On Finite Monoids over Nonnegative Integer Matrices and Short Killing Words

Stefan Kiefer
University of Oxford, UK

Corto Mascle
ENS Paris-Saclay, France

Abstract

Let n be a natural number and $\mathcal{M}$ a set of $n \times n$-matrices over the nonnegative integers such that $\mathcal{M}$ generates a finite multiplicative monoid. We show that if the zero matrix 0 is a product of matrices in $\mathcal{M}$, then there are $M_1, \ldots, M_{n^5} \in \mathcal{M}$ with $M_1 \cdots M_{n^5} = 0$. This result has applications in automata theory and the theory of codes. Specifically, if $X \subset \Sigma^*$ is a finite incomplete code, then there exists a word $w \in \Sigma^*$ of length polynomial in $\sum_{x \in X} |x|$ such that w is not a factor of any word in X^*. This proves a weak version of Restivo's conjecture.

2012 ACM Subject Classification Theory of computation → Formal languages and automata theory

Keywords and phrases matrix semigroups, unambiguous automata, codes, Restivo's conjecture

Digital Object Identifier 10.4230/LIPIcs.STACS.2019.43

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

1 Introduction

Let $\mathbb{N} = \{0, 1, 2, \ldots\}$. In this paper 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. Denote by $\overline{\mathcal{M}}$ the monoid generated by $\mathcal{M}$ under matrix multiplication. If $\overline{\mathcal{M}}$ is finite 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 in $\overline{\mathcal{M}}$. Further, $M_1, \ldots, M_\ell$ can be computed in time polynomial in the description size of $\mathcal{M}$.*

The mortality problem. Theorem 1 is related to the *mortality* problem for matrices: given a finite set $\mathcal{M}$ of matrices, can the zero matrix (which is defined to have rank 0) be expressed as a finite product of matrices in $\mathcal{M}$? Paterson [14] showed that the mortality problem is undecidable for 3×3 integer matrices, i.e., $\mathcal{M} \subset \mathbb{Z}^{3 \times 3}$. It remains undecidable for $\mathcal{M} \subset \mathbb{Z}^{3 \times 3}$ with $|\mathcal{M}| = 7$ and for $\mathcal{M} \subset \mathbb{Z}^{21 \times 21}$ with $|\mathcal{M}| = 2$, see [8]. Mortality for 2×2 integer matrices is NP-hard [1] and not known to be decidable, see [15] for recent work on the 2×2 case.

The mortality problem for *nonnegative* matrices is much easier, as for each matrix entry it only matters whether it is zero or nonzero, so one can assume $\mathcal{M} \subseteq \{0, 1\}^{n \times n}$. This version is naturally phrased in terms of automata. Let $\mathcal{A} = (\Sigma, Q, \delta)$ be a *nondeterministic finite automaton (NFA)* over a finite alphabet Σ, a finite set Q of states, and with transition function $\delta : Q \times \Sigma \to 2^Q$ (initial and final states do not play a role here). A word $w \in \Sigma^*$ is called *killing word* for $\mathcal{A}$ if w does not label any path in $\mathcal{A}$. Associate to $\mathcal{A}$ the monoid morphism $M_\mathcal{A} : \Sigma^* \to \mathbb{N}^{Q \times Q}$ where for all $a \in \Sigma$ we define $M_\mathcal{A}(a)(p, q) = 1$ if $\delta(p, a) \ni q$ and 0 otherwise. Then, for any word $w \in \Sigma^*$ we have that $M_\mathcal{A}(w)(p, q)$ is the number of w-labelled paths from p to q. 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 [12], and there are examples where the shortest killing word has exponential length in the number of states of the automaton [6, 12]. This implies that the assumption in Theorem 1 that the

© Stefan Kiefer and Corto Mascle;
licensed under Creative Commons License CC-BY
36th International Symposium on Theoretical Aspects of Computer Science (STACS 2019).
Editors: Rolf Niedermeier and Christophe Paul; Article No. 43; pp. 43:1–43:13
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

generated monoid $\overline{\mathcal{M}}$ be finite cannot be dropped. Whether $\overline{\mathcal{M}}$ is finite can be checked in polynomial time [11], see also [21] and the references therein. If $\overline{\mathcal{M}}$ is finite then the mortality problem for nonnegative integer matrices is solvable in polynomial time:

▶ **Proposition 2.** *Let $\mathcal{M} \subseteq \mathbb{N}^{n\times n}$ be a finite set of nonnegative integer matrices, generating a finite monoid $\overline{\mathcal{M}}$. One can decide in polynomial time if $0 \in \overline{\mathcal{M}}$.*

Short killing words for unambiguous finite automata. In the central proofs of this paper, the finiteness assumption can be further strengthened so that it corresponds to unambiguousness of NFAs. More precisely, an NFA $\mathcal{A} = (\Sigma, Q, \delta)$ 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 $\overline{\mathcal{M}} \subseteq \mathbb{N}^{n\times n}$ an *unambiguous monoid of relations* if $\overline{\mathcal{M}} \subseteq \{0,1\}^{n\times n}$. For any UFA $\mathcal{A}$ the image $M_{\mathcal{A}}(\Sigma^*)$ of the monoid morphism $M_{\mathcal{A}}$ is an unambiguous monoid of relations, and any unambiguous monoid of relations can be viewed in this way.

Proposition 2 provides a polynomial-time procedure for checking whether a UFA has a killing word. Define ρ as the spectral radius of the rational matrix $\frac{1}{|\Sigma|}\sum_{a\in\Sigma} M(a)$. One can show that $\mathcal{A}$ has a killing word if $\rho < 1$, and otherwise $\rho = 1$. Proposition 2 then follows from the fact that one can compare ρ with 1 in polynomial time. Thus the spectral radius tells whether there *exists* a killing word, but does not *provide* a killing word. Neither does this method imply a polynomial bound on the length of a minimal killing word, let alone a polynomial-time algorithm for computing a killing word. Theorem 1, which is proved purely combinatorially, fills this gap: if there is a killing word, then one can compute a killing word of length $O(|Q|^5)$ in polynomial time. NP-hardness results for approximating the length of a shortest killing word were proved in [17], even for the case $|\Sigma| = 2$ and for *partial DFAs*, which are UFAs with $|\delta(p, a)| \le 1$ for all $p \in Q$ and all $a \in \Sigma$.

Short minimum-rank words. Define the *rank* of a UFA $\mathcal{A} = (\Sigma, Q, \delta)$ as the minimum rank of the matrices $M_{\mathcal{A}}(w)$ for $w \in \Sigma^*$. A word w such that the rank of $M_{\mathcal{A}}(w)$ 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 $|\delta(p, a)| = 1$ for all $p \in Q$ and all $a \in \Sigma$. In DFAs of rank 1, minimum-rank words are called *synchronizing* because $\delta(Q, w)$ 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 [20] 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 $\mathcal{A} = (\Sigma, Q, \delta)$ be a UFA of rank $r \ge 1$ such that the state transition graph of $\mathcal{A}$ is strongly connected. Let $n := |Q| \ge 1$. Then $\mathcal{A}$ has a minimum-rank word of length at most $\frac{1}{2}rn(n-1)^2 + (2r-1)(n-1)$.*

This implies an $O(n^4)$ bound for the case where $r \ge 1$. 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. Theorem 1 provides, to the best of the authors' knowledge, the first polynomial bound, $O(n^5)$, on the length of shortest minimum-rank words for UFAs.

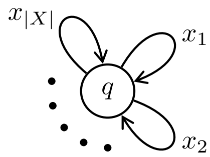


Figure 1 Given a finite language $X \subseteq \Sigma^*$, the flower automaton $\mathcal{A}_X$ has one "petal" for each word $x \in X$. Thus $\delta(q, w) \ni q$ holds if and only if $w \in X^*$. If X is a code then $\mathcal{A}_X$ is unambiguous.

Restivo's conjecture. Let $X \subseteq \Sigma^*$ be a finite set of words over a finite alphabet Σ, and define $k := \max_{x \in X} |x|$. A word $v \in \Sigma^*$ is called *uncompletable* in X if there are no words $u, w \in \Sigma^*$ such that $uvw \in X^*$, i.e., v is not a factor of any word in X^*. In 1981 Restivo [16] 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 [7]. A recent article [10] 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 $X \subseteq \Sigma^*$ is called a *code* if every word $w \in X^*$ has at most one decomposition $w = x_1 \cdots x_\ell$ with $x_1, \ldots, x_\ell \in X$. See [3] for a comprehensive reference on codes. For a finite code $X \subseteq \Sigma^*$ define $m := \sum_{x \in X} |x|$. Given X one can construct a *flower automaton* [3, Chapter 4.2], which is a UFA $\mathcal{A}_X = (\Sigma, Q, \delta)$ 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.

Is any product a short product? It was shown in [21] that if $\overline{\mathcal{M}} \subseteq \mathbb{N}^{n \times n}$ is finite then for *every* matrix $M \in \overline{\mathcal{M}}$ there are $M_1, \ldots, M_\ell \in \mathcal{M}$ with $\ell \leq \lceil e^2 n! \rceil - 2$ such that $M = M_1 \cdots M_\ell$. It was also shown in [21] that such a bound on ℓ cannot be smaller than 2^{n-2}. In view of Theorem 1 one may ask if a polynomial bound on ℓ exists for *low-rank* matrices M. The answer is no, even for unambiguous monoids of relations and even when M has rank 1 and when 1 is the minimum rank in $\overline{\mathcal{M}}$:

▶ **Theorem 4.** *There is no polynomial p such that the following holds:*

Let $n \in \mathbb{N}$, let $\mathcal{M} \subseteq \{0,1\}^{n \times n}$ generate an unambiguous monoid of relations $\overline{\mathcal{M}} \subseteq \{0,1\}^{n \times n}$. Let $M \in \overline{\mathcal{M}}$ have rank 1, and let 1 be the minimum rank in $\overline{\mathcal{M}}$. Then there are $M_1, \ldots, M_\ell \in \mathcal{M}$ with $\ell \leq p(n)$ such that $M = M_1 \cdots M_\ell$.

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 can the $O(n^5)$ upper bound be improved? A *synchronizing* 0*-automaton* is a DFA $\mathcal{A} = (\Sigma, Q, \delta)$ 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 $\mathcal{A}$ 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 $|\Sigma| = 2$ [13]. This implies that the $O(n^5)$ upper bound from Theorem 1 cannot be improved to $o(n^2)$, not even in the case that 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 paper. In the remaining three sections we prove Proposition 2, Theorem 1, and Theorem 4, respectively.

2 Proof of Proposition 2

Let $\mathcal{M} \subseteq \mathbb{N}^{n\times n}$ be a finite set of nonnegative integer matrices, generating a finite monoid $\overline{\mathcal{M}}$. 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 $M : \Sigma^* \to \overline{\mathcal{M}}$. Thus we may write $M(\Sigma^*)$ for $\overline{\mathcal{M}}$.

Towards a proof of Proposition 2, define the rational nonnegative matrix $A \in \mathbb{Q}^{n\times n}$ 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 5.** *We have $\rho \leq 1$.*

Proof. Since $M(\Sigma^*)$ is finite, it is bounded. Hence $(A^k)_{k\in\mathbb{N}}$ is bounded. By the Perron-Frobenius theorem, A has a nonnegative left eigenvector $u \in \mathbb{R}^n$ with $uA = \rho u$. So $uA^k = \rho^k u$. It follows $\rho \leq 1$. ◀

▶ **Lemma 6.** *We have $\rho < 1$ if and only if there is $w \in \Sigma^*$ 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 $w_0 \in \Sigma^*$ with $M(w_0) = 0$. Since $M(\Sigma^*)$ is finite, there is $B \in \mathbb{N}$ such that all entries of all matrices in $M(\Sigma^*)$ are at most B. For any $k \in \mathbb{N}$ define $W(k) := \Sigma^k \setminus (\Sigma^* w_0 \Sigma^*)$, 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 $w \in \Sigma^k \setminus W(k)$. It follows that any entry of A^k is at most $\frac{|W(k)|}{|\Sigma^k|} \cdot B$. 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

$$\left(1 - \frac{1}{|\Sigma^{|w_0|}|}\right)^m .$$

It follows that $\lim_{k\to\infty} \frac{|W(k)|}{|\Sigma^k|} = 0$. Hence $\lim_{k\to\infty} A^k = 0$ and so $\rho < 1$. ◀

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

▶ **Proposition 2.** *Let $\mathcal{M} \subseteq \mathbb{N}^{n\times n}$ be a finite set of nonnegative integer matrices, generating a finite monoid $\overline{\mathcal{M}}$. One can decide in polynomial time if $0 \in \overline{\mathcal{M}}$.*

Proof. By Lemma 6, it suffices to check whether $\rho < 1$.

If $\rho < 1$ then the linear system $xA = x$ does not have a nonzero solution. Conversely, if $\rho \geq 1$ then, by Lemma 5, we have $\rho = 1$ and thus, by the Perron-Frobenius theorem, the linear system $xA = x$ has a (real) nonzero solution.

Hence it suffices to check if $xA = x$ 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 a monoid morphism with finite image $M(\Sigma^*)$. Call M *strongly connected* if for all $i, j \in \{1, \dots, n\}$ there is $w \in \Sigma^*$ with $M(w)(i, j) \geq 1$. In subsection 3.1 we consider the case where 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 7.** *Let $M : \Sigma^* \to \mathbb{N}^{n\times n}$ be strongly connected with finite $M(\Sigma^*)$. Given $M : \Sigma \to \mathbb{N}^{n\times n}$, 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 8.** *If M is strongly connected, then $M(\Sigma^*) \subseteq \{0, 1\}^{n\times n}$.*

Proof. Let M be strongly connected. 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 finiteness of $M(\Sigma^*)$. ◀

Lemma 8 allows us to view the strongly connected case in terms of UFAs. Define a UFA $\mathcal{A} = (\Sigma, Q, \delta)$ with $Q = \{1, \dots, n\}$ 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. We extend $\delta : Q \times \Sigma \to 2^Q$ in the usual way to $\delta : 2^Q \times \Sigma^* \to 2^Q$ by setting $\delta(P, a) := \bigcup_{q\in P} \delta(q, a)$ and $\delta(P, \varepsilon) := P$ and $\delta(P, wa) := \delta(\delta(P, w), a)$, where $P \subseteq Q$ and $a \in \Sigma$ and ε is the empty word and $w \in \Sigma^*$. 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 $pw \neq \emptyset$. 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 $pw \supseteq \{q_1, q_2\}$), and they are called *mergeable* when there is $w \in \Sigma^*$ with $q_1w \cap q_2w \neq \emptyset$. 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 $m := \max\{|wq| : w \in \Sigma^*,\ q \in Q\}$. The following lemma says that one can compute short witnesses for coreachability:

▶ **Lemma 9.** *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 $qw_{q,q'} \supseteq \{q, q'\}$.*

Proof. Let $q \neq q'$ be coreachable states. Then there are $p \in Q$ and $v \in \Sigma^*$ with $pv \supseteq \{q, q'\}$. Since M is strongly connected, there is $u \in \Sigma^*$ with $qu \ni p$, hence $quv \supseteq \{q, q'\}$. Define an edge-labelled directed graph $G = (V, E)$ with vertex set $V = \{\{r, s\} : r, s \in Q\}$ and edge set

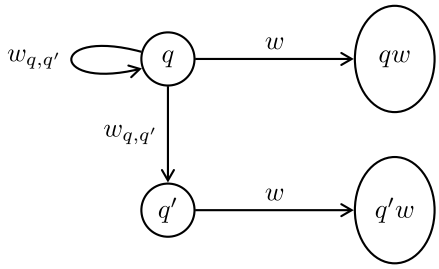
$E = \{(R, a, S) \in V \times \Sigma \times V : Ra \supseteq S\}$. Since $quv \supseteq \{q, q'\}$, the graph G has a path, labelled with uv, from $\{q\}$ to $\{q, q'\}$. The shortest path from $\{q\}$ to $\{q, q'\}$ has at most $|V| - 1$ edges and is thus labelled with a word $w \in \Sigma^*$ with $|w| \le |V| - 1 = \frac{1}{2}n(n+1) - 1 = \frac{1}{2}(n+2)(n-1)$. For this w we have $qw \supseteq \{q, q'\}$. ◀

▶ **Lemma 10.** *For each $q \in Q$ one can compute in polynomial time a word $w_q \in \Sigma^*$ with $|w_q| \le \frac{1}{2}(c-1)(n+2)(n-1)$ 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. $w := \varepsilon$ (the empty word)
2. while there is $q' \in C(q)$ such that q' survives w:
   $w := w_{q,q'}w$ (with $w_{q,q'}$ from Lemma 9)
3. 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 with $w_{q,q'}w$, contradicting unambiguousness. It follows that $qw_{q,q'}w \supsetneq qw$. 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 $|w_q| \le \frac{1}{2}(c-1)(n+2)(n-1)$. 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 11.** *One can compute in polynomial time words $z, y \in \Sigma^*$ such that:*

- $|z| \le \frac{1}{4}(c-1)(n+2)n(n-1)$ *and there are no two coreachable states that both survive z;*
- $|y| \le \frac{1}{4}(m-1)(n+2)n(n-1)$ *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. $w := \varepsilon$ (the empty word)
2. while there are coreachable p, p' that both survive w:
   $q :=$ arbitrary state from pw
   $w := ww_q$ (with w_q from Lemma 10)
3. return $z := w$

We show that the set

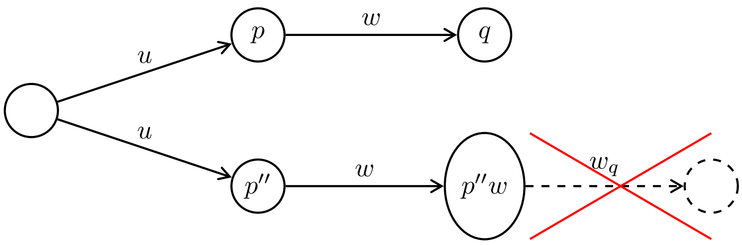
$$B \;:=\; \{p \in Q : \exists\, p'' \in C(p) \text{ such that both } p, p'' \text{ survive } w\}$$

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

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

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 unambiguousness and since $q \in pw$, we have $q \notin p''w$. 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 $p \notin B'$. 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 $p' \notin B'$.

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 10 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 11), see Figure 2.

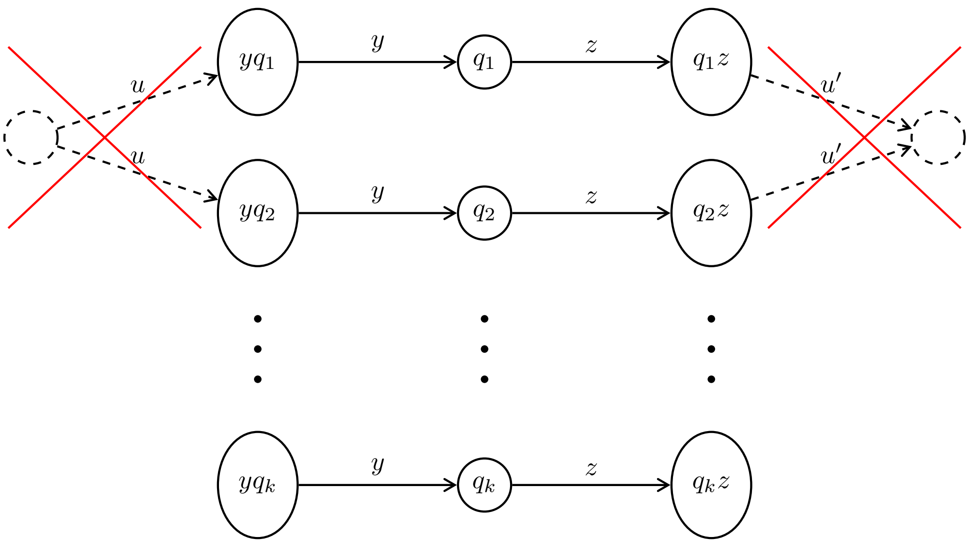


Figure 2 The states $q_1, \ldots, q_k$ are neither coreachable nor mergeable.

▶ **Lemma 12.** *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 11). ◀

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

▶ **Lemma 13.** *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 $q_i zxy \supseteq \{q_j, q_{j'}\}$ and $q_j, q_{j'}$ are not coreachable (by Lemma 12), we have $j' = j$. Hence $q_j z = q_{j'} z \ni q'$. ◀

Provided that there is a killing word (which can be checked via Proposition 2 in polynomial time), 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 based technique for checking equivalence of automata that are weighted over a field. This technique goes back to Schützenberger [18] and has often been rediscovered, see, e.g., [19].

▶ **Lemma 14.** *Suppose there exists $w_0 \in \Sigma^*$ with $M(w_0) = 0$ (this word w_0 may not be given). For each $i \in \{1, \ldots, k\}$ one can compute in polynomial time a word $x_i \in \Sigma^*$ with $|x_i| \le n$ such that $q_i z x_i yz = \emptyset$.*

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 $|x| \le n$ such that $q_i zx \cap y\{q_1, \ldots, q_k\} = \emptyset$.

Define $e \in \{0,1\}^Q$ as the row vector with $e(q) = 1$ if and only if $q \in q_i z$. Define $f \in \{0,1\}^Q$ as the row vector with $f(q) = 1$ if and only if $q \in y\{q_1, \ldots, q_k\}$. First we show that for any $x \in \Sigma^*$ we have $eM(x)f^\top \le 1$, where the superscript $\top$ denotes transpose. Towards a contradiction suppose $eM(x)f^\top \ge 2$. Then there are two distinct x-labelled paths from $q_i z$ 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 unambiguousness, these paths end in two distinct states $q_j, q_{j'}$. But then $q_j, q_{j'}$ are coreachable, contradicting Lemma 12. Hence we have shown that $eM(x)f^\top \le 1$ holds for all $x \in \Sigma^*$.

Define the (row) vector space

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

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

1. $B := \{\varepsilon\}$ (where ε is the empty word)
2. while there are $u \in B$ and $a \in \Sigma$ such that $\begin{pmatrix} eM(ua) & 1 \end{pmatrix} \notin \left\langle \begin{pmatrix} eM(x) & 1 \end{pmatrix} : x \in B \right\rangle$:
   $B := B \cup \{ua\}$
3. return B

Observe that the algorithm performs at most n iterations of the loop body, as every iteration increases the dimension of the space $\left\langle \begin{pmatrix} eM(x) & 1 \end{pmatrix} : x \in B \right\rangle$ by 1, but the dimension cannot grow larger than $n + 1$. Hence $|x| \le n$ holds for all $x \in B$. Since $eM(w_0)f^\top = 0 \ne 1$, the space V is not orthogonal to $\begin{pmatrix} f & -1 \end{pmatrix}$. So there exists $x \in B$ such that $eM(x)f^\top \ne 1$. Since $eM(x)f^\top \le 1$, we have $eM(x)f^\top = 0$. Hence $q_i zx \cap y\{q_1, \ldots, q_k\} = \emptyset$. ◀

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

▶ **Lemma 15.** *Suppose there is $w_0 \in \Sigma^*$ with $M(w_0) = 0$ (this word w_0 may not be given). One can compute in polynomial time a word $w \in \Sigma^*$ with $M(w) = 0$ and $|w| \le \frac{1}{16}n^5 + \frac{15}{16}n^4$.*

Proof. For any $1 \le j < j' \le k$ the sets $q_j z$ and $q_{j'} z$ are disjoint by Lemma 12 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 14, i.e., $q_i z x_i yz = \emptyset$. By Lemma 13, for any $j \in \{1, \ldots, k\}$ the generator of $q_j z x_i yz$ 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 Pzx_iyz.

Consider the following algorithm:

1. $w := yz$
2. while $Qw \neq \emptyset$:
   $q_i :=$ arbitrary element of the generator of Qw
   $w := wx_iyz$
3. 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 11 and 14,

$$|w| \;\le\; |yz|+k(n+|yz|) \;\le\; n^2+(k+1)(|y|+|z|) \;\le\; n^2+\frac{1}{4}(k+1)(c+m-2)(n+2)n(n-1)\,.$$

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:

$$c+m+k \;\le\; n + |qu \cap u'q'| + |qu \cap \{q_1, \ldots, q_k\}| + |\{q_1, \ldots, q_k\} \cap u'q'|$$

The sets qu and $u'q'$ overlap in at most one state by unambiguousness. The sets qu and $\{q_1, \ldots, q_k\}$ overlap in at most one state by Lemma 12, and similarly for $\{q_1, \ldots, q_k\}$ and $u'q'$. It follows $c+m+k \le n+3$, thus $(k+1)+(c+m-2) \le n+2$, hence $(k+1)(c+m-2) \le \frac{1}{4}(n+2)^2$. With the bound on the length of w above we conclude that $|w| \le n^2 + \frac{1}{16}(n+2)^3 n(n-1)$, which is bounded by $\frac{1}{16}n^5 + \frac{15}{16}n^4$ for $n \ge 1$. ◀

We combine Lemma 15 and Carpi's Theorem 3 to prove Proposition 7:

▶ **Proposition 7.** *Let $M : \Sigma^* \to \mathbb{N}^{n \times n}$ be strongly connected with finite $M(\Sigma^*)$. Given $M : \Sigma \to \mathbb{N}^{n \times n}$, one can compute in polynomial time a word $w \in \Sigma^*$ with $|w| \le \frac{1}{16}n^5 + \frac{15}{16}n^4$ such that $M(w)$ has minimum rank in $M(\Sigma^*)$.*

Proof. One can check in polynomial time whether there is $w_0 \in \Sigma^*$ with $M(w_0) = 0$, see Proposition 2. If yes, then the minimum rank is 0, and Lemma 15 gives the result.

Otherwise, the minimum rank r is between 1 and n, and hence $n \ge 1$. Theorem 3 asserts the existence of a word w such that $M(w)$ has rank r and $|w| \le \frac{1}{2}n^4 - n^3 + \frac{5}{2}n^2 - 3n + 1$, which is bounded by $\frac{1}{16}n^5 + \frac{15}{16}n^4$ for $n \ge 1$. 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. ◀

3.2 Not Necessarily Strongly Connected

We prove Theorem 1:

▶ **Theorem 1.** *Let $n \in \mathbb{N}$ and $\mathcal{M} \subseteq \mathbb{N}^{n\times n}$ be a finite set of nonnegative integer matrices. Denote by $\overline{\mathcal{M}}$ the monoid generated by $\mathcal{M}$ under matrix multiplication. If $\overline{\mathcal{M}}$ is finite 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 in $\overline{\mathcal{M}}$. Further, $M_1, \ldots, M_\ell$ can be computed in time polynomial in the description size of $\mathcal{M}$.*

In terms of the previous notions in the proof we can rephrase Theorem 1 as follows:

▶ **Theorem 1** (rephrased)**.** *Let $M : \Sigma^* \to \mathbb{N}^{n\times n}$ be a monoid morphism whose image $M(\Sigma^*)$ is finite. Given $M : \Sigma \to \mathbb{N}^{n\times n}$, 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., [9, Chapter 0.9.4]). 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 7 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 $rk(M_k(w_1 \cdots w_k)) \leq \sum_{i=1}^{k} r_i$ 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:

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

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 (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 $rk(M_k(w_1 \cdots w_k)) \leq \sum_{i=1}^{k} r_i$, completing the induction proof. ◀

4 Proof of Theorem 4

In terms of the previous notions we can rephrase Theorem 4 as follows:

▶ **Theorem 4** (rephrased). *There is no polynomial p such that the following holds:*

Let $M : \Sigma^* \to \{0,1\}^{Q\times Q}$ 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 $|w| \le p(|Q|)$ such that $M(w_0) = M(w)$.

Proof. Denote by p_i the ith prime number (so $p_1 = 2$). Let $m \ge 1$. Define:

$$\begin{aligned} \Sigma &:= \{a, b_1, \ldots, b_m\} \\ Q_i &:= \{(i,0), (i,1), \ldots, (i, p_i - 1)\} \quad \text{for every } i \in \{1, \ldots, m\} \\ Q &:= \{0\} \cup \bigcup_{i=1}^{m} Q_i \end{aligned}$$

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

$$\begin{aligned} M(a)(0,(i,0)) &:= 1 \\ M(a)((i,j),(i,j+1 \bmod p_i)) &:= 1 \quad \text{for all } j \in \{0, \ldots, p_i - 1\} \\ M(b_i)(0,0) &:= 1 \\ M(b_i)((i,j),0) &:= 1 \quad \text{for all } j \in \{0, \ldots, p_i - 1\} \end{aligned}$$

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 $w \in \Sigma^*$ there is $q \in Q$ with $M(w)(0,q) = 1$, i.e., 1 is the minimum rank in $M(\Sigma^*)$. 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 $P = \prod_{i=1}^m p_i \ge 2^m$. 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 $P \le p(|Q|)$ holds for all m. ◀

References

1. P.C. Bell, M. Hirvensalo, and I. Potapov. Mortality for 2 ×2 Matrices Is NP-Hard. In *Proceedings of Mathematical Foundations of Computer Science (MFCS)*, pages 148–159. Springer, 2012.
2. J. Berstel and D. Perrin. Trends in the theory of codes. *Bulletin of the EATCS*, 29:84–95, 1986.
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(3):285–296, 1988.
5. A. Carpi and F. D'Alessandro. On incomplete and synchronizing finite sets. *Theoretical Computer Science*, 664:67–77, 2017.
6. P. Goralčík, Z. Hedrlín, V. Koubek, and J. Ryšlinková. A game of composing binary relations. *R.A.I.R.O. Informatique théorique*, 16(4):365–369, 1982.
7. V.V. Gusev and E.V. Pribavkina. On Non-complete Sets and Restivo's Conjecture. In *Proceedings of Developments in Language Theory (DLT)*, pages 239–250. Springer, 2011.

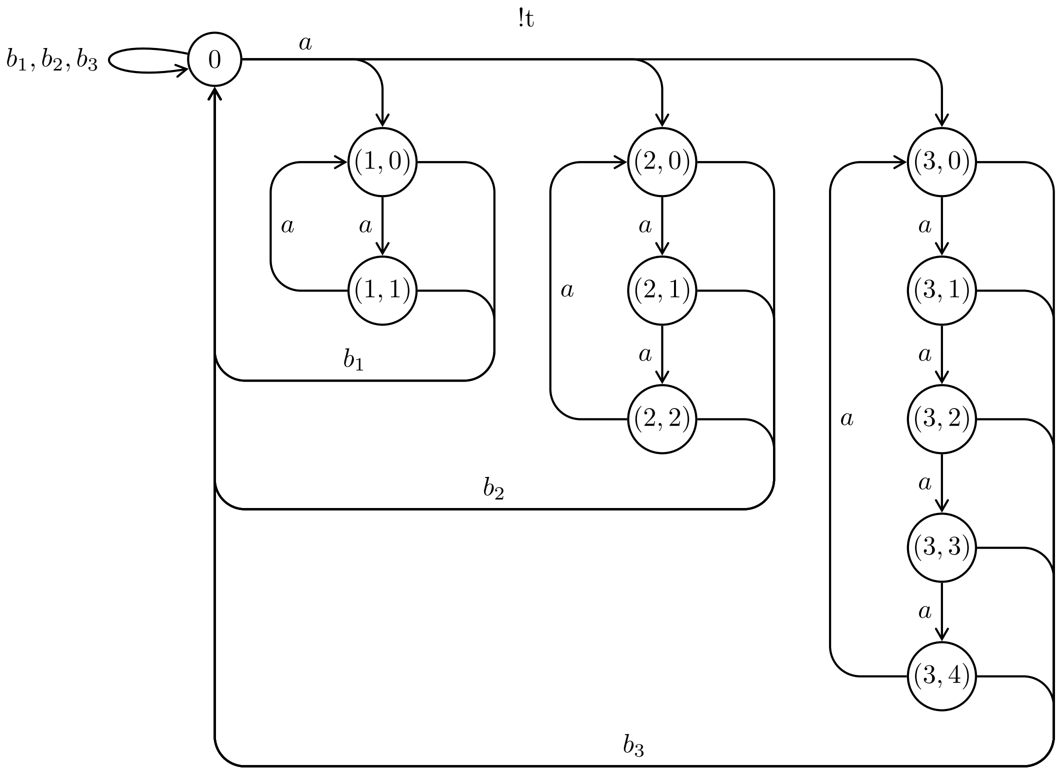


Figure 3 Automaton representation of M for $m = 3$.

8 V. Halava, T. Harju, and M. Hirvensalo. Undecidability Bounds for Integer Matrices Using Claus Instances. *International Journal of Foundations of Computer Science*, 18(5):931–948, 2007.

9 R.A. Horn and C.R. Johnson. *Matrix analysis*. Cambridge University Press, 2nd edition, 2013.

10 S. Julia, A. Malapert, and J. Provillard. A Synergic Approach to the Minimal Uncompletable Words Problem. *Journal of Automata, Languages and Combinatorics*, 22(4):271–286, 2017.

11 R.M. Jungers, V. Protasov, and V.D. Blondel. Efficient algorithms for deciding the type of growth of products of integer matrices. *Linear Algebra and its Applications*, 428(10):2296–2311, 2008.

12 J.-Y. Kao, N. Rampersad, and J. Shallit. On NFAs where all states are final, initial, or both. *Theoretical Computer Science*, 410(47):5010–5021, 2009.

13 P.V. Martugin. A series of slowly synchronizing automata with a zero state over a small alphabet. *Information and Computation*, 206(9-10):1197–1203, 2008.

14 M.S. Paterson. Unsolvability in 3 × 3 Matrices. *Studies in Applied Mathematics*, 49(1):105–107, 1970.

15 I. Potapov and P. Semukhin. Decidability of the Membership Problem for 2 × 2 integer matrices. In *Proceedings of the Symposium on Discrete Algorithms (SODA)*, pages 170–186. SIAM, 2017.

16 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*, volume 109, pages 19–25. Consiglio Nazionale Delle Ricerche, 1981.

17 A. Ryzhikov and M. Szykuła. Finding Short Synchronizing Words for Prefix Codes. In *Proceedings of Mathematical Foundations of Computer Science (MFCS)*, volume 117 of *LIPIcs*, pages 21:1–21:14, 2018.

18 M.-P. Schützenberger. On the definition of a family of automata. *Information and Control*, 4:245–270, 1961.

19 W. Tzeng. A Polynomial-Time Algorithm for the Equivalence of Probabilistic Automata. *SIAM Journal on Computing*, 21(2):216–227, 1992.

20 M.V. Volkov. Synchronizing Automata and the Černý Conjecture. In *Proceedings of Language and Automata Theory and Applications (LATA)*, pages 11–27. Springer, 2008.

21 A. Weber and H. Seidl. On finitely generated monoids of matrices with entries in ℕ. *Informatique Théorique et Applications*, 25(1):19–38, 1991.