Linear Algebra and its Applications 556 (2018) 421–427

Contents lists available at ScienceDirect

Linear Algebra and its Applications

www.elsevier.com/locate/laa

Corrigendum

Corrigendum to "On the numerical range of matrices over a finite field" [Linear Algebra Appl. 512 (2017) 162–171]

E. Ballico [1]

Dept. of Mathematics, University of Trento, 38123 Povo (TN), Italy

ARTICLE INFO

Article history:
Received 4 November 2016
Accepted 20 July 2018
Available online 27 July 2018
Submitted by C.-K. Li

MSC:
15A33
15A60
12E20

Keywords:
Numerical range
Matrix
Finite field

We correct 3 key mistakes in [1]. We use the notation of [1] and in particular for each matrix $M \in M_{n,n}(\mathbb{F}_{q^2})$ let $\operatorname{Num}(M)$ denote the *numerical range* of M.

First correction: In the statement of [1, Proposition 2] $c_2 \in \operatorname{Num}(M)$ if $\langle v_2, v_2\rangle \neq 0$, but if $\langle v_2, v_2\rangle = 0$, then $c_2 \in \operatorname{Num}(M)$ only if c_2 is contained in one of the other ρ circles, i.e. if $\langle v_2, v_2\rangle = 0$ we cannot guarantee that $c_2 \in \operatorname{Num}(M)$.

DOI of original article: https://doi.org/10.1016/j.laa.2016.09.036.
E-mail address: ballico@science.unitn.it.
[1] The author was partially supported by MIUR and GNSAGA of INdAM (Italy).

https://doi.org/10.1016/j.laa.2018.07.027

Second correction: The following statement corrects [1, Proposition 3], i.e. we have $0 \notin \mathrm{Num}(M)$.

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

Proof. In the proof of [1, Proposition 3] we correctly reduced to the case $c_1 = 0$ and $c := c_2 - c_1 \neq 0$ with $\langle v_1, v_2 \rangle = \langle v_2, v_1 \rangle = 1$. The error was the claim in the sixth line of the proof of [1, Proposition 3] that $0 \in \mathrm{Num}(M)$. Now we check that $0 \notin \mathrm{Num}(M)$. Take $u = xv_1 + yv_2 \in C_2(1)$ with $\langle u, u \rangle = 1$, i.e. with $x^q y + xy^q = 1$ and hence $xy \neq 0$. We have $\langle u, Mu \rangle = cx^q y \neq 0$. □

Third correction: Proposition 1 is a counterexample to part (d) of [1, Theorem 1]. The error is in the proof of [1, Lemma 5]. The corrected version is the following one (in which we only claim that $\sharp(\mathrm{Num}(M)) \geq q$ instead of the strict inequality and that even this weaker inequality has one exception).

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

See Examples 1 and 2 for explicit counterexamples.

1. Proof of Theorem 1

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

Lemma 1. *Take $M \in M_{n,n}(\mathbb{F}_{q^2})$ such that $M^\dagger = M$. Then $\langle u, Mu \rangle \in \mathbb{F}_q$ for all $u \in C_n(1) := \{z \in \mathbb{F}_{q^2}^n \mid \langle z, z \rangle = 1\}$.*

Proof. We have $\langle u, Mu \rangle = \langle Mu, u \rangle = \sigma(\langle u, Mu \rangle)$ and hence $\langle u, Mu \rangle \in \mathbb{F}_q$ ([1, Remark 1]). □

First assume q odd. If q is odd, $\mathbb{F}_{q^2}$ is obtained from $\mathbb{F}_q$ adding a root β of the polynomial $f(t) := t^2 - \alpha$, where α is not a square in $\mathbb{F}_q$. The other root is $-\beta$ and hence $\sigma(\beta) = -\beta$, i.e. $\beta^q = -\beta$. Thus $\mathbb{F}_{q^2} = \mathbb{F}_q + \mathbb{F}_q\beta$ as an $\mathbb{F}_q$-vector space. For any $z = x + y\beta \in \mathbb{F}_{q^2}$ with $x, y \in \mathbb{F}_q$ set $\Re z := x$ and $\Im z := y$. Since $\sigma(z) = x - \beta y$, we have $\Re z = (z + z^q)/2$ and $\Im z = (z - z^q)/2\beta$. For any $M \in M_{n,n}(\mathbb{F}_{q^2})$ set $M_+ := (M + M^\dagger)/2$ and $M_- := (M - M^\dagger)/2\beta$. We have $M_+^\dagger = M_+$. Since $\beta^q = -\beta$, we have $M_-^\dagger = M_-$. Hence $M = M_+ + \beta M_-$ with M_+ and M_- Hermitian matrices. For any $u \in \mathbb{F}_{q^2}^n$ we have $\langle u, Mu \rangle = \langle u, M_+ u \rangle + \beta \langle u, M_- u \rangle$ with $\langle u, M_+ u \rangle \in \mathbb{F}_q$ and