ON NONNEGATIVE INTEGER MATRICES AND SHORT KILLING WORDS*

STEFLAN KIEFER† AND CORTO MASCLE‡

Abstract. Let $n$ be a natural number and $\mathcal{M}$ a set of $n \times n$-matrices over the nonnegative integers such that the joint spectral radius of $\mathcal{M}$ is at most one. We show that if the zero matrix $0$ is a product of matrices in $\mathcal{M}$, then there are $M_1, \ldots, M_5 \in \mathcal{M}$ with $M_1 \cdots M_5 = 0$. This result has applications in automata theory and the theory of codes. Specifically, if $\Sigma \subseteq \Sigma^*$ is a finite incomplete code, then there exists a word $w \in \Sigma^*$ of length polynomial in $\sum_{x \in \Sigma} |x|$ such that $w$ is not a factor of any word in $\Sigma^*$. This proves a weak version of Restivo’s conjecture.

Key words. Matrix semigroups, unambiguous automata, codes, Restivo’s conjecture

AMS subject classifications. 20M35, 68Q45, 68R05

1. Introduction. Let $n \in \mathbb{N}$ and $\mathcal{M} \subseteq \mathbb{R}^{n \times n}$ be a finite set of matrices. The joint spectral radius of $\mathcal{M}$, denoted by $\rho(\mathcal{M})$, is defined by the following limit:

$$
\rho(\mathcal{M}) := \lim_{k \to \infty} \max \{ \| M_1 \cdots M_k \|^1/k : M_i \in \mathcal{M} \}
$$

This limit exists and does not depend on the chosen norm [6]. In this article we focus on nonnegative integer matrices: we assume $\mathcal{M} \subseteq \mathbb{N}^{n \times n}$ where $\mathbb{N} = \{0, 1, 2, \ldots \}$. Denote by $\overline{\mathcal{M}}$ the monoid (semigroup) generated by $\mathcal{M}$ under matrix multiplication, i.e., the set of products of matrices from $\mathcal{M}$. If $\overline{\mathcal{M}}$ is finite then $\rho(\mathcal{M}) \leq 1$, but the converse does not hold [12].

In this article we show the following theorem:

**Theorem 1.** Let $n \in \mathbb{N}$ and $\mathcal{M} \subseteq \mathbb{N}^{n \times n}$ be a finite set of nonnegative integer matrices with $\rho(\mathcal{M}) \leq 1$. Then there are $M_1, \ldots, M_\ell \in \mathcal{M}$ with $\ell \leq \frac{1}{16} n^5 + \frac{15}{16} n^4$ such that the matrix product $M_1 \cdots M_\ell$ has minimum rank among the matrices in $\overline{\mathcal{M}}$. Further, $M_1, \ldots, M_\ell$ can be computed in time polynomial in the description size of $\mathcal{M}$.

Let $\mathcal{M} \subseteq \mathbb{N}^{n \times n}$ be a finite set of nonnegative integer matrices. For notational convenience, throughout the paper, we associate to $\mathcal{M}$ a bijection $M : \Sigma \to \mathcal{M}$ and extend it to the monoid morphism $M : \Sigma^* \to \overline{\mathcal{M}}$, where $\Sigma^* = \bigcup_{i=0}^{\infty} \Sigma^i$ denotes the set of words over $\Sigma$. For a word $w \in \Sigma^i$, its length $|w|$ is $i$. We write $\varepsilon$ for the word of length $0$. We may write $M(\Sigma)$ for $\mathcal{M}$ and $M(\Sigma^*)$ for $\overline{\mathcal{M}}$ and $\rho(M)$ for $\rho(M(\Sigma))$. Then one may rephrase the main theorem as follows:

**Theorem 1 (rephrased).** Given $M : \Sigma \to \mathbb{N}_{n \times n}$ with $\rho(M) \leq 1$, one can compute in polynomial time a word $w \in \Sigma^*$ with $|w| \leq \frac{1}{16} n^5 + \frac{15}{16} n^4$ such that $M(w)$ has minimum rank in $M(\Sigma^*)$.

The condition $\rho(M) \leq 1$ should be viewed in light of the following dichotomy [12]: if $\rho(M) \leq 1$ then $B(k) := \max \{ \| M(w) \| : w \in \Sigma^k \}$ is in $O(k^n)$, i.e., $B(k)$ grows polynomially in $k$; if $\rho(M) > 1$ then (by definition) $B(k)$ grows exponentially in $k$.

---

*A preliminary version of this article is appearing at STACS’19 under the title On Finite Monoids over Nonnegative Integer Matrices and Short Killing Words. This article is more self-contained and slightly generalizes the results by relaxing the finiteness condition to a condition on the joint spectral radius. In addition we prove a more precise result related to Restivo’s conjecture for finite codes.

**Funding:** Kiefer is supported by a Royal Society University Research Fellowship.

‡University of Oxford, UK (https://www.cs.ox.ac.uk/people/stefan.kiefer/).

‡ENS Paris-Saclay, France.

---

18 Mar 2019
Automata definitions. A morphism $M : \Sigma \rightarrow \{0,1\}^{n \times n}$ is naturally associated with an automaton. A nondeterministic finite automaton (NFA) is a triple $A = (\Sigma, Q, \delta)$, where $\Sigma$ is a finite alphabet, $Q$ is a finite set of states, and $\delta : Q \times \Sigma \rightarrow 2^Q$ is a transition function (initial and final states do not play a role here). We extend $\delta$ in the usual way to $:\Sigma^* \times \Sigma \rightarrow 2^Q$ by setting $\delta(P, a) := \bigcup_{q \in P} \delta(q, a)$ and $\delta(P, \varepsilon) := P$ and $\delta(P, wa) := \delta(P, w) \cup \delta(P, a)$, where $P \subseteq Q$ and $a \in \Sigma$ and $w \in \Sigma^*$. A sequence $\psi = q_0a_1q_1a_2\cdots q_{n-1}a_nq_n$ with $q_i \in Q$ and $a_i \in \Sigma$ is called a path from $q_0$ to $q_n$ if $\delta(q_{i-1}, a_i) \ni q_i$ holds for all $i \in \{1, \ldots, n\}$. The word $a_1 \cdots a_n$ is said to label the path $\psi$. Note that a word $w \in \Sigma^*$ labels a path from $p$ to $q$ if and only if $\delta(\{p\}, w) \ni q$. A word $w$ is called killing word if it does not label any path. Associate to $A$ the monoid morphism $M_A : \Sigma^* \rightarrow \mathbb{N}^Q \times Q$ where for all $a \in \Sigma$ we define $M_A(a)(p, q) = 1$ if $\delta(p, a) \ni q$ and 0 otherwise. Then, for any word $w \in \Sigma^*$ we have that $M_A(w)(p, q)$ is the number of $w$-labelled paths from $p$ to $q$. In particular, $M_A(w)$ is the zero matrix 0 if and only if $w$ is a killing word.

An NFA $A = (\Sigma, Q, \delta)$ is called an unambiguous finite automaton (UFA) if for all states $p, q$ all paths from $p$ to $q$ are labelled by different words, i.e., for each word $w \in \Sigma^*$ there is at most one $w$-labelled path from $p$ to $q$. Call a monoid $M \subseteq \mathbb{N}^{n \times n}$ an unambiguous monoid of relations if $M$ is an unambiguous monoid of relations, and every unambiguous monoid of relations can be viewed as generated by a UFA. UFAs play a central role in our proofs.

The mortality problem. Theorem 1 is related to the mortality problem for integer matrices: given $M : \Sigma \rightarrow Z^{n \times n}$, is $0 \in M(\Sigma^*)$, i.e., can the zero matrix (which is defined to have rank 0) be expressed as a finite product of matrices in $M(\Sigma)$? Paterson [15] showed that the mortality problem for integer matrices is undecidable for $n = 3$. It remains undecidable for $n = 3$ with $|\Sigma| = 7$ and for $n = 21$ with $|\Sigma| = 2$, see [9]. Mortality for $n = 2$ is NP-hard [1] and not known to be decidable, see [16] for recent work on $n = 2$.

The mortality problem for nonnegative matrices (even for matrices over the non-negative reals) is much easier, as for each matrix entry it only matters whether it is zero or nonzero, so one can assume $M : \Sigma \rightarrow \{0,1\}^{n \times n}$. It follows that the mortality problem for nonnegative matrices is equivalent to the problem whether an NFA has a killing word. The problem is PSPACE-complete [13], and there are examples where the shortest killing word has exponential length in the number of states of the automaton [7, 13]. This implies that the assumption in Theorem 1 about the joint spectral radius $\rho(M)$ cannot be dropped. Whether $\rho(M) \leq 1$ indeed holds can be checked in polynomial time [12]. The condition is satisfied whenever $M(\Sigma^*)$ is finite. Whether $M(\Sigma^*)$ is finite can also be checked in polynomial time, see, e.g., [22] and the references therein. The authors are not aware of an easier proof of Theorem 1 under the stronger assumption that $M(\Sigma^*)$ is finite. If $\rho(M) \leq 1$ then the mortality problem for nonnegative integer matrices is solvable in polynomial time:

**Proposition 2.** Given $M : \Sigma \rightarrow \mathbb{N}^{n \times n}$ with $\rho(M) \leq 1$, one can decide in polynomial time if $0 \in M(\Sigma^*)$.

Proposition 2 is implied by Theorem 1, but has an easier proof.

Short killing words for unambiguous finite automata. Proposition 2 provides a polynomial-time procedure for checking whether a UFA has a killing word. Define $\rho$ as the spectral radius of the rational matrix $\sum_{a \in \Sigma} M(a)$. One can show that $\rho < 1$ if $A$ has a killing word, and $\rho = 1$ otherwise. Proposition 2 then follows from the fact that one can compare $\rho$ with 1 in polynomial time. Thus the spectral
Theorem 1 provides, to the best of the authors’ knowledge, the first polynomial bound, 18
3
4
2
18
11
8
we then obtain Theorem 3. Based for all p ∈ Q and all a ∈ Σ. In fact, by combining our main result with [18, Theorem 17] the following problem is NP-complete: given an unambiguous automaton and a number ℓ ∈ N in binary, does there exist a killing word of length at most ℓ?

**Short minimum-rank words.** Define the rank of a UFA A = (Σ, Q, δ) as the minimum rank of the matrices M_A(w) for w ∈ Σ*. A word w such that the rank of M_A(w) attains that minimum is called a minimum-rank word. Minimum-rank words have been very well studied for deterministic finite automata (DFAs). DFAs are UFAs with |δ(p, a)| = 1 for all p ∈ Q and all a ∈ Σ. In DFAs of rank 1, minimum-rank words are called synchronizing because δ(Q, w) is a singleton when w is a minimum-rank word. It is the famous Černý conjecture that whenever a DFA has a synchronizing word then it has a synchronizing word of length at most (n − 1)^2 where n := |Q|. There are DFAs whose shortest synchronizing words have that length, but the best known upper bound is cubic in n, see [21] for a survey on the Černý conjecture.

In 1986 Berstel and Perrin generalized the Černý conjecture from DFAs to UFAs by conjecturing [2] that in any UFA a shortest minimum-rank word has length O(n^2). They remarked that no polynomial upper bound was known. Then Carpi [4] showed the following:

**Theorem 3 (Carpi [4]).** Let A = (Σ, Q, δ) be a UFA of rank r ≥ 1 such that the state transition graph of A is strongly connected. Let n := |Q| ≥ 1. Then A has a minimum-rank word of length at most 1/2 r n(n − 1)^2 + (2r − 1)(n − 1).

This implies an O(n^4) bound for the case where r ≥ 1. Carpi left open the case r = 0, i.e., when a killing word exists. The main technical contribution of our paper concerns the case r = 0. Combined with Carpi’s Theorem 3 we then obtain Theorem 1. Based on our technical development, we also provide a short proof of a variant of Carpi’s Theorem 3, which suffices for our purposes and makes this article self-contained. Theorem 1 provides, to the best of the authors’ knowledge, the first polynomial bound, O(n^3), on the length of shortest minimum-rank words for UFAs.

**Restivo’s conjecture.** Let X ⊆ Σ* be a finite set of words over a finite alphabet Σ, and define k := \max_{x \in X} |x|. A word v ∈ Σ* is called uncompletable in X if there are no words u, w ∈ Σ* such that uw ∈ X*, i.e., v is not a factor of any word in X*. In 1981 Restivo [17] conjectured that if there exists an uncompletable word then there is an uncompletable word of length at most 2k^2. This strong form of Restivo’s conjecture has been refuted, with a lower bound of 5k^2 − O(k), see [8]. A recent article [11] describes a sophisticated computer-assisted search for sets X with long shortest uncompletable words. While these experiments do not formally disprove a quadratic upper bound in k, they seem to hint at an exponential behaviour in k. See also [5] for recent work and open problems related to Restivo’s conjecture.

A set X ⊆ Σ* is called a code if every word w ∈ X* has at most one decomposition w = x_1 · · · x_k with x_1, . . . , x_k ∈ X. See [3] for a comprehensive reference on codes. For a finite code X ⊆ Σ* define m := \sum_{x \in X} |x|. Given such X one can construct a flower automaton [3, Chapter 4.2], which is a UFA A_X = (Σ, Q, δ) with m − |X| + 1 states,
see Figure 1. In this UFA any word is killing if and only if it is uncompletable in \( X \). Hence Theorem 1 implies an \( O(m^5) \) bound on the length of the shortest uncompletable word in a finite code. This proves a weak (note that \( m^5 \) may be much larger than \( k^2 \)) version of Restivo’s conjecture for finite codes. By adapting our main argument so that it exploits the special structure of flower automata, we get a better result:

**Theorem 4.** Let \( X \subseteq \Sigma^* \) be a finite code that has an uncompletable word. Define \( k := \max_{x \in X} |x| \) and \( m := \sum_{x \in X} |x| \) and assume \( k > 0 \). Then one can compute in polynomial time an uncompletable word of length at most \( (k + 1)k^2(m + 2)(m + 1) \).

Is any product a short product? It was shown in [22] that if \( M(\Sigma^*) \subseteq \mathbb{N}^{n \times n} \) is finite then for every \( w_0 \in \Sigma^* \) there exists \( w \in \Sigma^* \) with \( |w| \leq \lfloor e^2 nt \rfloor - 2 \) such that \( M(w_0) = M(w) \). It was also shown in [22] that such a length bound cannot be smaller than \( 2^{n-2} \). In view of Theorem 1 one may ask if a polynomial length bound exists for low-rank matrices \( M(w_0) \). The answer is no, even for unambiguous monoids of relations and even when \( M(w_0) \) has rank 1 and 1 is the minimum rank in \( M(\Sigma^*) \):

**Theorem 5.** There is no polynomial \( p \) such that the following holds:

Let \( M : \Sigma^* \to \{0, 1\}^{n \times n} \) be a monoid morphism. Let \( w_0 \in \Sigma^* \) be such that \( M(w) \) has rank 1, and let 1 be the minimum rank in \( M(\Sigma^*) \).

Then there is \( w \in \Sigma^* \) with \( |w| \leq p(n) \) such that \( M(w_0) = M(w) \).

Thus, while Theorem 1 guarantees that some minimum-rank matrix in the monoid is a short product, this is not the case for every minimum-rank matrix in the monoid.

By how much could the \( O(n^5) \) upper bound be improved? A synchronizing 0-automaton is a DFA \( A = (\Sigma, Q, \delta) \) that has a state \( 0 \in Q \) and a word \( w \in \Sigma^* \) such that \( \delta(Q, wx) = \{0\} \) holds for all \( x \in \Sigma^* \). The shortest such synchronizing words \( w \) are exactly the shortest killing words in the partial DFA obtained from \( A \) by omitting all transitions into the state 0. There exist synchronizing 0-automata with \( n \) states where the shortest synchronizing word has length \( n(n-1)/2 \), and an \( \frac{n^2}{4} - 4 \) lower bound exists even for synchronizing 0-automata with \( |\Sigma| = 2 \) [14]. This implies that the \( O(n^5) \) upper bound from Theorem 1 cannot be improved to \( o(n^2) \), not even when a killing word exists. One might generalize the Černý conjecture by claiming Theorem 1 with an upper bound of \( (n - 1)^2 \) (note that such a conjecture would concern minimum-rank words, not minimum nonzero-rank words). To the best of the authors’ knowledge, this vast generalization of the Černý conjecture has not yet been refuted.

**Organization of the article.** In the remaining four sections we prove Proposition 2 and Theorems 1, 4 and 5, respectively.

2. Proof of Proposition 2. Let \( M : \Sigma \to \mathbb{N}^{n \times n} \) be such that \( \rho(M) \leq 1 \).
Towards a proof of Proposition 2, define the rational nonnegative matrix
\[ A \in \mathbb{Q}^{n \times n} \text{ by } A := \frac{1}{|\Sigma|} \sum_{a \in \Sigma} M(a). \]
Observe that for \( k \in \mathbb{N} \) we have \( A^k = \frac{1}{|\Sigma|^k} \sum_{w \in \Sigma^k} M(w) \), i.e., \( A^k \) is the average of the \( M(w) \), where \( w \) ranges over all words of length \( k \). Define \( \rho \geq 0 \) as the spectral radius of \( A \).

**Lemma 6.** We have \( \rho \leq 1 \).

**Proof.** By the Perron-Frobenius theorem, \( A \) has a nonnegative eigenvector \( u \in \mathbb{R}^n \) with \( Au = \rho u \). So \( A^k u = \rho^k u \). Thus \( \max\{|M(w)| : w \in \Sigma^k\} \in \Omega(\rho^k) \). Hence \( \rho \leq \rho(M) \leq 1 \).

**Lemma 7.** We have \( \rho < 1 \) if and only if there is \( w \in \Sigma^\ast \) with \( M(w) = 0 \).

**Proof.** Suppose \( \rho < 1 \). Then \( \lim_{k \to \infty} A^k = 0 \), and so there is \( k \in \mathbb{N} \) such that the sum of all entries of \( A^k \) is less than 1. It follows that there is \( w \in \Sigma^k \) such that the sum of all entries of \( M(w) \) is less than 1. Since \( M(w) \in \mathbb{N}^{n \times n} \) it follows \( M(w) = 0 \).

Conversely, suppose there is \( w_0 \in \Sigma^\ast \) with \( M(w_0) = 0 \). Since \( \rho(M) \leq 1 \), by [12, Theorem 3] there exists \( c > 0 \) such that \( B(k) := \max\{|M(w)| : w \in \Sigma^k\} \leq ck^n \) holds for all \( k \in \mathbb{N} \setminus \{0\} \). For any \( k \in \mathbb{N} \) define \( W(k) := \Sigma^k \setminus \langle \Sigma^\ast w_0 \Sigma^\ast \rangle \), i.e., \( W(k) \) is the set of length-\( k \) words that do not contain \( w_0 \) as a factor. Note that \( M(w) = 0 \) holds for all \( w \in \Sigma^k \setminus W(k) \). Since matrix norms are sub-additive, it follows that \( \|A^k\| \) is at most \( \frac{|W(k)|}{|\Sigma|^k} \cdot B(k) \). On the other hand, for any \( m \in \mathbb{N} \), if a word of length \( m |w_0| \) is picked uniformly at random, then the probability of picking a word in \( W(m|w_0|) \) is at most
\[
\left(1 - \frac{1}{|\Sigma| |w_0|}\right)^m,
\]
thus
\[
\|A^m|w_0|\| \leq \left(1 - \frac{1}{|\Sigma| |w_0|}\right)^m c(m|w_0|)^n.
\]
Hence \( \lim_{k \to \infty} A^k = 0 \) and so \( \rho < 1 \).

With these lemmas at hand, we can prove Proposition 2:

**Proposition 2.** Given \( M : \Sigma \to \mathbb{N}^{n \times n} \) with \( \rho(M) \leq 1 \), one can decide in polynomial time if \( 0 \in M(\Sigma^\ast) \).

**Proof.** By Lemma 7, it suffices to check whether \( \rho < 1 \).

If \( \rho < 1 \) then the linear system \( Ax = x \) does not have a nonzero solution. Conversely, if \( \rho \geq 1 \) then, by Lemma 6, we have \( \rho = 1 \) and thus, by the Perron-Frobenius theorem, the linear system \( Ax = x \) has a (real) nonzero solution.

Hence it suffices to check if \( Ax = x \) has a nonzero solution. This can be done in polynomial time.

As remarked in section 1, this algorithm does not exhibit a word \( w \) with \( M(w) = 0 \), even when it proves the existence of such \( w \).

3. Proof of Theorem 1. As before, let \( M : \Sigma \to \mathbb{N}^{n \times n} \) be such that \( \rho(M) \leq 1 \). Call \( M \) strongly connected if for all \( i, j \in \{1, \ldots, n\} \) there is \( w \in \Sigma^\ast \) with \( M(w)(i,j) \geq 1 \). In subsection 3.1 we consider the case that \( M \) is strongly connected. In subsection 3.2 we consider the general case.

3.1. Strongly Connected. In this section we consider the case that \( M \) is strongly connected and prove the following proposition, which extends Carpi’s Theorem 3:
Proposition 8. Given \( M : \Sigma \rightarrow \mathbb{N}^{n \times n} \) such that \( \rho(M) \leq 1 \) and \( M \) is strongly connected, one can compute in polynomial time a word \( w \in \Sigma^* \) with \(|w| \leq \frac{1}{16} n^5 + \frac{15}{16} n^4 \) such that \( M(w) \) has minimum rank in \( M(\Sigma^*) \).

In the strongly connected case, \( M(\Sigma^*) \) does not have numbers larger than 1:

Lemma 9. We have \( M(\Sigma^*) \subseteq \{0,1\}^{n \times n} \).

Proof. Suppose \( M(v)(i,j) \geq 2 \) for some \( v \in \Sigma^* \). Since \( M \) is strongly connected, there is \( w \in \Sigma^* \) with \( M(w)(j,i) \geq 1 \). Hence \( M(vw)(i,i) \geq 2 \). It follows that \( M((vw)^k)(i,i) \geq 2^k \) for all \( k \in \mathbb{N} \), contradicting the assumption \( \rho(M) \leq 1 \).

Lemma 9 allows us to view the strongly connected case in terms of UFAs. Define a UFA \( A = (\Sigma, Q, \delta) \) with \( Q = \{1, \ldots, n\} \) and \( \delta(p,a) \ni q \) if and only if \( M(a)(p,q) = 1 \).

For the rest of the subsection we will mostly consider \( Q \) as an arbitrary finite set of \( n \) states. When there is no confusion, we may write \( pw \) for \( \delta(p,w) \) and \( wq \) for \( \{p \in Q : pw \ni q\} \). We extend this to \( Pw := \bigcup_{p \in P} pw \) and \( wP := \bigcup_{p \in P} wp \). We say a state \( p \) is reached by a word \( w \) when \( wp \neq \emptyset \), and a state \( p \) survives a word \( w \) when \( wp \neq \emptyset \). Note that \( Qw \) is the set of states that are reached by \( w \), and \( wQ \) is the set of states that survive \( w \). Let \( q_1 \neq q_2 \) be two different states. Then \( q_1, q_2 \) are called coreachable when there is \( w \in \Sigma^* \) with \( wq_1 \cap wq_2 \neq \emptyset \) (i.e., there is \( p \in Q \) with \( pw \ni \{q_1, q_2\} \)), and they are called mergeable when there is \( w \in \Sigma^* \) with \( q_1 w \cap q_2 w \neq \emptyset \). For any \( q \in Q \) we define \( C(q) \) as the set of states coreachable with \( q \). Also, define \( c := \max\{|qw| : q \in Q, w \in \Sigma^* \} \) and \( m := \max\{|qw| : w \in \Sigma^*, q \in Q \} \). The following lemma says that one can compute short witnesses for coreachability:

Lemma 10. If states \( q \neq q' \) are coreachable, then one can compute in polynomial time \( w_{q,q'} \in \Sigma^* \) with \(|w_{q,q'}| \leq \frac{1}{2}(n+2)(n-1) \) such that \( qw_{q,q'} \ni \{q,q'\} \).

Proof. Let \( q \neq q' \) be coreachable states. Then there are \( p \in Q \) and \( v \in \Sigma^* \) with \( pv \ni \{q,q'\} \). Since \( M \) is strongly connected, there is \( u \in \Sigma^* \) with \( qu \ni p \), hence \( qw \ni \{q,q'\} \). Define an edge-labelled directed graph \( G = (V,E) \) with vertex set \( V = \{r,s : r,s \in Q\} \) and edge set \( E = \{(R,a,S) : R \times S : Ra \ni S\} \). Since \( qw \ni \{q,q'\} \), the graph \( G \) has a path, labelled by \( uv \), from \( \{q\} \) to \( \{q,q'\} \). The shortest path from \( \{q\} \) to \( \{q,q'\} \) has at most \( |V| - 1 \) edges and is thus labelled with a word \( w \in \Sigma^* \) with \(|w| \leq |V| - 1 = \frac{1}{2}n(n+1) - 1 = \frac{1}{2}(n+2)(n-1) \). For this \( w \) we have \( qw \ni \{q,q'\} \).

Lemma 11. For each \( q \in Q \) one can compute in polynomial time a word \( w_q \in \Sigma^* \) with \(|w_q| \leq \frac{1}{2}(c - 1)(n+2)(n-1) \) such that no state \( q' \neq q \) survives \( w_q \) and is coreachable with \( q \).

Proof. Let \( q \in Q \). Consider the following algorithm:

1. \( w := \varepsilon \)
2. while there is \( q' \in C(q) \) such that \( q' \) survives \( w \) do
3. \( w := w_{q,q'} w \) (with \( w_{q,q'} \) from Lemma 10)
4. return \( w_q := w \)

The following picture visualizes aspects of this algorithm:
We argue that the computed word $w_q$ has the required properties. First we show that the set $qw$ increases in each iteration of the algorithm. Indeed, let $w$ and $w_{q,q'}w$ be the words computed by two subsequent iterations. Since $qw_{q,q'} \supseteq \{q, q'\}$, we have $qw_{q,q'} w \supseteq qw \cup q'w$. The set $q'w$ is nonempty, as $q'$ survives $w$. As can be read off from the picture above, the sets $qw$ and $q'w$ are disjoint, as otherwise there would be two distinct paths from $q$ to a state in $qw \cap q'w$, both labelled by $w_{q,q'}w$, contradicting unambiguosness. It follows that $qw_{q,q'} w \supseteq qw$. Hence the algorithm must terminate.

Since in each iteration the set $qw$ increases by at least one element (starting from $\{q\}$), there are at most $c - 1$ iterations. Hence $|w_q| \leq \frac{1}{4}(c - 1)(n + 2)(n - 1)$. There is no state $q' \neq q$ that survives $w_q$ and is coreachable with $q$, as otherwise the algorithm would not have terminated.

**Lemma 12.** One can compute in polynomial time words $z, y \in \Sigma^*$ such that:

- $|z| \leq \frac{1}{4}(c - 1)(n + 2)n(n - 1)$ and there are no two coreachable states that both survive $z$;
- $|y| \leq \frac{1}{4}(m - 1)(n + 2)n(n - 1)$ and there are no two mergeable states that are both reached by $y$.

**Proof.** As the two statements are dual, we prove only the first one. Consider the following algorithm:

1: $w := \varepsilon$
2: while there are coreachable $p, p'$ that both survive $w$ do
3: \hspace{1em} $q :=$ arbitrary state from $pw$
4: \hspace{1em} $w := wq$ (with $w_q$ from Lemma 11)
5: return $z := w$

We show that the set

$$B := \{p_1 \in Q : \exists p_2 \in C(p_1) \text{ such that both } p_1, p_2 \text{ survive } w\}$$

loses at least two states in each iteration. First observe that

$$B' := \{p_1 \in Q : \exists p_2 \in C(p_1) \text{ such that both } p_1, p_2 \text{ survive } qw\}$$

is clearly a subset of $B$.

Let $p \in B$ be the state from line 2 of the algorithm, and let $q \in pw$ be the state from the body of the loop. We claim that no $p'' \in C(p)$ survives $ww_q$. Indeed, let $p'' \in C(p)$. The following picture visualizes the situation:

We show that the set $B' := \{p_1 \in Q : \exists p_2 \in C(p_1) \text{ such that both } p_1, p_2 \text{ survive } wq\}$

loses at least two states in each iteration. First observe that

$$B' := \{p_1 \in Q : \exists p_2 \in C(p_1) \text{ such that both } p_1, p_2 \text{ survive } wq\}$$

is clearly a subset of $B$.

Let $p \in B$ be the state from line 2 of the algorithm, and let $q \in pw$ be the state from the body of the loop. We claim that no $p'' \in C(p)$ survives $ww_q$. Indeed, let $p'' \in C(p)$. The following picture visualizes the situation:
By unambiguosness and since $q \in pw$, we have $q \not\in p''w$. By the definition of $w_q$ and since all states in $p''w$ are coreachable with $q$, we have $p''ww_q = \emptyset$, which proves the claim.

By the claim, we have $p \not\in B'$. Let $p' \in B$ be the state $p'$ from line 2 of the algorithm. We have $p' \in C(p)$. By the claim, $p'$ does not survive $ww_q$. Hence $p' \not\in B'$.

So we have shown that the algorithm removes at least two states from $B$ in every iteration. Thus it terminates after at most $\frac{n}{2}$ iterations. Using the length bound from Lemma 11 we get $|z| \leq \frac{1}{4}(c-1)(n+2)n(n-1)$. There are no coreachable $q, q'$ that both survive $z$, as otherwise the algorithm would not have terminated.

For the following development, let $q_1, \ldots, q_k$ be the states that are reached by $y$ and survive $z$ (with $y, z$ from Lemma 12), see Figure 2.

![Figure 2](image-url)

**Fig. 2.** The states $q_1, \ldots, q_k$ are neither coreachable nor mergeable.

**Lemma 13.** Let $1 \leq i < j \leq k$. Then $q_i, q_j$ are neither coreachable nor mergeable.

**Proof.** Immediate from the properties of $y, z$ (Lemma 12). □

The following lemma restricts sets of the form $q_i zxyz$ for $i \in \{1, \ldots, k\}$ and $x \in \Sigma^*$:

**Lemma 14.** Let $i \in \{1, \ldots, k\}$ and $x \in \Sigma^*$. Then there is $j \in \{1, \ldots, k\}$ such that $q_i zxyz \subseteq q_j z$.

**Proof.** If $q_i zxyz = \emptyset$ then choose $j$ arbitrarily. Otherwise, let $q \in q_i zxyz$. Then $q$ is reached by $yz$, so there is $j$ with $q_i zxy \ni q_j$ and $q_j z \ni q$. We show that $q_i zxyz \subseteq q_j z$. To this end, let $q' \in q_i zxyz$. Then $q'$ is reached by $yz$, so there is $j'$ with $q_i zxy \ni q_j'$ and $q_j' z \ni q'$. Since $q_i zxy \ni \{q_j, q_j'\}$ and $q_j, q_j'$ are not coreachable (by Lemma 13), we have $j' = j$. Hence $q_i zxyz \subseteq q_j z$.

Provided that there is a killing word (which can be checked in polynomial time via Proposition 2), the following lemma asserts that for each $i \in \{1, \ldots, k\}$ one can efficiently compute a short word $x_i$ such that no state in $q_i z$ survives $x_i yz$. The proof hinges on a linear-algebra technique for checking equivalence of automata that are weighted over a field. The argument goes back to Schützenberger [19] and has often been rediscovered, see, e.g., [20].
Lemma 15. Suppose that $0 \in M(\Sigma^*)$. For each $i \in \{1, \ldots, k\}$ one can compute in polynomial time a word $x_i \in \Sigma^*$ with $|x_i| \leq n$ such that $q_ixixyz = \emptyset$.

Proof. Let $i \in \{1, \ldots, k\}$. Since $y\{q_1, \ldots, q_k\}$ are the only states to survive $yz$, it suffices to compute $x \in \Sigma^*$ with $|x| \leq n$ such that $q_ixixyz = \emptyset$.

Define $e \in \{0,1\}^Q$ as the characteristic row vector of $q_i$, i.e., $e(q) = 1$ if and only if $q \in q_i$. Define $f \in \{0,1\}^Q$ as the characteristic column vector $y\{q_1, \ldots, q_k\}$. First we show that for any $x \in \Sigma^*$ we have $eM(x)f \leq 1$. Towards a contradiction suppose $eM(x)f > 2$. Then there are two distinct $x$-labelled paths from $q_i$ to $y\{q_1, \ldots, q_k\}$. It follows that there are two distinct $zxy$-labelled paths from $q_i$ to $\{q_1, \ldots, q_k\}$. By unambiguity, these paths end in two distinct states $q_j, q_j'$. But then $q_j, q_j'$ are coreachable, contradicting Lemma 13. Hence we have shown that $eM(x)f \leq 1$ holds for all $x \in \Sigma^*$.

Define the (row) vector space

$$V := \langle (eM(x) \ 1) : x \in \Sigma^* \rangle \subseteq \mathbb{R}^{n+1},$$

i.e., $V$ is spanned by the vectors $(eM(x) \ 1)$ for $x \in \Sigma^*$. The vector space $V$ can be equivalently characterized as the smallest vector space that contains $(e \ 1)$ and is closed under multiplication with $(M(a) \ 0)$ for all $a \in \Sigma$. Hence the following algorithm computes a set $B \subseteq \Sigma^*$ such that $\{eM(x) : x \in B\}$ is a basis of $V$:

1. $B := \{e\}$
2. while $\exists u \in B, a \in \Sigma$ such that $(eM(ua) \ 1) \notin \langle (eM(x) : x \in B) \rangle$ do
3. $B := B \cup \{ua\}$
4. return $B$

Observe that the algorithm performs at most $n$ iterations of the loop body, as every iteration increases the dimension of the space $\langle (eM(x) : x \in B) \rangle$ by 1, but the dimension cannot grow larger than $n+1$. Hence $|x| \leq n$ holds for all $x \in B$. Since $M(w_0) = 0$ holds for some $w_0 \in \Sigma^*$ and hence $eM(w_0)f = 0 \neq 1$, the space $V$ is not orthogonal to $(f \ 1)$. So there exists $x \in B$ such that $eM(x)f \neq 1$. Since $eM(x)f \leq 1$, we have $eM(x)f = 0$. Hence $q_ixixyz = \emptyset$.

Now we can prove the following lemma, which is our main technical contribution:

Lemma 16. Suppose that $0 \in M(\Sigma^*)$. One can compute in polynomial time a word $w \in \Sigma^*$ with $M(w) = 0$ and $|w| \leq \frac{1}{16}n^5 + \frac{1}{16}n^4$.

Proof. For any $1 \leq j < j' \leq k$ the sets $q_jz$ and $q_{j'}z$ are disjoint by Lemma 13 and nonempty. Hence any $P' \subseteq Q$ has at most one set $P \subseteq \{q_1, \ldots, q_k\}$ with $Pz = P'$, which we call the generator of $P'$. Note that all sets of the form $Q'yz$ where $Q' \subseteq Q$ have a generator. For any $i \in \{1, \ldots, k\}$, let $x_i$ be the word from Lemma 15, i.e., $q_ixixyz = \emptyset$. By Lemma 14, for any $j \in \{1, \ldots, k\}$ the generator of $q_jzxyz$ has at most one element. Thus, if $q_i \in P \subseteq \{q_1, \ldots, q_k\}$, then the generator, $P$, of $Pz$ has strictly more elements than the generator of $Pzxyz$.

Consider the following algorithm:

1. $w := yz$
2. while $Qw \neq \emptyset$ do
3. $q_i :=$ arbitrary element of the generator of $Qw$
4. $w := wx_iyz$
5. return $w$

It follows from the argument above that the size of the generator of $Qw$ decreases in every iteration of the loop. Hence the algorithm terminates after at most $k$ iterations.
and computes a word $w$ such that $Qw = \emptyset$ and, using Lemmas 12 and 15,
\[
|w| \leq |yz| + k(n + |yz|) \leq n^2 + (k + 1)(|y| + |z|) \\
\leq n^2 + \frac{1}{4}(k + 1)(c + m - 2)(n + 2)n(n - 1).
\]

Let $q, q' \in Q$ and $u, u' \in \Sigma^*$ such that $c = |qu|$ and $m = |u'q'|$. Clearly, $qu \cup u'q' \cup \{q_1, \ldots, q_k\} \subseteq Q$, and it follows from the inclusion-exclusion principle:
\[
c + m + k \leq n + |qu \cap u'q'| + |qu \cap \{q_1, \ldots, q_k\}| + |\{q_1, \ldots, q_k\} \cap u'q'|
\]
The sets $qu$ and $u'q'$ overlap in at most one state by unambiguosness. The sets $qu$ and $\{q_1, \ldots, q_k\}$ overlap in at most one state by Lemma 13, and similarly for $\{q_1, \ldots, q_k\}$ and $u'q'$. It follows $c + m + k \leq n + 3$, thus $(k + 1) + (c + m - 2) \leq n + 2$, hence $(k + 1)(c + m - 2) \leq \frac{1}{4}(n + 2)^2$. With the bound on $|w|$ from above we conclude that $|w| \leq n^2 + \frac{1}{4}(n + 2)n(n - 1)$, which is bounded by $\frac{1}{16}n^5 + \frac{15}{16}n^4$ for $n \geq 1$. \qed

The following lemma, which rests on the properties of $y$ and $z$, provides an alternative to the use of Carpi's Theorem 3 in the proof of Proposition 8.

**Lemma 17.** Suppose that $0 \notin M(\Sigma^*)$. Then $M(yz)$ has minimum rank in $M(\Sigma^*)$ and this rank is $k$.

**Proof.** It follows from Lemma 13 that each row of $M(yz)$ is either the zero vector or the characteristic vector of some $q_i z$. As the sets $q_i z$ for $i \in \{1, \ldots, k\}$ are nonempty and pairwise disjoint, it follows that $M(yz)$ has rank $k$.

Suppose $x \in \Sigma^*$ is such that $M(x)$ has rank less than $k$. Then $M(yzx)$ has rank less than $k$. Since the sets $q_i zx$ for $i \in \{1, \ldots, k\}$ are pairwise disjoint, there is $i \in \{1, \ldots, k\}$ such that $q_i zx = \emptyset$. In order to show that $0 \notin M(\Sigma^*)$ it suffices to show that for all $p \in Q$ and all $u \in \Sigma^*$ there is $w \in \Sigma^*$ such that $puw = \emptyset$. Let $p \in Q$ and $u \in \Sigma^*$. If $pu = \emptyset$ then choose $w = \epsilon$. Otherwise, let $v \in \Sigma^*$ be such that $puvy \ni q_i$. By Lemma 13, we have $puvy \cap \{q_1, \ldots, q_k\} = \{q_i\}$. Thus $puvyz = q_i z$ and $puvzyz = q_i zx = \emptyset$. Hence choose $w = vyzx$. \qed

To prove Proposition 8 we combine Lemma 16 with either Carpi’s Theorem 3 or Lemma 17.

**Proposition 8.** Given $M : \Sigma \to \mathbb{N}^{n \times n}$ such that $\rho(M) \leq 1$ and $M$ is strongly connected, one can compute in polynomial time a word $w \in \Sigma^*$ with $|w| \leq \frac{1}{16}n^5 + \frac{15}{16}n^4$ such that $M(w)$ has minimum rank in $M(\Sigma^*)$.

**Proof.** One can check in polynomial time whether $0 \notin M(\Sigma^*)$, see Proposition 2. If yes, then the minimum rank is 0, and Lemma 16 gives the result. Otherwise, 0 \notin M(\Sigma^*), and Lemmas 12 and 17 give the result.

In the case 0 \notin M(\Sigma^*) one may alternatively use Carpi’s Theorem 3: Indeed, the minimum rank $r$ is between 1 and $n$, and hence $n \geq 1$. Theorem 3 asserts the existence of a word $w$ such that $M(w)$ has rank $r$ and $|w| \leq \frac{1}{16}n^5 - n^3 + \frac{3}{4}n^2 - 3n + 1$, which is bounded by $\frac{1}{16}n^5 + \frac{15}{16}n^4$ for $n \geq 1$. An inspection of Carpi’s proof [4] shows that his proof is constructive and can be transformed into an algorithm that computes $w$ in polynomial time. \qed

### 3.2. Not Necessarily Strongly Connected

We prove Theorem 1:

**Theorem 1 (rephrased).** Given $M : \Sigma \to \mathbb{N}^{n \times n}$ with $\rho(M) \leq 1$, one can compute in polynomial time a word $w \in \Sigma^*$ with $|w| \leq \frac{1}{16}n^5 + \frac{15}{16}n^4$ such that $M(w)$ has minimum rank in $M(\Sigma^*)$. 
Proof. For any matrix $A$ denote by $rk(A)$ its rank. For $i, j \in \{1, \ldots, n\}$ write $i \to j$ if there is $u \in \Sigma^*$ such that $M(u)(i, j) > 0$, and write $i \leftrightarrow j$ if $i \to j$ and $j \to i$. The relation $\leftrightarrow$ is an equivalence relation. Denote by $C_1, \ldots, C_h \subseteq \{1, \ldots, n\}$ its equivalence classes ($h \leq n$). We can assume that whenever $i \in C_k$ and $j \in C_\ell$ and $i \to j$, then $k \leq \ell$. Hence, without loss of generality, $M(u)$ for any $u \in \Sigma^*$ has the following block-upper triangular form:

$$
M(u) = \begin{pmatrix}
M_{11}(u) & M_{12}(u) & \cdots & M_{1h}(u) \\
0 & M_{22}(u) & \cdots & M_{2h}(u) \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & M_{hh}(u)
\end{pmatrix},
$$

where $M_{ii}(u) \in \mathbb{N}[C_i \times C_i]$ for all $i \in \{1, \ldots, h\}$. For $i \in \{1, \ldots, h\}$ define $r_i := \min_{u \in \Sigma^*} rk(M_{ii}(u))$. For any $u \in \Sigma^*$ we have $rk(M(u)) \geq \sum_{i=1}^h rk(M_{ii}(u))$ (see, e.g., [10, Chapter 6.9.4]). It follows that the minimum rank among the matrices in $M(\Sigma^*)$ is at least $\sum_{i=1}^h r_i$.

Let $w_1, \ldots, w_h \in \Sigma^*$ be the words from Proposition 8 for $M_{11}, \ldots, M_{hh}$, respectively, so that $rk(M_{ii}(w_i)) = r_i$ holds for all $i \in \{1, \ldots, h\}$. Define $w := w_1 \cdots w_h$. Then we have:

$$
|w| \leq \sum_{i=1}^h |w_i| \leq \sum_{i=1}^h \frac{1}{16} |C_i|^5 + \frac{15}{16} |C_i|^4 \leq \frac{1}{16} n^5 + \frac{15}{16} n^4
$$

It remains to show that $rk(M(w)) \leq \sum_{i=1}^h r_i$. It suffices to prove that $rk(M_k(w_1 \cdots w_k)) \leq \sum_{i=1}^h r_i$ holds for all $k \in \{1, \ldots, h\}$, where $M_k(u)$ for any $u \in \Sigma^*$ is the principal submatrix obtained by restricting $M(u)$ to the rows and columns corresponding to $\bigcup_{i=1}^k C_i$. We proceed by induction on $k$. For the base case, $k = 1$, we have $rk(M_1(w_1)) = rk(M_{11}(w_1)) = r_1$. For the induction step, let $1 < k \leq h$. Then there are matrices $A_1, A_2, B_1, B_2$ such that:

$$
M_k(w_1 \cdots w_k) = M_k(w_1 \cdots w_{k-1})M_k(w_k) = 
\begin{pmatrix}
M_{k-1}(w_1 \cdots w_{k-1}) & A_1 \\
0 & A_2
\end{pmatrix}
\begin{pmatrix}
B_1 & B_2 \\
0 & M_{kk}(w_k)
\end{pmatrix}
= 
\begin{pmatrix}
M_{k-1}(w_1 \cdots w_{k-1}) & (B_1 A_2) \\
0 & B_2
\end{pmatrix} + 
\begin{pmatrix}
A_1 \\
A_2
\end{pmatrix}
\begin{pmatrix}
0 & M_{kk}(w_k)
\end{pmatrix}
$$

By the induction hypothesis, we have $rk(M_{k-1}(w_1 \cdots w_{k-1})) \leq \sum_{i=1}^{k-1} r_i$. Further, we have $rk(M_{kk}(w_k)) = r_k$. So the ranks of the two summands in (3.1) are at most $\sum_{i=1}^{k-1} r_i$ and $r_k$, respectively. Since for any matrices $A, B$ it holds $rk(A + B) \leq rk(A) + rk(B)$, we conclude that $rk(M_k(w_1 \cdots w_k)) \leq \sum_{i=1}^h r_i$, completing the induction proof.

4. Proof of Theorem 4.

THEOREM 4. Let $X \subseteq \Sigma^*$ be a finite code that has an uncompletable word. Define $k := \max_{x \in X} |x|$ and $m := \sum_{x \in X} |x|$ and assume $k > 0$. Then one can compute in polynomial time an uncompletable word of length at most $(k + 1)k^2(m + 2)(m + 1)$.

Consider the flower automaton associated to $X$, which is a UFA $\mathcal{A} = (\Sigma, Q, \delta)$ with $n = |Q| = m - |X| + 1$ states. The uncompletable words in $X$ are exactly the
killing words in $\mathcal{A}$. Towards a proof of Theorem 4 we first focus on computing a short killing word in $\mathcal{A}$.

To this end we optimize the construction from subsection 3.1 for flower automata. Denote by $0 \in Q$ the “central” state of $\mathcal{A}$ around which the petals are built. For each $q \in Q$ fix a word $u_q \in \Sigma^*$ such that $u_q = \{0\}$ and $|u_q| \leq k - 1$. The following lemma bounds the size of certain sets of states that survive long words:

**Lemma 18.** Let $w \in \Sigma^*$ with $|w| \geq k - 1$. Then for all $p \in Q$ and all $v \in \Sigma^*$ we have $|pv \cap vw| \leq k$, i.e., at most $k$ states of $pv$ survive $w$.

**Proof.** Towards a contradiction, suppose $|pv \cap w| > k$. By the pigeonhole principle, there are two different states $q_1, q_2$ with $q_1, q_2 \in pv \cap w$ such that $|u_{q_1}| = |u_{q_2}|$. Since $q_1, q_2$ both survive $w$, where $|w| \geq k - 1$, both $u_{q_1}$ and $u_{q_2}$ are prefixes of $w$. Hence $u_{q_1} = u_{q_2}$. It follows that $q_1 u_{q_1} = \{0\} = q_2 u_{q_1}$, i.e., $q_1, q_2$ are mergeable. But $q_1, q_2 \in pv$ are also coreachable, contradicting unambiguity. □

The following lemma adapts Lemma 11:

**Lemma 19.** For each $q \in Q$ one can compute in polynomial time a word $w_q \in \Sigma^*$ with $|w_q| \leq \frac{1}{2}(k - 1)(n + 2)n$ such that no state $q' \neq q$ survives $w_q$ and is coreachable with $q$.

**Proof.** We use the same algorithm as in the proof of Lemma 11, except that we initialize $w$ not to $\varepsilon$ but to some $w_{\text{init}} \in \Sigma^{k-1}$ with $qw_{\text{init}} \neq \emptyset$. Such $w_{\text{init}}$ exists, as $q$ is on some cycle. Let $\ell \in \mathbb{N}$ be the number of iterations of the loop in the algorithm. The computed word $w_q$ has the form $w_{q,q_1} \cdots w_{q,q_{\ell}} w_{\text{init}}$ for some states $q_1, \ldots, q_{\ell} \in Q$. It follows from the proof of Lemma 11 that for all $i \in \{1, \ldots, \ell\}$ we have $q w_{q,q_i} \cdots w_{q,q_i} w_{\text{init}} \supseteq q w_{q,q_i} \cdots w_{q,q_i} w_{\text{init}}$. Hence also $q w_{q,q_i} \cdots w_{q,q_i} w_{\text{init}} \supseteq q w_{q,q_i} \cdots w_{q,q_i} w_{\text{init}} Q$. Since $q \in w_{\text{init}} Q$, it follows that $|q w_{q,q_i} \cdots w_{q,q_i} w_{\text{init}} Q| \geq \ell + 1$. By Lemma 18 it follows $\ell + 1 \leq k$. Hence, using Lemma 10 we obtain $|w_q| = |w_{q,q_1} \cdots w_{q,q_{\ell}} w_{\text{init}}| \leq \frac{1}{2}(k - 1)(n + 2)(n - 1) + (k - 1) \leq \frac{1}{2}(k - 1)(n + 2)n$. □

The following lemma adapts Lemma 12:

**Lemma 20.** One can compute in polynomial time words $z, y \in \Sigma^*$ such that:

- $|z| \leq \frac{1}{2}(k - 1)(n + 2)(n + 1)$ and there are no two coreachable states that both survive $z$;
- $|y| \leq \frac{1}{2}(k - 1)(n + 2)(n + 1)$ and there are no two mergeable states that are both reached by $y$.

**Proof.** We use the same algorithm as in the proof of Lemma 12, except that we initialize $w$ not to $\varepsilon$ but to an arbitrary $w_{\text{init}} \in \Sigma^{k-1}$, and that for $w_q$ we use Lemma 19 instead of Lemma 11:

1: $w := w_{\text{init}}$
2: while there are coreachable $p, p'$ that both survive $w$ do
3: $q :=$ arbitrary state from $p w$
4: $w := w q w$ (with $w_q$ from Lemma 19)
5: return $z := w$

Consider a state $p \in Q$ picked in some iteration of the loop, i.e., $p$ survives the (current) word $w$. We claim that no state $\bar{p}$ with $|u_p| = |u_{\bar{p}}|$ will be picked in any future iteration. Indeed, let $\bar{p} \in Q$ be with $|u_p| = |u_{\bar{p}}|$ such that $\bar{p}$ survives a future $w$. Then $\bar{p}$ survives the current $w$. Since $|u_{p}| = |u_{\bar{p}}|$ and $p, \bar{p}$ both survive $w$ with $|w| \geq k - 1$, we have $u_p = u_{\bar{p}}$ and this word is a prefix of $w$. It follows that $p w = \bar{p} w$, thus $q \in p w$, where $q$ is the state from line 3. Suppose $\bar{p}'$ is an arbitrary state that is coreachable with $p$. 

Then the states in $\bar{p}'w$ are coreachable with $q$. Thus, $\bar{p}'ww_q = \emptyset$ and so $\bar{p}'$ does not survive any future $w$. It follows that $\bar{p}$ will not be picked in any future iteration.

Since for all $p \in Q$ we have $|u_p| \in \{0, \ldots, k - 1\}$, the algorithm performs at most $k$ loop iterations. Hence, using Lemma 19, the computed word $z$ has length at most $k \cdot \frac{1}{2}(k-1)(n+2)n + (k-1) \leq \frac{1}{2}k(k-1)(n+2)(n+1)$. The argument for $y$ is similar.

The following lemma adapts Lemma 16:

**Lemma 21.** One can compute in polynomial time a killing word of length at most $(k + 1)k^2(n + 2)(n + 1)$.

**Proof.** Let $z, y$ be the words from Lemma 20. We can assume that $|z| \geq k - 1$. First we argue that there are at most $k$ states that are reached by $y$ and survive $z$. Towards a contradiction, suppose otherwise. By the pigeonhole principle, there are two distinct states $q, q' \in Q$ that are reached by $y$ and survive $z$ and satisfy $|u_q| = |u_{q'}|$. Since $|z| \geq k - 1$, it follows that $u_q = u_{q'}$ is a prefix of $z$, thus $q, q'$ are mergeable. But $q, q'$ are reached by $y$, contradicting the definition of $y$.

It follows that the $k$ from subsection 3.1 is at most the $k$ from this section. Mirroring exactly the proof of Lemma 16 and using Lemma 20, we obtain a killing word $w$ of length at most

$$|w| \leq |yz| + k(n + |yz|) \leq n^2 + (k + 1)(|y| + |z|) \leq n^2 + (k + 1)k(k - 1)(n + 2)(n + 1) \leq (k + 1)k^2(n + 2)(n + 1).$$

Finally we prove Theorem 4:

**Proof of Theorem 4.** Since $k > 0$, it follows $|X| \geq 1$ and thus $n = m - |X| + 1 \leq m$. The result follows from Lemma 21.

5. **Proof of Theorem 5.**

**Theorem 5.** There is no polynomial $p$ such that the following holds:

Let $M : \Sigma^* \to \{0, 1\}^{n \times n}$ be a monoid morphism. Let $w_0 \in \Sigma^*$ be such that $M(w_0)$ has rank 1, and let $1$ be the minimum rank in $M(\Sigma^*)$.

Then there is $w \in \Sigma^*$ with $|w| \leq p(n)$ such that $M(w_0) = M(w)$.

**Proof.** Denote by $p_i$ the $i$th prime number (so $p_1 = 2$). Let $m \geq 1$. Define:

$$\Sigma := \{a, b_1, \ldots, b_m\}$$

$$Q_i := \{(i, 0), (i, 1), \ldots, (i, p_i - 1)\} \quad \text{for every } i \in \{1, \ldots, m\}$$

$$Q := \{0\} \cup \bigcup_{i=1}^m Q_i$$

Further, define a monoid morphism $M : \Sigma^* \to \mathbb{N}^{Q \times Q}$ by setting for all $i \in \{1, \ldots, m\}$

$$M(a)(0, (i, 0)) := 1$$

$$M(a)((i, j), (i, j + 1 \mod p_i)) := 1 \quad \text{for all } j \in \{0, \ldots, p_i - 1\}$$

$$M(b_i)(0, 0) := 1$$

$$M(b_i)((i, j), 0) := 1 \quad \text{for all } j \in \{0, \ldots, p_i - 1\}$$

and setting all other entries of $M(a), M(b_1), \ldots, M(b_m)$ to 0, see Figure 3. We have $M(\Sigma^*) \subseteq (0, 1)^{Q \times Q}$, i.e., $M(\Sigma^*)$ is an unambiguous monoid of relations. For all $q \in Q$ and all $q' \in Q \setminus \{0\}$ we have $M(b_1)(q, q') = 0$, i.e., $M(b_1)$ has rank 1. For all
Fig. 3. Automaton representation of $M$ for $m = 3$.

A shortest word $w_0 \in \Sigma^*$ such that $M(w_0)$ has rank 1 and $M(w_0)(0,(i,p_i - 1)) = 1$ holds for all $i \in \{1, \ldots, m\}$ is the word $w_0 = b_1 a^P$ where $P = \prod_{i=1}^{m} p_i \geq 2^m$. On the other hand, we have $|Q| = 1 + \sum_{i=1}^{m} p_i \in O(m^2 \log m)$ by the prime number theorem.

Hence there is no polynomial $p$ such that $P \leq p(|Q|)$ holds for all $m$.

REFERENCES

[1] P. Bell, M. Hirvensalo, and I. Potapov, *Mortality for $2 \times 2$ matrices is NP-hard*, in Proceedings of Mathematical Foundations of Computer Science (MFCS), Springer, 2012, pp. 148–159.

[2] J. Berstel and D. Perrin, *Trends in the theory of codes*, Bulletin of the EATCS, 29 (1986), pp. 84–95.

[3] J. Berstel, D. Perrin, and C. Reutenauer, *Codes and Automata*, Cambridge University Press, 2009.

[4] A. Carpi, *On synchronizing unambiguous automata*, Theoretical Computer Science, 60 (1988), pp. 285–296.

[5] A. Carpi and F. D’Alessandro, *On incomplete and synchronizing finite sets*, Theoretical Computer Science, 664 (2017), pp. 67–77.

[6] I. Daubechies and J. Lagarias, *Corrigendum/addendum to: Sets of matrices all infinite products of which converge*, Linear Algebra and its Applications, 327 (2001), pp. 69–83.

[7] P. Gorković, Z. Hedrlín, V. Koubek, and J. Ryšínková, *A game of composing binary relations*, R.A.I.R.O. Informatique théorique, 16 (1982), pp. 365–369.

[8] V. Gusev and E. Pribavkina, *On non-complete sets and Restivo’s conjecture*, in Proceedings of Developments in Language Theory (DLT), Springer, 2011, pp. 239–250.

[9] V. Halava, T. Harju, and M. Hirvensalo, *Undecidability bounds for integer matrices using Claus instances*, International Journal of Foundations of Computer Science, 18 (2007),
ON NONNEGATIVE INTEGER MATRICES AND SHORT KILLING WORDS

pp. 931–948.

[10] R. Horn and C. Johnson, *Matrix analysis*, Cambridge University Press, 2nd ed., 2013.

[11] S. Julia, A. Malapert, and J. Provillard, *A synergic approach to the minimal uncompletable words problem*, Journal of Automata, Languages and Combinatorics, 22 (2017), pp. 271–286.

[12] R. Jungers, V. Protasov, and V. Blondel, *Efficient algorithms for deciding the type of growth of products of integer matrices*, Linear Algebra and its Applications, 428 (2008), pp. 2296–2311.

[13] J.-Y. Kao, N. Rampersad, and J. Shallit, *On NFAs where all states are final, initial, or both*, Theoretical Computer Science, 410 (2009), pp. 5010–5021.

[14] P. Martugin, *A series of slowly synchronizing automata with a zero state over a small alphabet*, Information and Computation, 206 (2008), pp. 1197–1203.

[15] M. Paterson, *Unsolvability in 3×3 matrices*, Studies in Applied Mathematics, 49 (1970), pp. 105–107.

[16] I. Potapov and P. Semukhin, *Decidability of the membership problem for 2×2 integer matrices*, in Proceedings of the Symposium on Discrete Algorithms (SODA), SIAM, 2017, pp. 170–186.

[17] A. Restivo, *Some remarks on complete subsets of a free monoid*, in Quaderni de “La Ricerca Scientifica”. Non-Commutative Structures in Algebra and Geometric Combinatorics, vol. 109, Consiglio Nazionale Delle Ricerche, 1981, pp. 19–25.

[18] A. Ryzhikov and M. Szykułka, *Finding short synchronizing words for prefix codes*, in Proceedings of Mathematical Foundations of Computer Science (MFCS), vol. 117 of LIPIcs, 2018, pp. 21:1–21:14.

[19] M.-P. Schützenberger, *On the definition of a family of automata*, Information and Control, 4 (1961), pp. 245–270.

[20] W. Tzeng, *A polynomial-time algorithm for the equivalence of probabilistic automata*, SIAM Journal on Computing, 21 (1992), pp. 216–227.

[21] M. Volkov, *Synchronizing automata and the Černý conjecture*, in Proceedings of Language and Automata Theory and Applications (LATA), Springer, 2008, pp. 11–27.

[22] A. Weber and H. Seidl, *On finitely generated monoids of matrices with entries in N*, Informatique Théorique et Applications, 25 (1991), pp. 19–38.