GROWTH IN MATRIX ALGEBRAS AND A CONJECTURE OF PÉREZ-GARCÍA, VERSTRAETE, WOLF AND CIRAC

YAROSLAV SHITOV

Abstract. Let S be a family of $n \times n$ matrices over a field such that, for some integer ℓ, the products of the length ℓ of the matrices in S span the full $n \times n$ matrix algebra. We show this for any positive integer $\ell \geqslant n^2 + 2n - 4$.

1. Introduction

The arithmetic operations with matrices remain an essential part of the language of science for the whole of observable history, but many natural and surprisingly simply looking problems still remain unresolved. This work deals with one of such questions, which has attracted a significant attention after its appearance in a well known and highly cited paper by Pérez-García, Verstraete, Wolf and Cirac [35].

Remark 1. We write $\mathrm{Mat}_n(\mathbb{F})$ to denote the algebra of all $n \times n$ matrices over a field $\mathbb{F}$. For any k and $S \subset \mathrm{Mat}_n(\mathbb{F})$, the notation S^k stands for the set of all products of the length k of the matrices in S, and $S\,\mathbb{F}$ denotes the $\mathbb{F}$-linear span of S.

Question 2. For any positive integer n, what is the smallest value $w(n)$ such that, if $S^k\,\mathbb{C} = \mathrm{Mat}_n(\mathbb{C})$ for some S and k, then also $S^{w(n)}\,\mathbb{C} = \mathrm{Mat}_n(\mathbb{C})$?

In particular, Conjecture 2 in [35] states that $w(n) \in O(n^2)$, and this surmise has been reiterated in several further studies [6, 7, 13, 22, 29, 30, 36, 37, 38, 41, 40]. The value $w(n)$ is also known as the *injectivity index* or *injectivity length*, and many authors emphasize the question of improving the known bounds on it [1, 3, 8, 9, 11, 14, 15, 17, 20, 32]. In fact, it has been well known that, if the conjectured estimate $w(n) \in O(n^2)$ is true, then this $O(n^2)$ bound is optimal [47], and the further bounds

$$n^2 - n \leqslant w(n) \leqslant n^2\,(n^2 - 1) \tag{1.1}$$

are contained in [37]. In fact, as shown in [13], the existence of $w(n)$ is immediate by classical results of algebraic geometry if no specific upper bound is required, and the authors of [13] give a higher-dimensional generalization of this result in the context of *projected entangled pair states*. The work [41] shows that the length of the $n \times n$ matrix algebra is $O(n \log n)$, and hence it is true that $w(n) \in O(n^3 \log n)$. A stronger bound $w(n) \in O(n^2 \log n)$ was obtained in [30] and remained the best general result known to this date as an $O(\log n)$ upper bound was known in the case when the family S of Question 2 is chosen generically [22, 23]. A further evidence to the conjecture $w(n) \in O(n^2)$ came from the corresponding $O(n^2)$ upper bound for the so called *primitive positive maps* [36]. Our goal is to prove the following.

Theorem 3. *For any $n \geqslant 2$, we have $w(n) \leqslant n^2 + 2n - 4$.*

2010 *Mathematics Subject Classification.* 15A03, 15A22, 94A40.
Key words and phrases. Matrix product states, Wielandt's inequality, injectivity length.

This proves a strong form of the well known Conjecture 2 in [35], which predicted that $w(n) \in O(n^2)$. In fact, our bound is almost sharp as we have $w(n) \in n^2 + O(n)$ after a comparison of Theorem 3 with the lower bound in (1.1).

2. Related work

Apart from being a natural problem in linear algebra with strong connections to other well known topics in the field, Question 2 has an utmost importance related to the development of mathematical models of contemporary quantum theory. In this section, we briefly review several contexts associated to Question 2, including its initial appearance in a celebrated paper in quantum theory [35].

Definition 4 ([21, 35, 45])**.** A *matrix product state* is a tensor

$$|\Psi\rangle = \sum_{s_1=1}^{d} \sum_{s_2=1}^{d} \ldots \sum_{s_N=1}^{d} \operatorname{tr}\left(A_{s_1}^{[1]} \cdot A_{s_2}^{[2]} \cdot \ldots \cdot A_{s_N}^{[N]}\right) \cdot |s_1\, s_2\, \ldots s_N\rangle\,,$$

where every $A_j^{[k]}$ is a $D_k \times D_{k+1}$ matrix with entries in $\mathbb{C}$, and $|s_1\, s_2\, \ldots s_N\rangle$ is the tensor which has a one at the position $(s_1\, s_2\, \ldots s_N)$ and zeros everywhere else.

In quantum theory, matrix product states are intended to characterize a system of N *sites* corresponding to a d-dimensional Hilbert space, and, as further explained in [35], a typical situation arises when the corresponding *bond* dimensions D_k do not grow with N, which allows one to make a natural assumption $D_1 = \ldots = D_N = D$. A *site-independent* state arises if the further condition

$$A_i = A_i^{[1]} = A_i^{[2]} = \ldots = A_i^{[N]}$$

is imposed for all i, and such a state is called *injective* if the mapping

$$X \longrightarrow \sum_{s_1=1}^{d} \sum_{s_2=1}^{d} \ldots \sum_{s_N=1}^{d} \operatorname{tr}\left(X A_{s_1} A_{s_2} \ldots A_{s_N}\right) \cdot |s_1\, s_2\, \ldots s_N\rangle$$

is injective for an appropriate choice of N [35], which is equivalent to the property

$$\{A_1, \ldots, A_d\}^N\, \mathbb{C} = \operatorname{Mat}_D(\mathbb{C}), \tag{2.1}$$

and hence this explains the connection to Question 2. The relevance of the study of injective states $|\Psi\rangle$ is briefly explained by the possibility of an explicit construction of a frustration-free local parent Hamiltonian with a unique ground state for every such $|\Psi\rangle$ as in [35, 46], and, indeed, there are hundreds of subsequent publications that deal with this concept [3, 8, 9, 11, 14, 22, 32, 43]. Here, a potential improvement of an upper bound on the *injectivity length*, which can be thought of as the smallest N for which the condition (2.1) becomes possible, would give a new bound on the number of sites for which the ground space of the corresponding parent Hamiltonian should be exactly equal to the vector space generated by a basis of normal tensors of the initial tensor [11, 35]. One further application arises from the fact that the injectivity length is an upper bound for the index of primitivity of the so-called *transfer operator* associated to a given matrix product state [8, 10]. Concerning the bond dimensions of the potential matrix product state descriptions in several specifically relevant cases such as the W-state, an improvement of an upper bound on $w(n)$ may imply a stronger lower bound on such dimensions, which is put as an additional motivation to conjecture $w(n) \in O(n^2)$ in [35], and which is further explained in [6, 7, 15]. As to the connection of $w(n)$ to classical topics in matrix theory, many authors point out to an analogy with the following result.

Definition 5. A square matrix A with nonnegative real entries is called *primitive* if, for some positive integer k, the power A^k has all entries positive. In this case, the smallest k for which this happens is called the *index of primitivity* of A.

Theorem 6 (Wielandt's inequality [47])**.** *If A is an $n \times n$ primitive matrix, then the index of primitivity of A is at most $n^2 - 2n + 2$.*

An interested reader could proceed with [37, Section II] for a detailed description of the similarities between the indexes of injectivity, for matrix product states, and primitivity, for primitive matrices, which explains the term *'quantum Wielandt'* in the study of the lower bounds for the quantity $w(n)$ as suggested in several dozens of further papers [14, 16, 29, 36]. For the purpose of this introduction, we briefly note that the number $w(n)$ gives an upper bound to the so-called *primitivity index* of a *quantum channel* $\mathrm{Mat}_n(\mathbb{C}) \to \mathrm{Mat}_n(\mathbb{C})$ implemented with a family of $n \times n$ Kraus operators [1, 37], and, following the exposition in [37, Section II], we explain how do the primitivity indexes of primitive matrices imply lower bounds on $w(n)$. To this end, we first remark that the result of Theorem 6 is sharp.

Example 7 (see page 648 in [47])**.** The index of primitivity of the $n \times n$ matrix

$$\left(\sum_{i=1}^{n-1} |i\rangle \langle i+1| \right) + |n\rangle \langle 1| + |n\rangle \langle 2|$$

is n^2-2n+2, where $|i\rangle$ and $\langle i|$ are the column and row i-th unit vectors, respectively.

Indeed, as explained in [37, Proposition 2.2], the primitivity index of an $n \times n$ primitive matrix A is a lower bound on the injectivity length of the family S formed by the matrix units at the nonzero entries of A. In particular, the family

$$S = \{|1\rangle \langle 2|\,,\ |2\rangle \langle 3|\,,\ \ldots,\ |n-1\rangle \langle n|\} \cup \{|n\rangle \langle 1|\,,\ |n\rangle \langle 2|\}$$

certifies the above mentioned bound $w(n) \geqslant n^2 - 2n + 2$, which has further been slightly improved with a different method in [37] to have the form as in (1.1). Before we proceed with several other related topics, we recall that Wielandt's inequality has a variety of further applications in different fields ranging from graph theory and number theory [2] to Markov chains [39] and numerical analysis [44].

The studies related to the current work are also very common in algebra. Indeed, the study of growth appears in various algebraic structures, including algebras [33], groups [25], semigroups [5], Lie algebras [31], PI algebras [18] and many others. In this section, we briefly discuss one topic that is particularly close to our work.

Definition 8 ([19, 33, 34, 41])**.** The *length* of a family $S \subset \mathrm{Mat}_n(\mathbb{C})$ is the smallest number k such that the linear span $id\,\mathbb{C} + S\,\mathbb{C} + S^2\,\mathbb{C} + \ldots + S^k\,\mathbb{C}$ coincides with the algebra generated by S. The length of the algebra $\mathrm{Mat}_n(\mathbb{C})$ is the maximal value $\lambda(n)$ that appears as the length of any generating family of $\mathrm{Mat}_n(\mathbb{C})$.

Remark 9. The earlier progress includes the inequalities

$$\lambda(n) \leqslant n^2/3 + O(1) \text{ in [34]}, \quad \lambda(n) \leqslant \sqrt{2}\, n^{3/2} + O(n) \text{ in [33]}$$

and the current bound $\lambda(n) \leqslant 2n \log_2 n + 4n$ in [41]. A conjecture of Paz [34] implies $\lambda(n) = 2n - 2$, and the corresponding lower bound $\lambda(n) \geqslant 2n - 2$ is known [24].

Indeed, the definition of $\lambda(n)$ is obtained from the one of $w(n)$ by replacing the expressions such as $S^t\,\mathbb{C} = \mathrm{Mat}_n(\mathbb{C})$ with $id\,\mathbb{C} + S\,\mathbb{C} + S^2\,\mathbb{C} + \ldots + S^t\,\mathbb{C} = \mathrm{Mat}_n(\mathbb{C})$. Despite this noticeable similarity, the values $\lambda(n)$ and $w(n)$ seem only to have been studied separately until it has been noted that an $O(f(n))$ bound for $\lambda(n)$ implies an $O(n^2 \cdot f(n))$ bound for $w(n)$ as in [30], and, in turn, the paper [30] applies the method that was initially developed to work with $\lambda(n)$ in [41] to get the inequality

$$w(n) \leqslant 2n^2 \cdot (6 + \log_2 n) \in O(n^2 \log n),$$

which remained the strongest upper bound on $w(n)$ known to this date.

3. Hereditary languages, advantages and obstructions

In a fashion similar to how the work [30] demonstrates the power of a method introduced in an earlier study of the length [41], the current piece is, in turn, a remarkable example of the use of a technique—widely known in the works on the length—in the quantum version of Wielandt's inequality. Indeed, apart from a significant independent interest found in the study of *hereditary properties* of words [4], a related technique has been used by Pappacena [33] to give a back then best known upper bound on the length of matrix algebras, and a similar approach has been developed in several further works on the length [26, 27, 28]. Although the proof of our main result is self-contained, it does also employ this framework, which is also known as the study of *hereditary languages* [5] or *factorial languages* [12].

A standard part of the technique is to consider an arbitrary total ordering on a basis of the linear span of a given family S as in Question 2 and proceed with the inherited lexicographic order on the words with the letters in this basis. As we explain below, the lexicographically smallest basis $\mathcal{L}(q)$ of the space $S^q\,\mathbb{F}$ becomes well behaved because the property $\dim \mathrm{Mat}_n(\mathbb{F}) = n^2$ implies $\mathcal{L}(q) = n^2$ for large q, and hence several basic techniques of hereditary languages with bounded growth apply [4]. In contrast, a similar natural approach to the length computation would require one to consider the lexicographically smallest bases of

$$(S^q\,\mathbb{F}) \,/\, \big(id\,\mathbb{F} + S\,\mathbb{F} + S^2\,\mathbb{F} + \ldots + S^{q-1}\,\mathbb{F}\big) \tag{3.1}$$

instead of $S^q\,\mathbb{F}$, and the obstruction arises as the spaces (3.1) are zero whenever q is sufficiently large, which means that the corresponding hereditary languages are finite and hence potentially much harder to describe. Furthermore, the setting of the current paper allows us to show that, for all sufficiently large q, the words in $\mathcal{L}(q)$ are uniquely determined by a portion of several letters in the beginning and several letters in the end that total to at most $n^2 + O(1)$ positions, and the corresponding middle parts of these words are periodic with the periods not exceeding n.

This explains the language theoretic difference of our approach with the methods applied in [26, 27, 28, 33]. We proceed with the technical part of the paper.

4. The proof

In this section, we work over an arbitrary field $\mathbb{F}$, and we write S to denote a fixed linearly independent family $(s_1, \ldots, s_\mu)$ of square matrices of the order $n \geqslant 2$ with entries in $\mathbb{F}$ so that the condition $S^k\,\mathbb{F} = \mathrm{Mat}_n(\mathbb{F})$ holds for some k. We begin with some standard notation and basic observations required in our approach.

Remark 10. We write Λ to denote the smallest integer with $S^\Lambda\,\mathbb{F} = \mathrm{Mat}_n(\mathbb{F})$.

Remark 11. The set of all words in the alphabet $\{s_1, \ldots, s_\mu\}$ is denoted $\Sigma^*(S)$. The length $|w|$ of a word $w \in \Sigma^*(S)$ is the number of its letters, the notation uv stands for the concatenation of two words $u, v \in \Sigma^*(S)$, and a word v' is said to be a *subword* of $v \in \Sigma^*(S)$ if there are $u, w \in \Sigma^*(S)$ such that $v = uv'w$.

Remark 12. We define the map $\pi : \Sigma^*(S) \to \mathrm{Mat}_n(\mathbb{F})$ as the corresponding product of the matrices, that is, strictly speaking, we take $\pi(e) = \mathrm{id}$ for an empty word e, $\pi(s_i) = s_i$ for the words of length one, and $\pi(uv) = \pi(u) \cdot \pi(v)$ for all $u, v \in \Sigma^*(S)$.

Remark 13. We consider the natural lexicographic ordering of the words of equal lengths in $\Sigma^*(S)$. More precisely, we write $u \leqslant v$ for two words $u, v \in \Sigma^*(S)$ if $|u| = |v|$ and at least one of the following conditions holds:

- $u = v$,
- $u = s_i\, u'$ and $v = s_j\, v'$ with $i < j$,
- $u = s_i\, u'$ and $v = s_i\, v'$ with $u' \leqslant v'$.

Remark 14. As usual, we write $u < v$ whenever $u \leqslant v$ and $u \neq v$.

In a study of the lengths of matrix algebras, Pappacena [33] defined a *reducible* word to be the one that can be written as a linear combination of the words of the smaller lengths. In the current setting, a powerful alternative is the following.

Definition 15. A word $w \in \Sigma^*(S)$ is called *basic* if

$$\pi(w) \notin \sum_{w' < w} \pi(w')\, \mathbb{F}.$$

We write $\mathcal{L}(q)$ to denote the set of all basic words of the length q, and the notation $\mathcal{L}$ stands for the family of all basic words of any length.

Remark 16. We note that $\mathcal{L}$ is a *factorial language*, which means that, for any word $w \in \mathcal{L}$ and any subword w' of w, we must have $w' \in \mathcal{L}$ as well.

Remark 17. In what follows, for any $w \in \Sigma^*(S)$ and $p \in \{0, 1, \ldots, |w|\}$, we define the *p-head* of w as the word formed with the first p letters of w.

Definition 18. A pair (p, q) of positive integers is a *steady position* if $p \leqslant q$ and the p-th letter of a word $w \in \mathcal{L}(q)$ is uniquely identified by the $(p-1)$-head of w. In other words, this means that, for any two words $w, w' \in \mathcal{L}(q)$ which have the same $(p-1)$-heads, the p-th letters of w and w' are equal as well.

Observation 19. *If (p, q) is steady, then both $(p, q+1)$ and $(p+1, q+1)$ are steady.*

Proof. Immediate because $\mathcal{L}$ is a factorial language. □

Observation 20. *If, for some positive integers p and q, none of the positions*

$$(1, q),\ (2, q),\ \ldots,\ (p, q)$$

is steady, then the words in $\mathcal{L}(q)$ admit at least $p + 1$ different p-heads.

Proof. A straightforward induction. □

Our next goal is a structural characterization of the language $\mathcal{L}(q)$ with large q. In what follows, the notation $\mathrm{col}\, A$ refers to the family of the columns of a matrix A, and we recall that Λ is the smallest integer satisfying $S^\Lambda\, \mathbb{F} = \mathrm{Mat}_n(\mathbb{F})$.

Lemma 21. *Let $g \geqslant 1$ and $\Lambda' \geqslant \Lambda$ be integers, let $\omega_1 < \ldots < \omega_t$ be the lexicographic ordering of the family of all g-heads of the words in $\mathcal{L}(\Lambda' + g)$. Then the chain*

$$O \subset \sum_{i=1}^{1} (\operatorname{col} \pi(\omega_i))\, \mathbb{F} \subset \sum_{i=1}^{2} (\operatorname{col} \pi(\omega_i))\, \mathbb{F} \subset \ldots \subset \sum_{i=1}^{t} (\operatorname{col} \pi(\omega_i))\, \mathbb{F}$$

is strictly increasing.

Proof. If, for some $j \in \{1, \ldots, t\}$, we have

$$\sum_{i=1}^{j-1} (\operatorname{col} \pi(\omega_i))\, \mathbb{F} = \sum_{i=1}^{j} (\operatorname{col} \pi(\omega_i))\, \mathbb{F}, \tag{4.1}$$

then, since $S^\Lambda\, \mathbb{F} = \operatorname{Mat}_n(\mathbb{F})$ and $\Lambda' \geqslant \Lambda$, the set

$$\sum_{i=1}^{j-1} \pi(\omega_i\, \mathcal{L}(\Lambda'))\, \mathbb{F} \tag{4.2}$$

contains every matrix M such that all the columns of M are in (4.1). In particular, again because of (4.1), the set (4.2) contains all matrices of the form $\pi(u)$ provided that ω_j is the g-head of u, which means that ω_j cannot be the g-head of a word in $\mathcal{L}(\Lambda' + g)$ due to Definition 15. A contradiction to the assumptions of the lemma shows that, indeed, the desired chain of the inclusions is strictly increasing. □

Lemma 22. *At least of the positions*

$$(1, \Lambda + n),\ (2, \Lambda + n),\ \ldots,\ (\Lambda + n, \Lambda + n)$$

is steady. If h is the smallest index such that $(h+1, \Lambda+n)$ is steady, then $h \leqslant n-1$. Moreover, if $w_1 < \ldots < w_\tau$ is the lexicographic ordering of the family of all h-heads of the words in $\mathcal{L}(\Lambda + n)$, the chain of the inclusions

$$O \subset \sum_{i=1}^{1} (\operatorname{col} \pi(w_i))\, \mathbb{F} \subset \sum_{i=1}^{2} (\operatorname{col} \pi(w_i))\, \mathbb{F} \subset \ldots \subset \sum_{i=1}^{\tau} (\operatorname{col} \pi(w_i))\, \mathbb{F}$$

is strictly increasing.

Proof. By Lemma 21, there are at most n different n-heads in $\mathcal{L}(\Lambda + n)$. Therefore, at least one of the positions $(1, q)$, $(2, q)$, …, (n, q) is steady by Observation 20, and the strict monotonicity of the chain follows again from Lemma 21. □

Remark 23. In what follows, we use the symbols h and $(w_1, \ldots, w_\tau)$ exclusively to denote the values appearing in Lemma 22.

Remark 24. If the matrix s_1 is invertible, then $h = 0$.

Remark 25. We have $h < \tau \leqslant n$ immediately from Lemma 22.

Corollary 26. *For any integer $q \geqslant \Lambda + n$, the family of all h-heads of the words in $\mathcal{L}(q)$ is exactly equal to $\{w_1, \ldots, w_\tau\}$.*

Proof. As q increases from $\Lambda + n$ and gets large, no new member can show up in the family of the h-heads of the words in $\mathcal{L}(q)$ because $\mathcal{L}$ is a factorial language, and no member can disappear in view of Lemma 22. □

As we can further see in Lemma 22, the languages $\mathcal{L}(q)$ admit steady positions with all sufficiently large q. However, if the corresponding chain is not required to be strictly increasing, one can find a steady position already in $\mathcal{L}(n^2)$.

Observation 27. *There exists an index p such that (p, n^2) is a steady position.*

Proof. Otherwise, Observation 20 implies $|\mathcal{L}(q)| \geqslant n^2 + 1$. Since $\mathcal{L}(q) \subset \mathrm{Mat}_n(\mathbb{F})$, the set $\mathcal{L}(q)$ should be linearly dependent, but Definition 15 denies this. □

Remark 28. In what follows, we write $\overline{p}$ to denote the smallest index so that $(\overline{p}, n^2)$ is a steady position. In view of Observation 19 and Corollary 26, we have $\overline{p} \geqslant h+1$.

For large q, a relevant characterization of $\mathcal{L}(q)$ can be given with Lemma 22 and an adaptation of a standard technique in the study of factorial languages [4].

Lemma 29. *There exist $\rho_1, u_1, \ldots, \rho_\tau, u_\tau \in \mathcal{L}$ such that*

(o) $|u_i| \geqslant h$, and the h-head of u_i is w_i for all $i \in \{1, \ldots, \tau\}$,
(i) $|\rho_i| \in \{1, \ldots, \tau\}$, $|u_i| \leqslant h + \tau - |\rho_i| - 1 + \lfloor |\rho_i|/\tau \rfloor$ for all $i \in \{1, \ldots, \tau\}$,
(ii) for any integer $m \geqslant 1$, we have

$$\mathcal{L}(\Lambda + m\tau + 3n) \subseteq (u_1(\rho_1)^m \mathcal{L}(\delta_1)) \cup \ldots \cup (u_\tau(\rho_\tau)^m \mathcal{L}(\delta_\tau))$$

with $\delta_i = \Lambda + 3n - |u_i| + m(\tau - |\rho_i|)$, again for all $i \in \{1, \ldots, \tau\}$.

Proof. Using Lemma 22, we get the following conclusions for $\mathcal{L}(\Lambda + n + 1)$:

- the $(1 + h)$-th letter of any word $\omega \in \mathcal{L}(\Lambda + n + 1)$ is uniquely determined from the given h-head of ω,
- for the word w' obtained by taking h consecutive letters starting from the second letter in ω, we have $w' \in \{w_1, \ldots, w_\tau\}$.

In particular, we can define the mapping

$$\Omega : \ \{w_1, \ldots, w_\tau\} \to \{w_1, \ldots, w_\tau\}$$

by declaring that Ω sends the h-head of any word ω as above to its corresponding word w'. Since the language $\mathcal{L}$ is factorial, this implies that, for any integer $r' \geqslant 1$, for any $i \in \{1, \ldots, \tau\}$, and for any $u \in \mathcal{L}(\Lambda + n + r')$ such that w_i is the h-head of u, the word $\Omega^{r-1}(w_i)$ appears to be the subword of u obtained by taking h consecutive letters starting from any position $r \in \{1, \ldots, r' + 1\}$. Here, the sequence

$$w_i = \Omega^0(w_i), \ \Omega^1(w_i), \ \Omega^2(w_i), \ \Omega^3(w_i), \ \ldots \tag{4.3}$$

gives the iterations of Ω, and it remains to note that (4.3) has a period of the length $\lambda \leqslant \tau$ starting from the $(\tau - \lambda)$-th power iterate or earlier. Here, the addition of

$$\lfloor |\rho_i|/\tau \rfloor = \begin{cases} 1, & \text{if } |\rho_i| = \tau, \\ 0, & \text{otherwise} \end{cases} \tag{4.4}$$

to the upper bound on $|u_i|$ in the item (i) comes from the fact that, in the case $\lambda = \tau$, the periodic behavior of the sequence (4.3) starts from $w_i = \Omega^0(w_i)$ already, but we cannot include the h-th letter to the period ρ_i as in the item (ii) of the conclusion because u_i should be of the length at least h due to the corresponding item (o). Therefore, we should deal with the periods starting no earlier than from the first power iterate in (4.3), which explains the term (4.4) in the item (i). □

Summing up the results of Lemmas 22 and 29, we get the following.

Lemma 30. *There exist $\rho_1, u_1, \ldots, \rho_\tau, u_\tau \in \mathcal{L}$ such that*

(o) $|u_i| \geqslant h$, and the h-head of u_i is w_i for all $i \in \{1, \ldots, \tau\}$,
(i) $|\rho_i| \in \{1, \ldots, \tau\}$, $|u_i| \leqslant h + \tau - |\rho_i| - 1 + \lfloor |\rho_i|/\tau \rfloor$ for all $i \in \{1, \ldots, \tau\}$,

(ii) for any integer $q \geqslant \Lambda + 2n^2 + 3n$, there exist $\overline{\rho_1}, \ldots, \overline{\rho_\tau} \in \mathcal{L}$ such that

$$\mathcal{L}(q) \subseteq \left(u_1\,(\rho_1)^{\alpha_1}\,\overline{\rho_1}\,\mathcal{L}(n^2-\overline{p})\right) \cup \ldots \cup \left(u_\tau\,(\rho_\tau)^{\alpha_\tau}\,\overline{\rho_\tau}\,\mathcal{L}(n^2-\overline{p})\right),$$

where, for all $i \in \{1, \ldots, \tau\}$, we have $|\overline{\rho_i}| = \beta_i$ with (α_i, β_i) being the unique integers satisfying $q - n^2 - |u_i| + \overline{p} = \alpha_i \cdot |\rho_i| + \beta_i$ and $\beta_i \in \{0, 1, \ldots, |\rho_i| - 1\}$,

(iii) the chain of the inclusions

$$O \subset \sum_{i=1}^{1} (\operatorname{col}\pi(u_i))\,\mathbb{F} \subset \sum_{i=1}^{2} (\operatorname{col}\pi(u_i))\,\mathbb{F} \subset \ldots \subset \sum_{i=1}^{\tau} (\operatorname{col}\pi(u_i))\,\mathbb{F}$$

is strictly increasing.

Proof. We take $\rho_1, u_1, \ldots, \rho_\tau, u_\tau \in \mathcal{L}$ as in Lemma 29, so the items (o) and (i) in the current lemma are immediate from the items (o) and (i) of Lemma 29. Also, the point (iii) follows from Lemma 22 and the point (ii) of Lemma 29, so we can focus on the remaining point (ii) of the current lemma. Indeed, we apply Observation 19 to the integer $\overline{p}$ as in Remark 28, and we conclude that the positions

$$(\overline{p}, q),\ (\overline{p}+1, q),\ \ldots,\ (q - n^2 + \overline{p}, q) \tag{4.5}$$

are all steady. Similarly, Observation 19 and Lemma 22 show that the positions

$$(h+1, q),\ (h+2, q),\ \ldots,\ (n^2+1, q) \tag{4.6}$$

are steady as well. Taking the union of the families (4.5) and (4.6), we conclude that the letters at the positions $\{h+1, h+2, \ldots, q - n^2 + \overline{p}\}$ in a word in $\mathcal{L}(q)$ are determined by the h-head of that word. Further, in view of Corollary 26 and the item (ii) of Lemma 29, for any integer $m \geqslant 1$, we have

$$u_i\,(\rho_i)^m \in \mathcal{L}. \tag{4.7}$$

We take $m \geqslant q$ to arrange it that the lengths of such words are at least q, and, since the language $\mathcal{L}$ is factorial, we conclude that the q-heads of the words (4.7) appear in $\mathcal{L}(q)$, which is sufficient to pass to the item (ii) of the current lemma. □

We need one further simple general observation to complete the proof. We write $\operatorname{rows} M$ to denote the set of all rows of a matrix M, and, for two matrix families A and B, we write $A \cdot B$ to denote the set of all products $a \cdot b$ with $a \in A$ and $b \in B$. Also, we write $\operatorname{Mat}(m, n, \mathbb{F})$ to denote the set of all $m \times n$ matrices over $\mathbb{F}$.

Observation 31. *Let $M \in \operatorname{Mat}(p, n, \mathbb{F})$, $M' \in \operatorname{Mat}(p', n, \mathbb{F})$ satisfy $\operatorname{rk} M' = p'$ and $(\operatorname{rows} M')\,\mathbb{F} \subseteq (\operatorname{rows} M)\,\mathbb{F}$. Then, for any subset $H \subset \operatorname{Mat}_n(\mathbb{F})$,*

$$M \cdot H\,\mathbb{F} = \operatorname{Mat}(p, n, \mathbb{F}) \ \textit{ implies } \ M' \cdot H\,\mathbb{F} = \operatorname{Mat}(p', n, \mathbb{F}).$$

Proof. We have $M' = CM$ with some $p' \times p$ matrix of the rank p' over $\mathbb{F}$, and the result follows as $X \to CX$ is a surjective mapping $\operatorname{Mat}(p, n, \mathbb{F}) \to \operatorname{Mat}(p', n, \mathbb{F})$. □

We proceed with the finale of the argument.

Lemma 32. *Let $(\rho_1, u_1, \ldots, \rho_\tau, u_\tau)$ be as in Lemma 30. If $x_i \geqslant 0$ is an integer and b_i is the smallest integer satisfying $b_i \cdot |\rho_i| \geqslant h$, for all $i \in \{1, \ldots, \tau\}$, then*

$$\operatorname{Mat}_n(\mathbb{F}) = \left(\bigcup_{i=1}^{\tau} \pi\left(u_i\,(\rho_i)^{b_i}\,\mathcal{L}(n^2-\overline{p})\,\mathcal{L}(x_i)\right)\right)\mathbb{F}. \tag{4.8}$$

Proof. Using the item (iii) of Lemma 30, we split $\mathbb{F}^n$ into a direct sum of τ non-zero subspaces $V_1, V_2, \ldots, V_\tau$ so that, for any $j \in \{1, \ldots, \tau\}$, we have

$$\sum_{i=1}^{j} V_i = \sum_{i=1}^{j} (\operatorname{col}\pi(u_i))\,\mathbb{F}.$$

Further, we write the matrices in S in the basis corresponding to $(V_1, V_2, \ldots, V_\tau)$, and hence we get a sequence of non-empty pairwise disjoint sets $(I_1, \ldots, I_\tau)$ whose union is $\{1, \ldots, n\}$, and, for any $j \in \{1, \ldots, \tau\}$, all entries outside the rows $I_1 \cup \ldots \cup I_j$ are zero in $\pi(u_j)$. For any such j, we define M_j as the $|I_j| \times n$ matrix formed by taking the I_j rows of $\pi(u_j)$, and we are going to complete the proof by showing

$$M_j \cdot \pi(\rho_j)^{b_j} \cdot S^{n^2-\overline{p}}\,\mathbb{F} = \operatorname{Mat}\left(|I_j|, n, \mathbb{F}\right). \tag{4.9}$$

Indeed, for any nonnegative integer x, we have

$$\operatorname{Mat}\left(|I_j|, n, \mathbb{F}\right) \cdot S^x\,\mathbb{F} = \operatorname{Mat}\left(|I_j|, n, \mathbb{F}\right),$$

and hence, if the condtion (4.9) is true, the right hand side of (4.8) contains a matrix with the arbitrarily chosen entries in the I_j rows and with all entries outside the $I_1 \cup I_2 \cup \ldots \cup I_j$ rows zero. Since $j \in \{1, \ldots, \tau\}$ is arbitrary, we can express any $n \times n$ matrix as a linear combination of the matrices on the right hand side of (4.8), which confirms that the validity of (4.9) is sufficient to complete the proof.

In order to proceed with the proof of the condition (4.9), we define

$$D_j = \sum_{\varkappa=0}^{+\infty} \operatorname{rows}\left(M_j \cdot \pi(\rho_j)^{\varkappa}\right)\,\mathbb{F}, \tag{4.10}$$

where the 0-th power of a square matrix is the identity of the same size, and we get

$$D_j \cdot \pi(\rho_j) \subseteq D_j \tag{4.11}$$

immediately. Further, by the item (ii) of Lemma 30, we get the property

$$D_j \cdot \pi(w_\theta) = O, \text{ for any } \theta \in \{1, 2, \ldots, \widetilde{\jmath} - 1\}, \tag{4.12}$$

where the choice of the index $\widetilde{\jmath} \in \{1, \ldots, \tau\}$ satisfying the condition that

$$w_{\widetilde{\jmath}} \text{ equals the } h\text{-head of } (\rho_j)^{b_j}$$

is possible because $\mathcal{L}$ is factorial. In particular, the condition (4.12) implies

$$\Delta_j \cdot \pi(\rho_j)^m \cdot \operatorname{Mat}_n(\mathbb{F}) = \Delta_j \cdot \pi(\rho_j)^{b_j} \cdot \operatorname{Mat}_n(\mathbb{F}) \text{ for all integers } m \geqslant b_j \tag{4.13}$$

due to the item (ii) of Lemma 30, where Δ_j is an arbitrarily fixed matrix with the linearly independent rows so that $D_j = (\operatorname{rows}\Delta_j)\,\mathbb{F}$. Further, we can consider the restriction of the linear mapping $\{X \to X \cdot \pi(\rho_j)\}$ to the subspace D_j due to the inclusion (4.11), and the rank of the m-th power of such a restriction is the same for all integers $m \geqslant b_j$ because of the property (4.13). Therefore, we obtain

$$\bigcap_{\hat{\imath}=1}^{+\infty} D_j \cdot \pi(\rho_j)^{\hat{\imath}} = D_j \cdot \pi(\rho_j)^{b_j} \tag{4.14}$$

and conclude that the restriction of $\pi(\rho_j)$ on $\widetilde{D_j}$ is invertible, where $\widetilde{D_j}$ is the linear space in (4.14). In this notation, the definition (4.10) implies

$$\operatorname{rows}\left(M_j \cdot \pi(\rho_j)^{b_j}\right) \subseteq \widetilde{D_j} \tag{4.15}$$

immediately, and, also,

$$\text{the rows of } M_j \cdot \pi(\rho_j)^{b_j} \text{ are linearly independent} \tag{4.16}$$

by the item (ii) of Lemma 30. Now we define d_j as the dimension of $\widetilde{D_j}$ and pick

$$\widetilde{\Delta_j} \in \mathrm{Mat}(d_j, n, \mathbb{F}) \text{ so that } \widetilde{D_j} = \left(\mathrm{rows}\, \widetilde{\Delta_j}\right) \mathbb{F},$$

and then, for any sufficiently large integer ψ, we get

$$\widetilde{\Delta_j} \cdot \pi(\rho_j)^{\psi} \cdot S^{n^2 - \overline{p}}\, \mathbb{F} = \mathrm{Mat}(d_j, n, \mathbb{F})$$

by the item (ii) of Lemma 30, which implies

$$\widetilde{\Delta_j} \cdot S^{n^2 - \overline{p}}\, \mathbb{F} = \mathrm{Mat}(d_j, n, \mathbb{F}) \tag{4.17}$$

due to Observation 31. Finally, the conditions (4.15) and (4.16) allow an application of Observation 31 in turn to (4.17), and the desired condition (4.9) follows. □

A calculation of the lengths of the words in Lemma 32 leads to the main result.

Theorem 33. *We have $S^{\ell}\, \mathbb{F} = \mathrm{Mat}_n(\mathbb{F})$ for any positive integer $\ell \geqslant n^2 + 2n - 4$.*

Proof. We choose nonnegative integers $x_1, \ldots, x_\tau$ so that $0 \in \{x_1, \ldots, x_\tau\}$ and the lengths of all words appearing on the right hand side of (4.8) are equal, and we apply Lemma 32. Therefore, the desired bound can be taken as the maximum length of any word on the right hand side of (4.8) as computed with $x_1 = \ldots = x_\tau = 0$:

$$|u_i| + b_i \cdot |\rho_i| + (n^2 - \overline{p}). \tag{4.18}$$

Indeed, if $|\rho_i| \geqslant h$, then $b_i \leqslant 1$ by Lemma 32, and we also have $|u_i| \leqslant \tau + h - |\rho_i|$ due to the item (i) in Lemma 30. Since $\overline{p} \geqslant h + 1$ by Remark 28, we get

$$(\tau + h - |\rho_i|) + |\rho_i| + (n^2 - \overline{p}) \leqslant n^2 + n - 1 \tag{4.19}$$

as an upper bound on (4.18) applicable in the case $|\rho_i| \geqslant h$.

If $|\rho_i| < h$, we get $(b_i - 1) \cdot |\rho_i| \leqslant h - 1$ by Lemma 32. Also, we have $h < \tau \leqslant n$ due to Remark 25 and hence $|u_i| \leqslant \tau + h - |\rho_i| - 1$ by the item (i) in Lemma 30. Finally, we have $\overline{p} \geqslant h + 1$ due to Remark 28, and, summing up, we get

$$(\tau + h - |\rho_i| - 1) + b_i \cdot |\rho_i| + (n^2 - \overline{p})$$

or

$$n^2 + (h - \overline{p}) + \tau - 1 + (b_i - 1) \cdot |\rho_i| \leqslant n^2 + 2n - 4 \tag{4.20}$$

as an upper bound on (4.18) valid if $|\rho_i| < h$.

We put the results (4.19) and (4.20) together, which gives $S^{\ell}\, \mathbb{F} = \mathrm{Mat}_n(\mathbb{F})$ for any integer $\ell \geqslant \max\{n^2 + n - 1,\ n^2 + 2n - 4\}$. The maximum is attained at the second term except the cases $n = 1$ and $n = 2$, which can be checked separately. □

5. Concluding remarks

We proved the conjecture $w(n) \in O(n^2)$ proposed in [35] by showing a stronger property $w(n) \in n^2 + O(n)$. We did not make any specific attempt to improve the $O(n)$ part of our bound because the current technique does not seem to be sufficient to come within an $o(n)$ to the best known lower bound the author is aware of, which is $w(n) \geqslant n^2 - n$ in [37]. More precisely, the current approach cannot significantly reduce the term $\mathcal{L}(n^2 - \overline{p})$ in the assertions of Lemmas 30 and 32, and a particular problematic case arises with $(h, \overline{p}) = (0, 1)$. This situation may appear if the initial family contains an invertible matrix, and hence we make no significant progress on the bound of $n^2 - 1$ applicable in this case [35]. Indeed, we feel that an $O(1)$ improvement of Theorem 3 can be achieved immediately with a more careful calculation, and an $O(n)$ improvement can be possible with a slight modification of the current technique. Nevertheless, it might or might not be possible that

- our strong results would motivate the search of a particular value of $w(n)$ with potential improvements on the current upper and lower bounds,
- our approach would lead to some progress in the $2n-2$ conjecture of Paz [19, 33, 34, 41] on the lengths of matrix algebras and other related topics.

6. Release notes and acknowledgements

I would like to thank the administration of viXra for splitting my previous work into several pieces at their discretion and uploading the truncated version [42] on their website. An explanation that they are '*removing non-scholarly material*' is particularly sound as viXra is widely known as a host of a whole lot of outstanding research articles. This is a pretty good news in the world where most of the editorial boards, prize and hiring committees are essentially dissolved, which makes it almost impossible to publish your papers officially or to take some money for your work. If, in addition, a remaining few preprint servers which could have been used to freely disseminate your preprints run amok in their ignorance, the contemporary research community could rapidly become much more attractive as an object of a further investigation itself and also *diverse* at every natural criterion except the level of the mental health of its representatives. Thanks a lot for making this clear.

References

[1] J. Ahiable, D. W. Kribs, J. Levick, R. Pereira, M. Rahaman, Entanglement breaking channels, stochastic matrices, and primitivity, *Linear Algebra Appl.* 629 (2021) 219–231.
[2] J. L. R. Alfonsín, *The Diophantine Frobenius Problem*, Oxford Lecture Series in Mathematics and Its Applications 30, Oxford University Press, 2005.
[3] T. Barthel, J. Lu, G. Friesecke, On the closedness and geometry of tensor network state sets, *Lett. Math. Phys.* 112 (2022) 72.
[4] J. Balogh, B. Bollobás, Hereditary properties of words, *RAIRO-Inf. Theor. Appl.* 39 (2005) 49–65.
[5] J. Bell, E. Zelmanov, On the growth of algebras, semigroups, and hereditary languages, *Invent. Math.* 224 (2021) 683–697.
[6] M. Christandl, F. Gesmundo, D. S. França, A. H. Werner, Optimization at the boundary of the tensor network variety, *Phys. Rev. B* 103 (2021) 195139.
[7] M. Christandl, A. Lucia, P. Vrana, A. H. Werner, Tensor network representations from the geometry of entangled states, *SciPost Phys.* 9 (2020) 042.
[8] J. I. Cirac, J. Garre-Rubio, D. Pérez-García, Mathematical open problems in projected entangled pair states, *Rev. Mat. Complut.* 32 (2019) 579–599.
[9] J. I. Cirac, S. Michalakis, D. Pérez-García, N. Schuch, Robustness in projected entangled pair states, *Phys. Rev. B* 88 (2013) 115108.
[10] J. I. Cirac, D. Pérez-García, N. Schuch, F. Verstraete, Matrix product density operators: Renormalization fixed points and boundary theories, *Ann. Phys.* 378 (2017) 100–149.
[11] J. I. Cirac, D. Pérez-García, N. Schuch, F. Verstraete, Matrix product states and projected entangled pair states: Concepts, symmetries, theorems, *Rev. Mod. Phys.* 93 (2021), 045003.
[12] M. Crochemore, F. Mignosi, A. Restivo, Minimal forbidden words and factor automata, in *Mathematical Foundations of Computer Science 1998: 23rd International Symposium*, Springer, Berlin, Heidelberg, 1998. 665–673.
[13] A. Czapliński, M. Michałek, T. Seynnaeve, Uniform matrix product states from an algebraic geometer's point of view, *Adv. Appl. Math.* 142 (2023) 102417.
[14] G. de las Cuevas, T. S. Cubitt, J. I. Cirac, M. M. Wolf, D. Pérez-García, Fundamental limitations in the purifications of tensor networks, *J. Math. Phys.* 57 (2016) 071902.
[15] G. de las Cuevas, T. Netzer, Mixed states in one spatial dimension: Decompositions and correspondence with nonnegative matrices, *J. Math. Phys.* 61 (2020) 041901.
[16] J. Eisert, M. P. Mller, C. Gogolin, Quantum measurement occurrence is undecidable, *Phys. Rev. Lett.* 108 (2012) 260501.
[17] J. Garre Rubio, *Symmetries in topological tensor network states: classification, construction and detection* (Doctoral dissertation), Universidad Complutense de Madrid, 2019.

[18] A. Giambruno, M. Zaicev, Exponential codimension growth of PI algebras: an exact estimate, *Adv. Math.* 142 (1999) 221–243.
[19] A. Guterman, T. Laffey, O. Markova, H. Šmigoc, A resolution of Paz's conjecture in the presence of a nonderogatory matrix, *Linear Algebra Appl.* 543 (2009) 234-250.
[20] E. B. Guedes, F. M. De Assis, R. A. C. Medeiros, *Quantum Zero-Error Information Theory*, Springer International Publishing, Switzerland, 2016.
[21] C. Harris, M. Michałek, E. Sertöz, Computing images of polynomial maps, *Adv. Comput. Math.* 45 (2019) 2845–2865.
[22] Y. Jia, Á. Capel, A generic quantum Wielandt's inequality (2023) arXiv:2301.08241.
[23] I. Klep, Š. Špenko, Sweeping words and the length of a generic vector subspace of $\mathrm{M}_n(\mathbb{F})$, *J. Comb. Theory Ser. A*, 143 (2016) 56–65.
[24] T. Laffey, Simultaneous reduction of sets of matrices under similarity, *Linear Algebra Appl.* 84 (1986) 123–138.
[25] M. Larsen, A. Shalev, Word maps and Waring type problems, *J. Amer. Math. Soc.* 22 (2009) 437–466.
[26] M. S. Lambrou, W. E. Longstaff, On the lengths of pairs of complex matrices of size six, *B. Aust. Math. Soc.* 80 (2009) 177–201.
[27] W. E. Longstaff, A. C. Niemeyer, O. Panaia, On the lengths of pairs of complex matrices of size at most five, *B. Aust. Math. Soc.* 73 (2006) 461–472.
[28] W. Longstaff, P. Rosenthal, On the lengths of irreducible pairs of complex matrices, *Proc. Amer. Math. Soc.* 139 (2011) 3769–3777.
[29] M. Michałek, T. Seynnaeve, F. Verstraete, A tensor version of the quantum Wielandt theorem, *SIAM J. Matrix Anal. A.* 40 (2019) 1125–1130.
[30] M. Michałek, Y. Shitov, Quantum version of Wielandt's inequality revisited, *IEEE T. Inform. Theory* 65 (2019) 5239–5242.
[31] S. P. Mishchenko, Growth in varieties of Lie algebras, *Russ. Math. Surv.* 45 (1990) 27–52.
[32] S. Ohyama, K. Shiozaki, M. Sato, Generalized Thouless pumps in (1+1)-dimensional interacting fermionic systems, *Phys. Rev. B* 106 (2022) 165115.
[33] C. J. Pappacena, An upper bound for the length of a finite-dimensional algebra, *J. Algebra* 197 (1997) 535–545.
[34] A. Paz, An application of the Cayley–Hamilton theorem to matrix polynomials in several variables, *Linear Multilinear A.* 15 (1984) 161–170.
[35] D. Pérez-García, F. Verstraete, M. M. Wolf, J. I. Cirac, Matrix product state representations, *Quantum Inf. Comput.* 7 (2007) 401–430.
[36] M. Rahaman, A new bound on quantum Wielandt inequality, *IEEE T. Inform. Theory* 66 (2019) 147–154.
[37] M. Sanz, D. Pérez-García, M. M. Wolf, J. I. Cirac, A quantum version of Wielandt's inequality, *IEEE T. Inform. Theory* 56 (2010) 4668–4673.
[38] M. Sanz Ruiz, *Tensor networks in condensed matter* (Doctoral dissertation), Technische Universität München, 2011.
[39] E. Seneta, *Non-negative matrices and Markov chains*, Springer Series in Statistics, Springer-Verlag, Berlin, Heidelberg, 2006.
[40] T. Seynnaeve, *Algebraic geometry for tensor networks, matrix multiplication, and flag matroids* (Doctoral dissertation), Universität Leipzig, 2020.
[41] Y. Shitov, An improved bound for the lengths of matrix algebras, *Algebr. Number Theory* 13 (2019) 1501–1507.
[42] Y. Shitov, Higher Rank Substitutions for Tensor Decompositions. I. Direct Sum Conjectures, preprint (2023) viXra:2307.0100.
[43] R. Vanhove, M. Bal, D. J. Williamson, N. Bultinck, J. Haegeman, F. Verstraete, Mapping topological to conformal field theories through strange correlators, *Phys. Rev. Let.*, 121 (2018), 177–203.
[44] R. S. Varga, *Matrix Iterative Analysis*, Springer Series in Computational Mathematics 27, Springer-Verlag, Berlin, Heidelberg, 2000.
[45] F. Verstraete, V. Murg, J. I. Cirac, Matrix product states, projected entangled pair states, and variational renormalization group methods for quantum spin systems, *Adv. Phys.* 57 (2008) 143–224.
[46] B. A. Ware, *Tensor Network Wave functions for Topological Phases* (Doctoral dissertation), UC Santa Barbara, 2017.
[47] H. Wielandt, Unzerlegbare, nicht negative Matrizen, *Math. Z.* 52 (1950) 642–648.

E-mail address: yaroslav-shitov@yandex.ru