The Erdős-Ginzburg-Ziv theorem for finite nilpotent groups

Dongchun Han

Abstract. Let G be a finite group written multiplicatively. Define $\mathsf{E}(G)$ to be the minimal integer t such that every sequence of t elements (repetition allowed) in G contains a subsequence with length $|G|$ and with product one (in some order). Let p be the smallest prime divisor of $|G|$. In this paper we prove that if G is a noncyclic nilpotent group then $\mathsf{E}(G) \leq |G| + \frac{|G|}{p} + p - 2$, which confirms partially a conjecture by Gao and Li. We also determine the exact value of $\mathsf{E}(G)$ for $G = C_p \ltimes C_{pn}$ when p is a prime, which confirms partially another conjecture by Zhuang and Gao.

Mathematics Subject Classification (2010). 11B50 - 11B75.

Keywords. Erdős-Ginzburg-Ziv theorem - Product-one - Nilpotent.

1. Introduction

Let G be a finite group written multiplicatively (not necessarily commutative). Let $\mathsf{E}(G)$ be the minimal integer t such that given any t elements (repetition allowed) in G, there must be exactly $|G|$ of them that give product 1 when multiplied in some order. In 1961, Erdős,Ginzburg and Ziv proved that $\mathsf{E}(G) \leq 2|G| - 1$ for all finite cyclic groups. This result is well known as the Erdős-Ginzburg-Ziv theorem, and which implies that $\mathsf{E}(G) = 2|G| - 1$ for all finite cyclic groups. When G is a noncyclic solvable group, Yuster and Peterson [19] showed $\mathsf{E}(G) \leq 2|G| - 2$ in 1984. Later, in 1988, Yuster [18] proved that $\mathsf{E}(G) \leq 2|G| - r$ with the restriction that $n \geq 600((r-1)!)^2$. In 1996, Gao [4] improved the asymptotic bound of the theorem to $\mathsf{E}(G) \leq \frac{11|G|}{6} - 1$, and in 2009, Gao and Li [6] proved that $\mathsf{E}(G) \leq \frac{7|G|}{4} - 1$.

Let $\mathsf{d}(G)$ denote the small Davenport constant, which is defined as the maximal integer t such that there are t elements in G(repetition allowed), it is impossible to find some collection of these that has product 1 when multiplied in any order.

Gao [3] proved that $\mathsf{E}(G)=\mathsf{d}(G)+|G|$ for G being abelian(see [3], [9, Proposition 5.7.9], and see Chapter 16 in the monograph [11] for a weighted generalized of this result). The following conjecture is due to Zhuang and Gao [20].

Conjecture 1.1. *For any finite group G we have $\mathsf{E}(G)=\mathsf{d}(G)+|G|$.*

Also Gao and Li [6] conjectured the following

Conjecture 1.2. *For any finite non-cyclic group G we have $\mathsf{E}(G)\leq\frac{3|G|}{2}$.*

Conjecture 1.1 has been verified only for very special non-abelian groups. Zhuang and Gao [20] confirmed conjecture 1.1 for dihedral groups of order $2p$ with $p\geq 4001$ being a prime. Gao and Lu [7] confirmed conjecture 1.1 for all dihedral group of order $2n$, where $n\geq 23$ is an integer. Bass [1] extended the method of Gao and Lu to prove conjecture 1.1 is true for all dihedral groups, dicyclic groups and $C_p\ltimes C_q$, where p, q are primes.

In this paper, we will give a large improvement over these results mentioned above for nilpotent groups, and our main results are as follows.

Theorem 1.3. *Let G be a finite solvable group of order n. If G has a normal subgroup N such that $G/N\simeq C_m\times C_m$, then*

$$n+\mathsf{d}(G)\leq\mathsf{E}(G)\leq n+\frac{n}{m}+m-2.$$

Theorem 1.4. *Let G be a finite nilpotent non-cyclic group of order n, and let p be the smallest prime divisor of n. Then*

$$n+\mathsf{d}(G)\leq\mathsf{E}(G)\leq n+\frac{n}{p}+p-2.$$

In particular, $\mathsf{E}(G)\leq\frac{3n}{2}$.

From theorem 1.3, we can derive the following result.

Theorem 1.5. *Let G be a semidirect product of a normal cyclic subgroup of order pn and a subgroup of order p, where p is a prime and n is a positive integer. Then*

$$\mathsf{E}(G)=|G|+\mathsf{d}(G)=p^2n+p+pn-2.$$

2. preliminaries

This section will provide more rigorous definitions for the above concepts and introduce notations that will be used repeatedly below.

As before, G is a finite group of order n(written multiplicatively). For $a_1, \ldots, a_k \in G$(repetition allowed), we call $S = a_1 \cdot \ldots \cdot a_k$ a *sequence* in G. The *length* of S is $|S| = k$. A *product* of S is a value in G obtained by multiplying all elements of S, i.e., for σ a permutation of the integers $1, \ldots, k$, $a_{\sigma(1)}a_{\sigma(2)} \cdots a_{\sigma(k)}$ is a product of S. For example, we define $\pi(S) = a_1 a_2 \cdots a_k$ to be the specific product of S obtained by multiplying all elements in the order they appear in S. We call S a *product-one sequence* if one of its products is 1.

A *subsequence* is obtained from a sequence by taking a nonempty subset of its indices, so for any $\{i_1, \ldots, i_\ell\} \subset \{1, \ldots, k\}$, we have the subsequence $T_1 = a_{i_1} \cdot \ldots \cdot a_{i_\ell}$ of S. Note that the elements of a subsequence need not be in the same order as they appeared in the original sequence. Let ST_1^{-1} denote the deletion of T_1 from S, which is the subsequence of S corresponding to the set of indices $\{1, \ldots k\} \setminus \{i_1, \ldots i_\ell\}$ in ascending order.

Let $T_2 = a_{j_1} \cdot \ldots \cdot a_{j_k}$ be another subsequence of S. T_1 and T_2 are disjoint if the sets $\{i_1, \ldots, i_\ell\}$ and $\{j_1, \ldots, j_k\}$ are disjoint. We denote the concatenation of disjoint subsequences T_1 and T_2 by $T_1T_2 = a_{i_1} \cdot \ldots \cdot a_{i_\ell} a_{j_1} \cdot \ldots \cdot a_{j_k}$.

A product-one sequence S is called a *minimal product-one sequence* if it can not be partitioned into two nonempty, product-one subsequences.

We denote by $\prod_\ell(S)$ the set consisting of all elements which can be expressed as a product of a subsequence T of S with $|T| = \ell$. In particular,

$$\prod_\ell(S) = \{a_{i_1} \cdots a_{i_\ell} | 1 \leq i_j \leq k \text{ for each } j, \text{ and } i_j \neq i_t \text{ when } j \neq t\}.$$

Using these concepts, we can define

- the small Davenport constant $\mathsf{d}(G)$ to be the maximal length t of all sequence which contains no nonempty product-one subsequence.
- the large Davenport constant $\mathsf{D}(G)$ to be the maximal length t of all minimal product-one sequence.
- $\mathsf{E}(G)$ to be the least integer t such that any sequence S of length t in G has a product-one subsequence T of length $|T| = |G|$.

A simple argument [10, lemma 2.4] shows that

$$\mathsf{d}(G) + 1 \leq \mathsf{D}(G) \leq |G|.$$

When G is abelian, we define

- $\eta(G)$ to be the least integer t such that any sequence S of length t in G has a product-one subsequence T of length $|T| \in [1, \exp(G)]$, where $\exp(G)$ is the exponent of G.
- $\mathsf{s}(G)$ to be the least integer t such that any sequence of length t in G has a product-one subsequence T of length $|T| = \exp(G)$.

Next, we recall [17] the definition of $C_m \ltimes C_n$, it is generated by two elements x, y such that $\langle x\rangle \cap \langle y\rangle = 1$, where the order of y is m and the order of x is n, and $yxy^{-1} = x^s$, $1 \le s \le n-1$.

We begin with the bound of $\mathsf{E}(G)$.

Lemma 2.1. *For every finite group G, $\mathsf{d}(G) + |G| \le \mathsf{E}(G) \le 2|G| - 1$.*

Proof. The lower bound can be found in [20, lemma 4] and the upper bound can be found in [15]. □

Lemma 2.2. ([8]) *Any sequence S over $C_m \times C_m$ of length $|S| = 3m-2$ contains a product-one subsequence T of length $|T| \equiv 0 \pmod m$.*

Lemma 2.3. *Let $G = C_{n_1} \times C_{n_2}$ with $1 \le n_1 | n_2$. Then*

$$\mathsf{s}(G) = 2n_1 + 2n_2 - 3, \eta(G) = 2n_1 + n_2 - 2 \text{ and } \mathsf{d}(G) = n_1 + n_2 - 2.$$

Proof. Refer to [13], [16] and Theorem 5.8.3 in [9]. □

Lemma 2.4. *Let S be a sequence over C_n.*

1. *If $|S| = kn+n-1$ with $k \ge 1$, then S contains a product-one subsequence T of length kn;*
2. *If $|S| = kn+n-2$ with $k \ge 2$ and S contains no product-one subsequence of length kn, then S must be the type $S = a^{xn-1}b^{yn-1}$, where $x+y = k+1$ and $\langle ab^{-1}\rangle = C_n$. Moreover $\prod_{kn-2}(S) = C_n$.*

Proof. **(1)** By using the Erdős-Ginzburg-Ziv theorem of C_n repeatedly, we get the desired result.

(2) Let $S = a_1 \cdot \ldots \cdot a_{kn+n-2}$, we define $\mathsf{v}_a(S) = |\{a_i | a_i = a\}|$ for any $a \in C_n$.

Applying Lemma 2.2 in [5], we obtain that there exist two distinct elements $a, b \in C_n$ such that

$$\mathsf{v}_a(S) + \mathsf{v}_b(S) = (k+1)n - 2.$$

Then we have $S = a^{un+\ell}b^{vn+m}$ with $0 \le \ell \le n-1$ and $0 \le m \le n-1$.

If $0 \le \ell \le n-2$, then

$$(k+1)n > un + vn + m \ge (k+1)n - 2 - \ell \ge kn.$$

Hence $u+v = k$ and $a^{un}b^{vn}$ is a product-one subsequence of S with length kn. A contradiction. Otherwise $\ell = m = n-1$. In other words, $S = a^{xn-1}b^{yn-1}$ and $a^{n-1}b^{n-1}$ contains no product-one of length n.

Note that $\langle ab^{-1}\rangle = C_n$. If not, then we get

$$1 \in \textstyle\prod_n(a^{n-1}b^{n-1}) = \{a^t b^{n-t} = (ab^{-1})^t \mid 0 \le t \le n-1\}.$$

A contradiction.

Thus $S = a^{xn-1}b^{yn-1}$, where $x+y=k+1$ and $\langle ab^{-1}\rangle = C_n$. Therefore we have

$$\prod_{nk-2}(S) = \prod_n(S) = \{a^t b^{n-t} = (ab^{-1})^t \mid 0 \le t \le n-1\} = C_n.$$

□

Lemma 2.5. ([6]) *Let G be a non-cyclic finite solvable group of order n. Then every sequence over G of length $kn + \frac{3}{4}n - 1$ contains a product-one subsequence of length kn.*

We also need the following technical result.

Lemma 2.6. *Let G be a non-cyclic finite p-group, where p is a prime. Then there exists a normal subgroup N of G such that $G/N \simeq C_p \times C_p$.*

Proof. We proceed by induction on the order of G.

If $|G| = p^2$, it is well known that $G \simeq C_p \times C_p$.

If $|G| > p^2$, let $\mathsf{Z}(G) = \{x \in G | xy = yx \text{ for all } y \in G\}$ be the center of G. It is well known that $|\mathsf{Z}(G)| \ge p$ for any finite p-group G.

If $G/\mathsf{Z}(G)$ is cyclic, then G is abelian, there must be a subgroup $N \le G$ with $G/N \simeq C_p \times C_p$. Otherwise $G/\mathsf{Z}(G)$ is non-cyclic, then $p^2 \le |G/\mathsf{Z}(G)| < |G|$. Thus by induction there exists a normal subgroup N of G such that $\mathsf{Z}(G) \subseteq N \subseteq G$ and

$$\big(G/\mathsf{Z}(G)\big)/\big(N/\mathsf{Z}(G)\big) \simeq C_p \times C_p \simeq G/N.$$

□

Lemma 2.7. ([17]) *Let G be a finite nilpotent group, then $G = \prod_p G_p$, where p is a prime and G_p is the Sylow p-subgroup of G.*

3. Proof of the theorems

In this section we shall prove those theorems stated in section 1.

Proof of Theorem 1.3. If $m = 1$, then the upper bound follows from lemma 2.1. Suppose that $m \ge 2$.

Let S be a sequence over G of length $n + \frac{n}{m} + m - 2$. Let ϕ be the following homomorphism

$$\phi : G \to C_m \times C_m,$$

where $ker\phi \simeq N$.

We need to show $1 \in \prod_n(S)$, i.e., that S has a nonempty 1-product subsequence of length n. Since $G/N \simeq C_m \times C_m$, and from lemma 2.3, we know $\mathsf{s}(C_m \times C_m) = 4m-3$. Repeatedly applying the definition of $\mathsf{s}(C_m \times C_m)$ to $\phi(S)$, we can remove product-one subsequences from $\phi(S)$ of length m

until there are at most $4m-4$ terms of $\phi(S)$ left. In other words, we obtain a factorization $S = S_1 \cdot \ldots \cdot S_r S'$ with

$$|S_i| = m \text{ and } \pi(S_i) \in ker\phi \text{ for } 1 \le i \le r, \text{ and } |S'| \le 4m-4.$$

Consequently,

$$r \ge \lceil \frac{n + \frac{n}{m} + m - 2 - 4m + 4}{m} \rceil = \frac{n}{m} + \frac{n}{m^2} - 2.$$

If N is not a cyclic subgroup, then by lemma 2.5, $\pi(S_1) \cdot \ldots \cdot \pi(S_{\frac{n}{m}+\frac{n}{m^2}-2})$ contains a product-one subsequence of length $\frac{n}{m}$, therefore we complete the proof.

Now assume that N is a cyclic subgroup of G. Let $T = SS_1^{-1} \cdot \ldots \cdot S^{-1}_{\frac{n}{m}+\frac{n}{m^2}-2}$. Then $|T| = 3m-2$ and $\phi(T)$ contains a product-one subsequence of length m or $2m$ in $C_m \times C_m$ by lemma 2.2. We distinguish the following two cases.

Case 1: T contains a subsequence of length m, denoted by $S_{\frac{n}{m}+\frac{n}{m^2}-1}$ such that $\pi(S_{\frac{n}{m}+\frac{n}{m^2}-1}) \in ker\phi$.

Then by lemma 2.4 (1) the sequence $\pi(S_1) \cdot \ldots \cdot \pi(S_{\frac{n}{m}+\frac{n}{m^2}-1})$ over N contains a product-one subsequence of length $\frac{n}{m}$. By rearrangement we may assume that $\pi(S_1) \cdot \ldots \cdot \pi(S_{\frac{n}{m}}) = 1$. That is, $S_1 \cdot \ldots \cdot S_{\frac{n}{m}}$ is a product-one subsequence over G of length n.

Case 2: T contains no subsequence T' of length m with $\pi(T') \in ker\phi$.

Therefore T contains a subsequence J of length $2m$ with $\pi(J) \in ker\phi$. Let $W = \pi(S_1) \cdot \ldots \cdot \pi(S_{\frac{n}{m}+\frac{n}{m^2}-2})$, then W is a sequence of length $\frac{n}{m} + \frac{n}{m^2} - 2$ over $C_{\frac{n}{m^2}}$.

If W contains a product-one subsequence of length $\frac{n}{m}$, then we have done. Otherwise, from lemma 2.4(2), $\prod_{\frac{n}{m}-2}(W) = C_{\frac{n}{m^2}}$, thus $(\pi(J))^{-1} \in \prod_{\frac{n}{m}-2}(W)$ and $\pi(S_{i_1}) \cdots \pi(S_{i_{\frac{n}{m}-2}})\pi(J) = 1$ for $1 \le i_1 < \cdots < i_{\frac{n}{m}-2} \le \frac{n}{m} + \frac{n}{m^2} - 2$. Hence $S_{i_1} \cdot \ldots \cdot S_{i_{\frac{n}{m}-2}} J$ is a product-one subsequence of length $(\frac{n}{m} - 2)m + 2m = n$ over G. This completes the proof. □

Proof of Theorem 1.4. By lemma 2.7 we have $G = \prod_q G_q$, where q is a prime and G_q is the Sylow q-subgroup of G. By lemma 2.6 and G is non-cyclic, there exists a noncyclic Sylow q-subgroup G_q and a normal subgroup N_q of G_q such that $G_q/N_q \simeq C_q \times C_q$. Therefore we get the following isomorphism

$$G/(\prod_{p \ne q} G_p \times N_q) \simeq G_q/N_q \simeq C_q \times C_q.$$

Then from Theorem 1.3, we have

$$n + \mathsf{d}(G) \le \mathsf{E}(G) \le n + \frac{n}{q} + q - 2 \le n + \frac{n}{p} + p - 2 \le \frac{3}{2}n,$$

where p is the smallest prime divisor of n. □

Proof of Theorem 1.5. Let G be generated by two elements x, y such that $\langle x\rangle \cap \langle y\rangle = 1$, where the order of y is p and the order of x is pn, $yxy^{-1} = x^s$, $1 \le s \le pn-1$.

It is well known that $G/\langle x^p\rangle$ is abelian, since $G/\langle x^p\rangle$ is a group of order p^2 and p is a prime.

Note that $\bar{g}^p = \bar{1}$ for every element $g \in G$, since $\bar{x}^p = \bar{y}^p = \bar{1}$, where $\bar{g} = g\langle x^p\rangle \in G/\langle x^p\rangle$. Thus $G/\langle x^p\rangle$ is generated by two elements $\bar{x}, \bar{y}$ and $G/\langle x^p\rangle$ is a noncyclic group of order p^2. Then we have the following isomorphism

$$G/\langle x^p\rangle \simeq C_p \times C_p.$$

It is easy to check that the sequence $y^{p-1}x^{pn-1}$ of length $p+pn-2$ contains no non-empty product-one subsequence, since $y^u x^v = x^{s^u v} y^u$ for $u \ge 0, v \ge 0$(the power of y doesn't change). Then by Theorem 1.3 we get

$$np^2 + pn + p - 2 \le np^2 + \mathsf{d}(G) \le \mathsf{E}(G) \le np^2 + pn + p - 2,$$

which completes the proof. □

We end this section with the following

Conjecture 3.1. *Let G be a finite non-cyclic group. Then $\mathsf{E}(G) \le |G| + \frac{|G|}{p} + p - 2$, where p is the smallest prime divisor of $|G|$.*

Acknowledgement The author is very grateful to Professor Weidong Gao for his many useful suggestions. We would like to thank the referee for careful reading and for suggesting several improvements of the manuscripts. This work was supported by the National Science Foundation of China(Grant No. 11401542).

References

1. J. Bass, *Improving the Erdős-Ginzburg-Ziv theorem for non-abelian groups*, J. Number Theory 126 (2007), 217-236.
2. P. Erdős, A. Ginzburg, A. Ziv, *Theorem in the additive number theory*, Bull. Res. Council Israel 10 (1961), 41-43.
3. W. D. Gao, *A combinatorial problem on finite abelian groups*, J. Number Theory 58 (1996), 100-103.
4. W.D. Gao, *An improvement of Erdős-Ginzburg-Ziv theorem* , Acta Math. Sinica 39(1996), 514-523.
5. W.D. Gao, D.C. Han, J.T. Peng, F. Sun, *On zero-sum subsequences of length $k\exp(G)$*, J. Combin. Theory Ser. A 125 (2014), 240-253.
6. W.D. Gao, Y. L. Li, *The Erdős-Ginzburg-Ziv theorem for finite solvable groups*, J. Pure Appl. Algebra 214 (2010), no. 6, 898-909.
7. W.D. Gao, Z.P. Lu, *Erdős-Ginzburg-Ziv theorem for dihedral groups*, J. Pure Appl. Algebra 212 (2008), 311-319.
8. A. Geroldinger, D. J. Grynkiewicz, W. A. Schmid, *Zero-sum problems with congruence conditions*, Acta Math. Hungar. 131 (2011), no. 4, 323-345.

9. A. Geroldinger and F. Halter-Koch, *Non-Unique Factorizations. Algebraic, Combinatorical and Analytic theory*, Pure and Applied Mathmatics, vol. 278, Chapman and Hall/CRC, 2006.
10. A. Geroldinger, D. J. Grynkiewicz, *The large Davenport constant I: groups with a cyclic, index* 2 *subgroup*, J. Pure Appl. Algebra 217(5)(2013), 863-885.
11. D. J. Grynkiewicz, *Structural Additive Theory*, Developments in Mathematics, Springer, 2013.
12. D. J. Grynkiewicz, *The large Davenport constant II: general upper bounds*, J. Pure Appl. Algebra 217 (2013), no. 12, 2221-2246.
13. J. E. Olson, *A combinatorial problem on finite Abelian groups I*, J. Number Theory 1 (1969), 8-10.
14. J. E. Olson, *A combinatorial problem on finite Abelian groups II*, J. Number Theory 1 (1969), 195-199.
15. J. E. Olson, *On a combinatorial problem of Erdős, Ginzburg and Ziv*, J. Number Theory 8 (1976), 52-57.
16. C. Reiher, *On Kemnitz' conjecture concerning lattice points in the plane*, Ramanujan J. 13 (2007), 333-337.
17. D. Robinson, *A Course in the Theory of Groups*, Second edition, in: Graduate Textx in Mathematics, vol. 80, Springer-Verlag, New York, 1996.
18. T. Yuster, *Bounds for counter-example to addition theorem in solvable groups*, Arch. Math. (Basel)51(1988), 223-231.
19. T. Yuster, B. Peterson, *A generalization of an addition theorem for solvable groups*, Canad. J. Math. 36 (1984), 100-103.
20. J. J. Zhuang, W.D. Gao, *Erdős-Ginzburg-Ziv theorem for dihedral groups of large prime index*, European J. Combin. 26 (2005), 1053-1059.

Dongchun Han
Center for Combinatorics, Nankai University, Tianjin 300071, P.R. China
e-mail: `han-qingfeng@163.com`