SWEEPING WORDS AND THE LENGTH OF A GENERIC VECTOR SUBSPACE OF $M_n(\mathbb{F})$

IGOR KLEP[⋆] AND ŠPELA ŠPENKO[†]

Abstract. The main result of this short note is a generic version of Paz' conjecture on the length of generating sets in matrix algebras. Consider a generic g-tuple $\underline{A} = (A_1, \dots, A_g)$ of $n \times n$ matrices over an infinite field. We show that whenever $g^{2d} \geq n^2$, the set of all words of degree $2d$ in $\underline{A}$ spans the full $n \times n$ matrix algebra. Our proofs use generic matrices, are combinatorial and depend on the construction of special kinds of directed multigraphs with few edge-disjoint walks.

1. Introduction

Let $\mathbb{F}$ be an infinite field and let $\mathcal{A}$ be an associative $\mathbb{F}$-algebra. Given a generating set S of $\mathcal{A}$ containing 1, let S^k denote the set of all products of the form $s_1 \cdots s_k$ with $s_i \in S$. If

$$\operatorname{span} S^{\ell-1} \subsetneq \operatorname{span} S^{\ell} = \mathcal{A},$$

we say that S has (generating) **length** ℓ. These lengths feature prominently in the study of growth of algebras and the Gelfand-Kirillov dimension [KL00, BoKr76].

A fundamental problem is to find bounds on the length of generating sets. Much activity has focused on $\mathcal{A} = M_n(\mathbb{F})$ (see e.g. [Paz84, FGG97, Pap97, LR11, Ros12]), where the best known bound on the length of generating sets is $O(n^{3/2})$, due to Pappacena [Pap97]. The Paz conjecture [Paz84] states that the bound is $2n-2$, and it is easy to see that this bound would be sharp. We refer the reader to [LS09] for the study of an analogous problem in groups.

In this short note we establish a version of Paz' conjecture in a generic setting: the length of a generic[1] generating set in $M_n(\mathbb{F})$ is $O(\log n)$ (Corollary 2.3). To prove this bound we establish the existence of "sweeping" words $w_1, \dots, w_{n^2}$ of degree $2\lceil \log_g n \rceil$ in g freely noncommuting letters $x_1, \dots, x_g$. That is, there exist (symmetric) $n \times n$ matrices $A_1, \dots, A_g$ such that $w_1(A_1, \dots, A_g), \dots, w_{n^2}(A_1, \dots, A_g)$ span $M_n(\mathbb{F})$; see Theorem 2.2. Here is a simple corollary. Given $g^{2d} \geq n^2$ consider the set of all words w of degree $2d$ in g matrices $\underline{A} \in M_n(\mathbb{F})^g$.

Date: May 3, 2016.

2010 *Mathematics Subject Classification.* Primary 16R30, 68R15; Secondary 16S50, 15A24, 47A57.

Key words and phrases. free algebra, generic matrix, discriminant, local linear independence, length of a vector space, Paz conjecture, directed multigraph.

[⋆]Supported by the Marsden Fund Council from Government funding, administered by the Royal Society of New Zealand. Partially supported by the Slovenian Research Agency grants P1-0222, L1-4292 and L1-6722. Part of this research was done while the author was on leave from the University of Maribor.

[†]Supported by the Slovenian Research Agency and the L'Oréal-UNESCO scholarship "For women in science".

[1] Here a generic property is one that holds on a Zariski dense open set.

Vectorize each matrix $w(\underline{A})$ and arrange these vectors into a matrix (of size $n^2 \times g^{2d}$). Corollary 2.4 shows that this matrix is generically of full rank, generalizing a theorem of Rosenthal [Ros12] who established the special case $d = 1$.

The key step in the proofs is the construction of special kinds of directed multigraphs with few edge-disjoint walks (Subsection 3.1). Another ingredient going into our proofs are generic matrices and their properties [Row80, GRZ03].

The paper is organized as follows. Section 2 gives notation, preliminaries, and presents our main results on sweeping words and lengths in matrix algebras. Section 3 gives proofs of our results, including the graph-theoretic construction in Subsection 3.1.

Acknowledgments. The authors thank Benoit Collins for several stimulating discussions, Jason P. Bell for sharing his expertise, and Jurij Volčič for carefully reading a preliminary version of the manuscript. They would also like to thank the referees for many helpful suggestions which considerably improved the presentation of this paper.

2. Main results

2.1. **Notation and preliminaries.** Let $\mathbb{F}$ denote an infinite field and $M_n(\mathbb{F})$ the algebra of $n \times n$ matrices over $\mathbb{F}$. We denote the free associative algebra generated by $x_1, \dots, x_g$ by $\mathbb{F}\langle x_1, \dots, x_g \rangle$. By $\langle x_1, \dots, x_g \rangle$ we denote the free monoid generated by $x_1, \dots, x_g$, and by $\langle x_1, \dots, x_g \rangle_d$ words in $\langle x_1, \dots, x_g \rangle$ of degree d. In case $g = 2$ we write x, y instead of x_1, x_2. The set $\{1, \dots, d\}$ is denoted by $\mathbb{N}_d$.

2.1.1. *Generic matrices and the discriminant.* We denote by $C = \mathbb{F}[x_{ij}^{(k)} \mid 1 \leq i, j \leq n, 1 \leq k \leq g]$ a commutative polynomial algebra. The elements $X_k = (x_{ij}^{(k)}) \in M_n(C)$, $1 \leq k \leq g$, are called **generic matrices**. The **discriminant** $\Delta(A_1, \dots, A_{n^2})$ of $n \times n$ matrices $A_1, \dots, A_{n^2}$ is the determinant of the $n^2 \times n^2$ matrix whose k-th column $v^{(k)}$ is the vectorized matrix A_k; i.e., $v^{(k)}_{(n-1)i+j} = (A_k)_{ij}$. For future use we record the identity

$$\Delta(A_1 B, \dots, A_{n^2} B) = \det(B) \Delta(A_1, \dots, A_{n^2}). \tag{2.1}$$

2.1.2. *Locally linearly independent words.* We say that $w_1, \dots, w_m \in \langle x_1, \dots, x_g \rangle$ are $M_n(\mathbb{F})$-**locally linearly independent** if $w_1(A), \dots, w_m(A)$ are linearly independent for some $A \in M_n(\mathbb{F})^g$. This concept first appeared in [CHSY03], later it has been studied algebraically in [BrKl13], and recently in [BPŠ15].

We note the following easy observation.

Lemma 2.1. Words $w_1, \dots, w_{n^2} \in \langle x_1, \dots, x_g \rangle$ are $M_n(\mathbb{F})$-locally linearly independent if and only if the discriminant of $w_1(X_1, \dots, X_g), \dots, w_{n^2}(X_1, \dots, X_g)$ is nonzero.

We say that words $w_1, \dots, w_m \in \langle x_1, \dots, x_g \rangle$ **sweep** $M_n(\mathbb{F})$ if there exists $\underline{A} \in M_n(\mathbb{F})^g$ such that $w_1(\underline{A}), \dots, w_m(\underline{A})$ span $M_n(\mathbb{F})$.

2.2. Main result on words.

Theorem 2.2. *Let $g \geq 2$ and $d = \lceil \log_g n \rceil$. Then there exist $M_n(\mathbb{F})$-locally linearly independent words $w_1, \dots, w_{n^2} \in \langle x_1, \dots, x_g \rangle_{2d}$. That is, for some $\underline{A} \in M_n(\mathbb{F})^g$ the matrices $w_1(\underline{A}), \dots, w_{n^2}(\underline{A})$ are linearly independent and thus span $M_n(\mathbb{F})$.*

2.2.1. *Length of a vector space.* Let V be a vector subspace of $M_n(\mathbb{F})$. By V^k we denote the vector space spanned by the words of degree at most k evaluated at V. The **length** of V is the integer ℓ yielding a stationary chain

$$V \subsetneq V^2 \subsetneq \cdots \subsetneq V^\ell = V^{\ell+1}.$$

Given a subset S of $M_n(\mathbb{F})^g$, a vector space $V \subseteq M_n(\mathbb{F})$ of dimension g is S**-general** if it can be spanned by elements $A_1, \dots, A_g$ satisfying $(A_1, \dots, A_g) \in S$.

Corollary 2.3 (Generic version of Paz' conjecture)**.** *Let $g \geq 2$ and let $\mathbb{F}$ be an infinite field. There exists a nonempty Zariski open subset $S \subseteq M_n(\mathbb{F})^g$ such that the length of an S-general vector subspace of $M_n(\mathbb{F})$ is of order $O(\log n)$.*

Note that if $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$, then a nonempty Zariski open subset of $\mathbb{F}^m$ is automatically dense in the Euclidean topology.

2.2.2. *Words in random matrices span the full matrix algebra.* By Corollary 2.3, given a g-tuple $\underline{A}$ of random $n \times n$ matrices, words of degree $O(\log n)$ in $\underline{A}$ span $M_n(\mathbb{F})$. In particular, we have:

Corollary 2.4. *For each g satisfying $n^2 \leq g^{2d}$ there exists a set of g matrices such that words of degree $2d$ in those matrices span $M_n(\mathbb{F})$.*

Corollary 2.4 partially answers a question posed in [Ros12], where this result is established in the case $d = 1$. The answer is complete for $n \in \mathbb{N}$ satisfying $g^{2d-1} < n^2 \leq g^{2d}$. The question whether the words of degree $2d-1$ sweep $M_n(\mathbb{F})$ in the case $n^2 \leq g^{2d-1}$ remains.

3. Proofs

The proof of Theorem 2.2 reduces to the study of special kinds of graphs which we introduce in the first subsection. The main ideas can be revealed already in the case of two variables, and the general case is only notationally more difficult, so we focus on $g = 2$. In the next proposition we state for convenience this special case separately.

Proposition 3.1. *Let $d = \lceil \log_2 n \rceil$. There exist $M_n(\mathbb{F})$-locally linearly independent words $w_1, \dots, w_{n^2} \in \langle x, y \rangle_{2d}$.*

3.1. Graphs.

We recursively construct a family of graphs $(G_d)_{d \in \mathbb{N}}$. Let G_0 be a graph with one vertex labeled by 1 and no edges. We let G_d be a (directed) graph with 2^d vertices labeled by $\mathbb{N}_{2^d}$, and define the edges as follows. There is a (directed) edge from i to j in G_d of multiplicity $4e$ for $1 \leq i, j \leq 2^{d-1}$, if there is an edge of multiplicity e from i to j in G_{d-1}. Moreover, each vertex i for $1 \leq i \leq 2^{d-1}$ has additionally 2^{d+1} loops, and there are 2^d edges from i to $i+2^{d-1}$ and back for $1 \leq i \leq 2^{d-1}$. We label the loops by x, and other edges by y. Note that G_d contains $2^{2d+1}d$ edges, half of them labeled by x and the other half by y.

For example, the figures below show G_1 and G_2 with the numbers on edges corresponding to their respective multiplicities, and instead of the labels x and y we use dashed (resp. solid) edges for the edges corresponding to x (resp. y).

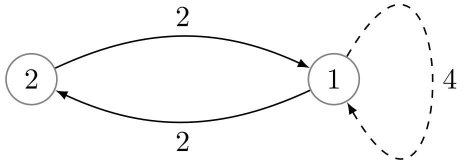

FIGURE 1. G_1

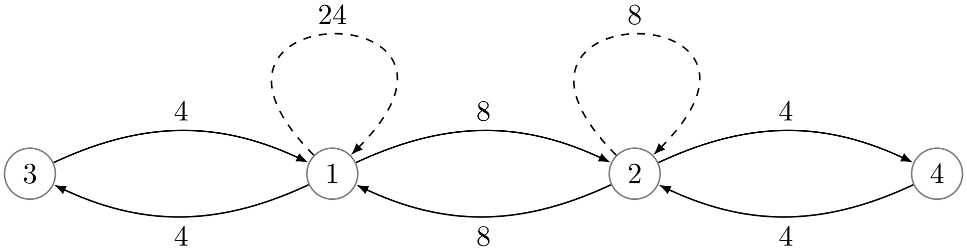

FIGURE 2. G_2

If p is a walk in the graph G_d then we associate to it a word corresponding to the labels on the edges passed by p in the respective order. When partitioning a graph into (edge-disjoint) walks we do not distinguish between the directed edges connecting the same vertices (i.e., two walks are considered the same if the associated words are equal).

We now state a technical lemma that will be used extensively in the proof of Proposition 3.1.

Lemma 3.2. The graph G_d can be partitioned uniquely into 2^{2d} (edge-disjoint) walks p_{ij} of length $2d$ for $1 \leq i,j \leq 2^d$, such that p_{ij} starts at i and ends at j, which yield all the words in $\langle x,y\rangle_{2d}$.

Proof. We prove the lemma by induction on d. Let us denote by $G_d^{(m)}$ the graph obtained from G_d by multiplying the multiplicity of each edge by m.

We claim that $G_d^{(m)}$ can be partitioned in only one way into $m2^{2d}$ walks of length $2d$ such that m walks start at i and end at j for $1 \leq i,j \leq 2^d$, and such that each word in $\langle x,y\rangle_{2d}$ corresponds to m walks. Consider first $G_1^{(m)}$. Then the only way of obtaining the desired partition is to take m walks $\{2 \to 1, 1 \to 2\}$, m walks $\{1 \to 1, 1 \to 2\}$, m walks $\{2 \to 1, 1 \to 1\}$

and m walks $\{1 \to 1, 1 \to 1\}$ as can easily be seen. Suppose that the claim holds for all graphs $G_\ell^{(m)}$, $\ell < d$. Consider now $G_d^{(m)}$. Since there are no loops on the vertices labeled by i for $2^{d-1}+1 \le i \le 2^d$, all words with the starting or ending point in these vertices need to begin, resp. end, with y. By the condition on the partition, exactly half of the walks have this property, thus words with another starting, resp. ending, point need to begin, resp. end, with x. Removing the edges starting or ending at i for $2^{d-1}+1 \le i \le 2^d$, and $m2^{d+1}$ loops on vertices i for $1 \le i \le 2^{d-1}$, we obtain a graph on 2^{d-1} vertices labeled by $\mathbb{N}_{2^{d-1}}$ (ignoring the isolated points) which coincides with $G_{d-1}^{(4m)}$ by construction, and which we need to partition into $4m2^{2(d-1)}$ walks of length $2(d-1)$ (as we have already removed the starting and the ending edge of walks in $G_d^{(m)}$) such that $4m$ walks start at i and end at j for $1 \le i, j \le 2^{d-1}$, and each word in $\langle x, y\rangle_{2d-2}$ corresponds to $4m$ walks. By the induction hypothesis, there is only one such a partition. The lemma thus follows by taking $m = 1$. ■

For the proof of Theorem 2.2 we will need a slight generalization of the previous lemma. We thus introduce a graph G_d^g which has g^d vertices and is defined recursively by setting G_0^g to be the graph with 1 vertex labeled by 1 and no edges. Having constructed G_{d-1}^g we let G_d^g be a directed graph with g^d vertices labeled by $\mathbb{N}_{g^d}$, and having a (directed) edge from i to j of multiplicity $g^2 e$, $i, j \in \mathbb{N}_{g^{d-1}}$, if there is an edge of multiplicity e from i to j in G_{d-1}^g, and is labeled as the corresponding edge in G_{d-1}^g, and there are g^d edges from i to $i + (k-1)g^{d-1}$ and back for $1 \le i \le g^{d-1}$, labeled by x_k, $1 \le k \le g$ (for $k = 1$ every loop has multiplicity g^{2d}). Note that G_d^g contains $2dg^{2d}$ edges.

Lemma 3.3. There is a unique partition of the graph G_d^g in g^{2d} (edge-disjoint) walks p_{ij} of length $2d$ for $1 \le i, j \le 2^d$, such that p_{ij} starts at i and ends at j, which yield all the words in $\langle x_1, \ldots, x_g\rangle_{2d}$.

The proof of Lemma 3.3 is a straightforward modification of Lemma 3.2 and is omitted.

3.2. **Proof of Theorem 2.2.**

Proof of Proposition 3.1. By Lemma 2.1 we need to show that

$$p(x_{11}, \ldots, x_{nn}, y_{11}, \ldots, y_{nn}) := \Delta(w_1(X, Y), \ldots, w_{n^2}(X, Y))$$

is nonzero for some $w_1, \ldots, w_{n^2} \in \langle x, y\rangle_{2d}$, where $X = (x_{ij})$, $Y = (y_{ij})$ are generic $n \times n$ matrices. (We may and we will assume that X is diagonal [Row80, Proposition 1.3.15].) By the definition of the discriminant,

$$p(x_{11}, \ldots, x_{nn}, y_{11}, \ldots, y_{nn}) = \sum_{\sigma \in S_{n^2}} (-1)^\sigma \prod_{1 \le i,j \le n} w_{\sigma(k_{ij})}(X, Y)_{ij}, \tag{3.1}$$

where $k_{ij} = (i-1)n + j$, and $w_k(X, Y)_{ij}$ denotes the commutative polynomial at the entry (i, j) of the word w_k evaluated at the tuple of generic matrices (X, Y).

Let us define the lexicographic order on $\langle x, y\rangle$ with $x > y$ and denote by v_s the vector of the words of degree s listed decreasingly with respect to this order. By v_s^t we denote its transpose.

We denote by e_{ij}, $1 \le i,j \le n$, the standard matrix units, and write $e_k = e_{11} + \cdots + e_{kk}$. Let $2^{d-1} < n \le 2^d$, $n' = n - 2^{d-1}$, and let

$$W_n = e_n v_d v_d^t e_n = \begin{pmatrix} x v_{d-1} v_{d-1}^t x & x v_{d-1} v_{d-1}^t y e_{n'} \\ e_{n'} y v_{d-1} v_{d-1}^t x & e_{n'} y v_{d-1} v_{d-1}^t y e_{n'} \end{pmatrix} \tag{3.2}$$

be the block matrix consisting of words with blocks of the size $2^{d-1} \times 2^{d-1}$, $2^{d-1} \times n'$, $n' \times 2^{d-1}$, and $n' \times n'$, respectively. The word appearing at the (i,j)-entry of W_n will be denoted by $W_{n,ij}$.

We proceed to find a monomial that appears in the product on the right-hand side of (3.1) for a unique $\sigma \in S_{n^2}$. We write $x_i = x_{ii}$ and define

$$r_{n,ij} = \begin{cases} x_i x_j & \text{if } 1 \le i,j \le 2^{d-1}, \\ x_i y_{j-2^{d-1},j} & \text{if } 1 \le i \le 2^{d-1}, 2^{d-1} < j \le n, \\ x_j y_{i,i-2^{d-1}} & \text{if } 2^{d-1} < i \le n, 1 \le j \le 2^{d-1}, \\ y_{i,i-2^{d-1}} y_{j-2^{d-1},j} & \text{if } 2^{d-1} < i,j \le n. \end{cases}$$

We further inductively define

$$m_{1,11} = 1, \quad m_{n,ij} = m_{2^{d-1},i_d j_d} r_{n,ij},$$

where $i_d \equiv i \mod 2^{d-1}$, $j_d \equiv j \mod 2^{d-1}$, $1 \le i_d, j_d \le 2^{d-1}$. Consider the monomial defined by

$$m_n = \prod_{1 \le i,j \le n} r_{n,ij}.$$

In particular, in the case $n = 2^d$ we have

$$m_{2^d} = (m_{2^{d-1}})^4 \prod_{1 \le i,j \le 2^d} r_{2^d,ij}.$$

Let $w_{(i-1)n+j} = W_{n,ij}$ for W_n defined in (3.2). We claim that m_n appears in

$$P_n^\sigma = \prod_{1 \le i,j \le n} w_{\sigma(k_{ij})}(X,Y)_{ij}$$

only for $\sigma = \mathrm{id}$. By the construction of $m_{n,ij}, m_n$ and (3.2), $m_{n,ij}$ has a nonzero coefficient in the commutative polynomial $W_{n,ij}(X,Y)_{ij}$ and thus the same holds for the monomial m_n in

$$\prod_{1 \le i,j \le n} w_{k_{ij}}(X,Y)_{ij} = \prod_{1 \le i,j \le n} W_{n,ij}(X,Y)_{ij}.$$

It remains to show that m_n does not appear in P_n^σ for $\sigma \ne \mathrm{id}$. For this we use graph-theoretic language.

We first consider the case $n = 2^d$. We can present the monomial m_n as a graph on n vertices, in which there is a directed edge of multiplicity s_{ij} between vertices i and j labeled by y if s_{ij} is the degree of y_{ij} in the monomial m_n, and there are s_i loops on the vertex i labeled by x if s_i is the degree of x_i in m_n. It follows by the (inductive) definition of m_n that the associated graph is G_d. Since m_n needs to be written as a product of n^2 monomials u_{ij}, $1 \le i,j \le n$, arising from monomials in $w_{\sigma(k_{ij})}(X,Y)_{ij}$, $w_{k_{ij}} \in \langle x,y \rangle_{2d}$, our problem reduces to finding partitions of the graph associated to m_n into n^2 walks p_{ij}, $1 \le i,j \le n$, of length $2d$ that yield all the words in $\langle x,y\rangle_{2d}$. Lemma 3.2 asserts that there is only one such partition, and thus concludes the proof in the case $n = 2^d$.

For arbitrary n we observe that if

$$\sum_{\sigma \in S_{n^2}} (-1)^\sigma \prod_{1\le i,j\le n} w_{\sigma((i-1)n+j)}(X,Y)_{ij}$$

equaled 0 then m_n would appear in P_n^{id} and in some other P_n^{ρ} with $\rho \in S_{n^2}$. As $m_{n,ij}$ can be identified with $m_{2^d,ij}$ for $1 \le i,j \le n$, m_{2^d} would have a nonzero coefficient in the product $P_{2^d}^{\sigma}$ for $\sigma = \mathrm{id}$ and $\sigma = \tilde\rho \in S_{2^d}$ (here $\tilde\rho$ is the permutation in S_{2^d} induced by ρ and fixing all $i > n$), which is impossible by the claim proved in the previous paragraph. Thus the words $W_{n,ij}$, $1 \le i,j \le n$, are $M_n(\mathbb{F})$-locally linearly independent. $\blacksquare$

Proof of Theorem 2.2. One follows the steps of the proof of Proposition 3.1 where initially one needs to consider the case $n = g^d$, and defines the monomial m_n inductively corresponding to the matrix

$$W_n = e_n v_d v_d^t e_n = \begin{pmatrix} x_1 v_{d-1} v_{d-1}^t x_1 & \dots & x_1 v_{d-1} v_{d-1}^t x_{g-1} & x_1 v_{d-1} v_{d-1}^t x_g e_{n'} \\ \vdots & \ddots & \vdots & \vdots \\ x_{g-1} v_{d-1} v_{d-1}^t x_1 & \dots & x_{g-1} v_{d-1} v_{d-1}^t x_{g-1} & x_{g-1} v_{d-1} v_{d-1}^t x_g e_{n'} \\ e_{n'} x_g v_{d-1} v_{d-1}^t x_1 & \dots & e_{n'} x_g v_{d-1} v_{d-1}^t x_{g-1} & e_{n'} x_g v_{d-1} v_{d-1}^t x_g e_{n'} \end{pmatrix}, \tag{3.3}$$

where $g^{d-1} < n \le g^d$, $n' = n - g^{d-1}$, and v_s denotes the vector of g^s words of degree s listed decreasingly in the monomial order induced by setting $x_1 > \cdots > x_g$. Instead of applying Lemma 3.2 one concludes the proof by applying Lemma 3.3. $\blacksquare$

Proof of Corollary 2.3. Let $w_1,\dots,w_{n^2}$ be the $M_n(\mathbb{F})$-locally linearly independent words of degree $2d = 2\lceil \log_g n\rceil$ whose existence was established in Theorem 2.2. As then the discriminant $\Delta := \Delta(w_1(X_1,\dots,X_g),\dots,w_{n^2}(X_1,\dots,X_g))$ is nonzero, the subset S of $\underline{A} \in M_n(\mathbb{F})^g$ where Δ does not vanish is a nonempty Zariski open subset, and therefore dense in $M_n(\mathbb{F})^g$. In the case $\mathbb{F} \in \{\mathbb{R},\mathbb{C}\}$, S is also dense in the Euclidean topology. By the definition of S it follows that every S-general vector subspace of $M_n(\mathbb{F})$ is of length $O(\log n)$. Indeed, the upper bound is $2\lceil\log_g n\rceil$, while the lower bound is $\lceil \log_g n^2\rceil$ (as the dimension of $M_n(\mathbb{F})$ equals n^2). $\blacksquare$

Proof of Corollary 2.4. Let $w_1,\dots,w_{n^2}$, Δ, and S be as in the proof of Corollary 2.3. Choose $A_1,\dots,A_m$ such that $(A_1,\dots,A_m) \in S \subseteq M_n(\mathbb{F})^m$, where m is the least $k \in \mathbb{N}$ satisfying $k^d \ge n$. For the remaining $A_{m+1},\dots,A_g$ take arbitrary $n\times n$ matrices. As the set S is Zariski open, we can further require that $\det(A_1) \ne 0$. Let $r = 2d - 2\lceil \log_m n\rceil$. Then $w_i x_1^r$, $1 \le i \le n^2$, are words of degree $2d$. As $\Delta(w_1(X_1,\dots,X_g)x_1^r,\dots,w_{n^2}(X_1,\dots,X_g)x_1^r) = \det(X_1^r)\Delta$, which is nonzero when evaluated at $(A_1,\dots,A_g)$, the words $w_i x_1^r$ for $1 \le i \le n^2$, evaluated at $(A_1,\dots,A_g)$ span $M_n(\mathbb{F})$. $\blacksquare$

Remark 3.4. (a) It is not difficult to see that one can take the matrices in Corollary 2.4 to be symmetric. One only needs to note that the proof of Lemma 3.3 also works for the undirected version of the graphs G_d^g and then use these in the proof of Theorem 2.2.

(b) The proof of Proposition 3.1 also leads to an explicit construction of $n \times n$ matrices such that words of degree $2d = 2\lceil \log_g n \rceil$ in these matrices span $M_n(\mathbb{F})$. We give an example in characteristic 0. Keep the notation from the proof of Corollary 2.4. Let $M = n!(n^{2d-1})^n$. We set all variables that do not appear in m_n to zero, and denote by C' the polynomial algebra in the remaining variables. Let us order the variables as follows: $x^{(k)}_{i,i+(k-1)m^{s-1}} < x^{(\ell)}_{j,j+(k-1)m^{t-1}}$, (resp. $x^{(k)}_{i,i+(k-1)m^{s-1}} < x^{(\ell)}_{j+(k-1)m^{t-1},j}$), if $(s,k,i) < (t,\ell,j)$ (resp. $(s,k,i) \leq (t,\ell,j)$) in the lexicographic order, and take the corresponding lexicographic ordering on C'. Let

$$c_1 = 3, \quad c_s = 2m^{s-1}(m-1) + m^{s-2} \ \ (s > 1), \quad c = \sum_{s=1}^{d} c_s.$$

We further define for $g^{s-2} < i \leq m^{s-1}$ and $1 \leq j \leq m^{s-1}$,

$$f_{1,s,i^+} = f_{1,s,i^-} = \sum_{t=0}^{s-1} c_t + j \ \ (m^{s-2} < j \leq m^{s-1}),$$

$$f_{k,s,j^+} = \sum_{t=0}^{s-1} c_t + m^{s-2} + 2m^{s-1}(k-2) + j, \quad f_{k,s,j^-} = \sum_{t=0}^{s-1} c_t + m^{s-2} + 2m^{s-1}(k-2) + m^{s-1} + j.$$

We set

$$A^{(k)}_{i,i+(k-1)m^{s-1}} = M^{2d(c-f_{k,s,i^+})},$$

$$A^{(k)}_{i+(k-1)m^{s-1},i} = M^{2d(c-f_{k,s,i^-})}.$$

Since the monomial m_n is the maximal monomial in C', the degree of monomials appearing in $\Delta(w_1(X_1,\dots,X_g),\dots,w_{n^2}(X_1,\dots,X_m))$ is $2d$, and there appear at most M monomials in Δ (counted with multiplicity). It is easy to see that the constructed $A^{(k)}$, $1 \leq k \leq m$, and arbitrary $A^{(k)}$, $m < k \leq g$, have the desired property of Corollary 2.4.

(c) It would be interesting to know whether *arbitrary* n^2 words in x, y of fixed degree $d \geq \lceil 2\log_2 n \rceil$ sweep $M_n(\mathbb{F})$. If the answer were positive then we could deduce that a quasi-identity of $M_n(\mathbb{F})$ (see [BPŠ15] for the definition) $\sum_M \lambda_M M$ with $\deg M = d$ cannot be a sum of fewer than n^2 monomials, and this bound is sharp. This should be seen in contrast with [Row80, Exercise 7.2.3], stating that a multilinear polynomial identity of $M_n(\mathbb{F})$ cannot be a sum of fewer than 2^n monomials. However, the sharp bound is to the best of our knowledge not known.

References

[BoKr76] W. Borho, H. Kraft, Über die Gelfand-Kirillov-Dimension, *Math. Ann.* **220** (1976), 1–24. 1

[BrKl13] M. Brešar, I. Klep, A local-global principle for linear dependence of noncommutative polynomials, *Israel J. Math.* **193** (2013), 71–82. 2

[BPŠ15] M. Brešar, C. Procesi, Š. Špenko, Quasi-identities on matrices and the Cayley-Hamilton polynomial, *Adv. Math.* **280** (2015), 439–471. 2, 8

[CHSY03] J. F. Camino, J. W. Helton, R. E. Skelton, J. Ye, Matrix inequalities: a symbolic procedure to determine convexity automatically, *Int. Eq. Oper. Th.* **46** (2003), 399–454. 2

[FGG97] A. Freedman, R. Gupta, R. Guralnick, Shirshov's theorem and representations of semigroups, *Pacific J. Math.* **181** (1997), 159–176. 1

[GRZ03] A. Giambruno, A. Regev, M. Zaicev (editors), *Polynomial identities and combinatorial methods*, Marcel Dekker, 2003. 2

[KL00] G. R. Krause, T. H. Lenagan, *Growth of algebras and Gelfand-Kirillov dimension*, Amer. Math. Soc., 2000. 1

[LS09] M. Larsen, A. Shalev, Word maps and Waring type problems, *J. Amer. Math. Soc.* **22** (2009), 437–466. 1

[LR11] W. E. Longstaff, P. Rosenthal, On the lengths of irreducible pairs of complex matrices, *Proc. Amer. Math. Soc.* **139** (2011), 3769–3777. 1

[Pap97] C. J. Pappacena, An upper bound for the length of a finite-dimensional algebra, *J. Algebra* **197** (1997), 535–545. 1

[Paz84] A. Paz, An application of the Cayley-Hamilton theorem to matrix polynomials in several variables, *Linear Multilinear Algebra* **15** (1984), 161–170. 1

[Ros12] D. Rosenthal, Words containing a basis for the algebra of all matrices, *Linear Algebra Appl.* **436** (2012), 2615–2617. 1, 2, 3

[Row80] L. H. Rowen, *Polynomial identities in ring theory*, Academic Press, 1980. 2, 5, 8

Igor Klep, Department of Mathematics, The University of Auckland, New Zealand
E-mail address: igor.klep@auckland.ac.nz

Špela Špenko, Faculty of Mathematics and Physics, University of Ljubljana, Slovenia
E-mail address: spela.spenko@fmf.uni-lj.si