# ON THE NUMERICAL RANGE OF MATRICES DEFINED OVER A FINITE FIELD

E. BALLICO

ABSTRACT. Let $q$ be a prime power. For $u = (u_1, \dots, u_n), v = (v_1, \dots, v_n) \in \mathbb{F}_{q^2}^n$ let $\langle u, v\rangle := \sum_{i=1}^n u_i^q v_i$ be the Hermitian form of $\mathbb{F}_{q^2}^n$. Fix an $n \times n$ matrix $M$ over $\mathbb{F}_{q^2}$. Set $\mathrm{Num}(M) := \{\langle u, Mu\rangle \mid u \in \mathbb{F}_{q^2}^n, \langle u, u\rangle = 1\}$ (the numerical range of $M$ introduced by Coons, Jenkins, Knowles, Luke and Rault (case $q$ a prime $q \equiv 3 \pmod 4$) and by the author (arbitrary $q$)). When $n = 2$ we prove an upper bound for $|\mathrm{Num}(M)|$. We describe $\mathrm{Num}(M)$ for several classes of matrices, mostly for $n = 2, 4$.

## 1. INTRODUCTION

Let $q$ be a prime power. Let $\mathbb{F}_q$ denote the only field, up to field isomorphisms, with $|\mathbb{F}_q| = q$ ([19, Theorem 2.5]). Let $e_1, \dots, e_n$ be the standard basis of $\mathbb{F}_{q^2}^n$. For all $v, w \in \mathbb{F}_{q^2}^n$, say $v = a_1e_1 + \cdots + a_ne_n$ and $w = b_1e_1 + \cdots + b_ne_n$, set $\langle v, w\rangle = \sum_{i=1}^n a_i^q b_i$. $\langle\ ,\ \rangle$ is the standard Hermitian form of $\mathbb{F}_{q^2}^n$. For any $n \geq 1$ and any $a \in \mathbb{F}_q$ set

$$C_n(a) := \{(x_1, \dots, x_n) \in \mathbb{F}_{q^2}^n \mid x_1^{q+1} + \cdots + x_n^{q+1} = a\}.$$

The set $C_n(1)$ is an affine chart of the Hermitian variety of $\mathbb{P}^n(\mathbb{F}_{q^2})$ ([14, Ch. 5], [16, Ch. 23]). Take $M \in M_{n,n}(\mathbb{F}_{q^2})$, i.e. let $M$ be an $n \times n$ matrix with coefficients in $\mathbb{F}_{q^2}$. For any $k \in \mathbb{F}_q$ set $\mathrm{Num}_k(M) := \{\langle u, Mu\rangle \mid u \in C_n(k)\} \subseteq \mathbb{F}_{q^2}$. Set $\mathrm{Num}(M) := \mathrm{Num}_1(M)$. The set $\mathrm{Num}(M)$ is called the *numerical range* of $M$. These concepts were introduced in [8] when $q$ is a prime $q \equiv 3 \pmod 4$ and in [1] in the general case.

If $n > 2$ we have $\mathrm{Num}(M) = \mathbb{F}_{q^2}$ for "most " $M \in M_{n,n}(\mathbb{F}_{q^2})$. This is the case for most diagonal matrices, as it is possible to describe the numerical range of block diagonal matrices. More precisely, fix $A \in M_{m,m}(\mathbb{F}_{q^2})$, $B \in M_{r,r}(\mathbb{F}_{q^2})$ and set

$$M = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}.$$

Thus $M \in M_{m+r,m+r}(\mathbb{F}_{q^2})$. There is a complete description of $\mathrm{Num}(M)$ in terms of all $\mathrm{Num}(A)$, $\mathrm{Num}_0(A)$, $\mathrm{Num}(B)$ and $\mathrm{Num}_0(B)$ ([8, Proposition 3.1], [1, Lemma 1]) and this description shows how easy from a given $A$ to find $B$ (even with $r = 1$ if $m \geq 2$ and $A$ is not too special) with $\mathrm{Num}(M) = \mathbb{F}_{q^2}$.

If $n = 2$ we may use $\mathrm{Num}(M)$ to give a good description of $M$, up to a unitary transformation, at least if $q \neq 2$. In particular $|\mathrm{Num}(M)|$ describes in which field

2010 *Mathematics Subject Classification.* 15A33; 15A60; 12E20.

*Key words and phrases.* numerical range; matrix; finite field.

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

the eigenvalues of $M$ are contained, if the eigenvectors of $M$ are in $C_2(0)$ or not and if they are orthogonal with respect to $\langle\ ,\ \rangle$ (Remark 1).

For any $M = (m_{ij}) \in M_{n,n}(\mathbb{F}_{q^2})$ set $M^\dagger := (m_{ji}^q) \in M_{n,n}(\mathbb{F}_{q^2})$. Note that $M^{\dagger\dagger} = M$ and that $\langle u, Mv\rangle = \langle M^\dagger u, v\rangle$ for all $u, v \in \mathbb{F}_{q^2}^n$. The matrix $M$ is unitary if and only if $M^\dagger = M$. In [2] the author defined the real part and the imaginary part first of any $x \in \mathbb{F}_{q^2}$ and then of any $M \in M_{n,n}(\mathbb{F}_{q^2})$. We briefly recall here the case $q$ odd. In Section 2 we give more details and explain the case $q$ even. Assume $q$ odd. Fix $\alpha \in \mathbb{F}_q$, which is not a square in $\mathbb{F}_q$ and fix a root $\beta \in \mathbb{F}_{q^2}$ of the equation $t^2 - \alpha = 0$, so that $\mathbb{F}_{q^2}$ is an $\mathbb{F}_q$-vector space with 1 and $\beta$. For any $z = x + y\beta \in \mathbb{F}_{q^2}$ with $x, y \in \mathbb{F}_q$ set $\Re z := x$ and $\Im z := y$. We have $z = (z + z^q)/2$ and $\Im z = (z - z^q)/2\beta$. For any square matrix $M \in M_{n,n}(\mathbb{F}_{q^2})$ set $M_+ := (M - M^\dagger)/2$ and $M_- := (M + M^\dagger)/2\beta$. We have $M = M_+ + \beta M_-$. If $M = M^\dagger$, then $\mathrm{Num}(M) \subseteq \mathbb{F}_q$ (Remark 4). Thus for any square matrix $M$ we have $\mathrm{Num}(M_+) \subseteq \mathbb{F}_q$ and $\mathrm{Num}(M_-) \subseteq \mathbb{F}_q$.

We first prove the following upper bound for $|\mathrm{Num}(M)|$.

**Theorem 1.** *Fix any $M \in M_{2,2}(\mathbb{F}_{q^2})$. Then:*

(i) $|\mathrm{Num}(M)| \le q^2 - 2q + 2$;

(ii) *if* $|\mathrm{Num}(M_+)| \le q-1$ *and* $|\mathrm{Num}(M_-)| \le q-1$, *then* $|\mathrm{Num}(M)| \le q^2-2q+1$;

(iii) *if either* $|\mathrm{Num}(M_+)| \le q-2$ *or* $|\mathrm{Num}(M_-)| \le q-2$, *then either* $M = c\mathbb{I}_{2\times 2}$ *and* $\mathrm{Num}(M) = \{c\}$ *or* $q-1 \le |\mathrm{Num}(M)| \le q$;

(iv) *if* $\{|\mathrm{Num}(M_+)|, |\mathrm{Num}(M_-)|\} = \{q-1, q\}$, *then* $|\mathrm{Num}(M)| \le q^2 - 2q + 2$;

(v) *if* $|\mathrm{Num}(M_+)| = |\mathrm{Num}(M_-)| = q$, *then* $|\mathrm{Num}(M)| \le q^2 - 4q + 8$.

Then we describe $\mathrm{Num}(M)$ for many classes of $2 \times 2$ matrices. In the classical case of the numerical range of complex matrices the case of $2 \times 2$ matrices was the critical one for the convexity theorem, while $n > 2$ was reduced to the $2 \times 2$ case ([10, Lemma 1.1.1 and Theorem 1.1.2], [11, 12, 20]).

Our interest in the classical, i.e. over $\mathbb{C}$, numerical range came from our interest in quantum computing, quantum error correcting codes and convolutional codes ([4, 5, 6, 9, 13, 17, 21, 22]). Let $V$ be a (finite-dimensional for error correcting code purpose) complex vector space equipped with an Hermitian form $\langle\ ,\ \rangle$, i.e. a finite dimensional Hilbert space. Over a finite field one uses the Hermitian form $\langle\ ,\ \rangle$ over $\mathbb{F}_{q^2}$. The map $\nu_M : C_n(1) \to \mathbb{F}_{q^2}$ defined by the formula $u \mapsto \langle u, Mu\rangle$ (which we call the *numerical range map*) should play an important role in the use of Hermitian forms over finite fields for these topics.

In [3] we proved that the restriction of the numerical range (over $\mathbb{F}_{q^2}$) to subspaces of $\mathbb{F}_{q^2}^n$ sometimes determines the matrix or it is sufficient to describe its main properties. This is another reason for the interest of $\mathrm{Num}(A)$ where $A \in M_{r,r}(\mathbb{F}_{q^2})$ and $r$ is very low. Restrictions are also usual in classical block codes.

Let $\mathbb{I}_{n\times n}$ denote the unity $n \times n$ matrix. The matrix $N \in M_{2,2}(\mathbb{F}_{q^2})$ is called unitary if $N^\dagger N = \mathbb{I}_{n\times n}$ (or equivalently $NN^\dagger = \mathbb{I}_{n\times n}$). Note that $\mathrm{Num}_k(M) = \mathrm{Num}_k(U^\dagger MU)$ for every unitary matrix $U$.

To state our results we consider the following geometric terminology.

As in [8] for any $a \in \mathbb{F}_{q^2}$ and any $b \in \mathbb{F}_q \setminus \{0\}$ the *circle* $S_{a,b}$ with center $a$ and squared-radius $b$ is the set $\{z \in \mathbb{F}_{q^2} \mid (z-a)^{q+1} = b\}$. We obviously have $|S_{a,b}| = q + 1$ (Remark 6 or [1, Remark 3]). If we know the center of a circle, to get its squared-radius (and so to get all points of the circle) it is sufficient to know one of its points. Two different circles with the same center are disjoint. In the set-up of [8] it was obvious that 2 distinct circles have at most 2 common points. We prove (Lemma 5) that this is the case for all finite fields with odd order and so if $q$ is odd a circle is uniquely determined by 3 of its points.

Fix $d \in \mathbb{F}_{q^2} \setminus \{0\}$ and $k \in \mathbb{F}_q \setminus \{0, 1\}$. The *ellipse associated to* $(d, k)$ or *of type* $(d, k)$ is the set of all $k(dz^q + z)$ for some $z \in \mathbb{F}_{q^2}$ with $z^{q+1} = k(1 - k)$. For any $b \in \mathbb{F}_{q^2}$ a set $B \subset \mathbb{F}_{q^2}$ is called an *un-centered ellipse of type* $(d, k, b)$ if $B - b$ (the set of all $a - b$ with $a \in B$) is an ellipse associated to $(d, k)$. Unions of un-centered ellipses (with respect to different translations $b$) occur in the statement of Proposition 2. See Lemma 2 for the cardinalities of the ellipses.

In Section 4 we prove the following results.

**Proposition 1.** *Take $M \in M_{2,2}(\mathbb{F}_{q^2})$. There are linearly independent $u_1, u_2 \in \mathbb{F}_{q^2}^2$ such that*

$$\langle u_1, u_2\rangle = \langle u_1, Mu_1\rangle = \langle u_2, Mu_2\rangle = 0$$

*if and only if there is a unitary transformation $U$ of $\mathbb{F}_{q^2}^2$ such that*

$$N := U^\dagger MU = \begin{pmatrix} 0 & b \\ b' & 0 \end{pmatrix}$$

*for some $b, b'$. In the latter case $\mathbb{F}_{q^2}u_1$ and $\mathbb{F}_{q^2}u_1$ are uniquely determined by $M$. If $bb' \neq 0$, then $b$ and $b'$ are uniquely determined by $M$.*

*(i) If $b = b' = 0$, then $\mathrm{Num}(M) = \{0\}$.*

*(ii) Assume $bb' = 0$ and $(b, b') \neq (0, 0)$. Set $\rho := q/2 - 1$ if $q$ is even and $\rho := (q - 1)/2$ if $q$ is odd. Then $\mathrm{Num}(M)$ is the union of $0$ and $\rho$ distinct circles with center at $0$.*

*(iii) Assume $bb' \neq 0$ and $q$ even. Let $c$ be the only element of $\mathbb{F}_{q^2}$ with $c^2 = bb'$. Set $y := c/b$. If $y^{q+1} = 1$, then $|\mathrm{Num}(M)| = q - 1$. If $y^{q+1} \neq 0$, then $\mathrm{Num}(M)$ is the union of $\{c\}$ and $q/2 - 1$ disjoint circles with center $c$ and hence $|\mathrm{Num}(M)| = 1 + (q + 1)(q/2 - 1)$.*

*(iv) Assume $q$ odd, $bb' \neq 0$ and that $bb'$ is a square in $\mathbb{F}_{q^2}$, say $bb' = c^2$. If $c^{q+1} \notin \{-1, 1\}$, then $\mathrm{Num}(M)$ is the union of $\{-c, c\}$ and $q - 2$ not necessarily disjoint circles. If $c^{q+1} = 1$, then $|\mathrm{Num}(M)| = q$ and $\mathrm{Num}(M) = \{z \in \mathbb{F}_{q^2} \mid z^q + z = 1\}$. If $c^{q+1} = -1$, then $|\mathrm{Num}(M)| = q - 1$.*

*(v) Assume $bb' \neq 0$, $q$ odd and that $bb'$ not a square in $\mathbb{F}_{q^2}$. Set $d := b/b'$ and $E := \frac{1}{b'}N$. Then $\mathrm{Num}(E)$ is the union of $0$ and of $q - 2$ ellipses of type $(d, k)$, one for each $k \in \mathbb{F}_q \setminus \{0, 1\}$.*

**Proposition 2.** *Take $q$ odd and let $N \in M_{2,2}(\mathbb{F}_{q^2})$ with no eigenvalue in $\mathbb{F}_{q^2}$. Then $N$ has two different eigenvalues in $\mathbb{F}_{q^4}$. Let $c \in \mathbb{F}_{q^2}$ be the trace of $N$ and set $M := N - (c/2)\mathbb{I}_{2\times 2}$. Write $a := m_{11}$, $b := m_{12}$, $d := m_{21}$. We have $m_{22} = -a$, $b \neq 0$, $d \neq 0$ and $b/d$ is not a square in $\mathbb{F}_{q^2}$. $\mathrm{Num}(M)$ is the union of $\{-a, a\}$ and the $q - 2$ sets $B(k, a, b, d)$, where $\frac{1}{d}(B(k, d, b, d) + a(2k - 1))$ is an ellipses of type $(b/d, k)$, $k \in \mathbb{F}_q \setminus \{0, 1\}$.*

In the next statement we use the trace map $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}$ ([19, Definition 2.22 and Theorem 2.23]) (see section 2).

**Proposition 3.** *Fix $M \in M_{2,2}(\mathbb{F}_{q^2})$ such that $M_+$ has a unique eigenvalue $c_1$ with eigenspace of dimension one spanned by $u_1 \in \mathbb{F}_{q^2}^2$ with $\langle u_1, u_1\rangle = 0$, $M_-$ has a unique eigenvalue $c_1$ with eigenspace of dimension one spanned by $u_2 \in \mathbb{F}_{q^2}^2$ with*

*$\langle u_2, u_2\rangle = 0$ and $u_2$ is not proportional to $u_1$. Then $|\mathrm{Num}(M)| = q$ and there is $b' \in \mathbb{F}_{q^2}^*$ and $b'' \in \mathbb{F}_q$ such that $\mathrm{Num}(M)/b'$ is the $\mathbb{F}_q$-line $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}^{-1}(b'')$.*

Assume $q$ odd. By Propositions 1 and 2 the assumptions of Proposition 3 are satisfied only in the case (iv) with $c^{q+1} = 1$ of Proposition 1. Compare Theorem 2 below to see why matrices with $|\mathrm{Num}(M)| = q$ are interesting.

**Proposition 4.** *Assume $q$ odd. Take $M \in M_{2,2}(\mathbb{F}_{q^2})$ such that $M$ has 2 eigenvalues $c_1, c_2 \in \mathbb{F}_{q^2}$, $c_1 \neq c_2$, with eigenvectors $u_1, u_2$ with $\langle u_i, u_j\rangle \neq 0$ for all $i, j$. If $q \geq 5$ (resp. $q = 3$), then $|\mathrm{Num}(M)| \geq (q + 1)(q + 3)/4$ (resp. $|\mathrm{Num}(M)| \geq 4$).*

**Remark 1.** It seems that (after [1, 2, 8]) Proposition 2 was the only missing piece for the rough classification of numerical ranges for $n = 2$: if we know $\mathrm{Num}(M)$ we more or less know if $M$ has eigenvalues in $\mathbb{F}_{q^2}$, if they are 2 or one with multiplicities 2, if an eigenspace is one dimensional spanned by a vector $v$ with $\langle v, v\rangle \neq 0$ or not and partial information on $\mathrm{Num}(M)$ may exclude some cases.

In [2, Theorem 1] we proved a lower bound for $|\mathrm{Num}(M)|$, unless $M$ is a specific class, when $q$ is odd. We complete the proof for the case $q$ even, $q \neq 2$, and prove the following result.

**Theorem 2.** *Assume $q \neq 2$. Take $M \in M_{n,n}(\mathbb{F}_{q^2})$ such that $M$ is not a multiple of the identity matrix $\mathbb{I}_{n\times n}$. Then either $|\mathrm{Num}(M)| \geq q$ or $n = 2$, $|\mathrm{Num}(M)| = q - 1$, $M$ has a unique eigenvalue, $c$, with $\dim \ker(M - c\mathbb{I}_{2\times 2}) = 1$ and the kernel of $M - c\mathbb{I}_{2\times 2}$ is spanned by a vector $v \in \ker(M - c\mathbb{I}_{2\times 2})$ with $\langle v, v\rangle = 0$.*

We conclude the paper with the description of $\mathrm{Num}_k(M)$ for the following class of $4 \times 4$ matrices.

**Proposition 5.** *Take*

$$M = \begin{pmatrix} d & b_1 & 0 & 0 \\ b_6 & d_1 & b_2 & b_3 \\ 0 & b_5 & d & b_4 \\ 0 & b_7 & 0 & d \end{pmatrix}$$

*with $d_1, d, b_i \in \mathbb{F}_{q^2}$, $1 \leq i \leq 7$, $b_4 \neq 0$ and $k \in \mathbb{F}_q$. Then $\mathrm{Num}_k(M) = \mathbb{F}_{q^2}$.*

We thanks the referees for feedback and suggestions.

## 2. Preliminaries

The Galois group of the inclusion $\mathbb{F}_q \subset \mathbb{F}_{q^2}$ has order 2 and it is generated by the Frobenius map $\sigma : t \mapsto t^q$.

Following [2] we recall the definitions of $\Im$, $\Re$, $M_+$ and $M_-$.

First assume $q$ odd. If $q$ is odd, $\mathbb{F}_{q^2}$ is obtained from $\mathbb{F}_q$ adding a root $\beta$ of the polynomial $f(t) := t^2 - \alpha$, where $\alpha$ is not a square in $\mathbb{F}_q$. The other root is $-\beta$ and hence $\sigma(\beta) = -\beta$, i.e. $\beta^q = -\beta$. Thus $\mathbb{F}_{q^2} = \mathbb{F}_q + \mathbb{F}_q\beta$ as an $\mathbb{F}_q$-vector space. For any $z = x + y\beta \in \mathbb{F}_{q^2}$ with $x, y \in \mathbb{F}_q$ set $\Re z := x$ and $\Im z := y$. Since $\sigma(z) = x - \beta y$, we have $\Re z = (z + z^q)/2$ and $\Im z = (z - z^q)/2\beta$. For any $M \in M_{n,n}(\mathbb{F}_{q^2})$ set $M_+ := (M+M^\dagger)/2$ and $M_- := (M-M^\dagger)/2\beta$. We have $M_+^\dagger = M_+$. Since $\beta^q = -\beta$, we have $M_-^\dagger = M_-$. Hence $M = M_+ + \beta M_-$ with $M_+$ and $M_-$ Hermitian matrices. For any $u \in \mathbb{F}_{q^2}^n$ we have $\langle u, Mu\rangle = \langle u, M_+u\rangle + \beta\langle u, M_-u\rangle$ with $\langle u, M_+u\rangle \in \mathbb{F}_q$ and $\langle u, M_-u\rangle \in \mathbb{F}_q$ ([2, Lemma 1]). Thus the map $z \mapsto \Re z$ (resp. $z \mapsto \Im z$) induces a surjection $\rho_1 : \mathrm{Num}(M) \to \mathrm{Num}(M_+) \subseteq \mathbb{F}_q$ (resp. $\rho_2 : \mathrm{Num}(M) \to \mathrm{Num}(M_-) \subseteq \mathbb{F}_q$) and in particular $|\mathrm{Num}(M)| \ge \max\{|\mathrm{Num}(M_+)|, |\mathrm{Num}(M_-)|\}$.

Now assume $q$ even. Since $\mathbb{F}_{q^2}$ is a degree 2 extension of $\mathbb{F}_q$, there is $\varepsilon \in \mathbb{F}_q$ such that the polynomial $f(t) = t^2+t+\varepsilon$ has no root in $\mathbb{F}_q$ and two distinct roots in $\mathbb{F}_{q^2}$. We fix one of these roots, $\beta$. Note that $(\beta+1)^2+\beta+1 = \beta^2+\beta$ and hence $\beta+1$ is the other root of $f(t)$. Since these two roots are conjugate by the Galois group of the extension $\mathbb{F}_q \hookrightarrow \mathbb{F}_{q^2}$ (which is generated by the Frobenius map $\sigma : t \mapsto t^q$), we have $\beta^q = \beta+1$ and $(\beta+1)^q = \beta$. If $z = x+y\beta \in \mathbb{F}_{q^2}$ with $x, y \in \mathbb{F}_q$, then set $\Re z := x$ and $\Im z := y$. The maps $\Re : \mathbb{F}_{q^2} \to \mathbb{F}_q$ and $\Im : \mathbb{F}_{q^2} \to \mathbb{F}_q$ are $\mathbb{F}_q$-linear. Since $\sigma : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ is $\mathbb{F}_q$-linear, $\sigma^2$ is the identity map and $\sigma(\beta) = \beta+1$, we have $z^q = \sigma(z) = x+y+y\beta$. Thus $y = z+z^q$ and $x = z+\beta y = (\beta+1)z+\beta z^q$. For any $M \in M_{n,n}(\mathbb{F}_{q^2})$ set $M_+ := (\beta+1)M+\beta M^\dagger$ and $M_- = M+M^\dagger$. Obviously $M_-$ is Hermitian and (since $2\beta = 0$) $M = M_+ + \beta M_-$. Since $(\beta+1)^q = \beta$ and $\beta^q = \beta+1$, $M_+$ is Hermitian. Thus the map $z \mapsto \Re z$ (resp. $z \mapsto \Im z$) induces surjections $\rho_1 : \mathrm{Num}(M) \to \mathrm{Num}(M_+) \subseteq \mathbb{F}_q$ (resp. $\rho_2 : \mathrm{Num}(M) \to \mathrm{Num}(M_-) \subseteq \mathbb{F}_q$).

Thus for arbitrary $q$ we have

$$\max\{|\mathrm{Num}(M_+)|, |\mathrm{Num}(M_+)|\} \le |\mathrm{Num}(M)|. \tag{1}$$

Since $\mathrm{Num}(M_+) \subseteq \mathbb{F}_q$, $\mathrm{Num}(M_-) \subseteq \mathbb{F}_q$, $\langle u, Mu\rangle = \langle u, M_+u\rangle + \beta\langle u, M_-\rangle$, $\langle u, M_+u\rangle \in \mathbb{F}_q$ and $\langle u, M_-u\rangle \in \mathbb{F}_q$ (Remark 4), we have

$$|\mathrm{Num}(M)| \le |\mathrm{Num}(M_+)||\mathrm{Num}(M_-)|. \tag{2}$$

**Remark 2.** If $q = 2$ and $n = 2$ with $M = (m_{ij})$, $i, j = 1, 2$, then $\mathrm{Num}(M) = \{m_{11}, m_{22}\}$ ([1, Remark 8]).

**Remark 3.** Fix $c, d \in \mathbb{F}_{q^2}$ and $k \in \mathbb{F}_q$. For any $n \times n$ matrix $M$ over $\mathbb{F}_{q^2}$ we have $\mathrm{Num}_k(c\mathbb{I}_{n\times n} + dM) = ck^2 + d\mathrm{Num}_k(M)$.

**Remark 4.** If $M = M^\dagger$, i.e. if $M$ is a Hermitian matrix, then $\mathrm{Num}(M) \subseteq \mathbb{F}_q$ ([2, Lemma 1]). In particular for any square matrix $N$, $\mathrm{Num}(N_+) \subseteq \mathbb{F}_q$ and $\mathrm{Num}(N_-) \subseteq \mathbb{F}_q$.

**Remark 5.** Let $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q} : \mathbb{F}_{q^2} \to \mathbb{F}_q$ denote the trace map. The formula $a \mapsto a^q + a$ defines the trace map $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q} : \mathbb{F}_{q^2} \to \mathbb{F}_q$ (case $m = 2$ of [19, Definition 2.22]). The function $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q} : \mathbb{F}_{q^2} \to \mathbb{F}_q$ is $\mathbb{F}_q$-linear and non-zero ([19, Theorem 2.23]) and hence it is surjective with as its kernel a 1-dimensional $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^2}$ seen as a 2-dimensional $\mathbb{F}_q$-vector space. Since $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}$ is an $\mathbb{F}_q$-linear surjective map, for each $a \in \mathbb{F}_q$ the set $\mathrm{Tr}^{-1}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(a)$ is an affine $\mathbb{F}_q$-line and in particular $|\mathrm{Tr}^{-1}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(a)| = q$.

We use the following lemma proved in [2].

**Lemma 1.** *([2, Lemma 2]) Assume $q \ne 2$ and take $M \in M_{2,2}(\mathbb{F}_{q^2})$ such that $M^\dagger = M$. Then either $M = c\mathbb{I}_{2\times 2}$ with $c \in \mathbb{F}_q$, or $M$ has two distinct eigenvalues $c_1, c_2 \in \mathbb{F}_q$ and $M$ is unitarily equivalent to $c_1\mathbb{I}_{1\times 1} \oplus c_2\mathbb{I}_{1\times 1}$, or $M$ has a unique eigenvalue $c \in \overline{\mathbb{F}}_{q^2}$ (and hence $c \in \mathbb{F}_q$), $\dim\ker(M - c\mathbb{I}_{2\times 2}) = 1$ and $\ker(M - c\mathbb{I}_{2\times 2})$ is generated by $v \in \mathbb{F}_{q^2}^2$ with $\langle v, v\rangle = 0$.*

**Remark 6.** Fix $a \in \mathbb{F}_q^*$. 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 $a^{q-1} = 1$([14, page 1], [19, Theorem 2.8]), we have $b^{q^2-1} = 1$. Hence $b \in \mathbb{F}_{q^2}^*$. Thus there are exactly $q+1$ elements $c \in \mathbb{F}_{q^2}^*$ with $c^{q+1} = a$.

We need the following 4 results proved in [1, 2, 8].

**Proposition 6.** *(*[1, Proposition 1], [8, Lemma 3.5]*) Assume $n = 2$ and that $M$ has a unique eigenvalue, c, that its eigenspace has dimension* 1*, and that $\langle v, v\rangle \neq 0$ for some eigenvector $v$. Set $\rho := q/2 - 1$ if $q$ is even and $\rho := (q-1)/2$ if $q$ is odd. Then* $|\mathrm{Num}(M)| = 1 + \rho(q+1)$ *and* $\mathrm{Num}(M)$ *is the disjoint union of* $\{c\}$ *and $\rho$ disjoint hermitian circles with centers at $c$.*

**Proposition 7.** *(*[2, Proposition 1]*) Assume $n = 2$ and that $M$ has eigenvalues $c_1, c_2 \in \mathbb{F}_{q^2}$ and $v_i \in \mathbb{F}_{q^2}^2 \setminus \{0\}$, $i = 1, 2$, such that $c_1 \neq c_2$, $Mv_i = c_iv_i$ and $\langle v_i, v_i\rangle = 0$ for all $i$. Then* $|\mathrm{Num}(M)| = q$ *and* $\mathrm{Num}(M) = \{t \in \mathbb{F}_{q^2} \mid t^q + t = 1\}$.

**Proposition 8.** *(*[2, Proposition 2], [8, Lemma 3.6]*) If $q$ is odd, set $\rho = (q-1)/2$. If $q$ is even, set $\rho := q/2-1$. Assume $n = 2$ and that $M$ has* 2 *different eigenvalues $c_1, c_2 \in \mathbb{F}_{q^2}$ and that for each $i = 1, 2$ there is $v_i \in \mathbb{F}_{q^2}^2$ with $Mv_i = c_iv_i$ and $\langle v_1, v_1\rangle \neq 0$. Assume $\langle v_1, v_2\rangle \neq 0$, i.e. assume that $M$ has not a unitary basis. Then* $\mathrm{Num}(M)$ *is the union of* $\{c_1, c_2\}$ *and $\rho$ Hermitian circles and hence we have* $\mathrm{Num}(M) \leq 2 + \rho(q+1)$.

## 3. Proofs of Theorems 1 and 2

*Proof of Theorem 1:* Write $M = (m_{ij})$, $i, j = 1, 2$. By Remark 2 we may assume $q \neq 2$ (note that the assumptions of (ii) imply $m_{11} = m_{22}$ if $q = 2$ by Remark 2). Part (ii) follows from (2). Part (i) is a logical consequence of parts (ii), (iii), (iv) and (v). Thus it is sufficient to prove parts (iii), (iv) and (v). Since $\mathrm{Num}(M_+) \subseteq \mathbb{F}_q$ and $\mathrm{Num}(M_-) \subseteq \mathbb{F}_q$, we have $|\mathrm{Num}(M_+)| \leq q$ and $|\mathrm{Num}(M_-)| \leq q$. By Lemma 1 (or by [2, Theorem 1]) if $|\mathrm{Num}(M_+)| < q-1$, then $|\mathrm{Num}(M_+)| = 1$ and $M_+ = a\mathbb{I}_{2\times 2}$ for some $a \in \mathbb{F}_q$. The same holds for $M_-$. Using this observation for $M_+$ and $M_-$ and using (1) and (2) we get that if $|\mathrm{Num}(M_+)| < q-1$, then either $M = c\mathbb{I}_{2\times 2}$ for some $c \in \mathbb{F}_{q^2}$ or $q-1 \leq |\mathrm{Num}(M)| \leq q$, concluding the proof of part (iii).

Now assume $|M_+| = q$, i.e. assume that $M_+$ has two distinct eigenvalues $c_1, c_2 \in \mathbb{F}_q$ with $c_1 \neq c_2$ ([2, Lemma 2]). In this case $M_+$ is unitarily equivalent to $c_1\mathbb{I}_{1\times 1} \oplus c_2\mathbb{I}_{1\times 1}$ (Lemma 1). Thus taking $U^\dagger MU$ instead of $M$ with $U$ a unitary matrix we reduce to the case $M_+ = c_1\mathbb{I}_{1\times 1} \oplus c_2\mathbb{I}_{1\times 1}$. Taking $(c_2 - c_1)^{-1}(M - c_1\mathbb{I}_{2\times 2})$ instead of $M$ ([8, Lemma 2.7] or [1, Lemma 1]), we reduce to the case $c_1 = 0$ and $c_2 = 1$, i.e. $\Re m_{11} = \Re m_{12} = \Re m_{21} = 0$ and $\Re m_{22} = 1$.

Taking $\beta M$ instead on $M$ if necessary, from now on we assume $|\mathrm{Num}(M)_+| \geq |\mathrm{Num}(M)_-|$.

(a) Now we also assume $|M_-| = q$. For any $A \in M_{2,2}(\mathbb{F}_{q^2})$ let $\rho_1 : \mathrm{Num}(A) \to \mathrm{Num}(A_+)$ (resp. $\rho_2 : \mathrm{Num}(A) \to \mathrm{Num}(A_-)$) be the surjection induced by the map $\Re : \mathbb{F}_{q^2} \to \mathbb{F}_q$ (resp. $\Im : \mathbb{F}_{q^2} \to \mathbb{F}_q$). Working with $M_+$ we proved (without any change of the unitary frame) the existence of $t_0, t_1 \in \mathbb{F}_q$ such that $t_0 \neq t_1$, and $|\rho_1^{-1}(t_i)| = 1$, $i = 0, 1$. In the same way we prove the existence of $a_0, a_1 \in \mathbb{F}_q$ such that $a_0 \neq a_1$ and $|\rho_2^{-1}(a_i)| = 1$, $i = 0, 1$. Hence $|\mathrm{Num}(M)| \leq q^2 - 4q + 8$, proving part (v).

(b) Assume $|M_-| = q - 1$. Since $\rho_2$ is well-defined and $|M_-| = q - 1$, to prove part (iv) of Theorem 1 it is sufficient to prove that $1 + \beta k \in \mathrm{Num}(M)$ with

$k \in \mathbb{F}_q$ if and only if $k = \Im m_{22}$. Take $u = (x, y) \in \mathbb{F}_{q^2}^2$ and assume $u \in C_2(1)$, i.e. $x^{q+1} + y^{q+1} = 1$. We have $\langle u, Mu\rangle = 1 + \beta k$ if and only if $\langle u, M_+u\rangle = 1$ and $\langle u, M_-u\rangle = k$. We have $\langle u, M_+u\rangle = y^{q+1}$ and thus $\langle u, M_+u\rangle = 1$ if and only if $x = 0$. If $x = 0$ and hence $y^{q+1} = 1$ we have $\langle u, M_-u\rangle = \Im m_{22}$. Hence $|\mathrm{Num}(M)| \le q^2 - 2q + 2$. □

*Proof of Theorem 2:* By [2, Theorem 1] to prove Theorem 2 it is sufficient to prove the case $q \ge 4$, $q$ even and $n \ge 3$. All cases with $n \ge 3$ of the proof of [2, Theorem 1] work verbatim for all even $q \ne 2$, except step (b2.2). Thus it is sufficient to prove Theorem 2 in the case $q$ even, $q \ne 2$, $n = 3$, and for the following very particular Hermitian matrices

$$A = \begin{pmatrix} 1 & a_{12} & a_{13} \\ a_{12}^q & 1 & a_{23} \\ a_{13}^q & a_{23}^q & 1 \end{pmatrix}$$

with $a_{12}, a_{13}, a_{23} \in \mathbb{F}_q \setminus \{0\}$. More precisely, it was proven that $\mathbb{F}_q \setminus \{0\} \subseteq \mathrm{Num}(A) \subseteq \mathbb{F}_q$ and so Theorem 2 is true for $A$ if and only $0 \in \mathrm{Num}(A)$. For all $x, y, z \in \mathbb{F}_{q^2}$ set $h(x, y, z) := \langle u, Au\rangle$ and $h_1(x, y, z) := h(x, y, z) - x^{q+1} - y^{q+1} - z^{q+1}$ with $u = (x, y, z) \in \mathbb{F}_{q^2}^3$. Since

$$Au = (x + a_{12}y + a_{13}z, a_{12}^q x + y + a_{23}z, a_{13}^q x + a_{23}^q y + z),$$

we have

$$h_1(x, y, z) = a_{12}x^q y + a_{13}x^q z + a_{12}^q x y^q + a_{13}^q x z^q + a_{23}y^q z + a_{23}^q y^q z.$$

Take $(a, b, c) \in \mathbb{F}_{q^2}^3$ and assume $h(a, b, c) = 0$ and $k := \langle (a, b, c), (a, b, c)\rangle \ne 0$, i.e. assume $k := a^{q+1} + b^{q+1} + c^{q+1} \ne 0$. Since $|\mathbb{F}_q^*| = q - 1$ and $\mathbb{F}_{q^2}^*$ is a cyclic group of order $(q + 1)(q - 1)$, there is $t \in \mathbb{F}_{q^2}$ such that $t^{q+1} = 1/k$. Thus, setting $u := (tx, ty, tz)$, we have $\langle u, Au\rangle = 0$ and $\langle u, u\rangle = 1$. Thus $u$ would prove that $0 \in \mathrm{Num}(A)$. Thus to conclude the proof of Theorem 2 we may assume that no such triple $(a, b, c)$ exists, i.e. that $\{h(x, y, z) = 0\} \subseteq \{x^{q+1} + y^{q+1} + z^{q+1} = 0\}$. Set $\mathcal{H} := \{x^{q+1} + y^{q+1} + z^{q+1} = 0\} \subset \mathbb{F}_{q^2}^3$. The set $\mathcal{H}$ is the affine cone of the Hermitian curve of $\mathbb{P}^2(\mathbb{F}_{q^2})$ ([14, 15, 16]) and we may see in this way (or check directly), that the degree $q + 1$ homogenous polynomial $x^{q+1} + y^{q+1} + z^{q+1}$ is irreducible. Since the degree $q + 1$ homogeneous polynomial $h(x, y, z)$ is not a multiple of $x^{q+1} + y^{q+1} + z^{q+1}$, Bezout's theorem applied to the curves of $\mathbb{P}^2(\mathbb{F}_{q^2})$ given by these homogeneous degree $q+1$ polynomials shows that $\{h(x, y, z) = 0\}$ has at most $1 + (q^2 - 1)(q + 1)^2$ elements. We have $1 + (q^2 - 1)(q + 1)^2 = q^4 + q^3 - q^2$. Set $\Delta' := \{h(x, y, z) = 0\}$ and $\Delta := \{h_1(x, y, z) = 0\}$. Since $\Delta \cap \mathcal{H} = \Delta' \cap \mathcal{H}$, it would be sufficient to prove that $|\Delta| > q^4 + q^3 - q^2$. Set $g(x, y, z) := a_{12}x^q y + a_{13}x^q z + a_{23}y^q z$. Let $\mathrm{Tr} : \mathbb{F}_{q^2} \to \mathbb{F}_q$ denote the trace. The trace Tr is non-zero, $\mathbb{F}_q$-linear and defined by the formula $\mathrm{Tr}(t) = t^q + t$. Thus the set $\gamma := \{\mathrm{Tr}(t) = 0\} \subseteq \mathbb{F}_{q^2}$ is a 1-dimensional $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^2}$. Since $q$ is even, we have $t^q + t = 0$ if and only if $t^q = t$, i.e. if and only if $t \in \mathbb{F}_q$ ([19, Theorem 2.5]). We get that $\Delta$ is the set of all $(a, b, c) \in \mathbb{F}_q$ such that $g(a, b, c) \in \mathbb{F}_q$. The Frobenius map $t \mapsto t^q$ is a bijection of $\mathbb{F}_{q^2}$. Since $a_{13} \ne 0$, $a_{23} \ne 0$ and the Frobenius map is injective, the set $\gamma_1 := \{(a, b) \in \mathbb{F}_{q^2}^2 \mid a_{13}x^q + a_{23}y^q = 0\}$ has $q^2$ elements. Fix $t \in \mathbb{F}_q$ and $(a, b) \in \mathbb{F}_{q^2}^2 \setminus \gamma_1$. There is a unique $z \in \mathbb{F}_q$ such that $z(a_{13}a^q + a_{23}y^q) + a_{12}a^q b = t$. Varying $a$, $b$ and $t$ get a subset $\Psi$ of $\Delta$ with cardinality $q(q^4 - q^2)$. Since $q \ge 4$, we have $q^5 - q^4 > q^4 + q^3 - q^2$. □

## 4. Specific matrices

**Lemma 2.** *The ellipse $A$ of $\mathbb{F}_{q^2}$ associated to $(d,k)$ has cardinality $q+1$, unless $d^{q+1}=1$.*

1. *If $d^{q+1}=1$ and $q$ is even, then $|A|=1+(q/2)$.*
2. *If $d^{q+1}=1$, $q$ is odd and either $dk(1-k)$ is not a square in $\mathbb{F}_{q^2}$ or any of its square roots, $c$, has $c^{q+1}=-k(1-k)$, then $|A|=(q+1)/2$.*
3. *Assume $d^{q+1}=1$ and $q$ odd. If $dk(1-k)$ is not as in (2), then $|A|=(q+3)/2$.*

*Proof.* Since $k(1-k)\in\mathbb{F}_q\backslash\{0\}$ and $\mathbb{F}_{q^2}^*$ is a cyclic group of order $(q+1)(q-1)$, the set $B:=\{z\in\mathbb{F}_{q^2}\mid z^{q+1}=k(1-k)\}$ has cardinality $q+1$. Thus to prove the first part it is sufficient to prove that if $z,w\in B$ and $dz^q+z=dw^q+w$, then $z=w$, unless $d^{k+1}=1$. Take $z,w\in B$ with $z\neq w$ and $dz^q+z=dw^q+w$, i.e. (since $zw\neq 0$) with $dz^{q+1}w+z^2w=dzw^{q+1}+zw^2$, i.e. with $dk(1-k)w+z^2w=dk(1-k)z+zw^2$. Set $f_z(t)=dk(1-k)z+zt^2-dk(1-k)t-z^2t$. Since $z\neq 0$, the polynomial $f_z(t)$ is a degree 2 polynomial with $f_z(z)=f_z(w)=0$, $zt^2$ as its leading term and $dk(1-k)z$ as its constant term. Hence $dk(1-k)=wz$. Thus $w=\frac{dk(1-k)}{z}$ and $d^{q+1}k^{q+1}(1-k)^{q+1}=(wz)^{q+1}=k^2(1-k)^2$, i.e. $d^{q+1}=k^{1-q}(1-k)^{1-q}=1$ (since $k^{q-1}=(1-k)^{q-1}=1$). For arbitrary $d$ and $z\neq 0$ we have $zf_z(\frac{dk(1-k)}{z})=dk(1-k)z^2+d^2k^2(1-k)^2-d^2k^2(1-k)^2-z^2dk(1-k)=0$. Thus if $(\frac{dk(1-k)}{z})^q+1=k(1-k)$, i.e. $d^{q+1}=1$ we have a solution $w\neq z$ if and only if $z^2\neq dk(1-k)$.

First assume $q$ even. In this case there is a unique $\alpha\in\mathbb{F}_{q^2}$ with $\alpha^2=dk(1-k)$. Since $(\alpha^2)^{q+1}=d^{q+1}k^{q+1}(1-k)^{q+1}=k^2(1-k)^2$, $\alpha^{q+1}$ is the unique $t\in\mathbb{F}_{q^2}$ with $t^2=k^2(1-k)^2$ and so $\alpha^{q+1}=k(1-k)$, i.e. $\alpha\in B$. Thus $|A|=1+(q/2)$.

Now assume $q$ odd. If $dk(1-k)$ is not a square in $\mathbb{F}_{q^2}$, then $z^2\neq dk(1-k)$. Hence $|A|=(q+1)/2$ if $dk(1-k)$ is not a square. Now assume $dk(1-k)=c^2$ for some $c\in\mathbb{F}_{q^2}$. We have $(c^{q+1})^2=k^2(1-k)^2$ and hence either $c^{q+1}=k(1-k)$ or $c^{q+1}=-k(1-k)$. Note that $(-c)^{q+1}=c^{q+1}$ and so if $c^{q+1}=-k(1-k)$, then no solution of $t^2=dk(1-k)$ is contained in $B$. If $c^{q+1}=k(1-k)$, then we have exactly two $z\in B$ with $z=w$ ($c$ and $-c$). We are in Case (3). □

**Lemma 3.** *Assume $q$ odd and fix $a,b\in\mathbb{F}_{q^2}$ with $a\neq b$. Set $\Theta:=\{z\in\mathbb{F}_{q^2}\mid z^{q-1}+1=0\}$ and $A_{a,b}:=\{z\in\mathbb{F}_{q^2}\mid (z-a)^{q+1}=(z-b)^{q+1}\}$. Then $A_{a,b}=\{(a+b)/2\}\cup\{(a+b)/2+t(b-a)/2\}_{t\in\Theta}$, $|A_{a,b}|=q$ and $A_{a,b}$ is an $\mathbb{F}_q$-line of the two-dimensional $\mathbb{F}_q$-space $\mathbb{F}_{q^2}$ containing $(a+b)/2$.*

*Proof.* Note that $(a+b)/2\in A_{a,b}$. Set $S':=A_{a,b}-(a+b)/2$ (translation) and $S:=\frac{2}{b-a}S'$. We have $S=A_{-1,1}$. By Remark 5 it is sufficient to prove that $S=\{0\}\cup\Theta$, i.e. that $S=\{z\in\mathbb{F}_{q^2}\mid z^q+z=0\}$. We have $(z-1)^{q+1}=(z-1)^q(z-1)=(z^q-1)(z-1)=z^{q+1}+1-z^q-z$ and $(z+1)^{q+1}=z^{q+1}+1+z^q+z$. Thus $(z-1)^{q+1}=(z+1)^{q+1}$ if and only if $2(z^q+z)=0$. □

**Lemma 4.** *Assume $q$ odd. Take a circle $S=\{(z-a)^{q+1}=b\}$ and $u,v,w\in S$ such that $|\{u,v,w\}|=3$. Then (with the notation of Lemma 3) we have $A_{u,v}\cap A_{u,w}=\{a\}$.*

*Proof.* Obviously the center of $S$ is contained in all $A_{O,Q}$ for all $O,Q\in S$ such that $O\neq Q$. Thus it is sufficient to prove that $A_{u,v}\neq A_{u,w}$. By Lemma 3 the affine $\mathbb{F}_q$-line $A_{u,v}$ (resp. $A_{u,w}$) is spanned by $a$ and $(u+v)/2$ (resp. $a$ and $(u+w)/2$). Thus $A_{u,v}\neq A_{u,w}$. □

**Lemma 5.** *Assume $q$ odd. Two distinct circles have at most 2 common points and any 3 distinct points of $\mathbb{F}_{q^2}$ are contained in at most one circle.*

*Proof.* Use Lemma 4 and that a circle is uniquely determined by its center and one of its points. □

*Proof of Proposition 4:* By Proposition 8 $\mathrm{Num}(M)$ is the union of 2 points and $q-2$ circles. If $q=3$ use the unique circle. For $q \geq 5$ use the first $(q+1)/2$ circles. By Lemma 5 we get $|\mathrm{Num}(M)| \geq (q+1)(q+1)/2-2(q+1)(q-1)/8 = (q+1)(q+3)/4$. □

**Remark 7.** Take $M \in M_{2,2}(\mathbb{F}_{q^2})$. There are $u_1$ and $u_2$ with $c := \langle u_1, Mu_1\rangle = \langle u_2, Mu_2\rangle$ and $\langle u_1, u_2\rangle = 0$ if and only if $M - c\mathbb{I}_{2,2}$ is as in Proposition 1.

*Proof of Proposition 1:* Since $\langle\ ,\ \rangle$ is non-degenerate and $\langle u_1, u_2\rangle = 0$, we have $\langle u_i, u_i\rangle \neq 0$, $i = 1, 2$. Since $\mathbb{F}_{q^2}^*$ is a cyclic group of order $(q+1)(q-1)$ and $\mathbb{F}_q^*$ is a subgroup of $\mathbb{F}_{q^2}^*$ of order $q-1$ ([19, Theorem 2.5]), there is $z_i \in \mathbb{F}_{q^2}$ such that $z_i^{q+1} = 1/\langle u_i, u_i\rangle$. Set $f_i := z_i u_i$. We have $\langle f_i, f_i\rangle = 1$, $i = 1, 2$, and $\langle f_i, f_j\rangle = 0$ for all $i \neq j$. Take $U$ such that $Ue_i = f_i$ for all $i$. We have $\langle u, Nu\rangle = \langle Uu, MUu\rangle$ for all $u \in \mathbb{F}_{q^2}^n$ and hence $\mathrm{Num}(N) = \mathrm{Num}(M)$. Let $f(t)$ be the characteristic polynomial of $N$. We have $b = b' = 0$ if and only if $M = 0\mathbb{I}_{2\times 2}$. Part (i) is obvious.

(a) Assume $b' = 0$ and $b \neq 0$. Hence $\frac{1}{b}N$ is as in Proposition 6 and in particular $\frac{1}{b}N$ is the union of 0 and $\rho$ different circles with center 0.

(b) Assume $b = 0$ and $b' \neq 0$. The transpose $N^t$ of $N$ is as in step (a) . For any matrix $A \in M_{n,n}(\mathbb{F}_{q^2})$ and any $u \in \mathbb{F}_{q^2}^n$ we have $\langle u, Au\rangle = \langle A^\dagger u, u\rangle = (\langle u, A^\dagger u\rangle)^q$. If $A \in M_{n,n}(\mathbb{F}_q)$, then $A^t = A^\dagger$. We apply this observation to the matrix $\frac{1}{b'}N$. The $q$-power of a circle centered at 0 is the same circle. Hence $\frac{1}{b'}\mathrm{Num}(M)$ is as in step (a), concluding the proof of (ii).

(c) From now on we assume $bb' \neq 0$. Since $\mathbb{F}_{q^4}^*$ is a cyclic group of order $(q^2+1)\cdot|\mathbb{F}_{q^2}^*|$, there is $c \in \mathbb{F}_{q^4}$ such that $c^2 = bb'$. Hence over $\mathbb{F}_{q^4}$ we have $f(t) = (t+c)(t-c)$.

(c1) Assume $q$ even. In this case every element of $\mathbb{F}_{q^2}$ is a square and hence $c \in \mathbb{F}_{q^2}$. In this case we have $f(t) = (t-c)^2$ and $c$ is the unique eigenvalue of $N$. Since $N$ is not a multiple of the diagonal, its eigenspace $V_1 = \ker(N - c\mathbb{I}_{2\times 2})$ has dimension 1 and $(N - c\mathbb{I}_{2\times 2})(V_1) = V_1$. Since $(b, b') \neq (0, 0)$, $e_2$ is not an eigenvector of $N$, and we may take $v = e_1 + ye_2$ as a generator of $V_1$. Thus $v \neq 0$ and $Nv = cv$, i.e. $c = by$ and $cy = b'$. We have $\langle v, v\rangle = 1 + y^{q+1}$. First assume $y^{q+1} \neq 1$. In this case $N$ has an eigenvector $u$ such that $\langle u, u\rangle \neq 0$ and $u$ spans the only eigenspace of $N$, because $N \neq c\mathbb{I}_{2\times 2}$. Thus $(N - c\mathbb{I}_{2\times 2})$ is a multiple of one of the matrices considered in Proposition 6, and hence $\mathrm{Num}(N)$ is the union of $\{c\}$ with $q/2-1$ distinct circles centered at $c$. Now assume $y^{q+1} = 1$. In this case $\langle v, v\rangle = 0$ and $|\mathrm{Num}(M)| = q-1$ by Theorem 2.

(c2) Now assume $q$ odd and that $bb'$ is a square in $\mathbb{F}_{q^2}$. In this case both $c$ and $-c$ are eigenvalues of $N$. Since neither $e_1$ nor $e_2$ is an eigenvector of $N$, we may find eigenvectors $v_1$ (resp. $v_2$) of $N$ with respect to $c$ (resp. $-c$) with $v_i = e_1 + y_i e_2$. We have $y_1 = c$ and $y_2 = -c$. Thus $\langle v_i, v_i\rangle = 1 + c^{q+1}$, $i = 1, 2$, and $\langle v_1, v_2\rangle = 1 - c^{q+1}$. First assume $c^{q+1} \notin \{-1, 1\}$. In this case $N$ has 2 distinct eigenvectors with non-zero hermitian norm and not mutually orthogonal. The set $\mathrm{Num}(M)$ is described in Proposition 8 and in Corollary 4 as a union of $q-2$ not necessarily disjoint circles plus 2 points (sometimes in the circles). Now assume $c^{q+1} = -1$. In this case $|\mathrm{Num}(M)| = q$ and $\mathrm{Num}(M) = \{z^q + z = 0\}$ (Proposition

7). Now assume $c^{q+1} = -1$. In this case $M$ and $N$ are unitarily equivalent to a diagonal matrix with $c$ and $-c$ on the diagonal. Hence $\mathrm{Num}(M) = \mathbb{F}_q c$.

(c3) Now assume $q$ odd and that $bb'$ is not a square. Take $u = xe_1 + ye_2$ with $\langle u, u\rangle = 1$, i.e. with $x^{q+1} + y^{q+1} = 1$. We have $\langle u, Nu\rangle = bx^q y + b'xy^q$. Set $E := \frac{1}{b'}N$ and $d := b/b'$. We have $\langle u, Eu\rangle = dx^q y + xy^q$. Taking either $x = 0$ and as $y$ any element of $\mathbb{F}_{q^2}$ with $y^{q+1} = 1$ (e.g. taking $y = 1$) or taking $y = 0$ and as $x$ any element of $\mathbb{F}_{q^2}$ with $x^{q+1} = 1$ (e.g. taking $x = 1$) we get $0 \in \mathrm{Num}(E)$ and hence $0 \in \mathrm{Num}(M)$. Now assume $xy \neq 0$. Fix $k \in \mathbb{F}_q \setminus \{0, 1\}$ and consider the subset of $\mathrm{Num}(M)$ obtained from all $u = (x, y) \in C_2(1)$ with $y^{q+1} = k$ and hence $x^{q+1} = 1 - k$. Set $z := x/y$. We have $z^{q+1} = (1 - k)/k$. Conversely, for any $z \in \mathbb{F}_{q^2}$ and for any $y_0 \in \mathbb{F}_{q^2}$ with $y_0^{q+1} = k$, we have $(z/y_0)^{k+1} = 1 - k$ and so $z = x_0/y_0$ with $x_0 := z/y_0$ and $x_0^{q+1} = 1 - k$. Since $y^{q+1} = k$ we have $\langle u, Eu\rangle = k(dx^q y + xy^q)/y^{k+1} = k(dz^q + z)$. Hence the part of $\mathrm{Num}(E)$ coming from all $x, y$ with $x^{q+1} = 1 - k$ and $y^{q+1} = k$ is an ellipse associated to $(d, k)$. □

*Proof of Proposition 2:* Take $u = (x, y) \in \mathbb{F}_{q^2}^2$ with $\langle u, u\rangle = 1$, i.e. with $x^{q+1} + y^{q+1} = 1$. If $x = 0$, i.e. $y$ is any $y$ with $y^{q+1} = 1$, e.g. $y = 1$, then $\langle u, Mu\rangle = m_{22} = -a$. If $y = 0$, i.e. $x^{q+1} = 1$ (e.g. $x = 1$), then $\langle u, Mu\rangle = m_{11} = a$. Now assume $xy \neq 0$ and $k := y^{q+1}$. We have $x^{k+1} = 1 - k$. We have $Mu = (ax + by, dx - ay)$ and $\langle u, Mu\rangle = ax^{q+1} + bx^q y + dxy^q - ay^{q+1} = bx^q y + dxy^q + a - 2ka$. Let $A(k, a, b, d)$ be the set of all $\langle u, Mu\rangle - a + 2ka$ for all $u = (x, y)$ with $x^{q+1} = 1 - k$ and $y^{q+1} = k$. The proof of Proposition 1, case $bb'$ not a square in $\mathbb{F}_{q^2}$, gives that $\frac{1}{d}B(k, a, b, d)$ is an ellipse of type $(b/d, k)$. □

*Proof of Proposition 3.* We have $c_1, c_2 \in \mathbb{F}_q$. Taking $M - (c_1 + c_2\beta)\mathbb{I}_{2\times 2}$ instead of $M$ we reduce to the case $c_1 = c_2 = 0$. Write $M = (m_{ij})$, $i, j = 1, 2$. Since $u_1$ and $u_2$ are not proportional, they form a basis of $\mathbb{F}_{q^2}^2$. Write $M = (b_{ij})$, $i, j = 1, 2$, in the basis $u_1, u_2$. By assumption $\Re a_{11} = \Re a_{21} = \Re a_{22} = 0$, $\Im a_{11} = \Im a_{22} = \Im a_{12} = 0$ and there are $b, d \in \mathbb{F}_{q^2}^*$ such that $\Re a_{12} = b$ and $\Im a_{12} = d$. Since $\langle\ ,\ \rangle$ is non-degenerate and $\langle u_i, u_i\rangle = 0$, $i = 1, 2$, we have $\langle u_1, u_2\rangle \neq 0$. Taking a multiple of $u_1$ instead of $u_1$ if necessary we reduce to the case $\langle u_1, u_2\rangle = 1$. Thus $\langle u_2, u_1\rangle = 1$. Take $u = xu_1 + yu_2 \in \mathbb{F}_{q^2}^2$ with $\langle u, u\rangle = 1$, i.e. with $x^q y + xy^q = 1$. We have $Mu = xbu_1 + \beta dyu_2$ and $\langle u, Mu\rangle = y^q xb + \beta dyx^q$. Since $x^q y = 1 - xy^q$, we get $\langle u, Mu\rangle = b + (b - \beta d)y^q b$. Since $q - 1 = |\mathrm{Num}(M_+)| \le |\mathrm{Num}(M)|$ by (1), we have $b - \beta d \neq 0$. Hence $(\mathrm{Num}(M) - b)/(b - \beta d)$ is the set $\Delta$ of all $y^q x$ such that $x^q y + xy^q = 1$. Note that $xy \neq 0$ for all $(x, y) \in \Delta$. Fix $c \in \mathbb{F}_{q^2}^*$ and set $\Theta_c := \{z \in \mathbb{F}_{q^2} \mid z^q + z = c^{-q-1}\}$. Since $\Theta_c = \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}^{-1}(c^{-q-1})$, we have $|\Theta_c| = q$. Take any $z \in \Theta_c$ and set $x := zc$ and $y := c$. Since $z \in \Theta_c$, we have $x^q y + xy^q = 1$. Thus $zc^{q+1} = x^q y \in \mathrm{Num}(M)$. Since $c \neq 0$, $zc^{q+1} \neq wc^{q+1}$ for all $z \neq w$. Hence $\Theta_c$ gives a subset $\Delta_c$ of $\mathrm{Num}(M)$ with cardinality $q$. Thus to prove that $|\mathrm{Num}(M)| = q$ it is sufficient to prove that $\Delta_c \subseteq \Delta_1$. Fix $z \in \Theta_c$, i.e assume

$$z^q c^{q+1} + zc^{q+1} = 1. \tag{3}$$

Take $w := zc^{q+1}$. Since $c \in \mathbb{F}_{q^2}$, we have $c^{q(q+1)} = c^{q+1}$. Hence $w^q = z^q c^{q+1}$. Thus (3) gives $w \in \Theta_1$. Thus $w^q \cdot 1 \in \Delta_1$. Since $(zc)^q c = w^q$, $\Delta_c \subseteq \Delta_1$. □

*Proof of Proposition 5:* Taking $M - d\mathbb{I}_{4\times 4}$ instead of $M$ we reduce to the case $d = 0$ with $d_1 - d$ instead of $d$. For any $u = (x_1, x_2, x_3, x_4)$ we have

$$Mu = (b_1x_2, b_6x_1 + (d_1 - d)x_2 + b_2x_3 + b_3x_4, b_4x_4 + b_5x_2, b_7x_2)$$

and hence

$$\langle u, Mu\rangle = x_2^q(b_6x_1 + (d_1-d)x_2 + b_2x_3 + b_3x_4) + x_2(b_1x_1^q + b_5x_3^q + b_7x_4^q) + b_4x_3^qx_4$$

Fix $c \in \mathbb{F}_{q^2}$ and set $x_3 := 1$, $x_4 = c/b_4$ and $x_2 = 0$. For any $x_1$ we have $\langle u, Mu\rangle = c$. Take $x_1$ such that $x_1^{q+1} = k - x_4^{q+1} - x_3^{q+1} - x_2^{q+1} = k - 1 - c^{q+1}/b_4^{q+1}$ (Remark 6). □

## References

1. E. Ballico, On the numerical range of matrices over a finite field, Linear Algebra Appl. 512 (2017) 162–171.
2. E. Ballico, Corrigendum to "On the numerical range of matrices over a finite field [Linear Algebra Appl. 512 (2017) 162–171], Linear Algebra Appl. 556 (2018) 421–427.
3. E. Ballico, Numerical range over finite fields: restriction to subspaces, Linear Algebra Appl. 571 (2019), 1–13.
4. D. Bartoli, M. Montanucci and G. Zini, AG codes and AG quantum codes from the GGS curve, Des. Codes Cryptogr. 66 (2018), 2315–2344.
5. D. Bartoli, M. Montanucci and G. Zini, On certain self-orthogonal AG codes with applications to quantum error-error correcting codes, arXiv:1912.08021.
6. A.R. Calderbank, E.M. Rains, P.W. Shor and N.J.A. Sloane, Quantum error correcting codes via codes over $GF(4)$, IEEE Trans. Inform. Theory 44 (1998), no. 4, 1369–1387.
7. H. Chen, Some good quantum error-correcting codes from algebraic geometry codes, IEEE Trans. Inf. Theory 47 (2001), 2059–2061.
8. J. I. Coons, J. Jenkins, D. Knowles, R. A. Luke and P. X. Rault, Numerical ranges over finite fields, Linear Algebra Appl. 501 (2016), 37–47.
9. C. Galindo and F. Hernando, Quantum codes from affine variety codes and their subfield-subcodes, Des. Codes and Cryptogr. 76 (2015), 89–100.
10. K. E. Gustafson and D. K. M. Rao, Numerical Range. The Field of Values of Linear Operators and Matrices, Springer, New York, 1997.
11. R.A. Horn and C.R. Johnson, Matrix Analysis, Cambridge University Press, New York, 1985.
12. R.A. Horn and C.R. Johnson, Topics in Matrix Analysis, Cambridge University Press, Cambridge, 1991.
13. F. Hernando, G. McGuire, F. Monserrat, and J.J. Moyano-Fernàndez, Quantum codes from a new construction of self-orthogonal algebraic geometry codes, Quantum Inf. Process. 19 (2020), no. 4, Paper No. 117.
14. J. W. P. Hirschfeld, Projective geometries over finite fields, Clarendon Press, Oxford, 1979.
15. J. W. P. Hirschfeld, Finite projective spaces of three dimensions, Oxford Mathematical Monographs, Oxford Science Publications, The Clarendon Press, Oxford University Press, New York, 1985.
16. J. W. P. Hirschfeld and J. A. Thas, General Galois geometries, Oxford Mathematical Monographs, Oxford Science Publications, The Clarendon Press, Oxford University Press, New York, 1991.
17. L. Jin and C. Xing, Euclidean and hermitian self-orthogonal algebraic geometry codes and their application to quantum codes, IEEE Trans. Inform. Theory 58 (2012), 5484–5489.
18. G. G. La Guardia and F. R. F. Pereira, Good and symptotically good quantum codes derived from Algebraic Geometry codes, arXiv:1612.07150.
19. R. Lindl and H. Niederreiter, Introduction to finite fields and their applications, Cambridge University Press, Cambridge, 1994.
20. P.J. Psarrakos and M.J. Tsatsomeros, Numerical range: (in) a matrix nutshell, Notes, National Technical University, Athens, Greece, 2004.
21. J. Roffe, Quantum error correction, arXiv:1907.11157.
22. A.M. Steane, Enlargement of Calderbank-Shor-Steane quantum codes, IEEE Trans. Inform. Theory 52 (2006), no. 5, 2218–2224.

Dept. of Mathematics, University of Trento, 38123 Povo (TN), Italy
*E-mail address*: ballico@science.unitn.it