Filomat 37:14 (2023), 4573–4586
https://doi.org/10.2298/FIL2314573D

Published by Faculty of Sciences and Mathematics,
University of Niš, Serbia
Available at: http://www.pmf.ni.ac.rs/filomat

On invertible modules and generalized bilinear forms

David Dolžan[a,d], Damjana Kokol Bukovšek[b,d], Bojan Kuzma[c,d]

[a] *Faculty of Mathematics and Physics, University of Ljubljana, Slovenia*
[b] *School of Economics and Business, University of Ljubljana, Slovenia*
[c] *Faculty of Mathematics, Natural Sciences and Information Technologies, University of Primorska, Slovenia*
[d] *Institute of Mathematics, Physics and Mechanics, Ljubljana, Slovenia*

Abstract. We construct invertible modules (as invertible linear spaces of matrices with an additional structure) and find a bijective correspondence between nondegenerate generalized bilinear forms and the invertible modules.

1. Introduction

This paper is motivated by the problem of finding the diameter of the commuting graph of the algebra of prime-squared sized matrices over a finite field. Recall that the commuting graph of a general magma $\mathcal{A}$ (i.e., a nonempty set equipped with a possibly non-associative binary operation) is a simple graph whose vertices are all noncentral elements of $\mathcal{A}$ and where two distinct vertices a, b are connected if they commute in $\mathcal{A}$, i.e., if $ab = ba$. It was first introduced in [2] in an early attempt towards classification of simple finite groups.

Recently, the (diameters of) commuting graphs of the matrix algebra $M_n(\mathbb{F})$ of n-by-n matrices over a field $\mathbb{F}$ have been studied extensively, see for example [6, 7, 10]. One of the first results in this vein was that when $\mathbb{F}$ is algebraically closed and $n \geqslant 3$, the diameter of the commuting graph $\Gamma(M_n(\mathbb{F}))$ is equal to four, [1]. In general, the diameter of a connected graph is at most six, and it has been proved that there exists a field such that the diameter of the commuting graph $\Gamma(M_n(\mathbb{F}))$ is equal to six, [11]. If $\mathbb{F}$ is a finite field, then the diameter of $\Gamma(M_n(\mathbb{F}))$ is equal to four when $n \geqslant 4$ is even, $\Gamma(M_n(\mathbb{F}))$ is disconnected when n is a prime, and if n is neither a prime nor a square of a prime, the diameter is at most five, [5] (see also concluding remarks in [4]). So, the only open problem in the case of finite fields remains the diameter of the commuting graph of p^2-by-p^2 matrices for a prime p. It is known that the diameter in this case is at least five for sufficiently large fields, [4], and at most six, [1]. Similar arguments as in the proof of [5, Theorem 3.3] would imply that the diameter is equal to five if one could show that every generalized bilinear form induced by an invertible matrix (defined by (2)) is degenerate. We show that this is not the case (see Corollary 4.3). We do this by constructing a maximal linear space of invertible matrices of special kind (see Theorem 3.3

2020 *Mathematics Subject Classification*. 16D20; 15A63
Keywords. Matrix module, Generalized bilinear form, Commuting graph
Received: 18 July 2022; Accepted: 22 November 2022
Communicated by Dragana Cvetković Ilić
D. Dolžan and D. Kokol Bukovšek acknowledge financial support from the Slovenian Research Agency (research core funding No. P1-0222). B. Kuzma acknowledges financial support from the Slovenian Research Agency (research core funding No. P1-0285 and research project N1-0210).

Email addresses: david.dolzan@fmf.uni-lj.si (David Dolžan), damjana.kokol.bukovsek@ef.uni-lj.si (Damjana Kokol Bukovšek), bojan.kuzma@famnit.upr.si (Bojan Kuzma)

and Remark 3.5). So, this approach does not solve the diameter problem, however we strongly believe that it might be of an independent interest (see also Section 5). The problem will be solved in our subsequent paper, based on different techniques.

The paper is structured as follows. In Section 2, we define the notion of invertible modules (as invertible linear spaces of matrices with an additional structure) and define (nondegenerate) generalized bilinear forms. In Section 3, we construct the invertible modules under some mild assumptions (see Theorem 3.3). In Section 4, we show that the nondegenerate bilinear forms are in a bijective correspondence with the invertible modules (see Theorem 4.2). We illustrate these constructions with some examples. The final section gives additional remarks with a view towards possible applications.

2. Preliminaries

2.1. Matrix modules

Throughout, let $d \geqslant 2$ be an integer, let $n = d^2$, let $\mathbb{F}$ be a field, and let $C = C(m) \in M_d(\mathbb{F})$ be a companion matrix of an irreducible polynomial $m \in \mathbb{F}[x]$ of degree d. Recall that

$$\mathbb{K} := \mathbb{F}[C],$$

the unital $\mathbb{F}$-algebra generated by C, is a d-dimensional $\mathbb{F}$-linear subspace of $M_d(\mathbb{F})$ which, besides 0, consists of invertible matrices only. In fact, it is a subspace of maximal possible dimension with such property (see, e.g., [13, p. 44]). As such, $\mathbb{K} = \mathbb{F}[C]$ is also a field extension of $\mathbb{F}$, and $\mathcal{V} := M_d(\mathbb{F})$ is a natural left $\mathbb{K}$-module, with the action given by matrix multiplication $p(C) \cdot X \mapsto p(C)X$ where $p(C) \in \mathbb{F}[C] = \mathbb{K}$ and $X \in M_d(\mathbb{F})$. Clearly, $\dim_{\mathbb{K}}(\mathcal{V}) = d$. Observe that this action, when restricted to a subfield $\mathbb{F} \simeq \mathbb{F}I \subseteq \mathbb{K}$, is the multiplication with scalar matrices with coefficients from $\mathbb{F}$, so it coincides with the usual scalar multiplication on $M_d(\mathbb{F})$. In particular, each left $\mathbb{K}$-submodule of $\mathcal{V}$ is simultaneously an $\mathbb{F}$-linear subspace. Consequently, (again by [13, p. 44]) the only *invertible* left $\mathbb{K}$-submodules of $\mathcal{V}$, i.e., $\mathbb{K}$-submodules which, besides 0, consist of invertible d-by-d matrices only are $\mathbb{K}A = \mathbb{F}[C]A$ for some invertible $A \in M_d(\mathbb{F})$.

To get more interesting examples of invertible $\mathbb{K}$-submodules, a natural way is to extend the scalars and, instead of $M_d(\mathbb{F})$, consider a left $\mathbb{K}$-module $M_d(\mathbb{K})$ whose $\mathbb{K}$-dimension equals d^2. The action of the field $\mathbb{K}$ on $M_d(\mathbb{K})$ remains the same as before, i.e., left multiplication with the matrices from $\mathbb{K} = \mathbb{F}[C]$. For example, if $\mathbb{F} = \mathbb{R}$, the field of real numbers, and $C = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \in M_2(\mathbb{R})$, then $\mathbb{K} = \mathbb{F}[C]$ is isomorphic to the field $\mathbb{C}$ of complex numbers, with matrix C identified as an imaginary unit $\sqrt{-1}$. However, contrary to the usual scalar multiplication on $M_2(\mathbb{K}) = M_2(\mathbb{C})$, the action of $C \in \mathbb{K}$ on $X = \left(\begin{smallmatrix} x & y \\ u & v \end{smallmatrix}\right) \in M_2(\mathbb{C})$ is $CX = \left(\begin{smallmatrix} -u & -v \\ x & y \end{smallmatrix}\right)$ which differs from the usual $\sqrt{-1}X = \left(\begin{smallmatrix} \sqrt{-1}x & \sqrt{-1}y \\ \sqrt{-1}u & \sqrt{-1}v \end{smallmatrix}\right)$.

More precisely, under the identification $M_d(\mathbb{K}) = \mathbb{K} \otimes_{\mathbb{F}} M_d(\mathbb{F}) = \mathbb{F}[C] \otimes M_d(\mathbb{F})$ the $\mathbb{K}$-action on $\mathbb{F}[C] \otimes M_d(\mathbb{F})$ is a left multiplication by the elements from $I \otimes \mathbb{F}[C] \simeq \mathbb{K}$. We remark that this contrasts with the usual module structure obtained by extending the scalars, that is, a left multiplication on $M_d(\mathbb{K}) = \mathbb{F}[C] \otimes M_d(\mathbb{F})$ by the elements from $\mathbb{K} \simeq \mathbb{F}[C] \otimes I$.

The following question is immediate:

Question 2.1. *If $\mathbb{K} = \mathbb{F}[C]$, does $M_d(\mathbb{K})$ contain an invertible left submodule of dimension d over $\mathbb{K}$ (that is, a submodule, which besides 0 consists solely of invertible d-by-d matrices)?*

Remark 2.2. *Note that $M_d(\mathbb{K})$ does not contain invertible $\mathbb{K}$-submodules of dimension $d+1$. Namely, let $\mathcal{B} := \mathbb{K}A_1 + \cdots + \mathbb{K}A_{d+1} \subseteq M_d(\mathbb{K})$ be an invertible $\mathbb{K}$-submodule with $\dim_{\mathbb{K}} \mathcal{B} = d+1$. Clearly, $\mathcal{B}$ is also an $\mathbb{F}$-vector space with $\dim_{\mathbb{F}} \mathcal{B} = \dim_{\mathbb{K}} \mathcal{B} \cdot \dim_{\mathbb{F}} \mathbb{K} = (d+1)d$. However, due to $\mathbb{K} = \mathbb{F}[C]$ we can regard $M_d(\mathbb{K}) = M_d(\mathbb{F}[C])$ as d-by-d block matrices whose blocks belong to $\mathbb{F}[C] \subseteq M_d(\mathbb{F})$. That is, as a matrix $\mathbb{F}$-algebra, we have an embedding $M_d(\mathbb{K}) \subseteq M_{d^2}(\mathbb{F})$ and it is well-known that in the latter algebra the maximum possible dimension for invertible $\mathbb{F}$-subspace is $d^2 < (d+1)d$, a contradiction.*

2.2. Bilinear forms

Invertible $\mathbb{K}$-modules have an equivalent reformulation which is interesting in its own. To place it into a proper perspective, let us first introduce an operation of transforming column vectors with entries in $M_d(\mathbb{F})$ into row vectors, and vice versa, as follows: If $\mathbf{V} = \begin{pmatrix} V_1 \\ \vdots \\ V_d \end{pmatrix}$ is a block matrix from $M_{d^2\times d}(\mathbb{F})$ with blocks $V_i \in M_d(\mathbb{F})$, then we let

$$\mathbf{V}^* := \begin{pmatrix} V_1^T \\ \vdots \\ V_d^T \end{pmatrix}^T = (V_1, \ldots, V_d). \tag{1}$$

In particular, if each $V_i \in \mathbb{K} = \mathbb{F}[C] \subseteq M_d(\mathbb{F})$ then also each (block) entry in $\mathbf{V}^*$ belongs to $\mathbb{F}[C]$.

Now, recall that each matrix $A \in M_d(\mathbb{K})$ induces a bilinear form on $\mathbb{K}^d$, defined by $(x, y) \mapsto y^T Ax \in \mathbb{K}$; here, y^T denotes the transposition of a column vector $y \in \mathbb{K}^d$. Its zeros are pairs of vectors $(x, y) \in \mathbb{K}^d \times \mathbb{K}^d$ such that $y^T Ax = 0 \in \mathbb{K}$. We call zeros of the form $(0, y)$ and $(x, 0)$ trivial zeros of bilinear form. However, the bilinear form also has nontrivial zeros because for each x there exists a nonzero vector y which is perpendicular to Ax relative to pairing $(x, y) \mapsto y^T x$.

Recall that $\mathbb{K} = \mathbb{F}[C] \subseteq M_d(\mathbb{F})$, so instead of $A \in M_d(\mathbb{K}) \subseteq M_{d^2}(\mathbb{F})$ we can consider any matrix $S \in M_{d^2}(\mathbb{F})$ and induce a *generalized bilinear form* $\mathscr{B}_S$ on $\mathbb{K}^d = \mathbb{F}[C]^d \subseteq M_{n\times d}(\mathbb{F})$ given by

$$\mathscr{B}_S \colon (\mathbf{X}, \mathbf{Y}) \mapsto \mathbf{Y}^* S\mathbf{X}, \tag{2}$$

where $\mathbf{Y}^*$ was defined with (1). This clearly no longer lies in $\mathbb{K} = \mathbb{F}[C]$ in general but in $M_d(\mathbb{F})$. In fact, we may partition $\mathbf{X}, \mathbf{Y}, S$ into blocks of size d-by-d, so that $\mathbf{X} = (X_1, \ldots, X_d)^*$, $\mathbf{Y} = (Y_1, \ldots, Y_d)^*$, and $S = \left(S_{ij}\right)_{ij}$, with $X_i, Y_j \in \mathbb{F}[C] \subseteq M_d(\mathbb{F})$ and with $S_{ij} \in M_d(\mathbb{F})$. Wherefrom the generalized bilinear form equals

$$\mathscr{B}_S(\mathbf{X}, \mathbf{Y}) = \mathbf{Y}^* S\mathbf{X} = \sum_{i,j=1}^{d} Y_i S_{ij} X_j \in M_d(\mathbb{F}). \tag{3}$$

A generalized bilinear form $\mathscr{B}_S$ is called *nondegenerate* if $\mathscr{B}_S(\mathbf{X}, \mathbf{Y}) = 0$ implies $\mathbf{X} = 0$ or $\mathbf{Y} = 0$. One should remark that generalized bilinear forms do not always satisfy $\mathscr{B}_S(\mathbf{X}\Delta, \mathbf{Y}) = \mathscr{B}_S(\mathbf{X}, \mathbf{Y}\Delta)$, $\Delta \in \mathbb{K}$, so they may not be $\mathbb{K}$-bilinear.

Question 2.3. *Does there exist a matrix $S \in M_{d^2}(\mathbb{F})$ so that the generalized bilinear form $\mathscr{B}_S$, defined in* (3), *is nondegenerate?*

3. Invertible submodules

In the present section we give a partial answer to the Question 2.1. Namely, we show that the answer is positive in the case $d = 2$ and also in the case when $\mathbb{F} = \mathrm{GF}(p^r)$ is a finite field (see Proposition 3.1 and Corollary 3.6 below).

Proposition 3.1. *Let $\mathbb{F}$ be a field and $C(m) \in M_2(\mathbb{F})$ a companion matrix of an irreducible polynomial $m \in \mathbb{F}[x]$ of degree* 2. *Then, there exists a matrix $A \in M_2(\mathbb{K})$, where $\mathbb{K} = \mathbb{F}[C]$ such that $\mathbb{K} + \mathbb{K}A \subseteq M_2(\mathbb{K})$ is an invertible $\mathbb{K}$-module.*

Proof. It will be helpful to view $\mathbb{K}$ as a field and also as a subspace of 2-by-2 matrices over $\mathbb{F}$; to avoid misinterpretations, we will denote elements in $\mathbb{K}$ by Greek letters when considering $\mathbb{K}$ as a field and with capital letters when considering it as a subset in $M_2(\mathbb{F})$.

By Cayley-Hamilton, C is a zero of its minimal polynomial $m(x)$ and as such $\mathbb{K} = \mathbb{F}[C]$ is a splitting field for m, i.e., $m(x) = (x - \alpha)(x - \beta)$ for some $\alpha, \beta \in \mathbb{K}$. Hence, the matrix C is triangularizable in $M_2(\mathbb{K})$

(diagonalizable if m is separable). After a suitable conjugation we may assume C is in Jordan form. Define the matrix

$$A := \begin{pmatrix} 0 & \alpha \\ 1 & 0 \end{pmatrix} \in M_2(\mathbb{K})$$

which is clearly invertible. We need to prove that $p_0(C) + p_1(C)A \in M_2(\mathbb{K})$, $p_0, p_1 \in \mathbb{F}[x]$, is invertible whenever at least one of matrices $p_0(C)$ and $p_1(C)$ is nonzero.

It clearly suffices to assume that $p_0(C)$ is nonzero. There exists $p \in \mathbb{F}[x]$ such that $p(C) = p_0(C)^{-1}p_1(C) \in M_2(\mathbb{K})$. Now, if $C \in M_2(\mathbb{F}) \subseteq M_2(\mathbb{K})$ is diagonal then

$$I + p(C)A = \begin{pmatrix} 1 & p(\alpha)\alpha \\ p(\beta) & 1 \end{pmatrix}$$

whose determinant equals $1 - p(\alpha)p(\beta)\alpha$. Since minimal polynomial of C has degree two we may clearly assume that p is linear. Write it as $p(x) = a_0 + a_1x \in \mathbb{F}[x]$, then $p(\alpha)p(\beta) = a_0^2 + a_0a_1(\alpha + \beta) + a_1^2\alpha\beta$ which, by Vieta's rules, belongs to $\mathbb{F}$. In view of the fact that α is algebraic of order two, this implies that determinant is always nonzero.

It remains to consider the case when C is triangular, that is, when its minimal polynomial m is nonseparable. This can happen only if $\operatorname{char} \mathbb{F} = 2$. Then $C = \left(\begin{smallmatrix} \alpha & 1 \\ 0 & \alpha \end{smallmatrix}\right)$ and so

$$I + p(C)A = \begin{pmatrix} 1 + a_1 & \alpha p(\alpha) \\ p(\alpha) & 1 \end{pmatrix}$$

whose determinant is $1 + a_1 + \alpha p(\alpha)^2$. Since now $m(x) = (x - \alpha)^2 \in \mathbb{F}[x]$, we have $\alpha^2 \in \mathbb{F}$ so also $p(\alpha)^2 = a_0^2 + a_1^2\alpha^2 \in \mathbb{F}$. Again, it suffices to consider p linear so $p(\alpha) \neq 0$, hence $p(\alpha)^2 \in \mathbb{F}\backslash\{0\}$ and therefore $1 + a_1 + \alpha p(\alpha)^2 \neq 0$, that is, determinant of $I + p(C)A$ is always nonzero. □

Example 3.2. *We may apply the preceding proposition to $C := C(x^2 + 1) \in M_2(\mathbb{R})$; here $\mathbb{K} = \mathbb{R}[C] \simeq \mathbb{C}$. Consequently, there exists a matrix $A \in M_2(\mathbb{C})$ such that the space*

$$\mathbb{R}[C] + \mathbb{R}[C]A \tag{4}$$

is invertible. Observe that $\mathbb{R}[C] \simeq \mathbb{C}$, so (4) *is a two-dimensional invertible $\mathbb{C}$-module in $M_2(\mathbb{C})$. Note in contrast that, with the usual scalar multiplication, there exists no two-dimensional complex vector subspace in $M_2(\mathbb{C})$ which would, besides zero matrix, consist of invertible matrices only (this is an easy consequence of the fact that every complex matrix has an eigenvalue; see also [3, Proof of Statement IV p. 486]).*

Proposition 3.1 can be generalized to d-by-d matrices over suitable fields. This will be proven in our first main result.

Theorem 3.3. *Let $\mathbb{F}$ be a field, $d \geqslant 2$ an integer and $C = C(m) \in M_d(\mathbb{F})$ a companion matrix of an irreducible polynomial $m \in \mathbb{F}[x]$. Suppose that the field extension $\mathbb{K} = \mathbb{F}[C]$ is Galois over $\mathbb{F}$ with the corresponding Galois group cyclic. Then, there exist matrices $A_0 = I, A_1, A_2, \dots, A_{d-1} \in M_d(\mathbb{K})$ such that $\mathbb{K} + \mathbb{K}A_1 + \cdots + \mathbb{K}A_{d-1}$ is an invertible $\mathbb{K}$-module.*

Proof. Recall that since $\mathbb{K}$ is Galois over $\mathbb{F}$, the polynomial m is separable, so it has d distinct roots in $\mathbb{K}$. Moreover, if ϕ is a generator of Galois group $\operatorname{Gal}(\mathbb{K}|\mathbb{F})$, then ϕ has degree d and cyclically permutes zeros of m. As such, if $m(\alpha) = 0$ then $\alpha, \phi(\alpha), \dots, \phi^{d-1}(\alpha) \in \mathbb{K}$ are all the zeros of m so that

$$m(x) = (x - \alpha)(x - \phi(\alpha))(x - \phi^2(\alpha)) \cdots (x - \phi^{d-1}(\alpha)) \in \mathbb{K}[x].$$

It follows that $C = C(m)$ is diagonalizable over $\mathbb{K}$ and we may clearly assume it is already diagonal. Thus,

$$p(C) = \operatorname{diag}(p(\alpha), p(\phi(\alpha)), \dots, p(\phi^{d-1}(\alpha))); \qquad p \in \mathbb{F}[x]. \tag{5}$$

Define

$$A_1 := \sum_{1\leqslant i<j\leqslant d} (E_{ji} + \alpha E_{ij}) = \begin{pmatrix} 0 & \alpha & \cdots & \cdots & \alpha \\ 1 & 0 & \alpha & \cdots & \alpha \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 1 & \cdots & 1 & 0 & \alpha \\ 1 & \cdots & \cdots & 1 & 0 \end{pmatrix}$$

and for $k = 2, 3, \dots, (d-1)$ define

$$A_k = A_1 + \alpha \sum_{i=1}^{d-k} \left(\phi^{i-1}(\alpha) - 1\right) E_{i\,(i+k)} + \sum_{i=1}^{k} \left(\phi^{d-k-1+i}(\alpha) - 1\right) E_{(d-k+i)\,i}$$

that is, A_k is obtained from A_1 by replacing k-th superdiagonal with

$$\alpha\left(\alpha, \phi(\alpha), \phi^2(\alpha), \dots, \phi^{d-k-1}(\alpha)\right)$$

and replacing $(d-k)$-th subdiagonal with

$$\left(\phi^{d-k}(\alpha), \phi^{d-k+1}(\alpha), \dots, \phi^{d-1}(\alpha)\right).$$

For example, with $d = 5$ we have

$$A_1 = \begin{pmatrix} 0 & \alpha & \alpha & \alpha & \alpha \\ 1 & 0 & \alpha & \alpha & \alpha \\ 1 & 1 & 0 & \alpha & \alpha \\ 1 & 1 & 1 & 0 & \alpha \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 0 & \alpha & \alpha^2 & \alpha & \alpha \\ 1 & 0 & \alpha & \alpha\phi(\alpha) & \alpha \\ 1 & 1 & 0 & \alpha & \alpha\phi^2(\alpha) \\ \phi^3(\alpha) & 1 & 1 & 0 & \alpha \\ 1 & \phi^4(\alpha) & 1 & 1 & 0 \end{pmatrix},$$

$$A_3 = \begin{pmatrix} 0 & \alpha & \alpha & \alpha^2 & \alpha \\ 1 & 0 & \alpha & \alpha & \alpha\phi(\alpha) \\ \phi^2(\alpha) & 1 & 0 & \alpha & \alpha \\ 1 & \phi^3(\alpha) & 1 & 0 & \alpha \\ 1 & 1 & \phi^4(\alpha) & 1 & 0 \end{pmatrix}, \quad A_4 = \begin{pmatrix} 0 & \alpha & \alpha & \alpha & \alpha^2 \\ \phi(\alpha) & 0 & \alpha & \alpha & \alpha \\ 1 & \phi^2(\alpha) & 0 & \alpha & \alpha \\ 1 & 1 & \phi^3(\alpha) & 0 & \alpha \\ 1 & 1 & 1 & \phi^4(\alpha) & 0 \end{pmatrix}$$

Observe that, with nonzero $p_0(C) \in \mathbb{F}[C]$, we have that the matrix $p_0(C) + p_1(C)A_1 + \cdots + p_{d-1}(C)A_{d-1}$ is invertible if and only if $I + \hat{p}_1(C)A_1 + \cdots + \hat{p}_{d-1}(C)A_{d-1}$ is invertible, where $\hat{p}_i(C) = p_0(C)^{-1}p_i(C) \in \mathbb{F}[C]$. Hence, to prove that $\mathbb{K}$-module $\mathbb{F}[C] + \mathbb{F}[C]A_1 + \cdots + \mathbb{F}[C]A_{d-1}$ is invertible, it suffices to show that, with $\varepsilon \in \{0, 1\}$ and $p_1, \dots, p_{d-1} \in \mathbb{F}[x]$, we have

$$\det\left(\varepsilon I + p_1(C)A_1 + \cdots + p_{d-1}(C)A_{d-1}\right)$$

is zero if and only if $\varepsilon = 0$ and $p_1(C) = \cdots = p_{d-1}(C) = 0$. After a straightforward calculation,

$$\begin{aligned} T_\varepsilon :&= \varepsilon I + p_1(C)A_1 + \cdots + p_{d-1}(C)A_{d-1} \\ &= \varepsilon I + \sum_{i<j} \alpha\phi^{i-1}(b_{j-i})\, E_{ij} + \sum_{i>j} \phi^{j-1}(b_{d-(j-i)})\, E_{ij} \\ &= \varepsilon I + \begin{pmatrix} 0 & \alpha b_1 & \cdots & \alpha b_{d-2} & \alpha b_{d-1} \\ \phi(b_{d-1}) & 0 & \alpha\phi(b_1) & \cdots & \alpha\phi(b_{d-2}) \\ \vdots & & \ddots & & \vdots \\ \phi^{d-2}(b_2) & \cdots & \phi^{d-2}(b_{d-1}) & 0 & \alpha\phi^{d-2}(b_1) \\ \phi^{d-1}(b_1) & \phi^{d-1}(b_2) & \cdots & \phi^{d-1}(b_{d-1}) & 0 \end{pmatrix} \end{aligned}$$

where

$$b_1 = \sum_{i=1}^{d-1} p_i(\alpha), \quad b_2 = (\alpha - 1)p_2(\alpha) + b_1, \quad \dots, \quad b_{d-1} = (\alpha - 1)p_{d-1}(\alpha) + b_1.$$

Now, let again x be an indeterminate over $\mathbb{K}$ and consider two matrix polynomials, obtained by formally replacing each explicit occurrence of α by x in the matrix T_ε:

$$F_\varepsilon(x) = \varepsilon I + \begin{pmatrix} 0 & xb_1 & \cdots & \cdots & xb_{d-1} \\ \phi(b_{d-1}) & 0 & x\phi(b_1) & \cdots & x\phi(b_{d-2}) \\ \vdots & & \ddots & & \vdots \\ \phi^{d-2}(b_2) & \cdots & \phi^{d-2}(b_{d-1}) & 0 & x\phi^{d-2}(b_1) \\ \phi^{d-1}(b_1) & \cdots & \cdots & \phi^{d-1}(b_{d-1}) & 0 \end{pmatrix}; \quad \varepsilon \in \{0,1\}.$$

In particular, $T_\varepsilon = F_\varepsilon(\alpha)$. Let us further introduce two polynomials

$$f_\varepsilon(x) := \det F_\varepsilon(x); \qquad \varepsilon \in \{0,1\}. \tag{6}$$

Clearly, f_ε are polynomials of degree at most $d-1$ because indeterminate x is present in F_ε only above the main diagonal and the entries of F_ε are linear in x. We claim that

$$\phi\big(f_\varepsilon(\gamma)\big) = \det \phi(F_\varepsilon(\gamma)) = f_\varepsilon\big(\phi(\gamma)\big); \qquad \gamma \in \mathbb{K}\backslash\{0\}. \tag{7}$$

The first equality in (7) is evident. To prove the second one, note that whatever the value of $\varepsilon \in \{0,1\}$, it is fixed by ϕ. Hence,

$$\phi(F_\varepsilon(\gamma)) = \varepsilon I + \begin{pmatrix} 0 & \phi(\gamma)\phi(b_1) & \cdots & \cdots & \phi(\gamma)\phi(b_{d-1}) \\ \phi^2(b_{d-1}) & 0 & \phi(\gamma)\phi^2(b_1) & \cdots & \phi(\gamma)\phi^2(b_{d-2}) \\ \vdots & & \ddots & & \vdots \\ \phi^{d-1}(b_2) & \cdots & \phi^{d-1}(b_{d-1}) & 0 & \phi(\gamma)\phi^{d-1}(b_1) \\ \phi^d(b_1) & \cdots & \cdots & \phi^d(b_{d-1}) & 0 \end{pmatrix}$$

Recall that ϕ^d is the identity map. Thus, if we cyclically permute the rows and then the columns of $\phi(F_\varepsilon(\gamma))$ by permutation $(1,2,\dots,d)$ then we end up with the matrix

$$\widehat{F}_\varepsilon = \varepsilon I + \begin{pmatrix} 0 & b_1 & \cdots & \cdots & b_{d-1} \\ \phi(\gamma)\phi(b_{d-1}) & 0 & \phi(\gamma)\phi(b_1) & \cdots & \phi(\gamma)\phi(b_{d-2}) \\ \vdots & \phi^2(b_{d-1}) & 0 & \cdots & \phi(\gamma)\phi^2(b_{d-3}) \\ \vdots & \vdots & & & \vdots \\ \phi(\gamma)\phi^{d-2}(b_2) & \phi^{d-2}(b_3) & \cdots & 0 & \phi(\gamma)\phi^{d-2}(b_1) \\ \phi(\gamma)\phi^{d-1}(b_1) & \phi^{d-1}(b_2) & \cdots & \phi^{d-1}(b_{d-1}) & 0 \end{pmatrix}$$

which has the same determinant as $\phi\big(F_\varepsilon(\gamma)\big)$. Observe that it is also the same matrix as $F_\varepsilon(\phi(\gamma))$ except that the first row of $F_\varepsilon(\phi(\gamma))$ is divided by $\widehat{F}_\varepsilon$ will not change if we divide its first column by $\phi(\gamma)$ and afterwards multiply its first row by $\phi(\gamma)$. This procedure produces the matrix

$$\varepsilon I + \begin{pmatrix} 0 & \phi(\gamma)b_1 & \cdots & \cdots & \phi(\gamma)b_{d-1} \\ \phi(b_{d-1}) & 0 & \phi(\gamma)\phi(b_1) & \cdots & \phi(\gamma)\phi(b_{d-2}) \\ \vdots & & \ddots & & \vdots \\ \phi^{d-2}(b_2) & \cdots & \phi^{d-2}(b_{d-1}) & 0 & \phi(\gamma)\phi^{d-2}(b_1) \\ \phi^{d-1}(b_1) & \cdots & \cdots & \phi^{d-1}(b_{d-1}) & 0 \end{pmatrix}$$

which clearly equals $F_\varepsilon\big(\phi(\gamma)\big)$. Hence, $\det \phi\big(F_\varepsilon(\gamma)\big) = \det F_\varepsilon\big(\phi(\gamma)\big)$, as claimed by the second equality in (7).

Now, assume

$$\det T_\varepsilon = 0$$

and recall that

$$\det T_\varepsilon = f_\varepsilon(\alpha).$$

By (7) then also $\phi\big(\det T_\varepsilon\big) = f_\varepsilon\big(\phi(\alpha)\big) = 0$. Proceeding inductively we derive

$$f_\varepsilon(\alpha) = f_\varepsilon(\phi(\alpha)) = \cdots = f_\varepsilon(\phi^{d-1}(\alpha)) = 0.$$

Thus, $\alpha, \phi(\alpha), \dots, \phi^{d-1}(\alpha)$ are d distinct zeros of f_ε (distinct because they are exactly all the zeros of polynomial m). Since the degree of f_ε is smaller than d, we have $f_\varepsilon = 0$. In particular, the leading coefficient of monomial x^{d-1} of f_ε vanishes:

$$b_1\phi(b_1)\cdots\phi^{d-1}(b_1) = 0$$

hence $b_1 = 0$. Also, the coefficient of monomial x^{d-2}, which equals to $b_2\phi(b_2)\cdots\phi^{d-1}(b_2)$, vanishes and so $b_2 = 0$. Proceeding inductively, we see that if $b_1 = b_2 = \cdots = b_i = 0$ then the coefficient of monomial of x^{d-i-1} equals

$$b_{i+1}\phi(b_{i+1})\cdots\phi^{d-1}(b_{i+1}) = 0.$$

Thus, by induction,

$$b_1 = b_2 = \cdots = b_{d-1} = 0 \tag{8}$$

As such, $T_\varepsilon = \varepsilon I$ and since its determinant vanishes, $\varepsilon = 0$. Moreover, it follows by definition of $b_1, \dots, b_{d-1}$ that $p_i(\alpha)$ are all zero. As such, also $p_i(C) = 0$. Hence, $T_\varepsilon \in \mathbb{F}[C] + \mathbb{F}[C]A_1 + \cdots + \mathbb{F}[C]A_{d-1}$ is singular if and only if it is a zero matrix. □

Remark 3.4. *Observe that Proposition 3.1 follows directly from Theorem 3.3 in the case $\mathbb{K}$ is a separable extension of $\mathbb{F}$ because a separable extension of degree two is always normal, hence Galois with a cyclic Galois group.*

Remark 3.5. *Note that we may view $M_d(\mathbb{K})$ as block matrices with d-by-d blocks from the field $\mathbb{K} = \mathbb{F}[C]$. Then, each invertible $\mathbb{K}$-module (with $\mathbb{K}$-dimension equal to t) is an $\mathbb{F}$-linear subspace of $M_{d^2}(\mathbb{F})$ (whose $\mathbb{F}$-dimension equals td), where every nonzero matrix is invertible.*

We can now give a positive answer to Question 2.1 in the case of finite fields.

Corollary 3.6. *Let $\mathbb{F} = \mathrm{GF}(p^r)$ be a finite field, $d \geqslant 2$ an integer, $C \in M_d(\mathbb{F})$ a companion matrix of some irreducible polynomial $m \in \mathbb{F}[x]$ and $\mathbb{K} = \mathbb{F}[C]$. Then, there exist matrices $A_0 = I, A_1, A_2, \dots, A_{d-1} \in M_d(\mathbb{K})$ such that $\mathbb{K} + \mathbb{K}A_1 + \cdots + \mathbb{K}A_{d-1}$ is an invertible $\mathbb{K}$-module.*

Proof. Clearly, $\mathbb{K}$ is a finite field. By [8, Corollary p. 96] it is a Galois extension of $\mathbb{F}$. It is well known (see e.g. [8, Theorem 3.11]) that within finite fields, the Galois group of field extension is always cyclic, and hence also $\mathrm{Gal}(\mathbb{K}|\mathbb{F})$ is cyclic. □

If the $\mathbb{K}$-module is generated by the d-by-d matrices with entries from the original field $\mathbb{F}$ instead of its field extension $\mathbb{K} = \mathbb{F}[C]$, the result is completely different – we had already mentioned in Section 2 that the only invertible $\mathbb{K}$-submodules of $M_d(\mathbb{F})$ are $\mathbb{K}A$ with $A \in M_d(\mathbb{F})$ invertible. We strengthen this in our next lemma.

Recall that $M_d(\mathbb{F})$ is a left $\mathbb{K} = \mathbb{F}[C]$-module under the standard multiplication of matrices. Each its $\mathbb{K}$-submodule takes the form $\mathbb{F}[C]B_1 + \cdots + \mathbb{F}[C]B_k$ for suitably chosen matrices $B_1, \dots, B_k \in M_d(\mathbb{F})$.

Lemma 3.7. *Let $k \leqslant d$ be an integer and let $\mathcal{B} \subseteq M_d(\mathbb{F})$ be a left $\mathbb{K}$-submodule of dimension $\dim_{\mathbb{K}} \mathcal{B} = k$. Then there exists a submodule $\mathcal{B}_0 \leqslant \mathcal{B}$ of dimension $\dim_{\mathbb{K}} \mathcal{B}_0 = k-1$ such that $0 \neq \bigcap_{A\in\mathcal{B}_0} \operatorname{Ker} A$.*

Proof. Observe that if $0 \neq X_i \in \mathbb{K} = \mathbb{F}[C]$ then X_iE_{ii} is nonzero only in i-th column (it equals the i-th column of invertible X_i). This shows that the matrices $E_{11}, \dots, E_{dd} \in M_d(\mathbb{F})$ are $\mathbb{K}$-linearly independent.

Now, if $k = d$ then $\mathcal{B} = M_d(\mathbb{F}) = \mathbb{F}[C]E_{11} + \cdots + \mathbb{F}[C]E_{dd}$. Then, $\mathcal{E} := \mathbb{F}[C]E_{11} + \cdots + \mathbb{F}[C]E_{(d-1)\,(d-1)}$ is a $(d-1)$-dimensional left $\mathbb{K}$ submodule of $M_d(\mathbb{F})$ with a common kernel spanned by e_d, the last vector of the standard basis in $\mathbb{F}^d$.

Assume $2 \leqslant k \leqslant d-1$. Then, due to $\operatorname{codim}_{\mathbb{K}} \mathcal{B} \cap \mathcal{E} \leqslant \operatorname{codim}_{\mathbb{K}} \mathcal{B} + \operatorname{codim}_{\mathbb{K}} \mathcal{E} = (d-k)+1$, so $\mathcal{B}_0 := \mathcal{B} \cap \mathcal{E}$ satisfies the claim. □

Remark 3.8. *Lemma does not hold if* $\dim_{\mathbb{K}} \mathcal{B}_0 = k-1$ *is replaced by* $\dim_{\mathbb{K}} \mathcal{B}_0 = k$. *Namely, if* $\mathcal{B}$ *contains an invertible matrix,* $\mathcal{B}_0$ *cannot be equal to* $\mathcal{B}$.

4. Generalized bilinear forms

In this section, we show that Question 2.3 is closely related to Question 2.1 (see Theorem 4.2 below). We start with a lemma which proves that a nondegenerate generalized bilinear form is induced by an invertible matrix.

Lemma 4.1. *Let* $\mathbb{F}$ *be a field,* $d \geqslant 2$ *an integer and* $C = C(m) \in M_d(\mathbb{F})$ *a companion matrix of an irreducible polynomial* $m \in \mathbb{F}[x]$. *Denote by* $\mathbb{K} = \mathbb{F}[C]$ *and* $n = d^2$. *Assume that a generalized bilinear form* $\mathcal{B}_S \colon \mathbb{K}^d \times \mathbb{K}^d \to M_d(\mathbb{F})$ *induced by a matrix* $S \in M_n(\mathbb{F})$ *is nondegenerate. Then,* S *is invertible.*

Proof. To prove the claim, we argue by contradiction. So, suppose that S is singular and let $x \in \mathbb{F}^n$ be a nonzero column vector annihilated by S. Then, the n-by-d matrix Ξ, defined by d column vectors as

$$\Xi := \big(x \,|\, \hat{C}x \,|\, \hat{C}^2 x \,|\, \ldots \,|\, \hat{C}^{d-1}x\big),$$

where $\hat{C} := \bigoplus_1^d C$, belongs to $\mathbb{K}^d \subseteq M_{n\times d}(\mathbb{F})$. Indeed, vectors in $\mathbb{K}^n$ are of the form $(p_1(C), \ldots, p_d(C))^*$ for some polynomials p_i. Observe that C is in its rational form and so $Ce_i = e_{i+1}$ for $i < n$ and $Ce_n = \sum_i c_{in} e_i$. Now, decompose $x = x_1 \oplus \cdots \oplus x_d$ and note that the algebra $\mathbb{K} = \mathbb{F}[C]$ acts transitively on $M_d(\mathbb{F})$, so there exists polynomials $p_1, \ldots, p_d$ over $\mathbb{F}$ with $p_i(C)e_1 = x_i$. Thus, the first column of the n-by-d matrix $\mathbf{X} = (p_1(C), \ldots, p_d(C))^*$ equals $(p_1(C) \oplus \cdots \oplus p_d(C))(e_1 \oplus \cdots \oplus e_1) = x_1 \oplus \cdots \oplus x_d = x$, which coincides with the first column of Ξ. The second column of $\mathbf{X}$ equals $(p_1(C) \oplus \cdots \oplus p_d(C))(e_2 \oplus \cdots \oplus e_2) = (p_1(C) \oplus \cdots \oplus p_d(C))\hat{C}(e_1 \oplus \cdots \oplus e_1) = \hat{C}(p_1(C) \oplus \cdots \oplus p_d(C))\hat{C}(e_1 \oplus \cdots \oplus e_1) = \hat{C}x$. Similarly, we show for all other columns of $\mathbf{X}$, so $\mathbf{X} = \Xi$ as claimed.

Hence, $\operatorname{rank}(S\Xi) \leqslant d-1$ because the first column of $S\Xi$ is zero. By [12] there exists an invertible (symmetric) matrix $Z \in M_d(\mathbb{F})$ such that

$$C = Z^{-1}C^T Z.$$

Define $\hat{Z} := \bigoplus_1^d Z$ and denote by

$$\mathcal{V} := \{\hat{Z}S\hat{C}x, \ldots, \hat{Z}S\hat{C}^{d-1}x\}^{\perp} \tag{9}$$

the vector subspace in $\mathbb{F}^n$ of codimension $\operatorname{codim}\mathcal{V} \leqslant d-1$; the orthogonal complement in (9) is relative to the standard nondegenerate bilinear form $(x, y) \mapsto x^T y \in \mathbb{F}$ on $\mathbb{F}^n \times \mathbb{F}^n$. By bijectivity of $\hat{C}$, we have that $\operatorname{codim}\hat{C}^i\mathcal{V} = \operatorname{codim}\mathcal{V}$ for every $i = 1, 2, \ldots, d-1$. Let

$$\mathcal{W} := \mathcal{V} \cap \hat{C}\mathcal{V} \cap \cdots \cap \hat{C}^{d-1}\mathcal{V}.$$

We have $\operatorname{codim}\mathcal{W} \leqslant d(d-1) < d^2$, and thus $\mathcal{W}$ is nonempty. Choose nonzero $w \in \mathcal{W}$. Since $w \in \hat{C}^{d-1}\mathcal{V}$, there exists $v \in \mathcal{V}$ so that $w = \hat{C}^{d-1}v$. Similarly, since $w \in \hat{C}^i\mathcal{V}$ for each $i = 0, \ldots, d-2$, there exists $v_i \in \mathcal{V}$ so that $w = \hat{C}^i v_i$. Since $\hat{C}$ is invertible, we get that $\hat{C}^j v = v_{d-1-j} \in \mathcal{V}$ for every $j = 1, \ldots, d-1$.

Let us form an n-by-d matrix $\mathbf{X} := \big(v \,|\, \hat{C}v \,|\, \ldots \,|\, \hat{C}^{d-1}v\big)$. The equation (9) then implies that $\mathbf{X}^T\hat{Z}S\Xi = 0$, so also

$$Z^{-1}\mathbf{X}^T\hat{Z} \cdot S\Xi = 0.$$

Clearly, $\mathbf{X}$ is nonzero and belongs to $\mathbb{K}^d$. As such, its transpose takes the form

$$\mathbf{X}^T = \big(p_1(C)^T, \ldots, p_d(C)^T\big)$$

for some polynomials $p_i \in \mathbb{F}[\lambda]$. Observe that

$$\begin{aligned} Z^{-1}\mathbf{X}^T\hat{Z} &= \big(Z^{-1}p_1(C)^T Z, \ldots, Z^{-1}p_d(C)^T Z\big) = \big(p_1(Z^{-1}C^T Z), \ldots, p_d(Z^{-1}C^T Z)\big) \\ &= \big(p_1(C), \ldots, p_d(C)\big) \end{aligned}$$

that is, $\mathbf{\Lambda} := (Z^{-1}\mathbf{X}^T\hat{Z})^*$ belongs to $\mathbb{K}^d$ and satisfies $\mathbf{\Lambda}^* S\Xi = 0$, and so $(\mathbf{\Lambda}, \Xi)$ is a nontrivial zero of generalized bilinear form induced by S, a contradiction. □

Recall from [3] that classical d-dimensional invertible vector subspaces in $M_d(\mathbb{F})$ are in one-to-one, onto correspondence with (possibly non-associative) division algebras on $\mathbb{F}^d$: given such an invertible subspace with basis $V_1, \ldots, V_d$, it induces the bilinear product on $\mathbb{F}^d \simeq \mathrm{Lin}_{\mathbb{F}}\{V_1, \ldots, V_d\}$ by letting $V_i \star V_j := \sum_k v_{kj}^{(i)} V_k$ where $V_i = \big(v_{kj}^{(i)}\big)_{kj}$. Observe firstly that this product indeed yields a division algebra: choose any non-zero $V = \sum_i \alpha_i V_i$ and assume that $V \star (\sum_j \beta_j V_j) = 0$. If we denote $V = \big(v_{kj}\big)_{kj}$, this gives us $\sum_j \beta_j v_{kj} = 0$ for every $k = 1, \ldots, d$, so $V \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_d \end{pmatrix} = 0$, and thus $\beta_1 = \ldots = \beta_d = 0$ since V is invertible. Conversely, given a (non-associative) division algebra of $\mathbb{F}^d$ with basis $\{a_1, \ldots, a_d\}$, we get an invertible vector subspace in $M_d(\mathbb{F})$ by constructing its basis $\{V_1, \ldots, V_d\}$, where for each $j = 1, \ldots, d$, V_j is the matrix corresponding to the left multiplication with a_j. It can be easily checked that this is indeed an invertible vector subspace, and also that the above two mappings are mutually inverse.

Similarly, we show that the generalized bilinear forms are in one-to-one, onto correspondence with invertible $\mathbb{K}$-modules.

Theorem 4.2. *Let $\mathbb{F}$ be a field, $d \geqslant 2$, and let $C = C(m) \in M_d(\mathbb{F})$ be a companion matrix of some irreducible polynomial $m \in \mathbb{F}[x]$; define $\mathbb{K} = \mathbb{F}[C]$. There exists a bijective correspondence between bases for invertible $\mathbb{K}$-sobmudules in $M_d(\mathbb{F})$ and generalized bilinear forms* (3) *which are nondegenerate.*

Proof. Let $\mathbb{F}[C]A_1 + \cdots + \mathbb{F}[C]A_d$ be an invertible $\mathbb{K}$-module spanned by $A_1, \ldots, A_d \in M_d(\mathbb{K})$. It will be essential to regard A_i as a d-by-d block matrix with entries from the field $\mathbb{K} = \mathbb{F}[C] \subseteq M_d(\mathbb{F})$. To avoid misinterpretations, we will denote elements from $\mathbb{K}$ as well as matrices from $M_d(\mathbb{K})$ and their entries in boldface:

$$\mathbf{A}_k := A_k = (\boldsymbol{\alpha}_{ij}^{(k)})_{ij}; \qquad \boldsymbol{\alpha}_{ij}^{(k)} \in \mathbb{F}[C] \subseteq M_d(\mathbb{F}).$$

Recall that $M_d(\mathbb{F})$ is a left $\mathbb{K}$-module of dimension d (this follows from $d^2 = \dim_{\mathbb{F}} M_d(\mathbb{F}) = (\dim_{\mathbb{F}} \mathbb{K}) \cdot (\dim_{\mathbb{K}} M_n(\mathbb{F}))$). Let $B_1, \ldots, B_d \in M_d(\mathbb{F})$ be its basis. Hence, by the action of $\mathbb{K} = \mathbb{F}[C]$ on $M_d(\mathbb{F})$,

$$M_d(\mathbb{F}) = \mathbb{F}[C]B_1 + \cdots + \mathbb{F}[C]B_d.$$

Now, a matrix $C \in \mathbb{F}[C] \subseteq M_d(\mathbb{F})$ induces a $\mathbb{K}$-linear mapping on $M_d(\mathbb{F})$ by $X \mapsto XC$. Relative to the basis $B_1, \ldots, B_d$, this mapping is represented by a matrix $\mathbf{T}_C \in M_d(\mathbb{K})$. Since the transformation $p(C) \mapsto \mathbf{T}_{p(C)}$ is a linear antiisomorphism of $\mathbb{F}[C]$ into $M_d(\mathbb{K})$, the minimal polynomial for $\mathbf{T}_C$ is the same as for C. It follows that the rational form of $\mathbf{T}_C$ is the same as for C, so there exists a change of basis in the left $\mathbb{K}$-module $M_d(\mathbb{F})$, relative to which

$$\mathbf{T}_{p(C)} = p(C); \qquad p \in \mathbb{F}[x]. \tag{10}$$

We can clearly assume that $B_1, \ldots, B_d$ were already chosen in such a way (c.f. Example 4.4 below for a specific construction).

Let us define d-by-d matrices $S_{ij} \in M_d(\mathbb{F})$ by

$$S_{ij} = \sum_{k=1}^{d} \boldsymbol{\alpha}_{ki}^{(j)} B_k, \tag{11}$$

so that S_{ij} equals the scalar product of i-th column of the matrix $\boldsymbol{A}_j$ with the left $\mathbb{K}$-basis $B_1, \ldots B_d$ of $M_d(\mathbb{F})$. Let

$$S = \big(S_{ij}\big)_{ij} \in M_{d^2}(\mathbb{F}).$$

Given vectors $\mathbf{X} = \begin{pmatrix} p_1(C) \\ \vdots \\ p_d(C) \end{pmatrix} \in \mathbb{K}^d$ and $\mathbf{Y} = \begin{pmatrix} q_1(C) \\ \vdots \\ q_d(C) \end{pmatrix} \in \mathbb{K}^d$, we then have

$$\mathbf{Y}^* S\mathbf{X} = \sum_{i,j=1}^{d} q_i(C) S_{ij} p_j(C) \in M_d(\mathbb{F}).$$

Denote $\lambda_i := q_i(C) \in \mathbb{K}$. Hence, with j kept fixed, the summands can be rewritten as $\sum_i q_i(C)S_{ij}p_j(C) = \sum_i \lambda_i S_{ij} p_j(C) = \sum_i \lambda_i \sum_{k=1}^{d} \alpha_{ki}^{(j)} B_k p_j(C)$. Recall that, relative to $\mathbb{K}$-basis $B_1, \dots, B_k$, one has $B_k p_j(C) = \mathbf{T}_{p_j(C)} \mathbf{e}_k$, where $\mathbf{e}_k \in \mathbb{K}^d$ is a column vector with 1 at k-th entry and zeros elsewhere ($\mathbf{e}_k$ represents B_k). By (10), the matrix $\mathbf{T}_{p_j(C)}$ coincides with the matrix $p_j(C) \in M_d(\mathbb{F}) \subseteq M_d(\mathbb{K})$, so

$$\begin{aligned} \sum_i q_i(C) S_{ij} p_j(C) &= \sum_i \lambda_i \sum_{k=1}^{d} \alpha_{ki}^{(j)} p_j(C) \mathbf{e}_k = p_j(C) \sum_i \lambda_i \sum_{k=1}^{d} \alpha_{ki}^{(j)} \mathbf{e}_k \\ &= p_j(C) \mathbf{A}_j \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_d \end{pmatrix} \end{aligned}$$

and so

$$\mathbf{Y}^* S\mathbf{X} = \sum_{i,j=1}^{d} q_i(C) S_{ij} p_j(C) = \left(\sum_{j=1}^{d} p_j(C) \mathbf{A}_j \right) \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_d \end{pmatrix}. \tag{12}$$

Now, by the assumptions, $p_1(C)\mathbf{A}_1 + \cdots + p_d(C)\mathbf{A}_d \in M_d(\mathbb{K})$ is nonsingular whenever at least one among $p_i(C) \in \mathbb{F}[C]$ is nonzero. Consequently, the generalized bilinear form (12) is nondegenerate.

Observe that, in the definition (11) of S, two different $\mathbf{A}_j$ will yield two different j-th columns of S. Hence the correspondence is one-to-one. Let us show it is also onto. If S induces a nondegenerate bilinear form, then the members of its j-th block column are linearly independent in the left $\mathbb{K}$-module $M_d(\mathbb{F})$, hence form its $\mathbb{K}$-basis. We define $\mathbf{A}_j$ to be the transition matrix between this basis and the basis $(B_1, \dots, B_d)$ so that $\mathbf{A}_j^* \begin{pmatrix} B_1 \\ \vdots \\ B_d \end{pmatrix}$ equals j-th block column of S. So we can repeat the previous arguments to derive (12) by which the transition matrices $\mathbf{A}_1, \dots, \mathbf{A}_d$ generate invertible $\mathbb{K}$-module (since S is nondegenerate). □

Corollary 4.3. *Let $\mathbb{F} = \mathrm{GF}(p^r)$ be a finite field, $d \geqslant 2$ an integer, $C \in M_d(\mathbb{F})$ a companion matrix of some irreducible polynomial $m \in \mathbb{F}[x]$ and $\mathbb{K} = \mathbb{F}[C]$. Then there exists a matrix $S \in M_{d^2}(\mathbb{F})$ so that the generalized bilinear form $\mathcal{B}_S$ is nondegenerate.*

Proof. The claim follows directly from Corollary 3.6 and Theorem 4.2. □

Example 4.4. *To compute a matrix S inside Theorem 4.2 one needs to choose a $\mathbb{K}$-basis $B_1, \dots, B_d \in M_d(\mathbb{F})$ with respect to which the linear map $X \mapsto XC$ is again represented by the matrix C. One possibility is to define*

$$B_i := E_{11} C^{i-1}.$$

Since C is already in its rational form and its minimal polynomial has a nonzero constant term λ_0, we see that $B_1 = E_{11}$ and $B_i = -\lambda_0 E_{(2+d-i)\,1} + \sum_{k>2+d-1} *E_{k1}$, $(i = 2, \dots, d)$ for appropriate scalars $* \in \mathbb{F}$. Clearly then, $B_1, \dots, B_d$ is a desired basis for left $\mathbb{K}$-module $M_d(\mathbb{F})$. Namely, assume

$$\sum_k T^{(k)} B_k = 0 \in M_d(\mathbb{K}) \tag{13}$$

for some $T^{(k)} \in \mathbb{K} = \mathbb{F}[C] \subseteq M_d(\mathbb{F})$. Note that the matrix $TB_1 = TE_{11}$ can be nonzero only in the first column, while TB_i vanishes in the first column for $i \geqslant 2$. In view of (13) *this implies that $T^{(1)}B_1 = 0$ and as $T^{(i)} \in \mathbb{K}$ is either zero* *or invertible, we get $T^{(1)} = 0$. Next, all TB_i vanishes in the second column unless $i = d$. Thus, comparing the second column in* (13) *we see that the second column of $T^{(d)}B_d$, which equals $-\lambda_0 T^{(d)} e_1$, vanishes. As before, $T^{(d)} \in \mathbb{K}$ is either invertible or zero, and therefore, $T^{(d)} = 0$.*

Assume we have already shown that $T^{(d)} = T^{(d-1)} = \cdots = T^{(d-k+1)} = 0$ for some $k \geqslant 1$. Note that $(k+2)$-nd columns of $TB_{d-(k+1)}, \ldots, TB_1$ all vanish. Thus, comparing the $(k+2)$-nd column inside (13)*, we get that $-\lambda_0 T^{(d-k)} e_1 = 0$, and as above $T^{(d-k)} = 0$. By induction, $T^{(i)}$ all vanish, as claimed.*

Example 4.5. *Let us further illustrate the above calculations with the construction of S in a concrete case. Suppose $\mathbb{F} = \mathbb{Z}_2$, $d = 3$. Notice that $m(x) = x^3 + x + 1 \in \mathbb{F}[x]$ is an irreducible polynomial, therefore $C = \left(\begin{smallmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{smallmatrix}\right)$. Denote $\mathbb{K} = \mathbb{F}[C]$ and let $\phi(x) = x^2$ be the generator of Galois group* $\mathrm{Gal}(\mathbb{K}|\mathbb{F})$*. We choose the $\mathbb{K}$-basis $B_1, B_2, B_3 \in M_3(\mathbb{F})$ as in Example 4.4, so $B_1 = E_{11}, B_2 = E_{11}C = E_{13}$ and $B_3 = E_{11}C^2 = E_{12}$. Theorem 3.3 yields the existence of a 3-dimensional invertible $\mathbb{K}$-module, generated by the matrices*

$$A_1' = I, A_2' = \left(\begin{smallmatrix} 0 & \alpha & \alpha \\ 1 & 0 & \alpha \\ 1 & 1 & 0 \end{smallmatrix}\right) \text{ and } A_3' = \begin{pmatrix} 0 & \alpha & \alpha^2 \\ \alpha^2 & 0 & \alpha \\ 1 & \alpha^4 & 0 \end{pmatrix} \in M_3(\mathbb{K}),$$

where α is a zero of polynomial m. Now, following the proof of Theorem 3.3, we have to firstly diagonalize the matrix C. This can be done, e.g., with the help of the modal matrix $P = \begin{pmatrix} \alpha^6 & \alpha^5 & \alpha^3 \\ \alpha & \alpha^2 & \alpha^4 \\ 1 & 1 & 1 \end{pmatrix}$. Since we need to have A_1', A_2' and A_3' in the same basis, we conjugate them with P to obtain

$$A_1 = PA_1'P^{-1} = I,\ A_2 = PA_2'P^{-1} = \begin{pmatrix} \alpha^6 & \alpha & \alpha^5 \\ \alpha^3 & 1 & \alpha^2 \\ \alpha^5 & 1 & \alpha^2 \end{pmatrix},\ \text{and } A_3 = PA_3'P^{-1} = \begin{pmatrix} 0 & \alpha^4 & \alpha^6 \\ \alpha^6 & \alpha & \alpha^3 \\ \alpha^6 & 0 & \alpha \end{pmatrix} \in M_3(\mathbb{K}).$$

We can now define matrices $S_{ij} \in M_d(\mathbb{F})$ as in Equation (11) by $S_{ij} = \sum_{k=1}^{3} \boldsymbol{\alpha}_{ki}^{(j)} B_k$ where $\boldsymbol{\alpha}_{ki}^{(j)}$ denotes the (k,i)-entry of matrix A_j. This finally yields by inserting C in place of α that

$$S = \begin{pmatrix} 1&0&0&1&1&1&0&1&1 \\ 0&0&0&0&1&1&0&0&0 \\ 0&0&0&1&1&0&0&1&1 \\ 0&0&1&0&1&1&0&0&0 \\ 0&0&0&1&0&0&1&0&1 \\ 0&0&0&0&0&0&1&0&0 \\ 0&1&0&1&0&0&1&0&1 \\ 0&0&0&1&0&0&0&1&1 \\ 0&0&0&1&1&1&1&0&0 \end{pmatrix}$$

and by Theorem 4.2, S generates a nondegenerate generalized bilinear form on $\mathbb{K}^3 = \mathbb{F}[C]^3$.

Example 4.6. *Another possibility for a $\mathbb{K}$-basis of a $\mathbb{K}$-module $M_d(\mathbb{F})$, in the case when the field extension $\mathbb{K}|\mathbb{F}$ is Galois with a cyclic Galois group, can be obtained with the help of Noether-Skolem theorem. Then, there exists an invertible matrix $U \in M_d(\mathbb{F})$ such that*

$$M_d(\mathbb{F}) = \mathbb{K} \oplus \mathbb{K}U \oplus \mathbb{K}U^2 \oplus \cdots \oplus \mathbb{K}U^{d-1}$$

and $X \mapsto UXU^{-1}$ is the generator of the cyclic group $\mathrm{Gal}\,(\mathbb{K}|\mathbb{F})$*, see [4, Lemma 2.2]; relative to this basis, the map $X \mapsto XC$ is given by diagonal matrix. Note that this is applicable to finite fields $\mathbb{F}$ when d is a prime integer, since every finite field extension has a cyclic Galois group (see [8, Corollary p. 96 and Theorem 3.11]). We acknowledge that the idea to use Noether-Skolem is based on [9, Lemma 3.2].*

Remark 4.7. *Suppose S_1 and S_2 are two matrices in $M_{d^2}(\mathbb{F})$. We say that bilinear forms $\mathcal{B}_{S_1}$ and $\mathcal{B}_{S_2}$ are equivalent ($\mathcal{B}_{S_1} \sim \mathcal{B}_{S_2}$) if there exist invertible matrices $G, H \in M_d(\mathbb{K})$ such that $S_2 = G^* S_1 H$. Note that $\sim$ is indeed an equivalence relation on the set of all generalized bilinear forms $\mathcal{B}_S \colon \mathbb{K}^d \times \mathbb{K}^d \to M_d(\mathbb{F})$ induced by matrices $S \in M_{d^2}(\mathbb{F})$. Also, observe that $S_2 = G^* S_1 H$ implies that $\mathcal{B}_{S_2}(X, Y) = \mathcal{B}_{S_1}(HX, GY)$ for all $X, Y \in \mathbb{K}^d$. In order for the calculations with the bilinear forms to be as manageable as possible, we can always replace a bilinear form with another equivalent bilinear form with a specified first block row and column. Assume therefore that $\mathcal{B}_{S_1}$ is nondegenerate and let $\{F_1, F_2, \ldots, F_d\}$ be a basis for the left $\mathbb{K}$-module $M_d(\mathbb{F})$ and $\{F_1' = F_1, F_2', \ldots, F_d'\}$ be a basis* *for the right $\mathbb{K}$-module $M_d(\mathbb{F})$. Then we prove that $\mathcal{B}_{S_1} \sim \mathcal{B}_{S_2}$ where in d-by-d block decomposition of S_2, the first column equals $\begin{pmatrix} F_1 \\ \vdots \\ F_d \end{pmatrix}$ and the first row equals $(F_1', F_2', \dots, F_d')$.*

To see this, denote by $S_1^{(1)}$ the first d-by-d block column vector of S_1 and observe that the blocks in $S_1^{(1)}$ form a basis for the left $\mathbb{K}$-module $M_d(\mathbb{F})$. Indeed, otherwise there exists a nonzero $Y \in \mathbb{K}^d$ such that $Y^* S_1^{(1)} = 0$ and thus $Y^* S_1 X = 0$ for $X = (I, 0, 0, \dots, 0)^*$ which is a contradiction since $\mathcal{B}_{S_1}$ is nondegenerate. This implies that there exists an invertible matrix $G \in M_d(\mathbb{K})$ such that the first column of $G^* S_1$ equals $(F_1, F_2, \dots, F_d)^*$. Since $\mathcal{B}_{G^* S_1}(X, Y) = \mathcal{B}_{S_1}(X, GY)$, the bilinear form $\mathcal{B}_{G^* S_1}$ is nondegenerate and we can prove with a similar reasoning as above that the blocks in the first d-by-d block row of $G^* S_1$ form a basis for the right $\mathbb{K}$-module $M_d(\mathbb{F})$. Therefore, there exists an invertible matrix $H \in M_d(\mathbb{K})$ such that the first row of $G^* S_1 H$ equals $(F_1', F_2', \dots, F_d')$. But since $F_1' = F_1$, the first block column of H equals $(I, 0, 0, \dots, 0)$, therefore the first block column of $G^* S_1 H$ remains equal to $(F_1, F_2, \dots, F_d)^*$, as claimed.

In particular, if the field extension $\mathbb{K}|\mathbb{F}$ is Galois with a cyclic Galois group then every nondegenerate generalized bilinear form is equivalent to $\mathcal{B}_S$, where the first block column of S equals $\begin{pmatrix} U^0 \\ \vdots \\ U^{d-1} \end{pmatrix}$ and the first block row of S equals $(U^0, \dots, U^{d-1})$, with $U \in M_d(\mathbb{F})$ from Example 4.6.

Example 4.8. *Assume $S \in M_{d^2}(\mathbb{F})$ induces a nondegenerate bilinear form and the field extension $\mathbb{K}|\mathbb{F}$ is Galois with a cyclic Galois group. By Remark 4.7, we can assume that the first block column of S equals $\begin{pmatrix} U^0 \\ \vdots \\ U^{d-1} \end{pmatrix}$, where $U \in M_d(\mathbb{F})$ is from Example 4.6. Since all block columns of S also form a basis for left $\mathbb{K}$-module $M_d(\mathbb{F})$, there exist transition matrices $P_i \in M_d(\mathbb{K})$ such that the i-th block column of S satisfies*

$$S_i = P_i S_1.$$

Then, with $\mathbf{X} = (X_1, \dots, X_d)^* \in \mathbb{K}^d$, we have

$$S\mathbf{X} = S_1 X_1 + \cdots + S_d X_d = S_1 X_1 + P_2 S_1 X_2 + \cdots + P_d S_1 X_d.$$

Now, note that $X_i = p_i(C) \in \mathbb{F}[C]$ and note that

$$S_1 X_i = \begin{pmatrix} I \cdot p_i(C) \\ U p_i(C) \\ \vdots \\ U^{d-1} p_i(C) \end{pmatrix} = \begin{pmatrix} p_i(C) \cdot I \\ \phi(p_i(C) U \\ \vdots \\ \phi^{d-1}(p_i(C)) U^{d-1} \end{pmatrix} = \begin{pmatrix} p_i(C) & & & \\ & \phi(p_i(C)) & & \\ & & \ddots & \\ & & & \phi^{d-1}(p_i(C)) \end{pmatrix} S_1$$

so,

$$S\mathbf{X} = \sum_{i=1}^{d} P_i \begin{pmatrix} X_i & & & \\ & \phi(X_i) & & \\ & & \ddots & \\ & & & \phi^{d-1}(X_i) \end{pmatrix} \begin{pmatrix} I \\ U \\ \vdots \\ U^{d-1} \end{pmatrix}$$

with P_1 the identity matrix in $M_d(\mathbb{K})$. Then S induces a nondegenerate generalized bilinear form if and only if the matrix

$$\sum_{i=1}^{d} P_i \begin{pmatrix} X_i & & & \\ & \phi(X_i) & & \\ & & \ddots & \\ & & & \phi^{d-1}(X_i) \end{pmatrix} = \begin{pmatrix} X_1 & & & \\ & \phi(X_1) & & \\ & & \ddots & \\ & & & \phi^{d-1}(X_1) \end{pmatrix} + P_2 \begin{pmatrix} X_2 & & & \\ & \phi(X_2) & & \\ & & \ddots & \\ & & & \phi^{d-1}(X_2) \end{pmatrix}$$
$$+ \cdots + P_d \begin{pmatrix} X_d & & & \\ & \phi(X_d) & & \\ & & \ddots & \\ & & & \phi^{d-1}(X_d) \end{pmatrix}$$

is always nonsingular whenever $(X_1,\dots,X_d)^* \in \mathbb{K}^d$ *is nonzero. We can multiply this matrix on the right with* $\widehat{U}^{-1} := \mathrm{diag}(I,U,\dots,U^{d-1})^{-1} \in M_{d^2}(\mathbb{F})$ *to see that*

$$\sum_i P_i\widehat{U}X_i$$

is nonsingular for every nonzero vector $(X_1,\dots,X_d) \in \mathbb{K}^d$*, that is, the transition matrices* $P_1,\dots,P_d \in M_d(\mathbb{K}) \subseteq M_{d^2}(\mathbb{F})$ *are such that* $P_1\widehat{U},\dots,P_d\widehat{U} \subseteq M_{d^2}(\mathbb{F})$ *span an invertible right* $\mathbb{K}$*-module. This construction reverses the construction of Example 4.6 using Theorem 4.2.*

5. Concluding remarks

Let us finish with some possible applications.

(i) Let $\mathbb{F}$ be a field and let $\mathbb{K} = \mathbb{F}[C]$, where $C \in M_d(\mathbb{F})$ is a companion matrix of some irreducible polynomial $x^d + c_{d-1}x^{d-1} + \cdots + c_1x + c_0$. Then, each invertible $\mathbb{K}$-module in $M_d(\mathbb{K})$ induces a left-unital division $\mathbb{F}$-algebra with dimension d^2 which contains $\mathbb{K}$ as a subfield. To see that, choose an ordered basis

$$(V_1,\dots,V_{d^2}) = (I, A_1,\dots,A_{d-1},\check{C},\check{C}A_1,\dots,\check{C}A_{d-1},\check{C}^2,\check{C}^2A_1,\dots,\check{C}^{d-1}A_{d-1}),$$

where

$$\check{C} = I\otimes C = \begin{pmatrix} 0 & \cdots & \cdots & -c_0I \\ I & 0 & \cdots & -c_1I \\ & \ddots & & \vdots \\ 0 & \cdots & I & -c_{d-1}I \end{pmatrix},$$

consider these matrices inside $M_{d^2}(\mathbb{F})$, and apply the procedure which returns a division algebra.

Observe that, relative to the lexicographically ordered basis

$$e_1\otimes e_1,\dots,e_d\otimes e_1\ ,\ e_1\otimes e_2,\dots,e_d\otimes e_2\ ,\ e_1\otimes e_3,\dots,e_d\otimes e_d$$

one has $V_{ad+1} = \check{C}^a = I\otimes_{\mathbb{F}} C^a$. So its $(bd+1)$-th column equals $\check{C}^a e_{bd+1} = (I\otimes C^a)(e_1\otimes e_{b+1}) = (I\otimes C^a)(e_1\otimes (C^b e_1)) = e_1\otimes(C^{a+b}e_1) = e_1\otimes\sum_k \lambda_k e_k = \sum_k \lambda_k e_1\otimes e_k = \sum_k \lambda_k e_{kd+1}$. This shows that

$$V_{ad+1}\star V_{bd+1} = \sum_k \lambda_k V_{kd+1} = \sum_k \lambda_k(I\otimes C^k) = I\otimes(\sum_k \lambda_k C^k) = I\otimes C^{a+b}$$

where at the end we used the fact, which follows from $C^te_1 = e_{t+1}$ for $t \leqslant d-1$, that if $C^te_1 = \sum_k \lambda_k e_k = \sum_k \lambda_k C^{k-1}e_1$, then $C^t = \sum_k \lambda_k C^{k-1}$. This shows that we have

$$V_{ad+1}\star V_{bd+1} = \check{C}^{a+b} = V_{ad+1}V_{bd+1}; \qquad 0\leqslant a,b\leqslant d-1.$$

Hence, the obtained left-unital division algebra $\mathcal{A}$ contains a field $\mathbb{K}\subseteq\mathcal{A}$ with $\dim_{\mathbb{F}}\mathbb{K} = \sqrt{\dim_{\mathbb{F}}\mathcal{A}}$.

(ii) Let $\mathbb{F} = \mathrm{GF}(q)$ be a finite field and $p \geqslant 3$ a prime. Suppose $S \in M_{p^2}(\mathbb{F})$ is an invertible matrix and the generalized bilinear forms induced by S and by S^{-1} are both degenerate. Choose any nonscalar matrix $A \in M_{p^2}(\mathbb{F})$ and let $B = S^{-1}AS$ be its conjugate. Then, there exists a chain of six nonscalar matrices $A = X_0 \sim X_1 \sim X_2 \sim X_3 \sim X_4 \sim X_5 = B$ such that X_i commutes with X_{i+1} (equivalently, the distance between A and B in a commuting graph is at most five, see [5]).

To see this, we only need to consider the case when $\mathbb{F}[A]$ is a field (otherwise we can apply the proof of [5, Theorem 3.3]). Observe that $\mathbb{F}[A] = \mathrm{GF}(q^{p^2})$, so it contains $\mathrm{GF}(q^p)$ as a proper intermediate subfield and in particular there exists a polynomial f such that $f(A)$ is its generator. Up to conjugation, $f(A)$ equals its rational form $\bigoplus_1^p C$, where $C \in M_p(\mathbb{F})$ is a companion matrix of some irreducible polynomial. Let $\mathbb{K} = \mathbb{F}[C]$

and choose nonzero matrices $\mathbf{X}, \mathbf{V}, \ \mathbf{Y}, \mathbf{U} \in \mathbb{K}^p$ such that $\mathcal{B}_S(\mathbf{X}, \mathbf{V}) = \mathbf{V}^* S\mathbf{X} = 0$ and $\mathcal{B}_{S^{-1}}(\mathbf{U}, \mathbf{Y}) = \mathbf{Y}^* S^{-1}\mathbf{U} = 0$. Since $f(A) = \bigoplus_1^p C$, it commutes with every block matrix of the form $(p_{ij}(C))_{ij}$ and in particular with $\mathbf{XY}^*$. This gives us a desired chain

$$A \sim f(A) \sim \mathbf{XY}^* \sim S^{-1}(\mathbf{UV}^*)S \sim S^{-1}f(A)S \sim B = S^{-1}AS.$$

(iii) The generalized bilinear form can be seen as a bunch of suitably dependent d^2 ordinary bilinear forms on $\mathbb{F}^n$ ($n = d^2$) stacked together into a d-by-d matrix. Namely, each vector $x = (x_1, \dots, x_d)^T \in \mathbb{F}^d$ induces an element $p_x(C) := x_1 I + x_2 C + \cdots + x_d C^{d-1} \in \mathbb{K}$ such that $p_x(C)e_1 = x$; observe that $x \mapsto p_x(C)$ is $\mathbb{F}$-linear and bijective. In this way, each $x \in \mathbb{F}^n$, partitioned into blocks of size d, induces a vector $\mathbf{V}_x \in \mathbb{K}^d$ and $x \mapsto \mathbf{V}_x$ is an $\mathbb{F}$-linear and bijective map from $\mathbb{F}^n$ to $\mathbb{K}^d$. Then, $B(x, y) := \mathbf{V}_y^* S\mathbf{V}_x = \mathcal{B}_S(\mathbf{V}_x, \mathbf{V}_y)$ is also an $\mathbb{F}$-bilinear map from $\mathbb{F}^n \times \mathbb{F}^n$ into $\mathbb{F}^d$.

References

[1] S. Akbari, A. Mohammadian, H. Radjavi, P. Raja, On the diameters of commuting graphs, Linear Algebra Appl. 418 (2006), no. 1, 161–176.

[2] R. Brauer, K .A. Fowler, On groups of even order, Ann. of Math. (2) 62 (1955), 565–583.

[3] C. de Seguins Pazzis, The singular linear preservers of non-singular matrices, Linear Algebra Appl. 433 (2010), no. 2, 483–490.

[4] D. Dolžan, D. Kokol Bukovšek, B. Kuzma, On the lower bound for diameter of commuting graph of prime-square sized matrices, Filomat 32 (2018), no. 17, 5993–6000.

[5] D. Dolžan, D. Kokol Bukovšek, B. Kuzma, Polona Oblak, On diameter of the commuting graph of a full matrix algebra over a finite field, Finite Fields Appl. 37 (2016), 36–45.

[6] H. R. Dorbidi, On a conjecture about the commuting graphs of finite matrix rings, Finite Fields Appl. 56 (2019), 93–96.

[7] M. Elyze, A. Guterman, R. Morrison, K. Šivic, Higher-distance commuting varieties, Linear Multilinear Algebra 70 (2022), no. 17, 3248–3270.

[8] L. C. Grove, Algebra, Pure and Applied Mathematics, vol. 110, Academic Press, Inc., New York, 1983.

[9] R. M. Guralnick, Invertible preservers and algebraic groups, Proceedings of the 3rd ILAS Conference (Pensacola, FL, 1993), vol. 212/213, 1994, pp. 249–257.

[10] S. Ou, J. Zhong, Automorphisms of commuting graph of rank one upper triangular matrices, Electron. J. Linear Algebra 31 (2016), 774–793.

[11] Y. Shitov, A matrix ring with commuting graph of maximal diameter, J. Combin. Theory Ser. A 141 (2016), 127–135.

[12] O. Taussky, H. Zassenhaus, On the similarity transformation between a matrix and its transpose, Pacific J. Math. 9 (1959), 893–896.

[13] P. Šemrl, Invertibility preservers on central simple algebras, J. Algebra 408 (2014), 42–60.