Difference sets in groups containing subgroups of index 2

Wai Chee Shiu
Department of Mathematics,
Hong Kong Baptist University,
224 Waterloo Road,
Kowloon, Hong Kong
E-mail: wcshiu@math.hkbu.hk

Abstract

In this paper, difference sets in groups containing subgroups of index 2 are considered, especially group of order $2m$ where m is odd. The author shows that the only difference sets in groups of order $2p^\alpha$ are trivial. The same conclusion is true for some special parameters.

1 Introduction

Let G be a finite (multiplicative) group of order $v \geqslant 2$ with identity e . Let $D \subseteq G$. We define $\overline{D^{(t)}} = \sum_{d \in D} d^t$ as an element of the group ring $\mathbb{Z}[G]$, where $t \in \mathbb{Z}$, and $\overline{D} = \overline{D^{(1)}}$. A (v, k, λ) *-difference set* D in G is a subset of G such that $\overline{D}\overline{D^{(-1)}} = ne + \lambda\overline{G}$, where $n = k - \lambda$ [11, section 3].

A difference set is a combinatorial object which can be used to construct a balanced incomplete block design [1]. Difference sets in groups have been studied by many authors (see, for instance, [3]). Most of them are concerned on abelian difference sets, especially cyclic different sets (see, for instance, [1], [8], [12] [13]). Recently, Fan, Siu and Ma (1985) [6, section 4] studied difference sets in dihedral groups, which is a non-abelian case. In this paper, the author is concerned difference sets in groups which obtain subgroups of index 2.

There are some constraints on the parameters v, k, λ of a difference set. Two common constraints are [1, section 1]:

(1) $k(k-1) = \lambda(v-1)$ or equivalently, $k^2 = n + \lambda u$ (1.1)
(2) If v is even, then n is a square. From (1.1) it is easy to see that λ is even.

When $n = 0$ it is easy to obtain that $k = 0$ or $k = v$; when $n = 1$ it is easy to see that $k = 1$ or $k = v - 1$. These two cases are called *trivial* cases. The corresponding difference sets are called *trivial difference sets*.

It is known that if D is a (v, k, λ)-difference set in G then $G \setminus D$ is a $(v, v-k, v-2k+\lambda)$-difference set in G. So without loss of generality we may assume $k < \frac{v}{2}$ ((1.1) shows that $k = \frac{v}{2}$ does not occur).

Fan, Siu and Ma [6, section 4] proved that only trivial difference sets in dihedral group of order $2m$ exist if $(m, n) = 1$ and proved that only trivial difference sets in dihedral group of

order $2p^\alpha$ exist, where p is an odd prime. They also showed that if $D = A \cup \sigma B$ is a $(2m, k, \lambda)$-difference set in $\mathcal{D}_m = \langle \rho, \sigma \mid \rho^m = \sigma^2 = e = \rho\sigma\rho\sigma \rangle$, the dihedral group of order $2m$, then $D' = \{\varphi^{2i} \mid \rho^i \in A\} \cup \{\varphi^{2i+1} \mid \rho^j \in B\}$ is a $(2m, k, \lambda)$-difference set in $\mathcal{C}_{2m} = \langle \varphi \mid \varphi^{2m} = e \rangle$, the cyclic group of order $2m$.

Since no difference sets in a cyclic group of order v are known which have $(v, n) > 1$ (or equivalently $(v, k) > 1$). Fan et al. conjectured that there is no non-trivial difference set in a dihedral group.

Remark 1.1: If D is above then $D'' = A \cup \tau B$ is a $(2m, k, \lambda)$-difference set in $\mathcal{C}_m \times \mathcal{C}_2 = \langle \rho, \tau \mid \rho^m = \tau^2 = e, \rho\tau = \tau\rho \rangle$.

In this paper we generalize the result above. We show that there are only trivial difference sets in groups of order $2p^\alpha$ where p is an odd prime.

2 General Properties

In this section we let G be a group of order $2m$ which contains a (normal) subgroup H of index 2. Then $G = H \cup \sigma H$ for some $\sigma \in G \setminus H$. Hence $\sigma^2 = h^{-1}$ or $\sigma h = \sigma^{-1}$ for some $h \in H$.

Suppose $D = A \cup \sigma\ B$ is a $(2m, k, 2\lambda_0)$-difference set in G where $A, B \subseteq H$.
We have,

$$\begin{aligned} \overline{A}\overline{A^{(-1)}} + \overline{\tilde{B}}\ \overline{\tilde{B}^{(-1)}} &= ne + 2\lambda_0\overline{H} \\ h\overline{\tilde{A}}\ \overline{\tilde{B}^{(-1)}} + \overline{B}\overline{A^{(-1)}} &= 2\lambda_0\overline{H} \end{aligned} \tag{2.1}$$

or

$$h\sigma\overline{A}\overline{B^{(-1)}}\sigma^{-1} + \overline{B}\overline{A^{(-1)}} = 2\lambda_0\overline{H} \tag{2.2}$$

where $\tilde{A} = \sigma A \sigma^{-1}$ and $\tilde{B} = \sigma B \sigma^{-1}$

Lemma 2.1. *If $D = A \cup \sigma B$ is a $(2m, k, 2\lambda_0)$-difference set in G as described, then $\sigma D = h^{-1}B \cup \sigma A$ is a $(2m, k, 2\lambda_0)$-difference set in G.*

Proof: Since $\sigma\ D$ is a shift of D □

Suppose D is as above. Let $k_1 = |A|$ and $k_2 = |B|$ then $k_1 = |\tilde{A}|$ and $k_2 = |\tilde{B}| = |h^{-1}B|$. Clearly $k_1, k_2 \leq k < m$. By Lemma 2.1, from now on, we assume $m > k_1 \geq k_2$. For convenience, the difference set $D = A \cup \sigma B$ as above is called a $(2m, k_1 \& k_2, 2\lambda_0)$-difference set in $G = H \cup \sigma H$. Note that if D is a $(2m, k, 2\lambda_0)$-difference set in $G = H \cup \sigma H$, then D is a $(2m, k_1 \& k_2, 2\lambda_0)$-difference set in G for some k_1, k_2 and λ_0.

By applying the trivial character of H on (2.1) and (2.2) we have

$$k_1^2 + k_2^2 = n + 2\lambda_0 m \tag{2.3}$$

$$k_1 k_2 = \lambda_0 m, \tag{2.4}$$

where $n = k - 2\lambda_0$ and $k = k_1 + k_2$. From (2.3) and (2.4) we have

$$n = (k_1 - k_2)^2. \tag{2.5}$$

Examples 2.2:

(1) The dihedral group $\mathcal{D}_m$ has a subgroup, which is isomorphic to $\mathcal{C}_m$, of index 2.

(2) The symmetric group $\mathcal{S}_m$ of order $m!$ has a subgroup $\mathcal{A}_m$, the alternating group, of index 2.

(3) Let G be a group of order $2m$, where m is odd. Since G is even order, there is $\sigma \in G$ such that $\sigma^2 = e$. Consider G_L, the group of left translations of G, it contains an odd permutation induced from σ. Thus G_L contains a subgroup of index 2. Since $G_L \cong G$, G contains a subgroup H of index 2. In this case $G = H \cup \sigma H$ where $\sigma^2 = e$.

(4) Let G be an abelian group of even order v. By Sylow Theorem [7, Theorem 2.12.1], if $2^\gamma \| v$ then there is a subgroup H of G having order $2^{\gamma-1}$ where $\gamma \geq 1$ and for any odd prime factors of v there is a (unique) Sylow p-subgroup of G. Thus G contains a subgroup of index 2. Note that not every group of even order contains a subgroup of index 2, for example $\mathcal{A}_m$ when $m \geq 4$.

Let a be a nonzero integer. By $v_p(a)$ we denote the power to which prime p enters in the factorization of a into prime factors. For convenience, we set $v_p(0) = \infty$ [2, p.175].

Theorem 2.3. *If integers k_1, k_2, λ_0, m and n satisfy (2.3), (2.4) and (2.5) where $n = k - 2\lambda_0$ and $k = k_1 + k_2$ then $v_p(k_1) \geq v_p(m)$ or $v_p(k_2) \geq v_p(m)$ for p is an odd prime and $v_2(k_1) + 1 \geq v_2(m)$ or $v_2(k_2) + 1 \geq v_2(m)$.*

Proof: For $p \neq 2$, from (2.4) and (2.5) we have

$$v_p(m) = v_p(k_1) + v_p(k_2) - v_p(2\lambda_0) \tag{2.6}$$

$$v_p(n) \geq 2(\min\{v_p(k_1), v_p(k_2)\}). \tag{2.7}$$

Since $n = k - 2\lambda_0$ and $k = k_1 + k_2$ and (2.7),

$$\begin{aligned} v_p(2\lambda_0) &\geq (\min\{v_p(k), v_p(n)\}) \\ &\geq (\min\{v_p(k_1), v_p(k_2), v_p(n)\}) \\ &= (\min\{v_p(k_1), v_p(k_2)\}). \end{aligned}$$

From (2.6) we have $v_p(m) \leq v_p(k_1) + v_p(k_2) - \min\{v_p(k_1), v_p(k_2)\}$. The lemma holds for p is an odd prime. By a similar proof, the lemma holds for $p = 2$. □

Corollary 2.4. *There are only trivial difference sets in groups of order $2p^\alpha$ where p is an odd prime.*

Proof: The theorem follows from Example 2.2 (3) and Theorem 2.3. □

When $p = 2$ there are many results on difference sets in 2-groups. Dillon [5] had classified all groups of order 16 containing nontrivial difference sets. In his paper, he showed that there is no nontrivial difference in $\mathcal{D}_8$. Leibler and Smith [10] and Davis and Smith [4] have some constructions of difference sets in high exponent 2-groups.

Corollary 2.5. *Suppose p and q are distinct odd primes. If there is a $(2pq, k_1\&k_2, 2\lambda_0)$-difference set then $(pq, (k_1 - k_2)^2) = 1$.*

Proof: By Theorem 2.3 and $k_2 \leq k_1 < pq$, we may assume $v_p(k_1) \geq 1$ and $v_q(k_2) \geq 1$. Then $q \nmid k_1$ and $p \nmid k_2$. By (2.5) we have $(pq, (k_1 - k_2)^2) = 1$. □

By Theorem 2.4 we see that there are only trivial difference sets in dihedral group of order $2p^\alpha$ exist where p is an odd prime. From the Theorem 4.1 in [6] and Corollary 2.5 we have

Corollary 2.6. *There are only trivial difference sets in $\mathcal{D}_{pq}$ where p and q are distinct odd primes.*

Our results apply to groups containing subgroup of index 2. Of course for certain specific groups, we may use specialized techniques exploiting properties not assume here. For example, our results do not say anything about (66, 26, 10), (70, 24, 8) and (154, 18, 2)-difference sets in general groups. However, if we consider the abelian case then it can be found in the Lander's table [9] that there are only trivial (66, 26, 10), (70, 24, 8) and (154, 18, 2)-abelian difference sets. For the dihedral groups, Corollary 2.6 shows that there are only trivial (66, 26, 10), (70, 24, 8) and (154, 18, 2)-difference sets in dihedral groups.

Let us go back to discuss the parameters of the $(2m, k_1\&k_2, 2\lambda_0)$-difference sets. From (2.3) and (2.4) we have

$$\begin{aligned} & k_1^2 + k_2^2 - 2k_1k_2 - k_1 - k_2 + 2\lambda_0 = 0 \ (k_1 \geq k_2) \qquad (2.8) \\ \Leftrightarrow k_1 &= \frac{2k_2 + 1 + \sqrt{8k_2 + 1 - 8\lambda_0}}{2} \\ \Leftrightarrow k_2 &= \frac{2k_1 + 1 - \sqrt{8k_1 + 1 - 8\lambda_0}}{2} \end{aligned}$$

Suppose $x_0, x_1 \in \mathbb{N}$, $x_0 < x_1$, satisfy (2.8). Let $x_{j+1} = \frac{2x_j+1+\sqrt{8x_j+1-8\lambda_0}}{2}$ for $j \geq 0$. It is easy to see that $x_{j+1} - x_j = 1 + x_j - x_{j-1}$ for $j \geq 1$.

Similarly, suppose $y_0, y_1 \in \mathbb{N}$, $y_0 > y_1$, satisfy (2.8).

Let $y_{j+1} = \frac{2y_j+1-\sqrt{8y_j+1-8\lambda_0}}{2}$ for $j \geq 0$ and $8y_j + 1 - 8\lambda_0 \geq 0$. We also have $1 + y_j - y_{j+1} = y_{j-1} - y_j$ for $j \geq 1$.

Finally, it is easy to see that if $k_1, k_2 \in \mathbb{N}$ satisfy (2.8) and $k_1 - k_2 = 1$ then $k_2 = x_{j-1}$. Combine the discussions above we have

Lemma 2.7. *Let* $x_j = \frac{j(j+1)}{2} + \lambda_0$, $j \geq 0$. *If* $k_1, k_2 \in \mathbb{N}$ *satisfy (2.8) then* $k_1 = x_j$, $k_2 = x_{j-1}$ *for some* $j \geq 1$.

Remark 2.8: From Lemma 2.7, there is only one set of parameters, namely $(2(\frac{j^4-j^2}{4\lambda_0} + j^2 + \lambda_0), \frac{j(j+1)}{2} + \lambda_0 \& \frac{(j-1)j}{2} + \lambda_0, 2\lambda_0)$, according to the given $\lambda_0 \geq 1$ and $n = k_1 + k_2 - 2\lambda_0 = j^2 \geq 1$.

Theorem 2.9. *Only* $(2(\frac{j^4-j^2}{4\lambda_0} + j^2 + \lambda_0), \frac{j(j+1)}{2} + \lambda_0 \& \frac{(j-1)j}{2} + \lambda_0, 2\lambda_0)$*-difference set may exist if* $\frac{j^4-j^2}{4} \equiv 0 \pmod{\lambda_0}$, $j \geq 1$.

Proof: it follows from (2.4). □

Let us consider two special cases, namely $\lambda_0 = 1$ or 2

Case 1: For $\lambda_0 = 1$.

Suppose m is odd and $\lambda_0 = 1$. From (2.4) we have $k_1 k_2 = m$. Thus k_1, k_2 are odd. From (2.3) we have $n \equiv 0$ and $k \equiv 2 \pmod 4$. Thus $k_1 \equiv k_2 \pmod 4$ and $m \equiv 1 \pmod 4$. Hence we have the following theorem.

Theorem 2.10. *There are only trivial* $(2m, k_1 \& k_2, 2)$*-difference sets if* $m \equiv 3 \pmod 4$.

Lemma 2.11. *Suppose* m *is odd. If there is a* $(2m, k_1 \& k_2, 2)$*-difference set then* $(m, (k_1 - k_2)^2) = 1$.

Proof: By Theorem 2.3 and (2.4) when $\lambda_0 = 1$ we have $k_1 = P$ and $k_2 = Q$, where $m = PQ$, $(P, Q) = 1$. Thus $(m, (k_1 - k_2)^2) = 1$. □

Suppose m is odd. By Lemma 2.11 and Theorem 4.1 in [6] we have

Theorem 2.12. *There are no non-trivial* $(2m, k_1 \& k_2, 2)$*-difference sets in* $\mathcal{D}_m$ *where* m *is odd.*

Case 2: For $\lambda_0 = 2$.

Theorem 2.13. *There is no non-trivial* $(2m, k_1 \& k_2, 4)$*-difference set when* $n = (k_1 - k_2)^2 \equiv 4 \pmod 8$.

Proof: $\frac{j^4-j^2}{4} \equiv 0 \pmod 2 \Leftrightarrow j^4 - j^2 \equiv 0 \pmod 8$. The equation does not hold when $j \equiv 2 \pmod 4$. Since $n = j^2$, then the equation does not hold when $n \equiv 4 \pmod 8$. □

For $\lambda_0 = 1$ or 2, consider the first ten terms of the sequence defined in Lemma 2.7. We can prove that there are only trivial difference sets in $\mathcal{D}_m$. Among these cases, some of them can be proved by applying Theorem 4.1 in [6] and the rest which indicated by "†" are proved by Corollary 3 in [11]. We list them as follows:

For $\lambda_0 = 1$, the sequence is $\{1, 2, 4, 7, 11, 16, 22, 29, 37, 46, 56, ...\}$.

According to the first ten terms of this sequence we have

$n = k - \lambda$	1	$4^\dagger$	9	16	25	$36^\dagger$	49	64	81	$100^\dagger$
k_2	1	2	4	7	11	16	22	29	37	46
k_1	2	4	7	11	16	22	29	37	46	56
k	3	6	11	18	27	38	51	66	83	102
m	2	8	28	77	176	352	638	1073	1702	2576
(m, n)	1	4	1	1	1	2	1	1	1	4

For $\lambda_0 = 2$, the sequence is {2, 3, 5, 8, 12, 17, 23, 30, 38, 47, 57,...}.
According to the first ten terms of this sequence we have

$n = k - \lambda$	1	4	9	$16^\dagger$	25	36	49	$64^\dagger$	81	100
k_2	2	3	5	8	12	17	23	30	38	47
k_1	3	5	8	12	17	23	30	38	47	57
k	5	8	13	20	29	40	53	68	85	104
m	3	-	20	48	102	-	345	570	893	-
(m, n)	1	-	1	16	1	-	1	2	1	-

References

[1] L.D. Baumert, *Cyclic Difference Sets*, Springer-Verlag, New York, 1971.

[2] Z.I. Borevich and I.R. Shafarevich, *Number Theory*, Academic Press, New York, 1966.

[3] R.H Bruck, Difference sets in a finite group, *Trans. Amer. Math. Soc.*, **78** (1955), 464−481.

[4] Davis and Smith, A construction of difference sets in high exponent 2-groups using representation theory, to appear in *J. Algebraic Combinatorics*.

[5] J.F. Dillon, Varations on a scheme of McFarland for noncyclic difference sets, *J. Comb. Theory Ser. A,* **40** (1985), 9−21.

[6] C.T. Fam, M.K. Siu and S.L. Ma, Difference sets in dihedral groups and interlocking difference sets, *Ars Combinatoria,* **20A** (1985), 99−107.

[7] I.N. Herstein, *Topics in Algebra*, 2nd ed., John Wiley & Sons, 1975.

[8] E.C. Johnsen, The inverse multiplier for abelian group difference sets, *Canad. J. Math.,* **16** (1964), 787−796.

[9] E.S. Lander, *Symmetric Designs: An Algebraic Approach*, Cambridge Univ. Press, 1983.

[10] Leibeler and Smith, On difference sets in certain 2-groups, *Coding Theory, Design Theory, Group Theory: Proceedings of the Marshall Hall Conference*, John Wiley, 1992.

[11] K.H. Leung, S.L. Ma and Y.L. Wong, Difference sets in dihedral groups, *Designs, Codes and Cryptograph,* **1**(1992), 333−338.

[12] P.K. Menon, Difference sets in Abelian Groups, *Proc. American Math. Soc.,* **11** (1960), 368−376.

[13] E. Spence, A family of difference sets, *J. Comb. Theory, Ser. A,* **22** (1977), 103−106.