Turkish Journal of Mathematics

http://journals.tubitak.gov.tr/math/

Research Article

Turk J Math
(2013) 37: 375 – 390
© TÜBİTAK
doi:10.3906/mat-1106-9

On the existence of (400, 57, 8) non-abelian difference sets

Adegoke Solomon OSIFODUNRIN[*]
Department of Mathematics, Division of Sciences and Mathematics, Livingstone College, Salisbury,
NC 28144, USA

Received: 07.06.2011 • **Accepted:** 20.04.2012 • **Published Online:** 26.04.2013 • **Printed:** 27.05.2013

Abstract: Difference sets with parameters $\left(\frac{q^{d+1}-1}{q-1}, \frac{q^d-1}{q-1}, \frac{q^{d-1}-1}{q-1}\right)$, where q is a prime power and $d \geq 1$, are known to exist in cyclic groups and are called classical Singer difference sets. We study a special case of this family with $q = 7$ and $d = 3$ in search of more difference sets. According to GAP, there are 220 groups of order 400 out of which 10 are abelian. E. Kopilovich and other authors showed that the remaining nine abelian groups of order 400 do not admit (400, 57, 8) difference sets. Also, Gao and Wei used the (400, 57, 8) Singer difference set to construct four inequivalent difference sets in a non-abelian group. In this paper, we demonstrate using group representation and factorization in cyclotomic rings that, out of the remaining 209 non-abelian groups of order 400, only 15 could possibly admit (400, 57, 8) difference sets.

Key words: Representation, idempotents, Singer difference sets, intersection numbers

1. Introduction

Suppose that G is a multiplicative group of order v. A non-trivial (v, k, λ) difference set D is a subset of G consisting of k elements, where $1 < k < v - 1$, in which every non-identity element of G 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 type determines the kind of difference set. For instance, if G is abelian (resp. non-abelian or cyclic), then D is abelian (resp. non-abelian or cyclic) difference set. Singer difference sets with parameters (v, k, λ), where

$$v = \frac{q^{d+1}-1}{q-1}, \quad k = \frac{q^d-1}{q-1}, \quad \lambda = \frac{q^{d-1}-1}{q-1}, \tag{1.1}$$

q is a prime power and $d \geq 1$, are known to exist in cyclic groups and there exist corresponding symmetric designs with these parameters. Singer's conjecture is that there is only one equivalence class of difference set with parameters (1.1) when $\lambda = 1$ is still open [1]. Gao and Wei [3] used multipliers to construct non-abelian difference sets from the Singer difference sets. In particular, in the case $q = 7$ and $d = 3$ in (1.1), their construction produced four inequivalent difference sets in the group $G = C_{25} \rtimes C_{16} = \langle x, y : x^{25} = y^{16} = 1, yxy^{-1} = x^{-1}\rangle$. The existence or otherwise of (400, 57, 8) difference sets in 10 abelian groups of order 400 has been decided. Our focus in this paper is on the remaining 209 non-abelian groups but our approach incorporates both abelian

[*]Correspondence: asaosifodunrin@yahoo.com

2000 *AMS Mathematics Subject Classification:* 05B10.

and non-abelian groups. Our search for other non-isomorphic (400, 57, 8) difference sets yields the following main result.

Theorem 1.1 *There are no non-isomorphic Singer (400, 57, 8) difference sets in other groups of order 400 except possibly in [400, cn], where cn = 3, 49, 50, 52, 56, 57, 58, 59, 116, 132, 133, 206, 207, 212, 213.*

[400, *cn*], is the GAP[4] catalog number of these groups. In this paper, G represents a group of order 400 and N is a suitable normal subgroup of G such that G/N is isomorphic to a group of order 16, 20 or 40. Section 2 gives basic results while in sections 3 and 4 we establish the main result.

2. Preliminary results

We look at background materials.

2.1. Difference sets

$\mathbb{Z}$ and $\mathbb{C}$ denote ring of integers and field of complex numbers, respectively. Let G be a group of order v and D be a (v, k, λ) difference set in a group G. For convenience, we 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

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

If g is a non-identity element and α is an automorphism of G, then the left translates of D, gD, and right translates of D, Dg and $D^{\alpha} := \{\alpha(d) : d \in D\}$ are difference sets. If we take the left translates of D as blocks, then the resulting structure is called the development of D, $Dev(D)$ and G is the automorphism group of $Dev(D)$. Difference sets are often used in the construction of symmetric design in that symmetric design admitting a sharply transitive automorphism group G is isomorphic to the development of a difference set in G (Theorem 4.2 [8]). The existence of symmetric designs does not necessarily imply the existence of corresponding difference sets (see [5]). The only known (400, 57, 8) symmetric designs are those associated with Singer and Gao et al. difference sets.

Given 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 corresponding group rings. 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 $\psi(D)$, and denote the number of times d_i equals i by $m_i \geq 0$ and $\Omega_{G/N}$ is the set of inequivalent difference set images in G/N. Also, the phrase **group** $|G/N|$ denotes groups of order $|G/N|$. The following lemma is a necessary but not sufficient condition for the existence of difference set image in G/N.

Lemma 2.1 *(The Variance Technique). Suppose that G is a group of order v and N is a normal subgroup of G. Suppose that D is a difference set in G and its image in G/N is $\hat{D}$. Suppose also that 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 the number of times d_i equals i. Then*

$$\sum_{i=0}^{|N|} m_i = |G/N|; \sum_{i=0}^{|N|} im_i = k; \sum_{i=0}^{|N|} i(i-1)m_i = \lambda(|N|-1) \tag{2.2}$$

2.2. A little about 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'. 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 $G^*/\sim$. Suppose that G is a group with exponent m', then $K_{m'} := \mathbb{Q}(\zeta_{m'})$ is the cyclotomic extension of the field of rational numbers, $\mathbb{Q}$, where $\zeta_{m'} := e^{\frac{2\pi}{m'}i}$ is a primitive m'-th root of unity. Without loss of generality, we may replace $\mathbb{C}$ by the field $K_{m'}$. This field is a Galois extension of degree $\phi(m')$, where ϕ is the Euler function. If G is a cyclic group, then a basis for $K_{m'}$ over $\mathbb{Q}$ is $S = \{1, \zeta_{m'}, \zeta_{m'}^2, \ldots, \zeta_{m'}^{\phi(m')-1}\}$. S is also the integral basis for $\mathbb{Z}[\zeta_{m'}]$. The central primitive idempotents in $\mathbb{C}[G]$ is

$$e_{\chi_i} = \frac{\chi_i(1)}{|G|}\sum_{g\in G}\chi_i(g)g^{-1} = \frac{1}{|G|}\sum_{g\in G}\overline{\chi_i(g)}g, \tag{2.3}$$

where χ_i is an irreducible character of G and the set $\{e_{\chi_i} : \chi_i \in G^*\}$ is a basis for $\mathbb{C}[G]$. Two difference sets D and D' are equivalent if there exists a group element g and automorphism σ such that $D = g\sigma(D')$.

Aliases are members of group ring and they enable us to transfer information from $\mathbb{C}[G]$ to group algebra $\mathbb{Q}[G]$ and then to $\mathbb{Z}[G]$. Let G be an abelian group and $\Omega = \{\chi_1, \chi_2, \ldots, \chi_h\}$ 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, and β is an element of $\mathbb{Z}[G]$. If $K_{m'}$ is the Galois over $\mathbb{Q}$, then **central rational idempotents** in $\mathbb{Q}[G]$ are obtained by summing over the equivalence classes $X_i = \{e_{\chi_i}|\chi_i \sim \chi_j\} \in G^*/\sim$ on the e_χ's under the action of the Galois group of $K_{m'}$ over $\mathbb{Q}$. That is,

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

In particular, if G is a cyclic group of the form $C_{p^m} = \langle x : x^{p^m} = 1\rangle$ (p is prime) whose characters are of the form $\chi_i(x) = \zeta_{p^m}^i, i = 0, \ldots, p^m - 1$, then the rational idempotents are

$$[e_{\chi_0}] = \frac{1}{p^m}\langle x\rangle \tag{2.4}$$

$$[e_{\chi_{p^j}}] = \frac{1}{p^{j+1}}\Big(p\langle x^{p^{m-j}}\rangle - \langle x^{p^{m-j-1}}\rangle\Big), 0 \le j \le m-1. \tag{2.5}$$

The following is the general formula employed in the search of difference set [12].

Theorem 2.2 *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*

$$A = \sum_{i=o}^{s} \alpha_i [e_{\chi_i}], \tag{2.6}$$

where α_i is any χ_i-alias for A.

Equation (2.6) is known as **the rational idempotent decomposition** of A.

The following lemma extends the properties of D to $\hat{D}$.

Lemma 2.3 *Let D be a difference set in a group G and N be a normal subgroup of G. Suppose that $\psi : G \longrightarrow G/N$ is a natural epimorphism. Then*

1. $\hat{D}\hat{D}^{(-1)} = n \cdot 1_{G/N} + |N|\lambda(G/N)$
2. $\sum d_i^2 = n + |N|\lambda$
3. $\chi(\hat{D})\overline{\chi(\hat{D})} = n \cdot 1_{G/N}$*, where χ is a non-trivial representation of G/N.*

The method used in this paper is known as a representation theoretic method made popular by Leibler [12]. Some authors like Iiams and Smith [6, 18] have used this method in search of difference sets. This approach entails obtaining comprehensive lists $\Omega_{G/N}$, of difference set image distribution in factor groups of G. We start by finding difference set image in factor group of least order and garner more information about D as we gradually increase the size of the factor group.

To successfully obtain the difference set images, we need the aliases. In our case, if χ is not a principal character, then $|\chi(\hat{D})| = 7$ and we require how the ideal generated by 7 factors in $\mathbb{Z}[\zeta_{m'}]$, $m' = 2, 4, 5, 8, 10,$ $16, 20$ and 50. Let $\delta := \chi(\hat{D})$. By (2.6), 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 $\langle\delta\rangle\langle\bar{\delta}\rangle = \langle n\rangle$. 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. We use a theorem due to Kronecker [16, 17] that states that any algebraic integer whose conjugates have absolute value 1 must be a root of unity. If there is any other solution to the algebraic equation, then it must be of the form $\delta' = \delta u$[13], where $u = \pm\zeta_{m'}^j$ is a unit. To construct alias from this information, we choose a group element g that is mapped to $\zeta_{m'}$ 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 $\langle p\rangle$ in the cyclotomic integer ring $\mathbb{Z}[\zeta_{m'}]$ is $\frac{\phi(m')}{d}$, where ϕ is the Euler ϕ-function, i.e. $\phi(m') = |\mathbb{Z}_{m'}^*|$ [9]. For instance, the ideal generated by 2 has two factors in $\mathbb{Z}[\zeta_7]$, the ideal generated by 7 has four factors in $\mathbb{Z}[\zeta_{16}]$, while the ideal generated by 7 has two factors in $\mathbb{Z}[\zeta_{20}]$. On the other hand, since 2^s is a power of 2, then the ideal generated by 2 is said to completely ramify 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 [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 $p^i \equiv -1 \mod m'$. In this case, -1 belongs to the multiplicative group generated by p. Furthermore, n is self conjugate modulo m' if every prime divisor of n is semi-primitive modulo m'_p, m'_p is the largest divisor of m' relatively prime to p. This means that every prime ideals over n in $\mathbb{Z}[\zeta_{m'}]$ are fixed by complex conjugation. For instance, $7^2 \equiv -1 \pmod{m'}$, where $m' = 5, 10, 50$ and $7 \equiv -1 \pmod{m'}$, $m' = 2, 4, 8$. Thus $\langle 7 \rangle$ is fixed by conjugation in $\mathbb{Z}[\zeta_{m'}]$, $m' = 2, 4, 5, 8, 10, 50$. 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'. Consequently, if $\hat{D}$ is the difference set image of order $n = m^2$ in the cyclic factor group G/N, a group with exponent m', where $m' = 2, 4, 5, 8, 10, 50$ and χ is a non-trivial representation of G/N, then $\chi(\hat{D}) = m\zeta^i_{m'}$, $\zeta_{m'}$ is the m'-th root of unity [17].

The ideal generated by 7 has four factors in $\mathbb{Z}[\zeta_{16}]$. Suppose $\sigma \in Gal(\mathbb{Q}(\zeta_{16})/\mathbb{Q})$, where $\sigma(\zeta_{16}) = \zeta^7_{16}$. This automorphism split the basis elements of $\mathbb{Q}(\zeta_{16})$ into four orbits as $\zeta_{16} + \zeta^7_{16}$, $\zeta^3_{16} + \zeta^5_{16}$, $\zeta^9_{16} + \zeta^{15}_{16}$ and $\zeta^{11}_{16} + \zeta^{13}_{16}$. It is easy to see that $(7) = (1 + \zeta_{16} + \zeta^7_{16})(1 + \zeta^3_{16} + \zeta^5_{16})(1 + \zeta^9_{16} + \zeta^{15}_{16})(1 + \zeta^{11}_{16} + \zeta^{13}_{16})$. Put $\pi_1 = (1 + \zeta_{16} + \zeta^7_{16})$ and $\pi_2 = (1 + \zeta^3_{16} + \zeta^5_{16})$. Let $\delta_1 = 1 + \zeta_{16} + \zeta^7_{16}$ and $\delta_2 = 1 + \zeta^3_{16} + \zeta^5_{16}$ be representatives of these ideals. Then the nine solutions to $\delta\bar{\delta} = 7^2$ are $\delta_1\delta_2\bar{\delta}_1\bar{\delta}_2 = 7$, $\delta_1^2\delta_2^2$, $\bar{\delta}_1^2\delta_2^2$, $\delta_1^2\bar{\delta}_2^2$, $\bar{\delta}_1^2\bar{\delta}_2^2$, $\delta_1^2\delta_2\bar{\delta}_2$, $\delta_2^2\delta_1\bar{\delta}_1$, $\bar{\delta}_1^2\delta_2\bar{\delta}_2$ or $\bar{\delta}_2^2\delta_1\bar{\delta}_1$. The Galois automorphism $\sigma(\zeta_{16}) = \zeta^3_{16}$ divides the solution set into three equivalence classes: $\delta_1\delta_2\bar{\delta}_1\bar{\delta}_2 = 7$; $\delta_1^2\delta_2^2$, $\bar{\delta}_1^2\delta_2^2$, $\delta_1^2\bar{\delta}_2^2$, $\bar{\delta}_1^2\bar{\delta}_2^2$; $\delta_1^2\delta_2\bar{\delta}_2$, $\delta_2^2\delta_1\bar{\delta}_1$, $\bar{\delta}_1^2\delta_2\bar{\delta}_2$ or $\bar{\delta}_2^2\delta_1\bar{\delta}_1$. As we need solutions up to equivalence, we pick a representative from each class. Thus, $\delta = 7$, $\delta_1^2\delta_2^2 = -1 + 2\zeta_{16} - 4\zeta^2_{16} - 2\zeta^3_{16} - 2\zeta^5_{16} + 4\zeta^6_{16} + 2\zeta^7_{16}$ or $\delta_1^2\delta_2\bar{\delta}_2 = -1 + 4\zeta_{16} + 2\zeta^2_{16} + 2\zeta^3_{16} + 2\zeta^5_{16} - 2\zeta^6_{16} + 4\zeta^7_{16}$. Similarly, in $\mathbb{Z}[\zeta_{20}]$ if $\theta = \zeta_{20} + \zeta^3_{20} + \zeta^7_{20} + \zeta^9_{20}$, then $\delta = 7$, $2 + 3\theta$, $-2 + 3\theta$ or their conjugates. In summary, suppose that $\hat{D}$ is a (400, 57, 8) difference set image in $C_{m'}$ and χ is any non-trivial character of $C_{m'}$ such that $\chi(\hat{D})\overline{\chi(\hat{D})} = 49$. If

- $m' = 2, 4, 5, 8, 10, 50$, then $\chi(D)$ is one of $\pm 7u, u$ is appropriate root of unity.
- $m' = 16$, then $\chi(D)$ is one of $\pm 7\zeta^j_{16}$, $\pm(-1 + 2\zeta_{16} - 4\zeta^2_{16} - 2\zeta^3_{16} - 2\zeta^5_{16} + 4\zeta^6_{16} + 2\zeta^7_{16})\zeta^j_{16}$, $\pm(-1 + 4\zeta_{16} + 2\zeta^2_{16} + 2\zeta^3_{16} + 2\zeta^5_{16} - 2\zeta^6_{16} + 4\zeta^7_{16})\zeta^j_{16}$, $j = 0, \ldots, 15$.
- $m' = 20$, then $\chi(D)$ is $\pm 7\zeta^j_{20}$, $(2 + 3(\zeta_{20} + \zeta^3_{20} + \zeta^7_{20} + \zeta^9_{20})\zeta^j_{20}$ or $(-2 + 3\zeta_{20} + \zeta^3_{20} + \zeta^7_{20} + \zeta^9_{20})\zeta^j_{20}$, $j = 0, \ldots, 19$.

Consequently, for (400, 57, 8) difference sets in C_{16}, the alias α in the rational idempotent decomposition of $\hat{D}$ is one of the two forms:

1. $\alpha = \pm 7x^j$,
2. $\pm(-1 + 2x - 4x^2 - 2x^3 - 2x^5 + 4x^6 + 2x^7)x^j$, $\pm(-1 + 4x + 2x^2 + 2x^3 + 2x^5 - 2x^6 + 4x^7)x^j$, $j = 0, \ldots, 15$.

Other aliases for the remaining cases are obtained in a similar manner.

2.3. Characteristics of difference set images in subgroup of a group

Dillon [2] 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 2.4 (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 2.5 *If the cyclic group Z_{2m} does not contain a (non-trivial) difference set, then neither does the dihedral group of order $2m$.*

The next result describes geometrically how properties of a factor group of a group can be lifted, under certain conditions, to the group itself [15].

Theorem 2.6 *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^m, $m \leq s$. Suppose also that $E_1, E_2, \ldots, E_t$, where $t = q^{m-d}(\frac{q^m-1}{q-1})$ are the subgroups of E and their cosets, each of order $q^d, d < m$ with $\hat{D}$ and $\hat{\hat{D}}_i$ being 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 exists an integer k' such that $\hat{D} \equiv a(k')^{-1}H \mod p$.*

Proof See [14] or [15]. □

It turns out that $k' = q^d$. We will use this result to determine the non-existence of (400, 57, 8) difference set images in some groups of order 16 with $q = 2$, $p = 7$, $k' = 2$, $m = 2$ and $d = 1$.

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 [10], we may write any element X of the group ring $\mathbb{Z}[H]$ in the form

$$X = X\left(\frac{1+z}{2}\right) + X\left(\frac{1-z}{2}\right). \tag{2.7}$$

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

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

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 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

$$H \cong K \times \langle z\rangle, \tag{2.9}$$

then the difference set image in H is

$$\hat{D} = A\left(\frac{\langle z\rangle}{2}\right) + gB\left(\frac{2 - \langle z\rangle}{2}\right), \tag{2.10}$$

where $g \in H$, A is a difference set in K, $\alpha = \frac{k+\sqrt{n}}{|K|}$ or $\alpha = \frac{k-\sqrt{n}}{|K|}$, $B = A - \alpha K$ and k is the size of the difference set. (2.10) is true as long as $|K| \mid (k+\sqrt{n})$ or $|K| \mid (k-\sqrt{n})$. In the next two sections, we shall analyze the non-existence of difference set images in factor groups of orders 16, 20 and 40.

3. Some group 16 images do not exist

3.1. The Group 8 images

We first obtain (400, 57, 8) difference set images in groups of order 8.

3.1.1. The C_2 image

Suppose that $G/N \cong C_2 = \langle x : x^2 = 1 \rangle$ and $\hat{D} = d_0 + d_1 x$ is the (400, 57, 8) difference set image in G/N. The distribution scheme, Ω_{C_2} for C_2 consists of $A = 32 + 25x$.

3.1.2. The C_4 image

Suppose that $G/N \cong C_4 = \langle x : x^4 = 1 \rangle$ and $\hat{D} = \sum_{s=0}^{3} d_s x^s$ is the (400, 57, 8) difference set image in G/N. We view this group ring element as a 1×4 matrix with columns indexed by powers of x. The distribution scheme, Ω_{C_4} for C_4 (up to translation), consists of only $A_1 = -7 + 16\langle x \rangle$.

3.1.3. The $C_2 \times C_2$ image

Using (2.10) with $\alpha = 32$, $K = C_2$ and $|K| = 2$, the difference set image in $C_2 \times C_2 = \langle x, y : x^2 = y^2 = 1 = [x,y] \rangle$ is $A_2 = -7 + 16(1+x)(1+y)$.

3.1.4. The C_8 images

Suppose that $G/N \cong C_4 = \langle x : x^4 = 1 \rangle$ and $\hat{D} = \sum_{s=0}^{3} d_s x^s$ is the (400, 57, 8) difference set image in G/N. Up to translation, the only element in Ω_{C_8} is $A' = -7 + 8\langle x \rangle$.

3.1.5. The D_4 image

Suppose that $G/N \cong D_4 = \langle x, y : x^4 = y^2 = 1, yxy = x^{-1} \rangle$. Let $\hat{D} = \sum_{t=0}^{1} \sum_{s=0}^{3} d_{st} x^s y^t$ be the difference set image in G/N. Using the Dillon Dihedral trick, it can be shown that $B_1' = -7 + 8\langle x \rangle \langle y \rangle$ is the only element of Ω_{D_4} up to equivalence.

3.1.6. The $C_4 \times C_2$ image

Consider $G/N \cong C_4 \times C_2 = \langle x, y : x^4 = y^2 = 1 = [x,y] \rangle$. We view the difference set image $\hat{D} = \sum_{i=0}^{3} \sum_{j=0}^{1} d_{ij} x^i y^j$ in $C_4 \times C_2$ as a 2×4 array with columns indexed by powers of x and rows indexed by powers of y. Using (2.10) with $\alpha = 16$, $|K| = 4$, and $B_1 = A_1 - 16K$, where $A_1 \in \Omega_{C_4}$, $B_2' = -7 + 8\langle x \rangle \langle y \rangle$ is the only viable difference set image in $C_4 \times C_2$ up to equivalence.

3.1.7. The $(C_2)^3$ image

Suppose that $G/N \cong (C_2)^3 = \langle a,b,c : a^2 = b^2 = c^2 = 1 = [a,b] = [b,c] = [a,c]\rangle$. Take $K = (C_2)^2$, $|K| = 4$, and $B_1 = A - 16K$, where $A \in \Omega_{C_2 \times C_2}$. By (2.10), $B_3' = -7 + 8(1+a)(1+b)(1+c)$ is the only viable difference set image in $(C_2)^3$ up to equivalence.

Remark 1 *Notice that the characteristics of the difference set images in* $(C_2)^3$ *and* $C_4 \times C_2$ *are described by Theorem 2.6, but we need more than that in this paper. The difference set images in* $(C_2)^2$ *and* C_4 *satisfy* $A \equiv 2 \pmod 7$*. If we choose* $a = 2$*,* $p = 7$ *and* $k' = 2$*, then the difference set images in* $(C_2)^3$ *and* $C_4 \times C_2$ *satisfy the condition* $B_j' \equiv 1 \pmod 7$*. This condition is also satisfied by the difference set image in* D_4*.*

3.1.8. The Q_4 image

Consider $G/N \cong Q_4 = \langle x, y : x^4 = 1, xy = yx^{-1}, x^2 = y^2\rangle$. The derived subgroup of G/N is isomorphic to $\langle x^2\rangle$. Let the difference set image in G/N be $\hat{D} = \sum_{t=0}^{1}\sum_{s=0}^{3} d_{st}x^s y^t$. We view this object as a 2×4 matrix with rows indexed by powers of y and columns indexed by powers of x. Since $Q_4/\langle x^2\rangle \cong C_2 \times C_2$, G/N has four characters. By applying these four characters to $\hat{D}$, we get $A^* = \frac{1}{2}\{9 + 16x + 9x^2 + 16x^3 + 16\langle x\rangle y\}$. The only degree two representation of G/N is

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

In a non-abelian group like this, the idempotents are obtained by applying the diagonal entries of χ to $\hat{D}$. Thus, the idempotents are

$$f = \frac{1}{4}\begin{bmatrix} 1 & -i & -1 & i \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad \bar{f} = \frac{1}{4}\begin{bmatrix} 1 & i & -1 & -i \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$f_y = \frac{1}{4}\begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & -i & -1 & i \end{bmatrix}, \quad \bar{f_y} = \frac{1}{4}\begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & i & -1 & -i \end{bmatrix}.$$

Therefore, the two rational idempotents (from χ) are
$[f] = f + \bar{f} = \frac{1}{4}\begin{bmatrix} 2 & 0 & -2 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$ and $[f_y] = f_y + \bar{f_y} = \frac{1}{4}\begin{bmatrix} 0 & 0 & 0 & 0 \\ 2 & 0 & -2 & 0 \end{bmatrix}$.
Consequently, the difference set equation is

$$\hat{D} = A^* + \alpha_1[f] + \alpha_2[f_y], \tag{3.1}$$

where $\alpha_j, j = 1,2$ is an alias. To find the aliases, α_j, we apply χ to $\hat{D}$ so that

$$\chi(\hat{D}) = \begin{pmatrix} z & w \\ \overline{w} & \overline{z} \end{pmatrix},$$

where $z = (d_{00} - d_{20}) + (d_{10} - d_{30})i$ and $w = (d_{01} - d_{21}) + (d_{11} - d_{31})i$, $w, z \in \mathbb{Z}[i]$. Thus

$$\chi(\hat{D})\overline{(\chi\hat{D})} = \begin{pmatrix} z\overline{z} + w\overline{w} & 0 \\ 0 & z\overline{z} + w\overline{w} \end{pmatrix} = 49I_2,$$

where I_2 is the 2×2 identity matrix and $z\overline{z} + w\overline{w} = 49$. By expanding this equation, we get

$$(d_{00} - d_{20})^2 + (d_{10} - d_{30})^2 + (d_{01} - d_{21})^2 + (d_{11} - d_{31})^2 = 49. \tag{3.2}$$

Up to permutations, the set of all possible values satisfying (3.2) is listed in Table 1.

Table 1. Up to permutations, the set of all possible coefficients satisfying (3.2).

S/N	$d_{00} - d_{20}$	$d_{10} - d_{30}$	$d_{01} - d_{21}$	$d_{11} - d_{31}$
i.	± 7	0	0	0
ii.	$\pm$ 6	± 3	± 2	0
iii.	± 5	± 4	± 2	± 2
iv.	± 4	± 4	± 4	± 1

Our next task is to find all sets of equivalent solutions to (3.2). The following facts assist with this objective:

1. $\{1, i\}$ is a basis of $\mathbb{Z}[i]$ and we can replace either z or w with zi^k or wi^j or their conjugates, where i is the fourth root of unity, if necessary.
2. In (3.1), observe that 2 entries of A^* are congruent to $1 \mod 2$ while 6 entries are congruent to zero modulo $\mod 2$.
3. The sum of the last two terms in (3.1) must have the above property, also.

Hence, up to negatives and permutations, we consider only the coefficients in Table 2.

By choosing aliases according to values in Table 2 and up to equivalence, the elements of Ω_{Q_4} are

- $F_1 = -7 + 8\langle x\rangle\langle y\rangle$, $F_2 = 6 + 11x + 3x^2 + 5x^3 + 9y + 8xy + 7x^2y + 8x^3y$;
- $F_3 = 3 + 8x + 6x^2 + 8x^3 + 11y + 9xy + 5x^2y + 7x^3y$, $F_4 = 6 + 9x + 3x^2 + 7x^3 + 11y + 8xy + 5x^2y + 8x^3y$;
- $F_5 = 5 + 10x + 4x^2 + 6x^3 + 10y + 10xy + 6x^2y + 6x^3y$, $F_6 = 7 + 10x + 2x^2 + 6x^3 + 9y + 9xy + 7x^2y + 7x^3y$;
- $F_7 = 7 + 9x + 2x^2 + 7x^3 + 10y + 9xy + 6x^2y + 7x^3y$.

Table 2. Possible coefficients.

S/N	$d_{00} - d_{20}$	$d_{10} - d_{30}$	$d_{01} - d_{21}$	$d_{11} - d_{31}$
i.	-7	0	0	0
ii.	3	6	2	0
iii.	3	2	6	0
iv.	3	0	6	2
v.	1	4	4	4
vi.	5	4	2	2
vii.	5	2	4	2

3.2. The C_{16} images

Consider the group $G/N \cong C_{16} = \langle x : x^{16} = 1\rangle$. Suppose that the difference image in this group is $\sum_{s=0}^{15} d_s x^s$. We view this element as a 1×16 matrix. Using (2.4) and (2.5), the five rational idempotents of C_{16} are $[e_{\chi_0}] = \frac{\langle x\rangle}{16}, [e_{\chi_8}] = \frac{2\langle x^2\rangle - \langle x\rangle}{16}, [e_{\chi_4}] = \frac{2\langle x^4\rangle - \langle x^2\rangle}{8}$, $[e_{\chi_1}] = \frac{2-\langle x^8\rangle}{2}$, and $[e_{\chi_2}] = \frac{2\langle x^8\rangle - \langle x^4\rangle}{4}$. Four of these rational idempotents have $\langle x^8\rangle$ in their kernel and we write their linear combination as

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

where $A' \in \Omega_{C_8}$ and α_{χ_j} is an alias. Hence, the difference set equation is

$$\hat{D} = Y + \alpha_{\chi_1}[e_{\chi_1}], \tag{3.3}$$

where $\alpha_{\chi_1} \in \{\pm 7x^s, \pm a_1 x^u, \pm a_2 x^t\}$, $a_1 = -1 + 2x - 4x^2 - 2x^3 - 2x^5 + 4x^6 + 2x^7$, $a_2 = -1 + 4x + 2x^2 + 2x^3 + 2x^5 - 2x^6 + 4x^7, s, t = 0, \ldots, 15$. Define $Z_1 = 7 \cdot [e_{\chi_1}] = \frac{7}{2}(2 - \langle x^8\rangle)$, $Z_2 = a_1[e_{\chi_1}] = (-1 + 2x - 4x^2 - 2x^3 - 2x^5 + 4x^6 + 2x^7)(1 - x^8)$ and $Z_3 = a_2[e_{\chi_1}] = (-1 + 4x + 2x^2 + 2x^3 + 2x^5 - 2x^6 + 4x^7)(1 - x^8)$. Rewrite (3.3) as

$$\hat{D} = Y \pm x^l Z_k, k = 1, 2, 3; l = 0, \ldots, 15. \tag{3.4}$$

The fractions in Y compelled (3.4) to be

$$\hat{D} = Y \pm x^l Z_k, k = 1, 2, 3; l = 0, 8. \tag{3.5}$$

The solutions to (3.5) are

1. $E_1 = -7 + 4\langle x\rangle$, $E_2 = 5x + 2x^2 + 3x^3 + 4x^4 + 3x^5 + 6x^6 + 5x^7 + x^8 + 3x^9 + 6x^{10} + 5x^{11} + 4x^{12} + 5x^{13} + 2x^{14} + 3x^{15}$;
2. $E_3 = 6x + 5x^2 + 5x^3 + 4x^4 + 5x^5 + 3x^6 + 6x^7 + x^8 + 2x^9 + 3x^{10} + 3x^{11} + 4x^{12} + 3x^{13} + 3x^{14} + 2x^{15}$.

As intersection number cannot be negative, up to equivalence, the elements of $\Omega_{C_{16}}$ are $E_k, k = 2, 3$.

3.3. There is no D_8 image

Suppose that $G/N \cong D_8 = \langle \theta, y : \theta^8 = y^2 = 1, y\theta y = \theta^{-1}\rangle$ and the difference set image is $\hat{D} = \sum_{s=0}^{7}\sum_{t=0}^{1} d_{st}\theta^s y^t$. This group ring element is perceived as a 2×8 matrix. In order to take advantage of the Dillon Dihedral trick using the difference set images in $C_{16} = \langle x : x^{16} = 1\rangle$, set $\theta = x^2$ in C_{16} and rewrite each of the two difference images as a 2×8 matrix. For instance, $E_2 \in \Omega_{C_{16}}$ becomes $E_2' = (5\theta + 4\theta^2 + 3\theta^3 + \theta^4 + 3\theta^5 + 4\theta^6 + 2\theta^7) + (6 + 5\theta + 5\theta^2 + 6\theta^3 + 2\theta^4 + 3\theta^5 + 3\theta^6 + 2\theta^7)y$. The factor group G/N has two equivalent degree two representations. One of them is:

$$\chi : \theta \mapsto \begin{pmatrix} \zeta_8 & 0 \\ 0 & \zeta_8^7 \end{pmatrix}, \quad y \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

We now apply this degree two representation to the transformed C_{16} difference set image $E_j', j = 2, 3$ and verify whether or not $\chi(E_j')\overline{\chi(E_j')} = 49I_2, j = 2, 3$. In the case of E_2', $\chi(E_2') = \begin{pmatrix} \beta & \alpha \\ \bar{\alpha} & \bar{\beta} \end{pmatrix}$, where $\alpha =$

$2(1-\zeta_8-\zeta_8^2+\zeta_8^3)\neq 0$, $\beta=-4\sqrt{2}i, i=\zeta_8^2$. Notice that $\chi(E_2)\overline{\chi(E_2)}\neq 49I_2$ since $\alpha\beta=-16(\zeta_8-\zeta_8^2)\neq 0$. Similarly, $\chi(E_3')\overline{\chi(E_3)}\neq 49I_2$, where E_3' is the transformed E_3. Thus, D_8 does not admit (400, 57, 8) difference set.

3.4. There is no $C_8\times C_2$ image

Let $G/N\cong C_8\times C_2=\langle x:x^8=y^2=1=[x,y]\rangle=K\times\langle y\rangle$, $K=\langle x\rangle$ and suppose that the difference set image $\hat{D}=\sum_{s=0}^{7}\sum_{t=0}^{1}d_{st}x^sy^t$ exists in G/N. Since this group is of the form (2.9), we choose $\alpha=8$, $K=C_8$, $|K|=8$ and $B=A'-8K$, where A' is the unique difference set image in C_8. Thus, (2.10) becomes $A'\left(\frac{1+y}{2}\right)+gB\left(\frac{1-y}{2}\right)$, where $g\in C_8\times C_2$. However, this equation has no integer solution because $A'\left(\frac{1+y}{2}\right)$ has 14 integer entries with 2 fractions while $B\left(\frac{1-y}{2}\right)$ has 2 integer entries with 14 fractions. Hence, $\Omega_{C_8\times C_2}$ is empty.

3.5. There is no $C_4\rtimes_{-1}C_4$ image

Suppose $G/N\cong C_4\rtimes_{-1}C_4=H=\langle x,y:x^4=y^4=1,yxy^{-1}=x^{-1}\rangle$. We assume that this factor group has a difference image, say, $\hat{D}=\sum_{s,t=0}^{3}d_{st}x^sy^t$. Consequently, to each point x^iy^j in H, we assign a weight d_{ij} equal to the size of the intersection of the coset x^iy^jN and putative difference set D. The center of H is $C(H)=\{1,x^2,y^2,x^2y^2\}\cong C_2\times C_2$, which is an elementary abelian 2-group of order 4. The three non-trivial subgroups of $C(H)$ are $\{1,x^2\}$, $\{1,y^2\}$ and $\{1,x^2y^2\}$. It turns out that these three subgroups are in fact normal subgroups of H. Thus, $H/\langle y^2\rangle\cong D_4$, $H/\langle x^2\rangle\cong C_4\times C_2$ and $H/\langle x^2y^2\rangle\cong Q_4$. The center of H, $C(H)$ along with its three cosets generates four copies of a (4, 6, 3, 2, 1) design. These designs are viewed as a plane in the form

$d_{i,j}$	$d_{2+i,j}$
$d_{i,2+j}$	$d_{2+i,2+j}$

where $i,j=0,1$. The terminology **row sum** denotes the sum $d_{i,j}+d_{2+i,j}$ or $d_{i,2+j}+d_{2+i,2+j}$; **column sum** denotes the sum $d_{i,j}+d_{i,2+j}$ or $d_{2+i,j}+d_{2+i,2+j}$; **diagonal sum** represents $d_{i,j}+d_{2+i,2+j}$ or $d_{i,2+j}+d_{2+i,j}$ and **plane weight** is the sum $\beta=d_{i,j}+d_{2+i,j}+d_{i,2+j}+d_{2+i,2+j}$. We also use the abbreviation **β-plane** for plane of weight β[6]. The fact that $H/\langle y^2\rangle\cong D_4$, $H/\langle x^2\rangle\cong C_4\times C_2$ and $H/\langle x^2y^2\rangle\cong Q_4$ implies that the sets of row, column and diagonal sums of each of the planes are valid sets of intersection numbers in $\Omega_{C_4\times C_2}$, Ω_{D_4}, and Ω_{Q_4} respectively. Also, as $H/C(H)\cong C_2\times C_2$, each plane weight is a valid intersection number of the unique difference set image in $C_2\times C_2$. Hence, the possible plane weights are 9 and 16. Precisely, in the collection of these four planes, there are three 16-planes and one 9-plane. Without loss of generality, take row sums to be intersection numbers of difference set image in $C_4\times C_2$ and column sums to be intersection numbers of difference set image in D_4. Finally, the diagonal sums will be intersection numbers of difference set images in Q_4. Q_4 has seven difference set images. We split these seven difference set images $F_s, s=1,\ldots,7$ into two categories. In the first case, we look at 9-plane and, in the other, we look at one of the three 16-planes.

Case 1: $F_s, s\neq 6,7$ We rearrange the four plane, if necessary, such that the 9-plane is

d_{00}	d_{20}
d_{02}	d_{22}

As $C_4 \times C_2$ and D_4 have unique difference set image, the row and column sums of the 9-plane must be of the form $\genfrac{}{}{0pt}{}{1}{8}$ (up to equivalence) while the diagonal sums must be one of the forms $\genfrac{}{}{0pt}{}{1}{8}$, $\genfrac{}{}{0pt}{}{5}{4}$, or $\genfrac{}{}{0pt}{}{3}{6}$ (up to equivalence). Thus, the system $d_{00} + d_{20} = c_1$, $d_{02} + d_{22} = c_2$, $d_{00} + d_{02} = c_3$, $d_{20} + d_{22} = c_4$, $d_{00} + d_{22} = c_5$ and $d_{02} + d_{20} = c_6$ does not have a solution, where $c_1, c_2, c_3, c_4 \in \{1, 8\}$, $c_5, c_6 \in \{1, 8\}$. Similar result holds for $c_5, c_6 \in \{3, 6\}$ or $c_5, c_6 \in \{4, 5\}$.

Case 2: $F_s, s = 6, 7$ Consider the 16-plane.

d_{01}	d_{21}
d_{03}	d_{23}

The diagonal sums are of the form $\genfrac{}{}{0pt}{}{10}{6}$ or $\genfrac{}{}{0pt}{}{9}{7}$ (up to equivalence). In particular, take the diagonal sums to be of the form $\genfrac{}{}{0pt}{}{9}{7}$. As the row and column sums of this plane are always of the form $\genfrac{}{}{0pt}{}{8}{8}$, then the system $d_{01} + d_{21} = c_1$, $d_{03} + d_{23} = c_2$, $d_{01} + d_{03} = c_3$, $d_{21} + d_{23} = c_4$, $d_{01} + d_{23} = c_5$ and $d_{03} + d_{21} = c_6$ does not have a solution, where $c_1, c_2, c_3, c_4 \in \{8, 8\}$, $c_5, c_6 \in \{7, 9\}$. The same conclusion holds for the other diagonal sums. Hence, $\Omega_{C_4 \rtimes C_4}$ is empty.

3.6. There are no $C_4 \times C_4, C_4 \times (C_2)^2, D_4 \times C_2, (C_2)^4$ or $(C_4 \times C_2) \rtimes C_2$ images

Let N be an appropriate normal subgroup of G such that $G/N \cong H$, where H is one of the above groups. Each H has a normal subgroup that is isomorphic to $(C_2)^2$ and let h be a non-trivial element of this normal subgroup. Then $H/\langle h \rangle$ is isomorphic to D_4, $(C_2)^3$ or $C_4 \times C_2$ (see remark 1). Theorem 2.6 with $p = 7$, $a = 1$ and $k' = 2$ indicates that the difference set image in H satisfies $\hat{D} \equiv 3 \pmod 7$. We verify this claim using the variance trick, Lemma 2.1. Since $|N| = 25$ and $\hat{D} \equiv 3 \pmod 7$, the intersection numbers in $\hat{D}$ must be 3, 10, 17 or 24. Thus, we use variance trick to find the values of m_i, where $i = 3, 10, 17, 24$ and

$$\begin{aligned} m_3 + m_{10} + m_{17} + m_{24} &= 16 \\ m_3 + 3m_{10} + 17m_{17} + 24m_{24} &= 57 \\ 6m_3 + 90m_{10} + 272m_{17} + 552m_{24} &= 192. \end{aligned} \tag{3.6}$$

The coefficients of m_{17} and m_{24} in the third equation are more than 192. Consequently, $m_{17} = m_{24} = 0$ and system (3.6) becomes

$$\begin{aligned} m_3 + m_{10} &= 16 \\ m_3 + 3m_{10} &= 57 \\ 6m_3 + 90m_{10} &= 192. \end{aligned} \tag{3.7}$$

The system (3.7) has no viable solution and G/N does not admit (400, 57, 8) difference sets.

4. Difference set images in groups of orders 20 and 40

In this section, we show that some factor groups of order 20 and 40 do not admit (400, 57, 8) difference sets.

4.1. The C_5 image

Suppose that $G/N \cong C_5 = \langle x : x^5 = 1\rangle$. Then the difference set image is $A' = 7 + 10\langle x\rangle$.

4.2. The C_{10} and D_5 images

Suppose that $G/N \cong C_{10} = \langle x, y : x^5 = y^2 = [x, y] = 1\rangle$. Then the difference set image is $E = 7 + 5\langle x\rangle\langle y\rangle$. We can also show using the Dillon trick that E is the only difference set image in $G/N \cong D_5 = \langle x, y : x^5 = y^2 = yxyx = 1\rangle$.

4.3. The C_{25} image

If $G/N \cong C_{25} = \langle x : x^{25} = 1\rangle$, then the unique difference set image is $7 + 2\langle x\rangle$.

4.4. The C_{50} image

If $G/N \cong C_{25} = \langle x, y : x^{25} = y^2 = [x, y] = 1\rangle$, then the unique difference set image is $7 + \langle x\rangle\langle y\rangle$.

4.5. There are no $C_{10} \times C_2$ and D_{10} images

Suppose that N are normal subgroups of G such that $G/N \cong C_{10} \times C_2$ or $G/N \cong D_{10} \cong D_5 \times C_2$. These groups are of the form (2.9) and we choose $K = C_{10}$ or D_5, $\alpha = 5$, $|K| = 10$, and $B = E - 5K$, where $E \in \Omega_{D_5}$ or $E \in \Omega_{C_{10}}$. Let z be the generator of C_2. Then, by (2.10)

$$\hat{D} = E\left(\frac{\langle z\rangle}{2}\right) + gB\left(\frac{2 - \langle z\rangle}{2}\right), \tag{4.1}$$

$g \in D_{10}$ or $g \in C_{10} \times C_2$. Notice that $E\big(\frac{\langle z\rangle}{2}\big)$ consists of 2 integers and 18 fractions while $B\big(\frac{2-\langle z\rangle}{2}\big)$ consists of 18 integers and 2 fractions. These observations show that the two terms on the right-hand side of (4.1) are not compatible to produce integer solutions. Hence, $(C_2)^2 \times C_5$ and D_{10} do not admit (400, 57, 8) difference set.

4.6. There are no $C_{50} \times C_2$ and $D_{25} \times C_2$ images

It can be shown that if $G/N \cong C_{50} \times C_2$ or $D_{25} \times C_2$, then G does not admit (400, 57, 8) difference sets.

4.7. The C_{20} image

Consider $G/N \cong C_{20} = \langle x, y : x^5 = y^4 = 1 = [x, y]\rangle$. We view the difference set in G/N, $\hat{D} = \sum_{t=0}^{3}\sum_{s=0}^{4} x^s y^t$ as a 4×5 matrix with the columns indexed by the powers of x and rows indexed by powers of y. This group has 6 rational idempotents out of which four have $\langle y^2\rangle$ in their kernel. The linear combination of these four rational idempotent is $\sum_{j=0,1}\sum_{k=0,2} \alpha_{\chi_{(j,k)}}[e_{\chi_{(j,k)}}] = \frac{E}{2}\langle y^2\rangle$, where E is the difference set image in C_{10} and $\alpha_{\chi_{(j,k)}}$ is an alias. The remaining two rational idempotents are

$$[e_{\chi_{(0,1)}}] = \frac{1}{10}\langle x\rangle(1 - y^2) \quad \text{and} \quad [e_{\chi_{(1,1)}}] = \frac{1}{10}(5 - \langle x\rangle)(1 - y^2).$$

Thus, the difference set image in C_{20} is

$$\hat{D} = \frac{E}{2}\langle y^2\rangle + \alpha_{\chi_{(0,1)}}[e_{\chi_{(0,1)}}] + \alpha_{\chi_{(1,1)}}[e_{\chi_{(1,1)}}] \tag{4.2}$$

with $\alpha_{\chi_{(1,1)}} \in \{\pm 7(xy)^{p_1}, \pm(2+3(x+x^3+x^7+x^9))(xy)^{p_2}\}$ and $\alpha_{\chi_{(0,1)}} \in \{\pm 7(xy)^{p_3}\}$, $p_1, p_2, p_3 = 0, \ldots, 19$. Put

$B_1 = (2+3(xy+(xy)^3+(xy)^7+(xy)^9)[e_{\chi_{(1,1)}}] = \frac{1}{10}\big((10-2\langle x\rangle)+15(x-x^2-x^3+x^4)-(10-2\langle x\rangle)-15(x-x^2-x^3+x^4)\big)$, $B_2 = 7[e_{\chi_{(1,1)}}] = \frac{7}{10}\big((5+\langle x\rangle)-(5+\langle x\rangle)\big)$ and $C = 7[e_{\chi_{(0,1)}}] = \frac{7}{10}\langle x\rangle(1-y^2)$. Then (4.2) becomes

$$\hat{D} = \frac{E}{2}\langle y^2\rangle \pm x^t y^s B_l \pm y^j C, t = 0, \cdots, 4;\ s, j = 0, 1, 2, 3;\ l = 1, 2. \tag{4.3}$$

It turns out that 18 entries of $\frac{E}{2}\langle y^2\rangle$ are congruent to $10 \mod 20$ while the remaining entries are congruent to $10 \mod 20$. Thus, (4.3) has solutions if and only if $t = 0$ and $s = j$. Up to equivalence, the unique difference set image is $E' = 6+x+4x^2+4x^3+x^4+(4+3x+3x^2+3x^3+3x^4)y+(6+4x+x^2+x^3+4x^4)y^2+(1+2x+2x^2+2x^3+2x^4)y^3$.

4.8. The $Frob(20)$ image

Suppose that $G/N \cong Frob(20) = C_5 \rtimes C_4 = \langle x, y : x^5 = y^4 = 1, yx = x^2y\rangle$, the Frobenius group of order 20. Suppose that $\hat{D} = \sum_{k=0}^{3}\sum_{j=0}^{4} d_{jk}x^j y^k$ is the difference set image in $Frob(20)$. This group ring element is perceived as a 4×5 matrix, where the rows are indexed by powers of y and columns are indexed by powers of x. By using permutation representation of $Frob(20)$ and Smith's approach [18], we can show that the only difference set image in $Frob(20)$ is $A_1 = 4+3x+x^3+x^4+(1+3x+3x^2+4x^3+5x^4)y+(2+3x+3x^2+2x^3+6x^4)y^2+(3+x+4x^2+3x^3+5x^4)y^3$.

4.9. There are no $Frob(20) \times C_2$ images

Suppose that there is a normal subgroup of G such that $G/N \cong Frob(20) \times C_2 = \langle x, y, z : x^5 = y^4 = z^2 = 1, yx = x^2y, xz = zx, yz = zy\rangle$. Let $\hat{D} = \sum_{k=0}^{4}\sum_{j=0}^{1}\sum_{i=0}^{3} d_{ijk}x^i y^j z^k$ be the difference set image in $Frob(20) \times C_2$. This group ring element is viewed as a 8×5 matrix. The derived group of G/N is isomorphic to $\langle x\rangle$ and $(Frob(20) \times C_2)/\langle x\rangle \cong C_4 \times C_2$. Also, $(Frob(20) \times C_2)/\langle z\rangle \cong Frob(20)$. By applying the eight characters of $Frob(20) \times C_2$ to $\hat{D}$, we get the following equations:

$$\begin{aligned} &\sum_{i=0}^{4} d_{i00} = c_{00}, && \sum_{i=0}^{4} d_{i10} = c_{10}, && \sum_{i=0}^{4} d_{i20} = c_{20}, && \sum_{i=0}^{4} d_{i30} = c_{30}, \\ &\sum_{i=0}^{4} d_{i01} = c_{01}, && \sum_{i=0}^{4} d_{i11} = c_{11}, && \sum_{i=0}^{4} d_{i21} = c_{21}, && \sum_{i=0}^{4} d_{i31} = c_{31},. \end{aligned} \tag{4.4}$$

where the 2×4 matrix (c_{ij}) is the unique difference set image in $C_4 \times C_2$. Also, using the map $z \mapsto 1$ we get 20 more linear equations

$$\begin{aligned} &d_{i00} + d_{i01} = b_{i0}, && d_{i10} + d_{i11} = b_{i1} && \\ &d_{i20} + d_{i21} = b_{i2}, && d_{i30} + d_{i31} = b_{i3}, && i = 0, \ldots, 4, \end{aligned} \tag{4.5}$$

where the 4×5 matrix (b_{ij}) is the unique element of $\Omega_{Frob(20)}$. One of the two equivalent degree four representations of $Frob(20) \times C_2$ is

$$\chi : x \mapsto \begin{pmatrix} \zeta & 0 & 0 & 0 \\ 0 & \zeta^2 & 0 & 0 \\ 0 & 0 & \zeta^4 & 0 \\ 0 & 0 & 0 & \zeta^3 \end{pmatrix}, \quad y \mapsto \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad z \mapsto \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix},$$

ζ is the fifth root of unity. By applying this representation to $\hat{D}$, we get

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

where $A = \sum_{s=0}^{4} a_s\zeta^s$, $B = \sum_{s=0}^{4} b_s\zeta^s$, $C = \sum_{s=0}^{4} c_s\zeta^s$, $D = \sum_{s=0}^{4} d_s\zeta^s$, $a_s = d_{s00} - d_{s01}$, $b_s = d_{s10} - d_{s11}$, $c_s = d_{s20} - d_{s21}$, $d_s = d_{s30} - d_{s31}$ and $\sigma(\zeta) = \zeta^2$.

By solving $\chi(\hat{D})\overline{\chi(\hat{D})} = 49I_4$, where I_4 is a 4×4 identity matrix, we get 16 equations which are equivalent to the following system:

$$A\bar{A} + B\bar{B} + C\bar{C} + D\bar{D} = 49 \tag{4.6}$$

$$AC + BD = 0 \tag{4.7}$$

$$A\overline{\sigma(D)} + B\overline{\sigma(A)} + C\overline{\sigma(B)} + D\overline{\sigma(C)} = 0 \tag{4.8}$$

$$A\overline{\sigma(B)} + B\overline{\sigma(C)} + C\overline{\sigma(D)} + D\overline{\sigma(A)} = 0 \tag{4.9}$$

Conditions (4.6)-(4.9) generate 14 more linear equations. We now use a computer to search for possible values of d_{ijk} by combining these 14 linear equations with (4.4) and (4.5). In order to have an exhaustive search, we fix the values of b_{ij} from the $Frob(20)$ image and allow c_{sk} in (4.4) to vary. This search yielded no result. Consequently, there is no difference set image in $Frob(20) \times C_2$.

Based on the above results and exploration with GAP, we conclude that if there are non-isomorphic (400, 57, 8) Singer difference sets, it must be in groups with GAP identification number $[400, cn]$, where $cn =$ 3, 49, 50, 52, 56, 57, 58, 59, 116, 132, 133, 206, 207, 212, 213.

References

[1] Baumert, L. D.: *Cyclic Difference Sets,* Springer-Verlag Publishers (1971).

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

[3] Gao, S., and Wei, W.: *On non-Abelian group difference sets.* Discrete Math. 112, 93–102 (1993).

[4] GAP Group: *Groups, Algorithms and Programming, Version 4. 4. 6.* Retrieved on July 30 2009 from: http://www.gap-system.org/Download/index.html.

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

[6] Iiams, J. E.: *Lander's Tables are complete.* Difference sets, sequences and their correlation properties. Kluwer, 239–257 (1999).

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

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

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

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

[11] Leung, K. H., Ma, S. L., and Schmidt, B.: *Non-existence of abelian sets: Lander's conjecture for prime power orders.* American Mathematical Society 356(11), 43–58 (2003).

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

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

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

[15] Osifodunrin, A. S., and Smith, K. W.: *On the existence of (160, 54, 18) difference sets*, to appear.

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

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

[18] Smith, K. W.: *Non-Abelian Hadamard Difference sets.* J. Comb. Theory A, 144–156 (1995).

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