EPIsciences

Communications in Mathematics **33** (2025), no. 1, Paper no. 5
DOI: https://doi.org/10.46298/cm.14627

Separating symmetric polynomials over finite fields

Artem Lopatin, Pedro Antonio Muniz Martins and Lael Viana Lima

Abstract. The set $S(n)$ of all elementary symmetric polynomials in n variables is a minimal generating set for the algebra of symmetric polynomials in n variables, but over a finite field $\mathbb{F}_q$ the set $S(n)$ is not a minimal separating set for symmetric polynomials in general. We determine when $S(n)$ is a minimal separating set for the algebra of symmetric polynomials having the least possible number of elements.

Contents

MSC 2020: 13A50 (primary); 12E20 (secondary).
Keywords: Finite field, Symmetric group, Symmetric polynomials, Invariant theory, Separating invariants.
Contact information:
Artem Lopatin:
Affiliation: State University of Campinas, Brazil.
Email: dr.artem.lopatin@gmail.com
Pedro Antonio Muniz Martins:
Affiliation: State University of Campinas, Brazil.
Email: p242894@dac.unicamp.br
Lael Viana Lima:
Affiliation: State University of Campinas, Brazil.
Email: l176809@dac.unicamp.br

1 Introduction

1.1 Symmetric polynomials

Assume that $\mathbb{F}$ is an arbitrary field (finite or infinite) and denote by $\mathbb{F}_q$ the finite field of order q with the characteristic $p = \operatorname{char} \mathbb{F}_q$.

Consider an n-dimensional vector space V over a field $\mathbb{F}$ with a fixed basis, where $n \geq 2$. For $v \in V$ let v_i denote the i^{th}-coordinate with respect to this basis of V. The symmetric group $\mathcal{S}_n$ acts on V by permutations of the coordinates with respect to the fixed basis of V. Namely, for $\sigma \in \mathcal{S}_n$ and $v = (v_1, \dots, v_n) \in V$ we have $\sigma \cdot v = (v_{\sigma^{-1}(1)}, \dots, v_{\sigma^{-1}(n)})$. The coordinate ring $\mathbb{F}[V] = \mathbb{F}[x_1, \dots, x_n]$ of V is isomorphic to the symmetric algebra $S(V^*)$ over the dual space V^* with the dual basis $x_1, \dots, x_n$ to the fixed basis of V. The group $\mathcal{S}_n$ acts on the set $\{x_1, \dots, x_n\}$ by $\sigma \cdot x_i = x_{\sigma(i)}$ and this action is extended to the action of $\mathcal{S}_n$ on $\mathbb{F}[V]$. The algebra of $\mathcal{S}_n$-*invariants*

$$\mathbb{F}[V]^{\mathcal{S}_n} = \{f \in \mathbb{F}[V] \,|\, \sigma \cdot f = f \text{ for all } \sigma \in \mathcal{S}_n\}$$

is the algebra of symmetric polynomials. It is well known that the algebra $\mathbb{F}[V]^{\mathcal{S}_n}$ is minimally (with respect to inclusion) generated by the set

$$S(n) = \{s_t(x_1, \dots, x_n) \,|\, 1 \leq t \leq n\}$$

of all elementary symmetric polynomials $s_t(x_1, \dots, x_n) = \sum_{1 \leq i_1 < \dots < i_t \leq n} x_{i_1} \cdots x_{i_t}$.

Any element f of $\mathbb{F}[V]$ can be considered as a function $f : V \to \mathbb{F}$. Obviously, any $f \in \mathbb{F}[V]^{\mathcal{S}_n}$ has a constant value over every $\mathcal{S}_n$-orbit on V. Given a subset S of $\mathbb{F}[V]^{\mathcal{S}_n}$, we say that elements u, v of V *are separated by* S if there exists an invariant $f \in S$ with $f(u) \neq f(v)$. If $u, v \in V$ are separated by $\mathbb{F}[V]^{\mathcal{S}_n}$, then we simply say that they *are separated*. A subset $S \subset \mathbb{F}[V]^{\mathcal{S}_n}$ is called *separating* if for any u, v from V that are separated we have that they are separated by S. We say that a separating set is *minimal* if it is minimal with respect to inclusion. Obviously, any generating set is also separating. Minimal separating sets for different actions of groups were constructed in [2–4, 6–13].

In the case of an algebraically closed field $\mathbb{F}$ as well as in the case of $\mathbb{F} = \mathbb{R}$ the set $S(n)$ is a minimal separating set for $\mathbb{F}[V]^{\mathcal{S}_n}$ having the least possible number of elements. On the other hand, over a finite field a minimal separating set for the algebra of symmetric polynomials is not known in general. For every $n \in \mathbb{N}$ denote

$$[n]_q = \{jp^k \,|\, 1 \leq j < q,\ k \in \mathbb{N}_0,\ jp^k \leq n\} \text{ and}$$

$$S_q(n) = \{s_t(x_1, \dots, x_n) \,|\, t \in [n]_q\},$$

where $\mathbb{N}_0 = \mathbb{N} \sqcup \{0\}$. In 1964 Aberth [1] established that $S_p(n)$ is a separating set for $\mathbb{F}_p[V]^{\mathcal{S}_n}$ for a prime p. In [8] it was proven that the set $S_2(n)$ is a minimal separating set for $\mathbb{F}_2[V]^{\mathcal{S}_n}$ having the least possible number of elements. Recently, Domokos and Miklósi [5] extended the result of Aberth to the case of an arbitrary finite field. Namely, they proved that $S_q(n)$ is a separating set for $\mathbb{F}_q[V]^{\mathcal{S}_n}$. Nevertheless, the set $S(n)$ is a minimal separating set for $\mathbb{F}_q[V]^{\mathcal{S}_n}$ in some cases.

1.2 Results

In Theorem 3.1 and Corollary 3.3 we prove that $S(n)$ is a minimal separating set for $\mathbb{F}_q[V]^{\mathcal{S}_n}$ having the least possible number of elements if and only if $n \le \chi_q$, where χ_q is defined by formula (9). The explicit values of χ_q for $q \le 10^4$ are given in Remark 3.4. Since $\chi_q \ge \lfloor \ln(\ln q) \rfloor$ by Theorem 3.6, for every $n \ge 2$ there exists q such that $S(n)$ is a minimal separating set for $\mathbb{F}_q[V]^{\mathcal{S}_n}$ having the least possible number of elements (see Corollary 3.8). In Proposition 2.3 we determine when the separating set $S_3(n)$ for $\mathbb{F}_3[V]^{\mathcal{S}_n}$ has the least possible number of elements.

1.3 Auxiliaries

Since the number of $\mathcal{S}_n$-orbits on V is the binomial coefficient $\binom{n+q-1}{q-1}$, Theorem 1.1 of [8] implies that the least possible number of elements of a separating set for $\mathbb{F}_q[V]^{\mathcal{S}_n}$ is

$$\gamma = \gamma_q(n) = \left\lceil \log_q \frac{(n+q-1)\cdot \ldots \cdot (n+1)}{(q-1)!} \right\rceil \tag{1}$$

Consider some properties of the floor and the ceiling functions. Obviously, for $x \in \mathbb{R}$ and $n \in \mathbb{Z}$ we have

$$\lfloor x+n \rfloor = \lfloor x \rfloor + n, \lceil x+n \rceil = \lceil x \rceil + n, \mathrm{frac}(x+n) = \mathrm{frac}(x), \text{ and } -\lfloor x \rfloor = \lceil -x \rceil,$$

where $\mathrm{frac}(x)$ stands for the fractional part of x, i.e., $x = \lfloor x \rfloor + \mathrm{frac}(x)$.

Remark 1.1. For $a, b \in \mathbb{R}$ with $b \notin \mathbb{Z}$ we have

(a)
$$\lfloor 2\,a \rfloor = \begin{cases} 2\lfloor a \rfloor + 1 & \text{if} \quad \mathrm{frac}(a) \ge 1/2 \\ 2\lfloor a \rfloor & \text{if} \quad \mathrm{frac}(a) < 1/2 \end{cases};$$

(b)
$$\lfloor a-b \rfloor = \begin{cases} \lfloor a \rfloor + \lfloor -b \rfloor + 1 & \text{if} \quad \mathrm{frac}(a) \ge \mathrm{frac}(b) \\ \lfloor a \rfloor + \lfloor -b \rfloor & \text{if} \quad \mathrm{frac}(a) < \mathrm{frac}(b) \end{cases}.$$

2 The case of $\mathbb{F}_3$

For short, we denote

$$a_r = 3^{\frac{r}{2}} \text{ and } b_r = \frac{-3+\sqrt{8\cdot 3^r+1}}{2}$$

for $r \in \mathbb{N}_0$. Note that

$$a_r < b_r < a_{r+1} \text{ for all } r \ge 3. \tag{2}$$

Lemma 2.1. *For every $n \geq 1$ we have*

$$2\lfloor \log_3 n \rfloor = \lfloor 2 \log_3 n \rfloor + \alpha,$$

where

- $\alpha = 0$, *if* $n \in [a_{2r}, a_{2r+1})$ *for some* $r \in \mathbb{N}_0$;
- $\alpha = -1$, *if* $n \in [a_{2r+1}, a_{2r+2})$ *for some* $r \in \mathbb{N}_0$.

Proof. By part (a) of Remark 1.1, the statement of the lemma follows from the following claim:

$$\operatorname{frac}(\log_3 n) < \frac{1}{2} \quad \text{if and only if} \quad n \in [a_{2r}, a_{2r+1}) \text{ for some } r \in \mathbb{N}_0. \tag{3}$$

Note $\operatorname{frac}(\log_3 n) = 0$ if and only if $n = a_{2r}$ for some $r \in \mathbb{N}_0$. Since $\log_3 n$ is a strictly increasing function, then $\operatorname{frac}(\log_3 n)$ is also strictly increasing on every interval $[a_{2r}, a_{2r+2})$ with $r \in \mathbb{N}_0$. The equality $\operatorname{frac}(\log_3 a_{2r+1}) = 1/2$ for every $r \in \mathbb{N}_0$ concludes the proof of claim (3). □

Lemma 2.2. *Assume that $n \geq 6$. Then for $f_1(x) = \log_3 x^2$, $f_2(x) = \log_3 \frac{(x+1)(x+2)}{2}$, and $f_3(x) = \log_3 \dfrac{2}{1 + \frac{3}{x} + \frac{2}{x^2}}$ we have*

$$\lfloor f_1(n) \rfloor + \lfloor -f_2(n) \rfloor = \lfloor f_3(n) \rfloor + \beta,$$

where

- $\beta = 0$, *if* $n \in [a_r, b_r)$ *for some* $r \in \mathbb{N}$;
- $\beta = -1$, *if* $n \in [b_r, a_{r+1})$ *for some* $r \in \mathbb{N}$.

Proof. Since $n \geq 6$, we have $a_3 < n$. Hence, $a_r < b_r < a_{r+1}$ in case $n \in [a_r, a_{r+1})$ by (2). It is easy to see that $f_2(n) \notin \mathbb{Z}$, since in case $(n+1)(n+2) = 2 \cdot 3^k$ for some $k \in \mathbb{N}$ we obtain a contradiction.

We assume that x lies in $\mathbb{R}_+ = (0, +\infty)$. Since $f_1(x) - f_2(x) = f_3(x)$ and $f_2(n) \notin \mathbb{Z}$, part (b) of Remark 1.1 implies that the statement of the lemma follows from the next claims:

$$\operatorname{frac}(f_1(x)) < \operatorname{frac}(f_2(x)), \quad \text{if} \quad x \in [a_r, b_r) \text{ for some } r \geq 3, \tag{4}$$

$$\operatorname{frac}(f_1(x)) \geq \operatorname{frac}(f_2(x)), \text{ if } x \in [b_r, a_{r+1}) \text{ for some } r \geq 3. \tag{5}$$

We have $\operatorname{frac}(f_1(x)) = 0$ if and only if $x = a_r$ for some $r \in \mathbb{N}_0$. Similarly, $\operatorname{frac}(f_2(x)) = 0$ if and only if $x = b_r$ for some $r \in \mathbb{N}_0$. Since $f_1(x)$ and $f_2(x)$ are strictly increasing, then $\operatorname{frac}(f_1(x))$ and $\operatorname{frac}(f_2(x))$ are also strictly increasing on intervals $[a_r, a_{r+1})$ and $[b_r, b_{r+1})$, respectively, where $r \in \mathbb{N}_0$.

Since $f_1'(x) > f_2'(x)$ for all $x \in \mathbb{R}_+$ and $\operatorname{frac}(f_1(b_r)) > \operatorname{frac}(f_2(b_r))$, we obtain claim (5).

Assume that $\operatorname{frac}(f_1(x)) \geq \operatorname{frac}(f_2(x))$ for some $x \in [a_r, b_r)$ with $r \geq 3$. Then there exists $x_0 \in [a_r, b_r)$ with $\operatorname{frac}(f_1(x_0)) = \operatorname{frac}(f_2(x_0))$. Since f_1 increases faster than f_2, we have $\operatorname{frac}(f_1(x)) > \operatorname{frac}(f_2(x))$ for all $x \in [x_0, b_r)$. Then the equality $\lim\limits_{x \to b_r^-} \operatorname{frac}(f_2(x)) = 1$ implies that $\lim\limits_{x \to b_r^-} \operatorname{frac}(f_1(x)) = 1$, i.e., $\operatorname{frac}(f_1(b_r)) = 0$; a contradiction to inequalities (2). Hence claim (4) is proven. □

Proposition 2.3. *Let $\Delta = \#S_3(n) - \gamma_3(n)$ be the difference between the number of elements of the separating set $S_3(n)$ for $\mathbb{F}_3[V]^{\mathcal{S}_n}$ and the least possible number of elements of a separating set for $\mathbb{F}_3[V]^{\mathcal{S}_n}$. Then*

- $\Delta = 0$ *in case* $2 \leq n \leq 8$;
- $\Delta = \begin{cases} 0, & \text{if } n \in [b_{2r}, 2\,a_{2r}) \cup [b_{2r+1}, a_{2r+2}) \text{ for some } r \in \mathbb{N} \\ 1, & \text{otherwise} \end{cases}$

  in case $n \geq 9$.

Proof. It is easy to see that $\#S_3(n) = 2\,\lfloor \log_3 n \rfloor + \delta$, where

- $\delta = 1$ in case $n \in [a_{2r}, 2\,a_{2r})$ for some $r \in \mathbb{N}_0$;
- $\delta = 2$ in case $n \in [2\,a_{2r}, a_{2r+2})$ for some $r \in \mathbb{N}_0$.

Since $\gamma_3(n) = \left\lceil \log_3 \frac{(n+2)(n+1)}{2} \right\rceil$ by formula (1), we obtain

$$\Delta = 2\lfloor \log_3 n \rfloor + \delta - \left\lceil \log_3 \frac{(n+2)(n+1)}{2} \right\rceil.$$

For $2 \leq n \leq 8$ by straightforward calculations, we can see that $\Delta = 0$.

Assume $n \geq 9$. Then $a_4 \leq n$ and inequalities (2) imply that

$$a_{2r} < b_{2r} < a_{2r+1} < 2\,a_{2r} < b_{2r+1} < a_{2r+2}$$

in case $n \in [a_{2r}, a_{2r+2})$ for some $r \in \mathbb{N}$. Note that here we have $r \geq 2$.

Using the properties of ceiling functions and Lemma 2.1, we obtain

$$\Delta = \lfloor 2 \log_3 n \rfloor + \left\lfloor - \log_3 \frac{(n+2)(n+1)}{2} \right\rfloor + \alpha + \delta.$$

Hence, Lemma 2.2 together with the fact that $\left\lfloor \log_3 \frac{2}{1+\frac{3}{n}+\frac{2}{n^2}} \right\rfloor = 0$ in case $n \geq 4$ implies

$$\Delta = \alpha + \beta + \delta,$$

where α and β are the same as in Lemmas 2.1 and 2.2, respectively. We complete the proof case-by-case consideration. Namely,

- for $n \in [a_{2r}, b_{2r})$ we have $\alpha + \beta + \delta = 0 + 0 + 1 = 1$;
- for $n \in [b_{2r}, a_{2r+1})$ we have $\alpha + \beta + \delta = 0 - 1 + 1 = 0$;
- for $n \in [a_{2r+1}, 2\,a_{2r})$ we have $\alpha + \beta + \delta = -1 + 0 + 1 = 0$;
- for $n \in [2\,a_{2r}, b_{2r+1})$ we have $\alpha + \beta + \delta = -1 + 0 + 2 = 1$;
- for $n \in [b_{2r+1}, a_{2r+2})$ we have $\alpha + \beta + \delta = -1 - 1 + 2 = 0$.

□

3 The general case

Theorem 3.1. *The set $S(n)$ is a minimal separating set for $\mathbb{F}_q[V]^{\mathcal{S}_n}$ having the least possible number of elements if and only if $n < x_0$, where $x_0 = x_0(q) \in \mathbb{R}_{\geq 1}$ is the unique solution of the following equation*

$$q^{x-1} = (x+1)\Big(\frac{x}{2}+1\Big)\cdot\ldots\cdot\Big(\frac{x}{q-1}+1\Big)$$

over $\mathbb{R}_{\geq 1} = [1, +\infty)$. Moreover,

- $x_0 > 1$;
- $x_0 < q$ *in case* $q > 3$.

Proof. Since $\#S(n) = n$ and $\gamma = \gamma_q(n) = \left\lceil \log_q \frac{(n+q-1)\cdot\ldots\cdot(n+1)}{(q-1)!} \right\rceil$ is the least possible number of elements of a separating set for $\mathbb{F}_q[V]^{\mathcal{S}_n}$ by formula (1), using the properties of the floor and ceiling functions we obtain

$$\#S(n) - \gamma = \left\lfloor \log_q \frac{(q-1)!\cdot q^n}{(n+q-1)\cdot\ldots\cdot(n+1)} \right\rfloor.$$

Hence,

$$\#S(n) = \gamma \text{ if and only if } \frac{(q-1)!\cdot q^n}{(n+q-1)\cdot\ldots\cdot(n+1)} < q. \tag{6}$$

Therefore,

$$\#S(n) = \gamma \text{ if and only if } q^{n-1} < (n+1)\Big(\frac{n}{2}+1\Big)\cdot\ldots\cdot\Big(\frac{n}{q-1}+1\Big).$$

Applying ln to both sides, we obtain that

$$\#S(n) = \gamma \text{ if and only if } f_1(n) < f_2(n),$$

where $f_1(x) = (x-1)\ln q$ and $f_2(x) = \sum_{i=1}^{q-1} \ln\left(\frac{x}{i}+1\right)$.

Assume $x \in \mathbb{R}_{\geq 1}$. Since $f_1'(x) = \ln q$ and $f_2'(x) = \sum_{i=1}^{q-1} \frac{1}{x+i}$, we obtain

$$f_1'(x) > f_2'(x), \tag{7}$$

where we use inequality $f_2'(1) \geq f_2'(x)$ and the well-known upper bound on a partial sum $f_2'(1)$ of the harmonic series:

$$f_2'(1) = \frac{1}{2} + \cdots + \frac{1}{q} < \ln q.$$

Functions $f_1(x)$ and $f_2(x)$ are strictly increasing over $\mathbb{R}_{\geq 1}$ and $f_1(1) < f_2(1)$. We claim that

$$f_1(a) > f_2(a) \text{ for some } a > 1. \tag{8}$$

To prove the claim, we consider the following three cases.

- If $q = 2$, then $f_2(x) = \ln(x+1)$ and $f_1(4) > f_2(4)$.
- If $q = 3$, then $f_2(x) = \ln(1+x) + \ln(1+x/2)$ and $f_1(4) > f_2(4)$.
- Assume $q > 3$. Then $f_1(q) = \ln q^2 + (q-3)\ln q$ and

$$f_2(q) = \ln \frac{(q+1)(q+2)}{2} + \sum_{i=3}^{q-1} \ln\left(\frac{q}{i}+1\right).$$

Since $q^2 > (q+1)(q+2)/2$ and $q > (q+i)/i$ for $i \geq 3$, we obtain that $f_1(q) > f_2(q)$.

Claim (8) together with inequality $f_1(1) < f_2(1)$ implies that $f_1(x_0) = f_2(x_0)$ for some $x_0 \in \mathbb{R}_{\geq 1}$ with $1 < x_0 < a$. Inequality (7) implies that $x_0 = x_0(q)$ is the unique solution of the equation $f_1(x) = f_2(x)$ over $\mathbb{R}_{\geq 1}$. Moreover, we can see that for $x \in \mathbb{R}_{\geq 1}$ we have $f_1(x) < f_2(x)$ if and only if $x < x_0$. Obviously, x_0 is also the unique solution of the equation

$$q^{x-1} = (x+1)\left(\frac{x}{2}+1\right) \cdot \ldots \cdot \left(\frac{x}{q-1}+1\right)$$

over $\mathbb{R}_{\geq 1}$.

In case $q > 3$ we have $f_1(q) > f_2(q)$ and we may take $a = q$; hence $x_0 < q$. The requirements is proven. □

Let us remark that the following lemma which is an easy corollary of [8, Theorem 1.1] describes when $S(n)$ is a minimal separating set having the least possible number of elements, but for our purposes, we need more explicit condition on n.

Lemma 3.2. *The set $S(n)$ is a minimal separating set for $\mathbb{F}_q[V]^{\mathcal{S}_n}$ having the least possible number of elements if and only if*

$$q^{n-1} < \binom{n+q-1}{n}.$$

Proof. It follows from equivalence (6). □

Given $x_0 = x_0(q)$ from the formulation of Theorem 3.1, define $\chi_q \in \mathbb{N}$ as follows:

$$\chi_q = \begin{cases} x_0 - 1, & \text{if } x_0 \in \mathbb{N} \\ \lfloor x_0 \rfloor, & \text{if } x_0 \notin \mathbb{N} \end{cases} \tag{9}$$

Note that χ_q is defined for an arbitrary integer $q \geq 2$, not only for the power of a prime. Theorem 3.1 implies the following corollary.

Corollary 3.3. *The set $S(n)$ is a minimal separating set for $\mathbb{F}_q[V]^{\mathcal{S}_n}$ having the least possible number of elements if and only if $n \leq \chi_q$. Moreover,*

$$1 \leq \chi_q < q \text{ in case } q > 3.$$

Definition 3.4. By straightforward calculations, using a computer, we can see that

- $\chi_2 = 2$;
- $\chi_q = 3$ for $3 \leq q \leq 17$;
- $\chi_q = 4$ for $18 \leq q \leq 109$;
- $\chi_q = 5$ for $110 \leq q \leq 704$;
- $\chi_q = 6$ for $705 \leq q \leq 5018$;
- $\chi_q = 7$ for $5019 \leq q \leq 10^4$.

To prove a lower bound on χ_q from Theorem 3.6 (see below) we need the following technical lemma.

Lemma 3.5. *For every $q \geq e^{e^2}$ we have*

$$\ln q - (2\ln(\ln q) + 1)\ln(\ln(\ln q)) > 0.$$

Proof. Assume $x \in \mathbb{R}_{\geq e}$. Then for

$$h(x) = x - (2\ln x + 1)\ln(\ln x).$$

we have

$$h'(x) = \frac{w(x)}{x \ln x}, \quad \text{where} \quad w(x) = x\ln x - 2\ln x - 2\ln(\ln x)\ln x - 1.$$

Since

$$w'(x) = \frac{(x\ln x - 2\ln(\ln x)) + (x-4)}{x} > 0,$$

for all $x \geq e^2$ and $w(e^2) = 2e^2 - 4\ln 2 - 5 > 0$, we obtain that $w(x) > 0$ for all $x \geq e^2$. Therefore, $h'(x) > 0$ for all $x \geq e^2$. Hence, the inequality $h(e^2) = e^2 - 5\ln 2 > 0$ implies that $h(x) > 0$ for all $x \geq e^2$. In particular, $h(\ln q) > 0$ for all $q \geq e^{e^2}$. The required statement is proven. □

Theorem 3.6. *We have* $\chi_q \geq \lfloor \ln(\ln q) \rfloor$.

Proof. If $q < e^{e^2}$, then $\lfloor \ln(\ln q) \rfloor \leq 1 \leq \chi_q$, and the required statement is proven.

Assume that $q \geq e^{e^2}$. Define

$$f(x) = q^{x-1}, \quad g(x) = \frac{(x+1)\cdot\ldots\cdot(x+q-1)}{(q-1)!}$$

for $x \in \mathbb{R}_{\geq 1}$. Recall that $x_0 = x_0(q)$ from definition (9) of χ_q is the unique solution of the equation $f(x) = g(x)$ over $\mathbb{R}_{\geq 1}$ and $1 = f(1) < g(1) = q$. Hence, to prove the theorem is sufficient to show that

$$f(b) < g(b) \tag{10}$$

for $b = \lfloor \ln(\ln q) \rfloor \geq 2$, since inequality (10) implies that $b < x_0$. Inequality (10) is equivalent to the inequality $\ln(f(b)) < \ln(g(b))$.

For short, define $a = b + q - 1 \geq q + 1$. Then

$$g(b) = \binom{a}{q-1} \quad \text{and} \quad \ln g(b) = \ln a! - \ln b! - \ln(q-1)!$$

Using well-known inequalities

$$\sqrt{2\pi k}\Big(\frac{k}{e}\Big)^k < k! < 2\sqrt{\pi k}\Big(\frac{k}{e}\Big)^k \quad \text{for all} \ \ k \geq 1,$$

we obtain that

$$\ln g(b) > a\ln(a) - \Big(q - \frac{1}{2}\Big)\ln(q-1) + \frac{1}{2}\Big(\ln(a) - 2b\ln(b) - \ln(b)\Big) - \frac{1}{2}\ln(8\pi). \tag{11}$$

By the definition of b, we have $2 \leq b \leq \ln(\ln q)$. Therefore,

$$\ln(a) - 2b\ln(b) - \ln(b) \geq \ln(q) - (2\ln(\ln q) + 1)\ln(\ln(\ln q)) > 0$$

by Lemma 3.5. Thus inequality (11) implies that

$$\ln g(b) > a\ln(a) - \Big(q - \frac{1}{2}\Big)\ln(q-1) - \frac{1}{2}\ln(8\pi).$$

Applying inequality $a \geq q+1$, we obtain

$$\ln g(b) > (q+b-1)\ln(q+1) - \left(q-\frac{1}{2}\right)\ln(q-1) - \frac{1}{2}\ln(8\pi) =$$
$$= (b-1)\ln(q+1) + \left(q-\frac{1}{2}\right)\Big(\ln(q+1) - \ln(q-1)\Big) +$$
$$+ \frac{1}{2}\Big(\ln(q+1) - \ln(8\pi)\Big) > (b-1)\ln q = \ln f(b).$$

The required statement is proven. □

Corollary 3.7. *We have* $\lim_{q\to\infty} \chi_q = +\infty$.

Corollary 3.8. *For every* $n \geq 2$ *there exists* q *such that* $S(n)$ *is a minimal separating set for* $\mathbb{F}_q[V]^{\mathcal{S}_n}$ *having the least possible number of elements.*

Acknowledgments

The first author was supported by FAPESP 2021/01690-7. We are grateful for this support.

References

[1] O. Aberth. The elementary functions in a finite field of prime order. *Illinois J. Math.*, 8:132–138, 1964.

[2] F. Cavalcante and A. Lopatin. Separating invariants of three nilpotent 3×3 matrices. *Linear Algebra Appl.*, 607:9–28, 2020.

[3] M. Domokos. Addendum to "Characteristic free description of semi-invariants of 2×2 matrices"[J. Pure Appl. Algebra 224 (2020), no. 5, 106220]. *J. Pure Appl. Algebra*, 224(6):106270, 2020.

[4] M. Domokos. Characteristic free description of semi-invariants of 2×2 matrices. *J. Pure Appl. Algebra*, 224(5):106220, 2020.

[5] M. Domokos and B. Miklós. Symmetric polynomials over finite fields. *Finite Fields Appl.*, 89:102224, 2023.

[6] R. Ferreira and A. Lopatin. Minimal generating and separating sets for $O(3)$-invariants of several matrices. *Operators and Matrices*, 17(3):639–651, 2023.

[7] I. Kaygorodov, A. Lopatin, and Y. Popov. Separating invariants for 2×2 matrices. *Linear Algebra Appl.*, 559:114–124, 2018.

[8] G. Kemper, A. Lopatin, and F. Reimers. Separating invariants over finite fields. *J. Pure Appl. Algebra*, 226:106904, 2022.

[9] A. Lopatin. On m-tuples of nilpotent 2×2 matrices over an arbitrary field. *Int. J. Algebra Comput.*, 34(8):1253–1272, 2024.

[10] A. Lopatin and P. Muniz Martins. Separating invariants for two-dimensional orthogonal groups over finite fields. *Linear Algebra Appl.*, 692:71–83, 2024.

[11] A. Lopatin and F. Reimers. Separating invariants for multisymmetric polynomials. *Proc. Amer. Math. Soc.*, 149:497–508, 2021.

[12] A. Lopatin and A. Zubkov. Separating G_2-invariants of several octonions. *Algebra Number Theory*, 18(12):2157–2177, 2024.

[13] F. Reimers. Separating invariants for two copies of the natural S_n-action. *Commun. Algebra*, 48:1584–1590, 2020.

Received: October 26, 2024
Accepted for publication: January 2, 2025
Communicated by: Ivan Kaygorodov