Connections between zero-sum theory and invariant theory

Cziszter Kálmán

Rényi Institute of Mathematics
Budapest

Combinatorial and Additive Number theory
Graz, January 5, 2016

The ring of polynomial invariants

- Let G be a finite group and V an n-dimensional G-module i.e. a homomorphism $\rho : G \to M_n(\mathbb{C})$ is given.
- This also induces an action of G on the polynomial ring $\mathbb{C}[V] := \mathbb{C}[x_1, ..., x_n]$ through linear substitutions:

$$(g \cdot f)(x_1, ..., x_n) = f(\rho(g^{-1})(x_1, ..., x_n)) \qquad g \in G, f \in \mathbb{C}[V]$$

- The ring of polynomial invariants is defined as:

$$\mathbb{C}[V]^G := \{f \in \mathbb{C}[V] : g \cdot f = f \text{ for all } g \in G\}$$

- E.g. the symmetric group S_n acts by permuting the variables:

$$\sigma \cdot x_i = x_{\sigma(i)} \qquad \sigma \in S_n.$$

Here $\mathbb{C}[V]^{S_n}$ is the ring of symmetric polynomials.

The Noether number

Hilbert proved that $\mathbb{C}[V]^G$ is a finitely generated algebra.
Noether gave an upper bound on the degree of the generators:

Definition

$\beta(G,V) = \min\{s \in \mathbb{N} : \mathbb{C}[V]^G \text{ is generated by } \oplus_{d=0}^{s} \mathbb{C}[V]_d^G\}$
$\beta(G) = \sup\{\beta(G,V) : V \text{ is a } G\text{-module over } \mathbb{C}\}$

Theorem (Noether 1916)

$\beta(G) \leq |G|$

Theorem (CzK-Domokos, 2013)

The inequality $\beta(G) \geq \frac{1}{2}|G|$ holds if and only if G contains a cyclic subgroup of index at most 2 (or G is one of four particular groups).

The case of Abelian groups

If G is abelian then all irreducible G-modules are 1-dimensional.
$\Rightarrow$ In a suitable basis each element of A acts by diagonal matrices.
$\Rightarrow$ The variables in $\mathbb{C}[V] = \mathbb{C}[x_1, ..., x_n]$ can be chosen so that :

$$a \cdot x_i = \theta_i(a) x_i \quad \text{for each } a \in A$$

where the character $\theta_i \in \mathrm{Hom}(A, \mathbb{C}^\times)$ is called the *weight* of x_i.

monomial $x_1^{e_1} \cdots x_n^{e_n}$	$\leftrightarrow$	sequence of the weights
monomials spanning $\mathbb{C}[V]^A$	$\leftrightarrow$	zero-sum sequences over A
generators of $\mathbb{C}[V]^A$	$\leftrightarrow$	minimal zero-sum sequences
Noether number $\beta(A)$	$\leftrightarrow$	Davenport constant $\mathsf{D}(A)$

Main question

How can we extend this nice correspondence between invariants and zero-sum sequences to the case of non-commutative groups?

Let G be a finite group with an abelian normal subgroup $A \triangleleft G$.

$$\mathbb{C}[x_1, ..., x_n]^A = \mathbb{C}[m_1, ..., m_k]$$

for some monomials m_i. The factor group G/A acts on them, so

$$\mathbb{C}[x_1, ..., x_n]^G = \mathbb{C}[m_1, ..., m_k]^{G/A}$$

If $G/A \cong B$ happens to be abelian, too, then the questions about invariants of G are reduced to questions about zero-sum sequences over A and B plus the way in which they interact.

Theorem (Reduction lemmas)

Let G be metabelian, i.e. $G/A \cong B$ for abelian groups A, B. Then

$$\beta(G) \geq \mathsf{D}(A) + \mathsf{D}(B) - 1 \tag{1}$$

$$\beta(G) \leq \mathsf{D}_{\mathsf{D}(B)}(A) \tag{2}$$

(Here D_k is the maximal length of a zero-sum sequence that cannot be factored into more than k parts.)

Sketch of proof for (2):
$\mathbb{C}[m_1, ..., m_k]^{G/A}$ is generated by polynomials $p(m_1, ..., m_k)$ with $\deg(p) \leq \mathsf{D}(G/A)$. So if an A-invariant monomial m has a factorisation $m = m_1 \cdots m_s$ with $s = \mathsf{D}(B)$ then m cannot occur in any generator of $\mathbb{C}[x_1, ..., x_n]^G$. But such a factorisation into $s = \mathsf{D}(B)$ parts always exists when $\deg(m) > \mathsf{D}_s(A)$.

Orbit sums

Let m be an A-invariant monomial and define the orbit-sum

$$\tau(m) := \sum_{b \in G/A} b \cdot m.$$

Then $\tau(m)$ is G-invariant and $\mathbb{C}[V]^G$ is spanned by such elements.
($\Rightarrow$ So instead of zero-sum sequences we work with *orbits* of them)

An invariant $f \in \mathbb{C}[V]^G$ is *decomposable* if $f = \sum_i c_i \tau(u_i)\tau(v_i)$.
$\beta(G, V) =$ the maximal degree of an indecomposable invariant.

Our strategy:

try to characterise the weight sequence of those monomials m for which $\tau(m)$ is an indecomposable invariant.

Example: (generalised) dihedral groups

Let $G = A \rtimes_{-1} C_2$ where A is an abelian group, and the generator of C_2 acts on the elements of A by sending them into their inverses.

Definition

If E, F, G are non-empty sequences over A and such that EF and EG are zero-sum sequences then $S := EFG$ is called *a zero-corner*.

Theorem

- *If $\tau(m)$ is indecomposable then the weight sequence S of the monomial m cannot contain a zero-corner.*
- *If $|S| \geq \mathsf{D}(A) + 2$ then S contains a zero-corner.*
- *As a result*

$$\beta(A \rtimes_{-1} C_2) = \mathsf{D}(A) + 1$$

Extremal invariants

Definition

We say that an invariant $f \in \mathbb{C}[V]^G$ is extremal if it is indecomposable of maximal degree, i.e. $\deg(f) = \beta(G, V)$.

Extremal invariants usually exhibit nice structural properties. E.g.:

Theorem

For a dihedral group $G = C_n \rtimes_{-1} C_2$ an invariant $\tau(m)$ is extremal if and only if the weight sequence of m is $(0, e^n)$ where $\langle e \rangle = C_n$.

Groups with a cyclic subgroup of index two I.

In general consider the group $C_{nm} \rtimes C_2$ where n, m are coprime and C_2 acts by inversion on C_n while it acts trivially on C_m.

Question:
can we reduce the case of this group G to the dihedral group?

Definition

Let S be a sequence over C_{nm} and $S = S_1 \cdots S_k$ a factorisation such that the sum $\sigma(S_i)$ belongs to C_n for all i. Then the sequence $(\sigma(S_1), ..., \sigma(S_k))$ will be called a C_n-*contraction* of S.

Definition

We say that $f, g \in \mathbb{C}[V]^G$ are *equivalent* if $f - g$ is decomposable.

In our case the equivalence of invariants $\tau(u)$ and $\tau(v)$ can also be formulated in terms of the corresponding weight sequences U, V.

Groups with a cyclic subgroup of index two II.

Theorem (Lifting)

Let U be a sequence over C_{nm} such that any C_n-contraction of any equivalent sequence V is of the form $(0, e^n)$ where $\langle e \rangle = C_n$. Then necessarily $U = (0, f^{nm})$ where $\langle f \rangle = C_{nm}$.

The above result had a key role in proving the following theorem:

Theorem (CzK-Domokos, 2012)

If G is a non-cyclic group with a cyclic subgroup of index two then

$$\beta(G) = \frac{1}{2}|G| + \begin{cases} 2 & \text{if } G = Dic_{4n},\ n > 1 \\ 1 & \text{otherwise} \end{cases}$$

(Dic_{4n} is the dicyclic group, e.g. a generalised quaternion group).

The non-abelian group of order pq for some primes p, q

Let $G = C_p \rtimes C_q$ where $q \mid p-1$. Here C_q acts on $C_p \cong \mathbb{Z}/p\mathbb{Z}$ by multiplication with a primitive q-th root of unit modulo p.

Conjecture (Pawale)

$$\beta(C_p \rtimes C_q) = p + q - 1$$

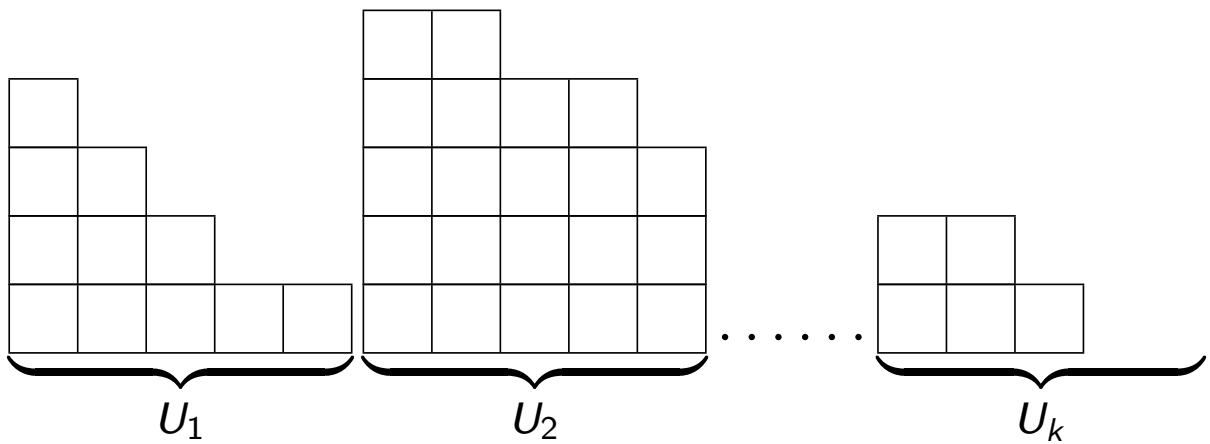
This is proven so far only for $q = 2$ and $q = 3$. For the rest we only have estimates.

Gapless sequences

Let $\{0\}\dot\cup U_1\dot\cup\cdots\dot\cup U_k$ be the decomposition of C_p into C_q-orbits. In a given sequence S let $\mathrm{v}_{i,1}\geq\mathrm{v}_{i,2}\geq\cdots\geq\mathrm{v}_{i,q}\geq 0$ denote the multiplicities of the elements belonging to U_i for every $i=1,\ldots,k$.

We say that S is *gapless* if for all i,j it holds that

$$\mathrm{v}_{i,j}-\mathrm{v}_{i,j+1}\leq 1.$$



Theorem

Let $\gamma(p, q)$ be the maximal length of a gapless zero-sum sequence over C_p which cannot be factored into more than $q - 2$ non-empty zero-sum subsequences. Then we have:

$$\beta(C_p \rtimes C_q) \leq p + 1 + \gamma(p, q)$$

Questions (conjectures)

Is there an upper bound on $\gamma(p, q)$ which is independent of q?
Is it true that $\gamma(p, q) < 2p$?
(This is already proven for the case when $p > q^2$.)

The Heisenberg group of order p^3

The Heisenberg group H has a normal subgroup $A \cong C_p \times C_p$ such that $H/A \cong C_p = \langle g \rangle$. From our reduction Lemma we get

$$\beta(H) \leq \mathsf{D}_p(C_p \times C_p) = p^2 + p - 1$$

But the structure of those zero-sum sequences over $C_p \times C_p$ which have length $p^2 + p - 1$ and cannot be factored into $p + 1$ part is known (Gao-Geroldinger). Using this we obtained:

Theorem

- *If u, v are monomials with weight sequences $U = U_1 \cdots U_p$, $V = g(U_1)g^{-1}(U_2) \cdots U_p$ then $\tau(u)$ and $\tau(v)$ are equivalent*
- *Any $\tau(u)$ with degree $p^2 + p - 1$ is equivalent to a $\tau(v)$ such that the weight sequence V of v factors into $p + 1$ parts*
- *As a result $\beta(H) < p^2 + p - 1$*

The small and large Davenport number

Definition

The sequence $(g_1, ..., g_n)$ over G is a *product-one sequence* if $g_{\sigma(1)}g_{\sigma(2)} \cdots g_{\sigma(n)} = 1$ for a permutation $\sigma \in S_n$.

$\mathsf{d}(G)$ is the maximal integer d such that there is a sequence over G of length d which has no nontrivial, product-one subsequence.

$\mathsf{D}(G)$ is the maximal length of a minimal product-one sequence.

Conjecture (Geroldinger-Grynkiewicz)

$$\mathsf{d}(G) + 1 \leq \beta(G) \leq \mathsf{D}(G)$$

This holds true for all the cases where the values of these constants are known so far. However, an invariant theoretic interpretation of $\mathsf{d}(G)$ and $\mathsf{D}(G)$ is still missing

References

1. K. Cziszter, M. Domokos: *Groups with large Noether bound*, Ann. de l'Institut Fourier 64:(3) pp. 909-944. (2014)

2. K. Cziszter, M. Domokos: *The Noether number for the groups with a cyclic subgroup of index two*, Journal of Algebra 399: pp. 546-560. (2014)

3. K. Cziszter, M. Domokos: *On the generalized Davenport constant and the Noether number*, Central European Journal of Mathematics 11:(9) pp. 1605-1615. (2013)

4. K. Cziszter: *The Noether number of the non-abelian group of order 3p*, Periodica Math. Hung. 68:(2) pp. 150-159. (2014)

5. K. Cziszter, M. Domokos, A. Geroldinger: *The interplay of Invariant Theory with Multiplicative Ideal Theory and with Arithmetic Combinatorics*, arXiv:1505.06059

Thank you for your attention!