On Davenport constant

Benjamin Girard

ON DAVENPORT CONSTANT

BENJAMIN GIRARD

Abstract. We prove that for every fixed integer $r \geqslant 1$ the Davenport constant $\mathsf{D}(C_n^r)$ is asymptotic to rn when n tends to infinity.

For every integer $n \geqslant 1$, let C_n be the cyclic group of order n. It is well known that every non-trivial finite Abelian group G can be uniquely decomposed as a direct product of cyclic groups $C_{n_1} \oplus \cdots \oplus C_{n_r}$ such that $1 < n_1 \mid \cdots \mid n_r \in \mathbb{N}$. The integers r and n_r - sometimes also denoted by $\exp(G)$ - appearing in this decomposition are respectively called the rank and exponent of G. For every integer $1 \leqslant d \mid \exp(G)$, we denote by G_d the subgroup of G consisting of all elements of order dividing d.

Any finite sequence S of ℓ elements of G will be called a sequence over G of length $|S| = \ell$. Also, we denote by $\sigma(S)$ the sum of all elements in S. The sequence S will be referred to as a zero-sum sequence whenever $\sigma(S) = 0$.

By $\mathsf{D}(G)$ we denote the smallest integer $t \geqslant 1$ such that every sequence S over G of length $|S| \geqslant t$ contains a non-empty zero-sum subsequence. This number, which is called the Davenport constant, drew over the last fifty years an ever growing interest, most notably in additive combinatorics and algebraic number theory. A detailed account on the many aspects of this invariant can be found in [8, 10, 13, 17].

To name but one striking feature, let us recall the Davenport constant has the following arithmetical interpretation. Given the ring of integers $\mathcal{O}_{\mathbf{K}}$ of some number field $\mathbf{K}$ with ideal class group G, the maximum number of prime ideals in the decomposition of an irreducible element of $\mathcal{O}_{\mathbf{K}}$ is $\mathsf{D}(G)$ [22]. The importance of this fact is best highlighted by the following generalization of the prime number theorem [17, Theorem 9.15], stating that the number $F(x)$ of pairwise non-associated irreducible elements in $\mathcal{O}_{\mathbf{K}}$ whose norms do not exceed x in absolute value satisfies,

$$F(x) \underset{x \to +\infty}{\sim} C \frac{x}{\log x} (\log \log x)^{\mathsf{D}(G)-1},$$

with a suitable constant $C > 0$ depending solely on G.

We are thus naturally led to the problem of determining the exact value of $\mathsf{D}(G)$. The best explicit bounds known so far are

$$\sum_{i=1}^{r} (n_i - 1) + 1 \leqslant \mathsf{D}(G) \leqslant n_r \left(1 + \log \frac{|G|}{n_r}\right). \tag{1}$$

The lower bound follows easily from the fact that if $(e_1, \ldots, e_r)$ is a basis of G such that $\mathrm{ord}(e_i) = n_i$ for all $i \in [\![1, r]\!]$, the sequence S consisting of $n_i - 1$ copies of e_i for each $i \in [\![1, r]\!]$ contains no non-empty zero-sum subsequence. The upper bound first appeared in [7, Theorem 7.1] and was rediscovered in [16, Theorem 1]. See also [1, Theorem 1.1] for a reformulation of the proof's original argument as well as an application of the Davenport constant to the study of Carmichael numbers.

$\mathsf{D}(G)$ has been proved to match the lower bound in (1) when G is either a p-group [18] or has rank at most 2 [19, Corollary 1.1]. Eventhough there are infinitely many finite Abelian groups whose Davenport constant is known to exceed this lower bound [7, 11, 12, 15], none of the ones identified so far either have rank 3 or the form C_n^r. These two types of groups are actually conjectured to have a Davenport constant matching the lower bound in (1).

2010 Mathematics Subject Classification: 05E15, 11B75, 11A25, 20D60, 20K01.

Sorbonne Universités, UPMC Univ Paris 06, Institut de Mathématiques de Jussieu - Paris Rive Gauche, UMR 7586, CNRS, Univ Paris Diderot, Sorbonne Paris Cité, Case 247, 4 Place Jussieu, 75252 Paris, France, email: benjamin.girard@imj-prg.fr.

Conjecture 1. *For all integers $n, r \geqslant 1$,*

$$\mathsf{D}(C_n^r) = r(n-1)+1.$$

Besides the already mentioned results settling Conjecture 1 for all r when n is a prime power and for all n when $r \leqslant 2$, note that $\mathsf{D}(C_n^3)$ is known only when $n = 2p^\alpha$, with p prime and $\alpha \geqslant 1$ [6, Corollary 4.3], or $n = 2^\alpha 3$ with $\alpha \geqslant 2$ [7, Corollary 5.1], and satisfies Conjecture 1 in both cases. To the best of our knowledge, the exact value of $\mathsf{D}(C_n^r)$ is currently unknown for all pairs (n, r) such that n is not a prime power and $r \geqslant 4$. In all those remaining cases, the bounds in (1) translate into

$$r(n-1)+1 \leqslant \mathsf{D}(C_n^r) \leqslant n\left(1+(r-1)\log n\right), \tag{2}$$

which leaves a substantial gap to be bridged. Conjecture 1 thus remains wide open.

The aim of the present note is to clarify the behavior of $\mathsf{D}(C_n^r)$ for any fixed $r \geqslant 1$ when n goes to infinity. Our main theorem proves Conjecture 1 in the following asymptotic sense.

Theorem 1. *For every integer $r \geqslant 1$,*

$$\mathsf{D}(C_n^r) \underset{n\to+\infty}{\sim} rn.$$

The proof of Theorem 1 relies on a new upper bound for $\mathsf{D}(C_n^r)$, turning out to be a lot sharper than the one in (2) for large values of n. So as to state it properly, we now make the following definition. For every integer $n \geqslant 1$, we denote by $P(n)$ the greatest prime power dividing n, with the convention $P(1) = 1$.

Theorem 2. *For every integer $r \geqslant 1$, there exists a constant $d_r \geqslant 0$ such that for every integer $n \geqslant 1$,*

$$\mathsf{D}(C_n^r) \leqslant r\,(n-1)+1+d_r\left(\frac{n}{P(n)}-1\right).$$

Now, since $P(n)$ tends to infinity when n does so, Theorem 2 allows us to deduce that, for every integer $r \geqslant 1$, the gap between the Davenport constant and its conjectural value

$$\Delta(C_n^r) = \mathsf{D}(C_n^r) - (r\,(n-1)+1)$$

is actually $o(n)$. This theorem will be obtained via the inductive method, which involves another key combinatorial invariant we now proceed to define.

By $\eta(G)$ we denote the smallest integer $t \geqslant 1$ such that every sequence S over G of length $|S| \geqslant t$ contains a non-empty zero-sum subsequence $S' \mid S$ with $|S'| \leqslant \exp(G)$. It is readily seen that $\mathsf{D}(G) \leqslant \eta(G)$ for every finite Abelian group G.

A natural construction shows that, for all integers $n, r \geqslant 1$, one has

$$(2^r-1)(n-1)+1 \leqslant \eta(C_n^r). \tag{3}$$

Indeed, if $(e_1, \ldots, e_r)$ is a basis of C_n^r, it is easily checked that the sequence S consisting of $n-1$ copies of $\sum_{i\in I} e_i$ for each non-empty subset $I \subseteq [\![1, r]\!]$ contains no non-empty zero-sum subsequence of length at most n.

The exact value of $\eta(C_n^r)$ is known to match the lower bound in (3) for all n when $r \leqslant 2$ [13, Theorem 5.8.3], and for all r when $n = 2^\alpha$, with $\alpha \geqslant 1$ [14, Satz 1]. Besides these two results, $\eta(C_n^r)$ is currently known only when $r = 3$ and $n = 3^\alpha 5^\beta$, with $\alpha, \beta \geqslant 0$ [9, Theorem 1.7], in which case $\eta(C_n^3) = 8n-7$, or $n = 2^\alpha 3$, with $\alpha \geqslant 1$ [9, Theorem 1.8], in which case $\eta(C_n^3) = 7n-6$. When $n = 3$, note that the problem of finding $\eta(C_3^r)$ is closely related to the well-known cap-set problem, and that for $r \geqslant 4$, the only known values so far are $\eta(C_3^4) = 39$ [20], $\eta(C_3^5) = 89$ [4] and $\eta(C_3^6) = 223$ [21]. For more details on this fascinating topic, see [3, 5] and the references contained therein.

In another direction, Alon and Dubiner showed [2] that when r is fixed, $\eta(C_n^r)$ grows linearly in the exponent n. More precisely, they proved that for every integer $r \geqslant 1$, there exists a constant $c_r > 0$ such that for every integer $n \geqslant 1$,

$$\eta\left(C_n^r\right) \leqslant c_r(n-1)+1. \tag{4}$$

From now on, we will identify c_r with its smallest possible value in this theorem.

On the one hand, it follows from (3) that $c_r \geqslant 2^r - 1$, for all $r \geqslant 1$. Since, as already mentioned, $\eta(C_n) = n$ and $\eta(C_n^2) = 3n-2$ for all $n \geqslant 1$, it is possible to choose $c_1 = 1$ and $c_2 = 3$, with equality in (4).

On the other hand, the method used in [2] yields $c_r \leqslant (cr\log r)^r$, where $c > 0$ is an absolute constant, and it is conjectured in [2] that there actually is an absolute constant $d > 0$ such that $c_r \leqslant d^r$ for all $r \geqslant 1$.

We can now state and prove our main technical result, which is the following.

Theorem 3. *For all integers $n, r \geqslant 1$,*

$$\mathsf{D}(C_n^r) \leqslant r\,(n-1) + 1 + (c_r - r)\left(\frac{n}{P(n)} - 1\right).$$

Proof of Theorem 3. We set $G = C_n^r$ and denote by $H = G_{P(n)}$ the largest Sylow subgroup of G. Since $H \simeq C_{P(n)}^r$ is a p-group, it follows from [18] that

$$\mathsf{D}(H) = r(P(n)-1)+1.$$

In addition, since the quotient group $G/H \simeq C_{n/P(n)}^r$ has rank r and exponent $n/P(n)$, it follows from (4) that

$$\eta(G/H) \leqslant c_r\left(\frac{n}{P(n)} - 1\right) + 1.$$

Now, from any sequence S over G such that

$$|S| \geqslant \exp(G/H)\,(\mathsf{D}(H)-1) + \eta(G/H),$$

one can sequentially extract at least $d = \mathsf{D}(H)$ disjoint non-empty subsequences $S_1', \ldots, S_d' \mid S$ such that $\sigma(S_i') \in H$ and $|S_i'| \leqslant \exp(G/H)$ for every $i \in [\![1, d]\!]$. Since $T = \prod_{i=1}^d \sigma(S_i')$ is a sequence over H of length $|T| = \mathsf{D}(H)$, there exists a non-empty subset $I \subseteq [\![1, d]\!]$ such that $T' = \prod_{i\in I}\sigma(S_i')$ is a zero-sum subsequence of T. Then, $S' = \prod_{i\in I} S_i'$ is a non-empty zero-sum subsequence of S.

Therefore, we have

$$\begin{aligned}
\mathsf{D}(G) &\leqslant \exp(G/H)\,(\mathsf{D}(H)-1) + \eta(G/H) \\
&\leqslant \frac{n}{P(n)}\,(r(P(n)-1)) + c_r\left(\frac{n}{P(n)} - 1\right) + 1 \\
&= r(n-1) + 1 + (c_r - r)\left(\frac{n}{P(n)} - 1\right),
\end{aligned}$$

which completes the proof. □

Theorems 1 and 2 are now direct corollaries of Theorem 3.

Proof of Theorem 2. The result follows from Theorem 3 by setting $d_r = c_r - r$. □

Proof of Theorem 1. Since $P(n)$ tends to infinity when n does so, the desired result follows easily from (1) and Theorem 2. □

Acknowledgements

The author is grateful to W.A. Schmid for his careful reading of the manuscript in an earlier version.

References

[1] W.R. Alford, A. Granville and C. Pomerance *There are infinitely many Carmichael numbers*, Annals of Math. **140** (3) (1994), 703-722.

[2] N. Alon and M. Dubiner *A lattice point problem and additive number theory*, Combinatorica **15** (1995), 301-309.

[3] Y. Edel, C. Elsholtz, A. Geroldinger, S. Kubertin and L. Rackham *Zero-sum problems in finite abelian groups and affine caps*, Q. J. Math. **58** (2007), 159-186.

[4] Y. Edel, S. Ferret, I. Landjev and L. Storme *The classification of the largest caps in AG(5,3)*, J. Combin. Theory Ser. A **99** (2002), 95-110.

[5] J. S. Ellenberg and D. Gijswijt *On large subsets of $\mathbb{F}_q^n$ with no three-term arithmetic progression*, Annals of Math. **185** (1) (2017), 339-343.

[6] P. van Emde Boas *A combinatorial problem on finite abelian groups II*, Reports ZW-1969-007, Math. Centre, Amsterdam (1969).

[7] P. van Emde Boas and D. Kruyswijk *A combinatorial problem on finite abelian groups III*, Reports ZW-1969-008, Math. Centre, Amsterdam (1969).

[8] W. Gao and A. Geroldinger *Zero-sum problems in finite abelian groups: a survey*, Expo. Math. **24** (2006), 337-369.

[9] W. Gao, Q. H. Hou, W. A. Schmid and R. Thangadurai *On short zero-sum subsequences II*, Integers **7** (2007), #A21.

[10] A. Geroldinger *Additive group theory and non-unique factorizations*, In A. Geroldinger and I. Ruzsa, *Combinatorial Number Theory and Additive Group Theory*, Advanced Courses in Mathematics, CRM Barcelona, Birkhäuser (2009), 1-86.

[11] A. Geroldinger, M. Liebmann and A. Philipp *On the Davenport constant and on the structure of extremal zero-sum free sequences*, Period. Math. Hungar. **64** (2) (2012), 213-225.

[12] A. Geroldinger and R. Schneider *On Davenport's constant*, J. Combin. Theory Ser. A **61** (1992), 147-152.

[13] A. Geroldinger and F. Halter-Koch *Non-unique factorizations. Algebraic, combinatorial and analytic theory*, Pure and Applied Mathematics **278**, Chapman & Hall/CRC (2006).

[14] H. Harborth *Ein Extremalproblem für Gitterpunkte*, J. Reine Angew. Math. **262** (1973), 356-360.

[15] M. Mazur *A note on the growth of Davenport constant*, Manuscripta Math. **74** (1992), 229-235.

[16] R. Meshulam *An uncertainty inequality and zero subsums*, Discrete Math. **84** (1990), 197-200.

[17] W. Narkiewicz *Elementary and analytic theory of algebraic numbers*, 3rd edition, Springer (2004).

[18] J. E. Olson *A combinatorial problem on finite abelian groups I*, J. Number Theory **1** (1969), 8-10.

[19] J. E. Olson *A combinatorial problem on finite abelian groups II*, J. Number Theory **1** (1969), 195-199.

[20] G. Pellegrino *The maximal order of the spherical cap in $S_{4,3}$*, Matematiche **25** (1971), 149-157.

[21] A. Potechin *Maximal caps in AG(6,3)*, Des. Codes Cryptogr. **46** (2008), 243-259.

[22] K. Rogers *A combinatorial problem in Abelian groups*, Proc. Camb. Philos. Soc. **59** (1963), 559-562.