Benjamin Girard

An asymptotically tight bound for the Davenport constant

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

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/).
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 \( 1 < n_1 | \cdots | n_r \in \mathbb{N} \). 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 \( 1 \leq d | \exp(G) \), we denote by \( G_d \) the subgroup of \( G \) consisting of all elements of order dividing \( d \).

Any finite sequence \( S \) of \( \ell \) 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 \( \mathcal{O}_K \) of some number field \( K \) with ideal class group \( G \), the maximum number of prime ideals in the decomposition of an irreducible element of \( \mathcal{O}_K \) is \( D(G) \) [26]. The importance of this fact is best highlighted by the following generalization of the prime number theorem.
stating that the number \( F(x) \) of pairwise non-associated irreducible elements in \( O_K \) whose norms do not exceed \( x \) in absolute value satisfies,

\[
F(x) \sim C \frac{x}{\log x} (\log \log x)^{D(G)-1},
\]

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

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

The lower bound follows easily from the fact that if \( (e_1, \ldots, e_r) \) is a basis of \( G \) such that \( \text{ord}(e_i) = n_i \) 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, 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 \( C_r^n \). 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 \( n, r \geq 1 \),

\[ D(C_r^n) = r(n - 1) + 1. \]

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 \( D(C_2^n) \) 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 \( D(C_r^n) \) 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

\[
r(n - 1) + 1 \leq D(C_r^n) \leq n(1 + (r - 1) \log n), \tag{2}
\]

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 \( D(C_r^n) \) 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 \( r \geq 1 \),
\[
\mathcal{D}(C_n^r) \sim_{n \to +\infty} r n.
\]

The proof of Theorem 1 relies on a new upper bound for \( \mathcal{D}(C_n^r) \), 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 \( n \geq 1 \),
\[
\mathcal{D}(C_n^r) \leq r(n-1) + d_r \left( \frac{n}{P(n)} - 1 \right).
\]

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
\[
\mathcal{D}(C_n^r) - (r(n-1) + 1)
\]
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 \( \mathcal{D}(G) \leq \eta(G) \) for every finite Abelian group \( G \).

A natural construction shows that, for all integers \( n, r \geq 1 \), one has
\[
(2^r - 1)(n-1) + 1 \leq \eta(C_n^r).
\]
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 \( r \leq 2 \) [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 \( \eta(C_3^3) \) 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 \( n \geq 1 \),

\[
\eta(C_n^r) \leq c_r(n - 1) + 1.
\]

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 \( S_1, \ldots, S_d \mid S \) such that \( \sigma(S_1') \in H \) and \( |S_i'| \leq \exp(G/H) \) for every \( i \in [1,d] \) (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 \( I \subseteq [1,d] \) 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

\[
D(G) \leq \exp(G/H) (D(H) - 1) + \eta(G/H) \\
\leq \frac{n}{P(n)} (r(P(n) - 1)) + c_r\left(\frac{n}{P(n)} - 1\right) + 1 \\
= r(n - 1) + 1 + (c_r - r)\left(\frac{n}{P(n)} - 1\right),
\]

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 \( d_r = c_r - r \). □

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 \( r \geq 1 \), we consider the groups defined by \( L^r_n = L \oplus C^r_n \), where \( n \geq 1 \) is any integer such that \( \exp(L) | n \). 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 \( r \geq 1 \), \( D(L^r_n) \) 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 \( L \simeq C_{n_1} \oplus \cdots \oplus C_{n_r} \), with \( 1 < n_1 | \cdots | n_r \in \mathbb{N} \), be a finite Abelian group. For every integer \( n \geq 1 \) such that \( \exp(L) | n \) and every integer \( r \geq 1 \),

\[
D(L^r_n) \leq r(n - 1) + 1 + (c_{\ell+r} - r)\left(\frac{n}{P(n)} - 1\right) + \frac{n}{P(n)} \sum_{i=1}^{\ell} (\gcd(n, P(n)) - 1).
\]

**Proof of Theorem 4.** — We set \( G = L^r_n \) and \( H = G_{P(n)} \). On the one hand, since \( H \simeq C_{n_1}^{r_1} \oplus \cdots \oplus C_{n_{\ell}}^{r_\ell} \subseteq C_{P(n)} \), with \( n_i = \gcd(n_i, P(n)) \) | \( n_i \) for all \( i \in [1, \ell] \) and \( 1 \leq n_1 | \cdots | n_\ell \leq P(n) \), 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

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

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

\[
D(G) \leq \exp(G/H) (D(H) - 1) + \eta(G/H)
\]

\[
\leq \frac{n}{P(n)} \left(\sum_{i=1}^{\ell} (n_i - 1) + r(P(n) - 1)\right) + c_{\ell+r}\left(\frac{n}{P(n)} - 1\right) + 1
\]

\[
= r(n - 1) + 1 + (c_{\ell+r} - r)\left(\frac{n}{P(n)} - 1\right) + \frac{n}{P(n)} \sum_{i=1}^{\ell} (n_i - 1),
\]

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 \( r \geq 1 \),

\[
D(L^r_n) \underset{n \to +\infty}{\sim} \frac{rn}{\exp(L)|n}
\]

Proof of Theorem 5. — We write $L \simeq C_{n_1} \oplus \cdots \oplus C_{n_\ell}$, with $1 < n_1 | \cdots | n_\ell \in \mathbb{N}$. For every integer $n \geq 1$ such that $\exp(L) | n$, one has $\gcd(n_i, P(n)) \leq n_i$ 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


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
E-mail: benjamin.girard@imj-prg.fr
Url: https://webusers.imj-prg.fr/~benjamin.girard/