order 16, apart from C_{16} and D_8. Recall that the difference set images in $G/N \cong C_4 \times C_2$, $(C_2)^3$ or D_4 satisfy $B'_j \equiv 0 \mod 3$. Let E be an elementary abelian subgroup of $C(G/N)$ such that $|E| = 2^2$. Consider the sequence $\{E_i\}$, where E_i is a subgroup of E of order 2. Suppose that for each i, $(G/N)/E_i$ is isomorphic to one of $C_4 \times C_2$, $(C_2)^3$ or D_4. Then by Theorem 5, the difference set image $\hat{D}$ in G/N satisfies $\hat{D} \equiv 0 \mod 3$. The groups of order 16 that satisfy this stipulation are: $C_4 \times C_4([16, 2])$, $(C_4 \times C_2) \rtimes C_2([16\ 3])$, $C_4 \times (C_2)^2([16, 10])$, $D_4 \times C_2([16, 11])$ and $(C_2)^4([16, 14])$, where $[|G/N|, \mathrm{cn}]$ is the GAP library number.

4.5. Non-existence of difference set images in some groups of order 32

We now show that there are no (288, 42, 6) difference set images in some groups of order 32.

4.5.1. There are no C_{32} and D_{16} images

Suppose that $\hat{D} = \sum_{i=0}^{31} d_i x^i$ is the difference set image in $G/N \cong C_{32} = \langle x : x^{32} = 1\rangle$. Out of the six rational idempotents of G/N, only $[e_{\chi_1}] = \frac{2-\langle x^{16}\rangle}{2}$ does not have $\langle x^{16}\rangle$ in its kernel. The linear combination of the remaining five rational idempotents can be written as $\sum_{j=0,2,4,8,16} \alpha_{e_{\chi_j}} [e_{e_{\chi_j}}] = F_k\big(\frac{\langle x^{16}\rangle}{2}\big)$, where $\alpha_{e_{\chi_j}}$ is an alias and $F_k, k = 1, \ldots, 13$, is a difference set image in C_{16}. The difference set image is

$$\hat{D} = F_k\left(\frac{\langle x^{16}\rangle}{2}\right) + \alpha_{e_{\chi_1}} [e_{e_{\chi_1}}], \tag{17}$$

where $\alpha_{e_{\chi_1}} \in \{\pm 6x^s, \pm 2(-1+2x^4+2x^{12})x^t, \pm 2(-1-2x^4-2x^{16})x^u\}$. We only have to use aliases 6 and $-1+2x^4+2x^{12}$. Define $Z_1 = 6\cdot[e_{\chi_1}] = 3(1-x^{16})$ and $Z_2 = 2(-1+2x^4+2x^{12})[e_{\chi_1}] = -1+2x^4+2x^{12}+x^{16}-2x^{20}-2x^{24}$. We can now rewrite (17) as $\hat{D} = F_k\left(\frac{\langle x^{16}\rangle}{2}\right) + x^s Z_l, l = 1,2; s = 0,\cdots,15$. The fact that $32Z_l \equiv 0$ mod 32 requires $32F_k\left(\frac{\langle x^{16}\rangle}{2}\right) \equiv 0 \mod 32$. However, there is no F_k in $\Omega_{C_{16}}$ such that $32F_k\left(\frac{\langle x^{16}\rangle}{2}\right) \equiv 0 \mod 32$. Thus, C_{32} and D_{16} (by the Dillon dihedral trick) do not admit a (288, 42, 6) difference set.

4.5.2. There are (288, 42, 6) difference set images in $D_8 \times C_2$ and $((C_4 \times C_2) \rtimes C_2) \times C_2$[32, 48]

Suppose that $G/N \cong K \times C_2$, where $K = D_8$ or $(C_4 \times C_2) \rtimes C_2$ and z is the generator of C_2. Put $\alpha = 3$, $|K| = 16$. Then using (6), the difference set image in G/N is of the form

$$\hat{D} = A_s\left(\frac{\langle z\rangle}{2}\right) + gB_s\left(\frac{2-\langle z\rangle}{2}\right), \tag{18}$$

$g \in G/N$, $B_s = A_j - 3K$ and A_j or A_s is a difference set image in K with distributions $0^3 3^{12} 6^1$, $0^2 1^2 2^1 3^8 4^1 5^2$ or $0^1 1^2 2^3 3^9 7^1$. In view of these distributions, $A_s\left(\frac{\langle z\rangle}{2}\right)$ consists of 24 fractions and 8 integers while $B_s\left(\frac{2-\langle z\rangle}{2}\right)$ consists of 8 fractions and 24 integers. Since the intersection numbers must be non negative integers, the two terms on the right-hand side of (18) are not compatible and hence, the equation has no integer solutions.

4.5.3. No difference set images in some factor groups of order 32

Suppose that $G/N \cong H$, where H is a group of order 32 satisfying the conditions of Theorem 5 with $p = 3$, $q = 2$ and $|C(H)| \geq 4$. Suppose that the difference set image exists in H and is $\hat{D}$. Take E to be a subgroup of $C(H)$ of order 4 and E_i is a subgroup of E such that H/E_i is isomorphic to one of the five groups of order 16 listed in subsection 4.4.4. Theorem 5 requires $\hat{D}$ satisfying $\hat{D} \equiv 0 \pmod 3$. This condition is verified using a variance technique with $|N| = 9$. Suppose that $\hat{D} \equiv 0 \pmod 3$. Then the intersection numbers in $\hat{D}$ could be 0, 3, 6 or 9. Thus by Lemma 2, we have

$$m_0 + m_3 + m_6 + m_9 = 32 \tag{19}$$

$$3m_3 + 6m_6 + 9m_9 = 42 \tag{20}$$

$$6m_3 + 30m_6 + 72m_9 = 48 \tag{21}$$

The coefficient of m_9 in (21) is 72 which is greater than 48. Thus, m_9 must be zero and the unique solution of the system of equations is $(m_0, m_3, m_6, m_9) = (16, 18, -2, 0)$. This solution involves a negative integer which is not admissible as $m_j \geq 0$. This shows that $\hat{D} \not\equiv 0 \pmod 3$ and this violation implies there is no difference set image in H. An exploration by GAP reveals that H is one of $(C_4 \times C_2) \rtimes C_4$([32, 2]), $(C_4)^2 \times C_2$([32, 21]), $D_4 \times (C_2)^2$([32, 46]), $((C_4 \times C_2) \rtimes C_2) \rtimes C_2$([32, 22]),

$((C_4\times C_2)\rtimes C_2)\rtimes C_2([32, 48])$, $(C_4\times (C_2)^3([32, 45])$, $(C_2)^5([32, 51])$, $(C_2)^4\rtimes C_2([32, 27])$ or $(C_4\times C_4)\rtimes C_2([32, 34])$. This work shows that 170 groups of the 1045 groups of order 288 do not admit (288, 42, 6) difference sets. In the GAP library, these groups are $[288, cn]$, cn =1, 2, 6, 33, 38, 45, 61, 64, 65, 66, 81, 84, 90, 92, 114, 120, 132, 137, 142, 147, 150, 162, 163, 164, 165, 170, 177, 182, 188, 193, 194, 227, 233, 260, 265, 274, 301, 306, 313, 329, 353, 354, 355, 356, 357, 360, 362, 365, 366, 367, 368, 370, 373, 382, 385, 395, 429, 441, 445, 469, 472, 523, 530, 559, 562, 568, 569, 570, 571, 572, 574, 602, 608, 611, 616, 622, 624, 625, 627, 629, 631, 642, 645, 651, 653, 674, 681, 693, 698, 702, 708, 711, 723, 724, 728, 731, 737, 739, 760, 767, 779, 784, 788, 794, 797, 809, 810, 811, 812, 817, 824, 829, 839, 840, 873, 879, 880, 883, 889, 932, 941, 943, 944, 948, 949, 950, 951, 952, 953, 954, 958, 959, 960, 966, 967, 969, 970, 971, 972, 973, 974, 976, 977, 989, 990, 991, 992, 993, 996, 998, 1001, 1002, 1004, 1005, 1006, 1007, 1008, 1011, 1013, 1016, 1017, 1018, 1019, 1021, 1031, 1039, 1040, 1043, 1044, 1045.

5. List of some parameter sets satisfying conjecture 1

The lower bound for Conjecture 1 is $s = 4$. Parameters that meet this bound for $a < 100$ and $k < 6500$ are listed in Table 3. By hand verification, the other parameter sets that are ruled out are listed in Tables 4, 7, 8, 9 and 10. However, for $s = 1$, $s = 2$ and $s = 3$ the largest 2-group is isomorphic to C_2, C_4 and C_8, respectively, and the difference set images exist in these groups. These parameters are listed in Tables 1, 2 and 5, respectively.

	v	k	λ	n
1	36	15	6	9
2	100	45	20	25
3	156	31	6	25
4	196	91	42	49
5	204	29	4	25
6	220	73	24	49
7	260	112	48	64
8	276	100	36	64
9	300	92	28	64
10	324	153	72	81
11	364	243	162	81
12	396	80	16	64

Table 1: *Parameters with $s = 2$, $a < 100$ and $k < 6500$*

	v	k	λ	n
1	40	13	4	9
2	56	11	2	9
3	120	35	10	25
4	280	63	14	49
5	408	111	30	81
6	456	105	24	81
7	616	165	44	121
8	760	253	84	169

Table 2: *Parameters with $s = 3$, $a < 100$ and $k < 6500$*

	v	k	λ	n
1	16	6	2	4
2	144	66	30	36
3	176	50	14	36
4	208	46	10	36
5	400	190	90	100
6	560	130	30	100
7	784	378	182	196
8	816	326	130	196
9	880	294	98	196
10	1008	266	70	196
11	1200	110	10	100
12	1296	630	306	324
13	1456	486	162	324

Table 3: *Parameters with* $s = 4$, $a < 100$ *and* $k < 6500$

	v	k	λ	n
1	96	20	4	16
2	160	54	18	36
3	288	42	6	36
4	416	166	66	100
5	672	122	22	100
6	736	196	52	144
7	800	188	44	144
8	1632	700	300	400
9	1696	226	30	196
10	1888	222	26	196
11	2016	156	12	144
12	2016	806	322	484
13	2080	540	140	400
14	2784	484	84	400
15	2912	1066	390	676
16	2976	476	76	400
17	3040	1014	338	676

Table 4: *Parameters with* $s = 5$, $a < 100$ *and* $k < 6500$ *satisfying Conjecture 1*

	v	k	λ	n
1	66	26	10	16
2	70	24	8	16
3	78	22	6	16
4	154	18	2	16

Table 5: *Parameters with* $s = 1$, $a <$ 100 *and* $k < 6500$

	v	k	λ	n	m	r
1	16	6	2	4	4	1
2	64	28	12	16	6	2
3	256	120	56	64	8	3
4	1024	496	240	256	10	4
5	4096	2016	992	1024	12	5
6	16384	8128	4032	4096	14	6

Table 6: *Menon-MacFaland-Hadamard Parameters set with* $s = 1$

	v	k	λ	n
1	320	88	24	64
2	448	150	50	100
3	576	276	132	144
4	704	38	2	36
5	960	274	78	196
6	1344	238	42	196
7	1600	780	380	400
8	1728	628	228	400
9	1856	106	6	100
10	2496	500	100	400
11	3008	776	200	576
12	3136	210	14	196
13	3136	760	184	576
14	3136	1540	756	784
15	3520	460	60	400
16	4032	696	120	576
17	4544	826	150	676
18	5184	2556	1260	1296
19	5440	148	4	144
20	5440	1666	510	1156
21	5568	2052	756	1296
22	5824	648	72	576
23	6336	1086	186	900

Table 7: *Parameters with* $s = 6$, $a < 100$ *and* $k < 6500$

	v	k	λ	n
1	640	72	8	64
2	896	180	36	144
3	1408	336	80	256
4	1920	304	48	256
5	2176	726	242	484
6	2432	936	360	576
7	3200	1372	588	784
8	4224	206	10	196
9	4992	806	130	676
10	5248	2332	1036	1296
11	6016	2406	962	1444
12	6528	428	28	400
13	6784	2584	984	1600
14	8064	2200	600	1600
15	8320	2538	774	1764
16	9088	2796	860	1936
17	9856	730	54	676
18	10368	2962	846	2116
19	10880	990	90	900
20	10880	3312	1008	2304
21	11136	1310	154	1156
22	11648	2452	516	1936
23	12160	3088	784	2304
24	12416	3056	752	2304

Table 8: *Parameters with* $s = 7$, $a < 100$ *and* $k < 6500$

	v	k	λ	n
1	1680	438	114	324
2	1776	426	102	324
3	2640	378	54	324
4	3440	362	38	324
5	3760	358	34	324
6	6480	342	18	324
7	18096	330	6	324
8	52976	326	2	324
9	40704	404	4	400
10	14112	412	12	400
11	8800	420	20	400
12	117856	486	2	484
13	17680	498	14	484
14	11616	506	22	484
15	6576	526	42	484
16	6096	530	46	484
17	4576	550	66	484
18	2800	2622	138	484
19	2640	638	154	484
20	2016	806	322	484
21	1936	946	462	484
22	14976	600	24	576
23	42560	584	8	576

Table 9: *More parameters with* $n = k - \lambda = (2^r b^t)^2$, $2^r b^t = 18, 20, 22, 24$ *satisfying Conjecture 1*

	v	k	λ	n	m
1	768	118	18	100	8
2	2304	1128	552	576	8
3	2816	1126	450	676	8
4	5376	1376	352	1024	8
5	6400	3160	1560	1600	8
6	7936	2646	882	1784	8
7	8960	868	84	784	8
8	9472	616	40	576	8
9	12544	6216	3080	3136	8
10	13056	1120	96	1024	8
11	14080	1444	148	1296	8
12	14080	3250	750	2500	8
13	20736	2640	336	2304	8
14	20736	3510	594	2916	8
15	23808	3402	486	2916	8
16	52480	5832	648	5184	8
17	4608	272	16	256	9
18	13824	4808	1672	3136	9
19	16896	3380	676	2704	9
20	17720	6336	2240	4096	9
21	19968	3896	760	3136	9
22	22016	5440	1344	4096	9
23	29184	4928	832	4096	9
24	50688	3900	300	3600	9
25	9216	4560	2256	2304	10
26	31744	3528	392	3136	10
27	37888	4672	576	4096	10
28	39936	490	6	484	10
29	46080	4544	448	4096	10
30	26624	5056	960	4096	11
31	34816	1056	32	1024	11
32	169984	5050	150	4900	11
33	270336	4160	64	4096	13

Table 10: *More parameters with* $8 \leq s \leq 15$, $a < 100$ *and* $k < 6500$ *in Conjecture 1*

Acknowledgment

The author would like to thank the anonymous referee for the invaluable suggestions.

References

[1] K. T. Arasu, *On Lander's Conjecture for the case* $\lambda = 3$. J. Combin. Math. and Combin. Computing **1**(1987), 5–11.

[2] K. T. Arasu, *Validity of Lander's Conjecture for* $\lambda = 3$ *and* $k \leq 500$, J. Combin. Math. and Combin. Computing **2**(1987), 73–76.

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

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

[5] *GAP-Groups, Algorithms and Programming, Version 4. 4. 6*(2006), Retrieved on June 20, 2008 from `http://www.gap.gap-system.org`.

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

[7] D. R. Hughes, *On biplanes and semibiplanes*, in: *Combin. Math*, (D. Holton and J. Seberry, Eds.), Springer Lecture Notes in Math. **686**, 1978, 55–58.

[8] J. E. Iiams, *Lander's tables are complete*, in: *Difference sets, Sequeneces and their Correlation properties* (A. Pott, P. V. Kumar, T. Helleseth, D. Jungnickel, Eds.), Kluwer Academic Publishers, 1999, 239–257.

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

[10] D. Jungnickel, A. Pott, K. W. Smith, *Difference sets*, in: *The CRC Handbook of Combinatorial Designs*, (C. J. Colbourn and J. H. Dinitz, Eds.), CRC Press, 2005, preprint.

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

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

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

[14] K. H. Leung, S. L. Ma, B. Schmidt, *Non-existence of abelian sets: Lander's conjecture for prime power orders,* American Mathematical Society **356**(2003), 43–58.

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

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

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

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

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