An asymptotically tight bound for the Davenport constant

Benjamin Girard

To cite this version:

Benjamin Girard. An asymptotically tight bound for the Davenport constant. Journal de l'École polytechnique - Mathématiques, 2018, 5, pp.605-611. 10.5802/jep.79 . hal-01592317v3

HAL Id: hal-01592317
https://hal.science/hal-01592317v3

Submitted on 2 Jul 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

AN ASYMPTOTICALLY TIGHT BOUND FOR THE DAVENPORT CONSTANT

BENJAMIN GIRARD

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

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 appearing in this decomposition are respectively called the rank and the exponent of G. The latter is denoted by $\exp(G)$. For the trivial group, the rank is 0 and the exponent is 1. 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 [4, 11, 13, 14, 21].

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 $\mathsf{D}(G)$ [26]. The importance of this fact is best highlighted by the following generalization of the prime number theorem [21, 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 (see [14, Chapter 9.1] and [18, Theorem 1.1] for sharper and more general results).

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 [9, Theorem 7.1] and was rediscovered in [20, 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.

2010 *Mathematics Subject Classification.* 05E15, 11B30, 11B75, 11A25, 20D60, 20K01.
Key words and phrases. Additive combinatorics, zero-sum sequences, Davenport constant, finite Abelian groups.
Sorbonne Université, Université Paris Diderot, CNRS, Institut de Mathématiques de Jussieu - Paris Rive Gauche, IMJ-PRG, F-75005, Paris, France, email: benjamin.girard@imj-prg.fr.

$\mathsf{D}(G)$ has been proved to match the lower bound in (1) when G is either a p-group [22] or has rank at most 2 [23, Corollary 1.1]. Even though there are infinitely many finite Abelian groups whose Davenport constant is known to exceed this lower bound [9, 15, 16, 19], none of the ones identified so far either have rank 3 or the form C_n^r. Since the late sixties, these two types of groups have been conjectured to have a Davenport constant matching the lower bound in (1). This open problem was first raised in [9, pages 13 and 29] and can be found formally stated as a conjecture in [11, Conjecture 3.5]. See also [3, Conjecture A.5] and [10, Theorem 6.6] for connections with graph theory and covering problems.

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 $\alpha \geqslant 1$ [8, Corollary 4.3], or $n = 2^\alpha 3$ with $\alpha \geqslant 2$ [9, Corollary 1.5], 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 $n \geqslant 1$,*

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

The relevance of this bound to the study of the Davenport constant is due to the fact that the arithmetic function $P(n)$ tends to infinity when n does so. Indeed, if we denote by $\mathcal{P}$ the set of prime numbers and let $(a_n)_{n \geqslant 1}$ be the sequence defined for every integer $n \geqslant 1$ by

$$a_n = \prod_{p \in \mathcal{P}} p^{\left\lfloor \frac{\log n}{\log p} \right\rfloor},$$

we easily notice that, for every integer $N \geqslant 1$, one has $P(n) > N$ as soon as $n > a_N$.

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

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

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 $r \leqslant 2$ [14, Theorem 5.8.3], and for all r when $n = 2^\alpha$, with $\alpha \geqslant 1$ [17, Satz 1]. Besides these two results, $\eta(C_n^r)$ is currently known only when $r = 3$ and $n = 3^\alpha 5^\beta$, with $\alpha, \beta \geqslant 0$ [12, Theorem 1.7], in which case $\eta(C_n^3) = 8n - 7$, or $n = 2^\alpha 3$, with $\alpha \geqslant 1$ [12, 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 $\eta(C_3^4) = 39$ [24], $\eta(C_3^5) = 89$ [6] and $\eta(C_3^6) = 223$ [25]. For more details on this fascinating topic, see [5, 7] 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 first 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 [22] that

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

In addition, since the quotient group $G/H \simeq C_{n/P(n)}^r$ has exponent $n/P(n)$ and rank at most r, 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 $i \in [\![1, d]\!]$ (see for instance [14, Lemma 5.7.10]). 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. □

Note that Theorem 3 is sharp for all n when $r = 1$ and for all r when n is a prime power. Also, 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 (2) and Theorem 2. □

To conclude this paper, we would like to offer a possibly useful extension of our theorems to the following wider framework. Given any finite Abelian group L and any integer $r \geqslant 1$, we consider the groups defined by $L^r_n = L \oplus C^r_n$, where $n \geqslant 1$ is any integer such that $\exp(L) \mid n$. Note that if L is the trivial group, then $L^r_n \simeq C^r_n$ whose Davenport constant is already covered by Theorems 1-3.

Our aim in this more general context is to prove that, for every finite Abelian group L and every integer $r \geqslant 1$, $\mathsf{D}(L^r_n)$ behaves asymptotically in the same way it would if L were trivial. To do so, we establish the following extension of Theorem 3.

Theorem 4. *Let $L \simeq C_{n_1} \oplus \cdots \oplus C_{n_\ell}$, with $1 < n_1 \mid \cdots \mid n_\ell \in \mathbb{N}$, be a finite Abelian group. For every integer $n \geqslant 1$ such that $\exp(L) \mid n$ and every integer $r \geqslant 1$,*

$$\mathsf{D}(L^r_n) \leqslant r\,(n-1) + 1 + (c_{\ell+r} - r)\left(\frac{n}{P(n)} - 1\right) + \frac{n}{P(n)} \sum_{i=1}^{\ell} (\gcd(n_i, P(n)) - 1).$$

Proof of Theorem 4. We set $G = L^r_n$ and $H = G_{P(n)}$. On the one hand, since $H \simeq C_{n'_1} \oplus \cdots \oplus C_{n'_\ell} \oplus C^r_{P(n)}$, with $n'_i = \gcd(n_i, P(n)) \mid n_i$ for all $i \in [\![1, \ell]\!]$ and $1 \leqslant n'_1 \mid \cdots \mid n'_\ell \mid P(n)$, is a p-group, it follows from [22] that

$$\mathsf{D}(H) = \sum_{i=1}^{\ell} (n'_i - 1) + r(P(n) - 1) + 1.$$

On the other hand, since the quotient group G/H has exponent $n/P(n)$ and rank at most $\ell + r$, it follows from (4) that

$$\eta(G/H) \leqslant \eta\left(C^{\ell+r}_{\frac{n}{P(n)}}\right) \leqslant c_{\ell+r}\left(\frac{n}{P(n)} - 1\right) + 1.$$

Therefore, the same argument we used in our proof of Theorem 3 yields

$$\begin{aligned}
\mathsf{D}(G) &\leqslant \exp(G/H)\,(\mathsf{D}(H)-1) + \eta(G/H) \\
&\leqslant \frac{n}{P(n)}\left(\sum_{i=1}^{\ell} (n'_i - 1) + r(P(n)-1)\right) + c_{\ell+r}\left(\frac{n}{P(n)} - 1\right) + 1 \\
&= r\,(n-1) + 1 + (c_{\ell+r} - r)\left(\frac{n}{P(n)} - 1\right) + \frac{n}{P(n)} \sum_{i=1}^{\ell} (n'_i - 1),
\end{aligned}$$

which is the desired upper bound. □

Theorem 4 now easily implies the following generalization of Theorem 1.

Theorem 5. *For every finite Abelian group L and every integer $r \geqslant 1$,*

$$\mathsf{D}(L_n^r) \underset{\substack{n \to +\infty \\ \exp(L) \mid n}}{\sim} rn.$$

Proof of Theorem 5. We write $L \simeq C_{n_1} \oplus \cdots \oplus C_{n_\ell}$, with $1 < n_1 \mid \cdots \mid n_\ell \in \mathbb{N}$. For every integer $n \geqslant 1$ such that $\exp(L) \mid n$, one has $\gcd(n_i, P(n)) \leqslant n_i$ for all $i \in [\![1, \ell]\!]$. Since $P(n)$ tends to infinity when n does so, the result follows easily from (1) and Theorem 4. □

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*, Ann. of Math. **139** (3) (1994), 703-722.
[2] N. Alon and M. Dubiner *A lattice point problem and additive number theory*, Combinatorica **15** (3) (1995), 301-309.
[3] N. Alon, S. Friedland and G. Kalai *Regular subgraphs of almost regular graphs*, J. Combin. Theory Ser. B **37** (1) (1984), 79-91.
[4] K. Cziszter, M. Domokos and A. Geroldinger *The interplay of invariant theory with multiplicative ideal theory and with arithmetic combinatorics*, in *Multiplicative ideal theory and factorization theory*, Springer Proc. Math. Stat. **170**, Springer (2016), 43-95.
[5] 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** (2) (2007), 159-186.
[6] 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** (1) (2002), 95-110.
[7] J.S. Ellenberg and D. Gijswijt *On large subsets of $\mathbb{F}_q^n$ with no three-term arithmetic progression*, Ann. of Math. **185** (1) (2017), 339-343.
[8] P. van Emde Boas *A combinatorial problem on finite abelian groups II*, Tech. Report ZW-007, Math. Centrum Amsterdam Afd. Zuivere Wisk. (1969).
[9] P. van Emde Boas and D. Kruyswijk *A combinatorial problem on finite abelian groups III*, Tech. Report ZW-008, Math. Centrum Amsterdam Afd. Zuivere Wisk. (1969).
[10] W. Gao and A. Geroldinger *Zero-sum problems and coverings by proper cosets*, European J. Combin. **24** (5) (2003), 531-549.
[11] W. Gao and A. Geroldinger *Zero-sum problems in finite abelian groups: a survey*, Expo. Math. **24** (4) (2006), 337-369.
[12] W.D. Gao, Q.H. Hou, W.A. Schmid and R. Thangadurai *On short zero-sum subsequences II*, Integers **7** (2007), #A21.
[13] A. Geroldinger *Additive group theory and non-unique factorizations*, in *Combinatorial number theory and additive group theory*, Adv. Courses Math. CRM Barcelona, Birkhäuser Verlag (2009), 1-86.
[14] A. Geroldinger and F. Halter-Koch *Non-unique factorizations. Algebraic, combinatorial and analytic theory*, Pure and Applied Mathematics **278**, Chapman & Hall/CRC (2006).
[15] 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.
[16] A. Geroldinger and R. Schneider *On Davenport's constant*, J. Combin. Theory Ser. A **61** (1) (1992), 147-152.
[17] H. Harborth *Ein Extremalproblem für Gitterpunkte*, J. reine angew. Math. **262/263** (1973), 356-360.
[18] J. Kaczorowski *On the distribution of irreducible algebraic integers*, Monatsh. Math. **156** (1) (2009), 47-71.
[19] M. Mazur *A note on the growth of Davenport's constant*, Manuscripta Math. **74** (3) (1992), 229-235.
[20] R. Meshulam *An uncertainty inequality and zero subsums*, Discrete Math. **84** (2) (1990), 197-200.
[21] W. Narkiewicz *Elementary and analytic theory of algebraic numbers*, 3rd edition, Springer Monographs in Math., Springer-Verlag (2004).

[22] J.E. Olson *A combinatorial problem on finite abelian groups I*, J. Number Theory **1** (1969), 8-10.
[23] J.E. Olson *A combinatorial problem on finite abelian groups II*, J. Number Theory **1** (1969), 195-199.
[24] G. Pellegrino *The maximal order of the spherical cap in* $S_{4,3}$, Matematiche **25** (1971), 149-157.
[25] A. Potechin *Maximal caps in* $AG(6,3)$, Des. Codes Cryptogr. **46** (3) (2008), 243-259.
[26] K. Rogers *A combinatorial problem in Abelian groups*, Math. Proc. Cambridge Philos. Soc. **59** (1963), 559-562.