ACTA ARITHMETICA
171.3 (2015)

The Davenport constant of a box

by

Alain Plagne (Palaiseau) and Salvatore Tringali (Doha)

1. Introduction. Let G be an additively written abelian group. Given $X \subseteq G$, we denote by $\mathscr{F}(X)$ the free abelian monoid of G over X and write it multiplicatively. Therefore, the reader should be warned that x^a is meant in this article as the sequence where x is repeated a times; there will be no risk of confusion. We use $\mathscr{B}(X)$ for the abelian submonoid of $\mathscr{F}(X)$ of *zero-sum sequences over* X, containing all the non-empty words $x_1 \cdots x_n$ such that $x_i \in X$ for each index i and $\sum_{i=1}^{n} x_i = 0$ [13, Definition 3.4.1]. Note that the sequences considered here are unordered.

Let $\mathfrak{s} = x_1 \cdots x_n$ be a non-empty sequence in $\mathscr{B}(X)$. By abuse of notation, we shall say that the x_i's are elements of $\mathfrak{s}$ or, simply, are in $\mathfrak{s}$ (that is, we identify sequences and multisets). We say that $\mathfrak{s}$ is *minimal* if $\sum_{i \in I} x_i \neq 0$ for every non-empty proper subset I of $\{1, \ldots, n\}$. We call n the *length* of $\mathfrak{s}$, which we denote by $\|\mathfrak{s}\|$, and we use $\mathcal{A}(X)$ for the set of minimal zero-sum sequences of $\mathscr{B}(X)$; notice that $\mathcal{A}(X) = \mathcal{A}(G) \cap \mathscr{B}(X)$. For further notation and terminology, we refer the reader to [10, Section 2].

For G an abelian group, the study of $\mathscr{B}(G)$ and its combinatorial properties is part of what is called zero-sum theory, a subfield of additive theory with applications to group theory, graph theory, Ramsey theory, geometry and factorization theory (see the survey [10] and references therein). One of the earliest questions in this area, and maybe one of the most important, is concerned with the *Davenport constant*, named after the mathematician who, according to [19], popularized it during the 1960s, starting from a problem of factorization in algebraic number theory (see for instance [11] or [13]); notice however that this group invariant was already discussed in [21]. The Davenport constant has become the prototype of algebraic invariants of combinatorial flavour. Since the 1960s, the theory of these invariants has

2010 *Mathematics Subject Classification*: Primary 11B75; Secondary 11B30, 11P70.
Key words and phrases: additive combinatorics, Davenport constant, inverse theorem, minimal zero-sum sequence.

DOI: 10.4064/aa171-3-1

developed in several directions (see for instance the survey article [10] or [13, Chapters 5–7]).

Given a finite abelian group G, it turns out that any long enough sequence of elements in it contains a zero-sum subsequence. More generally, the Davenport constant of an abelian group G, denoted by $\mathsf{D}(G)$, is defined as the smallest integer n such that each sequence over G of length at least n has a non-empty zero-sum subsequence. Equivalently, $\mathsf{D}(G)$ is the maximal length of a minimal zero-sum sequence over G, i.e. the maximal length of a sequence of elements of G summing to 0 and with no proper subsequence summing to 0. If G is decomposed, as is always possible if $G \neq \{0\}$, as a direct sum of cyclic groups $G \cong C_{n_1} \oplus \cdots \oplus C_{n_r}$ with integers $1 < n_1 \mid \cdots \mid n_r$ (here, C_k denotes a cyclic group with k elements, r is the rank of G, and $n_r = \exp G$, the exponent of G), an immediate lower bound for the Davenport constant is

$$\mathsf{D}(G) \geq 1 + \sum_{i=1}^{r} (n_i - 1); \tag{1}$$

to see this, notice that the sequence containing, for each $i = 1, \ldots, r$, one generator of the cyclic component C_{n_i} repeated $n_i - 1$ times, has no non-empty zero-sum subsequence. It is known that for groups of rank at most two and for p-groups (with p a prime), (1) is in fact an equality, as proved independently in [8] and [19, 20]. In particular, if G is cyclic then

$$\mathsf{D}(G) = |G|, \tag{2}$$

and this is characteristic of cyclic groups, as follows immediately for instance from (3) below. For groups of rank at least four, equality is definitely not the rule (see [1, 8, 14]). In the case of groups of rank three, it has been conjectured that equality holds again, but this conjecture is wide open (see [10]), and seemingly difficult. Concerning upper bounds, the best general result is the following:

$$\mathsf{D}(G) \leq \left(1 + \log \frac{|G|}{\exp G}\right) \exp G, \tag{3}$$

which is proved in [9, 18]. We do not know really more than this in general: In spite of so much work related to the Davenport constant over the years, its actual value has been determined only for a few additional families of groups beyond the ones for which it was already known by the end of the 1960s. The general impression is that, although it has a very simple definition, computing the Davenport constant of an abelian group (of rank at least three) is a challenging problem.

Be that as it may, it turns out that generalizing the question to a broader setting makes sense and can be useful. In particular, for any subset X of an abelian group G we may define its Davenport constant, which we denote by $\mathsf{D}(X)$, as the largest integer n for which there exists a minimal zero-sum sequence in $\mathscr{B}(X)$ of length n; this variant was first introduced by van Emde Boas [8], where it is however denoted by $\mu(G, X)$. It is trivial but worth remarking that in general, and in contrast to the case where $X = G$, it can happen that $\mathsf{D}(X)$ is finite and yet we can build arbitrarily long sequences with no non-empty proper zero-sum subsequence. Also, it is immediate that $\mathsf{D}(X) \le \mathsf{D}(G)$: this inequality is in general strict and it is well possible that $\mathsf{D}(X)$ is finite while $\mathsf{D}(G)$ is not.

The study of such a generalization of the Davenport constant to subsets of abelian groups, is of great interest for its applications to factorization theory, an area which is currently expanding from the classical setting of (mostly commutative) rings to the context of modules. Indeed, if H is a Krull monoid with class group G and if $X \subseteq G$ is the set of classes containing prime divisors, then the Davenport constant $\mathsf{D}(X)$ is a crucial invariant describing the arithmetic of H (see [13, Chapter 3.4] and [12]). It turns out that the study of direct-sum decompositions in module theory gives rise to Krull monoids with class groups which are precisely a power of the additive group $\mathbb{Z}$ of the integers. For this reason, Baeth and Geroldinger, in the final section of their recent paper [2], ask specifically, as part of a larger research programme, to study the Davenport constant of what we call a box, that is, a product of intervals of integers.

The main goal of the present paper is, in fact, to derive bounds and exact formulas for $\mathsf{D}(X)$ in the case when X is a subset of a power of the additive group $\mathbb{Z}$ of the integers; in particular, we mostly investigate the case of X being a box. Inverse results, describing the structure of the sequences of maximal or almost maximal length, are also presented, along with hybrid results involving the product of a group and a box.

2. New results. The first part of our study is concerned with the case of the integers; interesting results in this direction have recently been obtained by Sissokho [23]. As usual, we let the *diameter* of a set $X \subseteq \mathbb{Z}$ be given by

$$\operatorname{diam}(X) = \sup_{x,y \in X} |x - y|$$

and we denote, in all what follows, by χ the function defined, for all subsets S of $\mathbb{Z}$ containing both positive and negative elements, by the formula

$$\chi(S) = \sup_{x,y \in S \text{ with } xy<0} \frac{|x| + |y|}{\gcd(x, y)}.$$

Our first result can then be stated as follows.

THEOREM 1. *Let X be a non-empty set of integers. Then:*

(i) *if* $X \subseteq \mathbb{N} \setminus \{0\}$ *then* $\mathsf{D}(X) = 0$,
(ii) *if* $0 \in X \subseteq \mathbb{N}$ *then* $\mathsf{D}(X) = 1$,
(iii) *if X contains both positive and negative integers, then* $\chi(X) \le \mathsf{D}(X) \le \operatorname{diam}(X)$.

Since there are sets X for which $\chi(X) = \operatorname{diam}(X)$ (consider, e.g., the interval $[\![-m, M]\!]$, where m and M are coprime positive integers, or apply Corollary 1), point (iii) is in general sharp. We recall that, if a and b are real numbers with $a \le b$, then $[a, b]$ denotes the interval $\{x \in \mathbb{R} : a \le x \le b\}$, while we write $[\![a, b]\!]$ for the set $[a, b] \cap \mathbb{Z}$.

On the other hand, as will follow from our forthcoming results, there are sets X such that $\mathsf{D}(X) < \operatorname{diam}(X)$ (see, for instance, Corollary 2), and W. Schmid provided us with an example for which $\chi(X) < \mathsf{D}(X)$. Lastly, we have the following corollary (immediate from Theorem 1) in the case that X is an interval around zero.

COROLLARY 1. *Let m and M be positive integers. Then*

$$\frac{m+M}{\gcd(m,M)} \le \mathsf{D}([\![-m, M]\!]) \le m + M.$$

In particular, if m and M are coprime, then

$$\mathsf{D}([\![-m, M]\!]) = m + M.$$

From this first corollary, one can immediately deduce the value of the Davenport constant of a symmetrical interval around zero.

COROLLARY 2. *We have* $\mathsf{D}([\![-1, 1]\!]) = 2$ *and, for any integer* $m \ge 2$, $\mathsf{D}([\![-m, m]\!]) = 2m - 1$.

Moreover, the following asymptotic estimate holds.

COROLLARY 3. *For positive integers m and M, one has*

$$\mathsf{D}([\![-m, M]\!]) = M + m + o(\min(m, M)) \quad \text{as } \min(m, M) \to \infty.$$

It will be transparent from the proof that, in Corollary 3, we can replace the error term $o(\min(m, M))$ with an explicit power (slightly larger than $1/2$) of $\min(m, M)$.

In fact, Corollary 2 appears (in an alternative but equivalent form) as part of the main theorem in [22], where the focus is mainly on pairs (A, B) of non-empty subsets of *positive* integers, therein referred to as irreducible pairs, such that $\sum_{a \in A} a = \sum_{b \in B} b$ and $\sum_{a \in A'} a \neq \sum_{b \in B'} b$ for any other pair (A', B') of non-empty sets $A' \subsetneq A$ and $B' \subsetneq B$.

In the present paper, we shall adopt a strategy which looks quite different, both in spirit and in practice. In particular, the proof of Corollary 2 comes very quickly as a consequence of a technical lemma (essentially, Lemma 5(i) of Section 3) of general interest and which we reuse to go a step further.

Having a direct theorem at hand, we are naturally led to its inverse counterpart. The first result we obtain in this direction is concerned with the structure of minimal zero-sum sequences of maximal length in an interval.

THEOREM 2. *Let* m *and* M *be positive integers and let* $\mathfrak{s} = x_1 \cdots x_{m+M}$ *be a sequence of length* $m + M$ *in* $\mathscr{B}([\![-m, M]\!])$. *Then,* $\mathfrak{s}$ *is minimal if and only if* $\gcd(m, M) = 1$ *and* $\mathfrak{s} = M^m \cdot (-m)^M$.

This in turn leads to the following corollary.

COROLLARY 4. *Let* $m \geq 2$ *be an integer and let* $\mathfrak{s} = x_1 \cdots x_{2m-1}$ *be a sequence of length* $2m - 1$ *in* $\mathscr{B}([\![-m, m]\!])$. *Then* $\mathfrak{s}$ *is minimal if and only if* $\mathfrak{s} = m^{m-1} \cdot (-(m-1))^m$ *or* $\mathfrak{s} = (-m)^{m-1} \cdot (m-1)^m$.

Our next theorem is a more elaborate inverse result which reads as follows.

THEOREM 3. *Let* m *be an integer,* $m \geq 3$, *and let* $\mathfrak{s} = x_1 \cdots x_{2m-2}$ *be a sequence of length* $2m - 2$ *in* $\mathscr{B}([\![-m, m]\!])$. *Then* $\mathfrak{s}$ *is minimal if and only if one of the following holds:*

(i) m *is odd and either* $\mathfrak{s} = m^{m-2} \cdot (-m+2)^m$ *or* $\mathfrak{s} = (-m)^{m-2} \cdot (m-2)^m$;
(ii) $\mathfrak{s} = m^{m-2} \cdot (-(m-1))^{m-1} \cdot 1$ *or* $\mathfrak{s} = (-m)^{m-2} \cdot (m-1)^{m-1} \cdot (-1)$.

The next theorem is a partial generalization of the upper bound in Corollary 2 to higher dimensions. It will follow from the connection, already noticed in [7], of the Davenport constant with the Steinitz constant [24] and a generalization of it obtained in [6].

THEOREM 4. *Let* $m_1, \ldots, m_d$ *be positive integers. Then*

$$\mathsf{D}([\![-m_1, m_1]\!] \times \cdots \times [\![-m_d, m_d]\!]) \leq \prod_{i=1}^{d} (2(d + 1/d - 1)m_i + 1).$$

Our next result is concerned with the special case of hypercubes. We shall need a Kronecker-type notation (defined on positive integers m):

$$\delta_m = \begin{cases} 1 & \text{if } m = 1, \\ 0 & \text{otherwise.} \end{cases}$$

We obtain the following bounds.

THEOREM 5. *One has*

(i) $\mathsf{D}([\![-1, 1]\!]^2) = 4$,
(ii) *for any integer* $m \geq 2$,

$$(2m - 1)^2 \leq \mathsf{D}([\![-m, m]\!]^2) \leq (2m + 1)(4m + 1),$$

(iii) *if d is an integer, $d \geq 3$, and m is a positive integer, then*

$$(2m - 1 + \delta_m)^d \leq \mathsf{D}(\llbracket -m, m \rrbracket^d) \leq (2(d + 1/d - 1)m + 1)^d.$$

The lower bounds in this theorem are obtained thanks to direct constructions, while the upper bounds follow immediately from Theorem 4. Theorem 5 being proved, the general impression, supported by the special cases of the dimension $d = 1$ and the square $\llbracket -1, 1 \rrbracket^2$, is that the true size of $\mathsf{D}(\llbracket -m, m \rrbracket^d)$ is closer to the lower bound than to the upper bound.

We notice that in [3] the authors consider the case

$$X = \llbracket 0, 1 \rrbracket^d \cup \llbracket -1, 0 \rrbracket^d \setminus \{0^d\}$$

where 0^d is the origin in $\mathbb{R}^d$, and they prove a result that is reminiscent of our Theorem 5(iii) (see [3, Theorem 3.13]). Loosely speaking, they obtain the bounds

$$\left(\frac{1+\sqrt{5}}{2}\right)^d \leq \mathsf{D}(X) \leq (d+2)^{(d+2)/2}. \tag{4}$$

Although X is not a hypercube, as we consider here, we may still force the (somewhat unnatural) direct application of the upper bound of Theorem 5 (our lower bound gives nothing in this case), which implies for this case that $\mathsf{D}(X) \leq \mathsf{D}(\llbracket -1, 1 \rrbracket^d) \leq (2d + 2/d - 1)^d$ and is definitely worse than (4), but still of the same "type". It would be interesting to check if our method could be efficiently adapted to this special case.

We notice that Theorem 5 is enough to ensure that, for fixed d, the quantity $\mathsf{D}(\llbracket -m, m \rrbracket^d)$ grows like m^d. But it is not clear that a constant a_d should exist so that

$$\mathsf{D}(\llbracket -m, m \rrbracket^d) \sim a_d m^d \quad \text{as } m \to \infty.$$

However, if such a constant exists it must satisfy $2^d \leq a_d \leq (2\,(d + 1/d - 1))^d$.

Based on the above, we are led to ask whether, m and d being as in the statement of Theorem 5, the Davenport constant of the hypercube $\llbracket -m, m \rrbracket^d$ is equal to the dth power of the Davenport constant of $\llbracket -m, m \rrbracket$. Should this be true, it would suggest that some suitable assumptions could imply a sort of multiplicativity of Davenport constants for certain classes of sets. Our two last theorems and their corollary go more generally in this direction. The first of these theorems is a submultiplicativity result.

Theorem 6. *Let G and H be two abelian groups. If G is finite and X is a finite subset of H, then*

$$\mathsf{D}(G \times X) \leq \mathsf{D}(G)\mathsf{D}(X).$$

The final theorem shows a supermultiplicativity property, not with respect to the Davenport constants themselves but rather with respect to the lower bounds offered by Theorem 5. Indeed, we shall build long minimal zero-sum sequences on the basis of those already built for each component.

THEOREM 7. *Let m and d be positive integers and let G be a cyclic group. Then*

$$\mathsf{D}(G \times [\![-m, m]\!]^d) \geq \mathsf{D}(G)(2m - 1 + \delta_m)^d.$$

In general, both theorems are sharp, as shown by our final corollary which follows immediately from Theorems 6 and 7 and Corollary 2.

COROLLARY 5. *Let m be a positive integer and let G be a cyclic group. Then*

$$\mathsf{D}(G \times [\![-m, m]\!]) = \mathsf{D}(G)\mathsf{D}([\![-m, m]\!]).$$

The plan of the paper is as follows. In Section 3, we establish a few lemmas of general interest and which will be useful in the other parts of the article. In Section 4, we prove Theorem 1 and Corollaries 2 and 3. Section 5 contains the proofs of the inverse results, namely Theorem 2 and its Corollary 4 and of Theorem 3. Finally the proofs of Theorems 4 and 5 are presented in Section 6, while Section 7 contains the proofs of our final Theorems 6 and 7.

3. Preliminary lemmas. In this section, we collect a few lemmas that will be used later to prove our main results. We start with the following elementary lemma, the proof of which is immediate (and hence omitted).

LEMMA 1. *Let $\mathfrak{s} = x_1 \cdots x_n$ be a non-empty minimal zero-sum sequence in an abelian group G. Then:*

(i) *the sequence $-\mathfrak{s} = (-x_1) \cdots (-x_n)$ is itself a non-empty minimal zero-sum sequence in G,*
(ii) $0 \in \mathfrak{s}$ *if and only if* $n = 1$,
(iii) *the elements x and $-x$ are both in $\mathfrak{s}$ for some $x \in G \setminus \{0\}$ if and only if $n = 2$.*

The next lemma gives some elementary properties of the function D. It turns out that it is an even and non-decreasing function. As is usual, we shall denote

$$-X = \{-x : x \in X\}.$$

LEMMA 2. *Let G be an abelian group. If $X \subseteq Y \subseteq G$, then $\mathsf{D}(X) \leq \mathsf{D}(Y)$ and $\mathsf{D}(-X) = \mathsf{D}(X)$. Moreover, $\mathsf{D}([\![-m, m]\!]) = \mathsf{D}([\![-(m-1), m]\!])$ for every integer $m \geq 2$.*

Proof. The first inequality is immediate. The second relation follows from Lemma 1(i). As for the third, the first inequality implies $\mathsf{D}([\![-m, m]\!]) \geq \mathsf{D}([\![-(m-1), m]\!])$. Now, we notice that for $m \geq 2$, $\mathsf{D}([\![-m, m]\!]) > 2$ since the sequence $-m \cdot 1^m \in \mathcal{A}([\![-m, m]\!])$ has length $m + 1 \geq 3$. It follows by

Lemma 1(iii) that a minimal zero-sum sequence in $[\![-m, m]\!]$ cannot contain both m and $-m$, and therefore, up to symmetry, is included in $[\![-m+1, m]\!]$. This proves the third assertion of the lemma. ∎

Our methods heavily rely on considering partial sums of terms of the sequences we study. The following lemma is the first result of a series in this direction.

LEMMA 3. *Let $\mathfrak{s} = x_1 \cdots x_n$ be a non-empty minimal zero-sum sequence in an abelian group G. Then, for any permutation σ of $[\![1, n]\!]$ and all $i, j \in [\![1, n]\!]$, we have $\sum_{l=1}^{i} x_{\sigma(l)} \neq \sum_{l=1}^{j} x_{\sigma(l)}$ if and only if $i \neq j$.*

Proof. Suppose the result is false: there exist a permutation σ of $[\![1, n]\!]$ and distinct indices $i, j \in [\![1, n]\!]$ such that $\sum_{l=1}^{i} x_{\sigma(l)} = \sum_{l=1}^{j} x_{\sigma(l)}$. By symmetry, we can assume $i < j$. Then the non-empty sum $\sum_{l=i+1}^{j} x_{\sigma(l)}$ is 0, that is, $x_{\sigma(i+1)} \cdots x_{\sigma(j)}$ is a proper non-empty zero-sum subsequence of $\mathfrak{s}$, which is impossible by the minimality of $\mathfrak{s}$. ∎

Here is a useful companion result to the preceding lemma.

LEMMA 4. *Let $\mathfrak{s} = x_1 \cdots x_n$ be a non-empty minimal zero-sum sequence of length $n \geq 3$ in an abelian group G. Then, for any permutation σ of $[\![1, n]\!]$ and any index $i \in [\![1, n]\!] \setminus \{2\}$, the value of $\sum_{l=1}^{i} x_{\sigma(l)}$ is different from $x_{\sigma(1)} + x_{\sigma(3)}$.*

Proof. If $x_{\sigma(1)} = x_{\sigma(1)} + x_{\sigma(3)}$, then $x_{\sigma(3)} = 0$, a contradiction by Lemma 1(ii) since $n > 1$—this solves the case $i = 1$; while, if for some $i \geq 3$,

$$\sum_{l=1}^{i} x_{\sigma(l)} = x_{\sigma(1)} + x_{\sigma(3)},$$

then

$$x_{\sigma(2)} + \sum_{l=4}^{i} x_{\sigma(l)} = 0$$

(if $i = 3$, the sum on l on the left-hand side is empty), which contradicts the minimality of $\mathfrak{s}$. ∎

The preceding two lemmas will be used in the form of the following counting lemma which will be key in several proofs.

LEMMA 5. *Let $\mathfrak{s} = x_1 \cdots x_n$ be a non-empty minimal zero-sum sequence in an abelian group G. Assume that there exist a set X and a permutation σ of $[\![1, n]\!]$ such that for any $i \in [\![1, n]\!]$, the partial sum $\sum_{l=1}^{i} x_{\sigma(l)}$ belongs to X. Then*

(i) $n \leq |X|$,

(ii) *if we assume additionally that $n \geq 3$, $x_{\sigma(1)} \neq x_{\sigma(3)}$ and $x_{\sigma(1)} + x_{\sigma(3)}$ is in X, then $n \leq |X| - 1$.*

Proof. By Lemma 3, all the partial sums $\sum_{l=1}^{i} x_{\sigma(l)}$ $(1 \le i \le n)$ must be pairwise distinct. Since, by assumption, all these elements belong to X, this implies $n \le |X|$.

If $n \ge 3$, we may additionally apply Lemma 4. Since, by assumption, $x_{\sigma(2)} \ne x_{\sigma(3)}$, we see that for $i \in [\![1, n]\!]$, the partial sums $\sum_{l=1}^{i} x_{\sigma(l)}$ are pairwise distinct and different from $x_{\sigma(1)} + x_{\sigma(3)}$. We obtain

$$\Big|\Big\{ \sum_{l=1}^{i} x_{\sigma(l)} : 1 \le i \le n \Big\} \cup \{x_{\sigma(1)} + x_{\sigma(3)}\}\Big| = n + 1.$$

Since all the $n+1$ elements appearing on the left-hand side of this equality are in X, the result follows. ∎

A classical consequence of Lemma 5 is the well-known fact that if G is a finite abelian group, then $\mathsf{D}(G) \le |G|$ (this bound is sharp, as is seen in (2)).

Now we introduce a technical definition. We shall say that a triple $(\mathfrak{s}, k, \sigma)$ is *nyctalopic* if $\mathfrak{s} = x_1 \cdots x_n$ is a minimal zero-sum sequence of $\mathscr{B}(\mathbb{Z})$ of length $n \ge 2$, k is an integer in the range $1 \le k \le n$, and σ is an injective function defined on $[\![1, k]\!]$ and taking its values in $[\![1, n]\!]$ such that for any $i \in [\![2, k]\!]$,

$$x_{\sigma(i)} \sum_{l=1}^{i-1} x_{\sigma(l)} < 0.$$

When $k = n$, if there is no risk of confusion (that is, the $\mathfrak{s}$ involved is clear from the context), we will simply say that σ is a nyctalopic permutation.

Nyctalopic triples $(\mathfrak{s}, k, \sigma)$ have nice properties which justify their introduction. The following lemma of an algorithmic nature will be very useful in what follows.

LEMMA 6. *Let X be a finite subset of $\mathbb{Z}$. Let $\mathfrak{s} = x_1 \cdots x_n$ be a minimal zero-sum sequence in $\mathscr{B}(X)$ of length $n \ge 2$. Let k be an integer, $1 \le k \le n$, and σ be an injective function defined on $[\![1, k]\!]$ and taking its values in $[\![1, n]\!]$ such that the triple $(\mathfrak{s}, k, \sigma)$ is nyctalopic. Then one can extend σ to a nyctalopic permutation of $[\![1, n]\!]$.*

Proof. We proceed by induction. By assumption, $(\mathfrak{s}, k, \sigma)$ is nyctalopic.

Assume now that for some integer $i \in [\![k, n-1]\!]$, σ has been extended so that the values of $\sigma(k+1), \ldots, \sigma(i)$ are determined in such a way that $(\mathfrak{s}, i, \sigma)$ is nyctalopic. It is immediate to check that

$$\sum_{l=1}^{i} x_{\sigma(l)} \ne 0$$

since otherwise $\mathfrak{s}$ would not be a minimal zero-sum sequence in view of $i < n$. Since $\mathfrak{s}$ sums to zero, there should be an integer $j \notin \{\sigma(l) : 1 \le l \le i\}$ such that the sign of x_j is opposite to the one of $\sum_{l=1}^{i} x_{\sigma(l)}$. We fix one such j arbitrarily. Then we extend σ by defining

$$\sigma(i+1) = j$$

so that, by construction, $(\mathfrak{s}, i+1, \sigma)$ is nyctalopic. ∎

Here is the central property of nyctalopic triples we use in what follows.

LEMMA 7. *Let $\mathfrak{s}$ be a minimal zero-sum sequence in $\mathscr{B}(X)$ of length $n \geq 2$. Let σ be a nyctalopic permutation of $[\![1, n]\!]$. Then, for any $i \in [\![1, n]\!]$,*

$$\min X \leq \sum_{l=1}^{i} x_{\sigma(l)} \leq \max X.$$

Moreover, if $x_{\sigma(1)} \neq \max X$, the inequality on the right is strict, while if $x_{\sigma(1)} \neq \min X$, the inequality on the left is strict.

Proof. Notice first that $n \geq 2$ implies $\min X < 0 < \max X$, as follows from Theorem 1(i) & (ii).

The assertion of Lemma 7 is proved by induction, the lemma being trivial for $i = 1$. Suppose it is true for some $i \in [\![1, n-1]\!]$, we thus have

$$\min X \leq \sum_{l=1}^{i} x_{\sigma(l)} \leq \max X.$$

By minimality, this sum is also non-zero since $i < n$. Suppose that $\sum_{l=1}^{i} x_{\sigma(l)} > 0$. Then by nyctalopia, $x_{\sigma(i+1)} < 0$, that is, $\min X \leq x_{\sigma(i+1)} \leq -1$, and thus

$$\min X < 1 + \min X \leq \sum_{l=1}^{i} x_{\sigma(l)} + x_{\sigma(i+1)} \leq \max X - 1 < \max X.$$

The case $\sum_{l=1}^{i} x_{\sigma(l)} < 0$ is treated in a symmetric way. ∎

4. Proof of Theorem 1 and its corollaries. We start with a lemma.

LEMMA 8. *Let x and y be integers such that $xy < 0$ and let $X = \{x, y\}$. Then:*

(i) *the set $\mathcal{A}(X)$ has a unique element, $\mathfrak{x} = x^a \cdot y^b$ with $a = |y|/\gcd(x, y)$ and $b = |x|/\gcd(x, y)$,*
(ii) *$\mathscr{B}(X) = \{\mathfrak{x}^j : j \in \mathbb{N}\}$.*

Proof. By definition, the sequence $x^a \cdot y^b$ is in $\mathscr{B}(X)$ if and only if $ax + by = 0$, that is, $a|x| = b|y|$. This equality can be rewritten as

$$a\frac{|x|}{\gcd(x, y)} = b\frac{|y|}{\gcd(x, y)}.$$

But $|x|/\gcd(x,y)$ and $|y|/\gcd(x,y)$ are coprime, therefore the Gauss lemma gives the existence of a non-negative integer h such that $b = h|x|/\gcd(x,y)$ and $a = h|y|/\gcd(x,y)$. This proves (ii).

Among these sequences, only the one corresponding to $h = 1$ is minimal (and divides those for $h \geq 1$) and (i) follows. ∎

Here is the very proof of the theorem.

Proof of Theorem 1. Points (i) and (ii) are immediate. We thus turn directly to (iii).

In order to prove $\chi(X) \leq \mathsf{D}(X)$, we consider, for all $x, y \in X$ with $xy < 0$, the sequence $\mathfrak{s} = x^a \cdot y^b$ where

$$a = \frac{|y|}{\gcd(x,y)} \quad \text{and} \quad b = \frac{|x|}{\gcd(x,y)}.$$

By Lemma 8(i), this is a minimal zero-sum sequence. Consequently,

$$\frac{|x| + |y|}{\gcd(x,y)} = \|\mathfrak{s}\| \leq \mathsf{D}(G),$$

and hence the result, on taking the supremum on the left-hand side.

On the other hand, the upper bound $\mathsf{D}(X) \leq \operatorname{diam}(X)$ is trivial if $|X| = \infty$. So assume that X is finite, and let $m = -\min X$ and $M = \max X$. If $\mathfrak{s} = x_1 \cdots x_n \in \mathcal{A}(X)$, then $\|\mathfrak{s}\| \geq \chi(X) \geq 2$ by the inequality we just proved. Define $\sigma(1) = 1$. Lemma 6 implies that we can extend σ to a nyctalopic permutation of $[\![1, n]\!]$. Lemma 7 then implies that all the partial sums $x_{\sigma(1)} + \cdots + x_{\sigma(i)}$ (for $1 \leq i \leq n$) belong to either $[\![-m, M-1]\!]$ or $[\![-(m-1), M]\!]$, with the result that $n \leq M + m = \chi(X)$, in view of Lemma 5(i). ∎

We conclude this section with the proof of the two corollaries to Theorem 1.

Proof of Corollary 2. By Corollary 1, the claim is trivial if $m = 1$, while Lemma 2 and Corollary 1 give

$$\mathsf{D}([\![-m, m]\!]) = \mathsf{D}([\![-(m-1), m]\!]) = 2m - 1$$

for $m \geq 2$ since in this case $\gcd(m-1, m) = 1$. ∎

For the proof of Corollary 3, we shall need the symbol $[x]$ for the integral part of a real number x.

Proof of Corollary 3. Since Hoheisel [15], we have known that for some $\vartheta < 1$, when x is large enough, there is always a prime p_x in the real open interval $(x - x^\vartheta, x)$. One can even take $\vartheta = 0.525$ (see [4]).

Assume $\min(m, M) = m$ (the other case is analogous). Applying Hoheisel's result, we find a prime p in $[\![m - [m^\vartheta], m]\!]$. Since p cannot divide

M and $M-1$ at the same time, there must exist $\eta = 0$ or 1 such that $\gcd(M-\eta, p) = 1$. We infer

$$\begin{aligned} p + M - 1 \le p + M - \eta = \frac{p + M - \eta}{\gcd(p, M - \eta)} &\le \mathsf{D}(\llbracket -p, M - \eta \rrbracket) \\ &\le \mathsf{D}(\llbracket -m, M \rrbracket) \le m + M, \end{aligned}$$

where we have used the coprimality of p and $M-\eta$, Corollary 1 and the non-decreasingness of D given by Lemma 2. The result follows since

$$p + M - 1 = m + M + O(m^{\vartheta} + 1) = m + M + o(m). \ \blacksquare$$

5. Proofs of the inverse theorems and their corollaries

Proof of Theorem 2. Sufficiency follows from Lemma 8(i). We now investigate necessity.

Suppose that $\mathfrak{s}$ contains an element x_i different from both $-m$ and M. Define $\sigma(1) = i$ and apply Lemma 6 in order to extend σ to a nyctalopic permutation. By Lemma 7, the partial sums $x_{\sigma(1)} + \cdots + x_{\sigma(j)}$ all belong to $\llbracket -(m-1), M-1 \rrbracket$. This in turn implies $\|\mathfrak{s}\| \le M + m - 1$ by Lemma 5(i), which is a contradiction.

It follows that $\mathfrak{s}$ is of the form $(-m)^a \cdot M^b$ for some positive integers a and b, that is, $\mathfrak{s} \in \mathscr{B}(\{-m, M\})$. By Lemma 8(i), the minimality of $\mathfrak{s}$ implies

$$a = \frac{M}{\gcd(M, m)} \quad \text{and} \quad b = \frac{m}{\gcd(M, m)}.$$

From the assumption and this, we deduce that

$$M + m = \|\mathfrak{s}\| = a + b = \frac{M + m}{\gcd(M, m)},$$

and $\gcd(M, m) = 1$ follows. $\blacksquare$

The proof of its corollary is now easy.

Proof of Corollary 4. By Lemma 1(iii), since $2m-1 > 2$, $\mathfrak{s}$ cannot contain both m and $-m$. Assume that $\mathfrak{s}$ does not contain $-m$; then it belongs to $\mathscr{B}(\llbracket -(m-1), m \rrbracket)$ and we apply Theorem 2, which gives the result. The case where $\mathfrak{s}$ does not contain m is analogous. $\blacksquare$

We now come to the second inverse result. It turns out that its proof is far more intricate than the preceding one.

Proof of Theorem 3. In this proof, we will distinguish two cases (cases (i) and (ii)), the first one being very simple. The second case will use two internal lemmas (Lemmas 9 and 10 below).

Since $\mathsf{D}(\llbracket -(m-1), m-1 \rrbracket) = 2m - 3$ by Corollary 2, we can assume by symmetry and Lemma 1(iii) that $m \in \mathfrak{s}$ and $-m \notin \mathfrak{s}$. In other words $\mathfrak{s} \in \mathscr{B}(\llbracket -(m-1), m \rrbracket)$.

We distinguish two cases, the first one being almost immediate.

(i) If $-(m-1) \notin \mathfrak{s}$, then $\mathfrak{s} \in \mathscr{B}([\![-(m-2), m]\!])$. It follows from Theorem 2 that $\mathfrak{s}$ is the sequence $m^{m-2} \cdot (-(m-2))^m$ and $\gcd(m-2, m) = 1$, i.e. m is odd.

(ii) If $-(m-1) \in \mathfrak{s}$, then Lemma 1(iii) implies that $m-1 \notin \mathfrak{s}$. Up to reordering the elements of $\mathfrak{s}$, we may therefore assume from now on that

$$x_1 = m \quad \text{and} \quad x_2 = -(m-1).$$

LEMMA 9. *If, for some $i \in [\![3, n]\!]$, x_i is negative then $x_i = -(m-1)$.*

Proof. Suppose the lemma is false and let $i \geq 3$ be such that $-(m-1) < x_i \leq -1$. We consider the function σ defined on $[\![1, 3]\!]$ by

$$\sigma(1) = 1, \quad \sigma(2) = 2, \quad \sigma(3) = i.$$

The triple $(\mathfrak{s}, 3, \sigma)$ is nyctalopic. We apply Lemma 6 to $(\mathfrak{s}, 3, \sigma)$ to extend σ to a nyctalopic permutation of $[\![1, n]\!]$. We then apply Lemma 7. We infer that all the partial sums $\sum_{l=1}^{j} x_{\sigma(l)}$ $(1 \leq j \leq n)$ belong to $[\![-(m-2), m]\!]$.

But in fact even the following more precise statement is true:

$$\sum_{l=1}^{j} x_{\sigma(l)} \in [\![-(m-3), m]\!]. \tag{5}$$

This is the case when $j = 1$ or 2 and, indeed, if for some $j \geq 3$ one has $\sum_{l=1}^{j} x_{\sigma(l)} = -(m-2)$, then by definition of nyctalopia the sum $\sum_{l=1}^{j-1} x_{\sigma(l)}$ is either $< -(m-2)$ or positive. Since the first alternative is impossible (all the partial sums are at least $-(m-2)$), we have $\sum_{l=1}^{j-1} x_{\sigma(l)} \geq 1$. It follows that

$$x_{\sigma(j)} = \sum_{l=1}^{j} x_{\sigma(l)} - \sum_{l=1}^{j-1} x_{\sigma(l)} \leq -(m-2) - 1 = -(m-1).$$

The only possibility is that $x_{\sigma(j)} = -(m-1)$ and

$$\sum_{l=1}^{j-1} x_{\sigma(l)} = 1 = x_{\sigma(1)} + x_{\sigma(2)}.$$

By Lemma 3, this implies that we must have $j - 1 = 2$ and thus $x_{\sigma(j)} = x_{\sigma(3)} = x_i$, a contradiction since by assumption $x_i \neq -(m-1)$. Assertion (5) is proved.

Since all partial sums in (5) are distinct, included in $[\![-(m-3), m]\!]$ and different from $x_{\sigma(1)} + x_{\sigma(3)} = m + x_i \in [\![1, m-1]\!]$, by Lemma 5(ii), we obtain $n \leq 2m - 3$, a contradiction. ∎

Now that we know how negative elements look like, we study the positive ones.

We notice that there must exist in $\mathfrak{s}$ a positive element different from m, otherwise $\mathfrak{s}$ would be of the form $m^u \cdot (-(m-1))^v$ for some positive integers u and v and, by Lemma 8(i), we would get $u = m-1$ and $v = m$, and finally

$$2m-2 = \|\mathfrak{s}\| = u + v = (m-1) + m = 2m-1,$$

a contradiction.

Up to reordering the elements in the sequence, we may thus assume that

$$x_3 \in [\![1, m-2]\!].$$

Lemma 10. *The following hold:*

(i) $x_3 = 1$,
(ii) *if for some* $i \in [\![1, n]\!] \setminus \{3\}$, x_i *is positive, then it is equal to* m.

Proof. We consider σ such that

$$\sigma(1) = 3, \quad \sigma(2) = 2, \quad \sigma(3) = 1.$$

The triple $(\mathfrak{s}, 3, \sigma)$ is easily seen to be nyctalopic. We apply Lemma 6 to $(\mathfrak{s}, 3, \sigma)$ to extend σ to a nyctalopic permutation of $[\![1, n]\!]$. We then apply Lemma 7. We infer that all the partial sums $\sum_{l=1}^{j} x_{\sigma(l)}$ belong to $[\![-(m-2), m-1]\!]$. Since this set has cardinality $2m-2$, one must have precisely

$$\left\{ \sum_{l=1}^{j} x_{\sigma(l)} : j = 1, \ldots, 2m-3 \right\} = [\![-(m-2), m-1]\!] \setminus \{0\}. \tag{6}$$

We consider the function f defined on $[\![1, n]\!]$ by $f(j) = \sum_{l=1}^{j} x_{\sigma(l)}$. One has $f(1) = x_i > 0$, $f(2) = x_i + 1 - m < 0$, $f(3) = x_i + 1 > 0$. More generally, if $f(k) > 0$, by nyctalopia one must have $x_{\sigma(k+1)} < 0$ and thus, by Lemma 9, $x_{\sigma(k+1)} = -(m-1)$, which implies $f(k+1) = f(k) - (m-1) \le 0$, where equality can only happen for $k+1 = n$. Suppose now that the signs of the $f(k)$'s do not alternate when $k \in [\![1, n-1]\!]$; then we must have

$$|\{1 \le k \le 2m-3 : f(k) < 0\}| > |\{1 \le k \le 2m-3 : f(k) > 0\}|,$$

which is impossible in view of (6). Thus the signs alternate and we have

$$f(1), f(3), \ldots, f(2m-3) > 0, \qquad f(2), f(4), \ldots, f(2m-4) < 0.$$

We now prove, by induction, that $x_{\sigma(2m-2j-1)} = m$ for any $j \in [\![1, m-2]\!]$.

Indeed, $f(2m-2) = 0$ and $f(2m-3) > 0$, thus $x_{\sigma(2m-2)} < 0$ and so, by Lemma 9, $x_{\sigma(2m-2)} = -(m-1)$. It follows that $f(2m-3) = m-1$. But by the alternation of signs, $f(2m-4) < 0$, which implies $x_{\sigma(2m-3)} = f(2m-3) - f(2m-4) \ge m$ and therefore $x_{\sigma(2m-3)} = m$. This proves the statement for $j = 1$.

Assume now that for some $k \in [\![1, m-1]\!]$, the statement is proved for any $j \in [\![1, k]\!]$. It follows immediately that

$$\begin{array}{llll} f(2m-3) = m-1, & f(2m-5) = m-2, & \ldots, & f(2m-2k-1) = m-k, \\ f(2m-4) = -1, & f(2m-6) = -2, & \ldots, & f(2m-2k-2) = -k. \end{array}$$

Since $f(2m-2k-2) = -k < 0$, by the alternation of signs we must have $f(2m-2k-3) > 0$, which implies first that $x_{\sigma(2m-2k-2)} < 0$ and thus $x_{\sigma(2m-2k-2)} = -(m-1)$. Finally we find that

$$f(2m-2k-3) = f(2m-2k-2) - x_{\sigma(2m-2k-2)} = -k + (m-1) = m-(k+1).$$

Since, again by the alternation of signs, $f(2m-2k-4) < 0$, we have $x_{\sigma(2m-2k-3)} > 0$ and so

$$f(2m-2k-4) = f(2m-2k-3) - x_{\sigma(2m-2k-3)} \geq (m-(k+1)) - m = -(k+1).$$

Since, by Lemma 3, f never takes the same value twice, $f(2m-2k-4) \neq f(2m-4), f(2m-6), \ldots, f(2m-2k-2)$, that is, $f(2m-2k-4) \neq -1, -2, \ldots, -k$. This implies finally that $f(2m-2k-4) = -(k+1)$ and thus $x_{\sigma(2m-2k-3)} = m$, as required to conclude the induction.

Using the statement just proved and the explicit description of the first values of σ, we obtain statement (ii) of the lemma.

By summing all the elements in the zero-sum sequence $\mathfrak{s}$, thanks to the descriptive Lemma 9 and what we just proved we obtain

$$0 = x_3 + (m-2)m + (m-1)(-m+1) = x_3 - 1,$$

thus $x_3 = 1$ and (i) is proved. ■

We are now ready to conclude the proof of Theorem 3. One checks the minimality of the sequence $\mathfrak{s} = m^{m-2} \cdot (-(m-1))^{m-1} \cdot 1$, by noticing that, should this be false, $\mathcal{A}(\{-(m-1), m\})$ would contain a subsequence of $\mathfrak{s}$, which cannot be the case by Lemma 8(i). ■

6. Proofs of Theorems 4 and 5. To ease the reading, these proofs are decomposed into elementary components. Subsection 6.1 contains the proof of all the upper bounds, in particular the full proof of Theorem 4, its application to Theorem 5(iii) and the special improvement given in Theorem 5(ii). Subsection 6.2 contains the proof of Theorem 5(i). Finally, Subsection 6.3 contains the proof of the general lower bounds of Theorem 5(ii) & (iii) (case $m \geq 2$) and Subsection 6.4 contains the special case $m = 1$ of Theorem 5(iii).

6.1. Proof of Theorem 4 and of the upper bounds in Theorem 5. We start from an old question of Riemann and Lévy. This was investigated by Lévy [17] himself more than a century ago, but it was Steinitz [24] who gave the first complete proof of the following result (see [16, Remark 2.1.2]).

THEOREM 8. *Let d be a positive integer and B the closed unit ball relative to a norm $\|\cdot\|$ on $\mathbb{R}^d$. Then there exists a constant $c \in \mathbb{R}^+$ such that whenever $u_1, \ldots, u_n \in B$ and $u_1 + \cdots + u_n = 0$, there is a permutation π of the interval $[\![1, n]\!]$ such that $\|u_{\pi(1)} + \cdots + u_{\pi(i)}\| \leq c$ for each $i \in [\![1, n]\!]$.*

In this statement, we used the notation $\alpha \cdot B$ for the α-dilate of B,

$$\alpha \cdot B = \{\alpha u : u \in B\}.$$

We let the *Steinitz constant relative to* $\|\cdot\|$ be the infimum of all the constants $c \in \mathbb{R}^+$ that can be taken in Theorem 8. In particular, if $\|\cdot\|_\infty$ is the supremum norm on $\mathbb{R}^d$, that is,

$$\|(x_1, \ldots, x_d)\|_\infty = \max_{1 \leq i \leq d} |x_i|$$

for all $x_1, \ldots, x_d \in \mathbb{R}$, then we denote the corresponding Steinitz constant by C_d. It is known (see [5, Remark 3]) that

$$C_d \leq d + 1/d - 1. \tag{7}$$

Remarkably, upper estimates of C_d immediately yield upper bounds on the Davenport constant. This is the content of Theorem 4, which we prove now.

Proof of Theorem 4. Consider a sequence $\mathfrak{s} \in \mathscr{B}(X)$ and write $\mathfrak{s} = u_1 \cdots u_n$, let $u_i = (u_{i,1}, \ldots, u_{i,d})$ and set

$$v_i = (u_{i,1}/m_1, \ldots, u_{i,d}/m_d)$$

for each $1 \leq i \leq n$, so that $\|v_i\|_\infty \leq 1$ and $v_1 + \cdots + v_n = 0$. It follows that there exists a permutation π of $[\![1, n]\!]$ such that $v_{\pi(1)} + \cdots + v_{\pi(i)}$ belongs to the box $C_d \cdot B$ where B is the closed unit ball for $\|\cdot\|_\infty$, that is, the hypercube $[-1, 1]^d$. This implies that all the sums $u_{\pi(1)} + \cdots + u_{\pi(i)}$ are lattice points of $C_d \cdot X$. But the total number of lattice points in $C_d \cdot X = [-C_d m_1, C_d m_1] \times \cdots \times [-C_d m_d, C_d m_d]$ is

$$\prod_{i=1}^{d} (2[C_d m_i] + 1) \leq \prod_{i=1}^{d} (2C_d m_i + 1),$$

which finally yields, together with Lemma 5(i),

$$\mathsf{D}(X) \leq \prod_{i=1}^{d} (2C_d m_i + 1). \blacksquare$$

The general upper bound of Theorem 5 (the one valid for any integral $d \geq 3$) follows immediately from this lemma applied to $m_1 = \cdots = m_d$ and (7).

To prove the particular case $d = 2$ (the upper bound in Theorem 5(ii)), we slightly refine this reasoning using a result from [6] valid in 2-dimensional spaces, which is a variation on Steinitz' theme. The main theorem of Banaszczyk's paper [6] asserts that if a and b are two real numbers satisfying $a, b \geq 1$ and $a+b \geq 3$, then the following holds: if $u_1, \dots, u_n \in B$ (B is again the unit ball relative to the supremum norm) and $u_1 + \dots + u_n = 0$, there is a permutation π of $[\![1, n]\!]$ such that $u_{\pi(1)} + \dots + u_{\pi(i)} \in [-a, a] \times [-b, b]$. Following the same lines as in the preceding proof, this implies, choosing $a = 1$, $b = 2$ in this result, that starting from a sequence in $[\![-m_1, m_1]\!] \times [\![-m_2, m_2]\!]$, we may reorder the elements so that the partial sums stay in the rectangle $[\![-m_1, m_1]\!] \times [\![-2m_2, 2m_2]\!]$. As above, it follows that

$$\mathsf{D}([\![-m_1, m_1]\!] \times [\![-m_2, m_2]\!]) \leq (2m_1 + 1)(4m_2 + 1),$$

which concludes the proof.

6.2. Proof of Theorem 5(i): the case $d = 2$, $m = 1$. This subsection is devoted to the proof that $\mathsf{D}([\![-1, 1]\!]^2) = 4$.

We look at the sequence $\mathfrak{t} = (1, -1) \cdot (1, 1) \cdot (-1, 0)^2$. It is easily seen that $\mathfrak{t}$ is a minimal zero-sum sequence.

Suppose we want to construct a minimal zero-sum sequence of size $n > 2$ as large as possible; then such a sequence $\mathfrak{s}$ can contain at most four distinct elements (by Lemma 1(ii) & (iii), $(0, 0)$ is not in the sequence and there is at most one point on each line containing $(0, 0)$), and in particular two among $(1, 0), (0, 1), (-1, 0), (0, -1)$, without loss of generality, $(1, 0)$ and $(0, 1)$. The point $(-1, -1)$ must be in $\mathfrak{s}$, otherwise the other two points are $(1, 1)$ and up to symmetry $(1, -1)$, say, but then all the four points have a non-negative first coordinate, leading to a contradiction. Thus $(-1, -1)$ is in $\mathfrak{s}$. We finally choose as the fourth point, again without loss of generality by symmetry, $(1, -1)$. Write $\mathfrak{s} = (1, 0)^a \cdot (0, 1)^b \cdot (-1, -1)^c \cdot (1, -1)^d$ where a, b, c and d are non-negative integers. This sequence has zero sum if and only if $a - c + d = 0$ and $b - c - d = 0$, thus $\mathfrak{s}$ is of the form $(1, 0)^{c-d} \cdot (0, 1)^{c+d} \cdot (-1, -1)^c \cdot (1, -1)^d$ and $c \geq d$.

If $c > d$, then in particular, $c > 0$, which implies that $(1, 0) \cdot (0, 1) \cdot (-1, -1)$ is a zero-sum subsequence of $\mathfrak{s}$, which implies, by minimality of $\mathfrak{s}$, that $\mathfrak{s} = (1, 0) \cdot (0, 1) \cdot (-1, -1)$ and $n = 3$. If $c = d$, then $\mathfrak{s} = (0, 1)^{2c} \cdot (-1, -1)^c \cdot (1, -1)^c = ((0, 1)^2 \cdot (-1, -1) \cdot (1, -1))^c$, and the minimality of $\mathfrak{s}$ implies $c = 1$ and $n = 4$. The result is proved.

6.3. Proof of Theorem 5(ii) & (iii): the lower bound for $m \geq 2$. In this subsection m is a fixed integer satisfying $m \geq 2$.

We consider the following sequence of zero-sum sequences defined inductively. We let

$$\mathfrak{s}_1 = m^{m-1} \cdot (-(m-1))^m.$$

By Corollary 4, $\mathfrak{s}_1$ belongs to $\mathcal{A}([\![-m, m]\!])$ and it has length $\|\mathfrak{s}_1\| = 2m - 1$. Suppose we have already defined a minimal zero-sum sequence $\mathfrak{s}_d$ in

$\mathscr{B}(\llbracket -m,m\rrbracket^d)$ of size $\|\mathfrak{s}_d\| = (2m-1)^d$. Write $\mathfrak{s}_d = x_1 \cdots x_n$ where $n = (2m-1)^d$. We define

$$\mathfrak{s}_{d+1} = (x_1,m)^{m-1} \cdots (x_n,m)^{m-1} \cdot (0,-(m-1))^{mn}. \tag{8}$$

It is immediate that $\mathfrak{s}_{d+1} \in \mathscr{B}(\llbracket -m,m\rrbracket^{d+1})$ and

$$\|\mathfrak{s}_{d+1}\| = n(m-1) + mn = (2m-1)\|\mathfrak{s}_d\| = (2m-1)^{d+1}.$$

This inductive argument implies that, for any positive integer d,

$$\|\mathfrak{s}_d\| = (2m-1)^d. \tag{9}$$

We start with a basic property of this sequence which will be used in Section 7.

LEMMA 11. *For any positive integer d, the sequence $\mathfrak{s}_d$ can be written as*

$$\mathfrak{s}_d = u_1^{\alpha_1} \cdots u_{d+1}^{\alpha_{d+1}}$$

where the u_j $(1 \le j \le d+1)$ are distinct elements of $\llbracket -m,m\rrbracket^d$, the α_j $(1 \le j \le d+1)$ are positive integers and

$$\gcd(\alpha_1,\ldots,\alpha_{d+1}) = 1.$$

Proof. The proof is again by induction. For $d=1$, we have $\mathfrak{s}_1 = m^{m-1} \cdot (-(m-1))^m$ and we observe that $\mathfrak{s}_1$ contains two distinct elements repeated $\alpha_1 = m$ and $\alpha_2 = m-1$ times respectively. It is immediate that $\gcd(m,m-1) = 1$ and the result is proved.

Suppose the result is proved for some integer $d \ge 1$, that is, $\mathfrak{s}_d = u_1^{\beta_1} \cdots u_{d+1}^{\beta_{d+1}}$ for some distinct $u_j \in \llbracket -m,m\rrbracket^d$ and some positive integers β_j (for $1 \le j \le d+1$). A look at (8), taking into account (9), shows immediately that

$$\mathfrak{s}_{d+1} = (u_1,m)^{(m-1)\beta_1} \cdots (u_{d+1},m)^{(m-1)\beta_{d+1}} \cdot (0,-(m-1))^{m(2m-1)^d},$$

and we observe that if we write $(u_j,m) = v_j$ for $1 \le j \le d+1$ and $v_{d+2} = (0,-(m-1))$, then the v_j's are distinct. Moreover, writing $\alpha_j = (m-1)\beta_j$ for $1 \le j \le d+1$ and $\alpha_{d+2} = m(2m-1)^d$, one obtains

$$\mathfrak{s}_{d+1} = v_1^{\alpha_1} \cdots v_{d+2}^{\alpha_{d+2}}.$$

But

$$\begin{aligned}\gcd(\alpha_1,\ldots,\alpha_{d+2}) &= \gcd\big((m-1)\beta_1,\ldots,(m-1)\beta_{d+1}, m(2m-1)^d\big)\\ &= \gcd(\beta_1,\ldots,\beta_{d+1}, m(2m-1)^d)\end{aligned}$$

since $\gcd(m-1, m(2m-1)^d) = 1$. But using the induction hypothesis, we have

$$\gcd(\beta_1,\ldots,\beta_{d+1}, m(2m-1)^d) \mid \gcd(\beta_1,\ldots,\beta_{d+1}) = 1,$$

and finally $\gcd(\alpha_1,\ldots,\alpha_{d+2}) = 1$. ■

The following lemma is central for our purpose.

LEMMA 12. *For any two integers $d, u \geq 1$, the non-empty zero-sum subsequences of $\mathfrak{s}_d^u$ are exactly the sequences $\mathfrak{s}_d^j$ for $1 \leq j \leq u$.*

Proof. Again, this is proved by induction. For $d = 1$, we consider

$$\mathfrak{s}_1^u = m^{(m-1)u} \cdot (-(m-1))^{mu} \in \mathscr{B}(\{-(m-1), m\}).$$

Thus any subsequence $\mathfrak{t}$ of $\mathfrak{s}_1$ must belong to $\mathscr{B}(\{-(m-1), m\})$ and, in view of Lemma 8(ii), has to be of the form $\mathfrak{t} = \mathfrak{s}_1^j$ for some non-negative integer j.

Assume the result is true for some integer $d \geq 1$, and let $\mathfrak{t}$ be a zero-sum subsequence of

$$\mathfrak{s}_{d+1}^u = (x_1, m)^{(m-1)u} \cdots (x_n, m)^{(m-1)u} \cdot (0, -(m-1))^{mnu}$$

if we denote $\mathfrak{s}_d = x_1 \cdots x_n$. By considering the sequence obtained from $\mathfrak{t}$ by projection on the first d coordinates, which is nothing but the sequence $\mathfrak{s}_d^{(m-1)u}$ (up to the zeroes obtained from the projection of the elements $(0, -(m-1))^{mnu}$), and applying the induction hypothesis, we find that $\mathfrak{t}$ must contain each element (x_i, m) the same number of times, say j. It follows that $\mathfrak{t}$ is of the form

$$\mathfrak{t} = (x_1, m)^k \cdots (x_n, m)^k \cdot (0, -(m-1))^l$$

for some positive integers k and l. Summing over the last coordinate yields $knm = l(m-1)$. But, by (9), $n = \|\mathfrak{s}_k\| = (2m-1)^d$, which gives

$$k(2m-1)^d m = l(m-1),$$

from which it follows that $m-1$ divides k in view of $\gcd(m-1, m) = \gcd(m-1, 2m-1) = 1$. It follows that

$$k = j(m-1) \quad \text{and} \quad l = j(2m-1)^d m = jnm$$

for some integer $j \geq 1$. In other words, $\mathfrak{t} = \mathfrak{s}_{d+1}^j$, which was to be proved to complete the induction step. ∎

Applying the preceding lemma in the special case $u = 1$, we obtain the following result.

COROLLARY 6. *For any integer $d \geq 1$, $\mathfrak{s}_d$ is a minimal zero-sum sequence in $[\![-m, m]\!]^d$.*

The lower bounds in Theorem 5(ii) & (iii) (case $m \geq 2$) now follow from this corollary and (9).

6.4. Proof of Theorem 5(iii): the lower bound for $m = 1$. If $m = 1$, the construction will be slightly different but of the same type. We could have adapted the argument of the preceding subsection; however, we can be more direct since an explicit description of $\mathfrak{s}_d$ is possible.

We define $d+1$ elements of $[\![-1,1]\!]^d$ by

$$e_1 = (1,1,\dots,1), \quad e_2 = (-1,1,\dots,1), \quad e_3 = (0,-1,1,\dots,1), \ \dots, \\ e_d = (0,\dots,0,-1,1), \quad e_{d+1} = (0,\dots,0,-1).$$

In other words, for $1 \le k \le d+1$, the vector e_k has its $\min(k-2,0)$ first coordinates equal to 0, the $\min(k-1,0)$th equal to -1 and the kth to the $(d+1)$th equal to 1. We consider the sequence

$$\mathfrak{s}_d = e_1 \cdot e_2 \cdot e_3^2 \cdot e_4^4 \cdots e_d^{2^{d-2}} \cdot e_{d+1}^{2^{d-1}},$$

such that $\mathfrak{s}_d \in \mathscr{B}([\![-1,1]\!]^d)$ and $\|\mathfrak{s}_d\| = 2^d$.

It remains to prove that this sequence is minimal. Let $\mathfrak{t}$ be a non-empty zero-sum subsequence of $\mathfrak{s}_d$. Let j be the minimal index $(1 \le j \le d+1)$ such that there is at least one element in the sequence having a non-zero jth coordinate. If $j > 1$, then any element in $\mathfrak{t}$ is one of the e_k's for $k \ge j+1$ but then all the elements of the sequence have a non-positive jth coordinate, and at least one has a strictly negative one. Thus $\mathfrak{t}$ cannot be a zero-sum sequence. It follows that $j = 1$ and $\mathfrak{t}$ must contain either e_1 and e_2, and thus both, by looking at the first coordinate.

We now prove by induction that, for $k \ge 2$, $\mathfrak{t}$ must contain each e_k with multiplicity 2^{k-2}. We have just proved it for $k = 2$. Suppose this is true for some $k < d+1$; then considering the $(k+1)$th coordinate of the sum of $\mathfrak{t}$, we find that the multiplicity of e_{k+1} must be equal to

$$1 + 1 + 2 + \cdots + 2^{k-2} = 2^{k-1}.$$

This completes the induction step and finally the proof that $\mathfrak{t} = \mathfrak{s}_d$.

Thus $\mathfrak{s}_d$ is minimal, and since $\|\mathfrak{s}_d\| = 2^d$, the lower bound of Theorem 5(iii) is proved for $m = 1$.

7. Proofs of Theorems 6 and 7

Proof of Theorem 6. Take a sequence $\mathfrak{s} \in \mathscr{B}(G \times X)$ of length larger than or equal to $\mathsf{D}(G)\mathsf{D}(X) + 1$. Since this is larger than $\mathsf{D}(X)$, we may extract a subsequence $\mathfrak{s}_1$ which sums minimally to zero on the second component. By definition of an element of $\mathcal{A}(X)$, it has length at most $\mathsf{D}(X)$. Removing this subsequence from $\mathfrak{s}$, we get a new sequence, denoted $\mathfrak{s} \cdot \mathfrak{s}_1^{-1}$, and we have

$$\|\mathfrak{s} \cdot \mathfrak{s}_1^{-1}\| \ge \mathsf{D}(G)\mathsf{D}(X) + 1 - \mathsf{D}(X) = (\mathsf{D}(G) - 1)\mathsf{D}(X) + 1.$$

While $\mathfrak{s} \cdot \mathfrak{s}_1^{-1}$ does not a priori belong to $\mathscr{B}(G \times X)$ ($\mathfrak{s}_1$ may have a non-zero sum on its first component), it sums to zero on the second component. We can therefore continue this process and build recursively sequences $\mathfrak{s}_2, \dots, \mathfrak{s}_l$ whose projections on the second component belong to $\mathcal{A}(X)$. Since $\|\mathfrak{s}_j\| \le \mathsf{D}(X)$ for each $j \ge 1$, the process can continue as long as $l \le \mathsf{D}(G)$. Thus, we can assume that we have built $l = \mathsf{D}(G)$ distinct subsequences of $\mathfrak{s}$, namely $\mathfrak{s}_1, \dots, \mathfrak{s}_l$, each summing to zero on the second component. For each $j \in [\![1, l]\!]$, we denote by $g_j \in G$ the sum of the sequence $\mathfrak{s}_j$ on the first component. Notice that $\mathfrak{s} \cdot \mathfrak{s}_1^{-1} \dots \mathfrak{s}_l^{-1}$ is non-empty since

$$\|\mathfrak{s} \cdot \mathfrak{s}_1^{-1} \dots \mathfrak{s}_l^{-1}\| = \|\mathfrak{s}\| - (\|\mathfrak{s}_1\| + \dots + \|\mathfrak{s}_l\|) \geq \mathsf{D}(G)\mathsf{D}(X) + 1 - l\mathsf{D}(X) = 1.$$

Applying the definition of the Davenport constant of G to $\mathfrak{t} = g_1 \cdots g_l$ (notice that a priori it is not a zero-sum sequence in G), we can extract from $\mathfrak{t}$ a subsequence $g_{i_1} \cdots g_{i_q}$, for some $q \leq l$ and $1 \leq i_1 < \dots < i_q \leq l$, which sums to 0 in G. Finally, we consider $\mathfrak{s}' = \mathfrak{s}_{i_1} \cdots \mathfrak{s}_{i_q}$. It is a proper subsequence of $\mathfrak{s}$ and we check immediately that

$$\sum_{x \in \mathfrak{s}'} x = \sum_{j=1}^{q} \sum_{x \in \mathfrak{s}_{i_j}} x = \sum_{j=1}^{q} (g_{i_j}, 0) = 0,$$

which proves that $\mathfrak{s}$ cannot be minimal, and so $\mathsf{D}(G \times X) \leq \mathsf{D}(G)\mathsf{D}(X)$. ∎

Proof of Theorem 7. Let $n = |G|$ and g be a generator of G.

If $m \geq 2$, we use the sequence $\mathfrak{s}_d$ introduced in Subsection 6.3. In view of Lemma 11, we can write it in the form

$$\mathfrak{s}_d = u_1^{\alpha_1} \cdots u_{d+1}^{\alpha_{d+1}}$$

with distinct $u_j \in [\![-m, m]\!]^d$ and positive integers α_j (for $1 \leq j \leq d+1$). We also have

$$\gcd(\alpha_1, \dots, \alpha_{d+1}) = 1,$$

which implies by Bézout's theorem that we can find integers $w_1, \dots, w_{d+1}$ such that

$$\alpha_1 w_1 + \dots + \alpha_{d+1} w_{d+1} = 1. \tag{10}$$

We finally define

$$\mathfrak{t} = (w_1 g, u_1)^{n\alpha_1} \cdots (w_{d+1} g, u_{d+1})^{n\alpha_{d+1}}.$$

From (10) and $\mathfrak{s}_d \in \mathscr{B}([\![-m, m]\!]^d)$, it is immediate to check that

$$\sum_{x \in \mathfrak{t}} x = \sum_{j=1}^{d+1} \alpha_j n (w_j g, u_j) = \Big(ng, n \sum_{j=1}^{d+1} \alpha_j u_j\Big) = (0, 0).$$

Thus $\mathfrak{t} \in \mathscr{B}(G \times [\![-m, m]\!]^d)$.

Let us show that $\mathfrak{t}$ is minimal. Select a non-empty zero-sum subsequence of $\mathfrak{t}$, say $\mathfrak{u}$. By Lemma 12 applied to the second component, which is nothing but $\mathfrak{s}_d^n$, we observe that

$$\mathfrak{u} = (w_1 g, u_1)^{q\alpha_1} \cdots (w_{d+1} g, u_{d+1})^{q\alpha_{d+1}}$$

for some positive integer $q \leq n$. By summing $\mathfrak{u}$, we get, again from (10) and

$\mathfrak{s}_d \in \mathscr{B}(\llbracket -m, m \rrbracket^d)$,

$$\sum_{x \in \mathfrak{u}} x = \Big(q\Big(\sum_{j=1}^{d+1} \alpha_j w_j\Big) g, q \sum_{j=1}^{d+1} \alpha_j u_j\Big) = (qg, 0),$$

which can be zero only for q a multiple of $|G| = n$, g being a generator. Thus $q = n$. It follows that $\mathfrak{t} \in \mathcal{A}(G \times \llbracket -m, m \rrbracket^d)$.

The theorem now follows from $\|\mathfrak{t}\| = n\|\mathfrak{s}_d\| = (2m-1)^d \mathsf{D}(G)$.

If $m = 1$, the same proof applies in an analogous way. This is even simpler since we can take all but one (namely, w_1) of the w_j's equal to zero in view of $\alpha_1 = 1$. ∎

Acknowledgements. The authors are indebted to Alfred Geroldinger for having raised a question that motivated this paper. The second author is also grateful to Eric Balandraud and Benjamin Girard for useful discussions.

This research is supported by the ANR Project CAESAR No. ANR-12-BS01-0011.

References

[1] P. C. Baayen and P. van Emde Boas, *Een structuurconstante bepaald voor $C_2 \oplus C_2 \oplus C_2 \oplus C_2 \oplus C_6$*, Math. Centrum Amsterdam WZ 27 (1969), 6 pp.

[2] N. R. Baeth and A. Geroldinger, *Monoids of modules and arithmetic of direct-sum decompositions*, Pacific J. Math. 271 (2014), 257–319.

[3] N. R. Baeth, A. Geroldinger, D. J. Grynkiewicz and D. Smertnig, *A semigroup-theoretical view of direct-sum decompositions and associated combinatorial problems*, J. Algebra Appl. 14 (2015), 1550016, 60 pp.

[4] R. C. Baker, G. Harman and J. Pintz, *The difference between consecutive primes, II*, Proc. London Math. Soc. 83 (2001), 532–562.

[5] W. Banaszczyk, *The Steinitz constant of the plane*, J. Reine Angew. Math. 373 (1987), 218–220.

[6] W. Banaszczyk, *The Steinitz lemma in l_∞^2*, Period. Math. Hungar. 22 (1991), 183–186.

[7] P. Diaconis, R. L. Graham and B. Sturmfels, *Primitive partition identities*, in: D. Miklós et al. (eds.), Combinatorics, Paul Erdős is Eighty, Vol. 2, János Bolyai Math. Soc., Budapest, 1996, 173–192.

[8] P. van Emde Boas, *A combinatorial problem on finite abelian groups II*, Mathematisch Centrum Amsterdam ZW 1969-007 (1969), 60 pp.

[9] P. van Emde Boas and D. Kruyswijk, *A combinatorial problem on finite abelian groups III*, Math. Centrum Amsterdam ZW 1969-008 (1969), 34 pp.

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

[11] A. Geroldinger, *Additive group theory and non-unique factorizations*, in: Combinatorial Number Theory and Additive Group Theory, Adv. Courses Math. CRM Barcelona, Birkhäuser, 2009, 1–86.

[12] A. Geroldinger, D. J. Grynkiewicz, G. J. Schaeffer and W. A. Schmid, *On the arithmetic of Krull monoids with infinite cyclic class groups*, J. Pure Appl. Algebra 214 (2010), 2219–2250.

[13] A. Geroldinger and F. Halter-Koch, *Non-Unique Factorizations: Algebraic, Combinatorial and Analytic Theory*, Pure Appl. Math. 278, Chapman & Hall/CRC, 2006.

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

[15] G. Hoheisel, *Primzahlprobleme in der Analysis*, Sitz. Preuss. Akad. Wiss. 1930, 580–588.

[16] M. I. Kadets and V. M. Kadets, *Series in Banach Spaces: Conditional and Unconditional Convergence*, Oper. Theory Adv. Appl. 94, Birkhäuser, 1997.

[17] P. Lévy, *Sur les séries semi-convergentes*, Nouv. Ann. de Math. 64 (1905), 506–511.

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

[19] J. E. Olson, *A combinatorial problem on finite Abelian groups I*, J. Number Theory 1 (1969), 8–10.

[20] J. E. Olson, *A combinatorial problem on finite Abelian groups II*, J. Number Theory 1 (1969), 195–199.

[21] K. Rogers, *A combinatorial problem in Abelian groups*, Proc. Cambridge Philos. Soc. 59 (1963), 559–562.

[22] M. L. Sahs, P. A. Sissokho and J. N. Torf, *A zero-sum theorem over* $\mathbb{Z}$, Integers 13 (2013), #A71.

[23] P. A. Sissokho, *A note on minimal zero-sum sequences over* $\mathbb{Z}$, Acta Arith. 166 (2014), 279–288.

[24] E. Steinitz, *Bedingt konvergente Reihen und konvexe Systeme*, J. Reine Angew. Math. 143 (1913), 128–176.

Alain Plagne
Centre de mathématiques Laurent Schwartz
École polytechnique
91128 Palaiseau Cedex, France
E-mail: plagne@math.polytechnique.fr

Salvatore Tringali
Science Program
Texas A&M University at Qatar
Education City
PO Box 23874, Doha, Qatar
E-mail: salvo.tringali@gmail.com
URL: http://www.math.polytechnique.fr/~tringali/

Received on 12.2.2015
and in revised form on 25.8.2015 (8082)