On affine difference sets and their multipliers

Yutaka Hiramine
Department of Mathematics, Faculty of Education, Kumamoto University, Kurokami, Kumamoto, Japan
E-mail : 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. We denote by $\pi(s)$ the set of primes dividing an integer $s(>0)$ and set $H^* = H \setminus \{\omega\}$, where $H = G/N$ and $\omega = \prod_{\sigma \in H} \sigma$. In this article, using D we define a map g from H to N satisfying for $\tau, \rho \in H^*$, $g(\tau) = g(\rho)$ iff $\{\tau, \tau^{-1}\} = \{\rho, \rho^{-1}\}$ and show that $\mathrm{ord}_{\mathrm{o}(\sigma)}(m)/\mathrm{ord}_{\mathrm{o}(g(\sigma))}(m) \in \{1, 2\}$ for any $\sigma \in H^*$ and any integer $m > 0$ with $\pi(m) \subset \pi(n)$. This result is a generalization of J.C. Galati's theorem on even order n ([3]) and gives a new proof of a result of Arasu-Pott on the order of a multiplier modulo $\exp(H)$ ([1] Section 5).

Keywords: Relative difference set;Affine difference set;Multiplier

1 Introduction

Let G be an abelian 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 [8]). Therefore, D is an affine difference set if and only if $DD^{(-1)} = n + G - U$ in the group ring $\mathbb{Z}[G]$, where we identify a subset X of G with a group ring element $\sum_{x \in X} x \in \mathbb{Z}[G]$ and set $X^{(s)} = \sum_{x \in X} x^s$ for an integer s. An integer m is called *a multiplier* of D if $D^{(m)} = Da$ for some $a \in G$.

An affine difference set of order n corresponds to a projective plane of order n admitting a quasiregular collineation group and so it is conjectured that the order n is a power of a prime ([8]).

If n is even, then as $(n+1, n-1) = 1$, N is a direct factor of G and $G = Q \times N$ for a subgroup Q of G of order $n+1$. Using this fact J.C.Galati defined a map ϕ from Q to N and showed that for any $x \in Q$ and any numerical multiplier m of D, $\mathrm{ord}_{\mathrm{o}(x)}(m) = \mathrm{ord}_{\mathrm{o}(\phi(x))}(m)$ or $\mathrm{ord}_{\mathrm{o}(x)}(m) = 2\mathrm{ord}_{\mathrm{o}(\phi(x))}(m)$ (see [3] Theorem 15).

On the other hand, if n is odd, then N is not a direct factor of G as a Sylow 2-subgroup of G is cyclic ([1]). We denote by $\pi(s)$ the set of primes dividing an integer $s(>0)$ and set $H^* = H \setminus \{\omega\}$, where $H = G/N$ and $\omega = \prod_{\sigma \in H} \sigma$. In this article, using D we define a map g from H to N satisfying for $\tau, \rho \in H^*$, $g(\tau) = g(\rho)$ iff $\{\tau, \tau^{-1}\} = \{\rho, \rho^{-1}\}$ and show that for any $\sigma \in H^*$ and any integer $m > 0$ with $\pi(m) \subset \pi(n)$, there exists an integer $k_{\sigma,m} \in \{1,2\}$ such that $\mathrm{ord}_{\mathrm{o}(\sigma)}(m) = k_{\sigma,m}\mathrm{ord}_{\mathrm{o}(g(\sigma))}(m)$. This result is a generalization of a result of Galati on even order n mentioned above. As an application we give a new proof of a result of Arasu-Pott on multipliers m of D ([1] Section 5).

2 Preliminaries

In this section we give several results which will be needed later.

Result 2.1. *(Arasu-Pott [1]) If an abelian group G contains an affine difference set, then a 2-Sylow subgroup of G is cyclic.*

For an integer $s > 0$, we denote by $\pi(s)$ the set of primes dividing s.

Result 2.2. *(A.J. Hoffman [4]) Let D be an affine difference set of order n in an abelian group. Then, if an integer $m(> 0)$ satisfies $\pi(m) \subset \pi(n)$, then m is a multiplier of D.*

We denote by $\mathrm{l.c.m.}(S)$ the least common multiple of a set $S(\subset \mathbb{N})$.
We can easily check the following (see Theorem 1.3.1(iii) of [2]).

Lemma 2.3. *Let G be an abelian group with generators $g_1, \cdots, g_m$. Then $\exp(G) = \mathrm{l.c.m.}(\{\mathrm{o}(g_i) \mid 1 \leq i \leq m\})$, where $\mathrm{o}(g_i)$ is the order of g_i.*

Let $a, s \in \mathbb{N}$ and $(a, s) = 1$. We denote by $\mathrm{ord}_s(a)$ the order of $a \pmod{s}$.

Lemma 2.4. *Let u, v and m be positive integers with $(m, uv) = 1$. Then,*

$$\mathrm{ord}_{\,\mathrm{l.c.m.}(u,v)}(m) = \mathrm{l.c.m.}(\mathrm{ord}_u(m), \mathrm{ord}_v(m)).$$

Proof. Set $a = \mathrm{ord}_u(m)$ and $b = \mathrm{ord}_v(m)$. Then
$(*)\ \ u \mid m^a - 1,\ \ u \nmid m^i - 1\ \ (\forall i < a), \qquad v \mid m^b - 1,\ \ v \nmid m^j - 1\ \ (\forall j < b)$.
Clearly $u, v \mid m^{\mathrm{l.c.m.}(a,b)} - 1$ and so $\mathrm{l.c.m.}(u, v) \mid m^{\mathrm{l.c.m.}(a,b)} - 1$. Hence $\mathrm{ord}_{\,\mathrm{l.c.m.}(u,v)}(m) \mid \mathrm{l.c.m.}(\mathrm{ord}_u(m), \mathrm{ord}_v(m))$.

Set $w = \mathrm{ord}_{\,\mathrm{l.c.m.}(u,v)}(m)$. Then $\mathrm{l.c.m.}(u, v) \mid m^w - 1$ and so $u \mid m^w - 1$ and $v \mid m^w - 1$. By $(*)$, $w = sa, w = tb$ for some $s, t \in \mathbb{N}$. Hence $\mathrm{l.c.m.}(a, b) \mid w = \mathrm{ord}_{\,\mathrm{l.c.m.}(u,v)}(m)$. Thus the lemma holds. □

3 Abelian groups and group extensions

In this section we assume that H and N are abelian groups. A map $c : H \times H \longrightarrow N$ is called a *factor set* if the following conditions are satisfied.

$$c(\sigma, \tau)c(\sigma\tau, \rho) = c(\sigma, \tau\rho)c(\tau, \rho)\ (\forall \sigma, \tau, \rho \in H) \tag{1}$$

$$\exists k \in N,\ c(\sigma, 1) = c(1, \tau) = k\ (\forall \sigma, \tau \in H) \tag{2}$$

Remark 3.1. If we put $z(\sigma, \tau) = c(\sigma, \tau)k^{-1}$, then z is a factor set in the usual sense (see [5] page 86)

The following holds.

Lemma 3.2. *If a map* $c : H \times H \longrightarrow N$ *is a factor set, then* $c(\sigma, \sigma^{-1}) = c(\sigma^{-1}, \sigma)$.

Proof. Put $\tau = \sigma^{-1}, \rho = \sigma$ in (1) and use (2). Then, as N is abelian, we have the lemma. □

We can easily verify the following.

Lemma 3.3. *Assume (1) and (2) and define a multiplication in* $\widehat{G} = H \times N$ *by* $(\sigma, a)(\tau, b) = (\sigma\tau, c(\sigma, \tau)ab)$.
Then the following holds.

- *(i)* $\widehat{G}$ *is a group with identity* $(1, k^{-1})$.
- *(ii)* $(\sigma, a)^{-1} = (\sigma^{-1}, c(\sigma, \sigma^{-1})^{-1}a^{-1}k^{-1})$.
- *(iii)* *Set* $\widehat{N} = \{1\} \times N$. *Then* $\widehat{N}$ *is a normal subgroup of* $\widehat{G}$.
- *(iv)* $\widehat{G}$ *is abelian if and only if* $c(\sigma, \tau) = c(\tau, \sigma)$ *for all* $\sigma, \tau \in H$.

Lemma 3.4. *Let* N *be a subgroup of an abelian group* G *and let* S *be a complete set of coset representatives of* $H := G/N (= \{Nx, Ny, \cdots\})$. *We define a map* $\widetilde{}$ *from* G *to* S *by* $\{\widetilde{x}\} = Nx \cap S$ *and a map* $c : H \times H \longrightarrow N$ *by* $c(Nx, Ny) = \widetilde{x}\,\widetilde{y}\,(\widetilde{xy})^{-1} (\in N)$. *Then,* $c(*, *)$ *is a factor set with* $k = \widetilde{1}$ *in (2) and* $\widehat{G}$ *defined in Lemma 3.3 is isomorphic to* G.

Proof. We define a map $f : G \longrightarrow \widehat{G}$ by $f(x) = (Nx, (\widetilde{x})^{-1}x)$. Then, for each $x, y \in G$,

$$\begin{aligned} f(x)f(y) &= (Nx, (\widetilde{x})^{-1}x)(Ny, (\widetilde{y})^{-1}y) = (Nxy, c(Nx, Ny)(\widetilde{x})^{-1}x(\widetilde{y})^{-1}y) \\ &= (Nxy, \widetilde{x}\widetilde{y}(\widetilde{xy})^{-1}(\widetilde{x})^{-1}x(\widetilde{y})^{-1}y) = (Nxy, (\widetilde{xy})^{-1}xy) = f(xy) \end{aligned}$$

Hence f is a homomorphism. On the other hand, for $x \in \mathrm{Ker}(f)$, $(Nx, (\widetilde{x})^{-1}x) = (N, k^{-1})$, where $k = \widetilde{1}$. From this we have $x \in N$ and $(\widetilde{x})^{-1}x = k^{-1}$. The former implies $\widetilde{x} = k$. It follows that $k^{-1}x = k^{-1}$ and so $x = 1$. Hence f is a monomorphism. As $|G| = |\widehat{G}|$, f is an isomorphism. □

4 Affine Difference Sets

Throughout this section we assume that D is an affine difference set of order n in an abelian group G relative to a subgroup N of G. Clearly Da is also an affine difference set relative to N for each $a \in G$. Set $H = G/N$.

In the rest of the article, elements of G are denoted by small Roman letters and elements of H by small Greek letters : $G = \{a, b, c, \cdots\}$, $H = \{\sigma, \tau, \rho, \cdots\}$. We use the following notations :

$$\omega = \prod_{\sigma \in H} \sigma, \qquad H^* = H \setminus \{\omega\}, \qquad w_0 = \prod_{x \in N} x \tag{3}$$

Lemma 4.1. *Let ω and w_0 be as defined in (3) and set $\omega = Nw$ for some $w \in G$. Then the following hold.*

(i) If $2 \mid n$, then $\omega = 1$ and $w_0 = 1$. In particular, $w \in N$

(ii) If $2 \nmid n$, then $\omega \neq 1, \omega^2 = 1$ and $w_0 \neq 1, w_0^2 = 1$. In particular, $w \notin N, w^2 \in N$.

Proof. It is well known that for any abelian group M.

$$\prod_{x \in M} x = \begin{cases} t & \text{if } t \text{ is a unique involution in } M, \\ 1 & \text{otherwise.} \end{cases}$$

If $2 \mid n$, then $|N| \equiv |H| \equiv 1 \pmod 2$. On the other hand, if $2 \nmid n$, then $|N| \equiv |H| \equiv 0 \pmod 2$. By Result 2.1, the lemma holds. □

Let $\omega(= Nw)$ be as in (3). We may assume that $D \cap Nw = \emptyset$ by exchanging D for its suitable translate if necessary. Then $S = D \cup \{w\}$ is a complete set of coset representatives of $G/N(= H)$.

Lemma 4.2. *Exchanging D for its suitable translate Da $(a \in N)$ if necessary, we may assume that*

$$\prod_{x \in D} x = 1. \tag{4}$$

Proof. By Lemma 4.1, $Nw = \omega = (Nw)(\prod_{x \in D} Nx)$. Hence $\prod_{x \in D} x \in N$. Set $t = \prod_{x \in D} x$ and $D_1 = Dt^{-1}$. Then $t \in N$ and $\prod_{x \in Dt^{-1}} x = (t^{-1})^n \prod_{x \in D} x = (t^{-1})^{n-1} = 1$. Thus the lemma holds. □

Definition 4.3. Let $d : H \longrightarrow G$ be a map defined by $\{d(\xi)\} = Nx \cap S$ for $\xi = Nx \in H$. Clearly $D = \{d(\xi) \mid \xi \in H^*\}$.

Remark 4.4. If $2 \mid n$, then we have $d(1) \notin D$ as $\omega = 1$. On the other hand, if $2 \nmid n$, then $d(1) \in D$ as $\omega \neq 1$.

Proposition 4.5. *Let c be a map from $H \times H$ to N defined by $c(\sigma, \tau) = d(\sigma)d(\tau)d(\sigma\tau)^{-1}$. Then the following hold.*

(i) $c(\sigma, 1) = c(1, \sigma) = d(1)$, $c(\sigma, \tau) = c(\tau, \sigma)$

(ii) Set $H_\sigma = H \setminus \{\omega, \sigma^{-1}\omega\}$ $(\sigma \neq 1)$. Then a map $c(\sigma, *) : H_\sigma \longrightarrow N$ defined by $\xi \mapsto c(\sigma, \xi)$ is bijective.

Proof. (i) immediately follows from Lemmas 3.3 and 3.4. Let $\sigma(\in H \setminus \{1\})$ and assume $c(\sigma, \tau) = c(\sigma, \rho)$ for some $\tau, \rho \in H_\sigma$ $(\tau \neq \rho)$. Then $d(\sigma)d(\tau)d(\sigma\tau)^{-1} = d(\sigma)d(\rho)d(\sigma\rho)^{-1}$. Hence $d(\tau)d(\sigma\tau)^{-1} = d(\rho)d(\sigma\rho)^{-1}$. As $\tau, \rho, \sigma\tau, \sigma\rho \neq \omega$, we have $d(\tau), d(\sigma\tau), d(\rho), d(\sigma\rho) \in D$. Thus either $d(\tau) = d(\rho)$ or $d(\tau) = d(\sigma\tau)$, which implies $\tau = \rho$ or $\sigma = 1$, a contradiction. □

We note that the converse of Proposition 4.5 is also true (cf. Theorem 4 of [3]).

Proposition 4.6. *Let G an abelian group of order n^2-1 with a cyclic Sylow 2-subgroup and let N be a subgroup of G of order $n-1$. Let H, ω and w_0 be as defined in Lemma 4.1. Let d_1 be an injection from $H^*(=H\setminus\{\omega\})$ to G and set $D=d_1(H^*)$. Set $d_1(\omega)=w$ and $H_\sigma = H\setminus\{\omega,\sigma^{-1}\omega\}$ for $\sigma\in H\setminus\{1\}$. Assume that the map d satisfies the following conditions.*

(i) $d_1(H)$ *is a complete set of coset representatives of G/N.*

(ii) *Let $c: H\times H \longrightarrow N$ be a map defined by $c(\sigma,\tau)=d_1(\sigma)d_1(\tau)d_1(\sigma\tau)^{-1}$. Then a map $c(\sigma,*) : H_\sigma \longrightarrow N \quad (\xi \mapsto c(\sigma,\xi))$ is bijective for every $\sigma \in H\setminus\{1\}$.*

Then $D=\{d_1(\sigma)\mid \sigma\in H^*\}$ is an affine difference set in G relative to N.

Proof. Let $\tau,\rho,\xi,\eta\in H^*$. Then $d_1(\tau),d_1(\rho),d_1(\xi),d_1(\eta)\in D$. Assume $d_1(\tau)d_1(\rho)^{-1}=d_1(\xi)d_1(\eta)^{-1}$ and $\tau\neq\rho$. Set $\sigma=(\tau\rho^{-1})^{-1}$. Then $\sigma\neq 1$. As $\tau\rho^{-1}=\xi\eta^{-1}$, $\rho=\sigma\tau,\eta=\sigma\xi$. It follows that $d_1(\tau)d_1(\sigma\tau)^{-1}=d_1(\xi)d_1(\sigma\xi)^{-1}$. Hence $d_1(\sigma)d_1(\tau)d_1(\sigma\tau)^{-1}=d_1(\sigma)d_1(\xi)d_1(\sigma\xi)^{-1}$. Thus $c(\sigma,\tau)=c(\sigma,\xi)$. By (ii), $\tau=\xi$ and so $\rho=\eta$. Therefore we have shown that for $x_1,x_2,x_3,x_4\in D$, if $x_1x_2^{-1}=x_3x_4^{-1}$, then $\{x_1,x_4\}=\{x_2,x_3\}$. On the other hand, $|G\setminus N| = n^2-n=|D|(|D|-1)$. Hence D is an affine difference set in G relative to N. □

5 Multipliers of Affine Difference Sets

In this section we assume that D is an affine difference set of order n in an abelian group G relative to a subgroup $N(\leq G)$. Set $H=G/N$ and let ω,w,w_0,H^* be as defined in section 4. By Lemma 4.2, we may assume that $\prod_{x\in D} x = 1$. Let maps c and d be as defined in Proposition 4.5 and Definition 4.3, respectively. In this section we study multipliers of affine difference sets.

The following result is well known.

Lemma 5.1. *$D^{(m)}=D$ for each integer $m(>0)$ such that $\pi(m)\subset\pi(n)$.*

Proof. Let Ω be the set of translates of D. A map φ from Ω to G defined by $\varphi(Dx)=\prod_{y\in Dx} y$ is bijective as $(n,|G|)=1$ and $\varphi(Dx)=c_0x^n$, where $c_0=\prod_{d\in D} d$. By Result 2.2, $D^{(m)}=Da$ for some $a\in G$. Hence, as $\varphi(Da)=\varphi(D^{(m)})=\varphi(D)^m=1$, we have $Da=D$. Thus $D^{(m)}=D$ and the lemma holds. □

By the definition of d we have the following.

Lemma 5.2. *Let m be a positive integer such that $\pi(m)\subset\pi(n)$. If $\xi^m=\omega$ for some $\xi\,(\in H)$, then $\xi=\omega$.*

Proof. As $(m, n+1) = 1$, there exist $a, b \in \mathbb{Z}$ such that $am + b(n+1) = 1$. Hence $\xi = \xi^{am+b(n+1)} = (\xi^m)^a = \omega^a$. By Lemma 4.1, it suffices to consider the case $2 \nmid n$. Then $2 \nmid a$ and therefore $\xi = \omega$. □

Lemma 5.3. *Let m be a positive integer such that $\pi(m) \subset \pi(n)$. Then $d(\xi)^m = d(\xi^m)$ for any $\xi \in H^*(= H \setminus \{\omega\})$.*

Proof. By definition of d, $d(\xi)^m = ad(\xi^m)$ for some $a \in N$. By Lemma 5.2, $\xi^m \neq \omega$ and so $d(\xi^m) \in D$. As $D^{(m)} = D$, $a = 1$. □

Definition 5.4. We define a map $g : H \longrightarrow N$ by $g(\sigma) = \prod_{\xi \in H} c(\sigma, \xi)$.

Lemma 5.5. *The following hold.*

(i) $g(1) = d(1)^2$.

(ii) *If $\sigma \neq \omega$, then $g(\sigma) = d(\sigma)d(\sigma^{-1})$. In particular, for any $\sigma \in H$, $g(\sigma) = g(\sigma^{-1})$.*

Proof. By definition, $g(1) = d(1)^{n+1} = d(1)^{n-1}d(1)^2$. Hence (i) holds. We note that $g(\sigma) = \prod_{\xi \in H} d(\sigma)d(\xi)d(\sigma\xi)^{-1} = (\prod_{\xi \in H} d(\sigma))(\prod_{\xi \in H} d(\xi))(\prod_{\xi \in H} d(\sigma\xi))^{-1} = d(\sigma)^{n+1}$. On the other hand, by Lemma 5.3, $d(\sigma)^n = d(\sigma^n) = d(\sigma^{-1})$. Therefore $g(\sigma) = d(\sigma)d(\sigma^{-1})$. □

Lemma 5.6. *If $\pi(s) \subset \pi(n)$ and $\sigma \neq \omega$, then $g(\sigma)^s = g(\sigma^s)$.*

Proof. As $D^{(s)} = D$, the lemma follows immediately from Lemma 5.3. □

Proposition 5.7. *(i) If $\sigma \neq \omega, \tau \neq \omega$ and $g(\sigma) = g(\tau)$, then $\{\sigma, \sigma^{-1}\} = \{\tau, \tau^{-1}\}$.*
(ii) Assume $2 \nmid n$ and $\sigma \neq \omega$. If $g(\sigma) = g(1)$, then $\sigma = 1$.

Proof. Assume $g(\sigma) = g(\tau)$ for some $\sigma, \tau \in H^*$. Then, by Lemma 5.5(ii), $d(\sigma)d(\sigma^{-1}) = d(\tau)d(\tau^{-1})$. Hence $d(\sigma)d(\tau)^{-1} = d(\tau^{-1})d(\sigma^{-1})^{-1}$. From this, $\{\sigma, \sigma^{-1}\} = \{\tau, \tau^{-1}\}$. Thus (i) holds.

Assume $2 \nmid n$ and $g(\sigma) = g(1)$ for some $\sigma \in H^*$. Then, by assumption, $d(\sigma), d(1) \in D$. Since $g(\sigma) = g(1)$, $d(\sigma)d(\sigma^{-1}) = d(1)d(1)$ by Lemma 5.5. Hence $d(\sigma)d(1)^{-1} = d(1)d(\sigma^{-1})^{-1}$. Thus $\sigma = 1$ and (ii) holds. □

Lemma 5.8. *$N = \langle g(\sigma) \mid n\ \sigma \in H \rangle$. In particular* $\mathrm{l.c.m.}(\{\mathrm{o}(g(\sigma)) \mid \sigma \in H\}) = \exp(N)$.

Proof. Set $N_0 = \langle g(\sigma) \mid \sigma \in H \rangle$. If $2 \mid n$, $|\mathrm{Im}(g)| \geq \frac{n+1-1}{2} = \frac{n}{2}$ by Proposition 5.7. Hence $|N_0| \geq \frac{n}{2}$ and so $|N_0| = n-1 = |N|$ as $n-1$ is odd. If $2 \nmid n$, similarly $|\mathrm{Im}(g)| \geq \frac{n+1-2}{2} + 1 = \frac{n-1}{2} + 1$ by Proposition 5.7. Hence $|N_0| = |N|$. Therefore $N_0 = N$. By Lemma 2.3 we have $\mathrm{l.c.m.}(\{\mathrm{o}(g(\sigma)) \mid \sigma \in H\}) = \exp(N)$. □

The following is a generalization of Theorem 15 of [3].

Theorem 5.9. *Let D be an affine difference set satisfying (3)(4) in an abelian group G of order $n^2 - 1$ relative to N and let g be a map from $H(= G/N)$ to N defined in Definition 5.4. If $\pi(m) \subset \pi(n)$ and $\sigma \in H^*$, then there exists an integer $k_{\sigma,m} \in \{1, 2\}$ such that $\mathrm{ord}_{\mathrm{o}(\sigma)}(m) = k_{\sigma,m}\mathrm{ord}_{\mathrm{o}(g(\sigma))}(m)$.*

Proof. Set $e = \mathrm{ord}_{\mathrm{o}(g(\sigma))}(m)$ and $f = \mathrm{ord}_{\mathrm{o}(\sigma)}(m)$. Then $m^f - 1 = \mathrm{o}(\sigma)a$ for some $a \in \mathbb{N}$. By Lemma 5.6, $g(\sigma) = g(\sigma^{m^f - \mathrm{o}(\sigma)a}) = g(\sigma^{m^f}) = g(\sigma)^{m^f}$. Hence $m^f - 1 = \mathrm{o}(g(\sigma))b$ for some $b \in \mathbb{N}$. From this $e \mid f$. On the other hand, $m^e - 1 = \mathrm{o}(g(\sigma))k$ for some $k \in \mathbb{N}$. Hence $g(\sigma) = g(\sigma)^{m^e - \mathrm{o}(g(\sigma))k} = g(\sigma)^{m^e}$. By Lemma 5.6, $g(\sigma)^{m^e} = g(\sigma^{m^e})$. It follows from Lemma 5.2 and Proposition 5.7 that $\sigma^{m^e} \in \{\sigma, \sigma^{-1}\}$. If $\sigma^{m^e} = \sigma$, then $f \mid e$ and so $f = e$. If $\sigma^{m^e} = \sigma^{-1}$, then $\sigma^{m^{2e}} = \sigma$ and so $f \mid 2e$. Therefore, we have either $f = e$ or $f = 2e$ and hence the theorem holds. □

Though the following corollary is substantially contained in [1] Section5 (see also Corollary 18 of [3]), we give a new proof as an application of Theorem 5.9.

Corollary 5.10. ([1]) *Assume D is an affine difference set of order n in an abelian group G relative to a subgroup N of G. Let m be a positive integer satisfying $\pi(m) \subset \pi(n)$. Then one of the following holds.*

(i) $\mathrm{ord}_{\exp(H)}(m) = \mathrm{ord}_{\exp(N)}(m)$.

(ii) $\mathrm{ord}_{\exp(H)}(m) = 2 \cdot \mathrm{ord}_{\exp(N)}(m)$.

Proof. Set $e_H = \exp(H)$ and $e_N = \exp(N)$. Let α be an element of H satisfying $\mathrm{o}(\alpha) = e_H$. By Theorem 5.9, $\mathrm{ord}_{e_H}(m) = \mathrm{ord}_{\mathrm{o}(\alpha)}(m) = k_\alpha \mathrm{ord}_{\mathrm{o}(g(\alpha))}(m)$ for some integer $k_{\sigma,m} \in \{1, 2\}$. Hence $\mathrm{ord}_{e_H}(m) \mid 2\mathrm{ord}_{\mathrm{o}(g(\alpha))}(m)$. Applying Lemmas 2.4 and 5.8, we have $\mathrm{ord}_{e_H}(m) \mid 2\mathrm{ord}_{e_N}(m)$. On the other hand, $k_{\sigma,m}\mathrm{ord}_{\mathrm{o}(g(\sigma))}(m) = \mathrm{ord}_{\mathrm{o}(\sigma)}(m)$ for any $\sigma \in H$ by Theorem 5.9. Hence $\mathrm{ord}_{\mathrm{o}(g(\sigma))}(m) \mid \mathrm{ord}_{\mathrm{o}(\sigma)}(m)$. By Lemma 2.4, $\mathrm{ord}_{\mathrm{o}(g(\sigma))}(m) \mid \mathrm{ord}_{e_H}(m)$. Thus $\mathrm{ord}_{e_N}(m) \mid \mathrm{ord}_{e_H}(m)$ and the corollary holds. □

We also have the following.

Corollary 5.11. *Let G, N, H and n be as in Corollary 5.10. If $\pi(m) \subset \pi(n)$, then one of the following holds.*

(i) $\mathrm{ord}_{\exp(G)}(m) = \mathrm{ord}_{\exp(H)}(m)$.

(ii) $\mathrm{ord}_{\exp(G)}(m) = 2 \cdot \mathrm{ord}_{\exp(H)}(m)$.

Proof. Set $e_G = \exp(G), e_H = \exp(H), e_N = \exp(N)$ and $k = \mathrm{l.c.m.}(e_H, e_N)$.

Assume $2 \mid n$. Then $e_G = k = e_H e_N$. Hence $\mathrm{ord}_{e_G}(m) = \mathrm{l.c.m.}(\mathrm{ord}_{e_H}(m), \mathrm{ord}_{e_N}(m))$. Applying Corollary 5.10, the corollary holds.

Assume $2 \nmid n$. Then $e_G = 2k = e_H e_N$. Hence, $\mathrm{ord}_{e_G}(m) = \mathrm{ord}_{2k}(m) \in \{\mathrm{ord}_k(m), 2\mathrm{ord}_k(m)\}$. Thus the corollary also holds in this case. □

We note that computional results have confirmed the prime power conjecture for affine difference sets ([6], [7], [8]). In [7], it has been checked that the order n has to be a prime power in abelian case if $n \leq 1,0000$.

Applying Corollary 5.10 to abelian affine difference sets of odd order $n \leq 100,000$ we did the following test by GAP to get a list of n which can not be ruled out.

(i) Choose an odd integer $n \leq 100,000$ and let $\{p_1, p_2, \cdots, p_s\}$ be the set of prime divisors of n.

(ii) Let $q_1^{e_1} q_2^{e_2} \cdots q_t^{e_t}$ be the prime factorization of $n-1$.

(iii) Let $r_1^{f_1} r_2^{f_2} \cdots r_u^{f_u}$ be the prime factorization of $n+1$.

(iv) Choose $b = q_1^{i_1} q_2^{i_2} \cdots q_t^{i_t}$, where $1 \leq i_k \leq e_k$ for each $k(\leq t)$ and $c = r_1^{j_1} r_2^{j_2} \cdots r_u^{j_u}$, where $1 \leq j_k \leq f_k$ for each $k(\leq u)$.

(v) If $\mathrm{ord}_b(p_i)/\mathrm{ord}_c(p_i) \in \{1, 2\}$ for each $i(\leq s)$, then add n to the list.

Then the list is as follows.

$33, 55, 77, 259, 309, 325, 437, 511, 513, 611, 649, 687, 843, 901, 973, 1347, 1351, 1397, 1405, 1585, 1751, 1757, 1939, 2049, 2169, 2369, 2427, 2669, 2763, 3649, 5001, 5251, 5489, 5699, 5951, 7379, 7441, 8885, 8935, 9369, 9801, 10467, 10827, 11333, 11391, 12147, 12151, 12629, 12701, 13323, 13393, 13551, 13853, 14333, 14769, 15191, 15557, 15637, 16255, 18027, 18267, 18431, 19999, 22757, 23419, 24319, 24483, 24577, 24603, 25089, 25271, 28323, 30483, 30501, 31853, 32645, 32805, 33025, 34107, 34993, 36027, 36437, 36507, 36991, 37613, 44199, 45463, 45871, 46973, 47117, 52549, 52587, 56251, 57961, 59291, 60031, 60363, 60365, 60797, 61735, 62163, 62531, 62667, 63713, 64079, 67923, 68095, 68427, 72837, 76049, 76277, 77907, 80187, 81191, 82443, 82783, 85623, 87197, 90605, 92611, 94391, 95039, 95171, 95941, 97363, 98099, 99933$

References

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

[2] D. Gorenstein, *Finite Groups*, Harper & Row, New York, Evanston, and London (1968)

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

[4] A.J. Hoffman, Cyclic affine planes, *Cadad. J. Math.* Vol. 4 (1952), pp. 295-301.

[5] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, New York (1967)

[6] D. Jungnickel and A. Pott, Computional non-existence results for abelian affine difference sets, *Congr. Numer.* Vol. 68 (1989), pp. 91-98.

[7] D. Jungnickel and A. Pott, Perfect and almost perfect sequences, *Discrete Applied Mathematics* Vol. 95 (1999), pp. 331-359.

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