Determinantal polynomials and the base polynomial of a square matrix over a finite field

Edoardo Ballico
Department of Mathematics, University of Trento, Trento, Italy

Received 12 October 2022
Revised 14 January 2023
28 February 2023
Accepted 28 February 2023

Abstract

Purpose – The author studies forms over finite fields obtained as the determinant of Hermitian matrices and use these determinatal forms to define and study the base polynomial of a square matrix over a finite field.

Design/methodology/approach – The authors give full proofs for the new results, quoting previous works by other authors in the proofs. In the introduction, the authors quoted related references.

Findings – The authors get a few theorems, mainly describing some monic polynomial arising as a base polynomial of a square matrix.

Originality/value – As far as the author knows, all the results are new, and the approach is also new.

Keywords Finite field, Hermitian matrix, Base polynomial, Numerical range

Paper type Research paper

1. Introduction

For any field K, any positive integer m and any number of variables $t_1, \ldots, t_{m,}$ we call $K[t_1, \ldots, t_m]$ the polynomial ring over K with variables $t_1, \ldots, t_m$, not the vector space of all polynomial functions $K^m \to K$. These two rings are isomorphic if and only if the field K is infinite. If K is a finite field, then the ring of polynomial functions $K^m \to K$ is isomorphic to $K[t_1, \ldots, t_m]/(t_1^K - t_1, \ldots, t_m^K - t_m)$. In this paper, we are always taking K finite, with either $\#K = q$ or $\#K = q^2$, where q is a fixed prime power.

Fix a prime p and a p-power q. For any $M = (m_{ij}) \in M_{n,n}(\mathbb{F}_{q^2})$, let $M^\dagger$ denote the matrix (m_{ji}^q). M is said to be *Hermitian* if $M = M^\dagger$. Note that the diagonal elements of a Hermitian matrix are elements of $\mathbb{F}_q$ and that the set of all Hermitian $n \times n$ matrices forms an $\mathbb{F}_q$ vector space of dimension n^2. We briefly recall the notion of Hermitian geometry for the Galois degree 2 extension $\mathbb{F}_{q^2}$ of $\mathbb{F}_q$. The Frobenius map $\sigma : t \to t^q$ is a generator of the Galois group of this degree 2 extension. The Hermitian form (i.e. σ-sesquilinear form) $\langle , \rangle : \mathbb{F}_{q^2}^n \times \mathbb{F}_{q^2}^n \to \mathbb{F}_{q^2}$ is defined by the formula

$$\langle (u_1, \ldots, u_n), (v_1, \ldots, v_n) \rangle := \sum_{i=1}^{n} u_i^q v_i.$$

JEL Classification — 15A33, 15A60, 12E20

Funding: The author was partially supported by MIUR and GNSAGA of INdAM (Italy).

Conflict of interests and funding declaration: The author has no conflict of interest and this research received no funding.

Arab Journal of Mathematical Sciences
Emerald Publishing Limited
e-ISSN: 2588-9214
p-ISSN: 1319-5166
DOI 10.1108/AJMS-10-2022-0242

Fix positive integers m, n and m $n \times n$ Hermitian matrices $M_1, \ldots, M_m \in M_{n,n}(\mathbb{F}_{q^2})$. Set

$$f_{M_1,\ldots,M_m}(t_1, \ldots, t_m) := \det(t_1 M_1 + \cdots + t_m M_m)$$

and call it the *determinantal polynomial* of the Hermitian matrices $M_1, \ldots, M_m$. For $m \geq 2$ set

$$g_{M_1,\ldots,M_{m-1}}(t_1, \ldots, t_m) := f_{M_1,\ldots,M_{m-1},\mathbb{I}_{n\times n}}(t_1, \ldots, t_m).$$

We say that $g_{M_1,\ldots,M_{m-1},\mathbb{I}_{n\times n}}(t_1, \ldots, t_m)$ is the *base polynomial* of the Hermitian matrices M_1, $\ldots$, M_{m-1}.

All polynomials $f_{M_1,\ldots,M_m}(t_1, \ldots, t_m)$ are homogeneous degree n polynomials with coefficients in $\mathbb{F}_q$ (Lemma 1).

The motivation for this paper came from Kippenhahn's paper on the numerical range, his definition of the base polynomial $f(x, y, z)$ and his use of the dual curve of the plane curve $\{f(x, y, z) = 0\}$ to characterize the numerical range ([1, 2]), which is even now a source of inspirations ([3, 4]). The numerical range of a matrix is also defined for matrices $M \in M_{n,n}(\mathbb{F}_{q^2})$ ([5–8]), using a choice of a certain element $\beta \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$ ([5, 6]). With this choice for any $M \in M_{n,n}(\mathbb{F}_{q^2})$, we get uniquely determined Hermitian matrices $M_+, M_- \in M_{n,n}(\mathbb{F}_{q^2})$ such that $M = M_+ + \beta M_-$ (see References [1, 2] for more details). The field $\mathbb{F}_{q^2}$ is a degree 2 extension of $\mathbb{F}_q$. First assume q odd. There is $\alpha \in \mathbb{F}_q$, which is a square in $\mathbb{F}_{q^2}$, but not in $\mathbb{F}_q$. We take $\beta \in \mathbb{F}_{q^2}$ such that $\beta^2 = \alpha$ and set $M_+ := (M + M^\dagger)/2$ and $M_- := (M - M^\dagger)/2\beta$. Now assume q even. There is $\varepsilon \in \mathbb{F}_q$ such that the polynomial $t^2 + t + \varepsilon$ has no root in $\mathbb{F}_q$. We call β one of its root in $\mathbb{F}_{q^2}$ (the other one is $\beta + 1$). We set $M_- := M + M^\dagger$ and $M_+ := (\beta + 1)M + \beta M^\dagger$.

Using M_+ and $M_{-,}$ one can use Kippelmahn's definition of the base polynomial of a square complex matrix and set

$$bp(M)(x, y, z) = g_{M_+,M_-}(x, y, z) = \det(xM_+ + yM_- + z\mathbb{I}_{n\times n}).$$

Note that $bp(M)$ is a homogeneous degree n polynomial with z^n as one of its monomials and that its coefficient is 1. We call *monic* such degree n forms. A form $f \in \mathbb{F}_q[t_1, \ldots, t_m]$ is said to be *concise* if there is no linear change of coordinates such that in the new coordinates f does not depend on all coordinates. For degree 2 forms conciseness is equivalent to the smoothness of their zero-locus (Remark 10).

In Sections 4 and 5, we study the realizability problem (which monic forms are of the form $bp(A)$ for some A) for 2×2 matrices. At the end of Section 4, we collect several questions concerning the base polynomials.

We get some negative results, i.e. many matrices have base polynomials not interesting and unrelated to the numerical range of any non-zero matrix. We prove the following result.

Theorem 1. *Fix $A \in M_{n,n}(\mathbb{F}_{q^2})$.*
(i) Assume either $A = A_+$ or $A = \beta A_-$. Then $bp(A) = z^n$ if and only if 0 is the unique eigenvalue of A over $\overline{\mathbb{F}}_q$.
(ii) There are q^2 2×2 matrices A such that $A = A_+$ (resp. $A = \beta A_-$) and $bp(A) = z^2$.
(iii) Assume $n = 2$. Then $bp(A) = z^2$ if and only if there are $a \in \mathbb{F}_q$, $e \in \mathbb{F}_q$, $c \in \mathbb{F}_{q^2}$, $d \in \mathbb{F}_{q^2}$ such that

$$-a^2 = c^{q+1}, \ -e^2 = d^{q+1}, \ -2ae = c^q d + cd^q \tag{1}$$

and $A = A_+ + \beta A_-$, where

$$A_+ = \begin{pmatrix} a & c \\ c^q & -a \end{pmatrix} \tag{2}$$

$$A_- = \begin{pmatrix} e & d \\ d^q & -e \end{pmatrix} \tag{3}$$

(iv) Assume q even. There are $(q-1)(q^2-1)$ matrices $A \in M_{2,2}(\mathbb{F}_{q^2})$ such that $bp(A) = z^2$, $A_+ \neq 0$ and $A_- \neq 0$. Each such A is of the form $A = A_+ + \beta A_-$ with A_+ and A_- as in (2) *and* (3)*. Each such matrix A is obtaining taking $c \in \mathbb{F}_{q^2}\backslash\{0\}$, $t \in \mathbb{F}_q\backslash\{0\}$, setting $d := tc$ and taking as a and e the only elements of $\mathbb{F}_q$ such that $a^2 = c^{q+1}$ and $e^2 = d^{q+1}$.*
(v) Take q odd. There are at least q^2 matrices $A \in M_{2,2}(\mathbb{F}_{q^2})$ such that $A_+ \neq 0$, $A_- \neq 0$ and $bp(A) = z^2$. Some of them may be obtained taking A_+ as in (2) *and taking $A = A_+ + \beta A_+$.*

Remark 1. Concerning part (i) of Theorem 1, we have a complete description of the q^2 matrices. The ones with $A = A_+$ (resp. $A = \beta A_-$) are the ones described in (2) (resp. (3)) with a, c (resp. e, d) as in (1).

We get some positive results (obtaining a monic polynomial as the base polynomial of a square matrix). This is called the *reconstruction problem for monic polynomials*. We prove the case of 2 × 2 matrices, i.e. we prove the following result.

Proposition 1. All monic degree 2 forms are realized as a base polynomial.

Definition 1. Let K be a field. Take $f \in K[x_1, \ldots, x_n]$. We say that f depends on n variables or that it does not depend on $< n$ variables or that it is *concise* if there is no pair (g, M), where $M \in M_{n-1,n}(K)$, $g \in K[y_1, \ldots, y_{n-1}]$ and $f(x_1, \ldots, x_n) = g(y_1, \ldots, y_{n-1})$, where

$$(y_1, \ldots, y_{n-1}) = M(x_1, \ldots, x_n)^t.$$

We say that the polynomial 0 depends on 0 variables. In Section 3, we study the conciseness of some determinantal polynomial and of some base polynomial, with the main results only for 2 × 2 matrices. We conclude Section 3 with several questions.

We found only a weak connection between the study of our determinantal polynomial and the (in principle) very similar problem of the description of a homogeneous form as a determinant of a matrix of linear forms. A. Beauville wrote the beautiful paper [9], which also contains realization as the determinant of a symmetric matrix of linear forms and as the Pfaffian of an anti-symmetric matrix. We discuss this topic in Section 5 which studies $bp(A)$ for a matrix $M \in M_{n,n}(\mathbb{F}_{q^2})$ such that $M_+ \in M_{n,n}(\mathbb{F}_q)$ and $M_- \in M_{n,n}(\mathbb{F}_q)$. Of course, it depends on the choice of $\beta \in \mathbb{F}_{q^2}\backslash\mathbb{F}_q$. Section 5 also contains the use of [9] for $f_{M_1,\ldots,M_m}$, mainly for $m = 3$.

We thank a referee for useful suggestions.

2. Preliminaries

For any matrix $M = (a_{ij}) \in M_{n,n}(\mathbb{F}_{q^2})$ set $M^{(q)} = (a_{ij}^q)$. Thus, M is Hermitian if and only if $M^t = M^{(q)}$. Note that $(M_1 + M_2)^{(q)} = M_1^{(q)} + M_2^{(q)}$ and that $(tM)^{(q)} = t^q M^{(q)}$ for all $t \in \mathbb{F}_{q^2}$.

Remark. 2 Assume $q = p^e$ for some $e > 0$. The field $\mathbb{F}_q$ is the set of all $z \in \overline{\mathbb{F}}_p$ such that $z^q = z$ ([10, page 1], [11, Theorem 2.5]). Fix any $a \in \mathbb{F}_q\backslash\{0\}$. Since $q + 1$ is invertible in $\mathbb{F}_q$, the polynomial $t^{q+1} - a$ and its derivative $(q+1)t^q$ have no common zero. Hence, the polynomial $t^{q+1} - a$ has $q + 1$ distinct roots in $\overline{\mathbb{F}}_q$. Fix any one of them, b. Since $a^{q-1} = 1$, $b^{q^2-1} = 1$. Thus, $b \in \mathbb{F}_{q^2}$. Thus, for any $a \in \mathbb{F}_q\backslash\{0\}$ there are exactly $q + 1$ elements $c \in \mathbb{F}_{q^2}$ such that $c^{q+1} = a$. Obviously, 0 is the only element t of $\mathbb{F}_{q^2}$ such that $t^{q+1} = 0$.

Remark 3. Note that $(-1)^q = -1$ in $\mathbb{F}_q$. Since $(u+v)^q = u^q + v^q$ and $(u-v)^q = u^q + (-1)^q v^q = u^q - v^q$ for all $u, v \in \mathbb{F}_{q^2}$, $\det(M^{(q)}) = \det(M)^q$ for all $M \in M_{n,n}(\mathbb{F}_{q^2})$. Now assume that M is Hermitian, i.e. assume $M = M^\dagger$. Thus, $\det(M) = \det((M^{(q)})^t) = \det(M^{(q)}) = \det(M)^q$. Hence, $\det(M) \in \mathbb{F}_q$ by Remark 2.

Remark 4. For any two Hermitian matrices $A, B \in M_{n,n}(\mathbb{F}_{q^2})$, there is a unique $M \in M_{n,n}(\mathbb{F}_{q^2})$ such that $A = M_+$ and $B = M_-$, the matrix $M = A + \beta B$.

Remark 5. Take $A, B \in M_{n,n}(\mathbb{F}_{q^2})$ and $a, b \in \mathbb{F}_q$. We have $(aA + bB)_+ = aA_+ + bB_+$ and $(aA + bB)_- = aA_- + bB_-$. Usually these equalities fail if $a \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. For instance, if A is Hermitian, $A \neq 0$ and $a = \beta$, then $(aA)_+ = 0$, while $(aA)_- = A$.

For any $A = (a_{ij}) \in M_{n,n}(\mathbb{F}_{q^2})$ and any $B = (b_{ij}) \in M_{m,m}(\mathbb{F}_{q^2})$ let $A \oplus B$ denote the matrix $(c_{ij}) \in M_{n+m,n+m}(\mathbb{F}_{q^2})$ such that $c_{ij} = a_{ij}$ if $1 \le i \le n$ and $1 \le j \le n$, $c_{ij} = 0$ if either $i > n$ and $j \le n$ or $i \le n$ and $j > n$, $c_{ij} = b_{i-a,j-n}$ if $i > n$ and $j > n$. The matrix $A \oplus B$ is called the unitary direct sum of A and B. Since $(A \oplus B)_+ = A_+ \oplus B_+$ and $(A \oplus B)_- = A_- \oplus B_-$, $bp(A \oplus B) = bp(A)bp(B)$.

Lemma 1. *Fix positive integers m, n and take m $n \times n$ Hermitian matrices $M_1, \dots, M_m \in M_{n,n}(\mathbb{F}_{q^2})$. Then $f_{M_1,\dots,M_m}(t_1, \dots, t_m) \in \mathbb{F}_q[t_1, \dots, t_m]$*

Proof. Since $M_i \in M_{n,n}(\mathbb{F}_{q^2})$ for all i, $f_{M_1,\dots,M_m}(t_1, \dots, t_m) \in \mathbb{F}_{q^2}[t_1, \dots, t_m]$. Thus to prove that $f_{M_1,\dots,M_m}(t_1, \dots, t_m) \in \mathbb{F}_q[t_1, \dots, t_m]$, it is sufficient to prove that all its coefficients are preserved by the Frobenius map $x \mapsto x^q$. Let $\alpha \in \mathbb{F}_{q^2}$ be the coefficient of $t_1^{e_1} \cdots t_m^{e_m}$. Since the Frobenius map is additive, $\alpha^q t_1^{e_1} \cdots t_m^{e_m}$ is a monomial of $f_{M_1^q,\dots,M_m^q}(t_1, \dots, t_m)$. Recall that $\det(M_i)^q = \det(M_i^{(q)})$ (Remark 3). Since $\det(M_i^{(q)}) = \det((M_i^{(q)})^t)$ and $M_i^\dagger = (M_i^q)^t$, then $\alpha^q = \alpha$. Hence, $\alpha \in \mathbb{F}_q$ (Remark 2). □

Lemma 2. *Take $M \in M_{2,2}(\mathbb{F}_{q^2})$ such that $M = M^\dagger$. The matrix M has 0 as its unique eigenvalue in $\overline{\mathbb{F}}_q$ if and only if there are $a \in \mathbb{F}_q$ and $c \in \mathbb{F}_{q^2}$ such that*

$$M = \begin{pmatrix} a & c \\ c^q & -a \end{pmatrix}, \text{ where}$$

$$-a^2 = c^{q+1} \tag{4}$$

Moreover, there are exactly q^2 such matrices.

Proof. A 2×2 matrix over a field K has 0 as its unique eigenvalue over the algebraic closure of K if and only if its traces and determinant are 0. Since $M = M^\dagger$, these are exactly the conditions on the entries of M stated in the lemma. For any $a \in \mathbb{F}_q \setminus \{0\}$, there are $q+1$ elements $c \in \mathbb{F}_{q^2}$ such that $c^{q+1} = -a^2$ (Remark 2). 0 is the unique $c \in \mathbb{F}_{q^2}$ such that $c^{q+1} = 0$. Since $(\mathbb{F}_q \setminus \{0\}) = q - 1$, there are $1 + (q-1)(q+1) = q^2$ such matrices. □

Remark 6. The definition of $bp(A)$ depends on the definitions of A_+ and A_-, which depend on the choice of a suitable $\beta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. We explore the dependency of A_+, A_- and $bp(A)$ for different choices of β if q is odd. Assume q odd. Take a different choice and call it γ. We write $A_+(\beta)$, $A_-(\beta)$, $bp(A)_\beta$, $A_+(\gamma)$, $A_-(\gamma)$ and $bp(A)_\gamma$ for the matrices and polynomials obtained from these two choices. Since q is odd, $A_+(\beta) = A_+(\gamma)$ and $A_-(\gamma) = \frac{\gamma}{\beta} A_-(\beta)$. Thus, $bp(A)_\gamma(x, y, z) = bp(A)_\beta\left(x, \frac{\gamma}{\beta} y, z\right)$.

Remark 7. For all integers $d \geq 0$ and any field K, let $K[x,y,z]_d$ denote the set of all homogeneous degree d polynomials in the variables x, y, z with coefficients in K. The set $K[x,y,z]_d$ is a K-vector space of dimension $\binom{d+2}{2}$. Fix $M \in M_{n,n}(\mathbb{F}_{q^2})$. We have $bp(M) \in \mathbb{F}_q[x,y,z]_n$ for every $M \in M_{n,n}(\mathbb{F}_{q^2})$ (Lemma 1).

Lemma 3. *Take $f(x,y,z) \in \mathbb{F}_q[x,y,z]_n$ such that $f(x,y,z) = (z+ax+by)^n$ for some $a,b \in \overline{\mathbb{F}}_q$. Then $a,b \in \mathbb{F}_q$.*

Proof. Since $\mathbb{F}_q$ is a perfect field, the plane $\{z+ax+by=0\}$ is defined over $\mathbb{F}_q$. Thus, there is $c \in \overline{\mathbb{F}}_q$, $c \neq 0$, such that $c(z+ax+by) \in \mathbb{F}_q[x,y,z]_1$. Since $c \neq 0$, we first get $c \in \mathbb{F}_q$ and then $a,b \in \mathbb{F}_q$. □

Proof of Theorem 1. :Assume $A = A_+$, i.e. assume $A_- = 0$. Thus, $bp(A) = \det(Ax + \mathbb{I}_{n\times n}z) \in \mathbb{F}_q[x,z]$. Since the eigenvalues of A are the roots of the polynomial $\det(A - t\mathbb{I}_{n\times n})$, we get that $bp(A) = z^n$ if and only if all eigenvalues of A are 0, i.e. we get part (i) for $A = A_+$. If $A = \beta A_-$, then just note that $bp(A) = bp(A_-)$ up to changing the names of the variables.

Now assume $n = 2$. Part (ii) follows from Lemma 2. Part (iii) follows from part (ii) and the explicit computation of the coefficient of xy in the base polynomial $bp(A)$.

Now assume $n = 2$ and q even. Since q is a 2-power, $-2ae = 0$ in $\mathbb{F}_q$. Let $\mathcal{U}$ denote the set of all $(c,d) \in (\mathbb{F}_{q^2}\backslash\{0\})^2$ such that $c^q d + cd^q = 0$. Since q is even, $(c,d) \in \mathcal{U}$ if and only if c, d are non-zero elements of $\mathbb{F}_{q^2}$ and $\left(\frac{d}{c}\right)^{q-1} = 1$. By Remark 2, the set $\mathbb{F}_q\backslash\{0\}$ is the set of all $t \in \mathbb{F}_{q^2}$ such that $t^{q-1} = 1$. Thus for every $c \in \mathbb{F}_{q^2}\backslash\{0\}$, there are exactly $q-1$ elements $d \in \mathbb{F}_{q^2}$ such that $(c,d) \in \mathcal{U}$, the elements $\{tc\}_{t\in\mathbb{F}_q\backslash\{0\}}$. Take $(c,d) \in \mathcal{U}$. Since $\mathbb{F}_q$ is a perfect field and q is even, for every $z \in \mathbb{F}_q$ there is a unique $w \in \mathbb{F}_q$ such that $w^2 = z$. Thus for all $(c,d) \in \mathcal{U}$, there are unique a, e such that c, d, a, e satisfy (1).

Now we prove part (v). Assume $n = 2$ and q odd. Take a, c satisfying the first equation of (1) and set $e := a$ and $d := c$. Note that all equations in (1) are satisfied. □

3. Conciseness of determinantal polynomials

Remark 8. Fix a field K and $f \in K[x_1,\ldots,x_n]_d\backslash\{0\}$. The form f is concise over $\overline{K}$ if and only if the degree d hypersurface $\{f=0\} \subset \mathbb{P}^{n-1}(\overline{K})$ is not a cone. Note that this criterion gives the same answer if we take the irreducible components of the hypersurface $f = 0$ with their multiplicity or not.

Lemma 4. *Fix fields $K \subseteq L \subseteq \overline{K}$ and $f \in K[x_1,\ldots,x_n]_d$, $d \geq 2$, $f \neq 0$. Assume that K is perfect. The form f is concise over L if and only if it is concise over K.*

Proof. If f is concise over a field $K' \supset K$, then f is concise over K. Thus, it is sufficient to prove that if f is not concise over $\overline{K}$, then it is not concise over K. Assume that f is not concise over $\overline{K}$, i.e, that the closed hypersurface $X(\overline{K})$ of $\mathbb{P}^{n-1}(\overline{K})$ with f as its equation is a cone with, say, vertex $E(\overline{K})$; in the definition of $X(\overline{K})$, we allow the multiplicities of the indecomposable factors of f (Remark 8). The set $E(\overline{K})$ is a non-empty $\overline{K}$ linear subspace of $\mathbb{P}^{n-1}(\overline{K})$. The decomposition of f in its irreducible factors and the linear subspace $E(\overline{K})$ are defined over a finite extension K' of K. Since $K[x_1, \ldots, x_n]$ is UFD, we reduce to the case in which f is irreducible over K. Since K is perfect, each indecomposable factor of f over $\overline{K}$ has multiplicity 1 and hence, up to a non-zero multiplicative constant, f is uniquely determined by the set $X(\overline{K})$ (no multiplicity is required). Since K is perfect, there is a finite extension L of K' such that L is a Galois extension of K, say with Galois group G. The finite group G acts on $X(\overline{K})$.

Set $e := \dim E(\overline{K})$. Let v the minimsl dimension of a $\overline{K}$ linear subspace of $\mathbb{P}^n(\overline{K})$ contained in $X(\overline{K})$ and containing $E(\overline{K})$. Let $\mathcal{S}$ be the set of all v-dimensional $\overline{K}$ linear subspace of $\mathbb{P}^{n-1}(\overline{K})$ contained in $X(\overline{K})$. Since $X(\overline{K})$ is a cone with vertex $E(\overline{K})$, $v > 0$, $\cup_{L\in\mathcal{S}} L = X(\overline{K})$ and $\cap_{L\in\mathcal{S}} L = E(\overline{K})$. Since the embedding of $X(\overline{K})$ in $\mathbb{P}^{n-1}(\overline{K})$ is defined over K, G acts linearly on $\mathbb{P}^{n-1}(\overline{K})$ and hence it acts on $\mathcal{S}$, i.e. each $g \in G$ induces a permutation of $\mathcal{S}$. Thus, $g(\cap_{L\in\mathcal{S}} L) = \cap_{L\in\mathcal{S}} g(L)$ for all $g \in G$. Since each $g \in G$ induces a permutation of $\mathcal{S}$ and $\cap_{L\in\mathcal{S}} L = E(\overline{K})$, we get $g(E(\overline{K})) = E(\overline{K})$ for all $g \in G$. Thus $E(\overline{K})$ is defined over K. Since $E(\overline{K})$ is defined over K, there are $n - e$ linear forms $y_0, \dots, y_{n-e-1} \in K[x_1, \dots, x_n]_1$ such that $E(\overline{K}) = \{y_0 = \cdots = y_{n-e-1} = 0\}$. Since $E(\overline{K})$ is defined over K, there are $y_{n-e}, \dots, y_n \in K[x_1, \dots, x_n]_1$ such that $y_0, \dots, y_n$ is a new system of coordinates of $\mathbb{P}^{n-1}(\overline{K})$ and $y_{n-e}, \dots, y_n$ are the homogeneous coordinates of $E(\overline{K})$. Set $W := \{y_{n-e} = \cdots = y_n = 0\}$. Note that W is a linear subspace of $\mathbb{P}^{n-1}$ defined over K, $W(\overline{K}) \cap E(\overline{K}) = \emptyset$, $\dim W(\overline{K}) + \dim E(\overline{K}) = n - 2$ and $y_0, \dots, y_{n-e-1}$ are homogeneous coordinates of W. Call $\tilde{W}$ the linear subspace of $\overline{K}^n$ associated to W. Set $u := f_{|\tilde{W}} \in \overline{K}[y_0, \dots, y_{n-e-1}]_d$. Since $X(\overline{K}) \neq \mathbb{P}^{n-1}(\overline{K})$ and $X(\overline{K})$ is a cone with vertex $E(\overline{K})$, $X(\overline{K}) \cap W(\overline{K}) \neq W(\overline{K})$, i.e. $u \neq 0$. Since f and W are defined over K, $u \in K[y_0, \dots, y_{n-e-1}]_d$. Since $X(\overline{K})$ is a cone with vertex $E(\overline{K})$, u (as an element of $K[y_0, \dots, y_n]_d$) is an equation of $X(\overline{K})$. Thus, f is not concise over K. □

For each prime power q and each $n \geq 2$, let $m(q, n)$ be the maximal integer m such that there are m Hermitian matrices $M_1, \dots, M_m \in M_{n,n}(\mathbb{F}_{q^2})$ such that the degree n form $f_{M_1,\dots,M_m}(t_1, \dots, t_m) \in \mathbb{F}_q[t_1, \dots, t_m]_n$ is concise over $\overline{\mathbb{F}}_q$. By Lemma 4, we get the same integer $m(q, n)$ if we prescribe that $f_{M_1,\dots,M_m}(t_1, \dots, t_m) \in \mathbb{F}_q[t_1, \dots, t_m]_n$ is concise over $\mathbb{F}_q$.

Remark 9. Fix any q. Let $M_i \in M_{n,n}(\mathbb{F}_{q^2})$, $1 \leq i \leq n$, be the Hermitian matrix with 1 at (i, i) and 0 elsewhere. Since $f_{M_1,\dots,M_m}(t_1, \dots, t_m) = \prod_{i=1}^n t_i$, Remark 8 and Lemma 4 give $m(q, n) \geq n$.

Lemma 5. *Take Hermitian matrices $M_1, \dots, M_m \in M_{n,n}(\mathbb{F}_{q^2})$ which are linearly dependent over $\mathbb{F}_q$. Then $f_{M_1,\dots,M_m}(t_1, \dots, t_m)$ is not concise over $\mathbb{F}_q$.*

Proof. Suppose for instance that $M_m = c_1M_1 + \cdots + c_{m-1}M_{m-1}$ for some $c_i \in \mathbb{F}_q$. Take the new variables $x_i = t_i + c_it_m$, $1 \leq i \leq m-1$, and $x_m = t_m$. Note that $f_{M_1,\dots,M_m}(t_1, \dots, t_m) = f_{M_1,\dots,M_m}(x_1, \dots, x_{m-1}, 0)$. □

Proposition 2. For any prime power q we have $m(q, 2) = 4$.

Proof. The set of all Hermitian $M \in M_{n,n}(\mathbb{F}_{q^2})$ is an n^2-dimensional vector space over $\mathbb{F}_q$. Thus, Lemma 5 gives $m(q, 2) \leq 4$. Hence, it is sufficient to prove that $m(q, 2) \geq 4$. If q is even fix any $c \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$. If q is odd fix any $c \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$ such that $c^{4q} - 2c^{2q+2} + c^4 \neq 0$. Set

$$M_1 := \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},\ M_2 := \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},\ M_3 := \begin{pmatrix} 0 & c \\ c^q & 0 \end{pmatrix},\ M_4 := \begin{pmatrix} 0 & c^q \\ c & 0 \end{pmatrix}.$$

First assume q even. Since $c \notin \mathbb{F}_q$, then $c^{q-1} \neq 1$ and $c \neq 0$. Thus $c^q + c \neq 0$. Consider the degree 2 binary form $h(t_3, t_4) := c^{q+1}t_3^2 + c^{q+1}t_4^2 + (c^2 + c^{2q})t_3t_4$. Since the coefficients of t_3^2 and t_4^2 in $h(t_3, t_4)$ are the same and the coefficient of t_3t_4 is non-zero, $h(t_3, t_4)$ is not a square. Thus, $h(t_3, t_4)$ is concise. The binary form t_1t_2 in the variables t_1 and t_2 is concise. The quaternary form $f_{M_1,M_2,M_3,M_4}(t_1, t_2, t_3, t_4) = t_1t_2 + c^{q+1}t_3^2 + c^{q+1}t_4^2 + (c^2 + c^{2q})t_3t_4$ is concise, because the binary forms t_1t_2 and $h(t_3, t_4)$ are concise.

Now assume q odd. We show that we may take $c \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$ such that $c^{4q} - 2c^{2q+2} + c^4 \neq 0$, i.e. $c^{4q-4} - 2c^{2q-2} + 1 \neq 0$. If $q \geq 5$, it is sufficient to use that $(\mathbb{F}_{q^2} \backslash \mathbb{F}_q) = q^2 - q > 4q - 4$. Now assume $q = 3$. Each $c \in \mathbb{F}_9$, $c \neq 0$, satisfies $c^8 = 1$ and hence it is sufficient to take c such that $c^4 \neq -1$, i.e. $c^4 = 1$. The quaternary form $f_{M_1,M_2,M_3,M_4}(t_1,t_2,t_3,t_4) = t_1t_2 - c^{q+1}t_3^2 - c^{q+1}t_4^2 + (c^2 + c^{2q})t_3t_4$ is concise if and only if the binary form $u(t_3,t_4) := -c^{q+1}t_3^2 - c^{q+1}t_4^2 + (c^2 + c^{2q})t_3t_4$ in the variables t_3, t_4 is concise. The binary form $u(t_3, t_4)$ is concise, because it has degree 2, $-c^{q+1} \neq 0$, and the polynomial $-c^{q+1}t^2 + (c^2 + c^{2q})t - c^{q+1}$ has 2 distinct roots over $\overline{\mathbb{F}}_q$ by our assumptions on c. □

We ask the following question.

Question 1. Fix $n \geq 2$ and a prime power q. Set $m := m(q, n)$. Is it possible to find m Hermitian matrices $M_1, \ldots, M_m$ such that $f_{M_1,\ldots,M_m}$ defines a smooth hypersurface (smooth at all points of $\mathbb{P}^{m-1}(\overline{\mathbb{F}}_q)$)?

Remark 10. Recall that a form f in n variables is concise if and only if the hypersurface $\{f = 0\}$ is not a cone (Remark 8 and Lemma 4). For $n = 2$, Question 1 is trivially true, because for quadric hypersurfaces not to be a cone is equivalent to smoothness ([10, Lemma 5.1.1]).

Remark 11. Obviously $m(q, n + 1) \geq m(q, n)$ for all q and n. We do not know the rate of growth of $m(q, n)$ for a fixed q and $n \gg 0$. We have $m(q, n) \leq n^2$ for all n (Lemma 5), but we do not know the values of lim $\sup_{n\longrightarrow+\infty} m(q,n)/n^2$ and lim $\inf_{n\longrightarrow+\infty} m(q,n)/n^2$.

4. Realization of homogeneous polynomials

In this section, we consider the realization problem, i.e. we ask for which homogeneous polynomial $f \in \mathbb{F}_q[t_1, \ldots, t_m]_n$ there are Hermitian matrices $M_1, \ldots, M_m \in M_{n,n}(\mathbb{F}_{q^2})$ such that $f = f_{M_1,\ldots,M_m}$. The interested reader should consider the problem of the descriptions of the m-ples $(M_1, \ldots, M_m)$ such that $f = f_{M_1,\ldots,M_m}$.

We only consider the cases $m = 1$ and $m = 2$ and the case $m = 3$ with $M_3 = \mathbb{I}_{n\times n}$, i.e. the case of base polynomials, and prove Proposition 1.

4.1 Forms in m $\leq$ *2 variables*

Remark 12. Since $\det(M_1t_1) = \det(M_1)t_1^n$ and for each $a \in \mathbb{F}_q$ there is a Hermitian M_1 such that $\det(M_1) = a$ (even with M_1 diagonal), the realization problem is trivially satisfied for $m = 1$.

Remark 13. Here we observe that the set of all binary n-forms realized by some f_{M_1,M_2} is invariant for the action of $GL(2, \mathbb{F}_q)$ on the variables x, y. For instance, $f_{M_1,M_2}(y,x) = f_{M_2,M_1}(x,y)$ and $f_{M_1,M_2}(x + ay, y) = f_{M_1,aM_1+M_2}(x,y)$ for any $a \in \mathbb{F}_q$. Use that these transformations generate the group of projective transformations acting on binary forms.

Now take $m = 2$. We are looking to the realization of binary n-forms, and we call x and y the two variables and M_1 and M_2 the two Hermitian matrices.

Proposition 3. Take $f \in \mathbb{F}_q[x,y]$. Then there are Hermitian 2×2 matrices M_1, M_2 such that $f = f_{M_1,M_2}$.

Proof. By Remark 13, it is sufficient to realize at least one element for each orbit for the action of $GL(2, \mathbb{F}_q)$.

The binary form 0 is realized by $M_1 = M_2 = 0$. The binary form x^2 is realized taking $M_1 = \mathbb{I}_{2\times 2}$ and $M_2 = 0$. The binary form $x(x + y)$ is (up to an $\mathbb{F}_q$ linear transformation of $\mathbb{F}_q^2$)

the only one with 2 distinct roots over $\mathbb{F}_q$. This form is realized taking $M_1 = \mathbb{I}_{2\times 2}$ and $M_2 = (b_{ij})$, where $b_{11} = b_{12} = b_{21} = 0$ and $b_{22} = 1$.

Now we consider binary forms which split over $\mathbb{F}_{q^2}$, but not over $\mathbb{F}_q$.

First assume q odd. Up to an $\mathbb{F}_q$ linear transformation it is sufficient to realize the form $x^2 - ay^2$ with a not a square in $\mathbb{F}_q$. Take $c \in \mathbb{F}_{q^2}$ such that $c^{q+1} = a$ (Remark 2). Take $A = \mathbb{I}_{2\times 2}$ and $B = (b_{ij})$, where $b_{11} = b_{22} = 0$, $b_{12} = c$ and $b_{21} = c^q$.

Now assume $q = 2^e$ even. Since every element of $\mathbb{F}_q$ is a square, the form $x^2 + cy^2$ splits and hence up to an $\mathbb{F}_q$ linear transformation, it is sufficient to realize the form $x^2 + xy + \delta y^2$, where $\delta \in \mathbb{F}_q \setminus 0$ has non-zero absolute trace $D(\delta)$, where $D(u) = \sum_{i=0}^{e-1} u^{2^i}$ for any $u \in \mathbb{F}_q$ ([10, p. 3]). Fix any $\delta \in \mathbb{F}_q$ and take $c \in \mathbb{F}_{q^2}$ such that $c^{q+1} = \delta$. Take $A = \mathbb{I}_{2\times 2}$ and $B = (b_{ij})$, where $b_{11} = 1$, $b_{12} = c$, $b_{21} = c^q$ and $b_{22} = 0$. □

4.2 Base polynomials

Now we take $m = 3, M_3 = \mathbb{I}_{n\times n}, M_1 = A_+, M_2 = A_-$ for some $A \in M_{n,n}(\mathbb{F}_{q^2})$. By Remark 4, it is not restrictive to the existence of a matrix A such that $M_1 = A_+$ and $M_2 = A_-$. We call x, y and z the variables. Every degree n base polynomial contains the monomial z^n with degree 1. We call *monic* such forms.

Question 2. Are there other restrictions?

Remark 14. Let $\mathcal{R}$ denote the set of all polynomials $bp(A)$ with $A \in M_{3,3}(\mathbb{F}_{q^2})$. Take any $a, b \in \mathbb{F}_q$ and any $A \in M_{3,3}(\mathbb{F}_{q^2})$. Since $a \in \mathbb{F}_q$, we have $(A + aA_-)_+ = A_+ + aA_-$ and $(A + aA_-)_- = A_-$. Thus, $bp(A + aA_-)(x, y, z) = bp(A)(x + ay, y, z)$. Hence, $\mathcal{R}$ is invariant for the linear transformations $x \mapsto x + ay$, $y \mapsto y$, $z \mapsto z$. Since $a \in \mathbb{F}_q$, we have $(A + a\beta A_+)_+ = A_+$ and $(A + a\beta A_+)_- = A_- + aA_+$. Thus, $bp(A + a\beta A_+)(x, y, z) = bp(A)(x, ax + y, z)$. Hence, $\mathcal{R}$ is invariant for the linear transformations $x \mapsto x$, $y \mapsto ax + y$, $z \mapsto z$. Since $a, b \in \mathbb{F}_q$, we have $(A + (a + \beta b)\mathbb{I}_{n\times n})_+ = A_+ + a\mathbb{I}_{n\times n}$ and $(A + (a + \beta b)\mathbb{I}_{n\times n})_- = A_- + b\mathbb{I}_{n\times n}$. Thus, $bp(A + (a + \beta b)\mathbb{I}_{n\times n})(x, y, z) = bp(A)(x, y, z + ax + by)$. Thus, $\mathcal{R}$ is invariant for the linear transformations $x \mapsto x$, $y \mapsto y$, $z \mapsto z + ax + by$. Thus, the set $\mathcal{R}$ is invariant for all changes of coordinates $(g_{ij}) \in GL(3, \mathbb{F}_q)$ such that $g_{33} = 1$.

Remark 15. Take a monic $f(x, y, z) \in \mathbb{F}_q[x, y, z]_n$ such that $f = gh$ for some monic g, h and $0 < a := \deg(g) < d$. Assume $g = bp(A)$ and $h = bp(B)$ for some $A \in M_{a,a}(\mathbb{F}_{q^2})$, $B \in M_{n-a,n-a}(\mathbb{F}_{q^2})$. Then $f = bp(A \oplus B)$. In particular, if f splits over $\mathbb{F}_q$ as a product of n monic linear forms (we allow multiple linear forms), then $f = bp(M)$ for some $M \in M_{n,n}(\mathbb{F}_{q^2})$. Now assume that f is the product of n linear forms over $\mathbb{F}_q$, say $f = L_1 \cdots L_n$ with $L_i = c_i z_i + a_i x + b_i y$, but we allow that some of the forms are not monic. We get $\prod_{i=1}^{n} c_i = 1$, and hence f is the product of the n monic linear forms $z + \frac{a_i}{c_i} x + \frac{b_i}{c_i} y$.

Proof of Proposition 1. :By Remark 14, it is sufficient to realize at least one form for each orbit for the action of the subgroup of $GL(3, \mathbb{F}_q)$ described in Remark 15. The plane conics over $\mathbb{F}_q$ are classified in Ref. [10] in terms of their rank.

There is a unique rank 1 monic conic, z^2. The binary form z^2 is realized as a base polynomial taking $M_1 = M_2 = 0$.

Rank 2 monic conics form 2 orbits, the ones union of 2 lines defined over $\mathbb{F}_q$ and the one induced by a form indecomposable over $\mathbb{F}_q$, but decomposable over $\mathbb{F}_{q^2}$. We first check that all rank 2 monic conics which splits over $\mathbb{F}_q$ are realized as a base polynomial. For any q, we realize the polynomial $(z + x)(z + y)$ taking the matrix $A = A_+ + \beta A_- = (a_{ij})$ with $a_{12} = a_{21} = 0$, $a_{11} = 1$ and $a_{22} = \beta$.

There is, up to a projective transformation, another rank 2 conic ([10, Th. 5.1.6 for q odd, Th. 5.1.7 for q even]).

First assume q odd. We need to represent the equation $dx^2 + z^2$ with $d \in \mathbb{F}_q$ and d not a square. Take $A = (a_{ij})$ with $a_{11} = d$, $a_{22} = 1$ and $a_{12} = a_{21} = 0$ (so that $A_+ = A$ and $A_- = 0$).
Now assume q even, say $q = 2^e$ for some $e > 0$. Since every element of $\mathbb{F}_q$ is a square, the form $z^2 + cy^2$ splits and hence up to an $\mathbb{F}_q$ linear transformation it is sufficient to realize as a base polynomial the form $z^2 + zy + \delta y^2$, where $\delta \in \mathbb{F}_q \backslash 0$ has non-zero absolute trace $D(\delta)$, where $D(u) = \sum_{i=0}^{e-1} u^{2^i}$ for any $u \in \mathbb{F}_q$ ([10, p. 3]). Fix any $\delta \in \mathbb{F}_q$ and take $c \in \mathbb{F}_{q^2}$ such that $c^{q+1} = \delta$. Take $A = 0$ and $B = (b_{ij})$, where $b_{11} = 1$, $b_{12} = c$, $b_{21} = c^q$ and $b_{22} = 0$.
For any finite field up to a projective transformation, there is a unique smooth projective conic ([10, Theorems 5.1.6 and 5.1.7]), and we may take $z(z + x) - y^2$ as its equation. Use the matrix $C = (c_{ij})$ with $c_{11} = 1$, $c_{12} = c_{21} = \beta$ and $c_{22} = 0$, which have $bp(C) = z(z + x) - y^2$ (any q). □

Remark 16. Remark 15 and Proposition 1 gives that every reducible monic $f \in \mathbb{F}_q[x, y, z]_3$ is a base polynomial.

5. $M_+, M_- \in M_{n,n}(\mathbb{F}_q)$

A. Beauville studied the realization over a finite field of a form as the determinant of a matrix with entries linear forms ([9]). In this section, we use [9] for matrices $M \in M_{n,n}(\mathbb{F}_{q^2})$ such that $M_+ \in M_{n,n}(\mathbb{F}_q)$ and $M_- \in M_{n,n}(\mathbb{F}_q)$. Obviously this very strong assumption depends on the choice of $\beta \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$. For any q, it requires that $M + M^\dagger \in M_{n,n}(\mathbb{F}_q)$, but it is stronger.

Remark 17. Take symmetric matrices $A, B \in M_{n,n}(\mathbb{F}_q)$. Set $M := A + \beta B$. Since A, B are symmetric and with coefficients in $\mathbb{F}_q$, they are Hermitian. Thus, $M_+ = A$ and $M_- = B$. The matrix $Ax + By + z\mathbb{I}_{n,n}$ is symmetric, hence in this case $bp(M)$ is the determinant of a symmetric matrix of linear forms. Conversely, any symmetric matrix of linear forms over $\mathbb{F}_q$ with z appearing only in the diagonal and with all coefficients 1 is obtained in this way for some symmetric matrices.

Proposition 4. Assume $q \geq (n-1)(n-2)/2 + (n-1)(n-2)\sqrt{q}$. Then every smooth plane curve of degree n defined over $\mathbb{F}_q$ is of the form $\{f_{M_1,M_2,M_3} = 0\}$ for some $M_1, M_2, M_3 \in M_{n,n}(\mathbb{F}_q)$.

Proof. Let X be a smooth plane curve of degree n defined over $\mathbb{F}_q$. The curve X has genus $g := (n-1)(n-2)/2$. To get a determinantal equation of X over $\mathbb{F}_q$, it is necessary and sufficient to find a degree $g - 1$ line bundle L on X defined over $\mathbb{F}_q$ and such that $h^0(L) = 0$ ([9, Proposition 3.1]). Assume $q \geq g + 2g\sqrt{q}$. Any smooth projective curve C of genus g defined over $\mathbb{F}_q$ satisfies $C(\mathbb{F}_q) \geq g + 1$ by the Hasse–Weil theorem ([12, Theoren 9.18]). A theorem proved in Refs. [13, 14] and quoted in [15, Proposition 2.2] says that any smooth genus γ curve C such that $C(\mathbb{F}_q) \geq \gamma + 1$ has a degree $\gamma - 1$ line bundle L defined over $\mathbb{F}_q$ and with $h^0(L) = h^1(L) = 0$. □

The lower bound on q in Proposition 4 is not sharp. The existence of a line bundle L as in the proof of Proposition 4 is related to the computational complexity of the multiplication in finite extensions of a finite field ([13–17]).

The paper [18] and its references gives better information on the number of points of smooth plane curves with a fixed degree and large q. Hasse–Weil bound and related tools may also be used for singular plane curves ([19–21]). See Ref. [22] for results on $\mathrm{Pic}^0(C)(\mathbb{F}_q)$.

Note that given any $f \in \mathbb{F}_q[x, y, z]_n, f \neq 0$, it is computationally easy to check (a system with the coefficients of f and its partial derivatives) if the plane curve $\{f = 0\}$ is smooth (smooth at all points, not only at its $\mathbb{F}_q$ points). It is also very easy to check when a trivariate polynomial is monic with respect to z. We do not have an always working (or always working for large q) criterion to realize a monic polynomial as $bp(A)$ for some $A \in M_{n,n}(\mathbb{F}_{q^2})$, but Remark 17 is sufficient if the monic polynomial is the determinant of a symmetric matrix. If q is odd, this is the content of [9, Proposition 4.2].

References

1. Kippenhahn R. Über den Wertevorrat einer Matrix. Math Nachr. 1951; 6: 193-228.
2. Kippenhahn R. On the numerical range of a matrix. Linear Multilinear Algebra. 2008; 56(1-2): 185-225. Translated from the German by Paul F. Zachlin and Michiel E. Hochstenbach.
3. Camenga K, Daett L, Raoult PX, Sendova T, Spitkovsky I, Yates R. Singularities of base polynomials and Gau-Wu numbers. Linear Algebra Appl. 2019; 581: 112-27.
4. Chien M-T, Nakazato H. Singular points of the ternary polynomials associated with 4-by-4 matrices, Electron. J Linear Algebra. 2012; 23: 755-69.
5. Ballico E. On the numerical range of matrices over a finite field. Linear Algebra Appl. 2017; 512: 162-71.
6. Ballico E. Corrigendum to "On the numerical range of matrices over a finite field " [Linear Algebra Appl. 512 (2017) 162–171]. Linear Algebra Appl. 2018; 556: 421-7.
7. Camenga K, Collins B, Hoefer G, Quezada J, Rault PX, Willson J, *et al.* On the geometry of numerical ranges over finite fields. Linear Algebra Appl. 2022; 644: 192-218. arXiv: 2107.09191.
8. Coons JI, Jenkins J, Knowles D, Luke RA, Rault PX. Numerical ranges over finite fields. Linear Algebra Appl. 2016; 501: 37-47.
9. Beauville A. Determinantal hypersurfaces, Michigan. J Math. 2000; 48: 39-64.
10. Hirschfeld JWP. Projective geometries over finite fields. Oxford: Clarendon Press; 1979.
11. Lidl R, Niederreiter H. Finite fields. Cambridge: Cambridge University Press; 1997.
12. Hirschfeld JWP, Korchmáros G, Torres F. Algebraic curves over a finite field. Princeton Series in applied Mathematics. Princeton, NJ: Princeton University Press; 2008.
13. Ballet S. Curves with many points and multiplication complexity in any extension of $\mathbb{F}_q$. Finite Field Appl. 1999; 5: 364-77.
14. Ballet S, Le Brigand D. On the existence of non-special divisors of degree g and $g-1$ in algebraic function fields over $\mathbb{F}_q$. J Number Theor. 2006; 116(2): 293-310.
15. Ballet S, Ritzenthaler C, Rolland R. On the existence of dimension zero divisors in algebraic function fields defined over $\mathbb{F}_q$. Acta Arithmetica. 2010; 143(4): 377-92.
16. Ballet S, Bonnecaze A, Tukumuly M. On the construction of elliptic Chudnovsky-type algorithms for multiplication in large extensions of finite fields. J Algebra Its Appl. 2016; 15(1): 1650005. (26 pages).
17. Ballet S, Pieltant J, Rambaud M, Randriambololona H, Rolland R, Chaumine J. On the tensor rank of multiplication in finite extensions of finite fields and related issues in algebraic geometry. Russ Math Surv. 2021; 76(1): 29-89.
18. Bucur A, Chantal D, Feigon B, Laín M. Fluctuations in the number of points on smooth plane curves over finite fields. J Number Theor. 2010; 130(11): 2528-41.
19. Aubry Y, Iezzi A. On the maximum number of rational points on singular curves over finite fields. Mosc Math J. 2015; 15(4): 615-27.
20. Aubry Y and Iezzi A, Optimal and maximal singular curves, Arithmetic, geometry, cryptography and coding theory, 31–43. Contemp Math. 2017; 686, Amer. Math. Soc., Providence, RI.

21. Aubry Y, Perret M. A Weil theorem for singular curves, Arithmetic, geometry and coding theory (Luminy, 1993). Berlin: de Gruyter; 1996. 1–7.
22. Aubry Y, Haloui S, Lachaud G. On the number of points of Abelian and Jacobian varieties over finite fields. Acta Arithmetica. 2013; 160(3): 201-41.

Corresponding author

Edoardo Ballico can be contacted at: edoardo.ballico@unitn.it