Matematika, 1999, Jilid 15, bil. 1, hlm. 57–63

Exhaustion Numbers of Maximal Sum-free Sets of Certain Cyclic Groups

A. Y. M. Chin
Institute of Mathematical Sciences
University of Malaya
50603 Kuala Lumpur, Malaysia

Abstract Let G be a finite group written additively and S a non-empty subset of G. We say that S is *e-exhaustive* if $G = S + \ldots + S$ (e times). The minimal integer $e > 0$, if it exists, such that S is e-exhaustive, is called the *exhaustion number* of the set S and is denoted by $e(S)$. The exhaustion numbers of various subsets of finite abelian groups have been determined by the author [1]. In this paper the exhaustion numbers of maximal sum-free sets of the cyclic groups of prime power order are determined.

Keywords Exhaustion number, sum-free set, cyclic group

Abstrak *Biar G suatu kumpulan terhingga yang ditulis secara penambahan dan S suatu subset tak kosong bagi G. Kita katakan bahawa S adalah habisan-e jika $G = S + \ldots + S$ (e kali). Integer minimal $e > 0$, jika ianya wujud, supaya S adalah habisan-e dipanggil* nombor habisan *bagi set S dan ditandai sebagai $e(S)$. Nombor-nombor habisan bagi beberapa subset kumpulan-kumpulan abelan terhingga telah ditentukan oleh penulis [1]. Dalam kertas ini, nombor habisan bagi set-set bebas hasil tambah yang maksimal bagi kumpulan-kumpulan kitaran yang berperingkat kuasa nombor perdana akan ditentukan.*

Katakunci *Nombor habisan, set bebas-hasil tambah, kumpulan kitaran*

1 Introduction

Let G be a finite group written additively. For a non-empty subset S of G, we say that S is *e-exhaustive* if G is covered by the sum of e copies of S, that is,

$$G = S + \ldots + S \quad (e \text{ times}).$$

For convenience, we shall use $e \cdot \cdot S$ to denote $S + \ldots + S$ (e times). The minimal integer $e > 0$, if it exists, such that S is e-exhaustive, is called the *exhaustion number* of the set S

and is denoted by $e(S)$. If such $e > 0$ does not exist, we say that the exhaustion number of the set S is infinite and write $e(S) = \infty$. If $e(S)$ is finite, then we say that S is *exhaustive* in G. Clearly if S is e-exhaustive, then it is also e'-exhaustive for any $e' > e$. It is also clear that if S is exhaustive in G then $S \not\subseteq H$ for any proper subgroup H of G.

The exhaustion numbers of various subsets of finite abelian groups have been determined by the author in [1]. In this paper we shall determine the exhaustion numbers of maximal sum-free sets of cyclic groups of prime power order. A *sum-free* set S of G is a non-empty subset of G satisfying $(S + S) \cap S = \emptyset$. We say that S is a *maximal* sum-free set if S is sum-free and $|S| \geq |T|$ for every sum-free set T in G. Various properties of sum-free sets have been studied before (see for example [3]). We show in this paper that except for the cyclic group $\mathbb{Z}/7$, the maximal sum-free sets of cyclic groups of prime power order are either not exhaustive or exhaustive with exhaustion number four. For the cyclic group $\mathbb{Z}/7$, its maximal sum-free sets have exhaustion number six.

We shall use the notation $\lceil x \rceil$ to mean the smallest integer $\geq x$. As usual, the notation $[x]$ means the largest integer $\leq x$. It is not difficult to see that $\lceil x \rceil = [x] + 1$ if x is not an integer.

2 Exhaustion Numbers of Subsets of $\mathbb{Z}/m$, $m \geq 2$ Which are in Arithmetic Progression

The main result in this section is Theorem 2.2 which has been obtained in [1]. For the sake of convenience and since this result is used frequently in the next section, we shall reproduce it here. We first prove the following lemma:

Lemma 2.1 *Let m and s be positive integers with $s > 2$. If $s - 1$ does not divide $m - 1$, then*

$$m \leq \left\lceil \frac{m-1}{s-1} \right\rceil (s-1) + 1 \leq m + (s-2).$$

Proof: Since $s - 1$ does not divide $m - 1$, so $\left\lceil \frac{m-1}{s-1} \right\rceil = \left[\frac{m-1}{s-1} \right] + 1$. Suppose first that $\left(\left[\frac{m-1}{s-1} \right] + 1 \right)(s-1) + 1 < m$. Then

$$\left[\frac{m-1}{s-1} \right](s-1) < m - s$$

and hence

$$\left[\frac{m-1}{s-1} \right] < \frac{m-s}{s-1} = \frac{m-1}{s-1} - 1,$$

which is not possible. Therefore $\left(\left[\frac{m-1}{s-1} \right] + 1 \right)(s-1) + 1 \geq m$.

Now suppose that $\left(\left[\frac{m-1}{s-1} \right] + 1 \right)(s-1) + 1 \geq m + (s-1)$. Then

$$\left[\frac{m-1}{s-1} \right](s-1) \geq m - 1$$

and hence
$$\left\lceil \frac{m-1}{s-1} \right\rceil \geq \frac{m-1}{s-1},$$
which is not possible. Hence $\left(\left\lceil \frac{m-1}{s-1} \right\rceil + 1\right)(s-1)+1 \leq m+(s-2)$. $\square$

Theorem 2.2 *Let $S \subseteq \mathbb{Z}/m$, $m \geq 2$ with $|S| = s > 1$. If S is in arithmetic progression with difference d relatively prime to m, then*
$$e(S) = \left\lceil \frac{m-1}{s-1} \right\rceil .$$
If S is in arithmetic progression with difference d not relatively prime to m, then $e(S) = \infty$.

Proof: Let $S = \{a, a+d, a+2d, \ldots, a+(s-1)d\}$ where d is relatively prime to m. By induction, it can be shown that for any positive integer k, the first term in the (multi)set $k \cdot \cdot S$ is ka while the last term is $ka + k(s-1)d$. Suppose first that $s-1$ divides $m-1$ and let $e = \frac{m-1}{s-1}$. Then
$$e(s-1)d + d = \left(\frac{m-1}{s-1}\right)(s-1)d + d = md \equiv 0 \pmod{m}$$
and it follows that
$$(ea + e(s-1)d) + d \equiv ea \pmod{m},$$
that is, the difference between the first and last terms of $e \cdot \cdot S$ is d. Since d is relatively prime to m, so we must have that $e \cdot \cdot S = \mathbb{Z}/m$. Note that
$$(e-1)a + id \not\equiv (e-1)a + jd \qquad \pmod{m}$$
for any $i, j = 0, 1, \ldots, (e-1)(s-1)\ (= m-s)$. Otherwise, there exist $i, j \in \{0, 1, \ldots, m-s\}$ such that $(i-j)d \equiv 0 \pmod{m}$. Since d is relatively prime to m, so $i - j \equiv 0 \pmod{m}$. But this is impossible since $m - s < m$. We also note that
$$\begin{aligned}(e-1)(s-1)d + d &= (m-s)d + d \\ &= (m-(s-1))d \\ &\not\equiv 0 \pmod{m}.\end{aligned}$$
Therefore $((e-1)a + (e-1)(s-1)d) + d \not\equiv (e-1)a \pmod{m}$. It thus follows that $(e-1) \cdot \cdot S \neq \mathbb{Z}/m$ and hence $e(S) = e = \frac{m-1}{s-1}$.

Now suppose that $s-1$ does not divide $m-1$. Let $e = \left\lceil \frac{m-1}{s-1} \right\rceil + 1$. Then by Lemma 2.1
$$\begin{aligned}ea + e(s-1)d + d &= ea + \left(\left\lceil \frac{m-1}{s-1} \right\rceil + 1\right)(s-1)d + d \\ &= ea + (m+i)d \\ &\equiv ea + id \qquad \pmod{m}\end{aligned}$$
for some $i = 0, 1, \ldots, s-2$. We thus have that either the difference between the first and last terms of $e \cdot \cdot S$ is d (this happens if $i = 0$) or the last term in (the multiset) $e \cdot \cdot S$ coincides

with one of its earlier terms (this happens if $i \in \{1, \ldots, s-2\}$). In either case, since d is relatively prime to m it must follow that $e \cdot \cdot S = \mathbb{Z}/m$. Note that

$$(e-1)(s-1) = \left[\frac{m-1}{s-1}\right](s-1) < \left(\frac{m-1}{s-1}\right)(s-1) = m-1 < m.$$

Therefore

$$(e-1)a + id \not\equiv (e-1)a + jd \pmod{m}$$

for any $i, j = 0, 1, \ldots, (e-1)(s-1)$. Since

$$\begin{aligned}(e-1)a + (e-1)(s-1)d + d &< (e-1)a + (m-1)d + d \\ &= (e-1)a + md,\end{aligned}$$

so $(e-1)a + (e-1)(s-1)d + d \not\equiv (e-1)a \pmod{m}$. It follows that $(e-1) \cdot \cdot S \neq \mathbb{Z}/m$ and hence $e(S) = e = \left[\frac{m-1}{s-1}\right] + 1$.

Finally, suppose that m and d are not relatively prime. Let n be the smallest positive integer such that $nd \equiv 0 \pmod{m}$. Then $(da + (n-1)d) + d \equiv da \pmod{m}$ and we thus have that

$$\begin{aligned}d \cdot \cdot S &= \{da, da + d, da + 2d, \ldots, da + (n-1)d\} \\ &= \{da, d(a+1), d(a+2), \ldots, d(a+n-1)\}.\end{aligned}$$

That is, $d \cdot \cdot S$ is the subgroup of $\mathbb{Z}/m$ of order n and we can write

$$d \cdot \cdot S = \{0, d, 2d, \ldots, (n-1)d\}.$$

It follows that

$$(kd) \cdot \cdot S = \{0, d, 2d, \ldots, (n-1)d\}$$

for any positive integer k. Hence S cannot be exhaustive. $\square$

3 Exhaustion Numbers of Maximal Sum-free Sets of Cyclic Groups

In this section we show that except for the cyclic group $\mathbb{Z}/7$, the maximal sum-free sets of cyclic groups of prime power order are either not exhaustive or exhaustive with exhaustion number four. For the cyclic group $\mathbb{Z}/7$, its maximal sum-free sets have exhaustion number six.

3.1 The Case $p = 3$

Proposition 3.1 *The maximal sum-free sets of the cyclic group $\mathbb{Z}/3^n$ $(n \geq 1)$ are either not exhaustive or exhaustive with exhaustion number 4.*

Proof: It is not difficult to see that $\mathbb{Z}/3$ has 3 sum-free sets (that is, $\{0\}$, $\{1\}$ and $\{2\}$) and that these sets are not exhaustive. Now consider $n \geq 2$ and let S be a maximal sum-free set of $\mathbb{Z}/3^n$. From [2, Theorem 4] it can be worked out that S is automorphic to one of the following forms:

(i) $\{3i+1 \mid i = 0, 1, \ldots, 3^{n-1}-1\}$;

(ii) $\{3^{n-1} + (3j+1)i \mid i = 0, 1, \ldots, 3^{n-1}-1\}, \quad j = 0, 1, \ldots, 3^{n-1}-1$;

(iii) $\{j.3^{n-1} + (3^{n-2} + (3k+1)i) \mid i = 0, 1, \ldots, 3^{n-2}-1;\ j = 0, 1, 2\}, k = 0, 1, \ldots, 3^{n-2}-1 \qquad (n \geq 3)$.

If S is automorphic to a maximal sum-free set of the form (i), then it is in arithmetic progression with difference 3. By Theorem 2.2, it follows readily that $e(S) = \infty$. Suppose that S takes the form (ii). Then S is in arithmetic progression with difference $3j+1$ which is clearly relatively prime to 3. The number of elements s in S is 3^{n-1}. Note that

$$\frac{3^n-1}{s-1} = \frac{3^n-1}{3^{n-1}-1} = 3 + \frac{2}{3^{n-1}-1}.$$

Hence $3^n - 1$ is divisible by $3^{n-1}-1$ if and only if $n = 2$. We thus have by Theorem 2.2 that

$$e(S) = \left[\frac{3^n-1}{3^{n-1}-1}\right] + 1 = \left[3 + \frac{2}{3^{n-1}-1}\right] + 1 = 4$$

if $n \neq 2$. If $n = 2$ then by Theorem 2.2 again,

$$e(S) = \frac{3^2-1}{3^{2-1}-1} = 4.$$

Finally, suppose that S is automorphic to a maximal sum-free set of the form (iii). Then we can write S as the disjoint union of S_1, S_2 and S_3 where

$$\begin{aligned} S_r \;=\; & \{(r-1).3^{n-1} + 3^{n-2},\ (r-1).3^{n-1} + 3^{n-2} + (3k+1), \\ & \ldots, (r-1).3^{n-1} + 3^{n-2} + (3k+1)(3^{n-2}-1)\}, \quad r = 1, 2, 3. \end{aligned}$$

Clearly, each S_r is in arithmetic progression with difference $3k+1$. Note that

$$\begin{aligned} 4\cdot\cdot S_r \;=\; & \{4(r-1).3^{n-1} + 4.3^{n-2},\ 4(r-1).3^{n-1} + 4.3^{n-2} + (3k+1), \\ & \ldots, 4(r-1).3^{n-1} + 4.3^{n-2} + 4(3^{n-2}-1)(3k+1)\},\ r = 1, 2, 3. \end{aligned}$$

Since $4(3^{n-2}-1) = (3+1)(3^{n-2}-1) = 3^{n-1} + 3^{n-2} - 4$, so $|4\cdot\cdot S_r| = 3^{n-1} + 3^{n-2} - 4 + 1 = 3^{n-1} + 3^{n-2} - 3$. It is straightforward to check that $|4\cdot\cdot S_i \cap 4\cdot\cdot S_j| = 3^{n-2} - 3$ for every $i, j = 1, 2, 3\, (i \neq j)$ and that $4\cdot\cdot S_1 \cap 4\cdot\cdot S_2 \cap 4\cdot\cdot S_3 = \emptyset$. Therefore $|4\cdot\cdot S_1 \cup 4\cdot\cdot S_2 \cup 4\cdot\cdot S_3| = 3^n$ and it follows that $4\cdot\cdot S = 4\cdot\cdot S_1 \cup 4\cdot\cdot S_2 \cup 4\cdot\cdot S_3 = \mathbb{Z}/3^n$. By some straightforward (but tedious) calculation, it can be shown that $3\cdot\cdot S \neq \mathbb{Z}/3^n$. Therefore $e(S) = 4$. □

3.2 The Case $p \equiv 2 \pmod 3$

Proposition 3.2 *The maximal sum-free sets of the cyclic group $\mathbb{Z}/p^n$ where $p \equiv 2 \pmod 3$ and $n \geq 1$ are all exhaustive with exhaustion number 4.*

Proof: We may write $p = 3k + 2$ for some $k \in \mathbb{Z}$. Let S be a maximal sum-free set of $\mathbb{Z}/p^n$. Then by [2, Theorem 2] we may take

$$S = \{ip + (k + j) \mid i = 0, 1, \ldots, p^{n-1} - 1; j = 1, \ldots, k + 1\}.$$

First suppose that $n = 1$. In this case, S is in arithmetic progression with difference 1 and $s = |S| = k + 1$. Note that

$$\frac{p-1}{s-1} = \frac{3k+1}{k} = 3 + \frac{1}{k}.$$

Clearly, $3k+1$ is divisible by k if and only if $k = 1$, that is, $p = 5$. We thus have by Theorem 2.2 that

$$e(S) = \left\lceil \frac{3k+1}{k} \right\rceil + 1 = 3 + 1 = 4$$

if $p \neq 5$ and

$$e(S) = \frac{3(1)+1}{1} = 4$$

if $p = 5$.

Now suppose that $n \geq 2$. Since S is not in arithmetic progression we cannot make use of Theorem 2.2. It is however straightforward to show that

$$\begin{aligned} 3 \cdot \cdot S &= \{ip + j \mid i = 0, 1, \ldots, p^{n-1} - 1; j = 1, \ldots, 3k + 1\} \\ &\neq \mathbb{Z}/p^n \end{aligned}$$

but

$$\begin{aligned} 4 \cdot \cdot S &= \{ip + (k + j) \mid i = 0, 1, \ldots, p^{n-1} - 1; j = 2, \ldots, p + 1\} \\ &= \mathbb{Z}/p^n. \end{aligned}$$

Hence $e(S) = 4$ as asserted. □

3.3 The Case $p \equiv 1 \pmod 3$

Proposition 3.3 *The maximal sum-free sets of the cyclic group $\mathbb{Z}/p^n$ where $p \equiv 1 \pmod 3$ and $n \geq 1$ with $(p, n) \neq (7, 1)$ are all exhaustive with exhaustion number 4. If $(p, n) = (7, 1)$, then the maximal sum-free sets of $\mathbb{Z}/7$ have exhaustion number 6.*

Proof: We may write $p^n = 3k + 1$ for some $k \in \mathbb{Z}$. Let S be a maximal sum-free set of $\mathbb{Z}/p^n$. Then by [4, Theorem 2], S is automorphic to one of the following forms:

(i) $\{k, k + 1, \ldots, 2k - 1\}$;

(ii) $\{k + 1, k + 2, \ldots, 2k\}$;

(iii) $\{k, k + 2, k + 3, \ldots, 2k - 1, 2k + 1\}$.

First suppose that S is automorphic to the form (i) or (ii). Then S is in arithmetic progression with difference 1 and $s = |S| = k$. Note that

$$\frac{p^n - 1}{s - 1} = \frac{3k}{k - 1} = 3 + \frac{3}{k - 1}.$$

Hence $3k$ is divisible by $k - 1$ if and only if $k = 2$ or 4, that is, $p = 7$ or 13. We thus have by Theorem 2.2 that

$$e(S) = \left[\frac{3k}{k - 1}\right] + 1 = 3 + 1 = 4$$

if $p \neq 7$, 13,

$$e(S) = \frac{3k}{k - 1} = \frac{3(2)}{2 - 1} = 6$$

if $p = 7$ and

$$e(S) = \frac{3k}{k - 1} = \frac{3(4)}{4 - 1} = 4$$

if $p = 13$.

Now suppose that S is automorphic to the form (iii). Taking note that $3k + 1 \equiv 0 \pmod{p^n}$, we have

$$3 \cdot \cdot S = \{3k,\, 3k + 2,\, 3k + 3, \ldots,\, 3k + 3k\} \neq \mathbb{Z}/p^n.$$

Consider the $4k + 3$ elements

$$4k,\, 4k + 2,\, 4k + 3, \ldots,\, 4k + (4k + 2),\, 4k + (4k + 4).$$

Since $4k + 3 > p^n$, it is easy to see that $4 \cdot \cdot S$ must be $\mathbb{Z}/p^n$. Hence $e(S) = 4$. $\square$

References

[1] A. Y. M. Chin, *Exhaustion numbers of subsets of abelian groups*, submitted for publication.

[2] P. H. Diananda and H. P. Yap, *Maximal sum-free sets of elements of finite groups*, Proc. Japan Acad. **45** (1969), 1–5.

[3] A. P. Street, *Sum-free sets*, Springer Lecture Notes in Math. **292** (1972), 123–272.

[4] H. P. Yap, *Maximal sum-free sets in finite abelian groups, II*, Bull. Austral. Math. Soc. **5** (1971), 43–54.