A two-to-one map and abelian affine difference sets

Yutaka Hiramine
Department of Mathematics, Faculty of Education, Kumamoto University, Kurokami, Kumamoto, Japan

hiramine@gpo.kumamoto-u.ac.jp

Abstract. Let D be an affine difference set of order n in an abelian group G relative to a subgroup N. Set $\tilde{H} = H \setminus \{1, \omega\}$, where $H = G/N$ and $\omega = \prod_{\sigma \in H} \sigma$. Using D we define a two-to-one map g from $\tilde{H}$ to N. The map g satisfies $g(\sigma^m) = g(\sigma)^m$ and $g(\sigma) = g(\sigma^{-1})$ for any multiplier m of D and any element $\sigma \in \tilde{H}$. As applications, we present some results which give a restriction on the possible order n and the group theoretic structure of G/N.

Keywords: relative difference set, affine difference set, multiplier

1 Introduction

Let G be a group of order $n^2 - 1$ $(n > 1)$ and N a subgroup of G of order $n - 1$. An n-subset D of G is called *an affine difference set* of *order* n in G relative to N if each element $x \in G \setminus N$ is uniquely represented in the form $d_1 d_2^{-1}$ $(d_1, d_2 \in D)$ and no nonidentity element in N is represented in such a form (see [9]). An affine difference set D is said to be abelian or cyclic if the group G has the respective property. For a subset X of G and an integer s, we set $X^{(s)} = \{x^s \mid x \in X\}$. An integer m is called *a multiplier* of D if $D^{(m)} = Da$ for some $a \in G$.

It is a well-known conjecture that an abelian affine difference set is of prime power order and cyclic ([9]). Many results on abelian affine difference sets are known. We refer to [1], [2], [4], [7], [8] for the order of abelian affine difference sets, [3] for the group theoretic structure, and §5.2 of [9], §7 of [10] for a survey.

Recently, in [5], J. C. Galati studied abelian affine difference sets of even order from the group extension point of view and gave some non-existence results. In [6], the author also studied affine difference sets of order n including odd order case.

Set $H = G/N$ and $\omega = \displaystyle\prod_{\sigma \in H} \sigma = Nw$ $(\exists w \in G)$. If we exchange D for its suitable translate if necessary, we may assume that $D \cap Nw = \emptyset$, $\prod_{d \in D} d = 1$ and $S = D \cup \{w\}$ is a complete set of coset representatives of H. Set $H^* = H \setminus \{\omega\}$. Let d be a map from H^* to G defined by $\{d(\sigma)\} = Nx \cap D$ for $\sigma = Nx \in H^*$. Then, clearly $D = \{d(\sigma) \mid \sigma \in H^*\}$. We define a map g from H^* to N by $g(\sigma) = d(\sigma)d(\sigma^{-1})$ for $\sigma \in H^*$. Set $\tilde{H} = H \setminus \{1, \omega\}$. Then $g|_{\tilde{H}}$ is a two-to-one map (Lemma 2.4). Note that $\mathrm{o}(\omega) = 1$ or 2 according as n is even or odd since

$|H| = n+1$ and a Sylow 2-subgroup of G is cyclic by a result of Arasu-Pott ([3]). On the other hand $\mathrm{o}(g(\sigma))$ is a divisor of $m-1$ if and only if either $\sigma^{m-1} = 1$ or $\sigma^{m+1} = 1$ for $m \in \Lambda_n$, where $\Lambda_n = \{m \in \mathbb{N} \mid \pi(m) \subset \pi(n)\}$ and $\pi(k)$ is the set of primes dividing an integer k (see Proposition 3.1). As applications, we present some results which give a restriction on the orders n of abelian affine difference sets and the group theoretic structure of G/N (Theorems 3.2, 3.6, 4.1).

2 Preliminaries

Definition 2.1. An n-subset D of an abelian group G of order $n^2 - 1$ is called *an affine difference set* of *order* n relative to N if each element $x \in G \setminus N$ is uniquely represented in the form $d_1 d_2^{-1}$ $(d_1, d_2 \in D)$ and no nonidentity element in N is represented in such a form (see [9]).

Throughout the article we use the following notations.

Notation 2.2. (i) Let D be an affine difference set in an abelian group G of order $n^2 - 1$ relative to a subgroup N of G of order $n-1$. Set $H = \overline{G} = G/N$ and $\omega = \prod_{\sigma \in H} \sigma = Nw$ $(\exists w \in G)$. Then, as a Sylow 2-subgroup of G is cyclic by [3],

$$\mathrm{o}(\omega) = \begin{cases} 1 & \text{if } 2|n, \\ 2 & \text{otherwise.} \end{cases}$$

(ii) If we exchange D for its suitable translate if necessary, we may assume that $D \cap Nw = \emptyset$. Hence $\prod_{x \in D} x \in N$. Since $(|D|, |N|) = 1$, exchanging D for a suitable Da with $a \in N$ if necessary, we may assume that

$$\prod_{x \in D} x = 1.$$

(iii) Set $H^* = H \setminus \{\omega\}$ and $\tilde{H} = H \setminus \{1, \omega\}$. Note that $H^* = \tilde{H}$ iff $2 \mid n$.

(iv) Let $\pi(m)$ denote the set of primes dividing a positive integer m and set $\Lambda_n = \{m \in \mathbb{N} | \ \pi(m) \subset \pi(n)\}$ for $n \in \mathbb{N}$.

By Notation 2.2, $H = \overline{D} \cup \{\omega\}$, where $\overline{D} = \cup_{x \in D} Nx$. Let d be a map from H^* to G defined by $\{d(\sigma)\} = Nx \cap D$ for $\sigma = Nx \in H^*$. We define a map g from H^* to N by $g(\sigma) = d(\sigma)d(\sigma^{-1})$ for $\sigma \in H^*$. Then the following holds (see [6]).

Result 2.3. (i) $D^{(m)} = D \quad \forall m \in \Lambda_n$.

(ii) Let $m \in \Lambda_n$, then $d(\xi^m) = d(\xi)^m$ for any $\xi \in H^*$. In particular, $g(\xi^m) = g(\xi)^m$ for any $\xi \in H^*$ and $m \in \Lambda_n$.

(iii) If $\sigma, \tau \in H^*$, then $g(\sigma) = g(\tau)$ if and only if $\{\sigma, \sigma^{-1}\} = \{\tau, \tau^{-1}\}$.

By Result 2.3(iii) we have the following.

Lemma 2.4. *The map g restricted to $\tilde{H}$ is two-to-one.*

Remark 2.5. Assume n is even. Then $G = N \times Q$ for a subgroup Q of G of order $n+1$. In his paper [5] J.C. Galati defined a map ϕ from Q to N by $D = \{(\phi(x), x) \mid x \in Q \setminus \{1\}\}$ and $\phi(1) = 1$. We can easily verify that $g(Nx) = \phi(x)^2$ for $x \in Q \setminus \{1\}$ when n is even.

3 Multipliers and divisors of $n+1$

Let $G, N, H, \omega, H^*, \tilde{H}, \Lambda_n$ and the map g be as defined in the last section. In this section we present some results on the orders of abelian affine difference sets as applications of the two-to-one map g.

The map g has the following property which is used repeatedly in this article.

Proposition 3.1. *Let $\sigma \in H^*$ and $m \in \Lambda_n$. Then $\mathrm{o}(g(\sigma))|m-1$ if and only if either $\sigma^{m-1} = 1$ or $\sigma^{m+1} = 1$.*

Proof. Assume $\mathrm{o}(g(\sigma))|m-1$. Then, $g(\sigma)^m = g(\sigma)$ and so $g(\sigma^m) = g(\sigma)^m = g(\sigma)$ by Result 2.3(ii). Hence $\sigma^m \in \{\sigma, \sigma^{-1}\}$ by Result 2.3(iii). Therefore we have either $\sigma^{m-1} = 1$ or $\sigma^{m+1} = 1$. Conversely, assume either $\sigma^{m-1} = 1$ or $\sigma^{m+1} = 1$. Then, $\sigma^m = \sigma^{\pm 1}$. Hence $g(\sigma)^m = g(\sigma^m) = g(\sigma^{\pm 1}) = g(\sigma)$ by Result 2.3(iii). Thus $\mathrm{o}(g(\sigma)) \mid m-1$. □

If we have information on the group theoretic structure of N, the following holds.

Theorem 3.2. *Let G be an abelian group containing an affine difference set of order n relative to a subgroup N. Let $m \in \Lambda_n$ and assume a Sylow p-subgroup of N is cyclic for each $p \in \pi((m-1, n-1))$. Then, $(m+1, n+1) \leq 2(m-1, n-1) + (2, m+1)$.*

Proof. We note that $\sigma^{m+1} = 1$ if and only if $\sigma^{(m+1,n+1)} = 1$ for $m \in \Lambda$ and $\sigma \in H$. Set $H_1 = \{\sigma \in H \mid \sigma^{(m+1,n+1)} = 1\} \setminus \{1, \omega\}$. Then, clearly $|H_1| \geq (m+1, n+1) - (2, m+1)$. On the other hand $|\{x \in N \mid x^{m-1} = 1\}| = |\{x \in N \mid x^{(m-1,n-1)} = 1\}| = (m-1, n-1)$ by assumption. This, together with Lemma 2.4 and Result 2.3(iii), gives $|H_1|/2 \leq (m-1, n-1)$. Thus $(m+1, n+1) - (2, m+1) \leq 2(m-1, n-1)$. □

As a corollary of Theorem 3.2, we have the following.

Corollary 3.3. *Assume the existence of an abelian affine difference set of order n and let $m \in \Lambda_n$ such that $m+1 \mid n+1$. If $p^2 \nmid n-1$ for each odd prime p dividing $(m-1, n-1)$, then $\frac{m-1}{(m-1,2)}|n-1$.*

Proof. Assume m is even. Then, by Theorem 3.2, $m+1 \le 2(m-1, n-1)+1$ and so $m \le 2(m-1, n-1)$. Hence $(m-1, n-1) = m-1$ as $m-1$ is odd. Thus the corollary holds.

Assume m is odd. Then, by Theorem 3.2, $m+1 \le 2(m-1, n-1)+2$ and so $m-1 \le 2(m-1, n-1)$. Hence $(m-1, n-1) \in \{m-1, \frac{m-1}{2}\}$. Thus the corollary holds in both cases. $\square$

Proposition 3.4. *Assume the existence of an abelian affine difference set of order n and let q be a prime divisor of n such that $q+1 \mid n+1$ and $q = 2p+1$ for an odd prime p. Then $p \mid n-1$.*

Proof. Assume $p \nmid n-1$. Then $(q-1, n-1) = (2p, n-1) \mid 2$. Applying Corollary 3.3 with $m = q$ we have $\frac{q-1}{(q-1,2)} = p \mid n-1$, contrary to the assumption. Thus $p \mid n-1$. $\square$

Example 3.5. Assume the existence of an abelian affine difference set of order n. Applying Proposition 3.4 with $q = 7, 11$ or 23 we have the following.

(i) If $n \equiv 0 \pmod 7$ and $n \equiv 7 \pmod 8$, then $3 \mid n-1$.

(ii) If $n \equiv 0 \pmod{11}$ and $n \equiv 11 \pmod{12}$, then $5 \mid n-1$.

(iii) If $n \equiv 0 \pmod{23}$ and $n \equiv 23 \pmod{24}$, then $11 \mid n-1$.

The following is also an application of Proposition 3.1.

Theorem 3.6. *Let G be an abelian group containing an affine difference set of order n relative to a subgroup N. Let $m \in \Lambda_n$. Assume G/N contains an element of order r and set $e = \mathrm{ord}_r(m)$. If $e > 2$, then $(m^e-1, n-1) \nmid m-1$.*

Proof. Let notations H^* and g be as before. Let σ be an element of H^* of order r. As $e = \mathrm{ord}_r(m) > 2$, we have $\sigma^{m^e-1} = 1$. Hence $\sigma^{m^e} = \sigma$ and so $g(\sigma)^{m^e} = g(\sigma^{m^e}) = g(\sigma)$ by Result 2.3(ii). From this, $g(\sigma)^{m^e-1} = 1$. Thus $\mathrm{o}(g(\sigma)) \mid (m^e-1, n-1)$. Assume $(m^e-1, n-1) \mid m-1$. Then $\mathrm{o}(g(\sigma)) \mid m-1$ and so by Proposition 3.1, we have either $\sigma^{m-1} = 1$ or $\sigma^{m+1} = 1$. This implies $\sigma^{m^2-1} = 1$ and therefore $\mathrm{ord}_r(m) \mid 2$, a contradiction. $\square$

As a corollary of Theorem 3.6, the following holds.

Corollary 3.7. *Let G be an abelian group containing an affine difference set of order n relative to a subgroup N. Let $p \in \pi(n), q \in \pi(n+1)$ and set $e = \mathrm{ord}_q(p)$. If $e > 2$, then $(p^e-1, n-1) \nmid p-1$.*

Example 3.8. Assume $n = 39 \pmod{60}$. We take $p = 3 \in \pi(n)$ and $q = 5 \in \pi(n+1)$. Since $e = \mathrm{ord}_5(3) = 4$ and $(p^e-1, n-1) = (80, n-1) = 2 \mid p-1 = 2$, we have a contradiction by Corollary 3.7. Therefore, if $n = 39 + 60s$ for some integer s, then there exists no abelian affine difference set of order n.

The following is a slightly modified version of Theorem 3.6.

Theorem 3.9. *Let G be an abelian group containing an affine difference set of order n relative to a subgroup N. Let $m \in \Lambda_n$, $q \in \pi(n+1)$ and set $e = \mathrm{ord}_q(m)$. If e is even and $e > 2$, then $(m^{\frac{e}{2}} - 1, n-1) \nmid m-1$.*

Proof. Set $e = 2f$. By assumption, $f > 1$ and $q > 2$. Let σ be an element of H^* of order q. Since $q \mid (m^f - 1)(m^f + 1)$ and $(m^f - 1, m^f + 1) \leq 2$, we have $q \mid m^f + 1$. Hence $\sigma^{m^f} = \sigma^{-1}$. Thus $g(\sigma)^{m^f} = g(\sigma^{m^f}) = g(\sigma^{-1}) = g(\sigma)$ by Result 2.3. From this, $g(\sigma)^{m^f - 1} = 1$ and so $\mathrm{o}(g(\sigma)) \mid (m^f - 1, n-1)$. Assume $(m^f - 1, n-1) \mid m-1$. Then, by Proposition 3.1, $\sigma^{m^2 - 1} = 1$. Hence $q \mid m^2 - 1$. Thus $\mathrm{ord}_q(m) \mid 2$, contrary to the assumption. Therefore $(m^f - 1, n-1) \nmid m-1$. $\square$

As an application of Theorem 3.9, we have the following.

Example 3.10. Assume $n = 3(7s+2)$ for an integer s. We take $m = 3 \in \Lambda_n$ and $q = 7 \mid n+1$. Then, $\mathrm{ord}_q(m) = 6$. Applying Theorem 3.9, $(3^3 - 1, n-1) \nmid 2$. Since $(3^3 - 1, n-1) \in \{1, 2, 13, 26\}$, we have $13 \mid n-1$. Thus, if $n \equiv 6 \pmod{21}$ and there exists an abelian affine difference set of order n, then $13 \mid n-1$.

4 Sylow subgroups of G

As another application of Proposition 3.1 we consider the group theoretic structure of Sylow subgroups of G. Let m_p be the highest power of a prime p dividing an integer m. Then we have the following.

Theorem 4.1. *Let G be an abelian group containing an affine difference set of order n relative to a subgroup N. Let $m \in \Lambda_n$ and assume $m+1 \mid n+1$ and a Sylow p-subgroup of N is cyclic for each $p \in \pi((m-1, n-1))$. Then, a Sylow q-subgroup of G is cyclic for any prime $q \in \pi(n+1)$ such that $(m+1)_q < (n+1)_q$.*

Proof. Set $C = \{x \in N \mid x^{m-1} = 1\}$. Then $C = \{x \in N \mid x^{(m-1, n-1)} = 1\}$. By assumption, a Sylow p-subgroup of N is cyclic for each $p \in \pi((m-1, n-1))$. Hence $|C| = (m-1, n-1)$. Set $H_1 = \{\sigma \in H \mid \sigma^{m+1} = 1\}$ and let $q \in \pi(m+1) \cap \pi(\frac{n+1}{m+1})$. Assume a Sylow q-subgroup of G is non-cyclic. Then, q is an odd prime as a Sylow 2-subgroup of G is cyclic ([3]). Hence $|H_1| \geq (m+1)q$. From this, $|H_1| \geq 3(m+1)$. By Lemma 2.4, $|\{g(\sigma) \mid \sigma \in H_1\}| \geq (3m+1)/2 > 3(m-1, n-1)/2 + 1$. However, as a Sylow p-subgroup of N is cyclic for each prime $p \in \pi(m-1, n-1)$, $|\{g(\sigma) \mid \sigma \in H_1\}| - 1 \leq (m-1, n-1)$ by Proposition 3.1. Hence $(m-1, n-1) > (3(m-1, n-1)/2 + 1) - 1 = 3(m-1, n-1)/2$, a contradiction. $\square$

By Theorem 4.1, we have the following.

Corollary 4.2. *Let $m \in \Lambda_n$ and assume $m+1 \mid n+1$ and a Sylow p-subgroup of N is cyclic for each $p \in \pi((m-1, n-1))$. Let $q \in \pi(m+1)$ and $q^u = (m+1)_q$.*

(i) If $u = 1$, then a Sylow q-subgroup of G is cyclic.

(ii) *If $u = 2$, then a Sylow q-subgroup of G is either cyclic or isomorphic to $\mathbb{Z}_q \times \mathbb{Z}_q$.*

Proof. By a result of Arasu-Pott in [3] we may assume that $q > 2$ and so $q \nmid n - 1$. Assume a Sylow q-subgroup of G is non-cyclic. Then, applying Theorem 4.1, q^u exactly divides $|G|$. Hence, if $u \leq 2$, then $u = 2$ and a Sylow q-subgroup of G is isomorphic to $\mathbb{Z}_q \times \mathbb{Z}_q$. Thus the corollary holds. □

As an application of Corollary 4.2 we have the following.

Proposition 4.3. *Let G be an abelian group containing an affine difference set of order n relative to a subgroup N.*

(i) *If n is even and $n \equiv 2 \pmod 3$, then a Sylow 3-subgroup of G is cyclic. In particular, if $n = 2^{2s-1}$ for an integer s, then a Sylow 3-subgroup of G is cyclic.*

(ii) *If n is odd and $3 \mid n,\ 5 \mid n + 1$, then a Sylow 5-subgroup of G is cyclic. In particular, if $n = 3^{2(2s-1)}$ for an integer s, then a Sylow 5-subgroup of G is cyclic.*

(iii) *If n is odd and $5 \mid n,\ 3 \mid n + 1$, then a Sylow 3-subgroup of G is cyclic. In particular, if $n = 5^{2s-1}$ for an integer s, then a Sylow 3-subgroup of G is cyclic.*

Proof. Assume $2 \mid n$ and $n \equiv 2 \pmod 3$. Apply Corollary 4.2(i) with $m = 2 \in \Lambda_n$ and $q = 3$. Then we have (i).

Assume $2 \nmid n,\ 3 \mid n$ and $5 \mid n+1$. Take $m = 3^2 \in \Lambda_n$. Then $10 = m+1 \mid n+1$ and $(m-1, n-1) \mid 8$. Applying Corollary 4.2(i), we have (ii).

Assume $2 \nmid n,\ 5 \mid n$ and $3 \mid n+1$. Take $m = 5 \in \Lambda_n$. Then $6 = m+1 \mid n+1$ and $(m-1, n-1) \mid 4$. Applying Corollary 4.2(i), we have (iii). □

References

[1] K.T. Arasu and D. Jungnickel, Affine difference sets of even order, *J. of Combin. Theory, Ser. A*, Vol. 52 (1989), 188-196.

[2] K.T.Arasu, Cyclic affine planes of even order, *Discrete Math.*, Vol. 76 (1989),177-181.

[3] K. T. Arasu and A. Pott, On quasi-regular collineation groups of projective planes, *Designs Codes and Cryptography* Vol. 1 (1991), pp. 83-92.

[4] K. T. Arasu and A. Pott, Cyclic affine planes and Paley difference sets, *Discrete Math.*, vol 106-7 (1992), 19-23.

[5] J.C. Galati, A group extensions approach to affine relative difference sets of even order, *Discrete Mathematics* Vol.306 (2006), pp. 42-51.

[6] Y. Hiramine, On affine difference sets and their multipliers, to appear in Discrete Math.

[7] D. Jungnickel, A note on affine difference sets, .Arch. Math. vol.47 (1986), pp 279-280

[8] A. Pott, An affine analogue of Wilbrink's theorem, *J. of Combin. Theory, Ser. A*, Vol. 55 (1990), 313-315

[9] A. Pott, *Finite Geometry and Character Theory*, Lecture Notes in Mathematics 1601 Springer-Verlag, Berlin (1995)

[10] A. Pott, *Groups, Difference sets, and the Monster* (K.T. Arasu et al. eds.), Walter de Gruyter, 1996, pp 195-232.