Journal of the Nigerian Association of Mathematical Physics
Volume **15 (November, 2009), pp 13 - 26**

Class of intersection numbers of a homomorphic image in the study of difference sets with order 49

Adegoke S. Osifodunrin
Department of Mathematics,
University of Lagos, Lagos, Nigeria

Abstract

The investigation of (v,k,λ) ***difference sets involves the computation of intersection numbers of homomorphic images of the underlying group. Up to compliments, there are fifteen difference set parameters with order 49 but only three of these parameter sets, namely,* (400, 57, 8), (280, 63, 14) and (220, 73, 24) *satisfy v* ≡ 0 *mod* 20. *In this paper, we demonstrate how to construct difference set images for these parameter sets in Frobenius group of order* 20, *Frob(*20). *We also conclude that if Gis a group of order 220 with factor group H that is isomorphic to Frob(*20) *then Gdoes not admit* (220, 73, 24) *difference sets.***

Keywords
Difference sets, symmetric designs, affine plane, representations and groups

AMS subject classifications: 05B10 and 05B20

1.0 Introduction

Let G be a multiplicative group of order v. A k-subset D of G, is a (v,k,λ) difference set if every non-identity element, g, of the group can be reproduced exactly λ times by the multi-set $\{g = d_1 d_2^{-1} : d_1, d_2 \in D, d_1 \neq d_2, g \in D\}$. The natural number $n := k - \lambda$ is called the order of the difference set. Usually, we say that D is abelian (resp. non abelian or cyclic) difference set if the underlying group G is abelian (resp. non abelian or cyclic). Difference sets are closely associated with many fields of study and its strength lies in the combination of various techniques ranging from algebraic number theory to geometry, algebra and combinatorics [3].

The study of difference sets dates back to Paley [8] and Singer [10], also introduced them while working on symmetric designs obtained from points and hyperplanes of a finite projective geometry. Singer showed that for any two points (hyperplanes) there is a unique element of the group that maps one of the points (hyperplanes) to the other. Such groups are said to act regularly on points (hyperplanes) and are nowadays known as Singer groups.

e-mail address: asa_osifodunrin @ yahoo.com

Nowadays, the most popular method of investigating difference sets is the use of characters which were developed by Yamamoto [12] and Turyn [13]. The relationship between symmetric designs and difference sets is that a symmetric design admitting a group, G, as a regular automorphism group is isomorphic to the development of the difference set (Theorem 4.2, [4]). Since the development of a difference set yields a symmetric design, consequently difference sets are useful in the construction of symmetric designs. In this paper, we combine methods in geometry and representation theory to obtain difference set images in a factor group of group G, $|G| = 220, 280 \text{ or } 400$. Section 2 gives background information required for this work while Section 3 is an exposition of the group $Frob(20)$. Section 4 explains the methodology while Section 5 discusses the results. Ionin and Shrikhande [2], Lander [4] and Pott [9] give a good background information on difference sets.

2.0 Preliminary work

We discuss the basic information required for this work.

2.1 Difference sets

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

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

Let D be a (v,k,λ) difference set in a group G of order v and $\varphi: G \to H$ is a homomorphism with kernel N. The contraction of D (also called the difference set image in H) with respect to the kernel N is the multi-set $D/N = \{dN : d \in D\}$. If $T^* = \{1 = t_0, t_1, t_2, \text{K}, t_h\}$ is a left transversal of N in G, then $D/N = \sum_{t_i \in G} d_i t_i N$ and 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 $\varphi(D)$, the difference set image in a homomorphic image of G and denote the number of times d_i equals i by $m_i \geq 0$. The notation $\Omega_{G/N}$ represents the set of inequivalent difference set images in the factor group G/N. The following result is very useful in the study of difference sets.

***Lemma* 2.1**

Suppose that D is a (v,k,λ) difference set in a group G and N, a normal subgroup of G. Suppose that $\varphi: G \to G/N$ is a natural epimorphism. Then

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

(ii) $\sum_i d_i^{\,2} = n + \lambda |N|$

Lemma 2.1 enables us to search for difference sets image in factor groups of group G by solving equation (*i*). A counting argument can be used to prove the following lemma.

***Lemma* 2.2** (Variance trick)

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

$$\sum_{i=0}^{|N|} m_i = |H| \tag{2.2}$$

$$\sum_{i=0}^{|N|} i m_i = k \tag{2.3}$$

$$\sum_{i=0}^{|N|} i(i-1)m_i = \lambda(|N|-1) \tag{2.4}$$

2.2 A little about Designs

We briefly explore the connection between difference sets and a special type of design, called symmetric design. An incidence structure X = (*P*,*B*,*I*) is a system consisting of a set of points *P* and a set of blocks *B* with a binary relation *I* that gives the incidence relation. In particular, if the size of *P* is *v*, |*B*| = *b*, where distinct points of *P* are arranged such that each block is incident with *k* points, each point is incident with *r* (known as **replication** number) distinct blocks and every pair of points is incident with λ blocks, then we obtain a (*v*,*b*,*r*,*k*,*λ*) -design with parameters $v>1$, b being positive integers and r, k and λ are non-negative integers. If $v>1$, then the order of the (*v*,*b*,*r*,*k*,*λ*) -design is $n=r-\lambda\geq 0$. The basic equations of designs are(*v*,*b*,*r*,*k*,*λ*). One example of incidence structure is the symmetric design. This is a (*v*,*b*,*r*,*k*,*λ*) -design in which $b=v$ or $r=k$. Difference sets are known to be related to symmetric design in that the development of a difference set yields a symmetric design [4]. Another example of incidence structure is the affine plane. Suppose that *P* is the set of points and *B*, the class of subsets of *P* called lines. Then the pair (*P*,*B*) is called an affine plane if the following axioms are satisfied:

(A1) Two distinct points lie on a unique line.

(A2) For any point *x* and any line, *N* not on this point, there is a unique line, *M*, containing *x* and does not intersect *N*.

(A3) There is a set of three points which are not on a common line (existence of a triangle).

If we perceive P as a vector space of dimension m over a field, F of q elements then we denote the affine plane as $AG(m, q)$, otherwise we write $AG(m, F)$. Furthermore, two lines L and M are parallel $(L \| M)$ if $L=M$ or $L\cap M=\phi$. In other words, two lines are parallel if and only if they have the same slope. The relation on the set of lines of an affine plane is called "parallelism" and it is an equivalence relation. For any finite affine plane $AG(m, q)$ with $m\geq 2$, every line consists of exactly n points, every point lies on exactly $n+1$ points, every points lies on exactly $n+1$ lines. Also, $AG(m, q)$ has exactly n^2 points, n^2+n lines and $n+1$ parallel

classes. It has been proved that affine plane of order q exists for every prime power q. An affine plane of order m is a $2-(m^2, m, 1)$ design and conversely, for $m \geq 2$, any $2-(m^2, m, 1)$ design is an affine plane. The proof of this result can be found in Ionin and Shrikhande ([2], Prop. 3.2.13, page 63).

2.3 Representation theory

Suppose that K is the field of real or complex numbers. Then a representation of a group G is a homomorphism, $\chi : G \to GL(n, K)$, where $GL(n, K)$ is the group of invertible $n \times n$ matrices over K and n, a positive integer, is the degree of χ. This is also known as the K-representation of G. A linear representation (also called character) is a representation of degree one and we denote the group of characters of G by G^*. Every group possesses a principal (trivial) representation χ_0. That is, $\chi_0(x) = I_n$ for all $x \in G$. In this case, the kernel is the whole group. A faithful character is the character whose kernel is the identity. The following orthogonality relations (Pott, [8], Lemma 1.2.1) or Ledermann ([3], Chapter 2) explicitly summarizes a basic property of characters.

***Lemma* 2.4** (Orthogonality relations)

Let G be an abelian group of order v and exponent v^*. If the field K contains a primitive v^*th root of unity and characteristic of K and v are relatively prime, then for all characters of G,

$$\chi(G) = \begin{cases} |G| & if \quad \chi = \chi_0 \\ 0 & if \quad \chi \neq \chi_0 \end{cases} \quad \text{and} \quad \sum_{\chi \in G^*} \chi(g) = \begin{cases} |G| & if \quad g = 1 \\ 0 & if \quad g \neq 1 \end{cases}$$

By this lemma, it easy to show that if χ is any non trivial character of G, where $\chi(D) \in Z[\zeta]$, ζ, is a primitive root of unity, then $\chi(D)\overline{\chi(D)} = n \cdot I_n + \lambda\chi(G) = n \cdot I_n$. We extend this fact to $\hat{D}$ as follows:

***Lemma* 2.5**

Let φ be an epimorphism of a finite group G with kernel N and D be a difference set in the group. Then $\chi(\hat{D})\overline{\chi(\hat{D})} = n \cdot 1_m$ where χ is a non-trivial representation of G/N of order m which does not have χ_0 as a constituent.

Let m be the exponent of an abelian group, G with ξ the primitive m-th root of unity and K, a field containing ξ then $K := Q(\xi)$ is the splitting field for G. Without loss of generality, we may replace K with C, the set of complex numbers. Thus, the central primitive idempotents in $C[G]$ is

$$e_{\chi_i} = \frac{\chi_i(1)}{|G|} \sum_{g \in G} \chi_i(g) g^{(-1)} = \frac{1}{|G|} \sum_{g \in G} \overline{\chi_i(g)} g \qquad (2.5)$$

where, χ_i is an irreducible character of G and $\{e_{\chi_i} : \chi_i \in G^*\}$ is a basis for $C[G]$. Let G be an abelian group then every element $A \in C[G]$ can be expressed uniquely by its image under the character $\chi_i \in G^*$. That is, $A = \sum_{\chi_i \in G^*} \chi_i(A) e_{\chi_i}$ and consequently, $\chi_i(A) e_{\chi_i} = A e_{\chi_i}$. It then

follows that if $A \in C[G]$, then $A = A\sum_{\chi_i \in G^*} e_{\chi_i} = \sum_{\chi_i \in G^*} Ae_{\chi_i} = \sum_{\chi_i \in G^*} \chi(A)e_{\chi_i}$. This brings us to an essential instrument, called an alias that is an interface between the values of group rings and combinatorial analysis. Aliases are members of group ring. Let G be an abelian group and $\Omega = \{\chi_0, \chi_1, \chi_2, \mathrm{K}, \chi_h\}$, a set of characters of G. The element $\beta \in Z[G]$ is known as Ω-alias if for $A \in C[G]$ and all $\chi_i \in \Omega$, $\chi_i(A) = \chi_i(\beta)$. Primitive idempotents give rise to

rational idempotents as follows: If K is the Galois over Q, the set of rational numbers, then **central rational idempotents** in $Q[G]$ are obtained by summing over the equivalence classes X_i on the e_{χ_i}'s under the action of the Galois group of K over Q. That is, $[e_{\chi_i}] = \sum_{e_{j_i} \in \mathrm{X}_i} e_{\chi_j}$, $i = 1, \mathrm{K}, s \le h$. This yields the general formula employed in the search of difference set [8].

***Theorem* 2.1**

Let G be an abelian group and K a field of characteristic 0. Suppose that $G^*/\sim$ is the set of equivalence classes of characters with $\{\chi_0, \chi_1, \chi_2, \mathrm{K}, \chi_s\}$ a system of distinct representatives for the equivalence classes. If $A \in K[G]$, then

$$A = \sum_{i=0}^{s} \alpha_i [e_{\chi_i}] \tag{2.6}$$

where α_i is any χ_i-alias for A. (2.6) is known as the **rational idempotent decomposition** of A. For example, if G is a cyclic group of the form $C_{p^m} = \left\langle x : x^{p^m} = 1 \right\rangle$ (p is prime) whose characters are of the form $\chi_i = \xi^i, i = 0, 1, \mathrm{K}, m-1$ then the rational idempotents are

$$[e_{\chi_0}] = \frac{1}{p^m}\langle x \rangle, \text{ and } 0 \le j \le m-1 \tag{2.7}$$

$$[e_{\chi_{p^j}}] = \frac{1}{p^{j+1}}\left(p\left\langle x^{p^{m-j}} \right\rangle - \left\langle x^{p^{m-j-1}} \right\rangle\right). \tag{2.8}$$

The following lemma gives information about the character value of $\chi(D)$.

***Lemma* 2.6**

Suppose that G is group of order v with normal subgroup N such that G/N is abelian. If $\hat{D} \in Z[G/N]$ and $\chi \in (G/N)^*$ then

$$|\chi(\hat{D})| = \begin{cases} k, & \text{if } \chi \text{ is principal character of } G/N \\ \sqrt{k-\lambda} & \text{otherwise} \end{cases}$$

A nice way to study difference sets is to use representation theoretic method made popular by Leibler [7] . This approach entails obtaining the comprehensive list $\Omega_{G/N}$, of difference set image distribution in homomorphic images of G, of least order. We garner information about D as we gradually increase the size of the homomorphic image. If at a point the distribution list $\Omega_{G/N}$ is empty then this signifies non-existence. In obtaining this list, $\Omega_{G/N}$, we use Lemmas 2.5, 2.6 and the difference set equation (2.6). In some situation, computation of difference set image requires

the knowledge of the alias which involves knowing how to factor the ideal generated by $\chi(\hat{D})$ in the cyclotomic ring $Z[\xi_m]$, ξ_m is the m-th root of unity and m is the exponent of G/N. In this paper, if χ is not a principal character of Frob(20) then $|\chi(\hat{D})|=7$. We need to know how the ideal generated by 7 factors in $Z[\xi_4]$. Interestingly, the ideal generated by 7 is prime in $Z[\xi_m], m=2,4$. By a theorem due to Kronecker that states that any algebraic integer all whose conjugates have absolute value 1 must be a root of unity, we conclude that $\chi(\hat{D})=\pm 7\xi_4^j$, $j=0,1,2,3$. We use this information to obtain the difference set image in cyclic group C_4 for the difference sets with parameters (400, 57, 8).

Suppose that $(G/N)\cong C_4=\langle x:x^4=1\rangle$. Let the group ring element $\hat{D}=\sum_{j=0}^{3} d_j x^j$. We view this group ring elements as a 1×4 matrix with columns indexed by powers of x and the characters of G/N are of the form $\chi_j=\xi_4^j=i^j$, $j=0, 1, 2, 3$. The primitive idempotents are listed below:

$$e_{\chi_0}=\frac{1}{4}(1+x+x^2+x^3)=\frac{1}{4}\langle x\rangle;\quad e_{\chi_2}=\frac{1}{4}(1-x+x^2-x^3)$$

$$e_{\chi_1}=\frac{1}{4}(1-ix-x^2+ix^3);\quad e_{\chi_3}=\frac{1}{4}(1+ix-x^2+ix^3)$$

The idempotents e_{χ_1} and e_{χ_3} are algebraic conjugates, so they belong to the same equivalence class and $[e_{\chi_1}]=e_{\chi_1}+e_{\chi_3}=\frac{1}{2}(1-x^2)$. Hence using (2.7) and (2.8) the rational idempotents are: $[e_{\chi_0}]=\frac{1}{4}\langle x\rangle$, $[e_{\chi_2}]=\frac{1}{4}\langle x^2\rangle(1-x)$ and $[e_{\chi_1}]=\frac{1}{2}(1-x^2)$, The difference set equation, using (2.3.2) is

$$\hat{D}=\alpha_{\chi_0}[e_{\chi_0}]+\alpha_{\chi_1}[e_{\chi_1}]+\alpha_{\chi_2}[e_{\chi_2}] \qquad (2.9)$$

We know that $\chi_j(\hat{D})\overline{\chi_j(\hat{D})}=49$, $\chi_0(\hat{D}), \chi_2(\hat{D})\in Z$ and $\chi_1(\hat{D}), \chi_3(\hat{D})\in Z[i]$. In fact, $\chi_0(\hat{D})=57$, $\chi_2(\hat{D})=\pm 7$ and $\chi_1(\hat{D}), \chi_3(\hat{D})\in\{\pm 7,\pm 7i^j\}$, $j=0,1,2,3$. By choosing representatives of the solution sets $\chi_0(\hat{D})=57$, $\chi_2(\hat{D})=\pm 7$ and $\chi_1(\hat{D})=\{7,7i\}$. Consequently, the aliases are $\alpha_{\chi_0}=57, \alpha_{\chi_1}=7x^j$, $j=0,1,2,3$ *and* $\alpha_{\chi_2}=\pm 7$. Therefore, (2.9) becomes $\hat{D}=\frac{57}{4}\langle x\rangle\pm\frac{7}{4}\langle x\rangle(1-x)+\frac{7}{2}x^j(1-x^2)$. By translating (if necessary), the difference image in C_4 is $[9, 16, 16, 16]$ or $-7+16\langle x\rangle$. Similarly, the C_4 image for the other parameters are: (a) (220, 73, 24): $-7+20\langle x\rangle$ (b) (280, 63, 14): $7+14\langle x\rangle$. This information will be useful in sections 4 and 5.

3.0 The Frobenius group of order 20, Frob(20)

3.1 Preamble

We assume that some groups of order 400 have (400, 57, 8) difference sets and consequently, we look at their quotient group that is isomorphic to H, Frobenius group of order 20. The Frobenius groups are finite groups with non trivial normal subgroup N (known as Frobenius kernel) and a non trivial subgroup K, called Frobenius complement such that for each $t \in H/N$ there is a unique $s \in N$ with $t \in sKs^{-1}$ and $\gcd(|N|,|K|)=1$. The presentation of $H = \langle x, y : x^5 = y^4 = 1,\ yxy^{-1} = x^2 \rangle$ and its derived group, H', is a Sylow 5-subgroup. Notice that $H' \cong C_5$ and $H/H' \cong C_4$ with centre $C(H) = \{1\}$. Let $\hat{D} = \sum_{j=0}^{4}\sum_{k=0}^{3} d_{jk} x^j y^k$ be the difference set image in H. We perceive this group ring, $Z[H]$ element as a 4×5 matrix with rows indexed by powers of y and columns indexed by powers of x or

$$\hat{D} = \begin{bmatrix} d_{00} & d_{10} & d_{20} & d_{30} & d_{40} \\ d_{01} & d_{11} & d_{21} & d_{31} & d_{41} \\ d_{02} & d_{12} & d_{22} & d_{32} & d_{42} \\ d_{03} & d_{13} & d_{23} & d_{33} & d_{43} \end{bmatrix}$$

The coefficients of $x^j y^k$ are integers with $0 \le d_{jk} \le 20$ and subscripts of d_{jk} indicate the exponents of x *and* y and also the row $(k+1)$, $k = 0, 1, 2, 3$ and column $(j+1)$, $j = 0, 1, 2, 3, 4$ of the $\hat{D}$. Take $K = \langle y \rangle$. Since $H/H' \cong C_4$, H has four linear representations (characters) and one irreducible representation of degree four. The representation of degree four is induced by the faithful characters of $\langle x \rangle$. The linear representations are defined by $\chi_j(x) = 1,\ \chi_j(y) = i^j,\ j = 0, 1, 2, 3$ while the degree four representation is:

$$\chi' : x\,\alpha \begin{pmatrix} \xi_5 & 0 & 0 & 0 \\ 0 & \xi_5^2 & 0 & 0 \\ 0 & 0 & \xi_5^4 & 0 \\ 0 & 0 & 0 & \xi_5^3 \end{pmatrix} \qquad y\,\alpha \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

and ξ_5 is the fifth root of unity.

Unlike the usual case, we shall avoid carrying out our computation in $Q(\xi_5)$, the minimal splitting field of χ', by creating integral representations which are not unitary but equivalent to χ'. The Frobenius complement $\langle y \rangle$ is a Sylow 2-subgroup of H. Let $\{1, x, x^2, x^3, x^4\}$ be a left transversal of Sylow 2-subgroup of H, then we induce the trivial representation of this Sylow 2-subgroup to get integral-valued representation. This representation is equivalent to $\chi_0 \oplus \chi'$ and defined explicitly as:

$$\chi : x\ \alpha \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}, y\ \alpha \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} \tag{3.1}$$

3.2 The Background Work on Frob(20)

Let I denote a 5 by 5 identity matrix and J the corresponding matrix whose entries are one. Suppose that a (400, 57, 8) difference set, D exist in group G of order 400 then

$$DD^{(-1)} = 49 \cdot I_G + 8 \cdot G \tag{3.2}$$

Thus, the image of this difference set in H satisfies (χ is permutation representation (3.1) of H)

$$\begin{aligned} \chi(\hat{D})\overline{\chi(\hat{D})} &= 49 \cdot I + 8 \cdot \chi(G) \\ &= 49 \cdot I + 8 \cdot 20 \cdot \chi(H) \\ &= 49 \cdot I + 640J \end{aligned} \tag{3.3}$$

where, $\chi(G) \neq 0$ since his representation has the trivial representation in its constituent. Notice that $\chi(H) = 4J$ and $\chi(\hat{D})J = 57J$. Set $M = \chi(\hat{D}) - aJ$, a is an integer. As (3.3) does not satisfy orthogonality relations (see Lemma 2.4), we need to find the value of a such that $(\chi(\hat{D}) - aJ)\overline{(\chi(\hat{D}) - aJ)} = 49 \cdot I + \mu \cdot J$ with μ a small integer, possibly zero. To achieve this, we multiply out the left hand side of the last equation, to get $\chi(\hat{D})\overline{\chi(\hat{D})} - a\chi(\hat{D})J - aJ\overline{\chi(\hat{D})} - a^2J^2 = 49 \cdot I + (640 - 114a + 5a^2)J$. Since we need μ as small as possible, we choose $\mu = 0$, so that $640 - 114a + 5a^2 = 0$. Using the quadratic formula, we get $a = \frac{114 \pm 14}{10}$. But a must be an integer and we choose $a = 10$. Thus, $M = \chi(\hat{D}) - 10J$ and $M\overline{M} = 49 \cdot I$. Consequently, $MJ = \chi(\hat{D})J - 10J^2 = 7J$. Since $MM^t = 49I$ then $\left(\frac{1}{7}M\right)\left(\frac{1}{7}M^t\right) = I$, and $\left(\frac{1}{7}M\right)$ and $\left(\frac{1}{7}M^t\right)$ are inverses of each other. Using the results that states that matrices A and B are inverses if and only if *AB* = 1 and *BA* = 1, we conclude that $M^tM = 49 \cdot I$ In this situation, the columns of M also preserves the properties of the rows and *JM* = 7*J*. By a similar approach, we obtain information about the other two parameter sets as follows:

(220, 73, 24): If *G* is a group of order 220 and $\hat{D}$ is the difference image set in *H* then $\chi(\hat{D})\overline{\chi(\hat{D})} = 49 \cdot I + 1056 \cdot J$. In this case, $\chi(\hat{D})J = 73 \cdot J$, $a = 16$ and *JM* = *MJ* = -7*J*.

(280, 63, 14): If G is a group of order 280 and $\hat{D}$ is the difference image set in H then $\chi(\hat{D})\overline{\chi(\hat{D})} = 49 \cdot I + 784 \cdot J$. In this case, $\chi(\hat{D})J = 63 \cdot J$, $a = 14$ and *JM* = *MJ* = -7*J*.

For each of these parameter sets, suppose $(x_0 \quad x_1 \quad x_2 \quad x_3 \quad x_4)$ is a row(column) vector in M then the above conditions indicate that inner product of this row(column) by itself is

$$x_0^2 + x_1^2 + x_2^2 + x_3^2 + x_4^2 = 49, \tag{3.4}$$

and row(column)sum, $\sum_i x_i = 7$ or -7. However, if row (column) sum is 7 we only need to multiply the entries of the row (column) by $-1$to make the row (column) sum -7. Hence we shall concentrate on $\sum_i x_i = 7$. A careful consideration of the constraints shows that the row (column) of M will be generated by vectors (up to permutation)

$\underset{\sim}{a}_1 = (7 \quad 0 \quad 0 \quad 0 \quad 0), \underset{\sim}{a}_2 = (6 \quad 3 \quad -2 \quad 0 \quad 0)$,

$\underset{\sim}{a}_3 = (6 \quad 2 \quad 2 \quad -2 \quad -1), \underset{\sim}{a}_4 = (4 \quad 4 \quad 3 \quad -2 \quad -2), \underset{\sim}{a}_5 = (4 \quad -4 \quad 3 \quad 2 \quad 2).$

Since there are five distinct vectors, then there are $2^5 - 1 = 31$ways to use these vectors to construct M. Thus,

***Lemma* 3.1**

Let M be a 5 by 5 matrix with integer entries such that $JM = MJ = 7J$ and $MM^t = 49 \cdot I$. Then up to permutation of rows and columns, M is one of the following:

$$M_1 = 7I,\ M_2 = \begin{bmatrix} 7 & 0 & 0 & 0 & 0 \\ 0 & 7 & 0 & 0 & 0 \\ 0 & 0 & 3 & -2 & 6 \\ 0 & 0 & 6 & 3 & -2 \\ 0 & 0 & -2 & 6 & 3 \end{bmatrix},\ M_3 = \begin{bmatrix} -1 & 6 & 2 & -2 & 2 \\ 6 & -1 & 2 & -2 & 2 \\ 2 & 2 & 3 & 4 & -4 \\ -2 & -2 & 4 & 3 & 4 \\ 2 & 2 & -4 & 4 & 3 \end{bmatrix}$$

Proof

We split the five vectors into two categories. Category A consists of $\underset{\sim}{a}_1$ and $\underset{\sim}{a}_2$ while category B contains the remaining vectors. It is easy to see that the vectors in these categories are not orthogonal. This implies that any combination of at least one vector from each of the categories will not yield a viable matrix M. Also, only $\underset{\sim}{a}_1$ can by itself produce a viable matrix. Thus, out of the 31 combinations, only the following could generate a viable M : $\underset{\sim}{a}_1$ only, $\underset{\sim}{a}_1$ and $\underset{\sim}{a}_2$ only, $\underset{\sim}{a}_3$ and $\underset{\sim}{a}_4$ only, $\underset{\sim}{a}_3$ and $\underset{\sim}{a}_5$ only, $\underset{\sim}{a}_4$ and $\underset{\sim}{a}_5$ only and $\underset{\sim}{a}_3$, $\underset{\sim}{a}_4$ and $\underset{\sim}{a}_5$ only. It turns out that $\underset{\sim}{a}_1$ only yields M_1, $\underset{\sim}{a}_1$ and $\underset{\sim}{a}_2$ only generate M_2; $\underset{\sim}{a}_3$, $\underset{\sim}{a}_4$ and $\underset{\sim}{a}_5$ only yield M_3 while others could not produce any viable matrix.

Now, we have good information about M and of course, $\chi(\hat{D})$. Thus, $\chi(\hat{D}) = M_i + 10J,\ i = 1, 2, 3$. Also, for the other parameter sets whose row sum is -7, $\chi(\hat{D}) = -M_i + 14J$ or $-M_i + 16J,\ i = 1, 2, 3$.

4.0 The search for difference set images in H = Frob(20)

We now describe the technique for finding the intersection numbers of H. Frob(20) could be viewed in many ways but our chosen representation χ suggests that we think of this group as a permutation group, $\langle \alpha, \beta \rangle$ with $\alpha = (0 \quad 1 \quad 2 \quad 3 \quad 4)$ and $\beta = (1 \quad 2 \quad 4 \quad 3)$. We can now view this group as a subgroup of S_5, the permutation group on five symbols. In this case, χ represents elements of Frob(20) as 5×5 permutation matrices in four parallel (non horizontal nor vertical) classes,

$$W = \langle \alpha \rangle, W\beta, W\beta^2 \text{ and } W\beta^3.$$

Each of these parallel classes have slopes 1, 2, 4 and 3 respectively in the affine plane with 30 lines, 25 points, 6 parallel classes, 5 points on each line and 6 lines on a point. This characterization of elements of $\langle \alpha, \beta \rangle$ as permutation matrices can easily be extended to the permutations of S_5 acting naturally on the set $\{0, 1, 2, 3, 4\}$ [10]. In view of the problem at hand, we consider a left transversal of this subgroup, $\langle \alpha, \beta \rangle$ of S_5:

$$T = \{\pi_0 = 1, \ \pi_1 = (01), \pi_2 = (234), \pi_3 = (01)(234), \pi_4 = (243), \pi_5 = (01)(243)\}$$

The advantages of choosing this transversal in S_5 are:

* $T = T^{-1}$
* Most of the permutation matrices of elements of T commute with M_j, 1, 2, 3.

Therefore, a matrix equivalent to $\chi(\hat{D})$ (under the row and column permutations) has the form $\chi(\pi_k)\chi(g\hat{D}h)\chi(\pi_l)$, where g and h are elements of Frob(20) while π_k and π_l are in T.

With this correspondence,

$$\chi(g\hat{D}h) = \chi(\pi_k) M_i \chi(\pi_l), \ i = 1, 2, 3. \tag{4.1}$$

We know that if σ is an automorphism of a group H then $g\hat{D}^{\sigma}$ is an equivalent difference set of $\hat{D}$ for $g \in G$. But conjugation is an automorphism, thus $\hat{D}$ is a difference set if and only if $g\hat{D}h$ is a difference set. Therefore, we assume, without loss of generality that the difference set image is of the form

$$\chi(\hat{D}) = \chi(\pi_k) M_i \chi(\pi_l), \ i = 1, 2, 3 \tag{4.2}$$

where $\chi(\pi_k)$ is a permutation matrix corresponding to π_k in T, a representative of coset of $\langle \alpha, \beta \rangle$. This shows that, for each i, (4.2) has 36 choices of matrices for $\hat{D}$ and we attempt to reduce these possibilities as far as we can.

Notice that the matrix $M_1 = 7I$, a scalar matrix, is at the centre of the $Z[S_5]$ so it commutes with all the permutation matrices. Thus, the difference set image is transformed as

$$\chi(\hat{D}) = 10J + M_1 \chi(\pi_l), \ l = 0, 1, 2, 3, 4, 5.$$

To obtain the coset representative that commutes with M_2, we partition M_2 along the columns/rows that have similar entries. Thus,

$$M_2 = \left[\begin{array}{cc|ccc} 7 & 0 & 0 & 0 & 0 \\ 0 & 7 & 0 & 0 & 0 \\ \hline 0 & 0 & 3 & -2 & 6 \\ 0 & 0 & 6 & 3 & -2 \\ 0 & 0 & -2 & 6 & 3 \end{array}\right]$$

This partition suggests that we can permute rows (columns) 0 and 1 or rows (columns) 2, 3, and 4. So, we consider $S_{\{0,1\}} \times S_{\{2,3,4\}}$. This shows that some elements of this subgroup of S_5 commute with M_2. For instance, the permutation matrices of (1), (01), (234), (01)(234), (243) and (01)(243) commute with M_2. Therefore, the 36 choices of matrices reduce to

$$\chi(\hat{D}) = 10J + M_2\chi(\pi_l),\ l = 0, 1, 2, 3, 4, 5.$$

Notice that the structure of entries of matrix M_3 is similar to those of M_2 but only the permutation matrices of (1), (01)(24), (24) and (01) commute with M_3. Furthermore, (1) and (01)(24) are in the same coset while (01) and (24) are in the same coset of $\mathrm{Frob}(20)$. In this case, we have to multiply on the left by permutation matrices of elements in T that do not commute with M_3. Thus, the 36 choices of matrices reduced to $\chi(\hat{D}) = 10J + M_3\chi(\pi_l)$, $k = 0, 2, 3, 4, 5;\ l = 0, 1, 2, 3, 4, 5$. We worked through the 6 + 6 + 30 = 42 matrices by computing the respective line sums for the four out of the six equivalence classes (the other two are assigned zero value). We quickly look at individual cases for each of these three parameter sets:

Case 1: For (400, 57, 8)

Only $M_2\chi(\pi_5), M_3\chi(\pi_1), \chi(\pi_2)M_3\chi(\pi_5), \chi(\pi_3)M_3\chi(\pi_4), \chi(\pi_4)M_3\chi(\pi_3), \quad \chi(\pi_5)M_3\chi(\pi_2)$ and their transpose have desirable pattern and could potentially yield images as we shall see later.

Case 2: For (280, 63, 14)

Only $(-M_2)\chi(\pi_5), (-M_3)\chi(\pi_1), \chi(\pi_2)(-M_3)\chi(\pi_5), \chi(\pi_3)(-M_3)\chi(\pi_4), \chi(\pi_4)(-M_3)\chi(\pi_3)$, $\chi(\pi_5)(-M_3)\chi(\pi_2)$ and their transpose have desirable pattern and could potentially yield images.

Case 3: For (220, 73, 24)

Only M_1 and its transpose have desirable pattern and could potentially yield images.

The question now is how do we construct the corresponding element in $\mathbb{Z}[\mathrm{Frob}(20)]$ for any choice of $\chi(\hat{D})$? To answer this question, note that the rows and columns of the representation χ are indexed by $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ with the coordinates of the 5×5 matrix viewed as points of the affine plane $\mathrm{AG}(2, 5)$. For instance, $\chi(\alpha)$ is the characteristic function of the line $y = x + 1$ while $\chi(\beta)$ is the characteristic function of the line $y = 2x$. In general, $\chi(\alpha^s\beta^t)$ is the characteristic function of the line $y = 2^t x + s$ in $\mathrm{AG}(2, 5)$ and is an injection from the 20 members of $\mathrm{Frob}(20)$ into the 30 lines of $\mathrm{AG}(2, 5)$ missing the horizontal and vertical lines. By this correspondence, each member of $\mathbb{Z}[\mathrm{Frob}(20)]$ is associated with a member of the collection

of functions from the 30 lines of $AG(2,5)$ to Z which assign zero to the horizontal and vertical lines. Thus, the (y, x) coordinates of $\chi(\hat{D}) = \chi(\sum_{g \in Frob(20)} \alpha_g g)$ is the sum of the α_g for all lines g on the point (y, x). Next, we give some vital definitions that depend on Mobius inversion. The purpose is to enable us to invert the map χ and reconstruct $\hat{D}$ in the group ring $Z[Frob(20)]$. Define f to be a function from the lines of an affine plane of order q into the set of integers Z and another function $\hat{f}$ on the points and lines by $\hat{f}(p) := \sum_{L \text{ on } p} f(L)$ and $\hat{f}(L) := \sum_{p \in L} \hat{f}(p)$ respectively. Furthermore we extend f to parallel classes of the plane by defining $f(\Pi) := \sum_{L \in \Pi} f(L)$, where Π is a parallel class with slope j and L is a line in it. Thus, for any fixed line L in a parallel class Π_j,

$$\hat{f}(L) := \sum_{p \in L} \sum_{L' \text{on } p} f(L') = q \cdot f(L) - f(\Pi_j) + \sum_{all \ lines \ on \ L''} f(L')$$

With $k = \sum_{all \ lines \ L'} f(L')$, we can find $f(L)$ using the formula

$$f(L) = \frac{\hat{f}(L) - k + f(\Pi_j)}{q} \tag{4.3}$$

if $\hat{f}(L)$ and $f(\Pi_j)$ are known.

In considering our specific case, the members of $Frob(20)$ are the non- vertical nor horizontal lines and the six parallel classes are the four cosets of $W = \langle \alpha \rangle$ along with the 5-rows and 5-columns of the matrix. In the case of (400, 57, 8) , the size of our difference set is

57 and $k = \sum_{all \ lines \ L'} f(L') = 57$. From sub-section 2.3, $f(\Pi) = \{9, 16, 16, 16\}$ and the order of the plane is $q = 5$. Thus, for any point p with coordinates (y, x) in the affine plane, $\hat{f}(p)$ is the (y, x) coordinate of the matrix $\chi(\hat{D}_i)$, $i = 1, 2, 3$ while $\hat{f}(L)$ is the sum of the coordinates corresponding to the points of L. Therefore,

$$f(L) = \frac{\hat{f}(L) - 57 + f(\Pi_j)}{5} = \frac{\hat{f}(L) + f(\Pi_j) + 3}{5} - 12 \tag{4.4}$$

Furthermore, since $f(L)$ is the cardinality of the intersection of $\hat{D}$ and any coset of N and it must be non-negative integer not more than 20, then $(\hat{f}(L) + f(\Pi_j) + 3) \equiv 0 \bmod 5$ and $-10 \le \hat{f}(L) + f(\Pi_j) + 3 \le 90$. This constraint severely restricts the possible values of

$f(L)$ and the 42 choices of matrices reduced to six (as stated earlier) since the lines L of the affine plane such that $f(L)$ is negative integer or fraction is discarded. In summary, if $f(\Pi) = \{9, 16, 16, 16\}$ then only the matrices $M_2\chi(\pi_5), M_3\chi(\pi_1), \chi(\pi_2)M_3\chi(\pi_5)$, $\chi(\pi_3)M_3\chi(\pi_4), \chi(\pi_4)M_3\chi(\pi_3), \chi(\pi_5)M_3\chi(\pi_2)$ and their transposes can possibly generate homomorphic images of difference set in $\mathrm{Frob}(20)$. For (280, 63, 14), if $f(\Pi) = \{21, 14, 14, 14\}$ then only the matrices $(-M_2)\chi(\pi_5)$, $(-M_3)\chi(\pi_1)$, $\chi(\pi_2)(-M_3)\chi(\pi_5)$, $\chi(\pi_3)(-M_3)\chi(\pi_4)$, $\chi(\pi_4)(-M_3)\chi(\pi_3)$, $\chi(\pi_5)(-M_3)\chi(\pi_2)$ matrices and their transposes can possibly generate homomorphic images of difference set in $\mathrm{Frob}(20)$. Finally, for (220, 73, 24) with $f(\Pi) = \{13, 20, 20, 20\}$, only $-M_1$ and its transpose are likely to yield homomorphic images of the difference set in $\mathrm{Frob}(20)$.

5.0 The results

We conclude with examples that illustrate the use of information in section 4 to obtain difference set images in $\mathrm{Frob}(20)$. That is, we assume that N is an appropriate normal subgroup of a group G such that $\mathrm{G/N} \cong \mathrm{Frob}(20)$, where G is any group of order 220, 280 or 400.

5.1 The case $G/N \equiv$ Frob(20) with $|G| = 400$

We take $M_2\chi(\pi_5)$ and

$$\chi(\hat{D}) = 10J + M_2\chi(\pi_5) = \begin{bmatrix} 10 & 17 & 10 & 10 & \underline{10} \\ \underline{17} & 10 & 10 & 10 & 10 \\ 10 & \underline{10} & 16 & 13 & 8 \\ 10 & 10 & \underline{8} & 16 & 13 \\ 13 & 13 & 13 & \underline{8} & 16 \end{bmatrix}$$

The values of $\hat{f}(L)$ (sum of weights on a line) are given in Table 1, according to the parallel classes.

Table 1

Slope 1	Slope 3	Slope 4	Slope 2
68	46	51	56
53	56	56	46
48	56	56	51
53	61	51	56
53	66	71	66

Table 2

Slope 1	Slope 3	Slope 4	Slope 2
45	73	73	73
80	73	73	73
80	73	73	73
80	73	73	73
80	73	73	73

For instance, if we consider the line $y = x + 1$ of slope 1, the weights associated with points on this line are 17, 10, 8, 8 and 10. These are the underlined values in $\chi(\hat{D})$. Thus,

$\hat{f}(L)=17+10+8+8+10=53$ (the bold value in Table 1 under column -Slope 1). Using (4.4), $\hat{f}(L)-57+f(\Pi_j)\equiv 0 \bmod 5$ and $f(\Pi_j)\in f(\Pi)=\{9,16,16,16\}$, we choose $f(\Pi_j)=9$. In this case, $f(L)=1$ (This is the underlined value in A_1). By repeating this procedure several times, we get the image of $\mathrm{Frob}(20)$ corresponding to $M_2\chi(\pi_5)$ as

$$A_1=\begin{bmatrix} 4 & 3 & 0 & 1 & \underline{1} \\ 1 & 3 & 3 & 4 & 5 \\ 2 & 3 & 3 & 2 & 6 \\ 3 & 1 & 4 & 3 & 5 \end{bmatrix}.$$

This turns out to be the only viable image in $\mathrm{Frob}(20)$ as the rest of the potential matrices contain a negative value but intersection numbers must be non-negative. The information in this subsection will be used to decide the existence or otherwise of (400, 57, 8) difference set images in factor groups H, where H is $\mathrm{Frob}(20)\times \mathrm{C}_2$ or a group with GAP[1] location number [40, 3] (See [7]).

5.2 The case *G/N* ≡ Frob(20) with |*G*| = 220

In this case, only matrix $-M_1$ (and its transpose) is likely to yield difference set image in $\mathrm{Frob}(20)$. Thus,

$$\chi(\hat{D})=16J-M_1=\begin{bmatrix} 9 & 16 & 16 & 16 & 16 \\ 16 & 9 & 16 & 16 & 16 \\ 16 & 16 & 9 & 16 & 16 \\ 16 & 16 & 16 & 9 & 16 \\ 16 & 16 & 16 & 16 & 9 \end{bmatrix}$$

and the values of $\hat{f}(L)$ (sum of weights on a line) are given in Table 2, according to the parallel classes. The values of $f(L)$ are in matrix

$$A_2=\begin{bmatrix} -3 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 \end{bmatrix}$$

But as intersection numbers must be non-negative, it follows that there is no (220, 73, 24) difference set image in $\mathrm{G/N}\cong \mathrm{Frob}(20)$. Consequently, any group, G of order 220 having $\mathrm{Frob}(20)$ as homomorphic image does not admit (220, 73, 24) difference sets. One can use GAP[1] to identify these groups.

5.3 The case *G/N* ≡ Frob(20) with |*G*| = 280

The (280, 63, 14) difference set images in $\mathrm{Frob}(20)$, up to automorphism, are:

$$A_3=\begin{bmatrix}1&2&2&5&4\\1&5&3&3&2\\3&4&4&3&7\\3&1&3&5&2\end{bmatrix},\ A_4=\begin{bmatrix}0&2&5&5&2\\3&2&3&3&3\\2&5&5&2&7\\3&3&3&2&3\end{bmatrix},\ A_5=\begin{bmatrix}2&3&6&5&5\\5&3&3&2&1\\4&3&3&4&0\\3&5&2&3&1\end{bmatrix}$$

Just as in the case of (400, 57, 8) , the above information will be used to decide the existence or otherwise of difference set images in factor groups H where H is $\mathrm{Frob}(20)\times C_2$ or a group with GAP[1] location number [40, 3] (See [7, 8]).

References

[1] GAP-Groups, Algorithms and Programming, Version 4.4. 6 (2006) Retrieved on Jan. 2, 2006 from http://www.gap.gap-system.org

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

[3] D. Jungnickel and A. Pott, Difference sets: Abelian, The CRC Handbook of Combinatorial Designs, C.J. Colbourn and J.H. Dinitz (eds.), CRC Press (1996), 297-307.

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

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

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

[7] A. S. A. Osifodunrin, On the existence of (400, 57, 8) difference sets, to appear

[8] A. S. A. Osifodunrin, In search of (280, 63, 14) difference sets, to appear

[9] R. E. A. C. Paley, On orthogonal matrices, J. Math. and Phys. **12** (1933), 311-320.

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

[11] J. Singer, A theorem in finite geometry and some applications to number theory. Trans. Ame. Math. Soc., **43** (1938), 337- 385.

[12] K. W. Smith, Non-Abelian Difference sets, J.Comb.Theory A(1993) 144-156.

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

[14] K. Yamamoto, Decomposition fields of difference sets, Pacific J. Math. **13** (1963), 337-352.