Linear Algebra and its Applications 512 (2017) 162–171

Contents lists available at ScienceDirect

Linear Algebra and its Applications

www.elsevier.com/locate/laa

On the numerical range of matrices over a finite field

E. Ballico [1]

Dept. of Mathematics, University of Trento, 3123 Povo (TN), Italy

ARTICLE INFO

Article history:
Received 13 April 2016
Accepted 21 September 2016
Available online 23 September 2016
Submitted by C.-K. Li

MSC:
15A33
15A60

Keywords:
Numerical range
Finite field
2×2-matrix

ABSTRACT

Let q be a prime power. Following a paper by Coons, Jenkins, Knowles, Luke and Rault (case q a prime $p \equiv 3 \pmod 4$) we define the numerical range $\mathrm{Num}(M) \subseteq \mathbb{F}_{q^2}$ of an $n \times n$-matrix M with coefficients in $\mathbb{F}_{q^2}$ in terms of the usual Hermitian form. We prove that $\sharp(\mathrm{Num}(M)) > q$ (case $q \neq 2$), unless M is unitarily equivalent to a diagonal matrix with eigenvalues contained in an affine $\mathbb{F}_q$-line. We study in details $\mathrm{Num}(M)$ when $n = 2$.

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 $\sharp(\mathbb{F}_q) = q$ [9, 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 $\mathbb{F}_{q^2}^n$. 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 $\mathbb{F}_{q^2}$. The *numerical range* $\mathrm{Num}(M)$ of M is the set of all $\langle u, Mu\rangle$

E-mail address: ballico@science.unitn.it.

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

http://dx.doi.org/10.1016/j.laa.2016.09.036

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 [3,7,8,10]. This extension was introduced in [2] when q is a prime $p \equiv 3 \pmod 4$.

For any $d \in \mathbb{F}_q \setminus \{0\}$ and any $c \in \mathbb{F}_{q^2}$ the set $C_{c,d} := \{x \in \mathbb{F}_{q^2} \mid (x-c)^{q+1} = d\}$ is called the *Hermitian circle with center c and squared-radius d*. The map $x \mapsto x - c$ induces a bijection between $C_{c,d}$ and $C_{0,d}$. We have $\sharp(C_{0,d}) = q+1$ for all $d \in \mathbb{F}_q \setminus \{0\}$ (Remark 3). $\mathbb{F}_{q^2}$ is a 2-dimensional $\mathbb{F}_q$-vector space and hence it has q^2+q *affine* $\mathbb{F}_q$*-lines*, i.e. subsets of the form $\{ta + (1-t)b\}_{t\in\mathbb{F}_q}$ for some $a, b \in \mathbb{F}_{q^2}$ with $a \neq b$.

We prove the following result (in which $\mathbb{I}_{x\times x}$ is the identity $x \times x$ matrix).

Theorem 1. *Let M be an $n \times n$-matrix over $\mathbb{F}_{q^2}$.*

(a) *If $M = c\mathbb{I}_{n\times n}$, then* $\mathrm{Num}(M) = \{c\}$.
(b) *If M is unitarily equivalent to a direct sum of $k \geq 2$ diagonal matrices $c_i\mathbb{I}_{n_i\times n_i}$, $1 \leq i \leq k$, with $c_i \neq c_j$ for all $i \neq j$, then either* $\mathrm{Num}(M) = \mathbb{F}_{q^2}$ *or* $\mathrm{Num}(M)$ *is the affine $\mathbb{F}_q$-line $\{tc_1 + (1-t)c_2\}_{t\in\mathbb{F}_q}$, the latter case occurring if and only if $c_i \in \{tc_1 + (1-t)c_2\}_{t\in\mathbb{F}_q}$ for all i.*
(c) *If $M \neq c\mathbb{I}_{n\times n}$, then* $\mathrm{Num}(M)$ *contains either an affine $\mathbb{F}_q$-line or a Hermitian circle.*
(d) *If M is not as in (a) or (b) and $q \neq 2$, then* $\sharp(\mathrm{Num}(M)) > q$.

Except to prove Theorem 1 we only consider 2×2 matrices. For certain 2×2 matrices M we are able to describe $\mathrm{Num}(M)$. Obviously $\mathrm{Num}(M) = \{c\}$ if $M = c\mathbb{I}_{n\times n}$.

Proposition 1. *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* $\sharp(\mathrm{Num}(M)) = 1 + \rho(q+1)$ *and* $\mathrm{Num}(M)$ *is the disjoint union of $\{c\}$ and ρ disjoint Hermitian circles with centers at c.*

Proposition 2. *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 $Mv_i = c_iv_i$, $\langle v_1, v_1\rangle \neq 0$ and $\langle v_1, v_2\rangle \neq 0$. Then* $\mathrm{Num}(M)$ *is the union of $\{c_1, c_2\}$ and ρ Hermitian circles and hence* $\mathrm{Num}(M) \leq 2 + \rho(q+1)$.

In Proposition 4 and in Lemma 2 below we do not claim that the union is a disjoint union and hence we only claim the upper bound for $\sharp(\mathrm{Num}(M))$ (see [1, Example 3.7]).

Proposition 3. *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* $\sharp(\mathrm{Num}(M)) = 1+q$ *and* $\mathrm{Num}(M)$ *is the union of $\{0\}$ and the set $E := \{t \in \mathbb{F}_{q^2} \mid t^q + t = 1\}$.*