An Upper Bound for Davenport Constant of Finite Groups

July 11, 2013

Weidong Gao[1], **Yuanlin Li**[2], **Jiangtao Peng**[3]

[1] *Center for Combinatorics, LPMC-TJKLC, Nankai University, Tianjin 300071, P.R. China*

[2] *Department of Mathematics, Brock University, St. Catharines, Ontario, Canada L2S 3A1*

[3] *College of Science, Civil Aviation University of China, Tianjin 300300, P.R. China*

Abstract

Let G be a finite (not necessarily abelian) group and let $p = p(G)$ be the smallest prime number dividing $|G|$. We prove that $\mathsf{d}(G) \le \frac{|G|}{p} + 9p^2 - 10p$, where $\mathsf{d}(G)$ denotes the small Davenport constant of G which is defined as the maximal integer ℓ such that there is a sequence over G of length ℓ contains no nonempty one-product subsequence.

Keywords: one-product; one-product free; Davenport constant.

1. Introduction

Let G be a finite group written multiplicatively. By a sequence S over G, we mean a finite sequence of terms from G which is unordered and repetition of terms is allowed. We say that S is an one-product sequence if its terms can be ordered so that their product equals 1, the identity element of the group. An one-product sequence S is called a minimal one-product sequence if it cannot be partitioned into two nonempty, one-product subsequences. The small Davenport constant $\mathsf{d}(G)$ is the maximal integer t such that there is a sequence over G of length t which contains no nonempty one-product subsequence. The large Davenport constant $\mathsf{D}(G)$ is the maximal length of all minimal one-product sequences. A simple argument [3, Lemma 2.4] shows that

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

2010 Mathematics Subject Classification. 20D60, 11B75.

E-mail address: wdgao@nankai.edu.cn (W.D. Gao), yli@brocku.ca(Y.L. Li), jtpeng@cauc.edu.cn (J.T. Peng)

with equality in the first bound when G is abelian, and equality in the second when G is cyclic. The study of $\mathsf{D}(G)(= \mathsf{d}(G)+1)$, for G abelian, is a classical and very difficult problem in Combinatorial Number Theory. When G is non-abelian, there is more than one way to naturally extend the definition of the Davenport constant. This was first done by Olson and White [8] who introduced the small Davenport constant $\mathsf{d}(G)$ and gave the general upper bound $\mathsf{d}(G) \leq \frac{1}{2}|G|$ (for G non-cyclic) that was observed to be tight for non-cyclic groups having a cyclic, index 2 subgroup. When G is a p-group, $\mathsf{d}(G)$ was studied in [1, Lemma 1.4] and [2]. The large Davenport constant was introduced recently and studied in [3] and [4]. A most recent result of Grynkiewicz [4] states that $\mathsf{d}(G) + 1 \leq \mathsf{D}(G) \leq \frac{2|G|}{p}$. For an arbitrary finite non-abelian group G, let $p = p(G)$ denote the smallest prime divisor of $|G|$. In this paper we provide a better upper bound for the small Davenport constant and our main result is as follows.

Theorem 1.1 *Let G be a finite noncyclic group of order n and let p be the smallest prime divisor of n. Then $\mathsf{d}(G) \leq \frac{n}{p} + 9p^2 - 10p$.*

If G has a cyclic subgroup H of order $\frac{n}{p}$, then H is a normal subgroup of G ([6, Theorem 1]). Let h be a generator of H and let $g \in G \setminus H$. Then the sequence

$$S = \underbrace{g \cdot g \cdot \ldots \cdot g}_{p-1} \cdot \underbrace{h \cdot \ldots \cdot h}_{\frac{n}{p}-1}$$

is an one-product free sequence of length $|S| = \frac{n}{p} + p - 2$. Therefore,

$$\mathsf{d}(G) \geq \frac{n}{p} + p - 2$$

for any groups G having a cyclic subgroup of order $\frac{n}{p}$.

We believe that the above mentioned lower bound is also an upper bound for the small Davenport constant.

Conjecture 1.2 *Let G be a finite noncyclic group of order n, and let p be the smallest prime divisor of n. Then $\mathsf{d}(G) \leq \frac{n}{p} + p - 2$.*

2. Preliminaries

We use the notation and conventions described in detail in [3].

For real numbers $a, b \in \mathbb{R}$, we set $[a, b] = \{x \in \mathbb{Z} : a \leq x \leq b\}$. If A and B are sets, we define the product-set as $AB = \{ab : a \in A, b \in B\}$.

Let G be a finite multiplicative group. If $A \subseteq G$ is a nonempty subset, then denote by $\langle A \rangle$ the subgroup of G generated by A. Recall that by a sequence over a group G we mean a finite,

unordered sequence where the repetition of elements is allowed. We view sequences over G as elements of the free abelian monoid $\mathcal{F}(G)$ and we denote multiplication in $\mathcal{F}(G)$ by the bold symbol $\boldsymbol{\cdot}$ rather than by juxtaposition and use brackets for all exponentiation in $\mathcal{F}(G)$.

A sequence $S \in \mathcal{F}(G)$ can be written in the form $S = g_1 \boldsymbol{\cdot} g_2 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g_\ell$, where $|S| = \ell$ is the *length* of S. For $g \in G$, let

- $\mathsf{v}_g(S) = |\{i \in [1, \ell] : g_i = g\}|$ denote the *multiplicity* of g in S;
- $\mathsf{h}(S) = \max\{\mathsf{v}_g(S) : g \in G\}$ denote the *maximum multiplicity* of a term of S;
- $\mathrm{supp}(S) = \{g : \mathsf{v}_g(S) > 0\}$ denote the *support* of S.

A sequence $T \in \mathcal{F}(G)$ is called a *subsequence* of S and is denoted by $T \mid S$ if $\mathsf{v}_g(T) \le \mathsf{v}_g(S)$ for all $g \in G$. Denote by $T^{[-1]} \boldsymbol{\cdot} S$ or $S \boldsymbol{\cdot} T^{[-1]}$ the subsequence of S obtained by removing the terms of T from S.

If $S_1, S_2 \in \mathcal{F}(G)$, then $S_1 \boldsymbol{\cdot} S_2 \in \mathcal{F}(G)$ denotes the sequence satisfying that $\mathsf{v}_g(S_1 \boldsymbol{\cdot} S_2) = \mathsf{v}_g(S_1) + \mathsf{v}_g(S_2)$ for all $g \in G$. For convenience we write

$$g^{[k]} = \underbrace{g \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g}_{k} \in \mathcal{F}(G) \quad \text{and} \quad T^{[k]} = \underbrace{T \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} T}_{k} \in \mathcal{F}(G),$$

for $g \in G$, $T \in \mathcal{F}(G)$ and $k \in \mathbb{N}_0$. Let $T^{[-k]} = (T^{[k]})^{[-1]}$. If S_1 and S_2 are two subsequences of $S \in \mathcal{F}(G)$, then let $\gcd(S_1, S_2)$ denote the largest subsequence T of S such that $T \mid S_1$ and $T \mid S_2$.

Suppose $S = g_1 \boldsymbol{\cdot} g_2 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g_\ell \in \mathcal{F}(G)$, let

$$\pi(S) = \{g_{\tau(1)} \ldots g_{\tau(\ell)} : \tau \text{ a permutation of } [1, \ell]\} \subseteq G$$

denote the *set of products* of S. Let

$$\Pi(S) = \cup_{1 \le i \le \ell} \cup_{T \mid S,\ |T| = i} \pi(T)$$

denote the *set of all subsequence products* of S. The sequence S is called

- *squarefree* if $\mathsf{v}_g(S) \le 1$ for all $g \in G$;
- *one-product* if $1 \in \pi(S)$;
- *one-product free* if $1 \notin \Pi(S)$;
- *minimal one-product* if $1 \in \pi(S)$ and S cannot be factored into two nontrivial, one-product subsequences.

We call

$$\mathsf{D}(G) = \sup\{\,|S| : S \in \mathcal{F}(G) \text{ is minimal one-product }\} \in \mathbb{N}_0 \cup \{\infty\}$$

the *Large Davenport constant* of G, and

$$\mathsf{d}(G) = \sup\{\,|S| : S \in \mathcal{F}(G) \text{ is one-product free }\} \in \mathbb{N}_0 \cup \{\infty\}$$

the *small Davenport constant* of G.

Lemma 2.1 *[7] Let G be a group and let S be an one-product free sequence over G of length k. Then $|\Pi(S)| \geq \frac{1}{9}k^2$.*

Lemma 2.2 *[8] Suppose A and B are finite subsets of a group and $1 \in A \cap B$. If $1 = ab\,(a \in A, b \in B)$ has no solution except $a = b = 1$, then $|AB| \geq |A| + |B| - 1$.*

The proof of lemma 2.2 may be found in Kemperman [5] and Lemma 2.2 implies the following lemma.

Lemma 2.3 *Let G be a group and let S be an one-product free sequence over G. If $S = S_1 \cdot S_2 \cdot \ldots \cdot S_t$, then $|\Pi(S)| \geq \sum_{i=1}^{t}(|\Pi(S_i)|)$.*

Lemma 2.4 *Let S be an one-product free sequence over a group G. Then $|\Pi(S)| \geq |S|$.*

Let N be a subgroup of a finite group G. For any element $a \in G$, let $\overline{a} = aN$. For any subset A of G, let $\overline{A} = \{\overline{a} : a \in A\}$. Clearly $|\overline{A}| \leq |A|$, and the equality holds if and only if no two elements of A are in the same left coset of N.

Lemma 2.5 *Let N be a subgroup of a finite group G. Let A and B be two nonempty subsets of G with $\overline{1} \in \overline{A} \cap \overline{B}$. If $|\overline{B}| \geq 2$, then $|\overline{AB \cup BA}| \geq \min\{p(G), |\overline{A}| + 1\}$, where $AB = \{ab | a \in A, b \in B\}$, $BA = \{ba | a \in A, b \in B\}$ and $p(G)$ denotes the smallest prime divisor of $|G|$.*

Proof. Assume to the contrary that

$$|\overline{AB \cup BA}| \leq \min\{p(G), \overline{A} + 1\} - 1 = \min\{p(G) - 1, |\overline{A}|\}.$$

Then $|\overline{AB \cup BA}| \leq |\overline{A}|$. Since $\overline{1} \in \overline{B}$, we infer that $\overline{A} \subseteq \overline{AB} \subseteq \overline{AB \cup BA}$. Thus $\overline{A} = \overline{AB \cup BA}$, so $\overline{BA} \subseteq \overline{A}$. Since $\overline{1} \in \overline{A} \cap \overline{B}$, we conclude that $|\overline{BA}| \geq |\overline{A}|$. Thus we have $\overline{A} = \overline{BA}$. Let $b \in B \setminus N$ and let $a \in A$ such that $\overline{a} = \overline{1}$. Since $\overline{BA} = \overline{A}$, we obtain that $\overline{b} = \overline{ba} \in \overline{BA} = \overline{A}$. Thus we have $\overline{b^2} = b\overline{b} \in \overline{BA} = \overline{A}$. Continuing this way, we obtain that $\overline{b^i} \in \overline{A}$ for all nonnegative integers i. Let ℓ be the smallest positive integer such $b^\ell \in N$. Then by the minimality of ℓ, we get $\ell \mid \mathrm{ord}(b)$. Since $b \notin N$, we have $\ell > 1$. Hence $\ell \geq p(G)$. Again, by the minimality of ℓ, we conclude that $\overline{1}, \overline{b}, \cdots, \overline{b^{\ell-1}}$ are distinct elements in $\overline{A} = \overline{AB \cup BA}$. So, $|\overline{AB \cup BA}| \geq p(G)$, yielding a contradiction. □

Lemma 2.6 *Let N be a subgroup of a finite group G, and let S be a sequence over $G \setminus N$. Then* $|\{\overline{1}\} \cup \overline{\Pi(S)}| \geq \min\{p(G), |S| + 1\}$.

Proof. We proceed by induction on $|S|$. If $|S| = 1$ then $|\{\overline{1}\} \cup \overline{\Pi(S)}| = 2 = |S| + 1$. Assume that the lemma is true for $|S| = k$ ($k \geq 1$.) and we want to prove it is also true for $|S| = k + 1$. Take any term $b|S$. Let $T = Sb^{-1}$. Then $|T| = k$ and $|\{\overline{1}\} \cup \overline{\Pi(T)}| \geq \min\{p(G), |T| + 1\}$ by the inductive hypothesis. Let

$$A = \{1\} \cup \Pi(T)$$

and

$$B = \{1, b\}.$$

Then

$$\overline{AB} \cup \overline{BA} \subseteq \{\overline{1}\} \cup \overline{\Pi(S)}.$$

It follows from Lemma 2.5 that $|\{\overline{1}\} \cup \overline{\Pi(S)}| \geq |\overline{AB} \cup \overline{BA}| \geq \min\{p(G), |A|+1\} \geq \min\{p(G), |T|+2\} = \min\{p(G), |S| + 1\}$. □

3. Proof of the Main Theorem

We are now ready to prove our main theorem.

Proof of Theorem 1.1.

Let $S \in \mathcal{F}(G)$ be a sequence of length $\frac{n}{p} + c$ with $c = 9p^2 - 10p + 1$. Then we need to show that $1 \in \Pi(S)$. Without loss of generality we may assume that $\langle S \rangle = G$. We prove by the way of contradiction. Assume to the contrary that S is one-product free. Then

$$|\Pi(S)| \leq n - 1.$$

Let $t \in \mathbb{N}_0$ be maximal such that S has a representation in the form $S = S' \cdot S_1 \cdot S_2 \cdot \ldots \cdot S_t$, where $S_1, \ldots, S_t$ are squarefree, one-product free subsequences of length $|S_\nu| = 9p$ for all $\nu \in [1, t]$. Let $d = |\operatorname{supp}(S')|$. Then

$$|S'| + 9pt = |S| = \frac{n}{p} + c.$$

By the maximality of t we get $0 \leq d \leq 9p - 1$. Since S is one-product free, by Lemmas 2.1, 2.3, and 2.4, we have

$$\begin{aligned} n - 1 &\geq |\Pi(S)| \geq |\Pi(S')| + \textstyle\sum_{i=1}^{t}(|\Pi(S_i)|) \\ &\geq |S'| + 9p^2t = p(\tfrac{n}{p} + c - |S'|) + |S'| \\ &= n - 1 + p(c - |S'|) + |S'| + 1. \end{aligned}$$

It follows that

$$|S'| \geq c + 1 = 9p^2 - 10p + 2. \tag{2}$$

Since $d \le 9p-1$, we have

$$\mathsf{v}_g(S') \ge p.$$

for some $g \in G$.

For each $g \in G$ and each subsequence T of S, let $T_{\langle g\rangle}$ denote the subsequence of T consisting of all terms in $\langle g\rangle$. We first prove a useful claim.

Claim 1: For each $g \in G$, let $C \mid S_{\langle g\rangle}$ and $D \mid S \cdot S^{[-1]}_{\langle g\rangle}$ with $|D| = p-1$. Then $|\Pi(C \cdot D)| \ge p|C|$.

Let $N = \langle g\rangle$. Then $\Pi(C) \subseteq N$. By Lemma 2.4 we have $|\Pi(C)| \ge |C|$. For any element $a \in G$, let $\overline{a} = aN$. For any subset A of G, let $\overline{A} = \{\overline{a} : a \in A\}$. By Lemma 2.6 we have $|\{\overline{1}\} \cup \overline{\Pi(D)}| \ge p$. Thus we obtain that $|\Pi(C \cdot D)| \ge p|C|$. This proves our claim.

We next rewrite S' in a suitable form. Let $T = S'$ and choose $g_1 \in \mathrm{supp}(T)$. If $|T \cdot T^{[-1]}_{\langle g_1\rangle}| \ge p-1$, then S' has a representation

$$S' = D_1 \cdot T_1 \cdot T',$$

where $T_1 = T_{\langle g_1\rangle}$ and $D_1 | T \cdot T^{[-1]}_{\langle g_1\rangle}$ with $|D_1| = p-1$. Let $T = T'$ and repeat the above process on T. Thus $S' = D_1 \cdot T_1 \cdot D_2 \cdot T_2 \cdot T''$. Continuing this way, we obtain that S' has a representation

$$S' = D_1 \cdot T_1 \cdot D_2 \cdot T_2 \cdot \ldots \cdot D_\lambda \cdot T_\lambda \cdot T,$$

where $\lambda = 0$, or $\lambda \in [1, d-1]$ and $T_i | S'_{\langle g_i\rangle}, D_i | S' \cdot S'^{[-1]}_{\langle g_i\rangle}$ with $|D_i| = p-1$, $\mathsf{v}_{g_i}(T) = 0$ for each $i \in [1, \lambda]$, and $|T \cdot T^{[-1]}_{\langle g\rangle}| \le p-2$ for every $g \in \mathrm{supp}(T)$.

We now have the following two cases:

Case 1. $|T_{\langle g\rangle}| \le p-1$ for every $g \in \mathrm{supp}(T)$. We note that $|T| \le \min\{(p-1)(d-\lambda), 2p-3\}$. Since $|S'| \ge 9p^2 - 10p + 2 > 2p-3$, we have $\lambda \ge 1$. Therefore

$$|T| \le (p-1)(d-\lambda) \le (p-1)(9p-2).$$

Note that

$$\frac{n}{p} + c = |S| = 9pt + (p-1)\lambda + |T_1| + \cdots + |T_\lambda| + |T|.$$

By Lemmas 2.3, 2.4 and Claim 1, we conclude

$$\begin{aligned} n-1 &\ge |\Pi(S)| \ge |\Pi(S')| + \textstyle\sum_{i=1}^{t}(|\Pi(S_i)|) \\ &\ge |\Pi(T)| + \textstyle\sum_{i=1}^{\lambda} |\Pi(D_i \cdot T_i)| + \sum_{i=1}^{t}(|\Pi(S_i)|) \\ &\ge |T| + p(|T_1| + \cdots + |T_\lambda|) + 9p^2t \\ &= |T| + p(\tfrac{n}{p} + c - 9pt - (p-1)\lambda - |T|) + 9p^2t \\ &= n + p(c - (p-1)\lambda - |T|) + |T| \ \ (\text{Since } 0 \le |T| \le (p-1)(9p-2)) \\ &\ge n + p(c - (p-1)d) > n-1, \end{aligned}$$

yielding a contradiction.

Case 2. There exists some element $g_{\lambda+1} \in \mathrm{supp}(T)$ such that $|T_{\langle g_{\lambda+1}\rangle}| \ge p$.

If $T_1 \cdot \ldots \cdot T_\lambda \cdot T$ contains at least $p-1$ terms not in $\langle g_{\lambda+1}\rangle$, then S' has a representation

$$S' = D_1 \cdot T_1' \cdot \ldots \cdot D_\lambda \cdot T_\lambda' \cdot D_{\lambda+1} \cdot T_{\lambda+1}$$

such that $T_i' \mid T_i$ for every $i \in [1,\lambda]$, $T_{\lambda+1} = T_{\langle g_{\lambda+1}\rangle}$ and $D_{\lambda+1}$ is a sequence over $G \setminus \langle g_{\lambda+1}\rangle$ of length $p-1$. As in Case 1, we get

$$\begin{aligned} n-1 &\geq |\Pi(S)| \geq |\Pi(D_{\lambda+1} \cdot T_{\lambda+1}) + |\textstyle\sum_{i=1}^{\lambda} |\Pi(D_i \cdot T_i')| + \sum_{i=1}^{t}(|\Pi(S_i)|) \\ &\geq p(|T_1'| + \cdots + |T_\lambda'| + |T_{\lambda+1}|) + 9p^2t \\ &= p(\tfrac{n}{p} + c - 9pt - (p-1)(\lambda+1)) + 9p^2t \\ &\geq n + p(c - (p-1)d) > n-1, \end{aligned}$$

yielding a contradiction. Therefore, we may assume that $T_1 \cdot \ldots \cdot T_\lambda \cdot T$ contains at most $p-2$ terms not in $\langle g_{\lambda+1}\rangle$. It follows that

$$|S'_{\langle g_{\lambda+1}\rangle}| \geq |S'| - (p-2) - (|D_1| + \cdots + |D_\lambda|) \geq |S'| - (p-2) - (9p-2)(p-1).$$

If S' contains at least $p-1$ terms not in $\langle g_{\lambda+1}\rangle$, then S' has a representation $S' = D_{\lambda+1} \cdot T_{\langle g_{\lambda+1}\rangle} \cdot T'$ such that $D_{\lambda+1}$ is a sequence over $G \setminus \langle g_{\lambda+1}\rangle$ of length $p-1$ and $|T'| \leq (9p-3)(p-1) + p - 2$. Now as in Case 1, we can derive a contradiction.

Next we may assume that S' contains at most $p-2$ terms not in $\langle g_{\lambda+1}\rangle$. Let $g = g_{\lambda+1}$. Then S' has a representation

$$S' = D \cdot S'_{\langle g\rangle}$$

with $|D| \leq p-2$. Note that $\langle S\rangle = G$ is noncyclic. Thus we infer that $\langle g\rangle \neq G$. Since S is one-product free, $S_{\langle g\rangle}$ is one-product free, so we have $|S_{\langle g\rangle}| \leq |\langle g\rangle| - 1 \leq \frac{n}{p} - 1$ and thus $|S| - |S_{\langle g\rangle}| \geq c > p$. Therefore, S contains at least $p-1$ terms not in $\langle g\rangle$. By renumbering if necessary, we may assume that S has a representation

$$S = S_1 \cdot \ldots \cdot S_{t'} \cdot D' \cdot S'_{\langle g\rangle} \cdot W$$

with $t' \in [\max\{0, t-p+1+|D|\}, t]$, $D \mid D'$, (D' is a sequence over $G \setminus \langle g\rangle$ of length $p-1$) and $|W| \leq (9p-1)(t-t') \leq (9p-1)(p-1-|D|) \leq (9p-1)(p-1)$. Again as in Case 1, we can derive a contradiction.

In both cases we have found contradictions. Thus we must have $1 \in \Pi(S)$ and this completes the proof.

□

Acknowledgments.

The research was carried out during a visit by the second author to the Center for Combinatorics at Nankai University. He would like to gratefully acknowledge the kind hospitality from the host institution. This work was supported in part by the 973 Program of China (Grant No. 2013CB834204), the PCSIRT Project of the Ministry of Science and Technology, the National Science Foundation of China and a Discovery Grant from the Natural Science and Engineering Research Council of Canada.

References

[1] J. Bass, *Improving the Erdős-Ginzburg-Ziv theorem for some non-abelian groups*, Journal of Number Theory, 126(2007) 217-236.

[2] V. Dimitrov, *On the strong Davenport constant of non-abelian finite p-groups*, Math. Balkica, 18(2004) 131-140.

[3] A. Geroldinger and D. J. Grynkiewicz, *The Large Davenport Constant I: Groups with a Cyclcic, Index 2 Subgroup*, J. Pure and Appl. Alg., 217(2013) 863-885.

[4] D.J. Grynkiewicz, *The Large Davenport Constant II: General upper bounds*, J. Pure and Appl. Alg., to appear.

[5] J.H.B. Kemperman, *On complexes in a semigroup*, Indag. Math. 18(1956) 247-254.

[6] T.Y. Lam, *On subgroups of prime order*, American Mathematical Monthly, 111(2004) 256-258.

[7] J.E. Olson, *Sums of sets of group elements*, Acta Arith. 28(1975) 147-156.

[8] J.E. Olson and E.T. White, *Sums from a sequence of group elements*, Number Theory and Algebra (H. Zassenhaus, ed.), Academic Press, 1977, pp. 215-222.