Symmetric functions over finite fields

Mihai Prunescu *

Abstract

The number of linear independent algebraic relations among elementary symmetric polynomial functions over finite fields is computed. An algorithm able to find all such relations is described. The algorithm consists essentially of Gauss' upper triangular form algorithm. It is proved that the basis of the ideal of algebraic relations found by the algorithm consists of polynomials having coefficients in the prime field $\mathbb{F}_p$.
A.M.S.-Classification: 14-04, 15A03.

1 Introduction

The problem of interpolation for symmetric functions over fields is an important question in Algebra, and a lot of aspects of this problem have been treated by many authors; see for example the monograph [2] for the big panorama of symmetric polynomials, or [3] for more special results concerning the interpolation.

In the case of finite fields the problem of interpolation for symmetric functions is in the same time easier than but different from the general problem. It is easier because it can always be reduced to systems of linear equations. Indeed, there are only finitely many monomials leading to different polynomial functions, and only finitely many tuples to completely define a function. The reason making the problem different from the general one is not really deeper. Let S_i be the elementary symmetric polynomials in variables X_i $(i = 1, \ldots, n)$. If the exponents are bounded by q, one has exactly so many polynomials in S_i as polynomials in X_i, but strictly less symmetric functions from $\mathbb{F}_q^n \to \mathbb{F}_q$ than general functions. It follows that a lot of polynomials in S_i must express the constant 0 function. We call this set of polynomials the ideal of algebraic relations between elementary symmetric functions over the finite field $\mathbb{F}_q$ and denote this $\mathcal{I}(q, n)$. Every instance of the interpolation problem for a symmetric function has as set of solutions a class $f_0(\vec{S}) + \mathcal{I}(q, n)$.

In this paper we study the ideal of algebraic relations $\mathcal{I}(q, n)$ and we compute its dimension as a vector space over the finite field. The paper is organized as follows: In the Section 2 definitions and notations are rigorously given. The ideal $\mathcal{I}(q, n)$ is defined as the kernel of a morphism Φ. In the Section 3 the number of symmetric functions $\mathbb{F}_q^n \to \mathbb{F}_q$ is counted. Furtherly it is proved that the morphism Φ is surjective and the dimension of $\mathcal{I}(q, n)$ as a vector space over $\mathbb{F}_q$ is computed. As a byproduct of this Section, $\mathcal{I}(q, n)$ is also the kernel of a substitution morphism between two rings of polynomials. In the Section 3 we describe an algorithm for the automatic deduction of all such algebraic relations. The algorithm consists essentially of Gauss' upper triangular form algorithm to parametrically solve systems of linear equations. We prove that the algorithm always finds a basis of the vector space of algebraic relations, always consisting of polynomials with coefficients in the prime field $\mathbb{F}_p$. We also display in the Section 4 some examples of algebraic relations produced by the algorithm. The Section 5 contains an example of concrete interpolation problem. This problem was the original motivation of the author to do these computations.

*Brain Products, Freiburg, Germany, and Institute of Mathematics of the Romanian Academy, Bucharest, Romania. mihai.prunescu@math.uni-freiburg.de.

2 Definitions and notations

Consider a finite field $\mathbb{F}_q$ of characteristic p. The elements of $\mathbb{F}_q$ are identified with the set $\{0, 1, \ldots, q-1\}$ in an arbitrary way. For the rest of the paper we fix a natural number $n \geq 2$ and two sets of variables: S_1, ... , S_n and X_1, ... , X_n. The variables S_i will be in some contexts algebraically independent variables. In other contexts S_i shall denote the projection of the variable S_i in different homomorphic images of the polynomial ring $\mathbb{F}_q[S_1, \ldots, S_n]$ or shall mean an elementary symmetric polynomial in variables $X_1, \ldots, X_n$.

Definition: The set $\mathrm{Mon}(q, n)$ is the set of all monomials $S_1^{\alpha_1} S_2^{\alpha 2} \ldots S_n^{\alpha_n}$ with $0 \leq \alpha_i < q$. There are q^n many such monomials.

Definition: Let $\mathbb{F}_q\{S_1, \ldots, S_n\}$ be the vector space over $\mathbb{F}_q$ freely generated by the set $\mathrm{Mon}(q, n)$. $\mathbb{F}_q\{S_1, \ldots, S_n\}$ has dimension q^n over $\mathbb{F}_q$. It has also a canonical structure of finite ring induced by the epimorphism:

$$s : \mathbb{F}_q[S_1, \ldots, S_n] \longrightarrow \mathbb{F}_q\{S_1, \ldots, S_n\}$$

with $\mathrm{Ker}(s) = (S_1^q - S_1, \ldots, S_n^q - S_n)$ as ideal in $\mathbb{F}_q[S_1, \ldots, S_n]$. This construction is justified by the fact that $\mathbb{F}_q \models \forall x\ x^q = x$.

Definition: $\mathrm{Sym}(m)$ denotes the symmetric group of all permutations of m objects $\{1, \ldots m\}$.

Definition: For every function $f : \{0, \ldots, q-1\}^n \to \{0, \ldots, q-1\}$ and permutation $\sigma \in \mathrm{Sym}(n)$ we define $f^\sigma(x_1, \ldots, x_n) = f(\sigma(\vec{x}))$ where $\sigma(\vec{x}) = (x_{\sigma(1)}, \ldots, x_{\sigma(n)})$. The function f is called symmetric if for all $\sigma \in \mathrm{Sym}(n)$, $f = f^\sigma$.

Definition: Remember here that $\mathbb{F}_q$ and the set $\{0, \ldots, q-1\}$ have been identified. Let $\mathcal{F}(q, n)$ denote the set of all functions $f : \mathbb{F}_q^n \to \mathbb{F}_q$ and $\mathcal{S}(q, n) \subset \mathcal{F}(q, n)$ the subset of all symmetric functions. Both sets equiped with the point-wise operations are finite rings and finite vector spaces over $\mathbb{F}_q$.

Definition: For every $F \in \mathbb{F}_q[X_1, \ldots, X_n]$ and $\sigma \in \mathrm{Sym}(n)$ we define $F^\sigma(\vec{X}) = F(\sigma(\vec{X}))$, where $\sigma(\vec{X}) = (X_{\sigma(1)}, \ldots, X_{\sigma(n)})$. F is called symmetric if for all $\sigma \in \mathrm{Sym}(n)$, $F^\sigma = F$.

Definition: For $0 \leq k \leq n$ denote by $\mathcal{P}_k^n$ the set of subsets of $\{1, \ldots, n\}$ containing exactly k elements. Recall that the elementary symmetric polynomials $S_k(X_1, \ldots, X_n)$ are defined as:

$$S_k(X_1, \ldots, X_n) = \sum_{J \in \mathcal{P}_k^n} \prod_{i \in J} X_i.$$

Definition: Consider the function

$$\Phi : \mathbb{F}_q\{S_1, \ldots, S_n\} \longrightarrow \mathcal{S}(q, n)$$

defined such that

$$\forall \vec{a} \in \mathbb{F}_q^n \quad \Phi(f(\vec{S}))(\vec{a}) = f(S_1(\vec{a}), \ldots, S_n(\vec{a})),$$

where $f(\vec{S}) \in \mathbb{F}_q\{S_1, \ldots, S_n\}$. In the right hand side the variables S_i are interpreted as elementary symmetric polynomials which are evaluated in the tuple $\vec{a}$. Φ is a well defined homomorphism of finite rings and of finite vector spaces over $\mathbb{F}_q$.

Definition: The ideal $\mathcal{I}(q, n) = \mathrm{Ker}(\Phi) \subset \mathbb{F}_q\{S_1, \ldots, S_n\}$ is called **ideal of algebraic relations** between elementary symmetric functions over $\mathbb{F}_q$. $\mathcal{I}(q, n)$ is also a sub-space of $\mathbb{F}_q\{S_1, \ldots, S_n\}$.

The goal of this paper is to find out the dimension (cardinality) of $\mathcal{I}(q, n)$ and to describe a concrete method to find its the elements.

3 The number of algebraic relations

The fixed identification of $\mathbb{F}_q$ and $\{0, \ldots, q-1\}$ is crucial for this section.

Definition: Let $\mathrm{WM}(q,n)$ be the set of all (weakly) monotone increasing tuples $(a_1,\ldots,a_n)$ with all $a_i \in \{0,\ldots,q-1\}$. Denote by $\mathrm{wm}(q,n)$ the cardinality of the set $\mathrm{WM}(q,n)$.

Lemma 3.1

$$\dim_{\mathbb{F}_q} \mathcal{S}(q,n) = \mathrm{wm}(q,n) = \binom{n+q-1}{q-1}.$$

Proof: For the first equality: in order to define an $f \in \mathcal{S}(q,n)$, it is enough to define its values for every $w \in \mathrm{WM}(q,n)$.

For the second equality: the number of partitions with at most k parts and the largest part $\leq j$ is $\binom{k+j}{j}$, as proven for example in [1]. Now take $k=n$ and $j=q-1$. □

Definition: Consider the following matrix $M(q,n) \in \mathrm{Mat}(\mathrm{wm}(q,n)\times q^n, \mathbb{F}_q)$. The rows of $M(q,n)$ are indexed using the tuples $\vec{\iota} \in \mathrm{WM}(q,n)$, the columns are indexed using the monomials $m \in \mathrm{Mon}(q,n)$, and if $M(q,n) = (a(\vec{\iota},m) \mid \vec{\iota} \in \mathrm{WM}(q,n), m \in \mathrm{Mon}(q,n))$,

$$a(\vec{\iota},m) = [\Phi(m)](\vec{\iota}).$$

Theorem 3.2 *The rank of the matrix $M(q,n)$ is maximal:*

$$\mathrm{rank}\ M(q,n) = \mathrm{wm}(q,n) = \binom{n+q-1}{q-1}.$$

The dimension of the ideal $\mathcal{I}(q,n)$ of algebraic relations as a vector space over $\mathbb{F}_q$ is:

$$\dim_{\mathbb{F}_q} \mathcal{I}(q,n) = q^n - \mathrm{wm}(q,n) = q^n - \binom{n+q-1}{q-1}.$$

Proof: Linear algebra using Lemma 3.1 and the following Lemma 3.3. □

Lemma 3.3 *The morphism $\Phi : \mathbb{F}_q\{S_1,\ldots,S_n\} \to \mathcal{S}(q,n)$ with $\mathrm{Ker}\ \Phi = \mathcal{I}(q,n)$ is surjective.*

Proof: The proof consists of two steps. In the first step we repeat the interpolation over finite fields and check that by interpolating symmetric functions the method produces symmetric polynomials. In the second step, we repeat the argument that a symmetric polynomial can be written as a polynomial in elementary symmetric polynomials and convince us that the existence part of the proof behaves well with the degrees.

Step 1: Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ be some function, for the moment not necessarily symmetric. For $a \in \mathbb{F}_q$ define the polynomial $h_a \in \mathbb{F}_q[X]$:

$$h_a(X) = \prod_{\lambda \in \mathbb{F}_q \setminus \{a\}} \frac{X-\lambda}{a-\lambda}.$$

Observe that $h_a(a) = 1$ and $h_a(\mathbb{F}_q \setminus \{a\}) = 0$. For a tuple $\vec{a} \in \mathbb{F}_q^n$ define $h_{\vec{a}} \in \mathbb{F}_q[X_1,\ldots,X_n]$:

$$h_{\vec{a}}(\vec{X}) = h_{a_1}(X_1)\ldots h_{a_n}(X_n).$$

A polynomial interpolating f is:

$$H(\vec{X}) = \sum_{\vec{a} \in \mathbb{F}_q^n} h_{\vec{a}}(\vec{X}) f(\vec{a}).$$

We observe that for all $\sigma \in \mathrm{Sym}(n)$, $(h_{\vec{a}})^\sigma = h_{\sigma^{-1}(\vec{a})}$. If the function f is symmetric, then $f^\sigma = f$ and it follows:

$$H^\sigma(\vec{X}) = \sum_{\vec{a} \in \mathbb{F}_q^n} h_{\vec{a}}^\sigma(\vec{X}) f(\vec{a}) = \sum_{\sigma^{-1}(\vec{a}) \in \mathbb{F}_q^n} h_{\sigma^{-1}(\vec{a})}(\vec{X}) f(\sigma^{-1}(\vec{a})) = H(\vec{X}).$$

We proved that the interpolation algorithm applied to a symmetric function leads to a symmetric polynomial. Observe also that all exponents occurring in H are $< q$.

Step 2: We repeat the argument that a symmetric polynomial is a polynomial in elementary symmetric polynomials as given in [7] and reformulated in [6]. The following total order is defined over the set of monomials in $\vec{X}$: $X_1^{\alpha_1} \dots X_n^{\alpha_n} < X_1^{\beta_1} \dots X_n^{\beta_n}$ if and only if $\sum \alpha_i < \sum \beta_i$ or $\sum \alpha_i = \sum \beta_i$ but $(\alpha_i) < (\beta_i)$ lexicographically. For a polynomial $H(\vec{X}) \in \mathbb{F}_q[\vec{X}]$ define $\mathrm{Init}(H)$ to be the maximal monomial occurring in H, according to this order. It follows from symmetry that $\mathrm{Init}(H)$ has the form $cX_1^{\gamma_1} \dots X_n^{\gamma_n}$ with $\gamma_1 \geq \gamma_2 \geq \dots \geq \gamma_n$ with $c \in \mathbb{F}_q \setminus \{0\}$. Consider the polynomial:

$$H_1(\vec{X}) = H(\vec{X}) - cS_1(\vec{X})^{\gamma_1-\gamma_2} S_2(\vec{X})^{\gamma_2-\gamma_3} \dots S_{n-1}(\vec{X})^{\gamma_{n-1}-\gamma_n} S_n(\vec{X})^{\gamma_n}.$$

Observe that $\mathrm{Init}(H_1) < \mathrm{Init}(H)$. Continue by constructing in the same way a polynomial H_2 with $\mathrm{Init}(H_2) < \mathrm{Init}(H_1)$, and so on. This process ends in finitely many steps. Adding the S_i-monomials defined during the process, one gets a polynomial $F \in \mathbb{F}_q[S_1, \dots, S_n]$ with the property that for all $\vec{a} \in \mathbb{F}_q^n$, $F(S_1(\vec{a}), \dots, S_n(\vec{a})) = f(\vec{a})$. Finally, observe that all exponents occurring in F are again $< q$, so $F \in \mathbb{F}_q\{S_1, \dots, S_n\}$ and $\Phi(F) = f$.

□

Remark 1: If q is kept constant and $n \to \infty$,

$$\frac{\dim_{\mathbb{F}_q} \mathcal{I}(q,n)}{\dim_{\mathbb{F}_q} \mathbb{F}_q\{S_1, \dots, S_n\}} \longrightarrow 1.$$

If n is kept constant and $q \to \infty$,

$$\frac{\dim_{\mathbb{F}_q} \mathcal{I}(q,n)}{\dim_{\mathbb{F}_q} \mathbb{F}_q\{S_1, \dots, S_n\}} \longrightarrow 1 - \frac{1}{n!}.$$

Indeed, if q is kept constant and $n \to \infty$,

$$\frac{q^n - \binom{n+q-1}{q-1}}{q^n} = 1 - \frac{1}{(q-1)!} \frac{(n+1)\dots(n+q-1)}{q^n} \longrightarrow 1.$$

If n is kept constant and $q \to \infty$,

$$\frac{q^n - \binom{n+q-1}{q-1}}{q^n} = 1 - \frac{1}{n!} \frac{q(q+1)\dots(q+n-1)}{q^n} \longrightarrow 1 - \frac{1}{n!}.$$

Remark 2: Define the set of non-monotone tuples $\mathrm{NM}(q,p)$ as the set of tuples $(a_1, \dots, a_n)$ with $a_i \in \{0, \dots, q-1\}$ such that there are $1 \leq i < j \leq n$ with $a_i > a_j$. Let $\mathrm{nm}(q,n)$ be the cardinality of the set $\mathrm{NM}(q,n)$. According to Theorem 3.2, $\mathcal{I}(q,n)$ has dimension $\mathrm{nm}(q,n)$. But is there any natural correspondence between $\mathrm{NM}(q,n)$ and a basis of the vector space $\mathcal{I}(q,n)$?

Remark 3: Consider the following chain of homomorphisms:

$$\mathbb{F}_q\{S_1, \dots, S_n\} \xrightarrow{\Psi} \mathbb{F}_q\{X_1, \dots, X_n\} \xrightarrow{\Gamma} \mathcal{F}(q,n),$$

where $\Psi(P(\vec{S})) = P(\vec{S}(\vec{X}))$ is the substitution homomorphism and Γ is the homomorphism associating to every polynomial Q its polynomial function. Of course $\Phi = \Gamma \circ \Psi$. Using the interpolation part of the proof of Lemma 3.3 one sees that Γ is an isomorphism of rings and vector spaces. Indeed, Γ is a surjective homomorphism and both rings have q^{q^n} elements. As it follows:

Corollary 3.4 $\mathrm{Ker}\,\Psi = \mathcal{I}(q,n)$ *and* $\mathrm{Im}\,\Psi = \Gamma^{-1}(\mathcal{S}(q,n))$. *Consequently, the subring of symmetric polynomials in* $\mathbb{F}_q\{X_1, \dots, X_n\}$ *is a vector space of dimension* $\mathrm{wm}(q,n)$ *over* $\mathbb{F}_q$.

4 Deduction procedure

The following algorithm is able to find a basis over $\mathbb{F}_q$ for the vector space $\mathcal{I}(q,n)$ of algebraic relations between elementary symmetric functions over $\mathbb{F}_q$. The algorithm uses only linear algebra.

1. Consider q^n many new unknowns Y_m indexed using the set $\mathrm{Mon}(q,n)$, and the following homogenous system Σ of $\mathrm{wm}(q,n)$ many linear equations indexed using the set $\mathrm{WM}(q,n)$:

$$(\vec{\imath}): \qquad \sum_{m\in \mathrm{Mon}(q,n)} a(\vec{\imath},m)Y_m = 0.$$

   The matrix of this linear homogenous system is the matrix $M(q,n)$ defined in the previous section. One sees that for any polynomial $P \in \mathbb{F}_q\{S_1,\ldots,S_n\}$ following holds:

$$P(\vec{S}) = \sum_{m\in \mathrm{Mon}(q,n)} y_m \ m(\vec{S}) \ \in \ \mathcal{I}(q,n) \ \Leftrightarrow \ (y_m) \in (\mathbb{F}_q)^{q^n} \text{ satisfies } \Sigma.$$

2. Using Gauss' Algorithm over $\mathbb{F}_q$ transform $M(q,n)$ in an upper triangular matrix. Recall that $M(q,n)$ has maximal rank equal with $\mathrm{wm}(q,n)$.

3. Introduce a tuple $\vec{t}$ of $q^n - \mathrm{wm}(q,n)$ many new parameters and compute the parametric solution of Σ, consisting of linear functions in $\vec{t}$:

$$(y_m(\vec{t}))_{m\in \mathrm{Mon}(q,n)}.$$

4. Using the equivalence from (1) one has that:

$$\mathcal{I}(q,n) = \{ \sum_{m\in \mathrm{Mon}(q,n)} y_m(\vec{t}) \ m \ \mid \vec{t} \in (\mathbb{F}_q)^{q^n - \mathrm{wm}(q,n)} \ \}.$$

   For $i = 1,\ldots,q^n - \mathrm{wm}(q,n)$ set the parameter tuple $\vec{t_i} = (0,0,\ldots,t_i = 1,0,\ldots,0)$ in the general form $P_{\vec{t}} = \sum_{m\in \mathrm{Mon}(q,n)} y_m(\vec{t})m$ and call the result of the substitution $P_i = P_{\vec{t_i}}$. The application $\vec{t} \rightsquigarrow P_{\vec{t}}$ is an isomorphism of vector spaces over $\mathbb{F}_q$ because it is a surjective linear application between vector spaces of equal dimensions. As an isomorphism, this application transports basis to basis, so $\{ P_i \mid i = 1,\ldots,q^n - \mathrm{wm}(q,n) \}$ is a basis of $\mathcal{I}(q,n)$ over $\mathbb{F}_q$.

In all cases computed by the author over finite fields $\mathbb{F}_q$ with $q > p = \mathrm{char}\ \mathbb{F}_q$ both the matrix $M(q,n)$ and the corresponding upper triangular form contained elements in $\mathbb{F}_q \setminus \mathbb{F}_p$, but the computed basis of $\mathcal{I}(q,n)$ always had coefficients in the prime field $\mathbb{F}_p$. The author was very surprised to understand that this fact is true in general:

Theorem 4.1 *Let $\mathbb{F}_q$ be some finite field, $p = \mathrm{char}\ \mathbb{F}_q$ and $n \geq 2$. Then the algorithm presented above finds a basis of $\mathcal{I}(q,n)$ consisting of polynomials with coefficients in the prime field $\mathbb{F}_p$. In particular, such a basis always exists.*

Before proving the Theorem 4.1, we must fix some notations concerning Gauss' Algorithm.

Definition: In the following notations for elementary operations one always has $i < j$:

$A(i,j)$ means that the equation i multiplied with an apropriate element is added to equation j. The element is choosed such that the first non-zero coefficient in the equation j becomes 0.

$L(i,j)$ means that equations (lines) i and j are inter-changed.

$C(i,j)$ means that the columns i and j are inter-changed.

Definition: The step number i of the deterministic Gauss' Algorithm: If $a_{i,i} = 0$ and the whole line i consists only of zeros, find the first $j > i$ such that the line j contains non-zero elements, and apply $L(i, j)$. If $a_{i,i}$ continues to be zero, find the first $k > i$ such that $a_{i,k} \neq 0$ and apply $C(i, k)$. Now, for each $r > i$ if the element $a_{r,i} \neq 0$ below $a_{i,i}$ apply $A(i, r)$.

Definition: Let K be some field and S, S' two systems of linear equations over K; both of them consisting of e equations with u unknowns. We say that Gauss' Algorithm works in parallel for systems S and S' if the application of Gauss' Algorithm on the systems leads to the same sequence of operations $O_1, O_2, \ldots, O_s$ in the above notation. (For example, $O_1 = A(1, 2)$, . . . , $O_s = L(3, 4)$, $O_{s+1} = C(3, 5)$, . . . and so on.)

Lemma 4.2 *Let K be a field and S, S' two homogenous systems of linear equations over K, satisfying the following conditions:*

1. *S and S' have both e equations and u unknowns, $k = u - e \geq 0$ and* rank $S = e$.
2. *S' has been obtained from S by some permutation of equations.*
3. *Gauss' Algorithm works in parallel over S and S'.*

In this situation, Gauss' Algorithm independently applied for the systems S and S' computes the same parametrization of the common space of solutions:

$$\forall\ i = 1, \ldots, u \qquad y_i(\vec{t}) = y'_i(\vec{t}),$$

where $|\vec{t}| = k$ is the tuple of parameters.

Proof: First of all, observe that condition 2 implies that both systems have the same rank and the same space of solutions. The rank being maximal, transformations of type $L(i, j)$ do not arise during Gauss' Algorithm. The condition 3 implies that the same set of columns $i_1, i_2, \ldots, i_e$ define in both systems quadratic $e \times e$ non-singular minors. Without restricting the generality, we consider these columns to be $1, 2, \ldots, e$. The proof works by induction on k.

Induction start: If $k = 0$ there is only the trivial solution $\vec{0}$, so the parametrizations found by the Gauss' Algorithm must be also identic: $y_i = y'_i = 0$.

Induction step: Let $k \geq 1$. Suppose that the Lemma is true for all instances with $u - e = k - 1$, and consider a situation with $u - e = k$:

$$S: \quad M \cdot \vec{y} = 0; \qquad S': \quad M' \cdot \vec{y} = 0.$$

Put $y_u = 1$ and transfer the former coefficients of y_u at the right-hand side. One gets the non-homogenous systems:

$$T: \quad N \cdot \vec{x} = \vec{b}; \qquad T': \quad N' \cdot \vec{x} = \vec{b'},$$

where the tuple $\vec{x}$ occurring in T and T' have length $u - 1$. Now consider the $e \times e$ non-singular minors of M and M' found during the parallel working Gauss' Algorithm; call the minors A and A'. Consider the non-homogenous systems:

$$U: \quad A \cdot \vec{z} = \vec{b}; \qquad U': \quad A' \cdot \vec{z} = \vec{b'},$$

where the tuple $\vec{z}$ occurring in U and U' has length e. Finally, let V and V' be the systems obtained from T and T' by substituting the free terms $\vec{b}$ and $\vec{b'}$ with $\vec{0}$:

$$V: \quad N \cdot \vec{x} = \vec{0}; \qquad V': \quad N' \cdot \vec{x} = \vec{0}.$$

First of all, the systems U and U' are non-singular square systems which differ by a permutation of lines only, so they have a common unique solution $\vec{z} \in K^e$. On the other hand one can apply the hypothesis of induction for the pair V, V'; so Gauss' Algorithm computes the same parametrisation for their common space of solutions. Let this parametrisation be $(x_i(\vec{t}))$ with $i = 1, \ldots, u-1$ and $|\vec{t}| = k-1$. It follows that Gauss' Algorithm computes for the systems T, T' a common parametrization for the common affine space of solutions:

$$(x_1(\vec{t}) + z_1, \ldots, x_e(\vec{t}) + z_e, t_1, \ldots, t_{k-1}).$$

But Gauss' Algorithm makes the same computations for the system pair T, T' as for the pair of homogenous systems S, S'. It follows that Gauss' Algorithm shall compute for both systems the same parametrization for their common space of solutions, which is:

$$(x_1(\vec{t}) + z_1 t_k, \ldots, x_e(\vec{t}) + z_e t_k, t_1, \ldots, t_{k-1}, t_k).$$

□

Proof of the Theorem 4.1: If $\mathbb{F}_q = \mathbb{F}_p$ there is nothing to prove. Consider some automorphism $\varphi \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$. The fact that φ is a power of Frobenius' Automorphism is not relevant here. Consider the system Σ used in the algorithm given above and the system $\Sigma' = \varphi(\Sigma)$.

Claim 1: Σ' can be obtained from Σ by some permutation of equations. Indeed, the elements of the matrix $\varphi(M(q,n))$ are $\varphi(a(\vec{\iota}, m)) = \varphi([\Phi(m)](\vec{\iota})) = [\Phi(m)](\varphi(\vec{\iota}))$. The automorphism φ is a permutation of $\mathbb{F}_q$ and changes the identification with the set $\{0, \ldots, q-1\}$. Consequently, the line formerly indexed $\vec{\iota}$ shall be found in Σ' at the index obtained by the weakly monotone reordering of the tuple $\varphi(\vec{\iota})$.

Claim 2: Gauss' Algorithm works in parallel over Σ and Σ'. At the beginning, coefficients in Σ' are images of corresponding coefficients in Σ by φ. This situation remains true after every computation step done by the algorithm. In particular, at every step one has in both transformed systems Σ and Σ' the same situation concerning elements which are zero or not. According to this situation, at every step the same decision concerning the next step shall be taken: an $A(i,j)$ or a $C(i,j)$.

So all conditions requested by Lemma 4.2 are satisfied, and Gauss' Algorithm computes the same parametrization $(y_i(\vec{t}))$ for both systems Σ and $\varphi(\Sigma)$. But using the same argument as for proving Claim 2, one sees that Gauss' Algorithm applied on the system $\varphi(\Sigma)$ computes the parametrization $(\varphi(y_i(\vec{t})))$. So for all i, $y_i(\vec{t}) = \varphi(y_i(\vec{t}))$; and this takes place for all automorphisms $\varphi \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$. It follows that the linear functions $y_i(\vec{t})$ have coefficients in $\mathbb{F}_p$, and the same is true for the basis of $\mathcal{I}(q,n)$ found by the algorithm. □

5 Some examples

This algorithm has been implemented by the author using the language C♯ and the platform Visual Studio 2005, and has been running for the fields $\mathbb{F}_q$ with $q \in \{2, 3, 4, 5, 7, 8, 9, 11, 16, 25, 27, 49, 81\}$ and values of $n \leq 5$. The implementation uses the fact that the elementary symmetric polynomials in $x_1, \ldots, x_n$ can be computed all at a time in quadratic time and linear space. In general huge text documents with very long expressions are produced. We can show here only some very small examples. The reader might find amusing to verify them.

$\mathbb{F}_2[X_1, X_2]$: $\dim_{\mathbb{F}_2} \mathcal{I}(2,2) = 2^2 - \mathrm{wn}(2,2) = 4 - 3 = 1$. The only one algebraic relation is:

$$S_1 S_2 \quad = \quad 0$$

Observe already by this first example that the polynomial $\Psi(S_1 S_2) = X_1^2 X_2 + X_1 X_2^2$, which in

$\mathbb{F}_2\{X_1, X_2\}$ is $= 2X_1X_2 = 0$. All other examples should be understood in this way and verified from this point of view.

$\mathbb{F}_2[X_1, X_2, X_3]$: $\dim_{\mathbb{F}_2}\mathcal{I}(2,3) = 2^3 - \mathrm{wn}(2,3) = 8 - 4 = 4$. Following basis has been found:

$$\begin{aligned} S_3 + S_2S_3 &= 0 \\ S_3 + S_1S_3 &= 0 \\ S_3 + S_1S_2 &= 0 \\ S_3 + S_1S_2S_3 &= 0 \end{aligned}$$

$\mathbb{F}_3[X_1, X_2, X_3]$: $\dim_{\mathbb{F}_3}\mathcal{I}(3,3) = 3^3 - \mathrm{wn}(3,3) = 27 - 10 = 17$. Following basis has been found:

$$\begin{aligned} 2S_2S_3^2 + S_1S_3 &= 0 \\ 2S_2S_3 + S_1S_3^2 &= 0 \\ S_2S_3^2 + S_2^2S_3^2 &= 0 \\ S_2S_3^2 + S_1S_2S_3 &= 0 \\ S_2S_3 + S_1S_2S_3^2 &= 0 \\ S_2S_3 + 2S_1S_2 + S_1S_2^2 &= 0 \\ 2S_2S_3^2 + S_1S_2^2S_3 &= 0 \\ 2S_2S_3 + S_1S_2^2S_3^2 &= 0 \\ S_2S_3 + S_2^2S_3 &= 0 \\ S_2S_3 + S_1^2S_3 &= 0 \\ S_2S_3^2 + S_1^2S_3^2 &= 0 \\ S_2 + 2S_2S_3^2 + S_2^2 + S_1^2S_2 &= 0 \\ 2S_2S_3 + S_1^2S_2S_3 &= 0 \\ 2S_2S_3^2 + S_1^2S_2S_3^2 &= 0 \\ S_2 + S_2S_3^2 + S_2^2 + S_1^2S_2^2 &= 0 \\ S_2S_3 + S_1^2S_2^2S_3 &= 0 \\ S_2S_3^2 + S_1^2S_2^2S_3^2 &= 0 \end{aligned}$$

$\mathbb{F}_4[X_1, X_2]$: The field $\mathbb{F}_4$ has been realized using the polynomial X^2+X+1 over $\mathbb{F}_2$. $\dim_{\mathbb{F}_4}\mathcal{I}(4,2) = 4^2 - \mathrm{wn}(4,2) = 16 - 10 = 6$. The found basis has really coefficients in $\mathbb{F}_2$:

$$\begin{aligned} S_1S_2 + S_1^2S_2^2 &= 0 \\ S_1S_2^2 + S_1^2S_2^3 &= 0 \\ S_1S_2^3 + S_1^2S_2 &= 0 \\ S_1S_2^2 + S_1^3S_2 &= 0 \\ S_1S_2^3 + S_1^3S_2^2 &= 0 \\ S_1S_2 + S_1^3S_2^3 &= 0 \end{aligned}$$

$\mathbb{F}_5[X_1, \ldots, X_5]$: $\dim_{\mathbb{F}_5}\mathcal{I}(5,5) = 5^5 - \mathrm{wn}(5,5) = 3125 - 126 = 2999$. The first identity found was:

$$4S_4^2S_5 + S_4^4S_5 + 3S_3S_4S_5^2 + 4S_3S_4^3S_5^2 + 3S_3S_4^4S_5^2 + 4S_3^2S_4S_5^3 + S_3^2S_4^4S_5^3 = 0.$$

$\mathbb{F}_7[X_1, \ldots, X_4]$: $\dim_{\mathbb{F}_7}\mathcal{I}(7,4) = 7^4 - \text{wn}(7,4) = 2401 - 210 = 2191$. The first identity found was:

$$S_4 + 6S_4^4 + 6S_3^6S_4 + S_3^6S_4^4 + 5S_2S_4^2 + 2S_2S_4^5 + 5S_2S_3^2S_4^2 + 2S_2S_3^2S_4^5 + 5S_2S_3^4S_4^2 +$$
$$+2S_2S_3^4S_4^5 + 6S_2^2S_4^3 + S_2^2S_4^6 + 6S_2^2S_3^2S_4^3 + S_2^2S_3^2S_4^6 + 6S_2^2S_3^4S_4^3 + S_2^2S_3^4S_4^6 = 0.$$

6 The original motivation

The original motivation for these computations was a graphical experiment did by the author.

Definition: Consider a finite set A, a fixed element $u \in A$ and a function $f : A^3 \to A$. Call **carpet** the recurrent double sequence $a : \mathbb{N} \times \mathbb{N} \to A$ with $a(0,m) = a(n,0) = u$ and $a(n,m) = f(a(n-1,m), a(n-1,m-1), a(n,m-1))$. The name carpet is justified by the fact that left upper minors of the infinite matrix $(a(n,m))$ can be represented as images, with a set of colours A.

In [4] the author proved that the recurrent double sequences encodes Turing machines even if we restrict them to the special case with commutative function f, and so have a lot of undecidable properties.

Using the interpolation, all carpets can be realized using polynomials over sufficiently big finite fields. In [5] the author showed that the carpets given by the polynomials $f(x,y,z) = x + my + z$ over $A = \mathbb{F}_q$ are self-similar and classified them according to their groups of symmetries.

Figures 1 and 2 show a carpet with $A = \mathbb{F}_5$, $u = 1$, and

$$f(x,y,z) = x^3y^3z^3 + 2x^2y^2z^2 + 2xyz + 3.$$

Let us call this carpet Spiderman. Looking at Spiderman, one sees that the border consists only of the colour 1, and that inside the carpet only the colours 2, 3, 4 occur. If the product of the elements x, y and z in $\mathbb{F}_5$ is p and $f(x,y,z) = g(p)$, then g operates on $\{2,3,4\}$ as the cycle $(2,3,4)$ and $g(1) = 3$.

After these remarks I was convinced that one can get Spiderman working over $\mathbb{F}_3$ if one forgets the border colour 1. I redefined the inner colours as $\{0,1,2\}$ such that the most frequently arising white colour was denoted by 0, and the former colour 2 is now 1 and I realized that the inner Spiderman is the iteration of a symmetric function $h \in \mathcal{S}(3,3)$ such that $h(0,0,2)$, $h(0,1,1)$ and $h(2,2,2)$ are 1; $h(0,1,2)$ and $h(1,1,1)$ are 2; and for the remaining 5 tuples in $\text{WM}(3,3)$ the value of h is 0. I started by writing a very naive program searching the solution as polynomial in elementary symmetric functions S_1, S_2 and S_3 and it found in a very short time some thousands of solutions. As we know now, all the naively found solutions lead to one and the same symmetric polynomial in $\vec{X}$.

Indeed, the non-homogenous system:

$$M(3,3)\ \vec{Y} = \vec{h}$$

has as set of solutions the class:

$$S_1 + 2S_2 + 2S_3 + 2S_1^2 + S_2^2 + S_2S_3 + S_2S_3^2 \quad + \quad \mathcal{I}(3,3).$$

The whole class is projected by Ψ on the polynomial $f \in \mathbb{F}_3\{x,y,z\}$:

$$f(x,y,z) = (x^2y^2z + x^2yz^2 + xy^2z^2) \ + \ (x^2y^2 + x^2z^2 + y^2z^2) \ + \ 2\ xyz \ +$$

$$+\ 2\ (x^2+y^2+z^2)\ +\ (x+y+z).$$

This polynomial constructs the Spiderman with $A = \mathbb{F}_3$ and $u = 1$. In our figures 0 = white, 1 = red and 2 = blue.

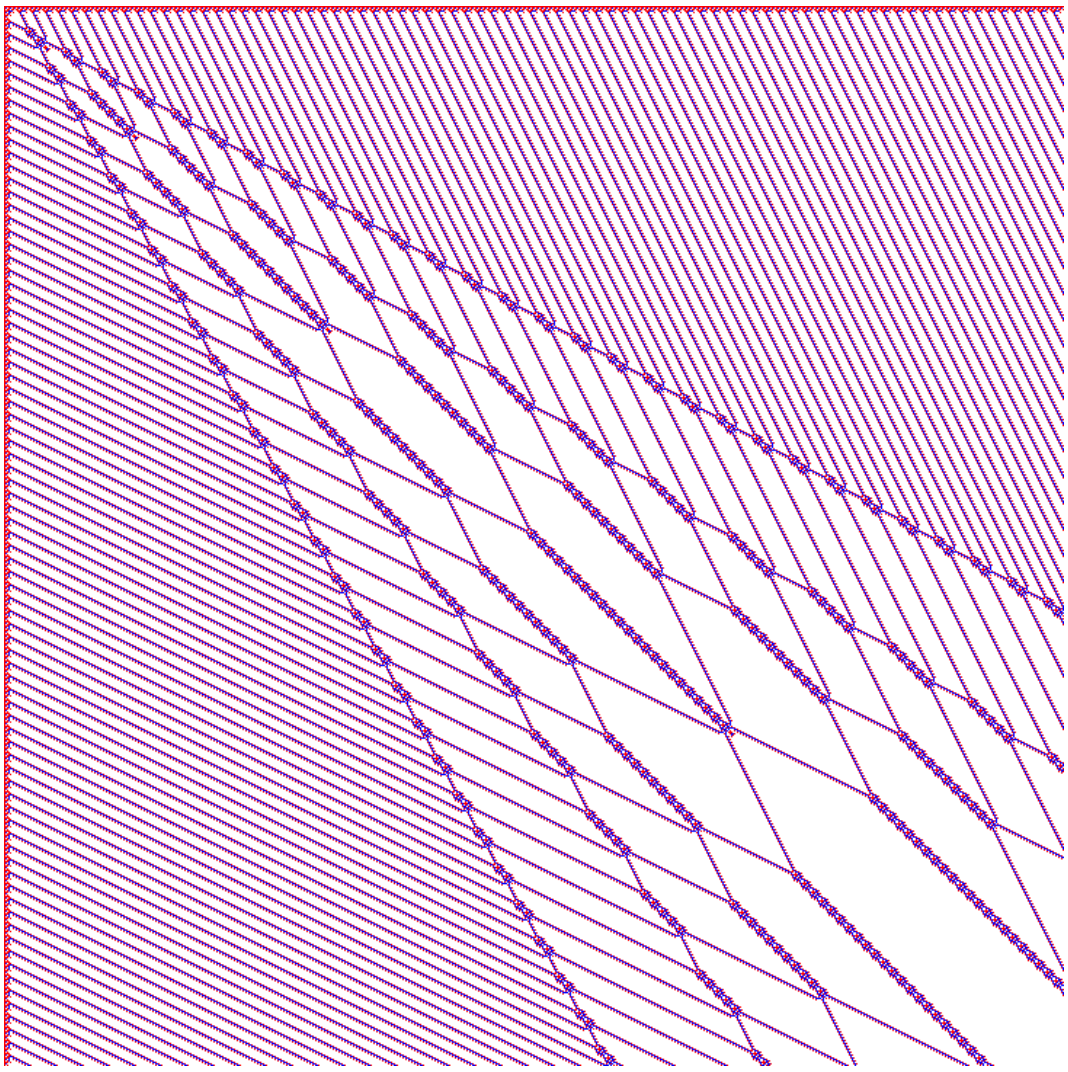

Figure 1: The $3^6 \times 3^6$ left upper minor of Spiderman.

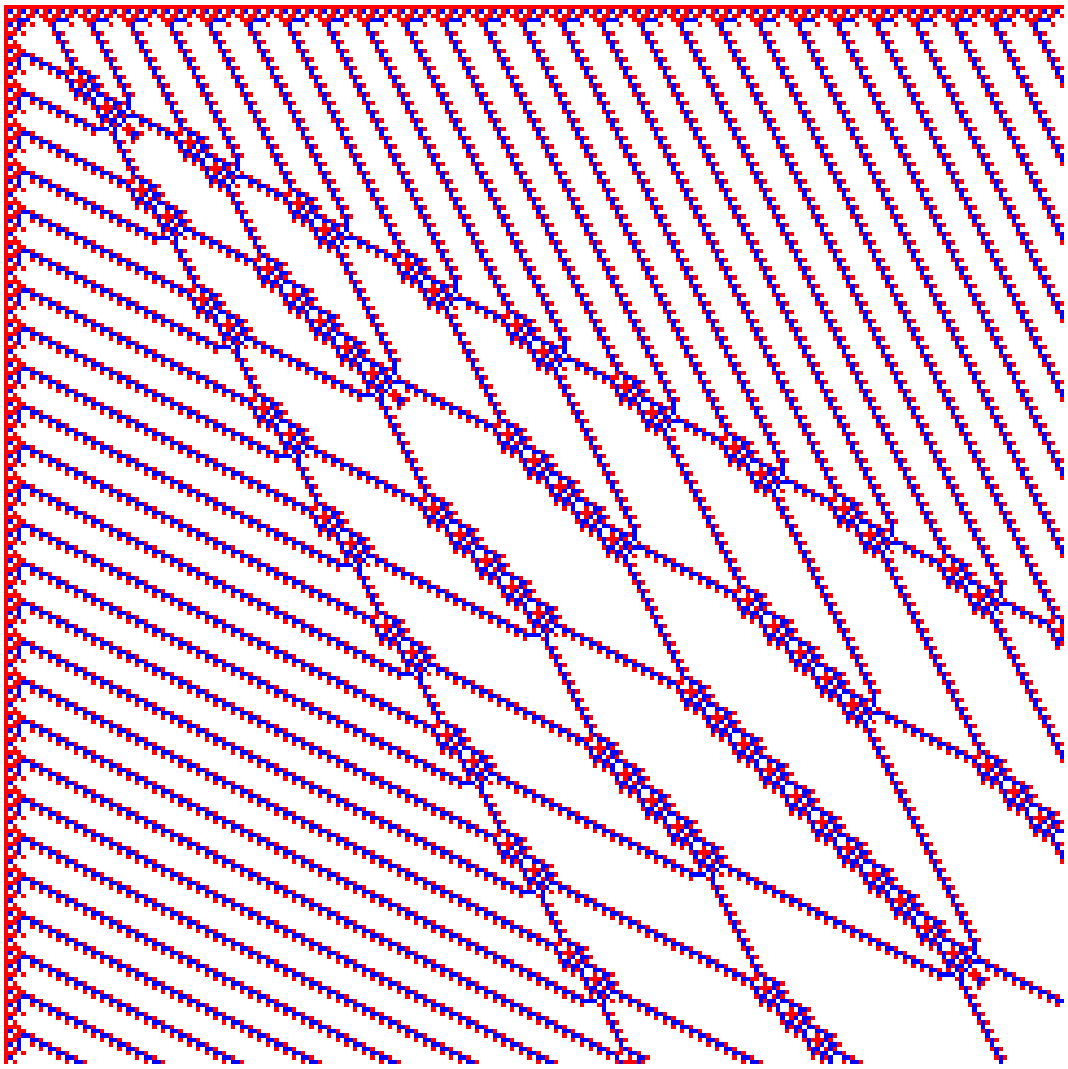

Figure 2: The $3^5 \times 3^5$ left upper minor of Spiderman.

References

[1] **Stasys Jukna**: *Extremal combinatorics.* Springer Verlag, Berlin, 2001.

[2] **I. G. Macdonald**: *Symmetric functions and Hall polynomials.* Oxford Science Publications, Clarendon Press, 1995.

[3] **A. Okounkov**: *On Newton interpolation of symmetric functions: A characterization of interpolation Macdonald polynomials.* Advances in Applied Mathematics, 20, 4, 395 - 428, 1998.

[4] **Mihai Prunescu**: *Undecidable properties of recurrent double sequences.* Notre Dame Journal of Formal Logic, 49, 2, 143 - 151, 2008.

[5] **Mihai Prunescu**: *Self-similar carpets over finite fields.* To appear in European Journal of Combinatorics.

[6] **Bernd Sturmfels**: *Algorithms in invariant theory.* Springer Verlag, Wien, 1993.

[7] **Bartel L. van der Waerden**: *Moderne Algebra I.* Springer Verlag Berlin, 1971.