The numerical range of matrices over $\mathbb{F}_4$

Edoardo BALLICO

Deptartment of Mathematics, University of Trento Povo, Italy

Received: 23.10.2018 • Accepted/Published Online: 15.02.2019 • Final Version: 27.03.2019

Abstract: For any prime power $q$ and any $u = (x_1, \ldots, x_n), v = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$ set $\langle u, v \rangle := \sum_{i=1}^n x_i^q y_i$. For any $k \in \mathbb{F}_q$ and any $n \times n$ matrix $M$ over $\mathbb{F}_q$, the $k$-numerical range $\text{Num}_k(M)$ of $M$ is the set of all $\langle u, Mu \rangle$ for $u \in \mathbb{F}_q^n$, with $\langle u, u \rangle = k$ [5]. Here, we study the case $q = 2$, which is quite different from the case $q \neq 2$.

Key words: numerical range, finite field, binary field

1. Introduction and main results

Let $q$ be a prime power. Let $\mathbb{F}_q$ denote the only field, up to field isomorphisms, with $|\mathbb{F}_q| = q$ ([8, Theorem 2.5]). Let $e_1, \ldots, e_n$ be the standard basis of $\mathbb{F}_q^n$. For all $v, w \in \mathbb{F}_q^n$, say $v = a_1 e_1 + \cdots + a_n e_n$ and $w = b_1 e_1 + \cdots + b_n e_n$, set $\langle v, w \rangle = \sum_{i=1}^n a_i^q b_i$. $(\cdot, \cdot)$ is the standard Hermitian form of $\mathbb{F}_q^n$. For any $n \geq 1$ and any $a \in \mathbb{F}_q$ set

$$C_n(a) := \{ (x_1, \ldots, x_n) \in \mathbb{F}_q^n | x_1^{q+1} + \cdots + x_n^{q+1} = a \}.$$ 

The set $C_n(1)$ is an affine chart of the Hermitian variety of $\mathbb{P}^n(\mathbb{F}_q^2)$ ([6, Chapter 5], [7, Chapter 23]). Take $M \in M_{n,n}(\mathbb{F}_q)$, i.e. let $M$ be an $n \times n$ matrix with coefficients in $\mathbb{F}_q$. For any $k \in \mathbb{F}_q$ set $\text{Num}_k(M) := \{ \langle u, Mu \rangle | u \in C_n(k) \} \subseteq \mathbb{F}_q$. Set $\text{Num}(M) := \text{Num}_1(M)$. The set $\text{Num}(M)$ is called the numerical range of $M$. These concepts were introduced in [5] when $q$ is a prime $p \equiv 3 \pmod{4}$ and in [1] in the general case. We always have $0 \in \text{Num}_0(M)$. When $n \geq 2$, we defined in [4] the set $\text{Num}_0(M)$ as the set of all $\langle u, Mu \rangle$ for some $u \in \mathbb{F}_q \setminus \{0\}$ such that $\langle u, u \rangle = 0$. We have $\text{Num}_0(M) \setminus \{0\} \subseteq \text{Num}_0(M) \subseteq \text{Num}_0(M)$.

For any $M = (m_{ij}) \in M_{n,n}(\mathbb{F}_q)$, set $(M^t)_{ij} = m_{ji}^q$. For any $M \in M_{n,n}(\mathbb{F}_q^2)$ and any $u \in \mathbb{F}_q^n$, set $\nu_M(u) := \langle u, Mu \rangle$.

If $q = 2$ then in the definition of $C_n(a)$ we just take $a \in \mathbb{F}_2 = \{0, 1\}$. In particular for $q = 2$ (and for all even $q$ by Remark 2.6), we only have to compute $\text{Num}_1(M)$ and $\text{Num}_0(M)$. The cases “$q = 2$” and “$q \neq 2$” (independently of the parity of $q$) are quite different, because if $x \in \mathbb{F}_4 \setminus \{0\}$, then $x^3 = 1$ and therefore when $q = 2$, the set $C_n(a)$ is just the set of all $(x_1, \ldots, x_n) \in \mathbb{F}_4^n$ such that the number of nonzero entries $x_i$ is $\equiv a \pmod{2}$ (Remark 2.8).

*Correspondence: ballico@science.unitn.it

© TÜBİTAK

This work is licensed under a Creative Commons Attribution 4.0 International License.
Obviously all diagonal entries \(m_{ii}\) of a matrix \(M\) belong to \(\text{Num}(M)\). If \(q = 2\) and \(n = 2\) and \(M = (m_{ij})\), then \(\text{Num}(M) = \{m_{11}, m_{22}\}\) (Remark 2.10).

We summarize our main results in the following way (here we take \(q = 2\) and \(M = (m_{ij}) \in M_{n,n}(\mathbb{F}_4)\)).

**Proposition 1.1** Assume \(n \geq 3\). We have \(\text{Num}_0(M) = \{0\}\) if and only if \(M = cI_{n \times n}\) for some \(c \in \mathbb{F}_4\).

**Theorem 1.2** Assume \(n \geq 2\). We have \(\text{Num}_0(M) = \{0, b\}\) with \(b \neq 0\) if and only if \((\frac{1}{b}(M - m_{11}I_{n \times n}))^t = \frac{1}{b}(M - m_{11}I_{n \times n})\) and \(M \neq m_{11}I_{n \times n}\) and this is the case if and only if \(M \neq dI_{n \times n}\) for any \(d\) and there is \(c \in \mathbb{F}_4\) such that \((\frac{1}{b}(M - cI_{n \times n}))^t = \frac{1}{b}(M - cI_{n \times n})\).

**Theorem 1.3** Take \(N \in M_{n,n}(\mathbb{F}_4)\), \(n \geq 3\). We have \(\text{Num}_1(N) = \{a, b\}\) with \(a \neq b\) if and only if \((\frac{1}{b-a}(N - aI_{n,n}))^t = \frac{1}{b-a}(N - aI_{n,n})\) and \(N \neq cI_{n,n}\) for some \(c\).

**Corollary 1.4** Assume \(n \geq 3\). We have \(\text{Num}(M) \subseteq \mathbb{F}_2\) if and only if \(M^t = M\).

**Proposition 1.5** We have \(|\text{Num}(M)| \leq 1\) if and only if \(\text{Num}(M) = \{m_{11}\}\).

(a) If \(n = 2\) we have \(|\text{Num}(M)| = 1\) if and only if \(m_{11} = m_{22}\).

(b) If \(n \geq 3\), then \(\text{Num}(M) = \{m_{11}\}\) if and only if \(M = m_{11}I_{n \times n}\).

We also prove that \(\text{Num}(M) = \mathbb{F}_4\) if \(n \geq 3\), \(M \neq 0I_{n \times n}\) and \(M\) is strictly triangular (Remark 3.5).

2. Preliminaries

For any matrix \(M = (m_{ij}) \in M_{n,n}(\mathbb{F}_q)\), let \(M^t = (a_{ij})\) be the matrix with \(a_{ij} = m_{ji}^q\) for all \(i, j\). \(M\) is said to be Hermitian if \(M^t = M\). Note that the diagonal elements of a Hermitian matrix are contained in \(\mathbb{F}_q\). Let \(e_1 = (1, 0, \ldots, 0), \ldots, e_n = (0, \ldots, 0, 1)\) be the standard basis of \(\mathbb{F}_q^n\). Let \(I_{n \times n}\) denote the identity \(n \times n\) matrix. For any \(a \in \mathbb{F}_q\) and any \(n > 0\) we have \(C_n(a) \neq \emptyset\) by [1, Remark 3] and hence, \(\text{Num}_a(M) \neq \emptyset\) for any \(a\), any \(n\), and any matrix \(M\).

**Notation 2.1** Write \(M = (m_{ij}), i, j = 1, \ldots, n\).

**Remark 2.2** Take \(M = (m_{ij}) \in M_{n,n}(\mathbb{F}_q)\). The vector \(e_i\) gives \(m_{ii} \in \text{Num}(M)\). Hence, \(\text{Num}(M)\) contains all diagonal elements of \(M\).

**Remark 2.3** For any \(a, b \in \mathbb{F}_q^*\), any \(k \in \mathbb{F}_q\), and any \(M \in M_{n,n}(\mathbb{F}_q^*)\), we have \(\text{Num}_k(aM) = a\text{Num}_k(M)\) and \(\text{Num}_k(M + bI_{n,n}) = \text{Num}_k(M) + kb^{q+1}\) ([5, Proposition 3.1], [1, Remark 7], [4, Remark 2.4]).

**Remark 2.4** Take \(M = (m_{ij}) \in M_{n,n}(\mathbb{F}_q)\) such that \(M^t = M\). For any \(u \in \mathbb{F}_q^n\), we have \(\langle M^t u, u \rangle = \langle Mu, u \rangle\). Hence, \(\langle u, Mu \rangle \in \mathbb{F}_q\). Thus, \(\text{Num}_k(M) \subseteq \mathbb{F}_q\) for every \(k \in \mathbb{F}_q\).

We recall from [5] the following definitions. For any \(O, P \in \mathbb{F}_q^2\) the strict affine \(\mathbb{F}_q\)-hull \(((O, P))\) of \(O\) and \(P\) is the set \(\{tO + (1 - t)P\}_{t \in \mathbb{F}_q \backslash \{0, 1\}}\). If \(O = P\), then \(((O, P)) = \{O\}\). If \(O \neq P\), then \(((O, P))\) is the complement of \(\{O, P\}\) in the affine \(\mathbb{F}_q\)-line of \(\mathbb{F}_q^2 \cong \mathbb{F}_q^2\) spanned by \(O\) and \(P\) and hence it has cardinality.
q - 2. For any two nonempty subsets \( S, S' \subseteq \mathbb{F}_q^2 \) set \( ((S, S')) := \cup_{O \in S, P \in S'} ((O, P)) \). With this notation we have the following lemma ([1, Lemma 1]).

**Lemma 2.5** Let \( M \) be unitarily equivalent to the direct sums of matrices \( A \) and \( B \). Then \( \text{Num}(M) = ((\text{Num}(A), \text{Num}(B))) \cup \{ \text{Num}_{0}(A) + \text{Num}(B) \} \cup \{ \text{Num}(A) + \text{Num}_{0}(B) \} \).

**Remark 2.6** Each element of \( \mathbb{F}_q^* \), \( q \) even, is a square. Hence to compute all \( \text{Num}_k(M) \) when \( q \) is even it is sufficient to compute \( \text{Num}_0(M) \) and \( \text{Num}_1(M) \).

Unless otherwise stated, from now on \( m_{ij} \in \mathbb{F}_4 \) and \( q = 2 \).

**Notation 2.7** Fix \( e \in \mathbb{F}_4 \setminus \mathbb{F}_2 \). We have \( e^3 = 1, e^2 + e = 1 \) and \( \mathbb{F}_4 = \{ 0, 1, e, e^2 \} \). If \( a \in \mathbb{F}_4^3 \), then \( a^3 = 1 \). If \( a, b, c \) are 3 different elements of \( \mathbb{F}_4 \), then \( \{ a, b, c, a + b + c \} = \mathbb{F}_4 \). Hence for any \( a \in \mathbb{F}_4 \) the set \( a + \mathbb{F}_4^3 \) of all \( a + b, b \in \mathbb{F}_4^3 \) is the set \( \mathbb{F}_4 \setminus \{ a \} \). We fix some \( e \in \mathbb{F}_4 \setminus \mathbb{F}_2 \) and write \( \mathbb{F}_4 = \{ 0, 1, e, e^2 \} \).

**Remark 2.8** For each \( x \in \mathbb{F}_4^3 \) we have \( x^3 = 1 \). We obviously have \( 0^3 = 0 \). Take \( u = (1, 2, \ldots, n) \in \mathbb{F}_4^n \). We have \( x_1^3 + \cdots + x_n^3 = 1 \) (resp. \( x_1^3 + \cdots + x_n^3 = 0 \)) if and only if \( x_i \neq 0 \) for an odd (resp. an even) number of indices \( i \).

**Remark 2.9** Take \( u \in \mathbb{F}_4^n \) and \( t \in \mathbb{F}_4^* \). We have \( \langle tu, M(tu) \rangle = t^{q+1} \langle u, Mu \rangle = \langle u, Mu \rangle \), because \( t^3 = 1 \).

**Remark 2.10** Assume \( n = 2 \). By Remark 2.8, we have \( \text{Num}(M) = \{ m_{11}, m_{22} \} \).

3. **Strictly triangular matrices**

We first list some cases with \( n = 3 \) in which we prove that \( \text{Num}(M) = \mathbb{F}_4 \). All these matrices are triangular matrices with equal entries, \( m_{11} \), on the diagonal. By [5, Lemma 2.7] to compute \( \text{Num}(M) \), it is sufficient to compute \( \text{Num}(N) \), where \( N \) is the strictly triangular matrix \( M - m_{11}I_{3 \times 3} \).

**Proposition 3.1** Fix \( a, b, c \in \mathbb{F}_4 \) with \( ab \neq 0 \). Take

\[
M = \begin{pmatrix}
  c & b & 0 \\
  0 & c & a \\
  0 & 0 & c
\end{pmatrix}
\]

Then \( \text{Num}(M) = \mathbb{F}_4 \).

**Proof** Taking \( \frac{1}{3}(M - cI_{3 \times 3}) \) instead of \( M \) and applying [5, Lemma 2.7], we reduce to the case \( c = 0 \) and \( a = 1 \). Note that even after this reduction step, we have \( b \in \mathbb{F}_4 \setminus \{ 0 \} \). Take \( u = (x_1, x_2, x_3) \in C_3(1) \), i.e. assume \( x_1^3 + x_2^3 + x_3^3 = 1 \). We have \( \langle u, Mu \rangle = x_2(bx_1^2 + x_2x_3) \). Taking \( x_1 = x_3 = 1 \) and \( x_2 = 0 \), we get \( 0 \in \text{Num}(M) \). From now on we always take \( x_2 = 1 \) and in particular \( x_3^3 = 1 \). Thus, we may use any \( x_1, x_2 \) with \( x_1^3 + x_3^3 = 0 \), i.e. any \( (x_1, x_3) \in \mathbb{F}_4^2 \) with either \( x_1 = x_3 = 0 \) or \( x_1x_3 \neq 0 \). Fix \( c \in \mathbb{F}_4 \setminus \{ b \} \). If \( u = (1, 1, c - b) \), then \( \langle u, Mu \rangle = 1(b + c - b) = c \). Note that \( 1 + e \neq 0 \) and hence, \( b(1 + e) \neq 0 \). We take \( u = (e, 1, b(1 + e)) = be + b + be = b \). \( \square \)
Proposition 3.2 Fix $a, b, c, d \in \mathbb{F}_4$ with $abd \neq 0$. Take

$$M = \begin{pmatrix} c & b & d \\ 0 & c & a \\ 0 & 0 & c \end{pmatrix}$$

Then $\text{Num}(M) = \mathbb{F}_4$.

Proof As in the proof of Proposition 3.1, we reduce to the case $c = 0$ and $d = 1$. Take $u = (x_1, x_2, x_3) \in C_3(1)$, i.e. assume $x_1^3 + x_2^3 + x_3^3 = 1$. We have $Mu = (bx_2 + x_3, ax_3, 0)$ and hence, $\langle u, Mu \rangle = bx_2x_1^2 + x_3x_1^2 + ax_3x_2^2$. Taking $u = (1, 0, 0)$, we get $0 \in \text{Num}(M)$. From now on we always take $x_2 = 1$ and in particular $x_3^2 = 1$. Thus, we may use any $x_1, x_2$ with $x_1^3 + x_2^3 = 0$, i.e. any $(x_1, x_3) \in \mathbb{F}_2^2$ with either $x_1 = x_3 = 0$ or $x_1x_3 \neq 0$. Fix $c \in \mathbb{F}_4 \setminus \{0\}$. It is sufficient to find $x_1, x_3 \in \mathbb{F}_4 \setminus \{0\}$ with $x_1^2(b + x_3) = c + ax_3$. Since $a \neq 0$ and $|\mathbb{F}_4 \setminus \{0\}| = 3$, there is $w \in \mathbb{F}_4 \setminus \{0\}$ such that $b + w \neq 0$ and $c + aw \neq 0$. Since the Frobenius map $t \mapsto t^2$ induces a permutation $\mathbb{F}_4 \setminus \{0\} \rightarrow \mathbb{F}_4 \setminus \{0\}$, there is $z \in \mathbb{F}_4 \setminus \{0\}$ such that $z^2 = (c + aw)/(b + w)$. Take $u = (z, 1, w)$.

Proposition 3.3 Fix $a, b, c \in \mathbb{F}_4$ with $(a, b) \neq (0, 0)$. Take

$$M = \begin{pmatrix} c & a & b \\ 0 & c & 0 \\ 0 & 0 & c \end{pmatrix}$$

Then $\text{Num}(M) = \mathbb{F}_4$.

Proof It is sufficient to do the case $c = 0$. Take $u = (x_1, x_2, x_3) \in C_3(1)$, i.e. assume that 2 or none among $x_1, x_2, x_3$ are zeroes. We have $Mu = (ax_2 + bx_3, 0, 0)$ and hence, $\langle u, Mu \rangle = x_1^2(ax_2 + bx_3)$. Taking $u = (1, 0, 0)$, we get $0 \in \text{Num}(M)$. Fix $w \in \mathbb{F}_4 \setminus \{0\}$. Since $(a, b) \neq (0, 0)$, there is $(a_2, a_3) \in (\mathbb{F}_4 \setminus \{0\})^2$ such that $aa_2 + ba_3 \neq 0$. Since the Frobenius map $t \mapsto t^2$ induces a permutation $\mathbb{F}_4 \setminus \{0\} \rightarrow \mathbb{F}_4 \setminus \{0\}$, there is $z \in \mathbb{F}_4 \setminus \{0\}$ such that $z^2 = w/(aa_2 + ba_3)$. Take $u = (z, a_2, a_3)$.

Proposition 3.4 Take $M = (m_{ij}) \in M_n, n(\mathbb{F}_4)$, $n \geq 3$, such that $m_{ij} = 0$ for all $i \geq j$. We have $\text{Num}(M) = \mathbb{F}_4$ if and only if $M \neq 0$.

Proof Since $\text{Num}(0_{n \times n}) = \{0\}$, we only need to prove the “if” part. Assume $m_{ij} \neq 0$ for some $i < j$. Take any principal minor of $M$ associated to $i, j$ and some $h \in \{1, \ldots, n\} \setminus \{i, j\}$ and apply one of the Propositions above.

Remark 3.5 Take $M$ as in one of the Propositions 3.1, 3.2, 3.3, 3.4. A similar proof works for $M^t$. Thus, we computed $\text{Num}(M)$ for all strictly triangular matrices and proved that $\text{Num}(M) = \mathbb{F}_4$, unless either $n = 2$ or $M = m_{11}I_3x_3$.

4. The proofs

Lemma 4.1 Take $n = 2$. We have $\text{Num}_0(M) = \{0, m_{11} + m_{22} + m_{12} + m_{21}, m_{11} + m_{22} + m_{12}e + m_{21}e^2, m_{11} + m_{22} + m_{12}e^2 + m_{21}e\}$. 

958
1. $\text{Num}_0(M) = \{0\}$ if and only if $m_{11} = m_{22}$ and $m_{12} = m_{21} = 0$.

2. If $m_{11} = m_{22}$ and $m_{12} = m_{21} \neq 0$, then $\text{Num}_0(M) = \{0, m_{12}\}$.

3. Assume $m_{11} = m_{22}$. If either $m_{12} = 0$ and $m_{21} \neq 0$ or $m_{21} = 0$ and $m_{12} \neq 0$, then $\text{Num}_0(M) = \mathbb{F}_4$.

4. If $m_{11} = m_{22}$, $m_{12} \neq m_{21}$ and $m_{12} m_{21} \neq 0$, then $\text{Num}_0(M) = \{0, m_{12}, m_{21}\}$.

5. If $m_{11} \neq m_{22}$ and $m_{21} = m_{12} = 0$, then $\text{Num}_0(M) = \{0, m_{11} + m_{22}\}$.

6. If $m_{11} \neq m_{22}$ and $m_{21} = m_{12} \neq 0$, then $\text{Num}_0(M) = \{0, m_{11} + m_{22}, m_{11} + m_{22} + m_{12}\}$; this set has two elements if and only if $m_{22} = m_{11} + m_{21}$.

7. Assume $m_{11} \neq m_{22}$ and either $m_{12} = 0$ and $m_{21} \neq 0$ or $m_{12} \neq 0$ and $m_{21} = 0$, then $|\text{Num}_0(M)| = 3$ and $\text{Num}_0(M) = \mathbb{F}_4 \setminus \{m_{11} + m_{22}\}$.

8. If $m_{11} \neq m_{22}$, $m_{21} m_{12} \neq 0$ and $m_{12} \neq m_{21}$, then $\text{Num}_0(M) = \{0, m_{11} + m_{22} + e m_{12} + e^2 m_{21}, m_{11} + m_{22} + e^2 m_{12} + e m_{21}\}$; we have $|\text{Num}_0(M)| = 2$ if and only if either $m_{11} + m_{22} + e m_{12} + e^2 m_{21} = 0$ or $m_{11} + m_{22} + e^2 m_{12} + e m_{21} = 0$.

**Proof** Take $u = (x_1, x_2) \in \mathbb{F}_4^2$ with $x_1^2 + x_2^2 = 0$. The case $u = (0, 0)$ gives $0 \in \text{Num}_0(M)$. By Remark 2.8 to compute the other elements of $\text{Num}_0(M)$, we may assume $x_1 \neq 0$ and $x_2 \neq 0$. Using Remark 2.9 with $t = x_1^{-1}$ we reduce to the case $x_1 = 1$. Taking $x_2 = 1$ (resp. $x_2 = e$, resp. $x_2 = e^2$), we get $m_{11} + m_{12} + m_{21} + m_{22} \in \text{Num}_0(M)$ (resp. $m_{11} + m_{12} e + m_{21} e^2 + m_{22} \in \text{Num}_0(M)$, $m_{11} + m_{22} + m_{12} e^2 + m_{21} e \in \text{Num}_0(M)$). We have $m_{12} e + m_{21} e^2 = m_{12} e^2 + m_{21} e$ if and only if $m_{12} (e + e^2) = m_{21} (e + e^2)$, i.e. if and only $m_{12} = m_{21}$. We have $m_{12} + m_{21} = m_{12} e + m_{21} e^2$ if and only if $m_{12} (1 + e) = m_{21} (1 + e^2)$, i.e. if and only if $m_{12} = m_{21}$. We have $m_{12} + m_{21} = m_{12} e^2 + m_{21} e$ if and only if $(m_{12} (1 + e^2) = m_{21} (1 + e)$, i.e. if and only if $m_{12} = m_{21}$, i.e. $m_{12} e^2 = m_{21}$.

(a) Assume $m_{11} = m_{22}$. If $m_{12} = m_{21} = 0$, then $\text{Num}_0(M) = \{0\}$. Now assume $m_{12} = m_{21} \neq 0$. Since $e^2 + e^1 = 1$, we get that $\text{Num}_0(M) = \{0, m_{12} e, m_{12}\}$. If $m_{12} = 0 \neq m_{21}$ (resp. $m_{21} = 0$ and $m_{12} \neq 0$), then $\text{Num}_0(M)$ contains 0, $m_{21}$, $e m_{21}$, $e^2 m_{21}$ (resp. 0, $m_{12}$, $e m_{12}$, $e^2 m_{12}$); in both cases we get $\text{Num}_0(M) = \mathbb{F}_4$. Now assume $m_{12} \neq m_{21}$ and $m_{12} m_{21} \neq 0$. Set $t := m_{12} / m_{21}$. Either $t = e$ or $t = e^2$. Assume $t = e$ (the case $t = e^2$ being similar). $\text{Num}_0(M)$ is the union of 0, $m_{21} (1 + e) = m_{21} e^2 = m_{12}$, $m_{21} (e + e^2) = m_{21}$ and $m_{21} (e^2 + e^3) = 0$. Hence, $\text{Num}_0(M) = \{0, m_{12}, m_{21}\}$.

(b) Assume $m_{11} \neq m_{22}$. If $m_{21} = m_{12} = 0$, then $\text{Num}_0(M) = \{0, m_{11} + m_{22}\}$. If $m_{21} = m_{12} \neq 0$, then $\text{Num}_0(M)$ is the union of 0, $m_{11} + m_{22}$ and $m_{11} + m_{22} + m_{12}$ (recall that $2 m_{12} = 0$ and $e + e^2 = 0$, Assume $m_{12} = 0$ and $m_{21} \neq 0$. We get $\text{Num}_0(M) = \{0, m_{11} + m_{22} + m_{21}, m_{11} + m_{22} + m_{21} e, m_{11} + m_{22} + m_{21} e^2\}$. Since $\{m_{21}, m_{21} e, m_{21} e^2\} = \mathbb{F}_4$, we get $|\text{Num}_0(M)| = 3$ and $\text{Num}_0(M) = \mathbb{F}_4 \setminus \{m_{11} + m_{22}\}$. The same answer comes if $m_{12} \neq 0$ and $m_{21} = 0$. Now assume $m_{12} \neq 0$, $m_{21} \neq 0$, and $m_{12} \neq m_{21}$. We first check that $A := \{m_{12} + m_{21}, e m_{12} + e^2 m_{21}, e^2 m_{12} + e m_{21}\}$ has cardinality 2. Since $e^2 \neq 2$ and $m_{12} \neq m_{21}$, we have $e m_{12} + e^2 m_{21} \neq e^2 m_{12} + e m_{21}$ and $m_{12} + m_{21}$ (if only if $(1 + e) m_{12} = (1 + e^2) m_{21}$, i.e. if and only if $e^2 m_{12} = e m_{21}$, i.e. if and only if $e m_{12} = m_{21}$. In the same way, we see that $m_{12} + m_{21} = e^2 m_{12} + e m_{21}$ and $m_{12} + m_{21}$ (if only if $e^2 m_{12} = m_{21}$. Since $m_{21} / m_{12} \notin \{0, 1\}$, we have $m_{21} / m_{12} \in \{e, e^2\}$. Hence $A = \{e m_{12} + e^2 m_{21}, e^2 m_{12} + e m_{21}\}$. We get part (8).
Lemma 4.2 Take $q = 2$, $n = 3$ and $m_{11} = m_{22} = m_{33}$.

1. If $m_{ij} = 0$ for all $i \neq j$, then $\text{Num}_0(M) = \{0\}$.

2. If $m_{ij} = 0$ and $m_{ji} \neq 0$ for some $i, j$, then $\text{Num}_0(M) = \mathbb{F}_4$.

3. If $m_{ij} \neq m_{ji}$, then $\text{Num}_0(M) \supseteq \{0, m_{ij}, m_{ji}\}$.

4. If $m_{ij} = m_{ji} \neq 0$, then $\text{Num}_0(M) \supseteq \{0, m_{ij}\}$.

All nonzero $m_{ij}$ are in $\text{Num}_0(M) \setminus \{0\}$ and they are the only elements of $\text{Num}_0(M) \setminus \{0\}$ unless there is $i, j$ with $m_{ij} = 0$ and $m_{ji} \neq 0$.

Proof Take $u = (x_1, x_2, x_3) \in \mathbb{F}_4$ with $x_1^2 + x_2^2 + x_3^3 = 0$. By Remark 2.8 either $u = 0$ or there is $i, j \in \{1, 2, 3\}$ with $i \neq j$ and $x_i \neq 0$ if and only if $h \in \{i, j\}$. Apply Lemma 4.1 to the restriction of $M$ to $\mathbb{F}_4 e_i + \mathbb{F}_4 e_j$. □

Remark 2.8, Lemma 4.1, and the proof of Lemma 4.2 give the following result.

Lemma 4.3 Take $n = 3$ and $m_{11} = m_{22} \neq m_{33}$. Let $A = (a_{ij})$ and $B = (b_{ij})$ be the $2 \times 2$ matrices with $a_{ij} = m_{hk}$, $h = i + 1$, $k = i + 1$, and $b_{ij} = m_{vw}$, $v = i$ if $i = 1$, $v = 3$ if $i = 2$, $w = j$ if $j = 1$, $w = 3$ if $j = 2$. $A$ and $B$ are as in one of the last 4 cases of Lemma 4.1.

1. If $m_{12}m_{21} = 0$ and $m_{12} \neq m_{21}$, then $\text{Num}_0(M) = \mathbb{F}_4$

2. If $m_{12} = m_{21} = 0$, then $\text{Num}_0(M) = \text{Num}_0(A) \cup \text{Num}_0(B)$.

3. If $m_{12}m_{21} \neq 0$ and $m_{12} \neq m_{21}$, then $\text{Num}_0(M) = \text{Num}_0(A) \cup \text{Num}_0(B) \cup \{m_{12}, m_{21}\}$; we have $|\text{Num}_0(M)| \geq 3$; we have $\text{Num}_0(M) \neq \mathbb{F}_4$ if and only if $\text{Num}_0(A) \cup \text{Num}_0(B) \supseteq \{0, m_{12}, m_{21}\}$.

Take the set-up of (3), i.e. assume $m_{12}m_{21} \neq 0$ and $m_{12} \neq m_{21}$. $\text{Num}_0(A) \supseteq \{0, m_{12}, m_{21}\}$ if and only if either $m_{13} = m_{31} = 0$ and $m_{11} + m_{33} \in \{m_{12}, m_{21} \text{ or } m_{31}\} \neq m_{13} = m_{31} \neq 0$ and $m_{11} + m_{33}$, $m_{11} + m_{33} + m_{13}$ \subseteq $\{0, m_{12}, m_{21}\}$ or $m_{13} \neq m_{31}$ and $m_{11} + m_{33} + m_{13} + m_{21}$ \subseteq $\{0, m_{12}, m_{21}\}$. The same list works for $B$ exchanging the indices 1 and 2.

Lemma 4.4 Take $n = 3$ and $|\{m_{11}, m_{22}, m_{33}\}| = 3$. Let $A_h = (a_{ij}^h)$, $i, j = 1, 2$, $h = 1, 2, 3$, be the matrix obtained from $M$ deleting the $h$-th row and the $h$-th column; each $A_h$ is as in one of the last 4 cases of Lemma 4.1. We have $\text{Num}_0(M) = \text{Num}_0(A_1) \cup \text{Num}_0(A_2) \cup \text{Num}_0(A_3)$. Hence, $\text{Num}_0(M) = \mathbb{F}_4$ if one of the following conditions is satisfied:

1. $m_{ij} = 0$ for all $i \neq j$.

2. There is $i \in \{1, 2, 3\}$ such that, writing $\{1, 2, 3\} = \{i, j, h\}$, we have $m_{jh}m_{jh} = 0$ and $m_{jh} \neq m_{hj}$.

3. There is $i \in \{1, 2, 3\}$ such that, writing $\{1, 2, 3\} = \{i, j, h\}$, we have $m_{ij} \neq 0$, $m_{ji} \neq 0$, $m_{hi} \neq 0$, $m_{hi} \neq 0$, and $\{m_{ij}, m_{ji}, m_{ih}, m_{hi}\} = \mathbb{F}_4^*$. 

960
Proof  Remark 2.8, Lemma 4.1, and the proof of Lemma 4.2 give Num₀(M) = Num₀(A₁) ∪ Num₀(A₂) ∪ Num₀(A₃).

(a) Assume mᵢₗ = 0 for all i ≠ j. Since mᵢ₁ + mᵢ₂, mᵢ₁ + m₃₃, and mᵢ₂ + m₃₃ are distinct elements of F₄, we have \{0, mᵢ₁ + mᵢ₂, mᵢ₁ + m₃₃, mᵢ₂ + m₃₃\} = F₄.

(b) Assume m₁₂m₂₁ = m₁₃m₃₁ = 0 and m₁₂ + m₂₁ ≠ 0, m₁₃ + m₃₁ ≠ 0. We have Num₀(A₃) = F₄ \ \{m₁₁ + m₁₂\} and Num₀(A₂) = F₄ \ \{m₁₁ + m₃₁\} and thus, Num₀(M) = F₄. The same proof works if either m₂₃m₃₂ = m₁₃m₃₁ = 0 and m₂₃ + m₃₂ ≠ 0, m₁₃ + m₃₁ ≠ 0 or m₁₂m₂₁ = m₂₃m₃₂ = 0 and m₁₂ + m₂₁ ≠ 0, m₂₃ + m₃₂ ≠ 0.

(c) Assume m₁₂ ≠ 0, m₂₁ ≠ 0, m₁₃ ≠ 0, and m₃₁ ≠ 0 and {m₁₂, m₂₁, m₃₁, m₃₁} = F₄. The last 2 cases in Lemma 4.1 give Num₀(A₃) ∪ Num₀(A₂) = F₄. The same proof works for Num₀(A₁) ∪ Num₀(A₂) and Num₀(A₃) ∪ Num₀(A₁).

Lemma 4.5 Assume n = 3. Num(M) is the union of \{m₁₁, m₁₂, m₃₃\}, \sum_{i,j=1}^{3} mᵢᵣ, mᵢ₁ + mᵢ₂ + m₃₃ + e(m₁₂ + m₁₃ + m₃₁) + e²(m₁₂ + m₁₃ + m₃₁), m₁₁ + m₂₂ + m₃₃ + e²(m₁₂ + m₁₃ + m₃₁) + e(m₁₁ + m₁₂ + m₃₂) and Bₕ, h = 1, 2, 3, where (writing \{i,j,h\} = \{1,2,3\}) Bₕ = \{mᵢᵣ + mᵢₗ + mᵢₗ + m₃₃ + e(mᵢᵣ + mᵢₗ + m₃₃) + e²(mᵢᵣ + mᵢₗ + m₃₃) + e₂(mᵢᵣ + mᵢₗ + m₃₃)\}. Now assume that \{i,j,h\} = \{1,2,3\}. By Remark 2.9, we may assume that xᵢ = 1 and hence, either xₕ = e or xₕ = e². In the first case, we have (u, Mu) = mᵢᵣ + mᵢₗ + mᵢₗ + m₃₃ + e(mᵢᵣ + mᵢₗ + m₃₃) + e²(mᵢᵣ + mᵢₗ + m₃₃). In the second case, we have (u, Mu) = mᵢᵣ + mᵢₗ + mᵢₗ + m₃₃ + e²(mᵢᵣ + mᵢₗ + m₃₃) + e(mᵢᵣ + mᵢₗ + m₃₃). Now assume that all entries of u are different. By Remark 2.9, we may assume that x₁ = 1. Hence, either (x₂, x₃) = (e, e²) or (x₂, x₃) = (e², e). In the first case, we have (u, Mu) = m₁₁ + m₁₂ + m₃₃ + e(m₁₁ + m₁₂ + m₃₃) + e²(m₁₁ + m₁₂ + m₃₂) + e(m₁₁ + m₁₂ + m₃₂). In the second case, we have (u, Mu) = m₁₁ + m₁₂ + m₃₃ + e²(m₁₁ + m₁₂ + m₃₁) + e(m₁₁ + m₁₂ + m₃₁). We have Num(M) = F₄ if one of the following conditions is satisfied.

1. m₁₂ + m₂₃ + m₃₁ = t(m₁₃ + m₂₁ + m₃₂) with t ∈ \{e, e²\};
2. mᵢᵣ = mᵢₗ for all i ≠ j.

Corollary 4.6 Assume n = 3 and |\{m₁₁, m₁₂, m₃₃\}| = 3. We have Num(M) = F₄ if one of the following conditions is satisfied.

1. m₁₂ + m₂₃ + m₃₁ = t(m₁₃ + m₂₁ + m₃₂) with t ∈ \{e, e²\};
2. mᵢᵣ = mᵢₗ for all i ≠ j.

Corollary 4.7 Assume n = 3 and |\{m₁₁, m₁₂, m₃₃\}| = 3. Fix 5 of the elements mᵢᵣ with i ≠ j, say all except mₕₖ. There is a choice of mₕₖ with Num(M) = F₄.
**Proof** Since $|\{m_{11}, m_{22}, m_{33}\}| = 3$, we have $\mathbb{F}_4 = \{m_{11}, m_{22}, m_{33}, m_{11} + m_{22} + m_{33}\}$ (Remark 2.7). Hence, it is sufficient to check that $m_{11} + m_{22} + m_{33} \in \text{Num}(M)$ for some choice of $m_{kk}$. We do the case $h = 1$, $k = 2$, because the other cases are similar. We take $m_{12} := e(m_{13} + m_{21} + m_{32}) + m_{23} + m_{31}$ and apply part (1) of Corollary 4.6. The proof shows that if $m_{13} + m_{21} + m_{32} \neq 0$, we have at least 2 choices for $m_{12}$. \[ \square \]

**Lemma 4.8** Take $n = 3$. We have $|\text{Num}(M)| = 1$ if and only if $M = m_{11} I_{3 \times 3}$.

**Proof** Since the “if” part is trivial, we assume $|\text{Num}(M)| = 1$. Since we have $\{m_{11}, m_{22}, m_{33}\} \subseteq \text{Num}(M)$ (Remark 2.2), we have $m_{11} = m_{22} = m_{33}$. Since $e^3 = 1$, Lemma 4.5 gives $m_{12} + m_{23} + m_{31} = e(m_{13} + m_{21} + m_{32})$ and $m_{12} + m_{23} + m_{31} = e^2(m_{13} + m_{21} + m_{32})$. Hence, $m_{12} + m_{23} + m_{31} = m_{13} + m_{21} + m_{32} = 0$, i.e. $m_{31} = m_{12} + m_{23}$ and $m_{32} = m_{13} + m_{21}$. Lemma 4.5 implies that $m_{ij} + m_{ji} + e(m_{ih} + m_{jh}) + e^2(m_{hi} + m_{hj}) = 0$ and $m_{ij} + m_{ji} + e^2(m_{ih} + m_{jh}) + e(m_{hi} + m_{hj}) = 0$ for all $\{i,j,h\} = \{1,2,3\}$. Since $e^2 - e = 1$, subtracting these equalities, we get $m_{ih} + m_{jh} = m_{ki} + m_{jh}$ for all $i, j, h$. In particular, we have $m_{13} + m_{23} = m_{31} + m_{32} = m_{12} + m_{23} + m_{13} + m_{21}$, i.e. $m_{12} = m_{21}$. In the same way, we get $m_{ij} = m_{ji}$ for all $i \neq j$. Then the set $B_h$ in the statement of Lemma 4.6 gives $e(m_{ih} + m_{jh}) + e^2(m_{ih} + m_{ji}) = 0$. Since $e \neq e^2$, we get $m_{ih} + m_{jh} = 0$, i.e. $m_{ik} = m_{jk}$, for all $\{i,j,h\} = \{1,2,3\}$. Since $M$ is symmetric, we get $m_{ij} = m_{12}$ for all $i \neq j$. Since $m_{12} = 3m_{12} = m_{12} + m_{23} + m_{31} = 0$, we get $m_{ij} = 0$ for all $i \neq j$. \[ \square \]

**Proof** [Proof of Proposition 1.1]: The “if” part is obvious, while the “only if” part follows from part (1) of Lemma 4.1. \[ \square \]

**Proof** [Proof of Proposition 1.5]: We always have $\{m_{11}, \ldots, m_{nn}\} \subseteq \text{Num}(M)$ (Remark 2.2) and this inclusion is an equality if $n = 2$ (Remark 2.10), proving the case $n = 2$. The case $n = 3$ is true by Lemma 4.8. Now assume $n \geq 4$ and $|\text{Num}(M)| = 1$. Hence $m_{ii} = m_{11}$ for all $i$. By Lemma 4.8 applied to all $F_4 e_i + F_4 e_j + F_4 e_k$ we have $m_{ij} = 0$ for all $i \neq j$. \[ \square \]

**Proof** [Proof of Theorem 1.2]: Taking $\frac{1}{2} M$ instead of $M$, we reduce to the case $b = 1$ (Remark 2.3). Note that $\text{Num}_0(M) = \text{Num}_0(M - c I_{n \times n})$ for any $c \in \mathbb{F}_4$ (Remark 2.3). Hence, Remark 2.4 and Proposition 4.4 give the “if” part. Note that $M - m_{11} I_{n \times n}$ is Hermitian if and only if $m^2_{ij} = m_{ji}$ for all $i \neq j$ and $m_{ii} - m_{11} \in \mathbb{F}_2$ for all $i$. Hence, $M - m_{11} I_{n \times n}$ is Hermitian if and only if $M - m_{ii} I_{n \times n}$ is Hermitian for some $i \in \{1, \ldots, n\}$ and hence, that $M - m_{11} I_{n \times n}$ is Hermitian if and only if there is $c \in \mathbb{F}_4$ with $M - c I_{n \times n}$ Hermitian.

Now, assume that $\text{Num}_0(M) \subseteq \{0,1\}$. Taking $A := M_{[F_4 e_i + F_4 e_j]}$ with $i \neq j$ we reduce to the case $n = 2$; we write $A = (a_{hk})$, $h, k = 1, 2$. Then taking $M - a_{11} I_{2 \times 2}$, we reduce to the case $a_{11} = 0$. After this reduction, we need to prove that $M^\dagger = M$. If $n = 2$ we assume $\text{Num}_0(M) = \{0,1\}$, but if $n \geq 3$ we only assume that $\text{Num}_0(A) \subseteq \{0,1\}$.

First, assume that $a_{22} = 0$. Set $\alpha := a_{12} + a_{21}$, $\beta := ea_{12} + e^2 a_{21}$ and $\gamma := e^2 a_{12} + a_{21}$. Since $2a = 0$ for all $a \in \mathbb{F}_4$, $e^2 + 1 = e$, $e + 1 = e^2$ and $e^2 + 1 = \alpha$, we have $\alpha + \beta = \gamma$, $\beta + \gamma = \alpha$ and $\alpha + \gamma = \beta$. Lemma 4.1 gives $\alpha, \beta, \gamma \in \mathbb{F}_2$. First, assume that $\alpha = 0$, i.e. $a_{12} = a_{21}$. We get $\beta = (e^2 + e)a_{12}$ and so $a_{12} \in \mathbb{F}_2$. Thus, $A$ is Hermitian in this case.

Now, assume that $a_{22} \neq 0 = a_{11}$. If $a_{12} = a_{21} = 0$, then part (5) of Lemma 4.1 implies that $a_{22} \in \mathbb{F}_2$ and hence, $A$ is Hermitian. Case (7) of Lemma 4.1 excludes the case where $a_{12}a_{21} = 0$ and
Lemma and \((e,F)\) restriction to proving the "if" part.

Since \(a_{12}=a_{21} \neq 0\), we have \(\beta=0\) and set \(M:=\frac{1}{a_{12}}(N-a_{12}I_n)\). By Remark 2.3, we have \(\det(M)=\{0,1\}\). By Theorem 1.2, the matrices \(N\) and \(M\) are not a multiple of \(I_n\). Hence, to prove Theorem 1.3, it is sufficient to prove Corollary 1.4. Also note that in the last assertion of Theorem 1.3, it is sufficient to assume that \(N \neq e_i e_j\) with \(i \neq j\).

If \(M^t=M\), then for any \(u \in \mathbb{F}_4^n\), we have \(\langle u, Mu \rangle = \langle Mu, u \rangle = (\langle u, Mu \rangle)^2\) and hence, \(\det(M) \subseteq \mathbb{F}_2\), proving the "if" part.

Now, assume that \(\det(M) \subseteq \mathbb{F}_2\). Since \(\langle e_i, Me_i \rangle = m_{ii}\), we have \(m_{ii} \in \mathbb{F}_2\) for all \(i\). Taking the restriction to \(\mathbb{F}_4\), we have \(m_{ii} \in \mathbb{F}_2\) for all \(i\). Taking the restriction to \(\mathbb{F}_4\), we have \(m_{ii} \in \mathbb{F}_2\) for all \(i\).

(a) First, assume that \(m_{ii}=1\) for all \(i\). By Remark 2.3, taking \(I_2+M\) instead of \(M\) if \(m_{ii}=1\), we reduce to the case \(m_{11}=m_{22}=m_{33}=0\). Set \(\alpha:=m_{12}+m_{23}+m_{31}\) and \(\beta:=m_{13}+m_{21}+m_{32}\). By Lemma 4.5 \(\alpha+\beta \in \mathbb{F}_2\), \(e\alpha+e^2\beta \in \mathbb{F}_2\) and \(e^2\alpha+e\beta \in \mathbb{F}_2\). Since \(e^2+e=1\), we get \(\alpha+\beta \in \mathbb{F}_2\). For any \(\{i,j,h\} \subseteq \{1,2,3\}\) set \(\delta_i:=m_{ij}+m_{hi}\). By Lemma 4.5, each element of \(B_h\), \(h=1,2,3\), is contained in \(\mathbb{F}_2\).

Since \(\sum_{ij} m_{ij} \in \det(M)\) (Lemma 4.5), we have \(\delta_1+\delta_2+\delta_3 \in \mathbb{F}_2\). Hence, \(\delta_i \in \mathbb{F}_2\) for all \(i\).

Let \(B=(b_{ij})\), \(i,j=1,2,3\), be the \(3 \times 3\) matrix with \(b_{ii}=0\) for all \(i\), \(b_{ij}=m_{ij}\) if \(j<i\) and \(b_{ji}=b_{ij}^2\) if \(i<j\). Thus, \(B\) is a Hermitian matrix and therefore, \(\det(D) \subseteq \mathbb{F}_2\) if \(D:=M+B\). Note that \(D=(d_{ij})\)
\[d_{ij}=0\] if either \(i \geq j\) or \(i<j\) and \(m_{ij}=m_{ji}^2\) and that \(d_{ij}=1\) if \(i<j\) and \(m_{ij} \neq m_{ji}^2\), because \(x^2+x=1\) if \(x \in \mathbb{F}_4 \setminus \{2\}\) and \(x^2+x=0\) if \(x \in \mathbb{F}_2\).

(a1) Assume that \(B\) has exactly one nonzero entry. First, assume that \(d_{12}=1\); take \(u=(1,e,1)\); we have \(Du=(e,0,0)\) and \(\langle u, Du \rangle = e \notin \mathbb{F}_2\), a contradiction. If \(d_{13}=1\) take \(u=(1,1,e)\). If \(d_{23}=1\), take \(u=(1,1,e)\).

(a2) Now, assume that \(B\) has 2 nonzero entries. First, assume that \(d_{12}=d_{13}=1\) and \(d_{23}=0\): take \(u=(1,e,1)\); we have \(Du=(e,1,0)\) and \(\langle u, Du \rangle = e+1 \notin \mathbb{F}_2\), a contradiction. Now, assume that \(d_{12}=0\) and \(d_{13}=d_{23}=1\); take \(u=(1,e,1)\); we have \(Du=(e,e,0)\) and \(\langle u, Du \rangle = e+e^3 = e+1 \notin \mathbb{F}_2\), a contradiction. Now, assume that \(d_{12}=d_{23}=1\) and \(d_{13}=0\); take \(u=(1,e,e)\); we have \(Du=(e,e,0)\) and \(\langle u, Du \rangle = e+e^3 = e+1 \notin \mathbb{F}_2\), a contradiction.

(a3) Now, assume that \(d_{12}=d_{13}=d_{23}=1\); take \(u=(1,e,1)\); since \(e+1=e^2\), we have \(Du=(e^2,e,0)\) and \(\langle u, Du \rangle = e^2+e^3 \notin \mathbb{F}_2\), a contradiction.

(b) Now, assume that \(m_{ii} \neq m_{jj} \) for some \(i \neq j\). Let \(E=(e_{ij}) \in M_{3,3}(\mathbb{F}_2)\) be the diagonal matrix with \(e_{ii}=m_{ii}\) for all \(i\). Since \(m_{ii} \in \mathbb{F}_2\) for all \(i\), we have \(E^t=E\) and hence, \(G:=M+E\) is Hermitian if and only.
if $G$ is Hermitian. Since $E$ is Hermitian, $\langle u, Eu \rangle \in \mathbb{F}_2$ for all $u \in \mathbb{F}_4$. Hence, $\langle u, Gu \rangle = \langle u, Mu \rangle + \langle u, Eu \rangle \in \mathbb{F}_2$ for all $u \in C_3(1)$. Since all diagonal elements of $G$ are zero, step (a) gives $G^\dagger = G$ and so $M^\dagger = M$. □

Acknowledgments

The author was partially supported by Ministero Istruzione Università Ricerca (Italy) and Gruppo Nazionale Geometria Algebra (Istituto di Alta Matematica, Italy).

References