Acta Math. Univ. Comenianae
Vol. XC, 1 (2021), pp. 1–6

NOTE ON THE DAVENPORT CONSTANT FOR FINITE ABELIAN GROUPS WITH RANK THREE

M. ZAKARCZEMNY

Abstract. Let G be a finite abelian group and $\mathsf{D}(G)$ denote the Davenport constant of G. We derive new upper bound for the Davenport constant for all finite abelian groups of rank three. Our main result is that

$$\mathsf{D}(C_{n_1} \oplus C_{n_2} \oplus C_{n_3}) \leq (n_1 - 1) + (n_2 - 1) + (n_3 - 1) + 1 + (a_3 - 3)(n_1 - 1),$$

where $1 < n_1|n_2|n_3 \in \mathbb{N}$ and $a_3 \leq 20369$ is a constant.
Therefore, $\mathsf{D}(C_{n_1} \oplus C_{n_2} \oplus C_{n_3})$ grows linearly with the variables n_1, n_2, n_3.
The new result is the given upper bound for a_3. Finally, we give an application of the Davenport constant to smooth numbers.

1. Introduction

We study the Davenport constant, a central combinatorial invariant which has been investigated since Davenport popularized it in the 60's, see [**8, 10, 14**] for a survey. We derive new explicit upper bound for the Davenport constant for groups of rank three. The exact value of the Davenport constant for groups of rank three is still unknown and this is an open and well-studied problem, see [**11, 15, 16, 17**].

2. Basic notations

Let $\mathbb{N}$ denote the set of the positive integers (natural numbers). We set $[a, b] = \{x : a \leq x \leq b,\ x \in \mathbb{Z}\}$, where $a, b \in \mathbb{Z}$. Let G be a non-trivial additive finite abelian group. G can be uniquely decomposed as a direct sum of cyclic groups $C_{n_1} \oplus C_{n_2} \oplus \cdots \oplus C_{n_r}$ with the integers satisfying $1 < n_1| \ldots |n_r$. The number of summands in the above decomposition of G is denoted by $r = r(G)$ and called the rank of G. The integer n_r denotes the exponent $\exp(G)$. In addition, we define $\mathsf{D}^*(G)$ as $\mathsf{D}^*(G) = 1 + \sum_{i=1}^{r} (n_i - 1)$. We denote By $\mathcal{F}(G)$ the free, abelian, multiplicatively written monoid with basis G. An element $S \in \mathcal{F}(G)$ is called

Received January 4, 2020; revised April 24, 2020.
2010 *Mathematics Subject Classification.* Primary 11P70, 20K01; Secondary 11B50.
Key words and phrases. Davenport constant; finite abelian group; zero-sum sequence.

sequence over G. We write any finite sequence S of l elements of G in the form $\prod_{g\in G} g^{\nu_g(S)} = g_1 \cdot \ldots \cdot g_l$, where l is the length of S, denoted by $|S|$; $\nu_g(S)$ is the multiplicity of g in S. The sum of S is defined as $\sigma(S) = \sum_{g\in G} \nu_g(S)g$. Our notation and terminology are consistent with [**14**] and [**4**].

The Davenport constant $\mathsf{D}(G)$ is defined as the smallest natural number t such that each sequence over G of length at least t has a non-empty zero-sum subsequence. Equivalently, $\mathsf{D}(G)$ is the maximal length of a zero-sum sequence of the elements of G and with no proper zero-sum subsequence. The best bounds for $\mathsf{D}(G)$ known so far are

$$\mathsf{D}^*(G) \leq \mathsf{D}(G) \leq \exp(G)\left(1 + \log \frac{|G|}{\exp(G)}\right). \tag{1}$$

See [**5**, Theorem 7.1] and [**1**, Theorem 1.1]. The new lower bounds for abelian non-p-groups were given recently in [**13**, Theorem 4.6].

3. Theorems and definitions

Definition 3.1. For an additive finite abelian group G, $m \in \mathbb{N}$, we denote by:

1. $\mathsf{D}_m(G)$, the smallest natural number t such that every sequence S over G of length $|S| \geq t$ contains at least m disjoint and non-empty subsequences $S'_1, S'_2, \ldots, S'_m$ such that $\sigma(S'_i) = 0$ for $i \in [1, m]$.
2. $\eta(G)$, the smallest natural number t such that every sequence S over G of length $|S| \geq t$ contains a non-empty subsequence S' such that $\sigma(S') = 0$, $|S'| \in [1, \exp(G)]$.
3. $\mathsf{s}(G)$, the smallest natural number t such that every sequence S over G of length $|S| \geq t$ contains a non-empty subsequence S' such that $\sigma(S') = 0$, $|S'| = \exp(G)$.

Remark 3.2. $\mathsf{D}_m(G)$ is called the m-th Davenport constant and $\mathsf{s}(G)$ the Erdös-Ginzburg-Ziv constant. In this notation, $\mathsf{D}(G) = \mathsf{D}_1(G)$, see [**6, 7, 12**].

Lemma 3.3. *Let G be a finite abelian group, H a subgroup of G, and k a natural number. Then*

$$\mathsf{D}(G) \leq \mathsf{D}_{\mathsf{D}(H)}(G/H), \tag{2}$$

$$\mathsf{D}_k(G) \leq \exp(G)(k-1) + \eta(G). \tag{3}$$

Proof. See [**7**, Remark 3.3.3, Theorem 3.6] and [**10**, Lemma 6.1.3]. □

Lemma 3.4. *Let G be a finite abelian group.*

1. *If $G = C_{n_1} \oplus C_{n_2}$ with $1 \leq n_1 | n_2$, then*

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

2. *For all finite abelian groups, $\mathsf{D}(G) \leq \eta(G) \leq \mathsf{s}(G) - \exp(G) + 1$.*

Proof. See [**10**, Theorem 5.8.3, Lemma 5.7.2] and [**8**, Theorem 6.3]. □

Remark 3.5. Alon and Dubiner proved that for every natural r and every prime p, we have

$$\mathsf{s}(C_p^r) \leq c(r)p, \tag{4}$$

where $c(r)$ is recursively defined as follows

$$c(r) = 256r(\log_2 r + 5)c(r-1) + (r+1) \qquad \text{for } r \geq 2,\ c(1) = 2. \tag{5}$$

There is a misprint in the corresponding formulas [**2**, (6)], [**3**, (1.4)].

It should be (5) instead of $c(r) = 256(r \log_2 r + 5)c(r-1) + (r+1)$, for more details, see [**4**, Remark 3.7]. Note that $\mathsf{s}(C_p^2) = 4p-3 \leq 4p$ (see, Lemma 3.4), thus we can start a recurrence with initial term $c(2) = 4$ and get $c(3) < 20233.005$.

Remark 3.6. The method used in [**2**], yields that for every natural number $r \geq 1$, there exists $a_r > 0$ such that for every natural number n, we have

$$\eta(C_n^r) \leq a_r(n-1) + 1. \tag{6}$$

We identify a_r with its smallest possible value. It is known that

$$2^r - 1 \leq a_r \leq (cr \log r)^r, \tag{7}$$

where $c > 0$ is an absolute constant. We know also that $a_1 = 1$, $a_2 = 3$. See, [**15**] and Lemma 3.4.

Theorem 3.7 (Edel, Elsholtz, Geroldinger, Kubertin, Rackam [**4**, Theorem 1.4])**.** *Let $G = C_{n_1} \oplus \cdots \oplus C_{n_r}$ with $r = r(G)$ and $1 < n_1 | \ldots | n_r$. Let $b_1, \ldots, b_r \in \mathbb{N}$ such that for all primes p with $p | n_r$ and all $i \in [1, r]$, we have $\mathsf{s}(C_p^i) \leq b_i(p-1) + 1$. Then*

$$\mathsf{s}(G) \leq \sum_{i=1}^{r} (b_{r+1-i} - b_{r-i})n_i - b_r + 1, \tag{8}$$

where $b_0 = 0$. In particular, if $n_1 = \cdots = n_r = n$, then $\mathsf{s}(G) \leq b_r(n-1) + 1$.

Lemma 3.8. *Let $n \geq 2$ be a natural number. Then*

$$\eta(C_n^3) \leq 20369(n-1) + 1 \qquad \text{and} \qquad \mathsf{s}(C_n^3) \leq 20370(n-1) + 1. \tag{9}$$

Therefore, $a_3 \leq 20369$.

Proof. For every finite abelian group G, by [**10**, Theorem 5.7.4], we have

$$\mathsf{s}(G) \leq |G| + \exp(G) - 1. \tag{10}$$

Thus, if p is a prime number such that $2 \leq p \leq p_{34} = 139$, then

$$\mathsf{s}(C_p^3) \leq p^3 + p - 1 < 20370(p-1) + 1. \tag{11}$$

Assume now that p is a prime number such that $p \geq p_{35} = 149$. By Remark 3.5, we have $\mathsf{s}(C_p^3) < 20233.005\,p < 20370(p-1) + 1$ since $p \geq 149$. Therefore, for all primes p, we have $\mathsf{s}(C_p^3) < 20370(p-1) + 1$. By Lemma 3.4, we also have $\mathsf{s}(C_p) = 2(p-1) + 1$, $\mathsf{s}(C_p^2) = 4(p-1) + 1$ for all primes p. Hence by Theorem 3.7 we obtain the upper bound $\mathsf{s}(C_n^3) \leq 20370(n-1) + 1$ for all natural $n \geq 2$. Thus, by Lemma 3.4 we obtain $\eta(C_n^3) \leq 20369(n-1) + 1$ for all natural $n \geq 2$. $\square$

Theorem 3.9. *For an abelian group $C_{n_1} \oplus C_{n_2} \oplus C_{n_3}$, where $1 < n_1|n_2|n_3 \in \mathbb{N}$, there exists an absolute constant $a_3 \leq 20369$ such that*

$$\begin{aligned}\mathsf{D}(C_{n_1} \oplus C_{n_2} \oplus C_{n_3}) \leq\ & (n_1 - 1) + (n_2 - 1) + (n_3 - 1) + 1 \\ & + (a_3 - 3)(n_1 - 1).\end{aligned} \tag{12}$$

Proof. This proof is build on the well-know strategy. Let G be a non-trivial finite abelian group $C_{n_1} \oplus C_{n_2} \oplus C_{n_3}$ such that $1 < n_1|n_2|n_3 \in \mathbb{N}$. We have that the exponent $\exp(G) = n_3$. Denoting a subgroup of G by H such that

$$H \cong C_{\frac{n_2}{n_1}} \oplus C_{\frac{n_3}{n_1}}, \tag{13}$$

where $\frac{n_2}{n_1}, \frac{n_3}{n_1} \in \mathbb{N}$. The quotient group $G/H \cong C_{n_1}^3$. By Lemma 3.3, we get

$$\mathsf{D}(G) \leq \mathsf{D}_{\mathsf{D}(H)}(G/H) = \mathsf{D}_{\frac{n_2}{n_1}+\frac{n_3}{n_1}-1}(C_{n_1}^3) \tag{14}$$

since $\mathsf{D}(H) = \frac{n_2}{n_1} + \frac{n_3}{n_1} - 1$ (see Lemma 3.4). By Lemma 3.3, and (6)

$$\begin{aligned}\mathsf{D}(G) &\leq \exp(C_{n_1}^3)(\tfrac{n_2}{n_1} + \tfrac{n_3}{n_1} - 2) + \eta(C_{n_1}^3) \\ &\leq n_1(\tfrac{n_2}{n_1} + \tfrac{n_3}{n_1} - 2) + a_3(n_1 - 1) + 1 \\ &= (n_1 - 1) + (n_2 - 1) + (n_3 - 1) + 1 + (a_3 - 3)(n_1 - 1),\end{aligned} \tag{15}$$

where a_3 is a constant. By Remark 3.6 and (9), we obtain $a_3 \leq 20369$. □

Remark 3.10. Let $1 < n_1|n_2|n_3 \in \mathbb{N}$. By Theorem 3.9, we have

$$\mathsf{D}(C_{n_1} \oplus C_{n_2} \oplus C_{n_3}) \leq 20367(n_1 - 1) + (n_2 - 1) + (n_3 - 1) + 1. \tag{16}$$

If $n_3 > \frac{20367(n_1-1)+n_2-1}{\log n_1+\log n_2}$, then the upper bound in (16) is smaller than the upper bound from (1). See also [**3**].

Corollary 3.11. *Let $n \geq 2$ be a natural number and let $\omega(n)$ denote the number of distinct prime factors of n. Then*

$$3(n - 1) + 1 \leq \mathsf{D}(C_n^3) \leq \min\{20369, 3^{\omega(n)}\}(n - 1) + 1. \tag{17}$$

Proof. Taking into account the inequality (1) and using Theorem 3.9, we obtain

$$3(n - 1) + 1 \leq \mathsf{D}(C_n^3) \leq 20369(n - 1) + 1.$$

By [**3**, Theorem 1.2], we get $\mathsf{D}(C_n^3) \leq 3^{\omega(n)}(n - 1) + 1$. □

Under the assumption that the conjecture of Gao and Thangadurai [**9**, Conjecture 0] is valid, we can surmise that $a_3 = 8$. Thus, it seemes desirable to attempt to put the following conjecture:

Conjecture 3.12. *Let G be an abelian group $C_{n_1} \oplus C_{n_2} \oplus C_{n_3}$ such that $1 < n_1|n_2|n_3 \in \mathbb{N}$. Then*

$$\mathsf{D}^*(G) \leq \mathsf{D}(G) \leq \mathsf{D}^*(G) + 5(n_1 - 1), \tag{18}$$

where $\mathsf{D}^*(G) = n_1 + n_2 + n_3 - 2$.

We conclude with an application of Theorem 3.9. If F is a set of prime integers, then we shall refer to a positive integer from which each of whose prime factors belongs to F as a smooth over a set F. The smooth numbers are related to the Quadratic sieve and are imported in cryptography in the fastest known integer factorization algorithms. Let $|F| = r$. By $\mathsf{c}(n, r)$ we denote the least positive integer t such that any sequence S of length t of smooth integers over F, has a nonempty subsequence S' such that the product of all the terms of S' is an n-th power of integer. It is known that $\mathsf{c}(n, r) = \mathsf{D}(C_n^r)$ see [**3**, Theorem 1.6]. Thus, by Corollary 3.11, we obtain the following theorem

Theorem 3.13. *If $n \geq 2$ integer, then*

$$\mathsf{c}(n, 3) \leq \min\{20369, 3^{\omega(n)}\}(n - 1) + 1. \tag{19}$$

References

1. Alford W. R., Granville A. and Pomerance C., *There are infinitely many Carmichael numbers*, Ann. of Math. **140**(3) (1994), 703–722.
2. Alon N. and Dubiner M., *A lattice point problem and additive number theory*, Combinatorica **15** (1995), 301–309.
3. Chintamani M. N., Moriya B. K., Gao W. D., Paul P. and Thangadurai R., *New upper bounds for the Davenport and for the Erdös-Ginzburg-Ziv constants*, Arch. Math. (Basel) **98**(2), (2012), 133–142.
4. Edel Y., Elsholtz Ch., Geroldinger A., Kubertin S. and Rackham L., *Zero-sum problems in finite abelian groups and affine caps*, Quart. J. Math. **58** (2007), 159–186.
5. Van Emde Boas P. and Kruyswijk D., *A Combinatorial Problem on Finite Abelian Groups. III*, Math. Centrum Amsterdam Afd. Zuivere Wisk, ZW-008, 1969 .
6. Fan Y., Gao W. and Zhong Q., *On the Erdös-Ginzburg-Ziv constant of finite abelian groups of high rank*, J. Number Theory **131** (2011), 1864–1874.
7. Freeze M. and Schmid W. A., *Remarks on a generalization of the Davenport constant*, Discrete Math. **310** (2010), 3373–3389.
8. Gao W. and Geroldinger A., *Zero-sum problems in finite abelian groups: A survey*, Expo. Math. **24** (2006), 337–369.
9. Gao W. and Thangadurai R., *On zero-sum sequences of prescribed length*, Aequationes Math. **72** (2006), 201–212.
10. Geroldinger A. and Halter-Koch F., *Non-Unique Facorizations. Algebraic, Combinatorial and Analytic Theory*, Pure Appl. Math. 278, Chapman & Hall/CRC, Boca Raton, 2006.
11. Geroldinger A. and Schneider R., *On Davenport's constant*, J. Combin. Theory Ser. A **61**(1) (1992), 147–152.
12. Halter-Koch F., *A generalization of Davenport's constant and its arithmetical applications*, Colloq. Math. **63**(2) (1992), 203–210.
13. Liu Ch., *On the lower bounds of Davenport constant*, J. Combin. Theory Ser. A **171** (2020), 105162.
14. Ruzsa I. and Geroldinger A., *Combinatorial Number Theory and Additive Group Theory*, Adv. Courses Math. CRM Barcelona, Birkhäuser, Basel, 2009.
15. Girard B., *An asymptotically tight bound for the Davenport constant*, J. Ec. Polytech. Math. **5** (2018), 605–611.
16. Girard B. and Schmid W. A., *Direct zero-sum problems for certain groups of rank three*, J. Number Theory **197** (2019), 297–316.
17. Girard B. and Schmid W. A., *Inverse zero-sum problems for certain groups of rank three*, Acta Math. Hungar. **160** (2020), 229–247.

M. Zakarczemny, Department of Applied Mathematics, Faculty of Computer Science and Telecommunications, Cracow University of Technology, Cracow, Poland