Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 34, pp. 205-216, May 2018.

THE HERMITIAN NULL-RANGE OF A MATRIX 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 $\mathbb{F}_{q^2}$. In this paper, it is considered the case $k = 0$ of the set $\mathrm{Num}_k(M) := \{\langle u, Mu\rangle \mid u \in \mathbb{F}_{q^2}^n, \langle u, u\rangle = k\}$. When M has coefficients in $\mathbb{F}_q$ the paper studies the set $\mathrm{Num}_k(M)_q := \{\langle u, Mu\rangle \mid u \in \mathbb{F}_q^n, \langle u, u\rangle = k\} \subseteq \mathbb{F}_q$. The set $\mathrm{Num}_1(M)$ is the numerical range of M, previously introduced in a paper by Coons, Jenkins, Knowles, Luke, and Rault (case q a prime $p \equiv 3 \pmod 4$), and by the author (arbitrary q). In this paper, it is studied in details $\mathrm{Num}_0(M)$ and $\mathrm{Num}_k(M)_q$ when $n = 2$. If q is even, $\mathrm{Num}_0(M)_q$ is easily described for arbitrary n. If q is odd, then either $\mathrm{Num}_0(M)_q = \{0\}$, or $\mathrm{Num}_0(M)_q = \mathbb{F}_q$, or $\sharp(\mathrm{Num}_0(M)_q) = (q + 1)/2$.

Key words. Numerical range, Finite field, Hermitian variety over a finite field.

AMS subject classifications. 12E20, 15A33, 15A60.

1. Introduction.

Fix a prime p and a power q of p. Up to field isomorphisms there is a unique field $\mathbb{F}_q$ such that $\sharp(\mathbb{F}_q) = q$ ([10, 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 $\langle v, w\rangle = \sum_{i=1}^n a_i^q b_i$. $\langle \cdot, \cdot\rangle$ is the standard Hermitian form of $\mathbb{F}_{q^2}^n$. The set $\{u \in \mathbb{F}_{q^2}^n \mid \langle u, u\rangle = 1\}$ is an affine chart of the Hermitian variety of $\mathbb{P}^n(\mathbb{F}_{q^2})$ ([4, Ch. 5], [6, Ch. 23]). Let M be an $n \times n$ matrix with coefficients in $\mathbb{F}_{q^2}$. In [1], we made the following definition. The *numerical range* $\mathrm{Num}(M)$ (or $\mathrm{Num}_1(M)$) of M is the set of all $\langle u, Mu\rangle$ with $\langle u, u\rangle = 1$. $\mathbb{C}$ is a degree 2 Galois extension of $\mathbb{R}$ with the complex conjugation as the generator of the Galois group. $\mathbb{F}_{q^2}$ is a degree 2 Galois extension of $\mathbb{F}_q$ with the map $t \mapsto t^q$ as a generator of the Galois group. Hence, $\langle\ ,\ \rangle$ is the Hermitian form associated to this Galois extension. Thus, the definition of $\mathrm{Num}(M)$ is a natural extension of the notion of numerical range in linear algebra ([3], [7], [8], [11]). This extension was introduced in [2] when q is a prime $p \equiv 3 \pmod 4$. In this paper, we consider related subsets $\mathrm{Num}_0'(M) \subseteq \mathrm{Num}_0(M) \subseteq \mathbb{F}_{q^2}$.

As in [2] for any $k \in \mathbb{F}_q$ set $C_n(k) := \{(a_1, \dots, a_n) \in \mathbb{F}_{q^2}^n \mid \sum_{i=1}^n a_i^{q+1} = k\}$. The set $C_n(0)$ is a cone of $\mathbb{F}_{q^2}^n$ and its proiectivization $\mathcal{H}_n \subset \mathbb{P}^{n-1}(\mathbb{F}_{q^2})$ is the Hermitian variety of dimension $n-2$ of $\mathbb{P}^{n-1}(\mathbb{F}_{q^2})$ with rank n. Set $C_n'(0) := C_n(0) \setminus \{0\}$. Recall that $\langle u, u\rangle \in \mathbb{F}_q$ for all $u \in \mathbb{F}_{q^2}^n$. For any $n \times n$ matrix over $\mathbb{F}_{q^2}$ and any $k \in \mathbb{F}_q$ let $\mathrm{Num}_k(M)$ (resp., $\mathrm{Num}_0'(M)$) be the set of all $a \in \mathbb{F}_{q^2}$ such that there is $u \in C_n(k)$ (resp., $u \in C_n'(0)$ and $n \geq 2$) with $a = \langle u, Mu\rangle$. We always have $0 \in \mathrm{Num}_0(M)$, $\mathrm{Num}_0(M) = \mathrm{Num}_0'(M) \cup \{0\}$ and quite often, but not always, we have $0 \in \mathrm{Num}_0'(M)$ (Propositions 2.8, 2.11, 2.12). For instance, we have $\mathrm{Num}_0'(\mathbb{I}_{n\times n}) = \{0\}$ for all $n \geq 2$, where $\mathbb{I}_{n\times n}$ denote the unity $n \times n$ matrix. If $n = 1$, i.e., M is the multiplication by a scalar m, we have $\mathrm{Num}_k(M) = mk$. There is an ambiguity if $n = 1$, because $C_1'(0) = \emptyset$. Hence, we do not define Num_0' for 1×1 matrices. We say that $\mathrm{Num}_0'(M)$ is the *Hermitian null-range* of the matrix M.

We have $\mathrm{Num}_k(M) = k\mathrm{Num}_1(M)$ for all $k \in \mathbb{F}_q^*$ (use Remark 2.2 to adapt the proof of [2, Lemma 2.3]). Thus, we know all numerical ranges of M if we know $\mathrm{Num}_1(M)$ and $\mathrm{Num}_0'(M)$. The first part of

*Received by the editors on October 3, 2016. Accepted for publication on April 5, 2018. Handling Editor: Ilya Spitkovsky.
†Department of Mathematics, University of Trento, 38123 Trento (TN), via Sommarive 14, Italy (ballico@science.unitn.it).
Partially supported by MIUR and GNSAGA (INdAM), Italy.

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 34, pp. 205-216, May 2018.

this paper studies $\mathrm{Num}_0'(M)$. If $n = 2$ we prove several results concerning the set $\mathrm{Num}_0'(M)$ under different assumptions on the eigenvalues and the eigenvectors of M. As a byproduct of our study of the case $n = 2$ we get the following result.

COROLLARY 1.1. *Assume that $M \neq c\mathbb{I}_{n\times n}$ for some $c \in \mathbb{F}_{q^2}$. Then we have* $\sharp(\mathrm{Num}_0(M)) \geq \lceil (q+1)/2\rceil$.

See Propositions 2.8, 2.11 and 2.12 and Lemma 2.10 for the cases in which we describe $\mathrm{Num}_0(M)$ and $\mathrm{Num}_0'(M)$, not just we give lower bounds for their cardinality.

In the second part of this paper, we consider the following question. Fix $k \in \mathbb{F}_q$ and suppose that all coefficient m_{ij} of the matrix M are elements of $\mathbb{F}_q$. For any $k \in \mathbb{F}_q$ let $\mathrm{Num}_k(M)_q$ be the set of all $a \in \mathbb{F}_q$ such that there is $u \in \mathbb{F}_q^n$ with $\langle u, u\rangle = k$ and $\langle u, Mu\rangle = a$. If $n > 1$, $k = 0$ and we also impose that $u \neq 0$, then we get the definition of $\mathrm{Num}_0'(M)_q$. Note that $\mathrm{Num}_k(M)_q \subseteq \mathrm{Num}_k(M) \cap \mathbb{F}_q$ and that $\mathrm{Num}_0'(M)_q \subseteq \mathrm{Num}_0'(M) \cap \mathbb{F}_q$. These inclusions are not always equalities (see Example 3.12). In this part, there are huge differences between the case q even and the case q odd.

First assume that q is even. For any matrix M we have $\mathrm{Num}_0'(M)_q \neq \emptyset$, either $\mathrm{Num}_0'(M)_q = \{0\}$ or $\mathrm{Num}_0'(M)_q \supseteq \mathbb{F}_q^*$, and $\mathrm{Num}_0'(M)_q = \{0\}$ if and only if $m_{ij}+m_{ji}+m_{ii}+m_{jj} = 0$ for all $i \neq j$ (see Proposition 3.13 for a more general result).

Now assume that q is odd. For any $M \in M_{n,n}(\mathbb{F}_q)$ either $\mathrm{Num}_0(M)_q = \{0\}$, or $\mathrm{Num}_0(M)_q = \mathbb{F}_q$, or $\sharp(\mathrm{Num}_0(M)_q) = (q + 1)/2$ (Lemma 3.2). There is a difference between the case $q \equiv 1 \pmod 4$ (in which -1 is a square in $\mathbb{F}_q$) and the case $q \equiv -1 \pmod 4$ (in which -1 is a not square in $\mathbb{F}_q$). For instance if $n = 2$ and $q \equiv -1 \pmod 4$, then $\mathrm{Num}_0'(M)_q = \emptyset$ (part (i) of Proposition 3.9). Now assume $n = 2$ and $q \equiv 1 \pmod 4$. By part (iii) of Proposition 3.9 we have:

1. If $m_{12}+m_{21} \neq 0$, then $\mathrm{Num}_0(M)_q$ contains at least $(q-1)/2$ elements of $\mathbb{F}_q^*$ and we give a condition on $m_{22} - m_{11}$ and $m_{12} + m_{21}$ which gives $\mathrm{Num}_0(M)_q = \mathbb{F}_q$.
2. Assume $m_{12}+m_{21} = 0$. If $m_{11} = m_{22}$, then $\mathrm{Num}_k(M)_q = \{km_{11}\}$ for all $k \in \mathbb{F}_q$ and $0 \in \mathrm{Num}_0'(M)_q$. If $m_{11} \neq m_{22}$, then $\sharp(\mathrm{Num}_k(M)_q) \leq (q + 1)/2$ for all $k \in \mathbb{F}_q$, $\sharp(\mathrm{Num}_0(M)_q) = (q + 1)/2$ and $0 \notin \mathrm{Num}_0'(M)_q$.

See Propositions 3.9 and 3.13 for cases in which we describe $\mathrm{Num}_0'(M)_q$.

2. Preliminaries. For any field K, set $K^* := K \setminus \{0\}$. For any $n \times n$ matrix $N = (n_{ij})$, $n_{ij} \in \mathbb{F}_{q^2}$ for all i, j, set $N^\dagger = (n_{ji}^q)$. For all $u, v \in \mathbb{F}_{q^2}^n$ we have $\langle u, Nv\rangle = \langle N^\dagger u, v\rangle$. The matrix N 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.

REMARK 2.1. Fix a prime p and let r be a power of p. Up to field isomorphisms there is a unique finite field, $\mathbb{F}_r$, with r elements and $\mathbb{F}_r = \{x \in \overline{\mathbb{F}_p} \mid x^r = x\}$. The group $\mathbb{F}_r^*$ is a cyclic group of order $r - 1$ and $\mathbb{F}_r^* = \{x \in \overline{\mathbb{F}_p} \mid x^{r-1} = 1\}$ ([4, page 1], [10, Theorem 2.8], [12, Proposition 1.6]).

REMARK 2.2. 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 $a^{q-1} = 1$ (Remark 2.1), we have $b^{q^2-1} = 1$. Hence, $b \in \mathbb{F}_{q^2}^*$ (Remark 2.1). Thus, there are exactly $q + 1$ elements $c \in \mathbb{F}_{q^2}^*$ with $c^{q+1} = a$.

REMARK 2.3. Let $\mathbb{F}$ be a finite field. If $\mathbb{F}$ has even characteristic, then for each $a \in \mathbb{F}$ there is a unique $b \in \mathbb{F}$ with $b^2 = a$ (e.g. because $\mathbb{F}^*$ is a cyclic group with odd order by Remark 2.1). Now assume that $\mathbb{F}$

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 34, pp. 205-216, May 2018.

has odd characteristic. Each element of $\mathbb{F}$ is a sum of 2 squares of elements of $\mathbb{F}$ ([4, Lemma 5.1.4]). For each $c \in \mathbb{F}^*$ there are either 0 or 2 elements $t \in \mathbb{F}$ with $t^2 = c$. Hence, each non-empty fiber of the map $t \mapsto t^2$ from $\mathbb{F}^*$ into $\mathbb{F}^*$ has cardinality 2. Thus, $\mathbb{F}^*$ has exactly $(\sharp(\mathbb{F})-1)/2$ elements, which are squares (this statement is the case $d = 2$ of [12, Ex. 1.7]). Obviously 0 is a square in $\mathbb{F}$.

Remark 2.4. If $n \geq 2$, then $\mathrm{Num}_0'(\mathbb{I}_{n\times n}) = \{0\}$, because $C_n(0) \neq \{0\}$ for all $n \geq 2$.

Lemma 2.5. *Fix $k \in \mathbb{F}_q$. We have $\alpha \in \mathrm{Num}_k(M)$ (resp., $\alpha \in \mathrm{Num}_0'(M)$) if and only if $\alpha^q \in \mathrm{Num}_k(M^\dagger)$ (resp., $\alpha^q \in \mathrm{Num}_0'(M^\dagger)$). Thus, $\sharp(\mathrm{Num}_k(M)) = \sharp(\mathrm{Num}_k(M^\dagger))$ and $\sharp(\mathrm{Num}_0'(M)) = \sharp(\mathrm{Num}_0'(M^\dagger))$.*

Proof. Fix $u \in \mathbb{F}_{q^2}^n$ and let M be an $n \times n$ matrix over $\mathbb{F}_{q^2}$. We have $\langle u, Mu\rangle = \langle M^\dagger u, u\rangle = (\langle u, M^\dagger u\rangle)^q$. Since $\mathbb{F}_{q^2}^*$ is a cyclic group of order $(q+1)(q-1)$ and q is coprime with $(q+1)(q-1)$, the map $t \mapsto t^q$ induces a bijection $\mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$, proving the lemma. ∎

Remark 2.6. 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 $\mathrm{Num}_k(c\mathbb{I}_{n\times n} + dM) = ck + d\mathrm{Num}_k(M)$.

Lemma 2.7. *Assume $n \geq 2$ and that $M = A \oplus B$ (orthonormal decomposition) with A an $x \times x$ matrix, B an $(n-x)\times(n-x)$ matrix and $0 < x < n$. Then $\mathrm{Num}_0(M) = \mathrm{Num}_0(A) + \mathrm{Num}_0(B) \cup \bigcup_{k\in\mathbb{F}_q^*}(k(\mathrm{Num}_1(A) - \mathrm{Num}_1(B))$. We have $0 \in \mathrm{Num}_0'(M)$ if and only if either $x \geq 2$ and $0 \in \mathrm{Num}_0'(A)$ or $x \leq n-2$ and $0 \in \mathrm{Num}_0'(B)$ or there is $a \in \mathrm{Num}_1(A)$ with $-a \in \mathrm{Num}_1(B)$.*

Proof. Take $u = (v, w) \in \mathbb{F}_{q^2}^n$ with $\langle u, u\rangle = 0$, $v \in \mathbb{F}_{q^2}^x$ and $w \in \mathbb{F}_{q^2}^{n-x}$. We have $\langle u, Mu\rangle = \langle v, Av\rangle + \langle v, Bv\rangle$. We have $\langle u, u\rangle = \langle v, v\rangle + \langle w, w\rangle$, and hence, the assumption "$\langle u, u\rangle = 0$" is equivalent to the assumption "$\langle w, w\rangle = -\langle v, v\rangle$" (note that this is also true when q is even). First assume $\langle v, v\rangle = 0$. We get $\langle w, w\rangle = 0$, $\langle v, Av\rangle \in \mathrm{Num}_0(A)$ and $\langle w, Aw\rangle \in \mathrm{Num}_0(B)$ and so $\mathrm{Num}_0(M) \supseteq \mathrm{Num}_0(A) + \mathrm{Num}_0(B)$. Now assume $k := \langle v, v\rangle \neq 0$. We get $\langle u, Mu\rangle = a + b$ with $a \in \mathrm{Num}_k(A)$ and $b \in \mathrm{Num}_{-k}(B)$. Since $\mathrm{Num}_x(M) = x\mathrm{Num}_1(M)$ for all $x \neq 0$, we have $\mathrm{Num}_k(M) = -\mathrm{Num}_{-k}(M)$ if $k \neq 0$. Hence, $\mathrm{Num}_0(M) \subseteq \mathrm{Num}_0(A) + \mathrm{Num}_0(B) \cup \bigcup_{k\in\mathbb{F}_q^*} k(\mathrm{Num}_1(A) - \mathrm{Num}_1(B))$. The same proof gives the opposite inclusion. Since $u = 0$ if and only if $v = 0$ and $w = 0$, we get that $0 \in \mathrm{Num}_0'(M)$ if and only if we came from a case with $k \neq 0$ or with a case in which $\langle v, v\rangle = \langle w, w\rangle = 0$ and either $v \neq 0$ or $w \neq 0$. ∎

Proposition 2.8. *Assume that M is unitarily equivalent to a diagonal matrix with $c_1, \dots, c_k$, $k \geq 2$, different eigenvalues, $c_i \in \mathbb{F}_{q^2}$ for all i, and c_i occurring with multiplicity $m_i > 0$.*

(a) Assume $k \geq 3$. If $(c_i - c_1)/(c_j - c_1) \in \mathbb{F}_q^*$ for all $1 < i < j \leq k$, then $\mathrm{Num}_0(M) = \{t(c_2 - c_1)\}_{t\in\mathbb{F}_q}$. In the other cases, we have $\mathrm{Num}_0(M) = \mathbb{F}_{q^2}$.

(b) If $k \geq 3$, then $0 \in \mathrm{Num}_0'(M)$ if and only if either $k \geq 4$ or $n \geq 4$ or $n = k = 3$ and $(c_3 - c_1)/(c_2 - c_1) \notin \mathbb{F}_q^*$.

(c) If $k = 2$ and $n \geq 3$, then $\mathrm{Num}_0'(M) = \{t(c_2 - c_1)\}_{t\in\mathbb{F}_q}$.

(d) If $k = n = 2$, then $\mathrm{Num}_0'(M) = \{t(c_2 - c_1)\}_{t\in\mathbb{F}_q^*}$.

Proof. Note that $c_i - c_j \in \mathbb{F}_{q^2}^*$ for all $i \neq j$. Assume for the moment $k \geq 3$ and fix integers i, j such that $2 \leq j < i \leq k$. Since $\mathbb{F}_{q^2}$ is a 2-dimensional $\mathbb{F}_q$-vector space, $c_i - c_1$ and $c_j - c_1$ are a basis of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$ (i.e., $(c_i - c_1)/(c_j - c_1) \notin \mathbb{F}_q^*$) if and only if $c_i - c_j$ and $c_1 - c_j$ are another basis of $\mathbb{F}_{q^2}$. Hence, $(c_i - c_1)/(c_j - c_1) \in \mathbb{F}_q^* \Leftrightarrow (c_i - c_j)/(c_1 - c_j) \in \mathbb{F}_q^* \Leftrightarrow (c_j - c_1)/(c_j - c_1) \in \mathbb{F}_q^*$.

By Remark 2.6, we reduce to the case $c_1 = 0$. Fix $a \in \mathbb{F}_{q^2}$.

(i) Assume $k = 2$. We reduced to the case $c_1 = 0$, and hence, $c_2 - c_1 \neq 0$. Let V_1 (resp., V_2) the eigenspace

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 34, pp. 205-216, May 2018.

for the eigenvalue 0 (resp., $c_2 - c_1$). Take $u \in \mathbb{F}_{q^2}$ and write $u = u_1 + u_2$ with $u_1 \in V_1$ and $u_2 \in V_2$. Since $\langle v, w\rangle = 0$ for all $v \in V_1$ and $w \in V_2$, we have $\langle u, u\rangle = \langle u_1, u_1\rangle + \langle u_2, u_2\rangle$ and $\langle u, Mu\rangle = (c_2 - c_1)\langle u_2, u_2\rangle$. Since $\langle u_2, u_2\rangle \in \mathbb{F}_q$, we get $\mathrm{Num}_0(M) \subseteq \{t(c_2 - c_1)\}_{t\in\mathbb{F}_q}$. Since we may take as $\langle u_2, u_2\rangle$ any $\alpha \in \mathbb{F}_q$ (Remark 2.2) and then take u_1 with $\langle u_1, u_1\rangle = -\alpha$ (Remark 2.2), we get $\mathrm{Num}_0(M) = \{t(c_2 - c_1)\}_{t\in\mathbb{F}_q}$. If $n = 2$ we have $\langle u, Mu\rangle = 0$ if and only if $u_2 = 0$. Hence, it $n = 2$ we have $\langle u, u\rangle = 0$ if and only if $u_1 = u_2 = 0$ and so $0 \notin \mathrm{Num}'_0(M)$. If $n \geq 3$, then $m_i \geq 2$ for some i, and hence, $0 \in \mathrm{Num}'_0(M)$ (Remark 2.4).

(ii) Assume $k \geq 3$, $c_1 = 0$, and that $c_i/c_j \notin \mathbb{F}_q^*$ for some $2 \leq i < j \leq k$, say $c_2/c_3 \notin \mathbb{F}_q^*$. Up to a unitary transformation we may assume that e_1 is an eigenvector of M with eigenvalue 0, e_2 is an eigenvector of M with eigenvalue $c_2 \in \mathbb{F}_{q^2} \setminus \{0\}$ and e_3 is an eigenvector of M with eigenvalue $c_3 \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q c_2$. Since $\mathbb{F}_{q^2}$ is a two-dimensional $\mathbb{F}_q$-vector space and c_2 and c_3 are $\mathbb{F}_q$-linearly independent, there are uniquely determined $a_2, a_3 \in \mathbb{F}_q$ such that $a = a_2c_2 + a_3c_3$. By Remark 2.2 there are $u_i \in \mathbb{F}_{q^2}$, $i = 2, 3$, such that $u_i^{q+1} = a_i$, $i = 2, 3$. Take $u_1 \in \mathbb{F}_{q^2}$ such that $u_1^{q+1} = -a_2 - a_3$ (Remark 2.2) and set $u := u_1e_1 + u_2e_2 + u_3e_3$. We have $\langle u, u\rangle = \sum_{i=1}^{3} u_i^{q+1} = 0$ and $\langle u, Mu\rangle = c_2u_2^{q+1} + c_3u_3^{q+1} = a$. Hence, $\mathrm{Num}_0(M) = \mathbb{F}_{q^2}$.

(iii) Assume $k \geq 3$ and that $(c_i - c_1)/(c_j - c_1) \in \mathbb{F}_q^*$ for all $1 < i < j \leq k$. Note that $\{t(c_2 - c_1)\}_{t\in\mathbb{F}_q} = \{t(c_i - c_1)\}_{t\in\mathbb{F}_q}$ for all $i = 3, \dots, k$. Hence, $z(c_x - c_1) \in \{t(c_2 - c_1)\}_{t\in\mathbb{F}_q}$ for all $z \in \mathbb{F}_q$ and all $x = 1, \dots, k$. Thus, $b^{q+1}(c_x - c_1) \in \{t(c_2 - c_1)\}_{t\in\mathbb{F}_q}$ for all $b \in \mathbb{F}_{q^2}$ and all $x = 1, \dots, k$. By assumption there is an orthonormal basis y_{ij}, $1 \leq i \leq k$, $1 \leq j \leq m_i$, of $\mathbb{F}_{q^2}^n$ such that $My_{ij} = c_iy_{ij}$ for all i, j. Take $u \in \mathbb{F}_{q^2}^n$ such that $\langle u, u\rangle = 0$. Write $u = \sum_{i=1}^{k}\sum_{j=1}^{m_i} b_{ij}y_{ij}$ for some $b_{ij} \in \mathbb{F}_{q^2}$. We have $\langle u, u\rangle = 0$ if and only if $\sum_{i=1}^{k}\sum_{j=1}^{m_i} b_{ij}^{q+1} = 0$. We have $\langle u, Mu\rangle = \sum_{i=1}^{k}\sum_{j=1}^{m_i} b_{ij}^{q+1}c_i$. Taking $\langle u, Mu\rangle - c_1\langle u, u\rangle$ we get $\mathrm{Num}_0(M) \subseteq \{t(c_2 - c_1)\}_{t\in\mathbb{F}_q}$. The case $n = k = 2$ done in step (i) gives $\mathrm{Num}_0(M) \supseteq \{t(c_2 - c_1)\}_{t\in\mathbb{F}_q}$, concluding the proof of part (a).

(iv) Now take $k = n = 3$. We need to check when $0 \in \mathrm{Num}'_0(M)$. We need to find $u_1, u_2, u_3 \in \mathbb{F}_{q^2}$ such that $(u_1, u_2, u_3) \neq (0, 0, 0)$, $u_1^{q+1} + u_2^{q+1} + u_3^{q+1} = 0$ and $c_1u_1^{q+1} + c_2u_2^{q+1} + c_3u_3^{q+1} = 0$. The previous conditions are satisfied if and only if there is $(u_2, u_3) \neq (0, 0)$ such that $(c_2 - c_1)u_2^{q+1} + (c_3 - c_1)u_3^{q+1} = 0$. Since u_2^{q+1} and u_3^{q+1} are elements of $\mathbb{F}_q$, $c_3 - c_2 \neq 0$ and $c_2 - c_1 \neq 0$, this is possible if and only if $(c_3 - c_1)/(c_2 - c_1) \in \mathbb{F}_q$.

(v) Now assume $k \geq 4$. We may assume $c_1 = 0$ and that e_i is an eigenvalue for c_i, $i = 1, \dots, k$. If $u = (x_1, \dots, x_n)$, then Mu and $\langle u, Mu\rangle$ depend only on $x_2, \dots, x_n$, not on x_1. If $n > 4$ take $x_i = 0$ for all $i > 4$. For any $x_2, x_3, x_4 \in \mathbb{F}_{q^2}$ there is $u_1 \in \mathbb{F}_{q^2}$ with $u_1^{q+1} = -x_2^{q+1} - x_3^{q+1} - x_4^{q+1}$ (Remark 2.2). Hence, it is sufficient to find u_2, u_3, u_4 with $(u_2, u_3, u_4) \neq (0, 0, 0)$ and $\sum_{i=2}^{4}(c_i - c_1)u_i^{q+1} = 0$. Since the map $\mathbb{F}_{q^2}^* \to \mathbb{F}_q^*$ defined by the formula $t \mapsto t^{q+1}$ is surjective (Remark 2.2), it is sufficient to find $b_i \in \mathbb{F}_q$, $2 \leq i \leq 4$, such that $(b_2, b_3, b_4) \neq (0, 0, 0)$ and

$$\sum_{i=2}^{4}(c_i - c_1)b_i = 0. \tag{2.1}$$

Since $\mathbb{F}_{q^2}$ is a 2-dimensional vector space over $\mathbb{F}_q$, (2.1) is equivalent to a homogenous linear system with 2 equations and 3 unknowns over $\mathbb{F}_q$, and hence, it has a non-trivial solution.

(vi) Now assume $k = 3$ and $n \geq 4$. Without losing generality we may assume that the eigenspace of c_1 contains e_1, e_2. Use Remark 2.4. $\square$

The case $a = -1$ of Remark 2.2 gives the following lemma.

Lemma 2.9. *Set* $\Theta := \{a \in \overline{\mathbb{F}_q} \mid a^{q+1} = -1\}$. *Then* $\sharp(\Theta) = q + 1$ *and* $\Theta \subset \mathbb{F}_{q^2}^*$.

We write $M = (m_{ij})$.

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 34, pp. 205-216, May 2018.

Lemma 2.10. *Assume $n = 2$, $m_{11} = m_{21} = m_{22} = 0$ and $m_{12} = 1$.*

1. *If q is even, then $\mathrm{Num}'_0(M) = \mathbb{F}^*_{q^2}$.*
2. *If q is odd, then $\sharp(\mathrm{Num}'_0(M)) = (q^2-1)/2$ and $\mathrm{Num}'_0(M)$ is the set of all zw with $z \in \Theta$ and $w \in \mathbb{F}^*_q$.*

Proof. Take $u = ae_1 + be_2$ such that $\langle u, u\rangle = 0$, i.e., such that $a^{q+1} + b^{q+1} = 0$. We have $\langle u, Mu\rangle = \langle u, be_1\rangle = a^q b$. Note that $a = 0$ if and only if $b = 0$, and hence, $0 \notin \mathrm{Num}'_0(M)$. Let Δ be the set of all $a^q b$ with $a, b \in \mathbb{F}^*_q$ and $a^{q+1} + b^{q+1} = 0$. Take $a^q b \in \Delta$. Since $ab \neq 0$ and $a^{q+1} + b^{q+1} = 0$, there is a unique $z \in \Theta$ such that $b = az$, but for a fixed a we may take any $z \in \Theta$ and then set $b := az$. Varying $a \in \mathbb{F}^*_{q^2}$ we get as a^{q+1} all elements of $\mathbb{F}^*_q$ (Remark 2.2). Thus, Δ is the set of all products cz with $c \in \mathbb{F}^*_q$ and $z \in \Theta$. Note that $\sharp(\mathbb{F}^*_q) \cdot \sharp(\Theta) = \sharp(\mathbb{F}^*_{q^2})$ by Lemma 2.9. Take $c, c_1 \in \mathbb{F}^*_q$ and $z, z_1 \in \Theta$ and assume $cz = c_1 z_1$. Hence, $c^{q+1} z^{q+1} = c_1^{q+1} z_1^{q+1}$. Since $z^{q+1} = z_1^{q+1} = -1$, we get $c^{q+1} = c_1^{q+1}$. Since $c, c_1 \in \mathbb{F}^*_q$, we get $c^2 = c_1^2$. If q is even, we get $c = c_1$. Hence, $z = z_1$. Hence, if q is even we get $\sharp(\mathrm{Num}'_0(M)) = q^2 - 1$ and (since $0 \notin \mathrm{Num}'_0(M)$), we get $\mathrm{Num}'_0(M) = \mathbb{F}^*_{q^2}$. Now assume that q is odd. We get that either $c = c_1$ or $c = -c_1$. If $c = c_1$, then we get $z = z_1$. Now assume $c = -c_1$, and hence, $z = -z_1$. We get $cz = (-c)(-z)$. In this case the set of all cz, $c \in \mathbb{F}^*_q$ and $z \in \Theta$ has cardinality $(q^2-1)/2$, and hence, $\sharp(\mathrm{Num}'_0(M)) = (q^2-1)/2$. □

Proposition 2.11. *Take $n = 2$ and assume that M has a unique eigenvalue, c, and that the associated eigenspace is one-dimensional and generated by an eigenvector u with $\langle u, u\rangle \neq 0$. We have $0 \notin \mathrm{Num}'_0(M)$. If q is even, then $\mathrm{Num}'_0(M) = \mathbb{F}^*_{q^2}$. If q is odd, then $\sharp(\mathrm{Num}'_0(M)) = (q^2-1)/2$ and there is a matrix M_1 unitarily equivalent to a multiple of M such that $\mathrm{Num}'_0(M_1)$ is the set of all zw with $z \in \Theta$ and $w \in \mathbb{F}^*_q$.*

Proof. Since $n = 2$ the characteristic polynomial $f(t) \in \mathbb{F}_{q^2}[t]$ of M has degree 2. By assumption $f(t)$ has a unique root, c. If q is odd, then the high school formula for the roots of a degree 2 polynomial gives $c \in \mathbb{F}_{q^2}$. The same holds for even q, because $\mathbb{F}_q$ is perfect ([12, Ex. 1.1]) and, since $p = 2$, the monic polynomial $f(t) = t^2 + d_1 t + d_2$ has c as its only root if and only if $f(t) = (t-c)^2$ (e.g. c is a root both of $f(t)$ and of $f'(t) = 2t + d_1 = d_1$ by [9, Theorem 1.68] and so $d_1 = 0$); see [4, pages 3–4] for the roots of an arbitrary degree 2 polynomial over a finite field with even characteristic. Taking $M - c\mathbb{I}_{2\times 2}$ instead of M we reduce to the case $c = 0$ (Remark 2.6). Take $t \in \mathbb{F}_{q^2}$ such that $t^{q+1} = \langle u, u\rangle$ (Remark 2.2). Using $t^{-1}u$ instead of u we reduce to the case $\langle u, u\rangle = 1$. Hence, up to a unitary transformation we reduce to the case $u = e_1$. In this case, we have $m_{11} = m_{21} = 0$. Since m_{22} is an eigenvalue of M, we have $m_{22} = 0$. Since e_2 is not an eigenvector of M, we have $m_{12} \neq 0$. Take $M_1 := \frac{1}{m_{12}} M$ and apply Lemma 2.10 to M_1. □

Proposition 2.12. *Take $n = 2$ and assume that M has two distinct eigenvalues $c_1, c_2 \in \mathbb{F}_{q^2}$ and eigenvectors u_i of c_i, $1 \le i \le 2$, with $\langle u_i, u_i\rangle = 0$ for all i. Then there is $o \in \mathbb{F}^*_{q^2}$ such that $\mathrm{Num}'_0(M) = \{to\}_{t\in\mathbb{F}_q}$.*

Proof. Each u_i gives that $0 \in \mathrm{Num}'_0(M)$. Since u_1 and u_2 are a basis of $\mathbb{F}^2_{q^2}$, $\langle\ ,\ \rangle$ is non-degenerate and $\langle u_i, u_i\rangle = 0$ for all i, we have $e := \langle u_1, u_2\rangle \neq 0$. Taking u_1 and u_2/e instead of u_1 and u_2 we reduce to the case $e = 1$. Note that $\langle u_2, u_1\rangle = 1$. Taking $M - c_1\mathbb{I}_{2\times 2}$ instead of M we reduce to the case $c_1 = 0$, and hence, $c := c_2 - c_1 \neq 0$. Take $a, b \in \mathbb{F}^*_{q^2}$ and set $u := au_1 + bu_2$. We have $\langle u, u\rangle = b^q a + a^q b$. Hence, $\langle u, u\rangle = 0$ if and only if $b^q a + a^q b = 0$. We have $\langle u, Mu\rangle = \langle u, cbu_2\rangle = a^q bc$. Set $w := b/a$. We have $\langle u, u\rangle = 0$ if and only if $w^q + w = 0$. Since $b \neq 0$, we have $w \neq 0$ and so $\langle u, u\rangle = 0$ if and only if $w^{q-1} + 1 = 0$. We have $\langle u, Mu\rangle = a^{q+1} wc$. By Remark 2.2 varying $a \in \mathbb{F}^*_{q^2}$ we get as a^{q+1} an arbitrary element of $\mathbb{F}^*_q$. If q is even, w is an arbitrary element of $\mathbb{F}^*_q$, because $w^{q-1} = 1$ and $\mathbb{F}^*_q = \{t \in \overline{\mathbb{F}_q} \mid t^{q-1} = 1\}$, and hence, varying a and w we get that $\mathrm{Num}'_0(M) = \{tc\}_{t\in\mathbb{F}_q}$. Now assume that q is odd. In this case, $w \notin \mathbb{F}_q$, because $w^{q-1} = -1 \neq 1$ (Remark 2.1). Take $w_1 \in \mathbb{F}_{q^2}$ with $w_1^{q-1} = -1$ (Remark 2.2). Since $(w/w_1)^{q-1} = 1$, we have $w/w_1 \in \mathbb{F}^*_q$. Hence, varying w with $w^{q-1} = 1$ and a^{q+1} with $a \in \mathbb{F}^*_{q^2}$ we get exactly $q-1$ elements of $\mathbb{F}^*_{q^2}$, all of them of the form $\{to\}_{t\in\mathbb{F}^*_q}$ with $o = wc$. □

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 34, pp. 205-216, May 2018.

Proposition 2.13. *Take $n = 2$ and assume $m_{21} \neq 0$ and $m_{12} \neq 0$. Then:*

(i) $\sharp(\mathrm{Num}_0'(M)) \geq \lceil (q+1)/2 \rceil$;

(ii) If $(-m_{12}/m_{21})^{q+1} \neq 1$, *then* $\sharp(\mathrm{Num}_0'(M)) \geq q+1$.

Proof. Using $M - m_{11}\mathbb{I}_{2\times 2}$ instead of M we reduce to the case $m_{11} = 0$ (Remark 2.6). Take $u = ae_1 + be_2$. We have $\langle u, u\rangle = a^{q+1} + b^{q+1}$, $Mu = bm_{21}e_1 + (am_{12} + m_{22}b)e_2$ and $\langle u, Mu\rangle = a^q bm_{21} + b^q(am_{12} + m_{22}b) = a^q bm_{21} + b^q am_{12} + m_{22}b^{q+1}$. We take only the solutions obtained taking $b = 1$ and so $a \in \Theta$, where Θ is as in Lemma 2.9. To get the lemma we study the number of different values of the restriction to Θ of the polynomial $g(t) = m_{21}t^q + m_{12}t + m_{22}$. This number is the number of different values of the restriction to Θ of the polynomial $f(t) = m_{21}t^q + m_{12}t$. Fix $z, w \in \Theta$ and assume $f(z) = f(w)$. Hence, $f(z)zw = f(w)zw$. Since $z^{q+1} = w^{q+1} = -1$, we get $-m_{21}w + m_{12}z^2 w = -m_{21}z + m_{12}zw^2$. Set $h_z(t) = m_{12}zt^2 - m_{12}z^2 t + m_{21}t - m_{21}z$. The polynomial $h_z(t)$ has at most two zeroes in $\mathbb{F}_{q^2}$, one of them being z. Hence, for each $z \in \Theta$ there is at most one $w \in \Theta$ with $w \neq z$ and $g(w) = g(z)$. Thus, $\sharp(\mathrm{Num}_0'(M)) \geq \lceil (q+1)/2 \rceil$. Assume the existence of $w \neq z$ with $h_z(w) = 0$. Since z and w are the two roots of $h_z(t)$, we have $m_{12}z^2 w = -m_{21}z$, i.e., (since $z \neq 0$) $m_{12}zw = -m_{21}$. Since $(zw)^{q+1} = 1$ and $(-1)^{q+1} = 1$ (even if q is even), we get part (ii). □

Proof of Corollary 1.1. By assumption there are $i, j \in \{1, \ldots, n\}$ such that $i \neq j$ and either $m_{ij} \neq 0$ or $m_{ii} \neq m_{jj}$. Up to a permutation of the indices $\{1, \ldots, n\}$ (which is induced by a unitary transformation of $\mathbb{F}_{q^2}$), we may assume $\{i, j\} = \{1, 2\}$. First assume $n = 2$. Using $M - m_{11}\mathbb{I}_{2\times 2}$ instead of M we reduce to the case $m_{11} = 0$ (Remark 2.6). If $m_{21} = 0$, then we use either Proposition 2.8 (if M is unitarily equivalent to a diagonal matrix) or Proposition 2.11 (if 0 is the unique eigenvalue of M with e_1 spanning its eigenspace). If $m_{21} = 0$ we apply the last sentence to $M^\dagger$ and use Lemma 2.5. Hence, we may assume that $m_{12}m_{21} \neq 0$. Apply Proposition 2.13. Now assume $n > 2$. Call $A = (a_{ij})$ the 2×2 matrix with $a_{ij} = m_{ij}$ for all $i, j = 1, 2$. Take $u = (x_1, \ldots, x_n)$ with $x_i = 0$ for all $i > 2$ and apply the case $n = 2$ to A. □

3. Matrices with coefficients in $\mathbb{F}_q$. We always assume $n \geq 2$. We assume $M = (m_{ij})$ with $m_{ij} \in \mathbb{F}_q$ for all i, j. Take $k \in \mathbb{F}_q$ and $u \in \mathbb{F}_q^n$ with $\langle u, u\rangle = k$ and write $u = \sum_{i=1}^n x_i e_i$ with $x_i \in \mathbb{F}_q$ for all i. Since $x_i \in \mathbb{F}_q$, we have $x_i^{q+1} = x_i^2$ and so the condition $\langle u, u\rangle = k$ is equivalent to the degree 2 equation

$$\sum_{i=1}^{n} x_i^2 = k. \tag{3.2}$$

Since $x_i^q = x_i$ for all i, the condition $\langle u, Mu\rangle = a$ is equivalent to

$$\sum_{i,j=1}^{n} m_{ij}x_i x_j = a. \tag{3.3}$$

Remark 3.1. Fix any $k \in \mathbb{F}_q$, any integer $n \geq 2$ and any $n \times n$ matrix M with coefficients in $\mathbb{F}_q$. Every element of $\mathbb{F}_q$ is a sum of two squares of elements of $\mathbb{F}_q$ (Remark 2.3). Hence, (3.2) has always a solution $(y_1, \ldots, y_n) \in \mathbb{F}_q^n$. Setting $x_i := y_i$ in the left hand side of (3.3) we get $\mathrm{Num}_k(M)_q \neq \emptyset$. However, there are a few cases with $\mathrm{Num}_0'(M)_q = \emptyset$ (part (i) of Proposition 3.9). We always have $\mathrm{Num}_0'(M)_q \neq \emptyset$ if q is even (part (a) of Proposition 3.13).

Lemma 3.2. *Take $M \in M_{n,n}(\mathbb{F}_q)$.*

(a) If q is even, then either $\mathrm{Num}_0(M)_q = \{0\}$ *or* $\mathrm{Num}_0(M)_q = \mathbb{F}_q$.

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 34, pp. 205-216, May 2018.

(b) Assume q odd and that neither $\mathrm{Num}_0(M)_q = \{0\}$ *nor* $\mathrm{Num}_0(M)_q = \mathbb{F}_q$*. Fix* $a \in \mathrm{Num}_0(M)_q \setminus \{0\}$*. Then* $\sharp(\mathrm{Num}_0(M)_q) = (q+1)/2$ *and* $\mathrm{Num}_0(M)_q$ *is the union of* 0 *and all* $b \in \mathbb{F}_q^*$ *such that b/a is a square in* $\mathbb{F}_q$*.*

Proof. Assume the existence of $a \in \mathrm{Num}_0(M)_q$ with $a \neq 0$. Take $u \in \mathbb{F}_q^n$ such that $\langle u, u\rangle = 0$ and $\langle u, Mu\rangle = a$. For any $t \in \mathbb{F}_q^*$ we have $\langle tu, tu\rangle = 0$ and $\langle tu, M(tu)\rangle = t^2a$. Hence, $\mathrm{Num}_0(M)_q \setminus \{0\}$ contains all $b \in \mathbb{F}_q^*$ such that b/a is a square in $\mathbb{F}_q$. If q is even, then every element of $\mathbb{F}_q$ is a square (Remark 2.3) and so $\mathrm{Num}_0(M)_q = \mathbb{F}_q$, proving part (a). Now assume q odd. Since $\mathbb{F}_q^*$ is a cyclic group of even order, $\mathbb{F}_q^*$ has $(q-1)/2$ squares (Remark 2.3). Hence, $\mathrm{Num}_0(M)_q \setminus \{0\}$ contains the set Σ_a of all t^2a, $t \in \mathbb{F}_q^*$. Note that $\sharp(\Sigma_a) = (q-1)/2$. Assume the existence of $d \in \mathrm{Num}_0(M)_q \setminus (\{0\} \cup \Sigma_a)$. If $\alpha, \beta \in \mathbb{F}_q^*$ and α is a square, β is a square if and only if $\alpha\beta$ (or $\alpha/\beta = \alpha\beta/\beta^2$) is a square. Thus, $\mathrm{Num}_0(M)_q \setminus (\{0\} \cup \Sigma_a)$ contains a set, Σ_d, of cardinality $(q-1)/2$. Hence, $\mathrm{Num}_0(M)_q = \mathbb{F}_q$. ∎

Remark 3.3. Take $M \in M_{n,n}(\mathbb{F}_q)$. By Lemma 3.2, if q is even to describe $\mathrm{Num}_0(M)_q$ we only need to say if $\mathrm{Num}_0(M)_q$ is 0 or $\mathbb{F}_q$. Now assume that q is odd. Lemma 3.2 gives $\sharp(\mathrm{Num}_0(M)_q) \in \{0, (q+1)/2, q\}$ and that if $\sharp(\mathrm{Num}_0(M)_q) = (q+1)/2$ to describe $\mathrm{Num}_0(M)_q$ it is sufficient to find a single element of $\mathrm{Num}_0(M)_q \setminus \{0\}$. For any q it is interesting to know if $0 \in \mathrm{Num}_0'(M)_q$.

Set $\mathcal{B}_n := \{u \in \mathbb{F}_q^n \mid \langle u, u\rangle = 0\}$. Let $\nu_M' : \mathcal{B}_n \to \mathbb{F}_q$ be the map defined by the formula $\nu_M'(u) = \langle u, Mu\rangle$.

Remark 3.4. Take another $n \times n$ matrix $N = (n_{ij}) \in M_{n,n}(\mathbb{F}_q)$ with $n_{ii} = m_{ii}$ for all i and $n_{ij} + n_{ji} = m_{ij} + m_{ji}$ for all $i \neq j$. The systems given by (3.2) and (3.3) for M and for N are the same, and hence, $\mathrm{Num}_k(M)_q = \mathrm{Num}_k(N)_q$ for all k and $\mathrm{Num}_0'(M)_q = \mathrm{Num}_0'(N)_q$. As a matrix N we may always take a triangular matrix. If q is odd (i.e., if we may divide by 2 in our fields $\mathbb{F}_q$ and $\mathbb{F}_{q^2}$), then we may take as N a symmetric matrix.

Remark 3.5. For all $c, d \in \mathbb{F}_q$ we have $\mathrm{Num}_0(c\mathbb{I}_{n\times n} + dM)_q = d\mathrm{Num}_0'(M)_q$ and $\mathrm{Num}_k(c\mathbb{I}_{n\times n} + dM)_q = ck + d\mathrm{Num}_k(M)_q$.

Remark 3.6. Fix $k, b \in \mathbb{F}_q^*$, $a \in \mathbb{F}_q$, and assume the existence of $d \in \mathbb{F}_q^*$ such that $b = kd^2$. The map $(x_1, \dots, x_n) \mapsto (dx_1, \dots, dx_n)$ shows that the system given by (3.2) and (3.3) has a solution if and only the system given by (3.2) and (3.3) with b instead of k and ad^2 instead of a has a solution. Hence, $\sharp(\mathrm{Num}_k(M)_q) = \sharp(\mathrm{Num}_b(M)_q)$. If q is even, for all $k, b \in \mathbb{F}_q^*$, $a \in \mathbb{F}_q$ there is $d \in \mathbb{F}_q^*$ such that $b = kd^2$ (Remark 2.3). Hence, if q is even, then $\sharp(\mathrm{Num}_k(M)_q) = \sharp(\mathrm{Num}_1(M)_q)$ for all $k \in \mathbb{F}_q^*$ and a description of $\mathrm{Num}_1(M)_q$ gives a description of $\mathrm{Num}_k(M)_q$ for all $k \neq 0$. Now assume q odd. The multiplicative group $\mathbb{F}_q^*$ is cyclic of order $q-1$ (Remark 2.1). Since $q-1$ is even, the group $\mathbb{F}_q^*/(\mathbb{F}_q^*)^2$ has cardinality 2, and hence, to know all integers $\sharp(\mathrm{Num}_k(M)_q)$, $k \in \mathbb{F}_q^*$, or to describe all $\mathrm{Num}_k(M)_q$, $k \in \mathbb{F}_q^*$, it is sufficient to know it for one k, which is a square in $\mathbb{F}_q^*$ (e.g. for $k = 1$) and for one k, which is not a square in $\mathbb{F}_q^*$.

(a) Assume that q is even. For any $k \in \mathbb{F}_q$ there is a unique $c \in \mathbb{F}_q$ with $c^2 = k$ (Remark 2.3). Hence, (3.2) is equivalent to $(\sum_{i=1}^n x_i + c)^2 = 0$, i.e., to

$$\sum_{i=1}^{n} x_i = c. \tag{3.4}$$

Hence, the system given by (3.2) and (3.3) is equivalent to the system given by (3.3) and (3.4). Writing $x_n = \sum_{i=1}^{n-1} x_i + c$ we translate the system given by (3.3) and (3.4) into a degree 2 polynomial in $x_1, \dots, x_{n-1}$. If $k = a = 0$, then this is a homogeneous polynomial of degree 2 in $n-1$ variables, and hence, it has a non-trivial solution if $n-1 \geq 3$ ([4, Corollary 1], [12, Theorem 3.1]), proving the following result.

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 34, pp. 205-216, May 2018.

Corollary 3.7. *If M has coefficients in $\mathbb{F}_q$, q is even and $n \ge 4$, then $0 \in \mathrm{Num}'_0(M)_q$.*

If k and/or a are arbitrary the system given by (3.3) and (3.4) is equivalent to find a solution in $\mathbb{F}_q^{n-1}$ of a certain polynomial in $\mathbb{F}_q[x_1, \dots, x_{n-1}]$ with degree at most 2. We only fix $c \in \mathbb{F}_q$, but not a. Call $f(x_1, \dots, x_{n-1})$ the left hand side of (3.3) obtaining substituting $x_n = -x_1 - \cdots - x_n + c$. $\mathrm{Num}_k(M)_q$ is described by the image of the map $\mathbb{F}_q^{n-1} \to \mathbb{F}_q$ associated to the polynomial $f(x_1, \dots, x_{n-1})$ with $\deg(f) \le 2$. We claim that if f is not a constant polynomial, then the image of f has cardinality at least $q/2$. Indeed, if $\deg(f) = 1$, then f induces a surjective map $\mathbb{F}_q^{n-1} \to \mathbb{F}_q$. Now assume $\deg(f) = 2$. For any map $h : \mathbb{F}_q \to \mathbb{F}_q$ induced by a degree 2 polynomial a fiber of h has cardinality at most 2. Hence, $\sharp(h(\mathbb{F}_q)) \ge q/2$. Hence, $\sharp(f(\mathbb{F}_q^{n-1})) \ge q/2$. See part (i) of Proposition 3.9 for a case with $f \equiv 0$, $\mathrm{Num}_0(M)_q = \{0\}$ and $\mathrm{Num}'_0(M)_q = \emptyset$.

(b) Assume that q is odd. Taking $a = k = 0$, we get that (3.2) and (3.3) are a system of two degree 2 homogeneous equations. Chevalley-Warning theorem ([12, Theorem 3.1]) gives the following corollary.

Corollary 3.8. *If M has coefficients in $\mathbb{F}_q$, q is odd and $n \ge 5$, then $0 \in \mathrm{Num}'_0(M)_q$.*

The left hand side of (3.2) is a non-degenerate quadratic form $\beta \in \mathbb{F}_q[x_1, \dots, x_n]$. If $n = 2s$ β is characterized in [4, Table 5.1] with $m = n$ (because all the coefficients, 1, appearing on the left hand side of (3.2) are squares in $\mathbb{F}_q$): it is a hyperbolic quadric if either s is even or $q \equiv 1 \pmod 4$ and s is odd, while it is elliptic if s is odd and $q \equiv -1 \pmod 4$.

Now we consider the case $n = 2$ for an arbitrary q.

Proposition 3.9. *Assume $n = 2$ and let $N = (n_{ij})$ be the 2×2-matrix with $n_{11} = m_{11}$, $n_{22} = m_{22}$, $n_{21} = 0$ and $n_{12} = m_{12} + m_{21}$. We have $\mathrm{Num}'_0(M)_q = \mathrm{Num}'_0(N)_q$ and $\mathrm{Num}_k(M)_q = \mathrm{Num}_k(N)_q$ for all $k \in \mathbb{F}_q$.*

(i) If $q \equiv -1 \pmod 4$, then $\mathrm{Num}'_0(M)_q = \emptyset$.

(ii) Assume that q is even. If $m_{22}+m_{12}+m_{21}+m_{11} \neq 0$, then $\mathrm{Num}'_0(M)_q = \mathbb{F}_q^*$ and $\sharp(\mathrm{Num}_k(M)_q) \ge q/2$ for all $k \in \mathbb{F}_q^*$. If $m_{22} + m_{12} + m_{21} + m_{11} = 0$, then $\mathrm{Num}'_0(M)_q = \{0\}$; for any fixed $k \in \mathbb{F}_q^*$ either $\mathrm{Num}_k(M)_q = \mathbb{F}_q$ or $\sharp(\mathrm{Num}_k(M)_q) = 1$. If $m_{12} + m_{21} = 0$ and $m_{11} \neq m_{22}$, then $\mathrm{Num}_k(M)_q = \mathbb{F}_q$ for all $k \in \mathbb{F}_q^*$.

(iii) Assume $q \equiv 1 \pmod 4$.

(iii-1) If $m_{12} + m_{21} \neq 0$, then $\mathrm{Num}_0(M)_q$ contains at least $(q-1)/2$ elements of $\mathbb{F}_q^*$. Take $e \in \mathbb{F}_q$ such that $e^2 = -1$; if $(m_{12}+m_{21})^2 \neq (m_{22}-m_{11})^2$ and $(-m_{11}+m_{22}+e(m_{12}+m_{21}))/(-m_{11}+m_{22}-e(m_{12}+m_{21}))$ is not a square in $\mathbb{F}_q$, then $\mathrm{Num}_0(M)_q = \mathbb{F}_q$.

(iii-2) Assume $m_{12} + m_{21} = 0$. If $m_{11} = m_{22}$, then $\mathrm{Num}_k(M)_q = \{km_{11}\}$ for all $k \in \mathbb{F}_q$ and $0 \in \mathrm{Num}'_0(M)_q$. If $m_{11} \neq m_{22}$, then $\sharp(\mathrm{Num}_k(M)_q) \le (q+1)/2$ for all $k \in \mathbb{F}_q$, $\sharp(\mathrm{Num}_0(M)_q) = (q+1)/2$ and $\sharp(\mathrm{Num}'_0(M)_q) = (q-1)/2$.

Proof. We have $\mathrm{Num}_k(N)_q = \mathrm{Num}_k(M)_q$ and $\mathrm{Num}'_0(N)_q = \mathrm{Num}'_0(M)_q$ by Remark 3.4.

Take $u = x_1e_1 + x_2e_2$ with $\langle u, u\rangle = k$ and $\langle u, Mu\rangle = a$. Hence, we get the system given by (3.2) and (3.3). If q is even, then instead of (3.2) we may use (3.4) with $c^2 = k$.

(a) Assume for the moment $q \equiv -1 \pmod 4$. Thus, q is odd and $(-1)^{(q-1)/2} = -1$ in $\mathbb{Z}$. Since $\mathbb{F}_q^*$ is a cyclic group of order $q-1$, we get that -1 is not a square in $\mathbb{F}_q^*$. Hence, (3.2) for $k = 0$ has only the solution

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 34, pp. 205-216, May 2018.

$x_1 = x_2 = 0$.

(b) Now assume that q is even. Take $k = 0$ in (3.4). We have $x_1 + x_2 = 0$ if and only if $x_1 = x_2$. When $x_1 = x_2$, (3.3) is equivalent to $(m_{22} + m_{12} + m_{21} + m_{11})x_1^2 = a$. If $m_{22} + m_{12} + m_{21} + m_{11} = 0$, then we get $a = 0$ and so $\mathrm{Num}_0(M)_q = \{0\}$; taking $x_1 = x_2 = 1$ we get $\mathrm{Num}_0'(M)_q = \{0\}$. Now assume $m_{22} + m_{12} + m_{21} + m_{11} \neq 0$. If $a = 0$, we get $x_1 = 0$ and so $x_2 = 0$, and hence, $0 \notin \mathrm{Num}_0'(M)_q$. Now assume $a \neq 0$. There is a unique $b \in \mathbb{F}_q^*$ such that $b^2 = a/(m_{22} + m_{12} + m_{21} + m_{11})$ (Remark 2.3). Taking $x_1 = x_2 = b$ we get $a \in \mathrm{Num}_0'(M)_q$.

Now we fix $k \in \mathbb{F}_q^*$ and write $c^2 = k$ with $c \in \mathbb{F}_q^*$ (Remark 2.3). We have $x_2 = x_1 + c$ by (3.4). Substituting this equation in (3.3) we get an equation $f(x_1) = a$ with $\deg(f) \leq 2$. The coefficient of x_1^2 in f is $m_{11}+m_{12}+m_{22}+m_{21}$. If $m_{11}+m_{12}+m_{22}+m_{21} \neq 0$, then $\sharp(f(\mathbb{F}_q)) \geq q/2$, because $\sharp(f^{-1}(t)) \leq 2$ for all $t \in \mathbb{F}_q$. If $m_{11}+m_{12}+m_{22}+m_{21} = 0$, then either f has degree 1 and so it induces a bijection $\mathbb{F}_q \to \mathbb{F}_q$ or it is a constant, α (we allow the case $\alpha = 0$), and hence, $\mathrm{Num}_k(M)_q = \{\alpha\}$. Now assume $m_{12} + m_{21} = 0$ and $m_{11} \neq m_{22}$. Take $k = c^2$. Substituting (3.4), i.e., $x_2 = x_1+c$ in (3.3) we get $(m_{11}+m_{22})x_1^2+c(m_{11}+m_{22}) = a$. Since $m_{11} + m_{22} \neq 0$ and every element of $\mathbb{F}_q$ is square (Remark 2.3), we get $\mathrm{Num}_k(M)_q = \mathbb{F}_q$ for all k.

(c) Now assume that $q \equiv 1 \pmod 4$. Since $q \equiv 1 \pmod 4$, then $(q-1)/2 \in \mathbb{N}$. Since $\mathbb{F}_q^*$ is a cyclic group of order $q-1$, there is $e \in \mathbb{F}_q^*$ with $e^2 = -1$. We have $e \neq -e$ and $t^2 = -1$ with $t \in \overline{\mathbb{F}_q}$ if and only if $t \in \{-e, e\}$. First take $k = 0$, and hence, $x_1 = tx_2$ with $t^2 = -1$, i.e., $t \in \{e, -e\}$. Assume for the moment $m_{12} + m_{12} \neq 0$. Hence, there is $g \in \{e, -e\}$ such that $-m_{11} + g(m_{12} + m_{21}) + m_{22} \neq 0$. Take $x_1 = gx_2$. Since $g^2 = -1$, we have $x_1^2 + x_2^2 = 0$ and (3.3) is transformed into $(-m_{11} + g(m_{12} + m_{21}) + m_{22})x_2^2 = a$. We get that $\mathrm{Num}_0(M)_q$ contains the set $\Delta_{a,g}$ of all $a \in \mathbb{F}_q^*$ such that $a/(-m_{11} + m_{22} + g(m_{12} + m_{21}))$ is a square. Since $(q-1)/2$ elements of $\mathbb{F}_q^*$ are squares (Remark 2.3), we get the first part of (iii1). Now assume the conditions of the second part of (iii1). If $\alpha, \beta \in \mathbb{F}_q^*$ are squares, then $\alpha\beta$ and $\alpha/\beta = \alpha\beta/\beta^2$ are squares. Hence, if $\alpha, \gamma \in \mathbb{F}_q^*$ and α is a square, then γ is a square $\Leftrightarrow \alpha\gamma$ is a square $\Leftrightarrow \alpha/\gamma$ is a square. Hence, $\Delta_{a,-g}$ is well-defined, $\Delta_{a,-g} \subset \mathrm{Num}_0(N)_q$ and $\Delta_{a,-g} \cap \Delta_{a,g} = \emptyset$. Thus, $\mathrm{Num}_0(N)_q = \mathbb{F}_q$.

Now assume $m_{12} + m_{21} = 0$. We have $\mathrm{Num}_0'(M)_q = \mathrm{Num}_0(N)_q$ and $\mathrm{Num}_k(M)_q = \mathrm{Num}_k(N)_q$, where $N = (n_{ij})$ is the diagonal matrix with $n_{11} = m_{11}$ and $n_{22} = m_{22}$. If $m_{11} = m_{22}$, then $N = m_{11}\mathbb{I}_{2\times 2}$, and hence, $\mathrm{Num}_k(N)_q = \{km_{11}\}$ for all $k \in \mathbb{F}_q$ and $0 \in \mathrm{Num}_0'(N)_q$, because $\nu'(e, 1) = 0$. Now assume $m_{11} \neq m_{22}$. We fix $k \in \mathbb{F}_q$, but not a. Subtracting m_{11} times (3.2) from (3.3) we get $(m_{22} - m_{11})x_2^2 = a - km_{11}$. Since $m_{22} \neq m_{11}$ and $(q+1)/2$ elements of $\mathbb{F}_q$ are squares, we get that $\sharp(\mathrm{Num}_k(N)_q) \leq (q+1)/2$ (we only get the inequality $\leq$, because for a given $b \in \mathbb{F}_q$, we are not sure that the equation $x_1^2 + b^2 = k$ has a solution). If $k = 0$, we may always take $x_1 = eb$ and so $\sharp(\mathrm{Num}_0(N)_q) = (q+1)/2$. We have $0 \notin \mathrm{Num}_0'(N)_q$, because we first get $x_2 = 0$ and then $x_1 = 0$. □

The case $k \neq 0$ of step (c) of the proof of Proposition 3.9 proves the following observation.

Remark 3.10. Assume $n = 2$, $q \equiv 1 \pmod 4$ and $m_{12} + m_{21} = 0$. If $m_{11} = m_{22}$, then $\mathrm{Num}_k(M)_q = \{km_{11}\}$ for all $k \in \mathbb{F}_q$. If $m_{11} \neq m_{22}$, then $\sharp(\mathrm{Num}_k(M)_q) \leq (q+1)/2$ for all $k \in \mathbb{F}_q^*$.

Corollary 3.11. *Assume $n \geq 2$, $q \equiv 1 \pmod 4$ and fix an $n \times n$-matrix $M = (m_{ij})$ with coefficients in $\mathbb{F}_q$.*

(i) Assume $m_{ij} + m_{ji} = 0$ for all i, j with $1 \leq i < j \leq n$ and $m_{ii} = m_{11}$ for all i. Then $\mathrm{Num}_k(M)_q = \{km_{11}\}$ for all $k \in \mathbb{F}_q$ and $0 \in \mathrm{Num}_0'(M)_q$.

(ii) If M is not as in (i), then $\mathrm{Num}_0(M)_q$ contains at least $(q-1)/2$ elements of $\mathbb{F}_q^*$.

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 34, pp. 205-216, May 2018.

Proof. Let N be the $n \times n$-matrix with $n_{ii} = m_{ii}$ for all i, $n_{ij} = 0$ for all $i < j$ and $n_{ij} = m_{ij} + m_{ji}$ for all $i < j$. We have $\mathrm{Num}_k(M)_q = \mathrm{Num}_k(N)_q$ and $\mathrm{Num}'_0(M)_q = \mathrm{Num}'_0(N)_q$ by Remark 3.4. Take M as in part (i). We have $N = m_{11}\mathbb{I}_{n\times n}$. Hence, $\mathrm{Num}_k(M)_q = \{km_{11}\}$ for all $k \in \mathbb{F}_q$. We have $0 \in \mathrm{Num}'_0(N)_q$, because the equation $x_1^2 + x_2^2 = 0$ has a non-trivial solution, e.g. $(e, 1)$ with $e^2 = -1$. Now assume that M is not as in (i). Hence, either there are $i < j$ with $m_{ij} + m_{ji} \neq 0$ or there is $i > 1$ with $m_{ii} \neq m_{11}$. In the former (resp., latter) case, we use part (iii1) (resp., (iii2)) of Proposition 3.9. □

Example 3.12. We always have $\mathrm{Num}_k(M)_q \subseteq \mathrm{Num}_k(M) \cap \mathbb{F}_q$ and $\mathrm{Num}'_0(M)_q \subseteq \mathrm{Num}'_0(M) \cap \mathbb{F}_q$, but often these inclusions are strict ones. In the examples, we take $n = 2$. Take $M = \mathbb{I}_{2\times 2}$. We have $0 \in \mathrm{Num}'_0(M)$ by Remark 2.4. If $q \equiv -1 \pmod 4$, then $0 \notin \mathrm{Num}'_0(M)_q$ by part (i) of Proposition 3.9. Now take $n = 2$ and $A = (a_{ij})$ with $a_{11} = a_{21} = a_{12} = 0$ and $a_{22} = 1$. We have $\mathrm{Num}_0(A) \cap \mathbb{F}_q = \mathrm{Num}_0(A) = \mathbb{F}_q$ (part (d) of Proposition 2.8). If $q \equiv -1 \pmod 4$ we have $\mathrm{Num}_0(A)_q = \{0\}$ (part (i) of Proposition 3.9). If $q \equiv 1 \pmod 4$ we have $\sharp(\mathrm{Num}'_0(A)_q) = (q - 1)/2$ (part (iii2) of Proposition 3.9).

Proposition 3.13. *Assume $n \geq 2$ and q even and fix an $n \times n$-matrix $M = (m_{ij})$ with coefficients in $\mathbb{F}_q$.*

(a) We have $\mathrm{Num}'_0(M)_q \neq \emptyset$ and either $0 \in \mathrm{Num}'_0(M)_q$ or $\mathrm{Num}_0(M)_q \supseteq \mathbb{F}_q^*$.

(b) We have $\mathrm{Num}'_0(M)_q = \{0\}$ if and only if $m_{ii} + m_{ij} + m_{ji} + m_{jj} = 0$ for all $i < j$.

(c) Assume $\mathrm{Num}'_0(M)_q \neq \{0\}$. If $n = 2$, (resp., $n = 3$, resp., $n \geq 4$), then $\mathrm{Num}'_0(M)_q = \mathbb{F}_q^*$ (resp., $\mathrm{Num}'_0(M)_q \supseteq \mathbb{F}_q^*$, resp., $\mathrm{Num}'_0(M)_q = \mathbb{F}_q$).

Proof. Part (a) follows from the case $n = 2$, which is true by part (ii) of Proposition 3.9.

The "only if" part of part (b) follows from part (a) and the case $n = 2$, which is true by part (ii) of Proposition 3.9.

Now assume $n \geq 3$ and $m_{ii} + m_{ij} + m_{ji} + m_{jj} = 0$ for all $i < j$. Take $u = \sum_{i=1}^n x_i e_i$, $x_i \in \mathbb{F}_q$. For $i = 1, \dots, n$, the coefficient of x_i^2 in $\langle u, Mu\rangle$ is m_{ii}. If $1 \leq i < j \leq n$ the coefficient of $x_i x_j$ in $\langle u, Mu\rangle$ is $m_{ij} + m_{ji}$. Now assume $\langle u, u\rangle = 0$, i.e., $x_n = x_1 + \cdots + x_{n-1}$. Note that $x_n^2 = x_1^2 + \cdots + x_{n-1}^2$. Fix $i \in \{1, \dots, n-1\}$. After this substitution the coefficient of x_i^2 in $\langle u, Mu\rangle$ is $m_{ii} + m_{nn} + m_{in} + m_{ni} = 0$. Fix $1 \leq i < j \leq n - 1$. After the substitution $x_n = x_1 + \cdots + x_{n-1}$ the coefficient of $x_i x_j$ in $\langle u, Mu\rangle$ is $m_{ij} + m_{ji} + m_{ni} + m_{in} + m_{nj} + m_{jn}$. By assumption we have $m_{ij} + m_{ji} = m_{ii} + m_{jj}$, $m_{ni} + m_{in} = m_{ii} + m_{nn}$ and $m_{nj} + m_{jn} = m_{jj} + m_{nn}$. Hence, $m_{ij} + m_{ji} + m_{ni} + m_{in} + m_{nj} + m_{jn} = 2m_{ii} + 2m_{jj} + 2m_{nn} = 0$. Part (a) gives $\mathrm{Num}'_0(M)_q = \{0\}$.

The case $n = 2$ of part (c) is true by part (ii) of Proposition 3.9. Part (c) for $n = 3$ follows from part (a). Part (c) for $n \geq 4$ follows from part (a) and Corollary 3.7. □

Lemma 3.14. *For every $k \in \mathbb{F}_q$, q odd, and any $a_1 \in \mathbb{F}_q^*$, $a_2 \in \mathbb{F}_q^*$ there are $x_1, x_2 \in \mathbb{F}_q$ such that $a_1x_1^2 + a_2x_2^2 = k$.*

Proof. If $k = 0$, then take $x_1 = x_2 = 0$. Now assume $k \neq 0$. The equation $a_1x_1^2 + a_2x_2^2 - kx_3^2 = 0$ is the equation of a smooth conic $C \subset \mathbb{P}^2(\mathbb{F}_q)$, because for odd q and non-zero a_1, a_2, k the partial derivatives of $a_1x_1^2 + a_2x_2^2 - kx_3^2$ have only $(0, 0, 0)$ as their common zero. We have $\sharp(C) = q + 1$ ([4, Part (i) of Theorem 5.2.6]) and at most two of its points are contained in the line $L \subset \mathbb{P}^2(\mathbb{F}_q)$ with $x_3 = 0$ as its equation. If $(b_1 : b_2 : b_3) \in C \setminus C \cap L$, then $b_3 \neq 0$ and $a_1(b_1/b_3)^2 + a_2(b_1/b_3)^2 = k$. □

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 34, pp. 205-216, May 2018.

Proposition 3.15. *Fix* $c \in \mathbb{F}_q^*$ *and set* $M := c\mathbb{I}_{n\times n}$.

(i) If q *is even, then* $\mathrm{Num}'_0(c\mathbb{I}_{n\times n})_q = \{0\}$ *for all* $n \geq 2$ *and* $\sharp({\nu'_M}^{-1}(0)) = q^{n-1}$.

(ii) Assume that q *is odd. We have* $\mathrm{Num}'_0(c\mathbb{I}_{n\times n})_q = \{0\}$ *if either* $n \geq 3$ *or* $n = 2$ *and* $q \equiv 1 \pmod 4$, *while* $\mathrm{Num}'_0(c\mathbb{I}_{n\times n})_q = \emptyset$ *if* $q \equiv -1 \pmod 4$. *If* $n = 2s+1$ *is odd, then* $\sharp({\nu'_M}^{-1}(0)) = q^{2s}$. *If* $n = 2s$ *with either* s *even or* $q \equiv 1 \pmod 4$, *then* $\sharp({\nu'_M}^{-1}(0)) = q^{2s-1} + q^s - q^{s-1}$. *If* $n = 2s$ *with* s *odd and* $q \equiv -1 \pmod 4$, *then* $\sharp({\nu'_M}^{-1}(0)) = q^{2s-1} - q^s + q^{s-1}$.

Proof. We obviously have $\langle u, c\mathbb{I}_{n\times n}u\rangle = 0$ for any $u \in \mathbb{F}_q$ with $\langle u, u\rangle = 0$. Thus, the only problem is if there is $u \in \mathbb{F}_q^n$, $u \neq 0$, with $\langle u, u\rangle = 0$ and to compute the cardinality of the set of all such u. Write $u = \sum_i x_i e_i$ with $x_i \in \mathbb{F}_q$. First assume that q is even. In this case, the condition $\langle u, u\rangle = 0$ is equivalent to (3.4) with $c = 0$ and it has a non-trivial solution for all $n \geq 2$; moreover the set $\langle u, u\rangle = 0$ is the hyperplane $x_1 + \cdots + x_n = 0$ of $\mathbb{F}_q^n$, and hence, it has cardinality q^{n-1}. Now assume that q is odd. In this case, (3.2) with $k = 0$ is the equation of a certain quadric hypersurface $Q \subset \mathbb{P}^{n-1}(\mathbb{F}_q)$ and $0 \in \mathrm{Num}'_0(c\mathbb{I}_{n\times n})_q$ if and only if $Q(\mathbb{F}_q) \neq \emptyset$, while (since we are working in the vector space $\mathbb{F}_q^n$, instead of the associated projective space) $\sharp({\nu'}_M^{-1}(0)) = 1 + (q-1)\sharp(Q)$. The quadric Q has always full rank, and hence, $Q \neq \emptyset$ if $n - 1 \geq 2$. The integer $\sharp(Q)$ is computed in [4, Table 5.1 and Theorem 5.2.6]. ∎

Proposition 3.16. *Assume* $q \equiv -1 \pmod 4$ *and* $n \geq 3$. *Then* $\mathrm{Num}'_0(M)_q \neq \emptyset$.

Proof. It is sufficient to do the case $n = 3$. Just use that $x_1^2 + x_2^2 + x_3^2 = 0$ has a solution $\neq (0,0,0)$ in $\mathbb{F}_q^3$ by Lemma 3.14 (since q is odd, it has exactly q^2 solutions in $\mathbb{F}_q^3$, because the associated conic $Q \subset \mathbb{P}^2(\mathbb{F}_q)$ has cardinality $q + 1$ ([4, Part (i) of Theorem 5.2.6])). ∎

The assumption "$q \equiv 1 \pmod 4$ if $n = 2$" in the next result is necessary by part (i) of Proposition 3.9.

Proposition 3.17. *Assume* q *odd. If* $n = 2$ *assume* $q \equiv 1 \pmod 4$. *Let* $M = (m_{ij})$ *be an* $n \times n$ *matrix such that* $m_{ij} + m_{ji} = 0$ *for all* $i \neq j$, $m_{11} \neq m_{22}$ *and* $m_{ii} = m_{22}$ *for all* $i > 2$. *Then* $\sharp(\mathrm{Num}_0(M)_q) = (q+1)/2$ *and* $\mathrm{Num}_0(M)_q \setminus \{0\}$ *is the set of all* $a \in \mathbb{F}_q^*$ *such that* $-a/(m_{22} - m_{11})$ *is a square. We have* $0 \in \mathrm{Num}'_0(M)_q$ *if and only if either* $n \geq 4$ *or* $n = 3$ *and* $q \equiv 1 \pmod 4$.

Proof. By Remark 3.4, it is sufficient to do the case in which M is a diagonal matrix. The case $n = 2$ is true by part (iii2) of Proposition 3.9. Now assume $n \geq 3$. Taking the difference of (3.3) with (3.2) multiplied by m_{11} we get $(m_{22} - m_{11})(x_2^2 + \cdots + x_n^2) = a$, while (3.2) gives $x_1^2 = -(x_2^2 + \cdots + x_n^2)$. Thus, if $-a/(m_{22} - m_{11})$ is not a square, then $a \notin \mathrm{Num}_0(M)_q$. If $-a/(m_{22} - m_{11})$ is a square, then we take $x_i = 0$ for $i > 3$, take x_2 and x_3 such that $(m_{22} - m_{11})(x_2^2 + x_3^2) = a$ (Lemma 3.17) and then take x_1 with $x_1^2 = -a/(m_{22} - m_{11})$. Now take $a = 0$. If $n \geq 4$ we take $x_1 = 0$, $x_j = 0$ for all $j > 4$ and find $(x_2, x_3, x_4) \in \mathbb{F}_q^3 \setminus \{(0,0,0)\}$ such that $x_2^2 + x_2^2 + x_3^2 = 0$ (take $x_3 = 1$ and use Lemma 3.14 with $a_1 = a_2 = 1$ and $k = -1$). Now assume $a = 0$ and $n = 3$. We proved that we need to have $x_2^2 + x_3^2 = 0$, and hence, we need to have $x_1 = 0$. There is $(x_2, x_3) \in \mathbb{F}_q^2 \setminus \{(0,0)\}$ with $x_2^2 + x_3^2 = 0$ if and only if -1 is a square in $\mathbb{F}_q$, i.e., if and only if $q \equiv 1 \pmod 4$. ∎

Lemma 3.18. *Let* r *be a prime power. Let* $f \in \mathbb{F}_r[t_1, t_2]$ *be a polynomial of degree at most* 2 *with* f *not a constant. Then* f *assumes at least* $\lceil r/2 \rceil$ *values over* $\mathbb{F}_r$.

Proof. Let $\phi : \mathbb{F}_r^2 \to \mathbb{F}_r$ be the map induced by f. Since $\deg(f) \leq 2$ and f is not constant, for each $a \in \mathbb{F}_r$, $\phi^{-1}(a)$ is an affine conic and in particular $\sharp(\phi^{-1}(a)) \leq 2r$. Hence, $\sharp(\phi(\mathbb{F}_r^2)) \geq \lceil r/2 \rfloor$. ∎

Proposition 3.19. *Assume* q *odd and* $n \geq 3$. *Let* $M = (m_{ij})$ *be an* $n \times n$ *matrix over* $\mathbb{F}_q$ *such that there is* $i \in \{1, \ldots, n\}$ *with* $m_{ij} + m_{ji} = 0$ *for at least* 2 *indices* $j \neq i$ *(say* j_1 *and* j_2*) and either* $m_{j_1 j_1} \neq m_{ii}$ *or* $m_{j_2 j_2} \neq m_{ii}$ *or* $m_{j_1 j_2} + m_{j_2 j_1} \neq 0$. *Then* $\sharp(\mathrm{Num}_k(M)_q) \geq (q+1)/2$ *for all* $k \in \mathbb{F}_q$.

Electronic Journal of Linear Algebra, ISSN 1081-3810
A publication of the International Linear Algebra Society
Volume 34, pp. 205-216, May 2018.

Proof. We reduce to the case $n = 3$ and $m_{32}+m_{23} = m_{31}+m_{13} = 0$ and either $m_{11} \neq m_{33}$ or $m_{22} \neq m_{33}$ or $m_{12} + m_{21} \neq 0$. By Remark 3.4 we may assume that $m_{32} = m_{23} = m_{31} = m_{13} = 0$. Taking the difference between (3.3) and m_{33} times (3.3) we get

$$(m_{11} - m_{33})x_1^2 + (m_{12} + m_{21})x_1x_2 + (m_{22} - m_{33})x_2^2 = a - km_{33}.$$

Solve for a and apply Lemma 3.18. □

Acknowledgment. We thank the referee for useful suggestions.

REFERENCES

[1] E. Ballico. On the numerical range of matrices over a finite field. *Linear Algebra Appl.*, 512:162–171, 2017.
[2] J.I. Coons, J. Jenkins, D. Knowles, R.A. Luke, and P.X. Rault. Numerical ranges over finite fields. *Linear Algebra Appl.*, 501:37–47, 2016.
[3] K.E. Gustafson and D.K.M. Rao. *Numerical Range. The Field of Values of Linear Operators and Matrices*. Springer, New York, 1997.
[4] J.W.P. Hirschfeld. *Projective Geometries Over Finite Fields*. Clarendon Press, Oxford, 1979.
[5] 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.
[6] 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.
[7] R.A. Horn and C.R. Johnson. *Matrix Analysis*. Cambridge University Press, New York, 1985.
[8] R.A. Horn and C.R. Johnson. *Topics in Matrix Analysis*. Cambridge University Press, Cambridge, 1991.
[9] R. Lindl and H. Niederreiter. *Finite Fields*. Cambridge University Press, Cambridge, 1997.
[10] R. Lindl and H. Niederreiter. *Introduction to Finite Fields and Their Applications*. Cambridge University Press, Cambridge, 1994.
[11] P.J. Psarrakos and M.J. Tsatsomeros. *Numerical range: (in) a matrix nutshell*. Mathematical Notes from Washington State University, Part 1, vol. 45, 2002; Part 2, vol. 46, 2003.
[12] C. Small. *Arithmetic of Finite Fields*. Marcel & Dekker, New York, 1973.