Covering finite groups by subset products

[1]H. V. Chen, [2]A. Y. M. Chin
[1]Department of Mathematical and Actuarial Sciences
Faculty of Engineering and Science
Universiti Tunku Abdul Rahman
Jalan Genting Kelang, 53300 Kuala Lumpur
Malaysia
[2]Institute of Mathematical Sciences
Faculty of Science
University of Malaya
50603 Kuala Lumpur
Malaysia
E-mail: [1]chenhv@utar.edu.my, [2]aymc@pc.jaring.my

Abstract

Let G be a finite group and let S be a nonempty subset of G. For any positive integer k, let S^k be the subset product given by the set $\{s_1 \dots s_k \mid s_1, \dots, s_k \in S\}$. If there exists a positive integer n such that $S^n = G$, then S is said to be exhaustive. Let $e(S)$ denote the smallest positive integer n, if it exists, such that $S^n = G$. We call $e(S)$ the exhaustion number of the set S. If $S^n \neq G$ for any positive integer n, then S is said to be non-exhaustive. In this paper, we obtain some properties of exhaustive and non-exhaustive subsets of finite groups.

AMS 2010 Subject Classifications: 20D60, 05E15

Key Words: finite group, subset product, exhaustive subset, exhaustion number.

1 Introduction

Let G be a finite group and let S be a non-empty subset of G. For any positive integer k, let S^k be the subset product given by the set $\{s_1 \dots s_k \mid$

$s_1, \ldots, s_k \in S\}$. If there exists a positive integer n such that $S^n = G$, then we say that S is exhaustive. Let $e(S)$ denote the smallest positive integer n, if it exists, such that $S^n = G$. We call $e(S)$ the exhaustion number of the set S. If $S^n \neq G$ for any positive integer n, then S is said to be non-exhaustive and we write $e(S) = \infty$. Clearly, $e(H) = \infty$ for any proper subgroup H of G.

For a finite group G of order at least 3, we define the critical exhaustion number $ce(G)$ of G to be the smallest positive integer s such that any subset S of G with $|S| \geq s$ is exhaustive. Clearly, $s \leq |G| - 1$. Note that the critical exhaustion number of a finite group is somewhat the multiplicative analogue of its critical number. Recall that the critical number $cr(G)$ of G is the smallest s such that the subset sums set $\sum(S) = \{\sum_{x \in A} x \mid A \subseteq S, A \neq \emptyset\}$ coincides with G for each subset $S \subset G \setminus \{0\}$ of cardinality $|S| \geq s$. The critical numbers for all finite abelian groups have been completely determined (see [2], [3], [4], [5], [6], [8], [9]). For non-abelian groups, some results have been obtained, for example in [7], [10] and [11], but the problem of obtaining the critical numbers is still not completely solved.

Exhaustion numbers of certain subsets of abelian groups have been studied in [1]. In this paper we further investigate properties of exhaustive and non-exhaustive subsets of finite groups. In Section 2, we obtain a characterization of non-exhaustive subsets of finite groups and use this to obtain an upper bound for the size of a non-exhaustive subset. In Section 3, we obtain some lower bounds for the size of exhaustive subsets. We also obtain, for a finite group G of order at least six, an upper bound less than $|G| - 1$ for its critical exhaustion number.

2 Non-exhaustive sets

We first obtain a characterization of non-exhaustive subsets of finite groups.

Theorem 2.1 *Let G be a finite group and let S be a non-empty proper subset of G. Then $e(S) = \infty$ if and only if S^n is a proper subgroup of G for some positive integer n.*

Proof. Assume that $e(S) = \infty$. It is known that every proper subgroup of a group is non-exhaustive. Thus $n = 1$ if S is a subgroup of G. Suppose now that S is not a subgroup of G. Note that $|S^i| \leq |S^{i+1}|$ for any integer $i \geq 1$. Let d be the smallest order among the orders of all the elements in S. Then $1 \in S^d$ and hence, $S^d \subseteq S^{2d} \subseteq S^{3d} \subseteq \ldots$. Since G is a finite group, there must exist an integer m such that $S^{kd} = S^{md}$ for all $k \geq m$. Thus S^{md} is a subgroup of G and since $e(S) = \infty$, S^{md} must be proper.

Conversely, if S^n is a proper subgroup of G for some integer n, then $S^m \neq G$ for any integer m and hence, $e(S) = \infty$.

An immediate consequence of Theorem 2.1 is the following:

Corollary 2.2 *Let G be a finite group and let S be a non-exhaustive subset of G. Then $|S| \leq n$ where n is the largest among the orders of all proper subgroups of G.*

Proof. By Theorem 2.1, there exists a positive integer k such that S^k is a proper subgroup of G. Hence, $|S| \leq |S^k| \leq n$ where n is the largest among the orders of all proper subgroups of G.

3 Exhaustive sets

An exhaustive subset of a group G is clearly a generating set of G. The converse of this is not necessarily true. For example, take G to be the cyclic group of order n with generator x. The generating set $S = \{x\}$ of G is non-exhaustive. We note, however, that the set $T = S \cup \{1\}$ is exhaustive with $T^{n-1} = G$. In general, it is not difficult to see that if S is a minimal generating set of a finite group G and S is not exhaustive, then the union $S \cup \{1\}$ is an exhaustive set. Thus, if G is a finite group with $|G| \geq 3$, then G has a proper exhaustive subset T and every element in G can be written as a product of a fixed number of elements belonging to T.

We first show that subsets which contain exhaustive subsets are also exhaustive.

Lemma 3.1 *Let G be a finite group and let S, T be subsets of G with $S \subseteq T$. If $e(S) = n$, then $e(T) \leq n$.*

Proof. Note that $S^k \subseteq T^k$ for any positive integer k. If $e(S) = n$, then $T^n = G$ and hence $e(T) \leq n$.

By using Lemma 3.1, we obtain the possible cardinalities of an exhaustive subset of a finite group as follows.

Proposition 3.2 *Let G be a finite group and let $d(G)$ be the minimum cardinality of a generating set of G. The minimum cardinality of an exhaustive subset S of G is $d(G)$ or $d(G)+1$. Moreover, given any integer k where $d(G)+1 \leq k \leq |G|$, there exists an exhaustive subset T of G with $|T| = k$.*

Proof. Since any exhaustive set is a generating set, the lower bound $|S| \geq d(G)$ holds if G has a generating set of minimum cardinality which is exhaustive. If none of the generating sets of minimum cardinality is exhaustive and D is such a set, then $D \cup \{1\}$ is exhaustive and hence, $|S| \geq d(G)+1$ holds. Since any set which contains an exhaustive subset is also exhaustive (by Lemma 3.1), the last assertion follows easily.

Remark. We note that the minimum cardinality $d(G)$ as given in Proposition 3.2 is attained for example when G is the symmetric group $S_3 = \langle x, y \mid x^3 = y^2 = 1, yx = x^2y \rangle$ and S is the minimal generating set $\{x, y\}$. If we take G to be the Klein 4-group $C_2 \times C_2 \cong \langle x, y \mid x^2 = y^2 = 1, xy = yx \rangle$, then the minimum cardinality of an exhaustive subset S of G is 3 ($= d(G)+1$).

Now let G be a finite group (not necessarily abelian) with $|G| \geq 6$. If S is a subset of G with $|S| \geq \left\lceil \frac{|G|}{2} \right\rceil + 1$, then S can clearly be written as a union of two subsets S_1, S_2 of G with $|S_1|, |S_2| \geq 2$. Moreover, if $e(S_1), e(S_2) < \infty$, then $e(S) < \infty$ and $e(S) \leq \min(e(S_1), e(S_2))$ (by Lemma 3.1). In fact, we show in the following that there exists a positive integer $n < |G| - 1$ such that any subset S of G with $|S| > n$ is exhaustive.

Proposition 3.3 *Let G be a finite group with*

$$|G| = \begin{cases} 2n, & \text{if } |G| \text{ is even} \\ 2n+1, & \text{if } |G| \text{ is odd} \end{cases} \quad (n \geq 3).$$

Let S be a subset of G such that $|S| > n$ where $n = \frac{|G|}{2}$ if $|G|$ is even and $n = \frac{|G|-1}{2}$ if $|G|$ is odd. Then $e(S) < \infty$.

Proof. Note that any proper subgroup of G has order $\leq n$. Thus, since $|S| \geq n+1$ and $|S^i| \geq |S|$ for any integer $i \geq 1$, so S^i cannot be a proper subgroup of G for any $i \geq 1$. It follows by Theorem 2.1 that $e(S) < \infty$.

For a finite group G, by Proposition 3.3, we readily have

Corollary 3.4 *Let G be a finite group with*

$$|G| = \begin{cases} 2n, & \text{if } |G| \text{ is even} \\ 2n+1, & \text{if } |G| \text{ is odd} \end{cases} \quad (n \geq 3).$$

Then $ce(G) \leq \frac{|G|}{2} + 1$ if $|G|$ is even and $ce(G) \leq \frac{|G|+1}{2}$ if $|G|$ is odd.

In the case of finite abelian groups, we obtain the following:

Proposition 3.5 *Let $G = C_{p_1^{\alpha_1}} \times \cdots \times C_{p_k^{\alpha_k}}$ where $p_1, \ldots, p_k$ are prime numbers, not necessarily distinct, and $\alpha_1, \ldots, \alpha_k$ are positive integers. Let D be a minimal generating set of G. The minimum cardinality of an exhaustive subset S of G is either k or $k+1$. In particular, if $S = D \cup \{1\}$, then $e(S) = p_1^{\alpha_1} + \cdots + p_k^{\alpha_k} - k$.*

Proof. The first assertion follows from Proposition 3.2 and the fact that $d(G) = k$. For the second assertion, let x_i be a generator of $C_{p_i^{\alpha_i}}$, $i = 1, \ldots, k$. We may then take $D = \{x_1, \ldots, x_k\}$. Let $S = D \cup \{1\}$. Then for any $r \in \{1, 2, \ldots\}$,

$$S^r = \{1\} \cup \{x_1^{r_1} \ldots x_k^{r_k} \mid 1 \leq r_1 + \cdots + r_k \leq r, r_i \text{ is a non-negative integer } (i = 1, \ldots, k)\}.$$

Clearly, every element in G can be written in the form $x_1^{r_1} \dots x_k^{r_k}$ where $0 \le r_i \le p_i^{\alpha_i} - 1$ $(i = 1, \dots, k)$. Thus $S^m = G$ but $S^{m-1} \ne G$ where $m = (p_1^{\alpha_1} - 1) + \dots + (p_k^{\alpha_k} - 1) = p_1^{\alpha_1} + \dots + p_k^{\alpha_k} - k$. This completes the proof.

We have shown in Proposition 3.2 that there are no gaps in the size of an exhaustive subset of a finite group. That is, given a finite group G and any integer k where $d(G)+1 \le k \le |G|$, there exists an exhaustive subset S of G with $|S| = k$. We now ask whether there is any gap in the exhaustion numbers of exhaustive subsets of G. That is, if a and b are, respectively, the smallest and the largest exhaustion numbers of exhaustive subsets of G, is every integer k, $a < k < b$, also the exhaustion number of some subset S of G? We answer this in the negative with an example.

Example: Consider the dihedral group $D_{12} = \langle x, y \mid x^6 = y^2 = 1, yx = x^5y \rangle$. The following table lists examples of subsets S of D_{12} with $e(S) = 2, 3, 4, 6$.

Table 1: Subsets $S \subseteq D_{12}$ where $e(S) \in \{2, 3, 4, 6\}$

$e(S)$	S
2	$\{1, x, y, xy, x^2y, x^3y\}$
3	$\{1, x, y, xy\}$
4	$\{1, x, xy\}$
6	$\{1, y, xy\}$

By hand calculations, we note however that there is no subset S of D_{12} with $e(S) = 5$.

References

[1] A. Y. M. Chin, Exhaustion numbers of subsets of abelian groups. Ars Comb. **68** (2003), 65–76.

[2] G. T. Diderrich and H. B. Mann, Combinatorial problems in finite Abelian groups, Survey of combinatorial theory (Proc. Internat. Sympos., Colorado State Univ., Fort Collins, Colo., 1971), pp. 95–100. North-Holland, Amsterdam, 1973.

[3] G. T. Diderrich, An addition theorem for abelian groups of order pq, J. Number Theory 7 (1995), 35–48.

[4] J.A. Dias da Silva and Y. O. Hamidoune, Cyclic spaces for Grassmann derivatives and additive theory, Bull. London Math. Soc. **26** (1994) 140–146.

[5] W. Gao, Y. O. Hamidoune, A. Lladó, O. Serra, Covering a finite abelian group by subset sums, Combinatorica **23** (2003), 599–611.

[6] W. Gao, Y. O. Hamidoune, On additive bases, Acta Arith. **88** (1999), 233–237.

[7] W. Gao, A combinatorial problem on finite groups, Acta Math Sinica **38** (1995), 395–399.

[8] J. R. Griggs, Spanning subsets sums for finite abelian groups, Discrete Math. **220** (2001), 89–99.

[9] M. Freeze, W. Gao, A. Geroldinger, The critical number of finite abelian groups. J. Number Theory **129** (2009), 2766-2777.

[10] Q. H. Wang and J. J. Zhuang, On the critical number of finite groups of order pq, Int. J. Number Theory **8** (2012), 1271–1279.

[11] Q. Wang and Y. Qu, On the critical number of finite groups (II), arXiv:1212.0595.