Filomat 32:17 (2018), 5993–6000
https://doi.org/10.2298/FIL1817993D

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

On the Lower Bound for Diameter of Commuting Graph of Prime-Square Sized Matrices

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

[a] *Faculty of Mathematics and Physics, University of Ljubljana, Jadranska 21, 1000 Ljubljana, Slovenia*
[b] *IMFM, Jadranska 19, 1000 Ljubljana, Slovenia*
[c] *Faculty of Economics, University of Ljubljana, Kardeljeva Ploščad 17, 1000 Ljubljana, Slovenia*
[d] *University of Primorska, Glagoljaška 8, 6000 Koper, Slovenia*

Abstract. It is known that the diameter of commuting graph of n-by-n matrices is bounded above by six if the graph is connected. In the commuting graph of p^2-by-p^2 matrices over a sufficiently large field which admits a cyclic Galois extension of degree p^2 we construct two matrices at distance at least five. This shows that five is the lower bound for its diameter. Our results are applicable for all sufficiently large finite fields as well as for the field of rational numbers.

1. Introduction

The essence of commutativity relation on a given magma $\mathcal{A}$ (i.e., a nonempty set equipped with an inner operation, written as product ab, which is also known as a grupoid) is captured in its commuting graph $\Gamma = \Gamma(\mathcal{A})$. By definition, this 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 $ab = ba$. As far as we know, the commuting graph was introduced in [4] in an early attempt towards classification of simple finite groups, although one needs to mention that their graph also contained the central elements.

Clearly, if $\mathcal{A}$ is abelian then $\Gamma(\mathcal{A})$ is an empty graph (has no vertices). At the other extreme, there are magmas where no two distinct elements commute. Their commuting graph is null, i.e. it consists of disjoint vertices with no edges. Such examples exists even in the category of semigroups. Consider, for example the semigroup on n elements $\{v_1, \ldots, v_n\}$ with the product $v_i v_j = v_i$. In those two examples the commuting graph only captures the presence of a complete commutativity or the complete lack of it.

2010 *Mathematics Subject Classification*. 05C50, 05C12, 15A27
Keywords. Matrix algebra, Field, Commuting graph, Diameter
Received: 26 March 2018; Accepted: 29 November 2018
Communicated by Francesco Belardo
The authors acknowledge the financial support from the Slovenian Research Agency (research core funding No. P1-0222).
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)

However, for important classes of magmas which contain just enough commuting pairs, the commuting graph can be a powerful tool. Say, in the category of groups, the commuting graph is able to characterize finite simple nonabelian groups [20]. Similarly, in the category of rings, the commuting graph is able to distinguish a ring $M_2(\mathbb{F})$ of 2-by-2 matrices over a finite field $\mathbb{F}$ among all finite unital rings [16, Corollary 5]. Recently, in [13] the author extended this result and showed that the commuting graph can distinguish among algebras of bounded operators on a complex Hilbert space — it can calculate the dimension of the underlying vector space.

On the other hand, every finite graph is an induced subgraph of a commuting graph of a finite group, see [18]. Unaware of this result, the authors proved in [3] a similar statement, valid also for countably infinite graphs by essentially the same technique, for induced subgraphs of commuting graph of $B(\ell^2)$, the algebra of bounded operators on a complex separable Hilbert space. It was also shown in [3] that not all finite graphs are induced subgraphs of a commuting graph of complex matrices if the size is kept fixed.

One of the basic properties of a graph is its diameter and connectedness. This question turned out to be surprisingly hard for the commuting graphs. For example, only recently it was shown in [11] that a commuting graph of a finite group can have an arbitrary large diameter. In contrast, if a group has a trivial center then every connected component of its commuting graph has diameter at most 10, see [17]. More is known for commuting graphs of $M_n(\mathbb{F})$, the algebra of n-by-n matrices over a field $\mathbb{F}$. If $\mathbb{F}$ is algebraically closed and $n \geq 3$ then the diameter of the commuting graph $\Gamma(M_n(\mathbb{F}))$ is 4, see [1]. This result was of fundamental importance in classifying surjections which preserve commutativity on complex matrices in one direction only [5]. For other fields it was shown in [1] that the diameter of a connected commuting graph of $M_n(\mathbb{F})$ is bounded above by 6 and it was shown in [19] that there exists $\mathbb{F}$ such that the commuting graph of $M_{219}(\mathbb{F})$ is connected with diameter 6. In our recent paper [7] we constructed, for each prime $p \geq 7$, two similar matrices $A, B \in M_{2p}(\mathbb{Q})$, at maximal possible distance, i.e., at distance 6 in the commuting graph $\Gamma(M_{2p}(\mathbb{Q}))$ (here, $\mathbb{Q}$ denotes the field of rational numbers). In contrast to these results, some peculiarities appear if one considers finite fields $\mathbb{F}$. Clearly, in this case $\Gamma(M_n(\mathbb{F}))$ is a finite graph and it is known to have the following properties (see [8]): if $n \geq 4$ is even, then its diameter is 4, if n is a prime, then it is disconnected, and if n is neither a prime nor a square of a prime (the smallest such n is 15), then its diameter is at most 5.

Presently, we consider the case of commuting graphs of $M_n(\mathbb{F})$ where $n = p^2$ is a square of an odd prime p. Our main result shows that, subject to some constraints which are satisfied for every finite field with sufficiently many elements, the commuting graph has diameter at least 5. We conclude with, up to our knowledge the first, example of a commuting graph of matrix algebras with diameter five. We show that this occurs in $M_{15}(\mathbb{F})$ for suitable finite fields $\mathbb{F}$.

2. Preliminaries

Throughout, let $p \geq 3$ be a prime, let $n = p^2$, let $\mathbb{F}$ be a field, and let $C = C(m(x)) \in M_p(\mathbb{F})$ be a companion matrix of an irreducible polynomial $m(x) \in \mathbb{F}[x]$ with degree p, so that $\mathbb{K} := \mathbb{F}[C]$ is a field extension of $\mathbb{F}$. Also, let $\mathrm{GF}(p^n)$ be the Galois field of order p^n and let $\mathbb{Z}_n$ be an additively written cyclic group of order n; if $n = p$ is a prime then $\mathbb{Z}_p$ has additional structure of a field in which case we also abbreviate $\mathbb{Z}_p = \mathrm{GF}(p)$.

The following definition will be essential for the construction of two matrices in $M_n(\mathbb{F})$ at distance at least 5.

Definition 2.1. For any matrix $X \in M_p(\mathbb{F})$ we define the block tridiagonal matrix

$$S(X) := \begin{pmatrix} I & X & 0 & \cdots & 0 & 0 \\ X^{p-1} & I & X & \ddots & 0 & 0 \\ 0 & X^{p-2} & I & \ddots & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & I & X \\ 0 & 0 & 0 & \cdots & X & I \end{pmatrix} \in M_n(\mathbb{F}); \qquad n = p^2. \tag{1}$$

A crucial step towards our goal is the construction of a matrix X in the next lemma. For convenience let us recall here the fundamental theorem of Galois theory. If the field extension $\mathbb{K}|\mathbb{F}$ is the splitting field of some irreducible separable polynomial over $\mathbb{F}$, then it is a Galois extension. The cardinality of its Galois group equals $[\mathbb{K} : \mathbb{F}]$, the degree of the extension. In particular, if $\mathbb{K} = \mathbb{F}[C]$ for a companion matrix $C \in M_p(\mathbb{F})$ of some irreducible polynomial and if its size p is a prime, then $[\mathbb{K} : \mathbb{F}] = p$ is a prime, so the Galois group of extension $\mathbb{K}|\mathbb{F}$ must be cyclic as this is the only group of prime order.

Lemma 2.2. *Let p be a prime and $\mathbb{F}$ a field with at least $\frac{p^2(p-1)}{2} + 2$ elements. Choose $C \in M_p(\mathbb{F})$, a companion matrix of some irreducible monic separable polynomial $m(x) \in \mathbb{F}[x]$ so that $\mathbb{K} := \mathbb{F}[C]$ is its splitting field. Then, there exists a matrix $\mathfrak{U} \in M_p(\mathbb{F})$ such that $S(\mathfrak{U})$ is invertible, $\mathfrak{U}^p \in \mathbb{F}I$,*

$$\mathfrak{U}\mathbb{K} = \mathbb{K}\mathfrak{U} \quad \textit{and} \quad M_p(\mathbb{F}) = \mathbb{K} + \mathbb{K}\mathfrak{U} + \mathbb{K}\mathfrak{U}^2 + \cdots + \mathbb{K}\mathfrak{U}^{p-1}. \tag{2}$$

Furthermore, $\phi(X) = \mathfrak{U}X\mathfrak{U}^{-1}$ $(X \in \mathbb{K})$ is a generator of the cyclic group $\mathrm{Gal}(\mathbb{K}|\mathbb{F})$*, and the sum* (2) *is direct as a sum of left $\mathbb{K}$-modules.*

Proof. Note that $M_p(\mathbb{F})$ is a central simple $\mathbb{F}$-algebra, $\mathbb{K} \subseteq M_p(\mathbb{F})$, $|\mathrm{Gal}(\mathbb{K}|\mathbb{F})| = [\mathbb{K} : \mathbb{F}] = p$, and $p^2 = \dim_{\mathbb{F}}(M_p(\mathbb{F}))$. By [9, §10, Lemma 2] this guarantees the existence of invertible $\mathfrak{U} \in M_p(\mathbb{F})$ such that (2) holds and that $X \mapsto \mathfrak{U}X\mathfrak{U}^{-1}$ generates $\mathrm{Gal}(\mathbb{K}|\mathbb{F})$. The only thing that is left for us to prove, is that $\mathfrak{U}$ can be chosen in such way that $S(\mathfrak{U})$ is invertible. It is obvious that we can freely interchange $\mathfrak{U}$ with $\lambda\mathfrak{U}$ for any nonzero $\lambda \in \mathbb{F}$ without disturbing any other properties of $\mathfrak{U}$. So, let us denote $q(\lambda) = \det S(\lambda\mathfrak{U}) \in \mathbb{F}[\lambda]$ and observe that by the construction of the matrix $S(\lambda\mathfrak{U})$, $q(\lambda)$ is a polynomial of degree at most $\frac{p^2(p-1)}{2}$. Since $q(0) = 1$, we can conclude that $q(\lambda)$ is a nonzero polynomial and hence there exists a nonzero $\lambda \in \mathbb{F}$ such that $q(\lambda) \neq 0$, which proves that $S(\lambda\mathfrak{U})$ is indeed an invertible matrix. □

3. Main Result

To prove our main result that in the commuting graph of p^2-by-p^2 matrices (p an odd prime) over suitable fields we can always find two matrices at distance at least five (see Theorem 3.2 below) it will be beneficial to find an invertible matrix $S \in M_n(\mathbb{F})$, such that any two nonscalar matrices $F \in M_p(\mathbb{K}) \subseteq M_n(\mathbb{F})$ and $H \in S^{-1}M_p(\mathbb{K})S$ are different. We show in Proposition 3.1 below that $S := S(\mathfrak{U})$ for the matrix $\mathfrak{U}$ from Lemma 2.2 yields the desired result.

Proposition 3.1. *If p-by-p block matrices $F, G \in M_p(\mathbb{K}) \subseteq M_n(\mathbb{F})$ are both nonscalar, then $F \neq S^{-1}GS$.*

Proof. Let $F = (F_{ij})_{i,j=1}^{p}, G = (G_{ij})_{i,j=1}^{p}$ with $F_{ij}, G_{ij} \in \mathbb{K}$. Suppose that $SF = GS$. We need to show that at least one of the matrices F and G is scalar. Denote by $E_{ij} \in M_p(\mathbb{K}) \subseteq M_n(\mathbb{F})$ the block matrix with identity matrix at the (i, j)-th place and 0's elsewhere. Choose $\mathfrak{U}$ from Lemma 2.2 and denote $\hat{\mathfrak{U}} = \operatorname{diag}(\mathfrak{U}, \dots, \mathfrak{U}) \in M_n(\mathbb{F})$. Expand the matrix S as

$$S = S_0 + S_1\hat{\mathfrak{U}} + S_2\hat{\mathfrak{U}}^2 + \cdots + S_{p-1}\hat{\mathfrak{U}}^{p-1} = I + R\hat{\mathfrak{U}} + E_{(p-1)\,(p-2)}\hat{\mathfrak{U}}^2 + \cdots + E_{21}\hat{\mathfrak{U}}^{p-1}$$

where

$$R = \begin{pmatrix} 0 & I & 0 & \cdots & 0 & 0 \\ 0 & 0 & I & \ddots & 0 & 0 \\ 0 & 0 & 0 & \ddots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & I \\ 0 & 0 & 0 & \cdots & I & 0 \end{pmatrix},$$

Comparing the (i, j)-th block of $SF = GS$ we get $\sum_{k=0}^{p-1}(S_k\hat{\mathfrak{U}}^k F)_{ij} = \sum_{k=0}^{p-1}(GS_k\hat{\mathfrak{U}}^k)_{ij}$. Since each block of each S_k belongs to $\mathbb{K} = \mathbb{F}[C]$ we can apply Lemma 2.2 blockwise and using $\mathfrak{U}^k F_{ij} = \phi^k(F_{ij})\mathfrak{U}^k$ we deduce that $S_k\hat{\mathfrak{U}}^k F = GS_k\hat{\mathfrak{U}}^k$ for every $k = 0, 1, \dots, p-1$. With $k = 0$ we get $F = G$. With $k = p-1$, we get

$$E_{21}\hat{\mathfrak{U}}^{p-1}F = \hat{\mathfrak{U}}^{p-1}\begin{pmatrix} 0 & 0 & \cdots & 0 \\ F_{11} & F_{12} & \cdots & F_{1p} \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} = FE_{21}\hat{\mathfrak{U}}^{p-1} = \begin{pmatrix} F_{12} & 0 & \cdots & 0 \\ F_{22} & 0 & \cdots & 0 \\ F_{32} & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ F_{p2} & 0 & \cdots & 0 \end{pmatrix}\hat{\mathfrak{U}}^{p-1}.$$

So $F_{1j} = 0$ for every $j \neq 1$, $F_{i2} = 0$ for every $i \neq 2$ and $\mathfrak{U}^{p-1}F_{11} = F_{22}\mathfrak{U}^{p-1}$. Similarly, for every $s = 2, \dots, p-2$, we get $E_{(s+1)\,s}\,\hat{\mathfrak{U}}^{p-s}F = FE_{(s+1)\,s}\,\hat{\mathfrak{U}}^{p-s}$, so $F_{sj} = 0$ for every $j \neq s$, $F_{i\,(j+1)} = 0$ for every $i \neq s+1$ and $\mathfrak{U}^{p-s}F_{ss} = F_{(s+1)\,(s+1)}\mathfrak{U}^{p-s}$. Thus

$$F = \begin{pmatrix} F_{11} & 0 & 0 & \cdots & 0 & 0 \\ 0 & F_{22} & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & & \vdots & \vdots \\ 0 & 0 & 0 & \ddots & 0 & 0 \\ F_{(p-1)\,1} & 0 & 0 & \cdots & F_{(p-1)\,(p-1)} & F_{(p-1)\,p} \\ F_{p1} & 0 & 0 & \cdots & 0 & F_{pp} \end{pmatrix}.$$

Now, with $k = 1$ we have $R\hat{\mathfrak{U}}F = FR\hat{\mathfrak{U}}$, so

$$\hat{\mathfrak{U}}\begin{pmatrix} 0 & F_{22} & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & F_{33} & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & \ddots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ F_{(p-1)\,1} & 0 & 0 & \cdots & 0 & F_{(p-1)\,(p-1)} & F_{(p-1)\,p} \\ F_{p1} & 0 & 0 & \cdots & 0 & 0 & F_{pp} \\ F_{(p-1)\,1} & 0 & 0 & \cdots & 0 & F_{(p-1)\,(p-1)} & F_{(p-1)\,p} \end{pmatrix} =$$

$$= \begin{pmatrix} 0 & F_{11} & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & F_{22} & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & \ddots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & F_{(p-2)\,(p-2)} & 0 \\ 0 & F_{(p-1)\,1} & 0 & \cdots & 0 & F_{(p-1)\,p} & F_{(p-1)\,(p-1)} \\ 0 & F_{p1} & 0 & \cdots & 0 & F_{pp} & 0 \end{pmatrix} \hat{\mathfrak{U}}.$$

Thus $F_{(p-1)\,1} = F_{p1} = F_{(p-1)\,p} = 0$, so F is block diagonal, and $\mathfrak{U}F_{(j+1)\,(j+1)} = F_{jj}\mathfrak{U}$, for every $j = 1, \ldots, p-1$, so $F_{jj} = \phi(F_{(j+1)\,(j+1)})$. We now have

$$F = \operatorname{diag}(\phi^{p-1}(F_{pp}), \phi^{p-2}(F_{pp}), \ldots, \phi(F_{pp}), F_{pp}).$$

In particular, $\mathfrak{U}F_{pp} = F_{(p-1)\,(p-1)}\mathfrak{U}$. Looking at the next to last entry in the last row, we see that also $\mathfrak{U}F_{(p-1)\,(p-1)} = F_{pp}\mathfrak{U}$, so $\mathfrak{U}^2F_{pp} = F_{pp}\mathfrak{U}^2$, or $\phi^2(F_{pp}) = F_{pp}$. Thus, ϕ^2 is also a generator of cyclic group $\mathrm{Gal}(\mathbb{K}|\mathbb{F})$ and F_{pp} is its fixed point, so $F_{pp} \in \mathbb{F}I$. Then $F_{jj} = F_{pp}$ for every j and matrix F is scalar, a contradiction. □

Theorem 3.2. *Let $p \geq 3$ be a prime, $\mathbb{F}$ be a field containing at least $\frac{p^2(p-1)}{2} + 2$ elements and let $n = p^2$. Suppose that $\mathbb{F}$ admits a Galois field extension $\mathbb{L}$ of degree n with a cyclic Galois group. Then there exist nonscalar matrices in $M_n(\mathbb{F})$ at a distance of at least 5. If the commuting graph of $M_n(\mathbb{F})$ is connected, it has a diameter of at least 5.*

Remark 3.3. *Any finite field with enough elements, and also the field of rational numbers $\mathbb{Q}$ satisfy the conditions of the theorem, see [15]. In the finite case, the commuting graph of $M_n(\mathbb{F})$ is connected, see [2, Theorem 6]. In the case of rational numbers $\mathbb{Q}$ it is not, see [2, Remark 8].*

Remark 3.4. *In [6, Theorem 3.1] it is proved that $\Gamma(M_9(\mathbb{Z}_2))$ is connected with diameter at least 5. We therefore conjecture that in Theorem 3.2 the condition $|\mathbb{F}| \geq \frac{p^2(p-1)}{2} + 2$ is superfluous.*

Proof. Since $\mathrm{Gal}(\mathbb{L}|\mathbb{F}) = \mathbb{Z}_n$ has a unique proper subgroup, by the Fundamental Theorem of Galois theory the field $\mathbb{L}$ has a unique proper subfield $\mathbb{K}$. Moreover, $\mathbb{L}$, hence also $\mathbb{K}$, are finite separable extensions of $\mathbb{F}$ so they are simple extensions ([12, Theorem 3.9, p. 95]). Therefore, there exist $\beta \in \mathbb{K}$ and $\alpha \in \mathbb{L}$ with

$$\mathbb{K} = \mathbb{F}[\beta] \quad \text{and} \quad \mathbb{L} = \mathbb{F}[\alpha] = \mathbb{K}[\alpha].$$

Let $m_\alpha(x)$ be the minimal polynomial of α over $\mathbb{K}$ and $m_\beta(x)$ be the minimal polynomial of β over $\mathbb{F}$. Let $C \in M_p(\mathbb{F})$ be the companion matrix of $m_\beta(x)$ and let

$$X = C \oplus \cdots \oplus C \in M_n(\mathbb{F}).$$

Then $\mathbb{F}[X] \simeq \mathbb{F}[C] \simeq \mathbb{K}$ and, by identifying $\mathbb{K} = \mathbb{F}[X]$,

$$C_{M_n(\mathbb{F})}(\mathbb{K}) = C_{M_n(\mathbb{F})}(\mathbb{F}[X]) = C_{M_n(\mathbb{F})}(X) = M_p(\mathbb{K}) \subseteq M_n(\mathbb{F}).$$

Similarly, let $A \in M_p(\mathbb{K}) \subseteq M_n(\mathbb{F})$ be the companion matrix of $m_\alpha(x) \in \mathbb{K}[x]$. Then $\mathbb{K}[A] \simeq \mathbb{L}$ and

$$C_{M_n(\mathbb{F})}(\mathbb{L}) = C_{M_n(\mathbb{F})}(\mathbb{K}) \cap C_{M_n(\mathbb{F})}(A) = M_p(\mathbb{K}) \cap C_{M_n(\mathbb{F})}(A) = C_{M_p(\mathbb{K})}(A) = \mathbb{K}[A] = \mathbb{L}.$$

Also, $\mathbb{F}[A] = \mathbb{L}$ implies $C_{M_n(\mathbb{F})}(A) = \mathbb{L}$. So we have the following picture

$$\mathbb{F} \subseteq \mathbb{K} = \mathbb{F}[X] \subseteq \mathbb{F}[A] = \mathbb{K}[A] = \mathbb{L} \subseteq M_p(\mathbb{K}) \subseteq M_n(\mathbb{F}).$$

Now let $S \in M_n(\mathbb{F})$ be a matrix defined in (1). We claim that in the commuting graph, the distance $d(A, SAS^{-1}) \geq 5$. To see this, let $B = S^{-1}AS$ and let

$$A = X_0 — X_1 — X_2 — \ldots — X_{k-2} — X_{k-1} — X_k = B \tag{3}$$

be the shortest path between A and B. Since $X_1 \in C_{M_n(\mathbb{F})}(A) = \mathbb{L} = \mathbb{F}[A]$ is nonscalar, either $\mathbb{F}[X_1] = \mathbb{F}[A]$ and $C_{M_n(\mathbb{F})}(X_1) = C_{M_n(\mathbb{F})}(A) = \mathbb{F}[A]$ or $\mathbb{F}[X_1] = \mathbb{K} = \mathbb{F}[X]$ and $C_{M_n(\mathbb{F})}(X_1) = C_{M_n(\mathbb{F})}(X) = M_p(\mathbb{K})$. In the first case, X_2 commutes with A, so (3) is not the shortest path. In the second case, we may assume without loss of generality that $X_1 = X \in \mathbb{F}[A]$. Similarly, we may assume without loss of generality that $X_{k-1} = S^{-1}XS \in \mathbb{F}[B]$. By Proposition 3.1, matrices X_1 and X_{k-1} are not equal, thus $d(A, B) > 2$. Since $X_2 \in C_{M_n(\mathbb{F})}(X_1)$, $X_2 \in M_p(\mathbb{K})$, and similarly $X_{k-2} \in S^{-1}M_p(\mathbb{K})S$. Clearly, also $X_1 \in M_p(\mathbb{K})$ and $X_{k-1} \in S^{-1}M_p(\mathbb{K})S$. Hence, whatever the choice of matrices $F \in \{X_1, X_2\}$ and $H \in \{X_{k-2}, X_{k-1}\}$, they are not equal by Proposition 3.1, thus $d(A, B) > 4$. □

4. Concluding Remarks and Examples

Let us show that the commuting graph of a matrix algebra can have diameter equal to 5. Below we provide a series of examples of such matrix algebras with the size 15-by-15 over various fields. To wit, let $A = C(m(x)) \in M_{15}(\mathbb{Z}_2)$ be the companion matrix of the polynomial $m(x) = x^{15} + x^5 + x^4 + x^2 + 1 \in \mathbb{Z}_2[x]$. It is easily seen that $m(x)$ is irreducible and that $\mathbb{Z}_2[A] \simeq \mathrm{GF}(2^{15})$ is its splitting field (in finite fields, every extension is a normal extension, see [14, Theorem 2.14]). Let $\mathbb{F}|\mathbb{Z}_2$ be a finite extension of fields, let $\bar{\mathbb{F}}$ be its algebraic closure and let $\alpha \in \bar{\mathbb{F}}$ be a zero of $m(x)$. Since $\mathbb{Z}_2[\alpha]$ is a subfield of $\mathbb{F}[\alpha]$ we have

$$\Big[\mathbb{F}[\alpha] : \mathbb{Z}_2\Big] = \Big[\mathbb{F}[\alpha] : \mathbb{Z}_2[\alpha]\Big] \times \Big[\mathbb{Z}_2[\alpha] : \mathbb{Z}_2\Big] = \Big[\mathbb{F}[\alpha] : \mathbb{Z}_2[\alpha]\Big] \times 15.$$

Hence, 15 divides $\Big[\mathbb{F}[\alpha] : \mathbb{Z}_2\Big] = \Big[\mathbb{F}[\alpha] : \mathbb{F}\Big] \times [\mathbb{F} : \mathbb{Z}_2]$. Now, if $[\mathbb{F} : \mathbb{Z}_2]$ is relatively prime with 15, then $15 \Big| [\mathbb{F}[\alpha] : \mathbb{F}] \leq 15$, so that $[\mathbb{F}[\alpha] : \mathbb{F}] = 15$ in which case $m(x)$ is irreducible over $\mathbb{F}$.

Hence, $m(x)$ is irreducible over a field $\mathrm{GF}(2^t)$ where t is not divisible by 3 nor by 5, so it is irreducible over an infinite sequence of field extensions of $\mathbb{Z}_2$. Let $\mathbb{F} = \mathrm{GF}(2^t)$ be such a finite field extension. Note that $A \in M_{15}(\mathbb{Z}_2) \subseteq M_{15}(\mathbb{F})$ generates a field $\mathbb{F}[A]$, isomorphic to $\mathrm{GF}(2^{15t})$ and it is well-known that there are exactly two intermediate subfields between $\mathbb{F}$ and $\mathbb{F}[A]$, namely the fields $\mathrm{GF}(2^{3t})$ and $\mathrm{GF}(2^{5t})$. Also, the multiplicative group $\mathbb{Z}_2[A]^* = \mathbb{Z}_2[A] \setminus \{0\}$ of a finite field $\mathbb{Z}_2[A]$ is cyclic of order $2^{15} - 1 = 7 \times 31 \times 151 = 32767$ and one easily checks that the multiplicative order of A is $|A| = 2^{15} - 1$. Thus, A generates $\mathbb{Z}_2[A]^*$. So, $|A^{31\times151}| = 7 = 2^3 - 1 = |\mathrm{GF}(2^3)^*|$ and $|A^{7\times151}| = 2^5 - 1 = |\mathrm{GF}(2^5)^*|$. Hence, $\mathbb{Z}_2[A_3] = GF(2^3)$ and $\mathbb{Z}_2[A_5] = GF(2^5)$ where

$$A_3 = A^{31\times151}, \qquad A_5 = A^{7\times151}.$$

As such, the minimal polynomials of A_3 and A_5 have degrees 3 and 5, respectively, so that

$$\mathrm{GF}(2^{3t}) = \mathbb{F}[A_3] \quad \text{and} \quad \mathrm{GF}(2^{5t}) = \mathbb{F}[A_5].$$

Consider a matrix

$$S = \begin{pmatrix} 0&0&0&0&0&0&0&0&0&1&0&1&1&0&0\\ 0&1&0&1&1&0&0&0&0&0&1&1&1&1&1\\ 0&0&1&0&0&1&1&0&0&1&0&0&1&0&0\\ 1&0&1&1&0&1&0&0&0&1&1&1&0&1&0\\ 0&0&1&0&0&0&0&0&0&0&0&1&1&0&0\\ 1&0&1&1&0&1&0&0&0&0&1&1&1&1&1\\ 0&0&1&1&0&0&1&1&0&0&1&0&1&0&0\\ 0&0&0&0&0&1&1&0&1&0&0&1&0&1&1\\ 1&0&1&0&0&0&1&0&1&1&0&0&0&1&0\\ 1&1&1&0&1&0&0&1&0&0&0&0&0&1&0\\ 1&0&0&0&1&1&0&0&0&1&0&1&1&1&1\\ 1&0&1&0&1&1&0&0&1&1&0&0&1&0&0\\ 0&1&1&0&0&1&0&0&0&1&1&0&0&1&0\\ 1&0&0&0&0&1&1&1&1&1&1&1&1&1&1\\ 0&1&0&1&1&1&1&1&0&0&1&0&1&0&1 \end{pmatrix} \in M_{15}(\mathbb{Z}_2) \subseteq M_{15}(\mathbb{F}).$$

One can check that S is invertible and that

$$\begin{aligned} C_{M_{15}(\mathbb{Z}_2)}(A_3) \cap C_{M_{15}(\mathbb{Z}_2)}(S^{-1}A_3S) &= C_{M_{15}(\mathbb{Z}_2)}(A_3) \cap C_{M_{15}(\mathbb{Z}_2)}(S^{-1}A_5S) \\ &= C_{M_{15}(\mathbb{Z}_2)}(A_5) \cap C_{M_{15}(\mathbb{Z}_2)}(S^{-1}A_3S) = C_{M_{15}(\mathbb{Z}_2)}(A_5) \cap C_{M_{15}(\mathbb{Z}_2)}(S^{-1}A_5S) = \mathbb{Z}_2 I. \end{aligned}$$

Observe that the dimension of the intersection of centralizers does not change under field extensions because the intersection $C(C) \cap C(D)$ corresponds to a solution of a system of homogeneous linear equations $XC - CX = XD - DX = 0$ with coefficients (i.e., matrices) C, D in the same field $\mathbb{Z}_2$. Hence, we also have

$$\begin{aligned} C_{M_{15}(\mathbb{F})}(A_3) \cap C_{M_{15}(\mathbb{F})}(S^{-1}A_3S) &= C_{M_{15}(\mathbb{F})}(A_3) \cap C_{M_{15}(\mathbb{F})}(S^{-1}A_5S) \\ &= C_{M_{15}(\mathbb{F})}(A_5) \cap C_{M_{15}(\mathbb{F})}(S^{-1}A_3S) = C_{M_{15}(\mathbb{F})}(A_5) \cap C_{M_{15}(\mathbb{F})}(S^{-1}A_5S) = \mathbb{F}I \quad (4) \end{aligned}$$

in any field extension $\mathbb{F}|\mathbb{Z}_2$ in which the polynomial $m(x)$ is irreducible.

Thus, if

$$A = X_0 — X_1 — X_2 — X_3 — X_4 = S^{-1}AS$$

is a path of length 4 in the commuting graph of $M_{15}(\mathbb{F})$, then we may assume that $\mathbb{F}[X_1] \in \{\mathbb{F}[A_3], \mathbb{F}[A_5]\}$ and we may likewise assume that $\mathbb{F}[X_3] \in \{S^{-1}\mathbb{F}[A_3]S, S^{-1}\mathbb{F}[A_5]S\}$. Note that there is no intermediate subfield between $\mathbb{F}$ and $\mathbb{F}[A_3]$, so every element in $\mathbb{F}[A_3] \setminus \mathbb{F}$ generates $\mathbb{F}[A_3]$. Similar arguments are valid for $\mathbb{F}[A_5]$. Thus, as far as commutativity is concerned, we may well assume that already $X_1 \in \{A_3, A_5\}$ and likewise $X_3 \in \{S^{-1}A_3S,\ S^{-1}A_5S\}$. Then, X_2 belongs to the intersection of the corresponding centralizers which by (4) consists of scalar matrices only, a contradiction.

Consequently, the distance between A and $S^{-1}AS$ is at least five. In combination with [7] this shows that $\operatorname{diam}\Gamma(M_{15}(\mathbb{F})) = 5$ for every finite field extension $\mathbb{F}|\mathbb{Z}_2$ in which the polynomial $m(x)$ is irreducible.

We acknowledge that all the relevant computations in this example were done by GAP, [10].

Acknowledgements We are grateful to the referee for communicating the reference [9] which simplified the proof of Lemma 2.2, and for communicating the present short version of the proof of Theorem 3.2; our initial proof was more involved.

References

[1] S. Akbari, A. Mohammadian, H. Radjavi, P. Raja, On the diameters of commuting graphs, Linear Algebra Appl. **418** (2006), 161–176.

[2] S. Akbari, H. Bidkhori, A. Mohammadian, Commuting graphs of matrix algebras. Comm. in Algebra, **36** (2008) 4020–4031.
[3] C. Ambrozie, J. Bračič, B. Kuzma, and V. Müller, The commuting graph of bounded linear operators on a Hilbert space. J. Funct. Anal. **264** (2013), no. 4, 1068–1087.
[4] R. Brauer, K.A. Fowler, On groups of even order. Ann. of Math. (2) **62** (1955), 565–583.
[5] G. Dolinar, B. Kuzma, Homomorphisms of commutativity relation. Linear Multilinear Algebra **64** (2016), No. 5, 897–922.
[6] G. Dolinar, A. Guterman, B. Kuzma, P. Oblak, Commuting graphs and extremal centralizers. Ars mathematica contemporanea **7** (2014), 453–459.
[7] D. Dolžan, D. Kokol Bukovšek, B. Kuzma, On diameter of components in commuting graphs. Linear Algebra Appl., **522** (2017) 161–174.
[8] D. Dolžan, D. Kokol Bukovšek, B. Kuzma, P. Oblak, On diameter of the commuting graph of a full matrix algebra over a finite field. Finite Fields Appl., **37** (2016), 36–45.
[9] P. L. Draxl, Skew Fields. Cambridge Univ. Press, Cambridge, (1983).
[10] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.8.8; 2017. (`https://www.gap-system.org`)
[11] M. Giudici, C. Parker, There is no upper bound for the diameter of the commuting graph of a finite group. J. Combin. Theory Ser. A **120** (2013), 1600–1603.
[12] L. C. Grove, Algebra. Academic Press, New-York, (1983).
[13] B. Kuzma, Dimensions of complex Hilbert spaces are determined by commutativity relation. submitted.
[14] R. Lidl, H. Niederreiter, Introduction to finite fields and their applications, Cambridge University Press, (1986).
[15] F. Lorenz, Algebraische Zahlentheorie, B. I. Wissenschaftsverlag, Mannheim, 1993.
[16] A. Mohammadian, On commuting graphs of finite matrix rings, Commun. Algebra **38** (2010), 988–994.
[17] G.L. Morgan, C.W. Parker, The diameter of the commuting graph of a finite group with trivial centre. Journal of Algebra **393** (2013), 41–59.
[18] T. Pisanski, Universal commutator graphs. Discrete Math. **78** (1989), no. 1–2, 155–156.
[19] Y. Shitov, A matrix ring with commuting graph of maximal diameter J. Combin. Theory Ser. A, **141** (2016), 127–135
[20] R. Solomon, A. Woldar, Simple groups are characterized by their non-commuting graphs. J. Group Theory **16** (2013), 793–824.