

Journal de l'École polytechnique

Mathématiques

Benjamin GIRARD

An asymptotically tight bound for the Davenport constant

Tome 5 (2018), p. 605-611.

http://jep.cedram.org/item?id=JEP_2018__5__605_0

© Les auteurs, 2018.

Certains droits réservés.



Cet article est mis à disposition selon les termes de la licence
CREATIVE COMMONS ATTRIBUTION – PAS DE MODIFICATION 3.0 FRANCE.
<http://creativecommons.org/licenses/by-nd/3.0/fr/>

L'accès aux articles de la revue « Journal de l'École polytechnique — Mathématiques » (<http://jep.cedram.org/>), implique l'accord avec les conditions générales d'utilisation (<http://jep.cedram.org/legal/>).

Publié avec le soutien
du Centre National de la Recherche Scientifique

cedram

Article mis en ligne dans le cadre du
Centre de diffusion des revues académiques de mathématiques
<http://www.cedram.org/>

AN ASYMPTOTICALLY TIGHT BOUND FOR
THE DAVENPORT CONSTANT

BY BENJAMIN GIRARD

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

RÉSUMÉ (Une borne asymptotiquement optimale pour la constante de Davenport)

Nous prouvons que pour tout entier $r \geq 1$, la constante de Davenport $D(C_n^r)$ est équivalente à rn lorsque n tend vers l'infini. Nous proposons aussi une extension de ce théorème.

For every integer $n \geq 1$, 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 $1 \leq d \mid \exp(G)$, 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 $D(G)$ we denote the smallest integer $t \geq 1$ such that every sequence S over G of length $|S| \geq t$ 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 $D(G)$ [26]. The importance of this fact is best highlighted by the following generalization of the prime number theorem

2010 MATHEMATICS SUBJECT CLASSIFICATION. — 05E15, 11B30, 11B75, 11A25, 20D60, 20K01.

KEYWORDS. — Additive combinatorics, zero-sum sequences, Davenport constant, finite Abelian groups.

[21, Th. 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,

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

with a suitable constant $C > 0$ depending solely on G (see [14, Chap. 9.1] and [18, Th. 1.1] for sharper and more general results).

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

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

The lower bound follows easily from the fact that if (e_1, \dots, e_r) is a basis of G such that $\text{ord}(e_i) = n_i$ for all $i \in \llbracket 1, r \rrbracket$, the sequence S consisting of $n_i - 1$ copies of e_i for each $i \in \llbracket 1, r \rrbracket$ contains no non-empty zero-sum subsequence. The upper bound first appeared in [9, Th. 7.1] and was rediscovered in [20, Th. 1]. See also [1, Th. 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.

$D(G)$ 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, Cor. 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, p. 13 & 29] and can be found formally stated as a conjecture in [11, Conj. 3.5]. See also [3, Conj. A.5] and [10, Th. 6.6] for connections with graph theory and covering problems.

CONJECTURE 1. — *For all integers $n, r \geq 1$,*

$$D(C_n^r) = r(n - 1) + 1.$$

Besides the already mentioned results settling Conjecture 1 for all r when n is a prime power and for all n when $r \leq 2$, note that $D(C_n^3)$ is known only when $n = 2p^\alpha$, with p prime and $\alpha \geq 1$ [8, Cor. 4.3], or $n = 2^\alpha 3$ with $\alpha \geq 2$ [9, Cor. 1.5], and satisfies Conjecture 1 in both cases. To the best of our knowledge, the exact value of $D(C_n^r)$ is currently unknown for all pairs (n, r) such that n is not a prime power and $r \geq 4$. In all those remaining cases, the bounds in (1) translate into

$$(2) \quad r(n - 1) + 1 \leq D(C_n^r) \leq n(1 + (r - 1) \log n),$$

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 $D(C_n^r)$ for any fixed $r \geq 1$ when n goes to infinity. Our main theorem proves Conjecture 1 in the following asymptotic sense.

THEOREM 1. — For every integer $r \geq 1$,

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

The proof of Theorem 1 relies on a new upper bound for $D(C_n^r)$, 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 $n \geq 1$, we denote by $P(n)$ the greatest prime power dividing n , with the convention $P(1) = 1$.

THEOREM 2. — For every integer $r \geq 1$, there exists a constant $d_r \geq 0$ such that for every integer $n \geq 1$,

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

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 $(a_n)_{n \geq 1}$ be the sequence defined for every integer $n \geq 1$ by

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

we easily notice that, for every integer $N \geq 1$, 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 $r \geq 1$, the gap between the Davenport constant and its conjectural value

$$D(C_n^r) - (r(n - 1) + 1)$$

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 $t \geq 1$ such that every sequence S over G of length $|S| \geq t$ contains a non-empty zero-sum subsequence $S' \mid S$ with $|S'| \leq \exp(G)$. It is readily seen that $D(G) \leq \eta(G)$ for every finite Abelian group G .

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

$$(3) \quad (2^r - 1)(n - 1) + 1 \leq \eta(C_n^r).$$

Indeed, if (e_1, \dots, 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 $I \subseteq \llbracket 1, r \rrbracket$ 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 $r \leq 2$ [14, Th. 5.8.3], and for all r when $n = 2^\alpha$, with $\alpha \geq 1$ [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 $\alpha, \beta \geq 0$ [12, Th. 1.7], in which case $\eta(C_n^3) = 8n - 7$, or $n = 2^\alpha 3$, with $\alpha \geq 1$ [12, Th. 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 $r \geq 4$, 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 $r \geq 1$, there exists a constant $c_r > 0$ such that for every integer $n \geq 1$,

$$(4) \quad \eta(C_n^r) \leq c_r(n-1) + 1.$$

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 $c_r \geq 2^r - 1$, for all $r \geq 1$. Since, as already mentioned, $\eta(C_n) = n$ and $\eta(C_n^2) = 3n - 2$ for all $n \geq 1$, 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 $c_r \leq (cr \log r)^r$, where $c > 0$ is an absolute constant, and it is conjectured in [2] that there actually is an absolute constant $d > 0$ such that $c_r \leq d^r$ for all $r \geq 1$.

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

THEOREM 3. — *For all integers $n, r \geq 1$,*

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

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

$$D(H) = r(P(n) - 1) + 1.$$

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

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

Now, from any sequence S over G such that

$$|S| \geq \exp(G/H) (D(H) - 1) + \eta(G/H),$$

one can sequentially extract at least $d = D(H)$ disjoint non-empty subsequences $S'_1, \dots, S'_d \mid S$ such that $\sigma(S'_i) \in H$ and $|S'_i| \leq \exp(G/H)$ for every $i \in \llbracket 1, d \rrbracket$ (see for instance [14, Lem. 5.7.10]). Since $T = \prod_{i=1}^d \sigma(S'_i)$ is a sequence over H of length $|T| = D(H)$, there exists a non-empty subset $I \subseteq \llbracket 1, d \rrbracket$ 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

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

which completes the proof. \square

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 $d_r = c_r - r$. \square

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

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 $r \geq 1$, we consider the groups defined by $L_n^r = L \oplus C_n^r$, where $n \geq 1$ is any integer such that $\exp(L) \mid n$. Note that if L is the trivial group, then $L_n^r \simeq C_n^r$ 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 $r \geq 1$, $D(L_n^r)$ 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 $L \simeq C_{n_1} \oplus \dots \oplus C_{n_\ell}$, with $1 < n_1 \mid \dots \mid n_\ell \in \mathbb{N}$, be a finite Abelian group. For every integer $n \geq 1$ such that $\exp(L) \mid n$ and every integer $r \geq 1$,*

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

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

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

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

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

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

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

which is the desired upper bound. \square

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

THEOREM 5. — *For every finite Abelian group L and every integer $r \geq 1$,*

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

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 $n \geq 1$ such that $\exp(L) \mid n$, one has $\gcd(n_i, P(n)) \leq n_i$ for all $i \in \llbracket 1, \ell \rrbracket$. Since $P(n)$ tends to infinity when n does so, the result follows easily from (1) and Theorem 4. \square

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 & C. POMERANCE — “There are infinitely many Carmichael numbers”, *Ann. of Math. (2)* **139** (1994), no. 3, p. 703–722.
- [2] N. ALON & M. DUBINER — “A lattice point problem and additive number theory”, *Combinatorica* **15** (1995), no. 3, p. 301–309.
- [3] N. ALON, S. FRIEDLAND & G. KALAI — “Regular subgraphs of almost regular graphs”, *J. Combin. Theory Ser. B* **37** (1984), no. 1, p. 79–91.
- [4] K. CZISZTER, M. DOMOKOS & 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., vol. 170, Springer, 2016, p. 43–95.
- [5] Y. EDEL, C. ELSHOLTZ, A. GEROLDINGER, S. KUBERTIN & L. RACKHAM — “Zero-sum problems in finite abelian groups and affine caps”, *Q. J. Math.* **58** (2007), no. 2, p. 159–186.
- [6] Y. EDEL, S. FERRET, I. LANDJEV & L. STORME — “The classification of the largest caps in $AG(5, 3)$ ”, *J. Combin. Theory Ser. A* **99** (2002), no. 1, p. 95–110.
- [7] J. S. ELLENBERG & D. GIJSWIJT — “On large subsets of \mathbb{F}_q^n with no three-term arithmetic progression”, *Ann. of Math. (2)* **185** (2017), no. 1, p. 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 & D. KRUYSWIJK — “A combinatorial problem on finite abelian groups. III”, Tech. Report ZW-008, Math. Centrum Amsterdam Afd. Zuivere Wisk., 1969.
- [10] W. GAO & A. GEROLDINGER — “Zero-sum problems and coverings by proper cosets”, *European J. Combin.* **24** (2003), no. 5, p. 531–549.
- [11] ———, “Zero-sum problems in finite abelian groups: a survey”, *Exposition. Math.* **24** (2006), no. 4, p. 337–369.
- [12] W. D. GAO, Q. H. HOU, W. A. SCHMID & R. THANGADURAI — “On short zero-sum subsequences. II”, *Integers* **7** (2007), article #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, Basel, 2009, p. 1–86.
- [14] A. GEROLDINGER & F. HALTER-KOCH — *Non-unique factorizations. Algebraic, combinatorial and analytic theory*, Pure and Applied Mathematics, vol. 278, Chapman & Hall/CRC, Boca Raton, FL, 2006.
- [15] A. GEROLDINGER, M. LIEBMAN & A. PHILIPP — “On the Davenport constant and on the structure of extremal zero-sum free sequences”, *Period. Math. Hungar.* **64** (2012), no. 2, p. 213–225.
- [16] A. GEROLDINGER & R. SCHNEIDER — “On Davenport’s constant”, *J. Combin. Theory Ser. A* **61** (1992), no. 1, p. 147–152.
- [17] H. HARBORTH — “Ein Extremalproblem für Gitterpunkte”, *J. reine angew. Math.* **262/263** (1973), p. 356–360.
- [18] J. KACZOROWSKI — “On the distribution of irreducible algebraic integers”, *Monatsh. Math.* **156** (2009), no. 1, p. 47–71.
- [19] M. MAZUR — “A note on the growth of Davenport’s constant”, *Manuscripta Math.* **74** (1992), no. 3, p. 229–235.
- [20] R. MESHULAM — “An uncertainty inequality and zero subsums”, *Discrete Math.* **84** (1990), no. 2, p. 197–200.

- [21] W. NARKIEWICZ – *Elementary and analytic theory of algebraic numbers*, third ed., Springer Monographs in Math., Springer-Verlag, Berlin, 2004.
- [22] J. E. OLSON – “A combinatorial problem on finite Abelian groups. I”, *J. Number Theory* **1** (1969), p. 8–10.
- [23] ———, “A combinatorial problem on finite Abelian groups. II”, *J. Number Theory* **1** (1969), p. 195–199.
- [24] G. PELLEGRINO – “The maximal order of the spherical cap in $S_{4,3}$ ”, *Matematiche* **25** (1971), p. 149–157.
- [25] A. POTECHIN – “Maximal caps in $AG(6, 3)$ ”, *Des. Codes Cryptogr.* **46** (2008), no. 3, p. 243–259.
- [26] K. ROGERS – “A combinatorial problem in Abelian groups”, *Math. Proc. Cambridge Philos. Soc.* **59** (1963), p. 559–562.

Manuscript received 20th February 2018

accepted 25th June 2018

BENJAMIN GIRARD, Sorbonne Université, Université Paris Diderot, CNRS, Institut de Mathématiques de Jussieu - Paris Rive Gauche, IMJ-PRG
F-75005, Paris, France
E-mail : benjamin.girard@imj-prg.fr
Url : <https://webusers.imj-prg.fr/~benjamin.girard/>