ASM Sc. J., 12, Special Issue 1, 2019 for IQRAC2018, 1-9

Results on Exhaustion Sets in Abelian Group

Denis C.K. Wong*

DMAS, LKC FES,
Universiti Tunku Abdul Rahman, Jalan Sungai Long,
Bandar Sungai Long, Cheras, 43000, Kajang,
Selangor Darul Ehsan, Malaysia.

**Corresponding author: deniswong@utar.edu.my*

In this paper, we improve earlier results on exhaustion sets in abelian group by presenting a systematical group ring approach together with group characters. Then, a new lower bound is constructing to determine the existence of an exhaustion set in abelian group H containing a cyclic Sylow $q-$subgroup and q is self-conjugate modulo $exp(H)$.
Keywords: Exhaustion set, group ring, character, self-conjugate

I. Introduction

Sumset was initially introduced by Cauchy in (Cauchy, 1813). His result was subsequently discussed by Davenport in (Davenport, 1935) and the theorem was later known as Cauchy-Davenport's theorem. Eliahou and Kervaire performed a thorough study on sumsets and its related concepts in vector spaces and various abelian groups, see (Eliahou and Kervaire, 1998, 2005, 2006, 2010, Eliahou et al., 2003). Beside of abelian groups, some recent results on sumsets in finite non-abelian groups (Eliahou and Kervaire, 2006, 2007) were derived by modifying the Cauchy-Davenport's theorem. For recent results on sumsets, see (Bajnok and Matzek, 2015, 2016, Eliahou and Kervaire, 2007, 2010, Klopsch and Lev, 2009). In this paper, we will study a different form of combinatorial objects, which is analogue to sumset. Here, we are interested in studying product set in abelian group. More formally, for a nonempty subset S of a finite abelian group G, we say that S is exhaustive if there exists a positive integer n such that $S^n = G$. The number $e(S) = \min\{t \mid S^t = G\}$ is called the exhaustion number of the set S. We said that S is an exhaustion set of G with exhaustion number $e(S)$. Note that we adopt the definition of exhaustion set used in (Chin, 2003). However, the definition of exhaustion set can be more intelligibly described using the notion of group ring. Traditionally, the notion of group ring has been used to describe many combinatorial objects (Beth et al., 1999, Davis and Jedwab, 1997, Ma and Ng, 2009, Pott, 1995, Turyn, 1965). In term of group ring, S is exhaustive if there exists a positive integer n such that $G \subseteq S^n$, that is, $S^n = G + X$ for some $X \in \mathbf{Z}[G]$.

Our approach to study exhaustion set is first by viewing it as an element of group ring. Then, with the help of character theory (Isaacs, 1976, Pott, 1995), we obtain more properties for exhaustion set. By using the well-known orthogonality relations, see Lemma 1.2.1 in (Pott, 1995), S is an exhaustion set with $e(S) = n$ that satisfies the properties: Suppose $\chi \in G^*$, where G^* is the group of all characters of G. If χ is the principal character of G, then we have $|S|^n = |G| + |X|$. On the other hand, if χ is a non-principal character of G, then $|\chi(S)|^n = |\chi(X)|$. Therefore, we introduce the following more general definition of exhaustion set, compare to Chin (2003).

Definition 1. *Let G be a finite abelian group. A subset $S \subset G$ is called an $(a, n)-$exhaustion set with modulus w provided*

(a) $e(S) = n$,

(b) $a = |S| = (|G| + |X|)^{\frac{1}{n}}$, *and*

(c) *For every non-principal character* χ *of* G, $|\chi(S)| = |\chi(X)|^{\frac{1}{n}} = w$.

From Definition 1, we see that the case when $a = 1$ is trivial since any S with $a = |S| = 1$ has the property $e(S) = \infty$. Also, if $a = |S| = |G|$, it follows that $e(S) = 1$, in which we also consider this as a trivial case. Thus, from now onward, we assume that $2 \leq a \leq |G| - 1$. For some cases when the parameter w is not needed for determining the existence of an $(a, n)-$exhaustion set, we should just mention the parameters a and n.

Contribution. The main contribution of this paper is to obtain some relationships between the parameters a, w and n. Our main result on the bound of exhaustion set which will be proved in Section 4 is given as follows:

Theorem 1. *Let* q *be a prime and* H *be an abelian group such that the Sylow* q*-subgroup of* H *is cyclic. Suppose* $Y \in \mathbf{Z}[H]$ *satisfies*

(a) q *is self-conjugate modulo* $\exp(H)$*;*

(b) $q^r \,||\chi(Y)|^2$ *for all non-principal character* χ *of* H*; and*

(c) *there exists at least one* i *with* $0 \leq i \leq n$, *such that* $\binom{n}{i} q^{(\lfloor r/2 \rfloor - 1)i + n - 1} > |H|$.

Then, $e(Y) > n$.

Paper Organization. In Section 2, we provide some examples and basic constructions of exhaustion sets in abelian groups. In Section 3, we derive some fundamental results which will be used to determine many families of exhaustion sets in abelian groups. In Section 4, we derive a lower bound for exhaustion sets in an abelian group H containing a cyclic Sylow $q-$subgroup and q is self-conjugate modulo $exp(H)$.

II. Preliminaries

We begin by stating some basic concepts which will be used throughout this paper. In general, the character values are uniquely determined by the group ring element as shown by the following well-known Fourier inversion formula, refer Lemma 1.2.2 (Beth et al., 1999) for a proof.

Lemma 1. *Let* G *be a finite abelian group and* $A = \sum_{g \in G} a_g g \in \mathbf{C}[G]$. *Then*

$$a_g = \frac{1}{|G|} \sum_{\chi \in G^*} \chi(A)\chi(g^{-1}).$$

The finite Fourier transform F is a mapping from $\mathbf{C}[G]$ to $\mathbf{C}[G^*]$ such that it maps $A \in \mathbf{C}[G]$ to $F(A) = \sum_{\chi \in G^*} \chi(A)\chi \in \mathbf{C}[G^*]$. For every $g \in G$, we identify g with the character $g : G^* \to \mathbf{C}$ of G^* such that $g(\chi) = \chi(g)$ for all $\chi \in G^*$. Suppose $B = \sum_{\chi \in G^*} b_\chi \chi \in \mathbf{C}[G^*]$. Then, we can also apply the finite Fourier transform to B as follows:

$$\begin{aligned} F(B) &= \sum_{g \in G} g\Big(\sum_{\chi \in G^*} b_\chi \chi\Big) g \\ &= \sum_{g \in G} \Big(\sum_{\chi \in G^*} b_\chi \chi(g)\Big) g \in \mathbf{C}[G]. \end{aligned}$$

We refer the reader to (Ma and Ng, 2009) for more information on the finite Fourier transform. The next lemma is important as it will be used to prove some results in this paper. We recall that if G is a finite abelian group of order mu and U is a subgroup of G of order u, then we define $U^\perp = \{\chi \in G^* | \chi(g) = 1, \forall g \in U\}$.

Lemma 2. *Let* G *be a finite abelian group of order* mu *and* U *be a subgroup of* G *of order* u. *Then, the following hold:*

(a) $U^\perp$ *is a subgroup of* G^* *of order* $|G/U|$.

(b) $F(\chi_0) = G$,

(c) $F(U^\perp) = mU$, *and*

(d) $F(G^*) = mu$.

(e) *For every* $A \in \mathbf{C}[G]$, $F(F(A)) = |G|A^{(-1)}$.

We start by giving some examples of exhaustion sets.

Example 1. *Let G be a cyclic group of order 7 with generator g. For $S = g+g^2+g^4$, we see that $e(S) = 3$ as S can be written in the form*

$$S^3 = 6+3g+3g^2+4g^3+3g^4+4g^5+4g^6 = G+X,$$

where $X = 5+2g+2g^2+3g^3+2g^4+3g^5+3g^6 \in \mathbf{Z}[G]$. Thus, S is an $(3,3)-$ exhaustion set in G.

Example 2. *Let $G = \langle x, y \mid x^2 = y^2 = 1\rangle \cong \mathbf{Z}_2^2$. Let $B_0 = 1+x$ and $B_1 = 1+xy$. Consider the set $\{B_0, B_1\}$ which is an $(2,2,2)-$ building set in G relative to $\langle x\rangle$, see Davis and Jedwab (1997). Suppose $S = B_0 + B_1$, then it is straightforward to verify that $e(S) = 2$, and so S is an $(3,2)-$exhaustion set in $\mathbf{Z}_2^2$.*

We list three families of difference sets. For some well-known constructions of difference sets, see (Beth et al., 1999, Chapter VI) and (Pott, 1995, Chapter 2).

(*i*) A k-subset A of G of order v is an $(v,k,\lambda)-$ difference set if and only if $AA^{(-1)} = (k-\lambda)+\lambda G$.

(*ii*) A k-subset R of G of order mn is an $(m,n,k,\lambda)-$ relative difference set relative to a subgroup N of order n if and only if $RR^{(-1)} = k+\lambda(G-N)$.

(*iii*) A k-subset D of G of order mn is an $(m,n,k,\lambda_1,\lambda_2)-$ divisible difference set relative to a subgroup N of order n if and only if $DD^{(-1)} = (k-\lambda_1)+(\lambda_1-\lambda_2)N+\lambda_2 G$.

Furthermore, a set S is called reversible if S is fixed by -1, that is, $S^{(-1)} = S$, see (Beth et al., 1999, Chapter IV).

Example 3. *Suppose there exist families of reversible difference sets as defined previously in parts (i) to (iii). Then, all these families of reversible difference sets are $(k,2)-$ exhaustion sets.*

We provide three constructions of exhaustion sets in abelian groups. The first and the second constructions are similar to the complementary and extension of many combinatorial objects. The last one is a result for elementary abelian 2-group.

Theorem 2. *Suppose G is a finite abelian group and let H be any subset of G. Then, $G-H$ is an $(|G|-|H|,2)-$ exhaustion set in G.*

Proof. Note that $(G-H)^2 = (|G|-2|H|)G + H^2$, and so $e(G-H) = 2$. □

Theorem 3. *Let $G = \langle\theta\rangle \times H$, where $o(\theta) = 2$ and H is an abelian group of odd order. Suppose $B \subseteq H$ with $e(B) = n$. Then, $B \cup \theta B$ is an $(2|B|,n)-$ exhaustion set in G provided n is odd.*

Proof. Since $B \subseteq H$ with $e(B) = n$, then we have $B^n = H + X_B$ for some $X_B \in \mathbf{Z}[H]$. Next, we compute

$$\begin{aligned}(\theta+\theta B)^n &= \sum_{i=0}^{n}\binom{n}{i}\theta^i B^n \\ &= \sum_{i=0}^{n}\binom{n}{i}\theta^i (H+X_B) \\ &= \sum_{i=0}^{n}\binom{n}{i}\theta^i H + \sum_{i=0}^{n}\binom{n}{i}\theta^i X_B \\ &= \sum_{i=0}^{n}\binom{n}{i}\theta^i H + A,\end{aligned}$$

for some $A \in \mathbf{Z}[G]$. Upon expanding the summation, we have

Case 1: If n is even, then $(\theta+\theta B)^n = \alpha\lceil\frac{n+1}{2}\rceil + \beta\lfloor\frac{n-1}{2}\rfloor\theta H + A'$,

Case 2: If n is odd, then $(\theta+\theta B)^n = \frac{n+1}{2}(\omega H + \lambda\theta H) + A''$,

where $\alpha,\beta,\omega,\lambda \in \mathbf{Z}^+, A', A'' \in \mathbf{Z}[G]$. Therefore, we see that $B \cup \theta B \subseteq G$ with $e(B\cup\theta B) = n$ provided n is odd. □

Theorem 4. *Let $G = \langle g_1, g_2, \ldots, g_t \mid g_i^2 = 1$ for all $i, 1 \le i \le t\rangle$ be an elementary abelian 2-group of order 2^t for every $t \ge 2$. Suppose $S = 1 + \sum_{i=1}^{t} g_i$. Then, S is an $(t+1,t)-$ exhaustion set.*

Proof. By using the multinomial theorem, we have

$$S^t = \sum_{\sum_{i=0}^{t} n_i = t} \binom{t}{n_0, n_1, \ldots, n_t} 1^{n_0} g_1^{n_1} \ldots g_t^{n_t}.$$

Next, we form the equation $n_1 + \cdots + n_t = t-1$, we see that by using the pigeonhole principle, at least one of the n_i must be 0. Thus, we conclude that $g_1 g_2 \ldots g_t \notin S^{t-1}$ which implies that $e(S) > t-1$. Finally, together with the equation of S^t, we deduce that S is an $(t+1, t)-$ exhaustion set. □

III. Results on Exhaustion Number

Let t be any integer, we define $A^{(t)} = \sum_{g \in G} a_g g^t$ for $A = \sum_{g \in G} a_g g \in \mathbf{Z}[G]$. We start with the following simple result.

Proposition 1. *Let G be a finite multiplicative abelian group and $A \subset G$. Then, $e(A) = n$ if and only if $e(A^{(-1)}) = n$.*

Proof. Given $e(A) = n$. Then, $A^n = G + X$ for some $X \in \mathbf{Z}[G]$. Hence, $(A^{(-1)})^n = (A^n)^{(-1)} = (G+X)^{(-1)} = G^{(-1)} + X^{(-1)} = G + X^{(-1)}$. Suppose there exists an integer $k < n$ such that $(A^{(-1)})^k = G + Y$ for some $Y \in \mathbf{Z}[G]$. Then, $A^k = ((A^k)^{(-1)})^{(-1)} = ((A^{(-1)})^k)^{(-1)} = (G + Y)^{(-1)} = G^{(-1)} + Y^{(-1)} = G + Y^{(-1)}$, which contradicts $e(A) = n$. Therefore, we conclude that $e(A^{(-1)}) = n$. On the other hand, the converse of this statement can be proved in a similar way.

□

From Example 1, by using Proposition 1, we see that $D^{(-1)} = g^6 + g^5 + g^3$ is also an $(3, 3)-$ exhaustion set in G.

Proposition 2. *Let G be a finite abelian group. Suppose $A \subseteq G$ with $e(A) = n$. Then, $A^{(n)} = G + Z$ for some $Z \in \mathbf{Z}[G]$.*

Proof. Given $A \subseteq G$. Then, we have $A^{(n)} \subseteq A^n$ for all $n \geq 1$. Thus, $A^n = A^{(n)} + X$, for some $X \in \mathbf{Z}[G]$. Since $e(A) = n$, it follows that $A^n = Y + G$ for some $Y \in \mathbf{Z}[G]$. Thus, we have $Y + G = A^{(n)} + X$ which implies that $A^{(n)} = G + (Y - X)$, where $Y - X \in \mathbf{Z}[G]$. □

The partial converse of Proposition 2 is also true.

Proposition 3. *Let G be a finite abelian group and $A \subseteq G$. Suppose n is the smallest integer such that $A^{(n)} = G + Z$ for some $Z \in \mathbf{Z}[G]$. Then $e(A) = n$.*

Proof. Clearly, $G + Z \subseteq A^n$. Hence, we can write $A^n = G + Z + W$ for some $W \in \mathbf{Z}[G]$. Suppose there exists a $k < n$ such that $A^k = G + V$ for some $V \in \mathbf{Z}[G]$. As $A^k \subset A^n$ and $A^k = A^{(k)} + T$ for some $T \in \mathbf{Z}[G]$, then we have $A^{(k)} = G + (V - T)$ which contradicts the choice of n. Therefore, $e(A) = n$. □

The following result is taken from (Chin, 2003), but we derive a proof by using the notation of group ring.

Proposition 4. *Let G be a finite abelian group and $S \subseteq T \subseteq G$. Then $e(T) \leq e(S)$.*

Proof. Given $S \subseteq T$, it follows that $T = S + X$ for some $X \in \mathbf{Z}[G]$. Since $e(S) = n$ and by using Proposition 3, we obtain $S^{(n)} = G + Y$ for some $Y \in \mathbf{Z}[G]$. Hence, we have $(T - X)^{(n)} = G + Y$. By applying the Binomial theorem to $(T - X)^{(n)}$, we obtain $T^{(n)} = G + W$ for some $W \in \mathbf{Z}[G]$. Therefore, $e(T) \leq n$. □

Proposition 5. *Let G be an abelian group. Suppose H is a subgroup of G and $S \subseteq H$. Then, when $S \subseteq G$, $e(S) = nm$ if and only if $e(X) = m$ provided $S^n = H + X$ for some $X \in \mathbf{Z}[H]$.*

Proof. By using the Binomial theorem, we have $(S^n)^m = (H + X)^m = \sum_{i=0}^{m} \binom{m}{i} H^i X^{m-i} = X^m + HA = Y + G + HA$, for some $A, Y \in \mathbf{Z}[G]$. Therefore, $e(S) = nm$. □

In many times, it is beneficial to work with homomorphic images of a group. To accomplish this, if $\alpha : G \to H$ is any mapping from G into a group H, it follows that we can extend α linearly from the group ring $R[G]$ into the

group ring $R[H]$. Thus, $\alpha(A) = \sum_{g\in G} a_g\alpha(g)$ for $A = \sum_{g\in G} a_g g \in R[G]$. We use α to denote both the group homomorphism and the group ring homomorphism when it is clear from the context that which homomorphism we are dealing with.

Theorem 5. *Let G and H be finite abelian groups and $\alpha : G \to H$ be an epimorphism. Suppose $S \subseteq G$ with $e(S) = n$. Then, $\alpha(S) \subseteq H$ with $e(\alpha(S)) = n$.*

Proof. Given $S \subseteq G$ with $e(S) = n$. Then, by using Proposition 3, we have $S^{(n)} = G + X$ for some $X \in \mathbf{Z}[G]$. Extend α linearly from $\mathbf{Z}[G]$ onto $\mathbf{Z}[H]$ so that α is a group ring epimorphism from $\mathbf{Z}[G]$ onto $\mathbf{Z}[H]$. Then $(\alpha(S))^{(n)} = \alpha(S^{(n)}) = \alpha(G + X) = \alpha(G) + \alpha(X) = H + \alpha(X)$, for some $\alpha(X) \in \mathbf{Z}[H]$. Now, assume that $e(\alpha(S)) = k < n$. Then, we have $(\alpha(S))^{(k)} = H + W$, for some $W \in \mathbf{Z}[H]$ and so $S^{(k)} = G + W' + ker(\alpha)$, for some $W' \in \mathbf{Z}[G]$, which contradicts $e(S) = n$. Therefore, $e(\alpha(S)) = n$. □

In the previous proof, the importance of the kernel of an epimorphism can be seen. The following result which is a refinement of a result in (Ma, 1996) derived a general form for the kernel of a ring homomorphism.

Theorem 6. *Let $G = \langle g\rangle \times H$ be an abelian group with $o(g) = q^r$ where q is a prime and $r \geq 1$. Suppose $\sigma : \mathbf{Z}[G] \to \mathbf{Z}[\xi_{q^r}][H]$ is the ring homomorphism such that $\sigma(g) = \xi_{q^r}$ and $\sigma(h) = h, \forall h \in H$. Then*

$$ker(\sigma) = \left\{\langle g^{q^{r-1}}\rangle X | X \in \mathbf{Z}[G]\right\}.$$

Proof. We write ξ_{q^r} as ξ. Let $A = \left\{\langle g^{q^{r-1}}\rangle X \mid X \in \mathbf{Z}[G]\right\}$. Suppose $y \in A$. Then $y = \langle g^{q^{r-1}}\rangle X$ for some $X \in \mathbf{Z}[G]$. Since $\langle g^{q^{r-1}}\rangle = \sum_{i=0}^{q-1} g^{iq^{r-1}}$ is the subgroup generated by $g^{q^{r-1}}$ and thus y can be written as

$$y = \left(\sum_{i=0}^{q-1} g^{iq^{r-1}}\right) X.$$

Hence, we have $\sigma(y) = 0$ and so $y \in ker(\sigma)$. Therefore, $A \subseteq ker(\sigma)$. Next, we let

$$y = \sum_{h\in H}\sum_{i=0}^{q^r-1} a_{ih} g^i h \in \mathbf{Z}[G]$$

with $a_{ih} \in \mathbf{Z}$. If $y \in ker(\sigma)$, then $\sigma(y) = 0$ and so $\sum_{i=0}^{q^r-1} a_{ih}\xi^i = 0$ for all $h \in H$. Since $\sum_{i=0}^{q-1} x^{iq^{r-1}}$ is a minimal polynomial of ξ over $\mathbf{Z}$, then $\langle g^{q^{r-1}}\rangle = \sum_{i=0}^{q-1} g^{iq^{r-1}}$ divides $\sum_{i=0}^{q^r-1} a_{ih} g^i$ for all $h \in H$. Thus, the results follows directly. □

The following corollary can be deduced directly from Theorem 6.

Corollary 1. *Let $G = \langle g\rangle \times H$ be an abelian group with $o(g) = q^r$ where q is a prime and $r \geq 1$. Suppose $\sigma : \mathbf{Z}[G] \to \mathbf{Z}[\xi_{q^r}][H]$ is the ring homomorphism such that $\sigma(g) = \xi_{q^r}$ and $\sigma(h) = h, \forall h \in H$. If $e(\sigma(X)) = n$, then $e(X) = n$ for every $X \in \mathbf{Z}[G]$.*

IV. Main Result: The Lower Bound for Exhaustion sets

As previously mentioned, knowing the character values of a group ring element can assist us to recover the group ring element. In this section, we state some well-known results from (Beth et al., 1999, Ma, 1996, Pott, 1995, Turyn, 1965). Hence, we relate all these results to the existence of exhaustion sets. For the reader's convenience, we include the proof which is derive by using the finite Fourier transform.

Proposition 6. *Let G be a finite abelian group. Suppose $S = \sum_{g\in G} a_g g \in \mathbf{Z}[G]$ satisfies $\chi(S) = 0$ for all non-principal characters χ of G. Then $S^{(-1)} = mG$ for some $m \in \mathbf{Z}$. Furthermore, $|G| \mid |S|$.*

Proof. By applying finite Fourier transform to S, we have $F(S) = \sum_{\chi\in G^*} \chi(S)\chi = \chi_0(S)\chi$. By applying finite Fourier transform again and by using Lemma 2, we obtain

$$|G|S^{(-1)} = F(F(S)) = |S|F(\chi_0)$$

and so $S^{(-1)} = \frac{|S|}{|G|}G$, where $\frac{|S|}{|G|} \in \mathbf{Z}$. It follows that $|G| \mid |S|$.

□

Proposition 6 together with propositions 1 and 3 immediately give the following result.

Corollary 2. *Suppose* $S = \sum_{g\in G} a_g g \in \mathbf{Z}[G]$ *satisfies* $\chi(S) = 0$ *for all non-principal characters* χ *of* G. *Then* $e(S) = 1$. *In other word,* S *is an* $(|S|, 1)$*-exhaustion set.*

Proposition 7. *Let* G *be a finite abelian group,* p *be a prime,* $S \subseteq G$ *with* $\chi(S) = p^r$ *for all non-principal characters* χ *of* G *and* $r \geq 1$. *Then* $|S| \equiv p^r (mod\ |G|)$.

Proof. Apply the finite Fourier transform to S to obtain

$$\begin{aligned} F(S) &= \sum_{\chi\in G^*} \chi(S)\chi \\ &= \chi_0(S)\chi_0 + \sum_{\chi\in G^*-\{\chi_0\}} \chi(S)\chi \\ &= |S|\chi + p^r(\sum_{\chi\in G^*-\{\chi_0\}} \chi). \end{aligned}$$

Next, we apply finite Fourier transform again to $F(S)$ and by using Lemma 2 to obtain

$$\begin{aligned} |G|S^{(-1)} &= F(F(S)) \\ &= |S|\widehat{\chi} + p^r F(\sum_{\chi\in G^*-\{\chi_0\}} \chi) \\ &= |S|F(\chi_0) + p^r(F(G^*) - F(\chi_0)) \\ &= |S|G + p^r(|G| - G). \end{aligned}$$

Therefore, $S^{(-1)} = p^r + \frac{|S|-p^r}{|G|}G$ is an element in $\mathbf{Z}[G]$. Thus, $|G| \mid |S| - p^r$ and so $|S| \equiv p^r (\mathrm{mod}\ |G|)$. □

By using propositions 1, 3 and 7, we obtain the following result.

Corollary 3. *Let* G *be a finite abelian group,* p *be a prime,* $S \subseteq G$ *with* $\chi(S) = p^r$ *for all non-principal characters* χ *of* G *and* $r \geq 1$. *Then* $|S| \equiv p^r(\ mod\ |G|)$. *Furthermore,* $e(S) = 1$.

Proposition 8. *Let* p *be a prime. Suppose* $\chi(S) = p^r$ *for all characters* χ *of* G *which is principal on* U. *Then* $S = \frac{p|U|}{|G|}U + X$ *for some* $X \in \mathbf{Z}[G]$ *and* $r \geq 1$.

Proof. Write $S = \sum_{g\in G} a_g g$. Then, apply the finite Fourier transform to S to obtain

$$\begin{aligned} F(S) &= \sum_{\chi\in G^*} \chi(S)\chi \\ &= \sum_{\chi\in U^\perp} \chi(S)\chi + \sum_{\chi\in G^*-U^\perp} \chi(S)\chi \\ &= p^r \sum_{\chi\in U^\perp} \chi + \sum_{\chi\in G^*-U^\perp} \chi(S)\chi. \end{aligned}$$

Next, we apply finite Fourier transform again to $F(S)$ to obtain

$$\begin{aligned} |G|S^{(-1)} &= p^r \frac{|G|}{|U|}U + F(\sum_{\chi\in G^*-U^\perp} \chi(S)\chi) \\ &= p^r \frac{|G|}{|U|}U + \sum_{\chi\in G^*-U^\perp} \chi(S)F(\chi) \\ &= p^r \frac{|G|}{|U|}U + \sum_{\chi\in G^*-U^\perp} \chi(g) \sum_{g\in G} \chi(S)g. \end{aligned}$$

Therefore, $S^{(-1)} = \frac{p|U|}{|G|}U + X$, where $X = \sum_{\chi\in G^*-U^\perp} \chi(g) \sum_{g\in G} \chi(S)g \in \mathbf{Z}[G]$. Clearly, $|U| \mid p^r$.

□

By using Lemma 2 , Proposition 1 and Proposition 3, it can be deduced from Proposition 8 that the subset S with $e(S) = mn$ only if X with $e(X) = m$.

The following result is a variation of the well-known Ma's Lemma (Beth et al., 1999).

Theorem 7. *Let* q *be a prime. Let* H *be an abelian group such that the Sylow* q*-subgroup of* H *is cyclic. Let* $Y \in \mathbf{Z}[H]$. *Suppose*

(a) q *is self-conjugate modulo* $\exp(H)$*; and*

(b) $q^r \mid \chi(Y)\overline{\chi(Y)}$ *for all non-principal character* χ *of* H.

Then

$$Y = q^{\lfloor r/2 \rfloor} X_1 + QX_2.$$

for some $X_1, X_2 \in \mathbf{Z}[H]$ *and* Q *is the subgroup of* H *of order* q.

Proof. Let $|H| = u$ and q^t strictly divides u, where $t \geq 0$. By the decomposition of prime ideal in the ring of algebraic integers, we know that $q\mathbf{Z}[\xi_u] = (\pi_1\pi_2 \dots \pi_g)^{\phi(q^t)}$, where $\pi_1, \pi_2, \dots, \pi_g$ are distinct prime ideal divisors of $q\mathbf{Z}[\xi_u]$, see Beth et al. (1999), Pott (1995). Let χ be any non-principal character of H. Then, $q^r \mid \chi(Y)\overline{\chi(Y)}$ which implies $\chi(Y)\overline{\chi(Y)} \equiv 0 \mod q^r$. Hence, we have

$$\begin{aligned}\chi(Y)\overline{\chi(Y)} &\in q^r\mathbf{Z}[\xi_u] \\ &= (q\mathbf{Z}[\xi_u])^r \\ &= (\pi_1\pi_2 \dots \pi_g)^{r\phi(q^t)}.\end{aligned}$$

Since we assume $t \geq 1$ and we let $Q = \langle h \rangle$, then $\chi(Y) \in (\pi_1\pi_2 \dots \pi_g)^{c\phi(q^t)}$ where $c = \left\lfloor \frac{r}{2} \right\rfloor$, and thus $\chi(Y) \equiv 0 (\mathrm{mod} q^c)$ for all non-principal characters χ on H. Write $H = P \times K$, where P is the Sylow q-subgroup of H. Take a character τ of P such that the order of τ is q^t. Define $\theta : \mathbf{Z}[H] \to \mathbf{Z}[\xi_{q^t}][K]$ such that $\theta(g) = \tau(g)$ for all $g \in P$ and $\theta(h) = h$ for all $h \in K$. For every character γ of K, by extending γ to a ring homomorphism from $\mathbf{Z}[\xi_{q^t}][K]$ to $\mathbf{C}$, we see that $\gamma(\theta(Y)) \equiv 0 (\mathrm{mod}\ q^c)$. Therefore, $q^c \mid \gamma(\theta(Y))$ which implies $\gamma(\theta(Y)) = q^c k_{\gamma\circ\theta}$ for some $k_{\gamma\circ\theta} \in \mathbf{Z}[\xi_u]$. Since

$$Y = \sum_{h\in K}\sum_{g\in P} a_{gh}gh \in \mathbf{Z}[H],$$

then

$$\begin{aligned}\theta(Y) &= \sum_{h\in K}\sum_{g\in P} a_{gh}\theta(g)\theta(h) \\ &= \sum_{h\in K}\sum_{g\in P} a_{gh}\tau(g)h \\ &= \sum_{h\in K}\sum_{g\in P} b_{gh}h,\end{aligned}$$

where $b_{gh} = a_{gh}\tau(g) \in \mathbf{Z}[\xi_{q^t}]$.

By Lemma 1, we have

$$b_{gh} = \frac{1}{|K|}\sum_{\gamma\in K^*} \gamma(\theta(Y))\gamma((gh)^{-1}).$$

Thus

$$|K|b_{gh} = \sum_{\gamma\in K^*} q^c k_{\gamma\circ\theta}\gamma((gh)^{-1}) = q^c d_{gh},$$

where $d_{gh} = \sum_{\gamma\in K^*} k_{\gamma\circ\theta}\gamma((gh)^{-1}) \in \mathbf{Z}[\xi_u]$. Note that $d_{gh} = \frac{|K|b_{gh}}{q^c} \in \mathbf{Q}$ and thus $d_{gh} \in \mathbf{Z}[\xi_u] \cap \mathbf{Q} = \mathbf{Z}$. Hence, we have

$$\theta(Y) = \sum_{h\in K}\sum_{g\in P} b_{gh}h$$

implies

$$\begin{aligned}|K|\theta(Y) &= \sum_{h\in K}\sum_{g\in P} |K|b_{gh}h \\ &= \sum_{h\in K}\sum_{g\in P} q^c d_{gh}h \\ &= q^c X,\end{aligned}$$

where $X = \sum_{h\in K}\sum_{g\in P} d_{gh}h \in \mathbf{Z}[K]$. Since $|K|$ and q^c are relatively prime, then there exists $e, f \in \mathbf{Z}$ such that $e|K| + fq^c = 1$. Thus, we see that

$$\begin{aligned}\theta(Y) &= e|K|\theta(Y) + fq^c\theta(Y) \\ &= eq^c X + fq^c\theta(Y) \\ &= q^c Z,\end{aligned}$$

where $Z = eX + f\theta(Y) \in Z[K]$. Therefore, $Y = q^c X_1 + ker(\theta)$, where $X_1 \in \mathbf{Z}[H]$ and by Theorem 6, we have $ker(\theta) = QX_2$ for some $X_2 \in \mathbf{Z}[H]$. □

Theorem 8. *Suppose* $Y \in \mathbf{Z}[H]$ *satisfies the conditions*

(a) q *is self-conjugate modulo* $\exp(H)$*; and*

(b) $q^r \mid \chi(Y)\overline{\chi(Y)}$ *for all non-principal character* χ *of* H.

If $e(Y) = n$, *then* $\binom{n}{i} q^{(\lfloor r/2 \rfloor - 1)i + n - 1} \leq |H|$ *for all* $i = 0, 1, 2, \dots, n$.

Proof. From Theorem 7, we have $Y = q^{\lfloor r/2 \rfloor}X_1 + QX_2$ and so by using the Binomial Theorem, we obtain

$$Y^n = \sum_{i=0}^{n} \binom{n}{i} q^{(\lfloor r/2 \rfloor - 1)i+n-1} Q X_1^i X_2^{n-i}.$$

Since $e(Y) = n$, then we have

$$H + W = \sum_{i=0}^{n} \binom{n}{i} q^{(\lfloor r/2 \rfloor - 1)i+n-1} Q X_1^i X_2^{n-i}$$

for some $W \in \mathbf{Z}[H]$. Next, consider any $h \in H$ such that $\chi(h) \neq 1$ for some non-principal character χ of H. Since $(1-h)H = 0$, then we have $(1-h)W = \sum_{i=0}^{n} \binom{n}{i} q^{(\lfloor r/2 \rfloor - 1)i+n-1}(1-h)QX_1^iX_2^{n-i}$. Thus, the coefficients of W lies between $-|H|$ and $|H|$. Also, the coefficients of the right hand side are multiple of $\pm\binom{n}{i}q^{(\lfloor r/2 \rfloor - 1)i+n-1}$. Thus, we have

$$\binom{n}{i} q^{(\lfloor r/2 \rfloor - 1)i+n-1} \leq |H|,$$

for $i = 0, 1, 2, \ldots, n$. □

By considering the contrapositive form of Theorem 8, we directly obtain Theorem 1. Finally, we illustrate Theorem 1 as follows:

Consider an abelian group $H \cong Z_3 \times Z_5^2$ containing the Sylow 3-subgroup $K \cong Z_3$ which is cyclic. Furthermore, $exp(H) = 15$. We take $q = 3$, which is self-conjugate modulo 15. Let $w = \chi(Y)\overline{\chi(Y)}$. Consider the case when $3^2|w$, that is, $r = 2$. We see that when $n = 4$, we have $\binom{4}{2}3^3 > |H| = 45$. Thus, we conclude that $e(Y) \geq 5$. Therefore, if $3^2 \mid |\chi(Y)|^2$, it follows that $e(Y) \geq 5$. Here, we demonstrate that by knowing the property of the character value we are able to estimate a lower bound for the exhaustion number. On the other hand, if we choose $r = 4$, then we see that $n = 3$ is the smallest integer such that $\binom{3}{i}3^{i+2} > |H| = 45$ when $i = 2$. Therefore, we conclude that if $3^4||\chi(Y)|^2$, then $e(Y) \geq 4$.

V. Concluding Remarks

In this paper, we performed a thorough study on exhaustion sets in abelian group using group ring notation and group characters. Furthermore, we derive a lower bound for exhaustion sets in abelian group. The self-conjugacy condition is used in constructing the bound, which is a useful method in the study of difference sets and the work did here is a standard treatment in combinatorial design theory. However, by releasing the self-conjugacy condition, we are not sure whether a similar bound can be obtained.

Acknowledgements

This work was supported by the Fundamental Research Grant Scheme (FRGS), Project No. FRGS/1/2017/STG06/UTAR/02/2.

References

[1] B. Bajnok and R. Matzek. The minimum size of signed sumsets. *Electron. J. Combin.*, 22(2):1–17, 2015.

[2] B. Bajnok and R. Matzek. On the minimum size of signed sumsets in elementary abelian groups. *J. Number Theory*, 159: 381–401, 2016.

[3] T. Beth, D. Jungnickel, and H. Lenz. *Design Theory*. Cambridge Univ. Press, 2nd edition, 1999.

[4] A. L. Cauchy. Recherches sur les nombres. *J. Ecole Polytechnique*, 9:99–123, 1813.

[5] A. Y. M. Chin. Exhaustion numbers of subsets of abelian groups. *Ars Comb.*, 68: 67–78, 2003.

[6] H. Davenport. On the addition of residue classes. *J. London Math. Soc.*, 10:30–32, 1935.

[7] J. A. Davis and J. Jedwab. A unifying construction for difference sets. *J. Combin. Theory, Ser. A.*, 80:13–78, 1997.

[8] S. Eliahou and M. Kervaire. Sumsets in vector spaces over finite fields. *J. Number Theory*, 71:12–39, 1998.

[9] S. Eliahou and M. Kervaire. Minimal sumsets in infinite abelian groups. *J. Algebra*, 287:449–457, 2005.

[10] S. Eliahou and M. Kervaire. Sumsets in dihedral groups. *European J. Combin.*, 27:617–628, 2006.

[11] S. Eliahou and M. Kervaire. The small sumsets property for solvable finite groups. *European J. Combin.*, 27:1102–1110, 2006.

[12] S. Eliahou and M. Kervaire. Some results on minimal sumset sizes in finite non-abelian groups. *J. Number Theory*, 124:234–247, 2007.

[13] S. Eliahou and M. Kervaire. Minimal sumsets in finite solvable groups. *Discrete Mathematics*, 310:471–479, 2010.

[14] S. Eliahou, M. Kervaire, and A. Plagne. Optimally small sumsets in finite abelian groups. *J. Number Theory*, 101:338–348, 2003.

[15] I. M. Isaacs. *Character Theory of Finite Groups*. Academic Press, 1976.

[16] B. Klopsch and V. F. Lev. Generating abelian groups by addition only. *Forum Math*, 21:23–41, 2009.

[17] S. L. Ma. Planar functions, relative difference sets, and character theory. *J. Algebra*, 185:342–356, 1996.

[18] S. L. Ma and W. S. Ng. On non-existence of perfect and nearly perfect sequences. *Int. J. Information and Coding Theory.*, 1:15–38, 2009.

[19] A. Pott. *Finite Geometry and Character Theory*. Springer-Verlag, 1995.

[20] R. J. Turyn. Character sums and difference sets. *Pacific J. Math*, 15:319–346, 1965.