Zero-Sum Multisets

Klaus Pommerening
Johannes-Gutenberg-Universität
Mainz, Germany

November 2017
last change: February 17, 2022

The subject of this little survey are finite sequences in a $\mathbb{Z}$-module (or additively written abelian group) M that sum up to 0. Typical questions are:

- In a given sequence find a subsequence with zero sum.
- Find conditions that minimal zero sum sequences must satisfy.
- Find all minimal zero-sum sequences.
- Count the minimal zero-sum sequences.

Prominent examples are the cyclic groups $M = \mathbb{Z}/m\mathbb{Z}$ and $M = \mathbb{Z}$ where zero-sum sequences correspond to solutions of linear congruences or linear Diophantine equations.

1 Multisets

Since addition in a $\mathbb{Z}$-module M is commutative, the order of the elements in a sequence doesn't matter for the summation, therefore we consider finite "multisets" of elements of M. Informally spoken these are "subsets" that may contain the same elements several times.

In general a subset S of a set M is characterized by its indicator function

$$\mu\colon M \longrightarrow \mathbb{N}, \quad \mu(a) = \begin{cases} 1, & \text{if } a \in S, \\ 0, & \text{if } a \notin S. \end{cases}$$

For a multiset we allow multiplicities other than 0 or 1, so we think of a subset where each element may occur several times. To be precise:

Definition Let M be a set.

1. A **multiset** S in M is a map

$$\mu\colon M \longrightarrow \mathbb{N}.$$

The subset $\operatorname{supp}(S) = \{a \in M \mid \mu(a) > 0\} \subseteq M$ is called the **support** of S. For an element $a \in \operatorname{supp}(S)$ the value $\mu(a)$ is called the **multiplicity** of a in S. The **size** of S is

$$\#S := \sum_{a \in \operatorname{supp}(S)} \mu(a)$$

(that is the number of its elements counted according to their multiplicities). The **width** of S is $\mathsf{w}(S) = \#\operatorname{supp}(S)$ (that is the number of different elements). The **height** of S is the maximum multiplicity, $\mathsf{h}(S) = \max\{\mu(a) \mid a \in \operatorname{supp}(S)\}$.

2. Let S (with multiplicity map μ) and T (with multiplicity map ν) be multisets in M. Then T is called a **submultiset** of S, written $T \subseteq S$, if $\nu \leq \mu$, that is, each element in the support of T occurs in S at most with the same multiplicity.
3. The multiset S is called **finite** if its support is finite.

Note that the size $\#S$ of a multiset is finite if and only if S is finite. We denote multisets by double braces. Thus in $\mathbb{Z}$ the multiset $\mu(1) = 2$, $\mu(3) = 1$, $\mu(-2) = 4$, $\mu(i) = 0$ otherwise, is written as

$$\{\{1, 1, 3, -2, -2, -2, -2\}\}.$$

Inside the braces the elements may be listed in any order. We may interpret $\{\{s_1, \ldots, s_n\}\}$ as the orbit of the sequence $(s_1, \ldots, s_n) \in M^n$ under the symmetric group $\mathcal{S}_n$. Thus the multisets in M of size n are the members of the group-theoretic quotient $M^n/\mathcal{S}_n$.

2 Multiset Sums

Definition Let M be a $\mathbb{Z}$-module and S be a finite multiset in M. The **(multiset) sum** of S is

$$\Sigma(S) := \sum_{a \in \operatorname{supp}(S)} \mu(a)\, a.$$

So we sum up the elements of S according to their multiplicities. If $S = \{\{s_1, \ldots, s_n\}\}$, then simply

$$\Sigma(S) = s_1 + \cdots + s_n$$

(and $\#S = n$). If $\operatorname{supp}(S) = \{a_1, \ldots, a_m\}$, and a_i has multiplicity x_i, the multiset sum is more intuitively written as

$$\Sigma(S) = x_1 a_1 + \cdots + x_m a_m.$$

Writing the sum as a linear combination with integer coefficients emphasizes the inherent algebraic (or geometric) structure of the $\mathbb{Z}$-module M. The vector $a = (a_1, \ldots, a_m) \in M^m$ defines a homomorphism

$$\Phi_a \colon \mathbb{Z}^m \longrightarrow M, \quad x \mapsto \sum x_i a_i,$$

whose kernel consists of the coefficient m-tuples that make the sum zero. Zero-sum problems address questions on multiset sums such as stated on the introduction:

- Given a multiset S, for which submultisets $T \subseteq S$ is $\Sigma(T) = 0$?
- What properties have minimal (nonvoid) multisets S with $\Sigma(S) = 0$?
- Count or estimate their number.

Examples Prominent zero-sum problems are the linear Diophantine problems that ask for the (restricted) kernel $\ker \Phi_a \cap \mathbb{N}^n$:

1. The linear equation ($M = \mathbb{Z}$). Given integer coefficients $a_1, \ldots, a_n \in \mathbb{Z}$, find non-negative integer solutions $x_1, \ldots, x_n \in \mathbb{N}$ of
$$a_1x_1 + \cdots + a_nx_n = 0.$$
2. The linear congruence ($M = \mathbb{Z}/m\mathbb{Z}$ with $m \in \mathbb{N}_2$). Given integer coefficients $a_1, \ldots, a_n \in \mathbb{Z}$, find non-negative integer solutions $x_1, \ldots, x_n \in \mathbb{N}$ of
$$a_1x_1 + \cdots + a_nx_n \equiv 0 \pmod{m}.$$

Note that we changed the meanings of m and n as well as the order of a_i and x_i according to the common usage for linear equations where the x_i are the unknowns. Note also that for the linear Diophantine problems the assumption that the coefficients a_i are different is unusual, and inadequate for some applications—however this is a minor technical issue.

Definition Let S be a (finite) **multiset** in the $\mathbb{Z}$-module M with support $\{a_1, \ldots, a_m\}$ and multiplicities $x_i = \mu(a_i)$, hence multiset sum $\Sigma(S) = x_1a_1 + \cdots + x_ma_m$.

1. S is called a **zero-sum multiset** if $\Sigma(S) = 0$.
2. A **subsum** of S is a sum
$$y_1a_1 + \cdots + y_ma_m \quad \text{with } y_1, \ldots, y_m \in \mathbb{N},$$
where $0 \leq y_i \leq x_i$ for all $i = 1, \ldots, m$, in other words, a sum over a submultiset $T \subseteq S$ defined by $\nu(a_i) = y_i$.
3. The multiset S is called a **minimal zero-sum multiset** if it is a zero-sum multiset, its size is positive, and no proper subsum is zero (except the empty one).
4. The multiset S is called **zerofree** if it isn't zero-sum and no nontrivial subsum is zero (where "nontrivial" means: except the empty one, but including $\Sigma(S)$ itself).

Examples

3. Obviously any multiset with support $\{0\}$ is a zero-sum multiset. It contains a unique minimal zero-sum subset $\{\{0\}\}$, given by $\mu(a) = 1$ for $a = 0$, and $\mu(a) = 0$ otherwise (thus $\mu(a) = \delta_{a0}$).
4. If $b \in M$ has order $r > 0$, then $\mu(a) = r\,\delta_{b0} = r$ if $a = b$ and $= 0$ otherwise, defines a zero-sum multiset $\{\{b, \ldots, b\}\}$ with support $\{b\}$, and this is a minimal one.
5. For $M = \mathbb{Z}$ a multiset S with support $\{1, -1\}$ is zero-sum if and only if $\mu(1) = \mu(-1)$. It is minimal if this multiplicity is 1, i. e. if $S = \{\{1, -1\}\}$.
6. For the Examples 1 and 2 above the minimal zero-sum multisets with support contained in $\{a_1, \ldots, a_n\}$ correspond to the minimal nonzero (or indecomposable) solutions of the linear Diophantine equation or the linear congruence with given coefficients $a_1, \ldots, a_n$, see [12, 13].

Additional questions

- How large can a zerofree multiset be? Note that this questions makes sense only if M is finite, or (for $M = \mathbb{Z}$) if we require that the elements of the submultisets are of bounded size and have different signs.
- How many values can the subsums of a zerofree multiset take?

3 The Davenport Constant

Definition Let $X \subseteq M$ be a subset of a $\mathbb{Z}$-module (or abelian group) M. The **Davenport constant** of X, $\mathsf{DC}(X)$, is the supremum of the sizes of minimal zero-sum multisets with support contained in X.

Examples

1. $\mathsf{DC}(\mathbb{Z}) = \infty$, since for any n the multiset $\{\{n, -1, \ldots, -1\}\}$ of size $n + 1$ in $\mathbb{Z}$ is minimal zero-sum.
2. $\mathsf{DC}(\mathbb{Z}/m\mathbb{Z}) = m$, see Proposition 1 below.
3. For the integer interval $X = [-1 \ldots 1] = \{-1, 0, 1\} \subseteq M = \mathbb{Z}$ the Davenport constant is $\mathsf{DC}(X) = 2$. (The minimal zero-sum multisets in X are given by the Examples 3 and 5 in Section 2: $\{\{0\}\}$ and $\{\{1, -1\}\}$.)
4. For the interval $X = [-q \ldots q] \subseteq M = \mathbb{Z}$ with $q \geq 2$ the result, $\mathsf{SD}(X) = 2q - 1$, is non-trivial, it follows from Lambert's Theorem below, see Theorem 4 (i) and Corollary 2.

Remark 1 Assume $\mathsf{DC}(X) < \infty$. There is a zerofree multiset S in X of size $\#S = \mathsf{DC}(X) - 1$.

For the proof take a minimal zero-sum multiset T in X of size $\mathsf{DC}(X)$, and remove (one instance) of an arbitrary $a \in T$. Then $S = T - \{a\}$ is a zerofree multiset in X of the required size.

Lemma 1 *Assume X is a sub*group *of M with $\mathsf{DC}(X) < \infty$. Then every multiset S of size $\#S \geq \mathsf{DC}(X)$ in X contains a nontrivial zero-sum submultiset.*

Proof. Assume the contrary, in particular $t := -\Sigma(S) \neq 0$, and $t \in X$. Thus $\hat{S} = S \cup \{t\}$ (multiplicity of t increased by 1) is a zerosum multiset in X of size $\#\hat{S} = \#S + 1 > \mathsf{DC}(X)$, and $\hat{S}$ contains a minimal zerosum submultiset T, in particular $\#T \leq \mathsf{DC}(X)$. By our assumption $T \not\subseteq S$, hence the additional element t is in T. However $T' = T - \{t\} \subseteq S$, and

$$\Sigma(T') = \Sigma(T) - t = -t = \Sigma(S).$$

Hence $S - T'$ is a zerosum submultiset of S, hence $= \emptyset$. Therefore $T' = S$, but $\#T' = \#T - 1 < \mathsf{DC}(X) \leq \#S$, contradiction. ◇

Remark 2 Thus for a subgroup X of M with finite Davenport constant $\mathsf{DC}(X) < \infty$ the Davenport constant is the smallest integer N such that every multiset of size $\geq N$ in X contains a nontrivial zero subsum.

Often this property is taken as definition of the Davenport constant—however then the applicability of this definition is somewhat restricted.

Proposition 1 *The Davenport constant of the cyclic group $M = \mathbb{Z}/m\mathbb{Z}$ is m.*

Proof. By Example 4 the multiset with support $\{1\}$ and multiplicity $\mu(1) = m$ is a minimal zero-sum multiset, hence the Davenport constant is at least m. On the other hand let $a_1, \ldots, a_m$ integers. Then by the pigeon hole principle among the $m+1$ residues

$$0,\ a_1,\ a_1 + a_2, \ldots,\ a_1 + \cdots + a_m \bmod m$$

at least two must coincide: $a_1 + \cdots + a_i \equiv a_1 + \cdots + a_j \pmod{m}$ with $0 \leq i < j \leq m$. Their difference $a_{i+1} + \cdots + a_j \bmod m$ yields a non-trivial subsum in with value 0. ◇

Corollary 1 *Every zerofree multiset of $\mathbb{Z}/m\mathbb{Z}$ has size $< m$. In other words, every multiset S of size $\#S \geq m$ in $\mathbb{Z}/m\mathbb{Z}$ contains a nontrivial zero-sum submultiset.*

Proof. Combine Proposition 1 with Lemma 1. ◇

We translate the setting into the algebraic language: The $\mathbb{Z}$-module $M = \mathbb{Z}/m\mathbb{Z}$ consists of the residue classes of $0, 1, \ldots, m-1$. (By abuse of notation we often write the integers when we mean their residue classes.) A multiset in M is defined by an assignment of multiplicities $r_i = \mu(i)$ to each of the integers $i = 0, \ldots, m-1$. If we interpret this as a vector $r = (r_0, \ldots, r_{m-1}) \in \mathbb{N}^m$, then the size of the multiset is the 1-norm $\|r\|_1 = \sum r_i$ of the vector, and Corollary 1 yields:

Corollary 2 *Let $r \in \mathbb{N}^m$ be a vector with $\|r\|_1 = m$. Then there is a vector $x \in \mathbb{N}^m$ with $0 < x \leq r$ such that*

$$\sum_{i=0}^{n-1} i\, x_i \equiv 0 \pmod{m}.$$

An independent version was given by Tinsley in [15] that however is a special case of Noether's bound for the invariants of finite groups [8]:

Corollary 3 *Let $x \in \mathbb{N}^n$ be a minimal solution > 0 of the linear congruence*

$$a_1 x_1 + \cdots + a_n x_n \equiv 0 \pmod{m}.$$

Then

$$x_1 + \cdots + x_n \leq m.$$

Proof. Collecting terms with coefficients a_i congruent $\bmod\, m$ we may assume that the a_i are distinct $\bmod\, m$ and thus form a subset of $\{0, \ldots, m-1\}$. The minimality of x implies $\|x\|_1 \leq m$ by Proposition 1. $\diamond$

The papers [4] and [12] contain a stronger version of Proposition 1 resp. Corollary 3:

Theorem 1 *Let S be a minimal zero-sum multiset in $\mathbb{Z}/m\mathbb{Z}$. Then:*

(i) (Eggleton/Erdős) $\#S + \mathsf{w}(S) \leq m + 1$.

(ii) (Pommerening) *If $\#S + \mathsf{w}(S) = m + 1$, then $\mathsf{w}(S) \leq 2$ except when $m = 6$ and $S = \{\{1, 3, 4, 4\}\}$ or $S = \{\{2, 2, 3, 5\}\}$.*

Proof. See [12]. $\diamond$

A famous non-trivial result on zero-sum submultisets, in a more general version, is:

Theorem 2 (Erdős/Ginzburg/Ziv) *Suppose $m \geq k \geq 2$ are integers with $k|m$. Let $a_1, a_2, \ldots, a_{m+k-1}$ be a sequence of integers. Then there exists a subset I of $\{1, 2, \ldots, m+k-1\}$, such that $\#I = m$ and $\sum_{i \in I} a_i \equiv 0 \pmod{k}$.*

Proof. Omitted. See [2]. $\diamond$

The theorem immediately implies the original result from [5]:

Corollary 1 *Every sequence of $2m - 1$ natural numbers contains m terms whose sum is divisible by m.*

And here is a geometric version:

Corollary 2 *Let $r = (r_0, \ldots, r_{m-1}) \in \mathbb{N}^m$ be a vector with $\|r\|_1 = 2m - 1$. Then there is a vector $x = (x_0, \ldots, x_{m-1}) \in \mathbb{N}^m$ with $0 < x \leq r$ and $\|x\|_1 = m$ such that*

$$\sum_{i=0}^{n-1} i\, x_i \equiv 0 \pmod{n}.$$

4 The Strong Davenport Constant

Definition Let $X \subseteq M$ be a subset of a $\mathbb{Z}$-module M. The **strong Davenport constant** of X, $\mathsf{SD}(X)$, is the supremum of the widths of the minimal zero-sum multisets with support contained in X, see [3].

Remarks

1. Since width $\leq$ size, $\mathsf{SD}(X) \leq \mathsf{DC}(X)$.
2. Since $\mathsf{w}(T) = 0 \iff T = \emptyset$ we have $\mathsf{w}(T) \geq 1$ if T is a minimal zero-sum multiset in X. Then $\mathsf{w}(T) = 1$ if and only if $T = \{\{0\}\}$ or if T consists of a single element $a \in X - \{0\}$ of finite order n repeated n times. If X is a subgroup of M, then $\{\{a, (n-1)\,a\}\}$ is also a zero-sum multiset in X and it has width 2 except when $n = 2$. Thus for a subgroup $X \subseteq M$:

$$\mathsf{SD}(X) = 1 \iff X \text{ is cyclic of order } 2.$$

Examples

1. $\mathsf{SD}(\mathbb{Z}) = \infty$, since for any n, $N = 1 + \cdots + n$ the set $\{N, -1, \ldots, -n\}$ of width $=$ size $n+1$ is minimal zero-sum.
2. $\mathsf{SD}(\mathbb{Z}/m\mathbb{Z})$ is unknown in the general case, see the notes at the end of this section. Of course for small m the values are known, for example

$$\mathsf{SD}(\mathbb{Z}/3\mathbb{Z}) = \mathsf{SD}(\mathbb{Z}/4\mathbb{Z}) = \mathsf{SD}(\mathbb{Z}/5\mathbb{Z}) = 2.$$

   For $m \geq 6$ we have $m - 3 \geq 3$, hence $S = \{1, 2, m-3\}$ is a minimal zero-sum set of width $=$ size $\mathsf{w}(S) = 3$. Therefore $\mathsf{SD}(\mathbb{Z}/m\mathbb{Z}) \geq 3$.
3. For the integer interval $X = [-1 \ldots 1] = \{-1, 0, 1\} \subseteq M = \mathbb{Z}$ the strong Davenport constant is $\mathsf{SD}(X) = 2$. (The minimal zero-sum multisets $\{\{0\}\}$ and $\{\{1, -1\}\}$ of Example 3 in Section 3 are in fact sets.)
4. For the interval $X = [-q \ldots q] \subseteq M = \mathbb{Z}$ with $q \geq 2$ the value of $\mathsf{SD}(X)$ is unknown in general.

By the next theorem if X is a subgroup it doesn't matter whether $\mathsf{SD}(X)$ is defined via multisets or via sets—in other words, the bound $\mathsf{SD}(X)$ (if finite) is attained by minimal zero-sum *set* $\subseteq X$. We use an elementary but useful technique of modifying multisets and start with some lemmas.

Definition Let $S = \{\{s_1, \ldots, s_n\}\}$ be a multiset in the $\mathbb{Z}$-module M. The **glued** multiset S_{ij} for two different indices $i \neq j$ consists of S with s_i and s_j removed and their sum $s_i + s_j$ inserted (s_i and s_j are "glued" together to $s_i + s_j$).

Example For $S = \{\{1, 1, 3, -2, -2, -2, -2\}\}$ we have $S_{34} = \{\{1, 1, 1, -2, -2, -2\}\}$.

Remarks

1. $\#S_{ij} = \#S - 1$, the size is decremented.
2. $\mathsf{w}(S_{ij})$ may be $= \mathsf{w}(S) - 1$ or $= \mathsf{w}(S)$ or $= \mathsf{w}(S) + 1$, the width changes by at most 1.
3. $\Sigma(S_{ij}) = \Sigma(S)$, the multiset sum is unchanged. In particular S_{ij} is zero-sum if S is.

Lemma 2 *If S is a minimal zero-sum multiset in M, so is every glued multiset S_{ij}.*

Proof. Let $S = \{\{s_1, \ldots, s_n\}\}$, and let $T \subseteq S_{ij}$ a (nonvoid) zero-sum multiset. If $s_i + s_j$ is not in T, then $T \subseteq S$, hence $T = S$, contradicting $\#T \leq \#S_{ij} = \#S - 1$. Otherwise $s_i + s_j$ is in T but not in $T' := S_{ij} - T$ that is also a zero-sum multiset (with the natural definition of the multiset difference), hence $T' \subseteq S$ with $\#T' < \#S$, forcing $T' = \emptyset$ and $T = S_{ij}$. $\diamond$

Lemma 3 *Let $2 \leq \mathsf{SD}(X) < \infty$ and T be a minimal zero-sum multiset in X of maximal width $\mathsf{w}(T) = \mathsf{SD}(X)$.*

(i) *If $a \in \operatorname{supp}(T)$, then $ka \neq 0$ for $1 \leq k \leq \mu(a)$.*

(ii) *If $a, b \in \operatorname{supp}(T)$, $a \neq b$, and $\#T \geq 3$, then $a + b \neq 0$.*

Proof. (i) Otherwise $\nu(a) = k$ defines a zero-sum submultiset $S \subseteq T$ of width 1. The minimality of T enforces $S = T$, hence $\mathsf{w}(T) = 1$, contradiction.

(ii) Otherwise $S = \{a, b\}$ is a zero-sum sub(multi)set $\subseteq T$, hence $= T$, hence $\#T = \#S = 2$, contradiction. $\diamond$

Lemma 4 *Let $2 \leq \mathsf{SD}(X) < \infty$ and T be a minimal zero-sum multiset in X of maximal width $\mathsf{w}(T) = \mathsf{SD}(X)$. Let $a \in \operatorname{supp}(T)$ have multiplicity $\mu(a) \geq 2$ in T. Then for each $b \in \operatorname{supp}(T) - \{a\}$ at least one of the following statements holds:*

(i) *$a + b \in \operatorname{supp}(T)$,*

(ii) *$\mu(b) = 1$,*

(iii) *$a + b \notin X$.*

Proof. Let $T = \{\{s_1, \ldots, s_n\}\}$ and $a = s_i$, $b = s_j$. Since $\mathsf{w}(T) \geq 2$ and $\mu(a) \geq 2$ we have $\#T \geq 3$. Thus Lemma 3 (ii) implies that $a + b \neq 0$.

Moreover the conditions $a+b \notin \operatorname{supp}(T)$ and $\mu(b) \geq 2$ together would imply that T_{ij} is a minimal zero-sum multiset with a, b, and $a+b$ in its support, hence $\mathsf{w}(T_{ij}) = \mathsf{SD}(X)+1$, contradiction if $a + b \in X$. Therefore T must satisfy at least one of the conditions (i), (ii), or (iii). $\diamond$

Theorem 3 (Chapman/Freeze/Smith) *Let M be a $\mathbb{Z}$-module, and suppose that $2 \le s := \mathsf{SD}(M) < \infty$. Let T be a minimal zero-sum multiset in M that assumes the maximal width $\mathsf{w}(T) = s$, and let the size $\#T$ be minimal under this condition. Then T is a set.*

Proof. We assume that $T = \{\{s_1, \ldots, s_n\}\}$ is not a set and derive a contradiction. Under this assumption T has an element $a = s_i$ of multiplicity $\mu(a) \ge 2$. Then $2a \ne 0$ by Lemma 3 (i). The glued multiset T_{ii} is a minimal zero-sum multiset in M with $\#T_{ii} = \#T - 1$. The minimality of $\#T$ enforces $\mathsf{w}(T_{ii}) < s$. Since $T_{ii} = T - \{\{a, a\}\} \cup \{\{2a\}\}$ this implies that

$$2a \in \mathrm{supp}(T) \tag{1}$$

and $a \notin \mathrm{supp}(T_{ii})$, hence $\mu(a) = 2$. By Lemma 4 for each $b \in \mathrm{supp}(T) - \{a\}$ the multiset T must satisfy at least one of the conditions $a + b \in \mathrm{supp}(T)$ or $\mu(b) = 1$.

Case I: Assume $\mu(b) \ge 2$ for some $b = s_j \in \mathrm{supp}(T) - \{a\}$. Then $a + b \in \mathrm{supp}(T)$, and the support of T_{ij} contains a and b, hence $\mathsf{w}(T_{ij}) = s$, but $\#T_{ij} = \#T - 1$ contradicts the minimality of $\#T$.

Case II: $\mu(b) = 1$ for all $b \in \mathrm{supp}(T) - \{a\}$. Then T_{ij} with $\#T_{ij} = \#T - 1$ has a and $a + b$ in its support, but not b. The minimality of $\#T$ enforces $\mathsf{w}(T_{ij}) = s - 1$, hence $a + b \in \mathrm{supp}(T)$.

Using equation (1) and Lemma 3 (ii) we get $3a = a + 2a \ne 0$ and by Lemma 4 (i) even $3a \in \mathrm{supp}(T)$. Continuing iteratively we see that all multiples ka are in $\mathrm{supp}(T)$, hence

$$\mathrm{supp}(T) = \{ka \mid 1 \le k \le s\}.$$

Continuing the iteration beyond s we also get $(s+1)\,a \in \mathrm{supp}(T)$, hence $(s+1)\,a = ka$ for some k with $1 \le k \le s$, and from this the contradiction $(s + 1 - k)\,a = 0$. ◇

By Theorem 3, for determining $\mathsf{SD}(\mathbb{Z}/m\mathbb{Z})$ we need to consider only minimal zero-sum sub*sets* of $\mathbb{Z}/m\mathbb{Z}$. Explicit values, easily determined by a simple program, see [11], are

$$\mathsf{SD}(\mathbb{Z}/m\mathbb{Z}) = \begin{cases} 2 & \text{for } m = 3,\ 4,\ 5, \\ 3 & \text{for } m = 6,\ 7, \\ 4 & \text{for } m = 8,\ 9,\ 10, \\ 5 & \text{for } m = 11,\ \ldots,\ 15, \\ 6 & \text{for } m = 16,\ \ldots,\ 23. \end{cases}$$

The program uses the trivial fact that if S is a minimal zerosum subset of size s, and $t \in S$, then $S - \{t\}$ is a zerofree subset of size $s - 1$. It proceeds successively by increasing size s and terminates as soon as it doesn't find any zerofree subsets of size s. This stop criterion relies on the following results:

Proposition 2 *Let S be a zerofree multiset in a $\mathbb{Z}$-module M. Then the number $\mathsf{w}(S)$ of different elements of S is at most $\mathsf{SD}(M)$.*

Proof. By definition $t := -\Sigma(S) \in M - \{0\}$, hence $T := S \cup \{t\}$ is a zero-sum multiset, $\Sigma(T) = \Sigma(S) + t = 0$. There is a minimal zero-sum multiset $U \subseteq T$. Since S is zerofree U is not contained in S, hence the multiplicity of t in U is 1+ the multiplicity of t in S, and $U' := U - \{t\}$ (multiplicity of t decreased by 1) is a submultiset of S. Moreover

$$\Sigma(U') = \Sigma(U) - t = -t = \Sigma(S).$$

Therefore $S - U'$ is a zero-sum multiset contained in S, hence $= \emptyset$, thus $U' = S$ and $U = U' \cup \{t\} = S \cup \{t\} = T$. Since U is minimal $\mathsf{w}(S) \leq \mathsf{w}(T) = \mathsf{w}(U) \leq \mathsf{SD}(M)$. $\diamond$

Corollary 1 *If $S \subseteq M$ is a zerofree subset, then $\#S \leq \mathsf{SD}(M)$.*

Proof. Since S is a set $\#S = \mathsf{w}(S)$. $\diamond$

Denote the maximum size of a zerofree subset of M by $\mathsf{zf}(M)$, called the **zerofree bound** of M.

Corollary 2 *Assume* $\mathsf{SD}(M) < \infty$*. Then* $\mathsf{zf}(M) = \mathsf{SD}(M)$ *or* $\mathsf{SD}(M) - 1$*.*

Proof. $\mathsf{zf}(M) \leq \mathsf{SD}(M)$ by Corollary 1. To get a zerofree set of size $\mathsf{SD}(M) - 1$ take a minimal zero-sum subset of size $\mathsf{SD}(M)$ and remove an arbitrary element. $\diamond$

Corollary 3 *Assume* $\mathsf{SD}(M) < \infty$ *and* $\mathsf{zf}(M) = \mathsf{SD}(M) - 1$*. Let T be a minimal zero-sum multiset in M of width* $\mathsf{w}(T) = \mathsf{SD}(M)$*. Then T is a set.*

Proof. Assume $a \in T$ has multiplicity $\mu(a) \geq 2$. Then $T' = T - \{\{a\}\}$ is zerofree and has width $\mathsf{w}(T') = \mathsf{w}(T) = \mathsf{SD}(M)$, contradiction. $\diamond$

Example The smallest module m for which all zerofree subsets of $\mathbb{Z}/m\mathbb{Z}$ have size $\leq \mathsf{SD}(Z/m\mathbb{Z}) - 1$ is $m = 8$ (with $\mathsf{SD}(Z/8\mathbb{Z}) = 4$). As a consequence for $m = 8$ minimal zero-sum multisets T that attain the maximum width $\mathsf{w}(T) = \mathsf{SD}(Z/8\mathbb{Z})$ must be sets.

Notes on the ERDŐS-HEILBRONN conjecture (EHC):

1. A version of the EHC claims that a subset S of a finite abelian group M has a nontrivial subsum equal to 0 if $r = \#S \geq c\sqrt{m}$ with $m = \#M$ for an absolute constant c, in other words, $\mathsf{zf}(M) \leq \lceil c\sqrt{m}\,\rceil$. ERDŐS AND HEILBRONN proved this for the cyclic group $M = \mathbb{Z}/p\mathbb{Z}$ of prime order p with $c = 3\sqrt{6}$. OLSON [9] dropped the constant to $c = 2$ for prime order p, and [10] to $c = 3$ for arbitrary (even non-abelian) M, and BALANDRAUD [1] proved that $\mathsf{zf}(\mathbb{Z}/p\mathbb{Z}) = \left\lceil \sqrt{2p + 1/4} - 3/2 \right\rceil$ for p prime ≥ 3, in particular $\mathsf{zf}(\mathbb{Z}/p\mathbb{Z}) < \lceil \sqrt{2p - 1}\,\rceil$, or $c = \sqrt{2}$ in this case.

2. Let c be the E-H constant valid for the finite abelian group M. Then $\mathsf{SD}(M) \leq \mathsf{zf}(M) + 1 \leq \lceil c\sqrt{m}\,\rceil$ by Corollary 2.
3. The strong form of the EHC (by Erdős) drops the constant to $c = \sqrt{2}$. In this strong form the conjecture is open, the best known bound is $c = \sqrt{2m} + \varepsilon(m)$ where $\varepsilon(m)$ is $\mathrm{O}(\sqrt[3]{m} \cdot \log(m))$ for M cyclic of order m, proved by Hamidoune and Zémor [6].

   Therefore we have

   - $\mathsf{SD}(\mathbb{Z}/m\mathbb{Z}) \leq \lceil 3\sqrt{m}\,\rceil$ (proved by Olson), and
   - $\mathsf{SD}(\mathbb{Z}/m\mathbb{Z}) \leq \lceil \sqrt{2m}\,\rceil$ (conjectured by Erdős).

   The explicit values above show that the bound $\lceil \sqrt{2m}\,\rceil$ is sharp for many values of m.

5 The Infinite Cyclic Group

Here we give a stronger version of Lambert's Theorem [7] combined with Sissokho's bound [14]. The proof is given in [13] in terms of linear Diophantine equations. Here we rephrase it in terms of multiset sums. For a multiset S in $\mathbb{Z}$ let S^+, S^- be the subsets of S consisting of the positive resp. negative elements with multiplicities inherited from S. Clearly S is zero-sum if and only if $\Sigma(S^+) = -\Sigma(S^-)$.

Example For the multiset $S = \{\{1, 1, 3, -2, -2, -2, -2\}\}$ we have $S^+ = \{\{1, 1, 3\}\}$, $S^- = \{\{-2, -2, -2, -2\}\}$, and S is not zero-sum.

Theorem 4 *Let S be a (finite) minimal zero-sum multiset in $\mathbb{Z}$. Suppose that S contains positive and negative integers, in particular $\#S \geq 2$. Let $A := \max(S^+)$ be the largest, and $B := -\min(S^-)$ be the additive inverse of the smallest element of S. Then*

(i) (Lambert) $\#S^+ \leq B$ *and* $\#S^- \leq A$.

(ii) (Pommerening) *If* $\#S^+ = B$, *then* $\mathrm{supp}(S^-) = \{-B\}$, *in particular* $\mathsf{w}(S^-) = 1$. *If* $\#S^- = A$, *then* $\mathrm{supp}(S^+) = \{A\}$, *in particular* $\mathsf{w}(S^+) = 1$.

(iii) (Sissokho) $\#S^+ \cdot \#S^- \leq \Sigma(S^+)$.

Proof. Let $\mathrm{supp}(S^+) = \{a_1, \ldots, a_p\}$ with $1 \leq a_1 < \ldots < a_p$, and $\mathrm{supp}(S^-) = \{-b_1, \ldots, -b_r\}$ with $1 \leq b_1 < \ldots < b_r$. Thus $m = p + r$, and $m = \mathsf{w}(S)$ since S, due to its minimality, doesn't contain 0. Furthermore $A = a_p$ and $B = b_r$.

We prove all three statements (i), (ii), and (iii) together by induction on $\#S$.

If $\#S = 2$, then necessarily $\#S^+ = \#S^- = 1$, $S^+ = \{\{a_1\}\}$, $S^- = \{\{-b_1\}\}$, $\Sigma(S^+) = a_1$, and $b_1 = a_1$. Thus (i) and (iii) hold true. The precondition $\#S^+ = B$ in (ii) implies $b_1 = 1$, so $S^- = \{\{-1\}\}$ and $\mathrm{supp}(S^-) = \{-1\}$. The same reasoning works if $\#S^- = A$. Thus also (ii) is true.

Now we assume that $\#S \geq 3$. If we find a pair (i, j) of indices with $a_i = b_j$, then we have the zero subsum $a_i + (-b_j) = 0$. The minimality of S enforces $S = \{\{a_i, -b_j\}\}$, contradicting $\#S \geq 3$.

Thus

$$\{a_1, \ldots, a_p\} \cap \{b_1, \ldots, b_r\} = \emptyset.$$

We may assume (without loss of generality) that $a_p > b_r$, and consider the derived multiset S' where from S one instance of both a_p and $-b_r$ is removed and the element $a_p - b_r$ is inserted. Then $\#S'^+ = \#S^+$ and $\#S'^- = \#S^- - 1$.

Could $\#S^- = 1$, hence $S'^- = \emptyset$, happen? Then necessarily $S^- = \{\{-b_1\}\}$, $\Sigma(S^+) = -\Sigma(S^-) = b_1$, contradicting $\Sigma(S^+) \geq a_r > b_1$. Thus $\#S^- \geq 2$.

Hence we may apply the induction hypothesis, for $\#S' = \#S - 1$, and from (i) and (iii) for S' get

$$(2) \quad \#S^+ = \#S'^+ \leq B' := -\min(S'^-) \leq B, \; \#S^- - 1 = \#S'^- \leq A' := \max(S'^+) = A,$$

$$(3) \qquad \#S^+ \cdot (\#S^- - 1) \leq \Sigma(S'^+) = (a_p - b_r) + \Sigma(S^+) - a_p = \Sigma(S^+) - b_r.$$

From Formula (3) and $b_r \cdot \#S^- = b_r \cdot (y_1 + \cdot + y_r) \geq y_1 b_1 + \cdots + y_r b_r = -\Sigma(S^-) = \Sigma(S^+)$ (where y_i is the multiplicity of $-b_i$ in S^-) we get

$$\begin{aligned} \Sigma(S^+) \cdot \#S^- - b_r \cdot \#S^- &\leq \Sigma(S^+) \cdot \#S^- - \Sigma(S^+), \\ \big(\Sigma(S^+) - b_r\big) \cdot \#S^- &\leq \Sigma(S^+) \cdot (\#S^- - 1), \\ \#S^+ \cdot (\#S^- - 1) \cdot \#S^- &\leq \Sigma(S^+) \cdot (\#S^- - 1). \end{aligned}$$

Since $\#S^- > 1$ we may divide by $\#S^- - 1$ and get (iii).

In Formula (2) we might have $\#S^- - 1 = A$. Then $\#S'^- = A'$, and the induction hypothesis implies $\operatorname{supp}(S'^+) = \{A'\} = \{A\}$, contradicting the additional element $a_p - b_r$ in S'^+. Hence $\#S^- - 1 \leq A - 1$, and the proof of (i) is complete.

For (ii) first assume that $\#S^+ = B = b_r$. Then

$$b_r y_1 + \cdots + b_r y_r = b_r \cdot \#S^- = \#S^+ \cdot \#S^- \leq \Sigma(S^+) = -\Sigma(S^-) = y_1 b_1 + \cdots + y_r b_r.$$

Hence the multiplicity $y_i > 0$ only if $i = r$. Thus $\operatorname{supp}(S^-) = \{b_r\} = \{-B\}$. The same reasoning shows that $\#S^- = A$ implies that $\operatorname{supp}(S^+) = \{A\}$ (since we didn't use the inequality $b_r < a_p$). $\diamond$

Corollary 1 *Let $a = (a_1, \ldots, a_n) \in \mathbb{Z}^n$ with $n \geq 1$, and $P = \{i \mid a_i > 0\}$ and $N = \{j \mid a_j < 0\}$. Assume $p := \#P \geq 1$ and $r := \#N \geq 1$, thus there are positive and negative coefficients. Let $A := \max\{a_i \mid i \in P\}$, $B := \max\{-a_j \mid j \in N\}$. Let $x = (x_1, \ldots, x_n) \in \mathbb{N}^n$ be an indecomposable solution of $a_1 x_1 + \cdots + a_n x_n = 0$. Then:*

(i) *The vector x is bounded by*

$$\sum_{i \in P} x_i \leq B \quad \text{and} \quad \sum_{j \in N} x_j \leq A.$$

In particular the linear Diophantine equation has only finitely many indecomposable solutions.

(ii) *If* $\sum_{i\in P} x_i = B$*, then* $x_j \neq 0$ *for* $j \in N$ *at most if* $a_j = -B$*. If* $\sum_{i\in N} x_i = A$*, then* $x_j \neq 0$ *for* $j \in P$ *at most if* $a_j = A$*.*

(iii) $\sum_{i\in P} x_i \times \sum_{j\in N} x_j \leq \sum_{i\in P} a_i x_i$.

Proof. If we collect together indices where the a_i coincide and add the corresponding vector coordinates x_i, this doesn't affect the properties of being a solution or an indecomposable solution. Also the statements (i)–(iii) are not affected. Thus without loss of generality we may assume that all coefficients a_i are distinct. Then the corollary is a reformulation of the theorem. ◇

Corollary 2 *For* $N = [-q \dots q] \subseteq M = \mathbb{Z}$ *with* $q \geq 2$ *the Davenport constant is* $2q - 1$.

Proof. A minimal zero-sum set in $[-q \dots q]$ may be supported by $\{0\}$ with multiplicity 1, and this has length 1. Otherwise it is represented by integers $x_1, \dots, x_q, x_1, \dots, y_q \in \mathbb{N}$ such that

$$\sum_{i=1}^{q} i\, x_i + \sum_{i=1}^{q} (-i)\, y_i = 0.$$

Corollary 1 (with $A \leq q$ and $B \leq q$) implies that

$$x_1 + \cdots + x_q \leq q \quad \text{and} \quad y_1 + \cdots + y_q \leq q,$$

hence our zero-sum set has length $\leq 2q$. We distinguish two cases:

1. The only non-zero coordinates are x_q and y_q. The minimality enforces $x_q = y_q = 1$, hence the length is $2 < 2q - 1$.

2. There is some non-zero coordinate other than x_q and y_q. Then only one of x_q and y_q may be non-zero, otherwise we may decrement both by 1 and still have a non-trivial zero sum. Hence $A < q$ or $B < q$. Thus the length is $\leq 2q - 1$.

On the other hand the equation $q\,(q-1) - (q-1)\,q = 0$ corresponds to the case $x_q = q-1$, $y_{q-1} = q$, and all other coefficients $= 0$, and yields a zero-sum set of length $2q - 1$ that is minimal. Hence the bound $2q - 1$ is sharp. ◇

References

[1] É. Balandraud: An addition theorem and maximal zero-sum free sets in $\mathbb{Z}/p\mathbb{Z}$. Israel J. Math. 188 (2012), 405–429, 1009–1010.

[2] J. D. Bovey, P. Erdős, I. Niven: Conditions for a zero sum modulo n. Canad. Math. Bull. 18 (1975), 27–29.

[3] S. T. Chapman, M. Freeze, W. W. Smith: Minimal zero sequences and the strong Davenport constant. Discr. Math. 203 (1999), 271–277.

[4] R. B. Eggleton, P. Erdős: Two combinatorial problems in group theory. Acta Arithmetica 21 (1972), 111–116.

[5] P. Erdős, A. Ginzburg, A. Ziv: A theorem in additive number theory. Bull. Res. Council Israel 10F (1961), 41–43.

[6] Y. O. Hamidoune, G. Zémor: On zero-free subset sums. Acta Arithm. 78 (1996), 143–152.

[7] J. L. Lambert: Une borne pour les générateurs des solutions entières positives d'une équation diophantienne linéaire. C.R. Acad. Sci. Paris Série I, 305 (1987), 39–40.

[8] E. Noether: Der Endlichkeitssatz der Invarianten endlicher Gruppen. Math. Ann. 77 (1916), 89–92.

[9] J. E. Olson: An addition theorem modulo p. J. Comb. Theory 5 (1968), 45–52.

[10] J. E. Olson: Sums of sets of group elements. Acta Aritm. 28 (1975), 147–156.

[11] K. Pommerening: Remarks on subset sums. Online: `http://www.staff.uni-mainz.de/pommeren/MathMisc/SubSum.pdf`

[12] K. Pommerening: The indecomposable solutions of linear congruences. Preprint online as arXiv:1703.03708 [math.NT]: `http://arxiv.org/abs/1703.03708`.

[13] K. Pommerening: The indecomposable solutions of linear Diophantine equations. Online: `http://www.staff.uni-mainz.de/pommeren/MathMisc/LinDio.pdf`

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

[15] M. F. Tinsley: A combinatorial theorem in number theory. Duke Math. J. 33 (1966), 75–79.