The Davenport constant of a box

Salvatore Tringali
(based on joint work with Alain Plagne: arXiv:1405.4363)

Séminaire Caesar – Sep 18, 2014

Centre de mathématiques Laurent Schwartz, $\mathfrak{X}$ - Palaiseau, Sep 18, 2014

Unordered sequences

Given a set X, we let X^* be the "abelian Kleene star" of X and by $\mathscr{F}(X) = (X^*, \cdot)$ the free *abelian* monoid over X, which we write multiplicatively (we use ε for the identity)

We think of a non-empty word in X^* as an *unordered sequence* and we write it as $x_1 \cdots x_n$ (if there is no ambiguity)

We have a (monoid) homomorphism $\|\cdot\| : \mathscr{F}(X) \to (\mathbf{N}, +)$ given by $\|\varepsilon\| := 0$ and $\|\mathfrak{s}\| := n$ for $\mathfrak{s} = x_1 \cdots x_n \in X^* \setminus \{\varepsilon\}$

For $\mathfrak{s} \in X^*$ we refer to $\|\mathfrak{s}\|$ as the length of $\mathfrak{s}$

Zero-sum sequences with support in a set

Let $\mathbb{G} = (G, +)$ be an additively written abelian group and assume $X \subseteq G$

The function $\pi : X^* \to G$ taking ε to 0 and a non-empty sequence $x_1 \cdots x_n$ to $x_1 + \cdots + x_n$ is then a (monoid) homomorphism $\mathscr{F}(X) \to \mathbb{G}$

> We use $\mathscr{B}(X)$ for the kernel of π, and we refer to the elements of $\mathscr{B}(X)$ as the *zero-sum sequences* (shortly, ZSSs) *of* $\mathbb{G}$ *with support in* X

A non-empty sequence $x_1 \cdots x_n \in X^*$ belongs to $\mathscr{B}(X)$ iff $\sum_{i=1}^{n} x_i = 0$

Minimal zero-sum sequences

A non-empty sequence $\mathfrak{s} = x_1 \cdot \cdots \cdot x_n \in \mathscr{B}(X)$ is called *minimal* if there does not exist any non-empty set $I \subsetneq \{1, \ldots, n\}$ s.t. $\sum_{i \in I} x_i = 0$

The set of all minimal ZSSs of $\mathbb{G}$ with support in X will be denoted by $\mathcal{A}(X)$: this is the set of atoms of $\mathscr{B}(X)$ regarded as a submonoid of $\mathscr{F}(X)$

[If $\mathbb{M} = (M, \cdot)$ is a multiplicatively written monoid, an element $a \in M$ is an atom of $\mathbb{M}$ if $a \notin \mathbb{M}^\times$ and $a = bc$ for some $b, c \in M$ implies $b \in \mathbb{M}^\times$ or $c \in \mathbb{M}^\times$]

We define the *Davenport constant* of $\mathbb{G}$ relative to X, here denoted by $\mathsf{D}(X)$, as the sup of $\|\mathfrak{a}\|$ for $\mathfrak{a} \in \mathcal{A}(X)$

In particular, we refer to $\mathsf{D}(G)$ as the Davenport constant of $\mathbb{G}$

Goals and motivations

> Compute or estimate $\mathsf{D}(X)$ in the case when $\mathbb{G} \cong \mathbb{H} \times (\mathbf{Z}, +)^d$, with $d \in \mathbf{N}^+$ and $\mathbb{H} = (H, +)$ a finite abelian group, and X is a *box* (or rectangle), viz. a set of the form $X_0 \times X_1 \times \cdots \times X_d$, with $X_0 \subseteq H$ and $X_i = [\![-m_i, M_i]\!]$ for some $m_i, M_i \in \mathbf{N}$

When $\mathbb{H}$ is trivial, this is motivated by the study of direct-sum decompositions in module theory and fits into a research from outlined in the final section of:

N. R. Baeth and A. Geroldinger
Monoids of modules and arithmetic of direct-sum decompositions
Pacific J. Math., to appear (arXiv:1401.6553)

More in general, $\mathsf{D}(\cdot)$ is a crucial invariant describing the arithmetic of certain monoids arising from the study of non-unique factorization in the ring of integers of a number field

What we did...

We derive

(i) elementary (upper and lower) bounds on $\mathrm{D}(X)$ when $\mathbb{G} = (\mathbf{Z}, +)$ along with an asymptotic bound in the special case when $X = [\![-m, M]\!]$ for some $m, M \in \mathbf{N}$

(ii) an explicit description of the ZSSs of $\mathscr{B}([\![-m, m]\!])$ of maximal (i.e., $2m-1$) or almost maximal (i.e., $2m-2$) length when $\mathbb{G} = (\mathbf{Z}, +)$ and m is an integer ≥ 2

(iii) "sharp" bounds on $\mathrm{D}(X)$ when $\mathbb{G} = (\mathbf{Z}, +)^d$ and X is a symmetric box (i.e., $X = [\![-m_1, m_1]\!] \times \cdots \times [\![-m_d, m_d]\!]$ for some $m_1, \ldots, m_d \in \mathbf{N}$)

(iv) some multiplicative properties of $\mathrm{D}(\cdot)$

In addition to this, we have some questions

...and what we knew

Point (iii) improves on an upper bound obtained in:

P. Diaconis, R. Graham, and B. Sturmfels, "Primitive partition identities"
in: D. Miklós, V. T. Sós, and T. Szõnyi (eds.)
Combinatorics: Paul Erdős is eighty, Vol. 2
János Bolyai Math. Soc., 1996, 173–192

In addition, work by P. A. Sissokho and coauthors relative to the case $\mathbb{G} = (\mathbf{Z}, +)$, e.g.

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

Bounds for the case $\mathbb{G} = (\mathbf{Z}, +)$

Theorem 1. We have $\chi(X) \leq \mathrm{D}(X) \leq \mathrm{diam}(X)$, where

$$\mathrm{diam}(X) := \sup_{x,y \in X} |x - y| \quad \text{and} \quad \chi(X) = \sup_{x,y \in X : xy \leq 0} \frac{|x| + |y|}{\gcd(x, y)}$$

(with the convention that $\sup(\emptyset) := 0$ and $0/0 := \gcd(0, 0) := 1$)

The above inequality is sharp:

Corollary 1. If m and M are non-negative integers, then

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

In particular, if m and M are coprime, then $\mathrm{D}([\![-m, M]\!]) = m + M$.

It follows that for an integer $m \geq 0$ it holds

$$\mathrm{D}([\![-m, m]\!]) = \begin{cases} 1 & \text{if } m = 0 \\ 2 & \text{if } m = 1 \\ 2m - 1 & \text{if} m \geq 2 \end{cases}$$

Asymptotic bounds for the case $\mathbb{G} = (\mathbf{Z}, +)$

We have the following asymptotic result:

Theorem 2. Let $m, M \in \mathbf{N}^+$, $m \leq M$. Then, for any real $\theta > 0$ it holds that

$$\mathrm{D}(\llbracket -m, M \rrbracket) = m + M + o(m^\theta) \quad \text{as } m \to \infty$$

In the preprint this is proved only for exponents $\theta \geq 0.525$, a value resulting from the application of Hoheisel's theorem on the existence of a prime in intervals of the form $(x - x^\theta, x)$, as improved in:

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

Later, we realized that this can be extended to any exponent $\theta > 0$ by the following:

Lemma 1. For every $\theta \in [0, 1[$ there exists $v \in \mathbf{N}$ such that for all $a, b \in \mathbf{N}$ with $b \geq a \geq v$ there exist coprime integers $h \in [a - a^\theta, a]$ and $k \in [b - a^\theta, b]$

Inverse theorems for the case $\mathbb{G} = (\mathbf{Z}, +)$

We have the following inverse theorems:

Theorem 3. Let m and M be positive integers, and let $\mathfrak{s} \in \mathscr{B}(\llbracket -m, M \rrbracket)$ be a ZSS of length $m + M$. Then, $\mathfrak{s}$ is minimal iff $\gcd(m, M) = 1$ and $\mathfrak{s} = M^m \cdot (-m)^M$

This leads to the following (well-known) result:

Corollary 2. Let m be an integer ≥ 2 and $\mathfrak{s} \in \mathscr{B}(\llbracket -m, m \rrbracket)$ be a ZSS of length $2m - 1$. Then, $\mathfrak{s}$ is minimal iff $\mathfrak{s} = m^{m-1} \cdot (-m + 1)^m$ or $\mathfrak{s} = (-m)^{m-1} \cdot (m - 1)^m$

The next theorem is somewhat more complicated:

Theorem 4. Let m be an integer ≥ 3, and let $\mathfrak{s} \in \mathscr{B}(\llbracket -m, m \rrbracket)$ be a ZSS of length $2m - 2$. Then, $\mathfrak{s}$ is minimal iff 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 $\mathfrak{s} = (-m)^{m-2} \cdot (m - 1)^{m-1} \cdot (-1)$

A couple of technical lemmas

Our proofs of Theorems 1, 3 and 4 are essentially based on the following lemmas

Lemma 2. Let $x_1 \cdots x_n \in \mathcal{A}(G)$, and assume there exist a set S 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 S. Then, $n \leq |S|$. Furthermore, if $n \geq 3$, $x_{\sigma(2)} \neq x_{\sigma(3)}$ and $x_{\sigma(2)} + x_{\sigma(3)} \in S$, then $n \leq |S| - 1$.

For $S = G$ this implies the classical result according to which the Davenport constant of a finite cyclic group of order n is n (...)

Lemma 3. Assume X is finite and non-empty, and let $\mathfrak{s} = x_1 \cdots x_n$ be a minimal ZSS of $\mathscr{B}(X)$ of length $n \geq 2$. There then exists a permutation σ of $[\![1, n]\!]$ such that

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

for every $i \in [\![1, n-1]\!]$. In particular,

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

for every $i \in [\![1, n]\!]$, where the inequality on the left (resp., on the right) holds as an equality only if $x_{\sigma(1)} = \min(X)$ (resp., $x_{\sigma(1)} = \max(X)$).

Bounds for the case $\mathbb{G} = (\mathbf{Z}, +)^d$

The following results give bounds on $\mathrm{D}(X)$ when X is a symmetric box of $\mathbf{Z}^d$ ($d \in \mathbf{N}^+$)

Theorem 5. Let $m_1, \ldots, m_d$ be non-negative integers, and set $k := d + \frac{1}{d} - 1$. Then,

$$\mathrm{D}(\llbracket -m_1, m_1 \rrbracket \times \cdots \times \llbracket -m_d, m_d \rrbracket) \leq \prod_{i=1}^{d} (2m_i k + 1) \tag{1}$$

More in particular, if m is a non-negative integer, then

$$(2m - 1 + 2\delta_{m,0} + \delta_{m,1})^d \leq \mathrm{D}(\llbracket -m, m \rrbracket^d) \leq (2mk + 1)^d \tag{2}$$

where $\delta_{i,j}$ is a Kronecker delta

For $d = 2$ the 2nd inequality in Theorem 5 can be improved to

$$\mathrm{D}(\llbracket -m, m \rrbracket^d) \leq (2m + 1)(4m + 1) \tag{3}$$

Some words on the proof

(1) and (3) are essentially based on a connection (first noticed by Diaconis, Graham and Sturmfels) between the Davenport constant and (a generalization of) the Steinitz constant of a finite-dimensional real normed space, see in particular

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

On the other hand, the inequality on the left of Equ. (2) is based on the explicit construction of a ZSS $\mathfrak{s}_d$ of length $(2m-1+2\delta_{m,0}+\delta_{m,1})^d$

In fact, $\mathfrak{s}_d$ is constructed recursively as follows (we focus on the case $m \geq 2$): If we write $\mathfrak{s}_d = x_1 \cdots x_n$, where $n = (2m-1)^d$ and $x_i \in [\![-m, m]\!]^d$, then

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

As a base of induction we consider $d = 2$, for which we have $\mathfrak{s}_2 = m^{m-1}(-m+1)^m$

Multiplicative properties of D(·)

In certain cases, $\mathbf{D}(\cdot)$ behaves as a submultiplicative function:

Theorem 6. Let $\mathbb{G} = \mathbb{G}_1 \times \mathbb{G}_2$, where $\mathbb{G}_i = (G_i, +)$ is an abelian group, and let $X_2 \subseteq G_2$. Then,

$$\mathrm{D}(G_1 \times X_2) \leq \mathrm{D}(G_1)\ \mathrm{D}(X_2)$$

On the other hand, there're cases when **D** is supermultiplicative:

Theorem 7. Let $\mathbb{G} = \mathbb{H} \times (\mathbf{Z}, +)^d$, where $\mathbb{H} = (H, +)$ is a finite abelian group and $d \in \mathbf{N}^+$, and let $X = H \times [\![-m, m]\!]^d$, where m is a non-negative integer. Then,

$$\mathrm{D}(X) \geq \mathrm{D}(H)\ (2m - 1 + 2\delta_{m,0} + \delta_{m,1})^d$$

The above theorems together imply the following:

Corollary 3. Let $\mathbb{G} = \mathbb{H} \times (\mathbf{Z}, +)$, where $\mathbb{H}$ is a finite cyclic group and $m \in \mathbf{N}$. Then,

$$\mathrm{D}(H \times [\![-m, m]\!]) = \mathrm{D}(H)\ \mathrm{D}([\![-m, m]\!])$$

Some questions

Here are some questions for which we do not know an answer:

(i) Let $\mathbb{G} = (\mathbf{Z}, +)$. Can you find at least one case when $\mathrm{D}(X) \neq \chi(X)$?

(ii) Let $\mathbb{G} = (\mathbf{Z}, +)^d$ and $m_1, \ldots, m_d \in \mathbf{N}$. Can you prove or disprove that

$$\mathrm{D}([\![-m_1, m_1]\!] \times \cdots \times [\![-m_d, m_d]\!]) = \prod_{i=1}^{d} \mathrm{D}([\![-m_i, m_i]\!])?$$

(iii) Is there a "nice characterization" of the cases in which Theorem 6 can be extended to prove that $\mathrm{D}(X_1 \times X_2) \leq \mathrm{D}(X_1)\ \mathrm{D}(X_2)$ for all finite sets $X_1 \subseteq G_1$ and $X_2 \subseteq G_2$?

(iv) Can Corollary 7 be extended to prove that if $\mathbb{G} = \mathbb{H} \times (\mathbf{Z}, +)^d$, $d \in \mathbb{N}^+$, and $X = H \times B$ for a symmetric box $B \subseteq \mathbf{Z}^d$ then $\mathrm{D}(H \times B) = \mathrm{D}(H) \times \mathrm{D}(B)$?

Merci bien pour votre attention !