Separating Noether number of finite abelian groups

Schefler Barna

Eötvös Loránd University, Budapest
supervisor: Domokos Mátyás, Rényi Institute, Budapest

Groups and their actions: algebraic, geometric and combinatorial aspects
June 3–7, 2024 Levico Terme

Outline

Outline

1. Invariant theory
2. Zero-sum sequences over finite abelian groups
3. Some new results

Suppose that a finite group G acts on a finite dimensional $\mathbb{C}$-vector space V via linear transformations. Let $x_1, x_2, \dots, x_n$ be a basis of the dual space V^*. Then we have a G-action on the coordinate ring $\mathbb{C}[V] = \mathbb{C}[x_1, \dots, x_n]$:

$$\text{for } \sigma \in G \text{ and } f \in \mathbb{C}[V] \text{ we have: } \sigma \cdot f(x_1, x_2, \dots, x_n) = f(\sigma \cdot x_1, \sigma \cdot x_2, \dots, \sigma \cdot x_n)$$

Suppose that a finite group G acts on a finite dimensional $\mathbb{C}$-vector space V via linear transformations. Let $x_1, x_2, \ldots, x_n$ be a basis of the dual space V^*. Then we have a G-action on the coordinate ring $\mathbb{C}[V] = \mathbb{C}[x_1, \ldots, x_n]$:

$$\text{for } \sigma \in G \text{ and } f \in \mathbb{C}[V] \text{ we have: } \sigma \cdot f(x_1, x_2, \ldots, x_n) = f(\sigma \cdot x_1, \sigma \cdot x_2, \ldots, \sigma \cdot x_n)$$

The invariant subalgebra $\mathbb{C}[V]^G := \{f \in \mathbb{C}[V] : \sigma \cdot f = f, \text{ for } \forall \sigma \in G\}$ is generated by homogeneous polynomials of degree $\leq |G|$ by a theorem of Noether. This motivates the definition of the *Noether number*: denote by $\beta(G, V)$ the maximal degree in a minimal homogeneous generating system of the algebra $\mathbb{C}[V]^G$.

$$\beta(G) = \sup_V \{\beta(G, V) |\ V \text{ finite dimensional}\}$$

Suppose that a finite group G acts on a finite dimensional $\mathbb{C}$-vector space V via linear transformations. Let $x_1, x_2, \dots, x_n$ be a basis of the dual space V^*. Then we have a G-action on the coordinate ring $\mathbb{C}[V] = \mathbb{C}[x_1, \dots, x_n]$:

$$\text{for } \sigma \in G \text{ and } f \in \mathbb{C}[V] \text{ we have: } \sigma \cdot f(x_1, x_2, \dots, x_n) = f(\sigma \cdot x_1, \sigma \cdot x_2, \dots, \sigma \cdot x_n)$$

The invariant subalgebra $\mathbb{C}[V]^G := \{f \in \mathbb{C}[V] : \sigma \cdot f = f, \text{ for } \forall \sigma \in G\}$ is generated by homogeneous polynomials of degree $\leq |G|$ by a theorem of Noether. This motivates the definition of the *Noether number*: denote by $\beta(G, V)$ the maximal degree in a minimal homogeneous generating system of the algebra $\mathbb{C}[V]^G$.

$$\beta(G) = \sup_V \{\beta(G, V) | \ V \text{ finite dimensional}\}$$

A subset $S \subset \mathbb{C}[V]^G$ is called *separating set* if the following holds:

$$\text{if for } v_1, v_2 \in V \text{ there exists } h \in \mathbb{C}[V]^G \text{ such that } h(v_1) \neq h(v_2), \text{ then there exists } f \in S, \text{ such that } f(v_1) \neq f(v_2)$$

A subset $S \subset \mathbb{C}[V]^G$ is called *separating set* if the following holds:

if for $v_1, v_2 \in V$ there exists $h \in \mathbb{C}[V]^G$ such that $h(v_1) \neq h(v_2)$, then there exists $f \in S$, such that $f(v_1) \neq f(v_2)$

If G is a *finite* group, then a subset $S \subset \mathbb{C}[V]^G$ is a *separating set* if and only if:

$Gv_1 \neq Gv_2$ implies the existence of an $f \in S$, such that $f(v_1) \neq f(v_2)$

A subset $S \subset \mathbb{C}[V]^G$ is called *separating set* if the following holds:

if for $v_1, v_2 \in V$ there exists $h \in \mathbb{C}[V]^G$ such that $h(v_1) \neq h(v_2)$, then there exists $f \in S$, such that $f(v_1) \neq f(v_2)$

If G is a *finite* group, then a subset $S \subset \mathbb{C}[V]^G$ is a *separating set* if and only if:

$Gv_1 \neq Gv_2$ implies the existence of an $f \in S$, such that $f(v_1) \neq f(v_2)$

Definition

Let $\beta_{sep}(G, V)$ be the minimal positive integer d such that $\mathbb{C}[V]^G$ contains a separating set whose elements are homogeneous polynomials of degree at most d. The separating Noether number $\beta_{sep}(G)$ of a finite group G is

$$\beta_{sep}(G) := \sup_V \{\beta_{sep}(G, V) : V \text{ finite dimensional}\}$$

A subset $S \subset \mathbb{C}[V]^G$ is called *separating set* if the following holds:

if for $v_1, v_2 \in V$ there exists $h \in \mathbb{C}[V]^G$ such that $h(v_1) \neq h(v_2)$, then there exists $f \in S$, such that $f(v_1) \neq f(v_2)$

If G is a *finite* group, then a subset $S \subset \mathbb{C}[V]^G$ is a *separating set* if and only if:

$Gv_1 \neq Gv_2$ implies the existence of an $f \in S$, such that $f(v_1) \neq f(v_2)$

Definition

Let $\beta_{sep}(G, V)$ be the minimal positive integer d such that $\mathbb{C}[V]^G$ contains a separating set whose elements are homogeneous polynomials of degree at most d. The separating Noether number $\beta_{sep}(G)$ of a finite group G is

$$\beta_{sep}(G) := \sup_V \{\beta_{sep}(G, V) : V \text{ finite dimensional}\}$$

Properties

- $\beta(G, V) \leq \beta(G, V + V')$
- $\beta(G, V_{reg}) = \beta(G)$
- if $H \leq G$, then $\beta(H) \leq \beta(G)$
- $\beta(G) \leq |G|$.

The same facts are also true for β_{sep}.

- $\beta_{sep}(G, V) \leq \beta(G, V)$, hence
- $\beta_{sep}(G) \leq \beta(G)$

Example

Let $\mathbb{C}[V] = \mathbb{C}[x, y]$, $G := C_3 = \langle \sigma \rangle$ *and* $\sigma \mapsto \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}$, *(*$\omega$ *third root of unity).*

Example

Let $\mathbb{C}[V] = \mathbb{C}[x, y]$, $G := C_3 = \langle\sigma\rangle$ *and* $\sigma \mapsto \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}$, *(*$\omega$ *third root of unity).*

For $f(x, y) = \sum a_{ij} x^i y^j \in \mathbb{C}[x, y]$, *we have* $\sigma \cdot f(x, y) = \sum a_{ij} \omega^{i-j} x^i y^j$.
$\mathbb{C}[V]^{C_3} = \mathbb{C}[x^3, y^3, xy]$, *so* $\beta(C_3, V) = 3$.

Example

Let $\mathbb{C}[V] = \mathbb{C}[x,y]$, $G := C_3 = \langle\sigma\rangle$ *and* $\sigma \mapsto \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}$, *(*$\omega$ *third root of unity).*

For $f(x,y) = \sum a_{ij}x^iy^j \in \mathbb{C}[x,y]$, *we have* $\sigma \cdot f(x,y) = \sum a_{ij}\omega^{i-j}x^iy^j$.
$\mathbb{C}[V]^{C_3} = \mathbb{C}[x^3, y^3, xy]$, *so* $\beta(C_3, V) = 3$.
Separating set with invariants of deg at most 2? Only possibility: $S = \{xy\}$. *This is not a separating set:* $(1,1)$ *and* $(\frac{1}{2}, 2)$ *are not separated, but are in different orbits. So* $\beta_{sep}(C_3, V) > 2$, *and* $\beta_{sep}(C_3, V) \leq \beta(C_3, V) = 3$, *hence* $\beta_{sep}(C_3, V) = 3$.
($\{x^3, y^3, xy\}$ *is a separating set.)*

Example

Let $\mathbb{C}[V] = \mathbb{C}[x,y]$, $G := C_3 = \langle \sigma \rangle$ *and* $\sigma \mapsto \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}$, *(*$\omega$ *third root of unity).*

For $f(x,y) = \sum a_{ij} x^i y^j \in \mathbb{C}[x,y]$, *we have* $\sigma \cdot f(x,y) = \sum a_{ij} \omega^{i-j} x^i y^j$.
$\mathbb{C}[V]^{C_3} = \mathbb{C}[x^3, y^3, xy]$, *so* $\beta(C_3, V) = 3$.
Separating set with invariants of deg at most 2? Only possibility: $S = \{xy\}$. *This is not a separating set:* $(1,1)$ *and* $(\frac{1}{2}, 2)$ *are not separated, but are in different orbits. So* $\beta_{sep}(C_3, V) > 2$, *and* $\beta_{sep}(C_3, V) \leq \beta(C_3, V) = 3$, *hence* $\beta_{sep}(C_3, V) = 3$.
($\{x^3, y^3, xy\}$ *is a separating set.)*

In general:

Theorem (B. Schmid, 1990)

$\beta_{sep}(C_n) = \beta(C_n) = n$. *Moreover for any noncyclic finite group* G: $\beta(G) < |G|$.

Outline

Question

Our goal is to determine the exact value of the separating Noether number of some infinite families of abelian groups.

Question

Our goal is to determine the exact value of the separating Noether number of some infinite families of abelian groups.

Fact

For a finite abelian group $\beta(G) = \mathsf{D}(G)$

Let $g_1, \ldots, g_k$ be distinct elements of the (additively written) finite abelian group G.

$$\mathcal{G}(g_1, \ldots, g_k) := \{[m_1, \ldots, m_k] \in \mathbb{Z}^k : \sum_{i=1}^{k} m_i g_i = 0 \in G\}$$

is a subgroup of the additive group of $\mathbb{Z}^k$. The *block monoid* is defined as:

$$\mathcal{B}(g_1, \ldots, g_k) := \mathbb{N}^k \cap \mathcal{G}(g_1, \ldots, g_k)$$

Let $g_1, \dots, g_k$ be distinct elements of the (additively written) finite abelian group G.

$$\mathcal{G}(g_1, \dots, g_k) := \{[m_1, \dots, m_k] \in \mathbb{Z}^k : \sum_{i=1}^k m_i g_i = 0 \in G\}$$

is a subgroup of the additive group of $\mathbb{Z}^k$. The *block monoid* is defined as:

$$\mathcal{B}(g_1, \dots, g_k) := \mathbb{N}^k \cap \mathcal{G}(g_1, \dots, g_k)$$

If $g_1, \dots, g_k$ is an enumeration of all the elements of G, then $\mathcal{B}(G) := \mathcal{B}(g_1, \dots, g_k)$. The *length* of an element $\mathrm{m} = [m_1, \dots, m_k] \in \mathcal{B}(g_1, \dots, g_k)$ is $|\mathrm{m}| = \sum_{i=1}^k m_i$.

Let $g_1, \ldots, g_k$ be distinct elements of the (additively written) finite abelian group G.

$$\mathcal{G}(g_1, \ldots, g_k) := \{[m_1, \ldots, m_k] \in \mathbb{Z}^k : \sum_{i=1}^k m_i g_i = 0 \in G\}$$

is a subgroup of the additive group of $\mathbb{Z}^k$. The *block monoid* is defined as:

$$\mathcal{B}(g_1, \ldots, g_k) := \mathbb{N}^k \cap \mathcal{G}(g_1, \ldots, g_k)$$

If $g_1, \ldots, g_k$ is an enumeration of all the elements of G, then $\mathcal{B}(G) := \mathcal{B}(g_1, \ldots, g_k)$. The *length* of an element $\mathrm{m} = [m_1, \ldots, m_k] \in \mathcal{B}(g_1, \ldots, g_k)$ is $|\mathrm{m}| = \sum_{i=1}^k m_i$.

Remark

- *we do not care about the order about in which the elements are written in* $\mathcal{B}(g_1, \ldots, g_k)$
- *the neutral element* 0 *can be omitted*

Definition

An element of $\mathcal{B}(g_1, \ldots, g_k)$ is an atom, if it can not be written as the sum of two non-zero elements of $\mathcal{B}(g_1, \ldots, g_k)$.

The maximal length of an atom in $\mathcal{B}(G)$ is the *Davenport constant* $\mathrm{D}(G)$ of the group.

Definition

An element of $\mathcal{B}(g_1, \ldots, g_k)$ is an atom*, if it can not be written as the sum of two non-zero elements of $\mathcal{B}(g_1, \ldots, g_k)$.*

The maximal length of an atom in $\mathcal{B}(G)$ is the *Davenport constant* $\mathrm{D}(G)$ of the group. Let $G = C_{n_1} \oplus C_{n_2} \oplus \cdots \oplus C_{n_r}$, where $2 \leq n_r \mid n_{r-1} \mid \cdots \mid n_1$. Let ε_i be a genarator of C_{n_i}, and introduce the notation $\varepsilon := \sum_{i=1}^{r} \varepsilon_i$. Then

$\varepsilon + \sum_{i=1}^{r}(n_i - 1)\varepsilon_i = 0 \in G$, hence $[1, n_1 - 1, ..., n_r - 1] \in \mathcal{B}(\varepsilon, \varepsilon_1, ..., \varepsilon_r)$ is an atom

So for any abelian group G, $\sum_{i=1}^{r}(n_i - 1) + 1 \leq \mathrm{D}(G)$.

Definition

An element of $\mathcal{B}(g_1, \dots, g_k)$ is an atom, if it can not be written as the sum of two non-zero elements of $\mathcal{B}(g_1, \dots, g_k)$.

The maximal length of an atom in $\mathcal{B}(G)$ is the *Davenport constant* $\mathsf{D}(G)$ of the group. Let $G = C_{n_1} \oplus C_{n_2} \oplus \cdots \oplus C_{n_r}$, where $2 \leq n_r \mid n_{r-1} \mid \cdots \mid n_1$. Let ε_i be a genarator of C_{n_i}, and introduce the notation $\varepsilon := \sum_{i=1}^r \varepsilon_i$. Then

$\varepsilon + \sum_{i=1}^r (n_i - 1)\varepsilon_i = 0 \in G$, hence $[1, n_1 - 1, ..., n_r - 1] \in \mathcal{B}(\varepsilon, \varepsilon_1, ..., \varepsilon_r)$ is an atom

So for any abelian group G, $\sum_{i=1}^r (n_i - 1) + 1 \leq \mathsf{D}(G)$.

Theorem (J. Olson, 1969)

(i) *If $G = C_{n_1} \oplus C_{n_2}$ is finite abelian group of rank two, then* $\mathsf{D}(G) = n_1 + n_2 - 1$

(ii) *If G is a finite abelian p-group, then* $\mathsf{D}(G) = \sum_{i=1}^r (n_i - 1) + 1$

Example

Let us have $G = C_2 \oplus C_2$*, and denote by* $\{0, a, b, c\}$ *the elements of the group.*

Example

Let us have $G = C_2 \oplus C_2$, *and denote by* $\{0, a, b, c\}$ *the elements of the group.*

$a + a = 0$, *hence* $\mathrm{m}_1 = [2, 0, 0] \in \mathcal{B}(a, b, c)$ *with* $|\mathrm{m}_1| = 2$

$b + b = 0$, *hence* $\mathrm{m}_2 = [0, 2, 0] \in \mathcal{B}(a, b, c)$ *with* $|\mathrm{m}_2| = 2$

$c + c = 0$, *hence* $\mathrm{m}_3 = [0, 0, 2] \in \mathcal{B}(a, b, c)$ *with* $|\mathrm{m}_3| = 2$

$a + b + c = 0$, *hence* $\mathrm{m}_4 = [1, 1, 1] \in \mathcal{B}(a, b, c)$ *with* $|\mathrm{m}_4| = 3$

Of course, the maximal length of the atoms is 3, *so* $\mathrm{D}(G) = 3$.

$$\beta(G) = D(G) \longleftrightarrow \text{max length of atoms in } \mathcal{B}(G)$$
$$\beta_{sep}(G) \longleftrightarrow ?$$

$$\beta(G) = D(G) \longleftrightarrow \text{max length of atoms in } \mathcal{B}(G)$$
$$\beta_{sep}(G) \longleftrightarrow ?$$

Definition

An element of $\mathcal{B}(g_1, \dots, g_k)$ is an atom, if it can not be written as the sum of two non-zero elements of $\mathcal{B}(g_1, \dots, g_k)$.

$$\beta(G) = D(G) \longleftrightarrow \text{max length of atoms in } \mathcal{B}(G)$$
$$\beta_{sep}(G) \longleftrightarrow ?$$

Definition

An element of $\mathcal{B}(g_1, \ldots, g_k)$ is an atom, if it can not be written as the sum of two non-zero elements of $\mathcal{B}(g_1, \ldots, g_k)$.

Definition

A group atom in $\mathcal{B}(g_1, \ldots, g_k)$ is such an element m, that can not be written as an integral linear combination of elements of $\mathcal{B}(g_1, \ldots, g_k)$ that have length strictly smaller than $|\mathrm{m}|$.

Example

Let $G = C_{12} \oplus C_4$, *and* $[11, 1, 3] \in \mathcal{B}(\varepsilon_1, \varepsilon_1 + \varepsilon_2, \varepsilon_2)$.

Example

Let $G = C_{12} \oplus C_4$*, and* $[11,1,3] \in \mathcal{B}(\varepsilon_1, \varepsilon_1+\varepsilon_2, \varepsilon_2)$*.*
If $[11,1,3]$ *is the sum of two elements of the monoid, then one of them must have* 0 *in the second coordinate:* $[m_1, 0, m_3] \in \mathcal{B}(\varepsilon_1, \varepsilon_1+\varepsilon_2, \varepsilon_2)$*, so* $m_1\varepsilon_1 + m_3\varepsilon_2 = 0 \in G$*.*
Hence $12 = \mathrm{ord}(\varepsilon_1)|m_1$ *and* $4 = \mathrm{ord}(\varepsilon_2)|m_3$*, and then* $m_1 = m_3 = 0$*, since* $m_1 \leq 11$*,* $m_3 \leq 3$*. So* $[11,1,3]$ *is an atom in* $\mathcal{B}(\varepsilon_1, \varepsilon_1+\varepsilon_2, \varepsilon_2)$*.*

Example

Let $G = C_{12} \oplus C_4$*, and* $[11,1,3] \in \mathcal{B}(\varepsilon_1, \varepsilon_1+\varepsilon_2, \varepsilon_2)$.
If $[11,1,3]$ *is the sum of two elements of the monoid, then one of them must have* 0 *in the second coordinate:* $[m_1, 0, m_3] \in \mathcal{B}(\varepsilon_1, \varepsilon_1+\varepsilon_2, \varepsilon_2)$*, so* $m_1\varepsilon_1 + m_3\varepsilon_2 = 0 \in G$.
Hence $12 = \mathrm{ord}(\varepsilon_1) | m_1$ *and* $4 = \mathrm{ord}(\varepsilon_2) | m_3$*, and then* $m_1 = m_3 = 0$*, since* $m_1 \leq 11$, $m_3 \leq 3$*. So* $[11,1,3]$ *is an atom in* $\mathcal{B}(\varepsilon_1, \varepsilon_1+\varepsilon_2, \varepsilon_2)$.
It is not a group atom, since it can be written as an integral linear combination of such elements of $\mathcal{B}(\varepsilon_1, \varepsilon_1+\varepsilon_2, \varepsilon_2)$ *that have length strictly smaller than* $11+1+3=15$*:*
$[11,1,3] = 7[5,7,1] - 2[12,0,0] - 4[0,12,0] - [0,0,4]$.

Theorem [M. Domokos, 2017]

The number $\beta_{sep}(G)$ is the maximal length of a group atom in $\mathcal{B}(g_1, \dots, g_k)$, where $\{g_1, \dots, g_k\}$ ranges over all subsets of size $k \leq \mathrm{rank}(G) + 1$ of the abelian group G.

$$\beta(G) \longleftrightarrow \text{max length of atoms in } \mathcal{B}(G)$$
$$\beta_{sep}(G) \longleftrightarrow \text{max length of the group atoms in any of the listed block monoids}$$

Outline

1. Invariant theory
2. Zero-sum sequences over finite abelian groups
3. Some new results

For any abelian group G, $\sum_{i=1}^{r}(n_i - 1) + 1 \leq \mathrm{D}(G)$

For any abelian group G, $\sum_{i=1}^{r}(n_i - 1) + 1 \leq \mathsf{D}(G)$
A finite abelian group of rank 2 can be written in the form $G = C_{n\ell} \oplus C_n$, where $\ell \geq 1$.

Theorem [J. Olson, 1969]

$\mathsf{D}(C_{n\ell} \oplus C_n) = n\ell + n - 1.$

For any abelian group G, $\sum_{i=1}^{r}(n_i - 1) + 1 \leq \mathrm{D}(G)$

A finite abelian group of rank 2 can be written in the form $G = C_{n\ell} \oplus C_n$, where $\ell \geq 1$.

Theorem [J. Olson, 1969]

$\mathrm{D}(C_{n\ell} \oplus C_n) = n\ell + n - 1.$

Theorem [S., 2023]

Let ℓ, n be positive integers and denote with p the minimal prime divisor of n. Then:

$$\beta_{sep}(C_{n\,\ell} \oplus C_n) = n\,\ell + \frac{n}{p}$$

Theorem [S., 2023]

For positive integers $n \geq 2$ and r denote by C_n^r the direct sum $C_n \oplus \cdots \oplus C_n$ of r copies of the cyclic group C_n of order n, and let p be the minimal prime divisor of n. Then we have

$$\beta_{sep}(C_n^r) = \begin{cases} ns, & \text{if } r = 2s-1 \text{ is odd} \\ ns + \frac{n}{p}, & \text{if } r = 2s \text{ is even.} \end{cases}$$

Theorem [S., 2023]

For positive integers $n \geq 2$ and r denote by C_n^r the direct sum $C_n \oplus \cdots \oplus C_n$ of r copies of the cyclic group C_n of order n, and let p be the minimal prime divisor of n. Then we have

$$\beta_{sep}(C_n^r) = \begin{cases} ns, & \text{if } r = 2s - 1 \text{ is odd} \\ ns + \frac{n}{p}, & \text{if } r = 2s \text{ is even.} \end{cases}$$

Conjecture

For the direct sum C_n^r of r copies of the cyclic group of order n: $D(C_n^r) = 1 + (n-1)r$

- B. Schefler: The separating Noether number of the direct sum of several copies of a cyclic group, https://doi.org/10.48550/arXiv.2311.09903
- B. Schefler: The separating Noether number of abelian groups of rank two, https://doi.org/10.48550/arXiv.2403.13200

Thank you for your attention!