Note On $(m,\ 2,\ m-1,\ \frac{m-2}{2})$ Relative Difference Sets *

Tao Feng Weisheng Qiu

School of Mathematical Sciences, Peking University, Beijing, China, 100871

Abstract

In this note, we consider relative difference sets with the parameter $(m,\ 2,\ m-1,\ \frac{m-2}{2})$ in a group G relative to a subgroup N. In the splitting case, $G = H \times N$, we give a lower bound for the size of the commutator group H', and we show that H can not have a homomorphic image which is generalized dihedral. In the non-splitting case, we prove that there is no $(2n,\ 2,\ 2n-1,\ n-1)$ relative difference set in a generalized dihedral group of order $4n$, $n > 1$.

Keywords: relative difference set, homomorphic image, commutator group

1 Introduction

A relative (m, n, k, λ)-difference set in a finite group G of order mn relative to a subgroup N of order n is a k-subset R of G such that every element $g \in G \setminus N$ has exactly λ representations $g = r_1 r_2^{-1}$ with r_1, $r_2 \in R$, and no non-identity element of N has such a representation. N is called the forbidden subgroup. R is called abelian (non-abelian) if G is abelian (non-abelian). R is called splitting if N is a direct factor of G. The readers are referred to Pott [7] for a survey on relative difference sets.

In a group G, we denote its identity element by 1_G, and simply write 1 if it is clear from the context. For a subset X (possibly a multi-set) of G, we define $X^{(-1)} = \{x^{-1} \mid x \in X\}$. We identify a subset X of G with the integral group ring element $\hat{X} = \sum_{x \in X} x \in ZG$. See [3], [6] for the standard facts about group rings and character theory.

In this note, we are interested in relative difference sets with the following parameter

$$(m, 2, m-1, \frac{m-2}{2}). \tag{1}$$

*Supported by National Natural Science Foundation of China(10331030).

This class of relative difference sets are of special interest because of their connections with other objects in combinatorial theory, such as negacyclic matrices, generalized balanced weighing matrices (GBW), strongly regular graphs. The existence of splitting (m, 2, m-1, $\frac{m-2}{2}$) relative difference sets in the group $G = H \times N$ relative to N is equivalent to the existence of H-invariant GBW(2, m, m-1) over N. This connection between splitting relative difference sets with GBW was first pointed out by Jungnickel, see [5]. Using this connection, he proved the following result in [5].

Result 1. *Assume the existence of a (m, 2, m-1, $\frac{m-2}{2}$) relative difference set R in the group $G = H \times N$ relative to N, then $m-1$ is a perfect square, and H is non-abelian.*

The following result is from Xiang [11].

Result 2. *Suppose G is abelian, and R is a (m, 2, m-1, $\frac{m-2}{2}$) relative difference set in G. Then the Sylow 2-subgroup of G is cyclic.*

In this note, we give some necessary conditions for groups containing relative difference sets with the parameter (1). In the splitting case, $G = H \times N$ with N the forbidden subgroup, we give a lower bound for the size of the commutator group of H, and we prove that H can not have a homomorphic image which is generalized dihedral. We also show there is no ($2n$, 2, $2n-1$, $n-1$) relative difference set in a generalized dihedral group of order $4n$, $n > 1$.

2 The splitting case

In this section, we fix the following notations: $G = H \times N$ is of order $2m$; R is a splitting relative difference set with the parameter (1) in G relative to N (hence H is non-abelian); $N = \{1, \theta\}$, $o(\theta) = 2$; write $R = A + B\theta$, $A, B \in \mathbf{Z}H$; $|A| = a, |B| = b$. We can assume $R \cap N = \emptyset$ and $a \geq b$ by replacing R with some translate of it if necessary. Now $RR^{(-1)} = (m-1) + \frac{m-2}{2}G$ is equivalent to

$$\begin{cases} AA^{(-1)} + BB^{(-1)} = m - 1 + \frac{m-2}{2}(H-1) \\ AB^{(-1)} + BA^{(-1)} = \frac{m-2}{2}(H-1) \\ A + B = H - 1 \end{cases} \tag{2}$$

An easy computation can show that the parameters satisfy:

$$m - 1 = u^2, a = \frac{u(u+1)}{2}, b = \frac{u(u-1)}{2},$$

where u is an odd positive integer.

For a prime p and a nonzero integer t, if k is the largest integer such that p^k divides t, we will write $p^k||t$. A direct consequence is the following easy lemma which seems to have been ignored in the literature.

Lemma 3. *If R is a splitting $(m, 2, m-1, \frac{m-2}{2})$ relative difference set in a group G, then $2||m$, and m has no prime divisor p such that $p \equiv 3 \mod 4$.*

Proof. Obviously $2|m$. If $4|m$, then $u^2 \equiv -1 \mod 4$, which is impossible. Hence $2||m$. Similarly, if $p \equiv 3 \mod 4$ and $p|m$, then $u^2 \equiv -1 \mod p$, which is again impossible. □

Lemma 3 can be used to give much simplified proofs of results in [11].

Substituting $B = H - A - 1$ into the second equation in (2), we get the following

$$(2A+1)(2A+1)^{(-1)} = (u+1)^2H + u^2 \tag{3}$$

This equation is what we will explore in this section. Throughout this article, we assume that $m > 2$.

2.1 The commutator group H'

Result 1 states that $H' = [H, H] > \{1\}$. In this subsection, we prove the following result which generalizes Result 1 in some cases.

Theorem 4. *If R is a splitting $(m, 2, m-1, \frac{m-2}{2})$ relative difference set in $G = H \times N$ relative to N, $m = 1 + u^2$ with u a positive integer, then $|H'| \geq \frac{u'-1}{2}$, where u' is the largest divisor of u that is self-conjugate mod m.*

Note: We call a prime p self-conjugate mod a nonzero integer n if there is such an integer f that $p^f \equiv -1 \mod n'$, where n' is the largest divisor of n that is coprime with p; an integer t is self-conjugate mod n if each prime divisor of t is self-conjugate mod n.

Proof. Take the natural epimorphism $\rho : H \mapsto K := H/H'$, and extend it to a map from $\mathbf{Z}H$ to $\mathbf{Z}K$ in the natural way. We have

$$(2\rho(A)+1)(2\rho(A)+1)^{(-1)} = (u+1)^2|H'|K + u^2.$$

Since K is abelian, take any non-principle character χ of K,

$$|2\chi(\rho(A)) + 1|^2 = u^2.$$

If $K = \{1\}$, then $H = H'$, $|H'| = m > \frac{u'-1}{2}$. So from now on we assume that $K \neq \{1\}$. A standard argument using the prime ideal decompositions in $\mathbf{Z}[\xi]$, where ξ is a primitive e-th root of unity, $e=\exp(K)$, shows that u' divides $2\chi(\rho(A))+1$, where u' is the largest divisor of u that is self-conjugate $\mod m$. Since u is coprime with $2m$, the inversion formula shows $2\rho(A)+1 = u'\ X + a\ K$ for some $X \in \mathbf{Z}K, a \in \mathbf{Z}$, see [8, p.18, Corollary 1.2.5]. For any non-identity element $k \in K$, we have $(2\rho(A)+1)(1-k) = u'X(1-k)$. The left side has coefficients between $-2|H'|-1$ and $2|H'|+1$. If $2|H'|+1 < u'$, then $2\rho(A)+1 = (2\rho(A)+1)k$. Take any character χ such that $\chi(k) \neq 1$, then $2\chi(\rho(A))+1 = 0$, contradicting the fact $|2\chi(\rho(A))+1|^2 = u^2$. Hence $|H'| \geq \frac{u'-1}{2}$. □

Corollary 5. *If R is a splitting $(m,\ 2,\ m-1,\ \frac{m-2}{2})$ relative difference set in $G = H \times N$ relative to N, $m = 1+u^2$ with $u = p^a$, p a prime, $a \geq 1$, then $|H'| \geq \frac{u-1}{2}$.*

Proof. Notice that $m = u^2+1$, $p^{2a} \equiv -1 \mod m$, hence u is self-conjugate $\mod m$. □

Example. With the same notations as in Theorem 4, we consider the case that $\frac{m}{2}$ is a prime power. For two coprime positive integers n', n, we write $ord_n(n')$ to denote the order of n' in the multiplicative group Z_n^*.

(1) $u = p^a q^b$, p, q are distinct primes, $a \geq 1$, $b \geq 1$, and $\frac{m}{2}$ is a prime power. In this case, at least one of $ord_m(p^a)$, $ord_m(q^b)$ must be even; otherwise $m = 2$. Since $\mathbf{Z}_m^*$ has a unique involution -1, at least one of p^a, q^b, say p^a, must be self-conjugate mod m, hence $|H'| \geq \frac{p^a-1}{2}$.

(2) $u = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$, where $p_1, \cdots, p_s$ are distinct primes, $a_i \geq 1 (1 \leq i \leq s)$, and $\frac{m}{2}$ is a prime power. Similar to the argument in (1), we know that one of the $p_1^{a_1}, p_2^{a_2}, \cdots, p_s^{a_s}$ must be self-conjugate mod m, hence $|H'| \geq \frac{\eta-1}{2}$, where $\eta = min\{p_1^{a_1}, p_2^{a_2}, \cdots, p_s^{a_s}\}$. Except for the case $3||u$, we can conclude directly that $|H'| > 1$.

2.2 Homomorphic images of H

Let's recall the definition of a generalized dihedral group. A generalized dihedral group K is the semidirect product of an abelian group K_1 and $C_2 = \{1, \alpha\}, o(\alpha) = 2$, where the action of α on K_1 is given by taking inverse, i.e. $K = \langle K_1, \alpha\ :\ \alpha^2 = 1, \alpha x \alpha = x^{-1}, \forall x \in K_1\rangle$, written as $K = K_1 \rtimes C_2$.

In this subsection, we show that H can not have a generalized dihedral group as its homomorphic image. We need the following result.

Proposition 6. *Suppose K is a generalized dihedral group, $K = K_1 \rtimes C_2$, $C_2 = \{1, \alpha\}, o(\alpha) = 2$. $R \in ZK$ satisfies $RR^{(-1)} = n + \lambda K$, with n being a positive integer. Write $R = E_1 + E_2\alpha$, $E_1, E_2 \in ZK_1$. Let K_1^* be the* *character group of K_1, and χ_0 be the principle character of K_1. Then we have the following:*

(1)$E_1E_1^{(-1)} + E_2E_2^{(-1)} = n + \lambda K_1$, $E_1E_2 = \frac{\lambda}{2}K_1$.

(2) Assume that n is a square, say $n = u^2$. Set $E_1^* = \{\chi \in K_1^* \setminus \{\chi_0\} : |\chi(E_1)| = u\}$, $E_2^* = \{\chi \in K_1^* \setminus \{\chi_0\} : |\chi(E_2)| = u\}$, then E_1^*, E_2^* form a partition of $K_1^* \setminus \{\chi_0\}$.

The proof is simple and we omit it. Now, we are in a position to prove our claim.

Theorem 7. *If R is a splitting $(m, 2, m-1, \frac{m-2}{2})$ relative difference set in $G = H \times N$ relative to N, then H can not have a homomorphic image which is generalized dihedral.*

Proof. Suppose there is a normal subgroup H_1 of H such that $K := H/H_1$ is generalized dihedral, i.e. $K = K_1 \rtimes C_2$ for some abelian group K_1, and $C_2 = \{1, \alpha\}, o(\alpha) = 2$. Take the natural epimorphism $\rho : H \mapsto K$ and extend it to a map from $\mathbf{Z}H$ to $\mathbf{Z}K$ in the natural way. Let χ_0 be the principle character of K_1. Recall our notations at the beginning of this section: $R = A + B\theta$, $A, B \in \mathbf{Z}H$, and $N = \{1, \theta\}$. Write $\rho(A) = A_1 + A_2\alpha$, A_1, $A_2 \in \mathbf{Z}K_1$, then from Equation (3) we have

$$(2\rho(A) + 1)(2\rho(A) + 1)^{(-1)} = (u + 1)^2|H_1|K + u^2,$$

where u is an odd positive integer such that $m = 1 + u^2$. Set $R = 2\rho(A) + 1$, $E_1 = 2A_1 + 1$, $E_2 = 2A_2$. Then R, E_1, E_2 correspond to those in Proposition 6. We define E_i^* $(i = 1, 2)$ in the same fashion as in Proposition 6. We show $E_2^* = \emptyset$; otherwise, there is a $\chi \in K_1^*$ such that $|\chi(2A_2)|^2 = u^2$. Then $\frac{u^2}{4}$ is both a rational integer and an algebraic integer, hence an integer, contradicting that u is odd. From $E_2^* = \emptyset$, we have that $A_2 = r\,K_1$ for some $r \in \mathbf{Z}$. Let χ_0 be the principle character of K_1, and assume $\chi_0(E_1) = x$, $\chi_0(E_2) = y$. We have $x + y = 2\frac{u(u+1)}{2} + 1 = u^2 + u + 1$, $y = 2r|K_1|$. From Proposition 6 (1), we can deduce that $x = \frac{1+u^2}{2} = \frac{m}{2}$, $y = \frac{m}{2} + u$. Hence $|K_1|$ divides $y = \frac{m}{2} + u$. But $|K_1|$ is a divisor of $\frac{m}{2}$, it follows that $|K_1|$ divides u, contradicting that $(m, u) = 1$. □

3 The non-splitting case

Suppose G is a generalized dihedral group of order $4n$, $n > 1$, $G = K \rtimes C_2 = \langle K, \alpha \ : \alpha^2 = 1, \alpha x \alpha = x^{-1}, \forall x \in K\rangle$, where K is abelian, $C_2 = \{1, \alpha\}$. In this section, we show that there is no $(2n, 2, 2n-1, n-1)$ relative difference set in G relative to a subgroup N. We consider the following two cases .

The first case. N is a subgroup of K of order 2. Suppose that R is a (2n, 2, 2$n-1$, $n-1$) relative difference set in G relative to N. Write $R = A + B\alpha$, where $A, B \in \mathbf{Z}K$. Then $RR^{(-1)} = 2n - 1 + (n-1)(G - N)$ is equivalent to

$$AA^{(-1)} + BB^{(-1)} = 2n - 1 + (n-1)(K - N), 2AB = (n-1)K.$$

Let χ_0 be the principle character of K. Set $a = |A|, b = |B|$, and suppose $a \leq b$ without loss of generality. It is easy to see that $a = n - 1, b = n$. Define four sets as follows: $A_1^* = \{\chi \in K^* : |\chi(A)| = 1$, χ is trivial on $N\}$, $A_2^* = \{\chi \in K^* : |\chi(A)|^2 = 2n - 1$, χ is nontrivial on $N\}$; B_1^*, B_2^* are defined in a similar fashion with B in place of A. Let a_1, a_2, b_1, b_2 be the sizes of the four sets defined above. It is easy to see that the four sets form a partition of $K^* \setminus \{\chi_0\}$, and A_1^*, B_1^* form a partition of the nontrivial characters of K which are principle on N. The following relations are restatements of these facts:

$$a_1 + a_2 + b_1 + b_2 = 2n - 1; a_1 + b_1 = n - 1.$$

The coefficient of 1 in $AA^{(-1)}$ is $n - 1 = \frac{1}{2n}[a_1 + (2n-1)a_2 + (n-1)^2]$. Hence $a_1 + (2n-1)a_2 = n^2 - 1$. Since $0 \leq a_1 \leq n - 1$, we have $\frac{n-1}{2} < \frac{n^2-n}{2n-1} \leq a_2 \leq \frac{n^2-1}{2n-1} < \frac{n+1}{2}$. But $2AB = (n-1)K$ indicates that n is odd, a contradiction. We have thus proved

Theorem 8. *Suppose G is a generalized dihedral group of order $4n$, $n > 1$, $G = K \rtimes C_2$, where K is abelian, $C_2 = \{1, \alpha\}$, $o(\alpha) = 2$. N is a subgroup of K of order 2. Then no relative difference set with the parameter (2n, 2, 2n-1, n-1) relative to N exists in G .*

The second case. N is a subgroup of G not contained in K. Then $G = K \rtimes N$, and we can assume that $N = C_2$. Suppose that R is a relative difference set with the parameter $(2n, 2, 2n-1, n-1)$ in G relative to N. Write $R = A + B\alpha$, where $A, B \in \mathbf{Z}K$. Then $RR^{(-1)} = 2n - 1 + (n-1)(G - N)$ is equivalent to

$$AA^{(-1)} + BB^{(-1)} = 2n - 1 + (n-1)(K - 1), 2AB = (n-1)(K - 1).$$

It follows that $2A^{(-1)}B^{(-1)} = (n-1)(K-1)$. Define $G_1 = K \times \langle\theta\rangle$, $o(\theta) = 2$, $R_1 = A + B^{(-1)}\theta$, then it is easily verified that R_1 is a splitting $(2n, 2, 2n-1, n-1)$ relative difference set in G_1 relative to $\langle\theta\rangle$. This is impossible from Result 1. Hence we have proved

Theorem 9. *Suppose G is a generalized dihedral group of order $4n$, $n > 1$, $G = K \rtimes N$, where K is abelian, $N = \{1, \alpha\}$, $o(\alpha) = 2$. Then no relative difference set with the parameter (2n, 2, 2n-1, n-1) relative to N exists in G.*

Combining these two cases, we have

Corollary 10. *No relative difference set with the parameter (2n, 2, 2n-1, n-1) exists in a generalized dihedral group of order* $4n$, $n > 1$.

Acknowledgement. The authors would like to thank the anonymous referee for valuable suggestions.

References

[1] K.T. Arasu, Q. Xiang, On the existence of periodic complementary binary sequences, Designs, codes and Crypt., 2 (1992), 257-262.

[2] K.T. Arasu, Y.Q. Chen, A. Pott, Hadamard and conference matrices, Journal of Algeb. Combin., 14 (2001), 103-117.

[3] T. Beth, D. Jungnickel, H. Lenz, Design Theory, Cambridge, 1986.

[4] Y.P. Deng, A note on difference sets in dihedral groups, Arch. Math., 82 (2004), 4-7.

[5] Jungnickel, On automorphism groups of divisible designs II: Group invariant generalized conference matrices, Arch. Math., 53 (1990), 200-208.

[6] Jungnickel, Difference sets, in: J.H. Dinitz and D.R. Stinson (eds.), Contemporary design theory: A collection of surveys, New York, 1992, pp.241-324.

[7] A. Pott, A survey on relative difference sets, in: K.T.Arasu et al (eds.), Groups, difference sets, and the monster, Walter de Gruyter, 1996.

[8] A. Pott, Finite geometry and character theory, LNM 1601, Springer-Verlag, Berlin, 1995.

[9] K.H. Leung, B. Schmidt, Asymptotic nonexistence of difference sets in dihedral groups, Journal of Combin. Theory, ser. A, 99 (2002), 261-280.

[10] W.C. Shiu, Difference sets in groups containing sobgroups of index 2. Ars Combin., 42 (1996), 99-205.

[11] Xiang Qing, A note on $(m, 2, m-1, \frac{m-2}{2})$ relative difference sets, Ars Combin., 41 (1995), 199-202.