# Symmetric polynomials over finite fields

B. Miklósi[1]

joint work with M. Domokos[2]

[1]Eötvös Loránd University Department of Algebra and Number Theory
[2]Alfréd Rényi Institute of Mathematics

June 06, 2024

# Table of Contents

# Table of Contents

# What is invariant theory?

- $k$ is any field, $V =$ alg. variety, $G =$ alg. group, consider an algebraic action of $G$ on $V$;
- induced action on the coordinate ring $k[V]$: $(g \cdot f)(v) = f(g^{-1} \cdot v)$;
- **invariant algebra**: $k[V]^G := \{f \in k[V] : g \cdot f = f \text{ for all } g \in G\}$;
- ex.: if $G = S_n$ and $V = k^n$, then the coordinate ring of $V$ is $k[x_1, ..., x_n]$ and the elementary symmetric polynomials $s_i$ (where $i \leq n$) are invariants, moreover $k[V]^G = k[s_1, ..., s_n]$;
- **question**: is $k[V]^G$ finitely generated as an algebra over $k$?

# History

- Hilbert (1890): the invariant algebras of linearly reductive groups (for ex. of the classical groups) are finitely generated $k$-algebras;
- Hilbert's fourteenth problem: is every invariant algebra finitely generated over $k$?
- NO, counterexample by Nagata (1959);

# Table of Contents

# Separating sets vs generating sets

- even if $k[V]^G$ is finitely generated in general it is a hard computational task to determine a generating set (involves Gröbner basis computation);
- we can investigate invariants from another point of view: by their separating properties;
- instead of seeking for generating (finite) subsets of $k[V]^G$ we consider sets of invariants which have exactly the same separating capabilities as the whole invariant algebra;
- every invariant algebra has a finite separating subset;

# Definition

- let $S \subset k[V]^G$, we say that elements $u, v \in V$ can be **separated** by $S$ if there exists an invariant $f \in S$ such that $f(u) \neq f(v)$;
- we call $S$ a **separating set** if for any $u, v \in V$ we have: if there exists an invariant $f \in k[V]^G$ with $f(u) \neq f(v)$, then there exists an element $g \in S$ with $g(u) \neq g(v)$;
- if $S \subset k[V]^G$ is a generating set then $S$ is a separating set;
- we say that a separating set
  - (i) is **minimal wrt. size** if it is of minimal size among the separating sets;
  - (ii) is **minimal wrt. inclusion** if no proper subset is separating;

# Table of Contents

# Kemper, Lopatin, Reimers

- [KLR22] is the first paper to systematically deal with separating invariants over finite fields;
- **main result**: they give an explicit formula for the number $\gamma$ of elements of a separating set of minimal size when $G$ is a matrix group over the finite field $\mathbb{F}_q$, namely if $k$ is the number of $G$-orbits then $\gamma = \gamma(q, k) := \lceil \log_q k \rceil$;
- fix: $G = S_n$ and $V = \mathbb{F}^n$ where $\mathbb{F} = \mathbb{F}_q$ is a finite field of $q = p^t$ elements;
- they proved that for $\mathbb{F} = \mathbb{F}_2$ the set

$$S = \{s_{2^r} : 0 \leq r \leq \lfloor \log_2 n \rfloor\}$$

form a separating set of minimal size in $k[x_1, ..., x_n]^{S_n}$;

# Over arbitrary finite fields

- we have managed to extend this result to arbitrary finite fields $\mathbb{F}_q$ in [DM23]:

**Theorem 1**

*The elementary symmetric polynomials $s_m$ with $m \in [n]_q$ form a separating subset in $\mathbb{F}_q[x_1, ..., x_n]^{S_n}$, where*

$$[n]_q = \{jp^k : j \in \{1, ..., q-1\},\ k \in \mathbb{Z}_{\geq 0},\ jp^k \leq n\}.$$

- we shall remark that the $p = q$ case was solved before in a different context by Aberth in 1964 [Ab64];

# An equivalent reformulation of *Theorem 1*

- there is an equivalent reformulation of *Theorem 1*:

**Theorem 1**

*Let $f, g \in \mathbb{F}_q[x]$ be monic polynomials of degree $n$, such that both $f$ and $g$ split as a product of root factors over $\mathbb{F}_q$. Assume that for all $j \in [n]_q$, the degree $n-j$ coefficients of $f$ and $g$ coincide. Then we have $f = g$.*

# Minimality

- the separating set given in *Theorem 1* is minimal with respect to inclusion for $q = 3, 4, 5$ wirth arbitrary $n$ and for $q = 7$ with $\log_7 n - \lfloor \log_7 n \rfloor < \log_7 5$ or $\log_7 n - \lfloor \log_7 n \rfloor \geq \log_7 6$;
- when $n = 5$ in $\{s_i : i = 1, 2, 3, 4\} \subset \mathbb{F}_7[x_1, ..., x_5]^{S_5}$ is minimal wrt. size ($\gamma = \log_q(\binom{q-1+k}{k}) = \log_7 462 = 4$);
- denote by $d_p(n)$ the difference $\mid [n]_p \mid$ and the number of elements in a separating set of minimal size (i.e. $\gamma$) in $\mathbb{F}_p[x_1, ..., x_n]$, then we have $d_p(n) \leq p - 2$ meaning that if $n$ is large compared to $p$ then the separating set given by *Theorem 1* is not much bigger than a separating set of minimal size;

# Table of Contents

# Key ingredients of the proof

- we can easily characterize $S_n$-orbits: for $v \in \mathbb{F}_q^n$ the orbit $S_n \cdot v$ can be described with a map $\mathcal{O} : \mathbb{F}_q \to \mathbb{Z}_{\geq 0}$ such that $\mathcal{O}(a) = \mid \{j : v_j = a\} \mid$, this is a bijection and we will refere to $S_n$-orbits as such kind of maps;
- we shall write $s_k(\mathcal{O})$ for the value of the elementary symmetric polynomial $s_k \in \mathbb{F}_q[x_1, ..., x_n]$ on the vectors in $\mathbb{F}_q^n$ that belong to the orbit labelled by $\mathcal{O}$;

# Key ingredients of the proof

- we will need the following lemmas:

## Lemma 2

*Let $\mathcal{O}, \mathcal{P}$ be $S_n$-orbits and assume that*

$$s_j(\mathcal{O}) = s_j(\mathcal{P}) \quad \text{for} \quad j = 1, 2, ..., q-1.$$

*Then $\mathcal{O}(a) \equiv \mathcal{P}(a) \bmod p$ for all $a \in \mathbb{F}_q$.*

## Lemma 3

*Suppose that for $\mathcal{O}, \mathcal{P}$ and for some $k$ we have $\mathcal{O}(a) \equiv \mathcal{P}(a) \bmod p^k$ for all $a \in \mathbb{F}_q$ and $s_{jp^k}(\mathcal{O}) = s_{jp^k}(\mathcal{P})$ for $j = 1, 2, ..., q-1$. Then $\mathcal{O}(a) \equiv \mathcal{P}(a) \bmod p^{k+1}$ for all $a \in \mathbb{F}_q$.*

# Outline of the proof

- let $\mathcal{O}, \mathcal{P}$ be arbitrary $S_n$-orbits and suppose that for all $j \in [n]_q$ we have $s_j(\mathcal{O}) = s_j(\mathcal{P})$;
- by *Lemma 2* and *Lemma 3* using an inductive argument on $k$ we get that $\mathcal{O}(a) \equiv \mathcal{P}(a) \bmod p^k$ for all $a \in \mathbb{F}_q$ and $k$;
- thus for large enough $k$ we get that $\mathcal{O} = \mathcal{P}$;

# Bibliography


O. Aberth.

The elementary symmetric functions in a finite field of prime order.

*Illinois J. Math. 8 (1) 132 - 138, 1964.*

M. Domokos, B.Miklósi.

Symmetric polynomials over finite fields.

*Finite Fields and Their Applications 89 (2023) 102224.*

G. Kemper, A. Lopatin, F. Reimers.

Separating invariants over finite fields.

*J. Pure Appl. Algebra 226 (2022) 106904.*

Thank you for your attention!