Matrix Mortality and the Černý-Pin Conjecture

Jorge Almeida[1⋆] and Benjamin Steinberg[2⋆⋆]

[1] Departamento de Matemática Pura, Faculdade de Ciências, Universidade do Porto, Rua do Campo Alegre, 687, 4169-007 Porto, Portugal
[2] School of Mathematics and Statistics, Carleton University, 1125 Colonel By Drive, Ottawa, Ontario K1S 5B6, Canada
jalmeida@fc.up.pt, bsteinbg@math.carleton.ca

Abstract. In this paper, we establish the Černý-Pin conjecture for automata with the property that their transition monoid cannot recognize the language $\{a,b\}^*ab\{a,b\}^*$. For the subclass of automata whose transition monoids have the property that each regular $\mathscr{J}$-class is a subsemigroup, we give a tight bound on lengths of reset words for synchronizing automata thereby answering a question of Volkov.

1 Introduction

In 1964 Černý conjectured that any n-state synchronizing automaton has a reset word of length at most $(n-1)^2$. Despite years of intensive work [2–6, 8, 12, 18, 19, 27, 28, 34–37, 39, 41–43], the best known upper bound is $\frac{n^3-n}{6}$, due to Pin [29] based on a non-trivial result of Frankl from extremal set theory; see also [20]. Černý, himself, showed that $(n-1)^2$ is the best one can hope for [8]. Pin generalized the conjecture as follows [28]. Suppose (Q,Σ) is an automaton such that some word $w \in \Sigma^*$ acts on Q as a transformation of rank r. Then he proposed that there should be a word of length at most $(n-r)^2$ acting as a rank r transformation. This generalized conjecture was disproved by Kari [18]. However, there is a reformulation of the Pin conjecture that is still open (and that was interpreted by Rystsov as being the Pin conjecture [35]). This conjecture is sometimes known as the Rank conjecture or the Černý-Pin conjecture. It states that if r is the minimal rank of a transformation in the transition monoid of an n-state automaton (in which case we say the automaton has rank r), then there is a word of length at most $(n-r)^2$ that acts as a transformation of rank r. The case $r=1$ is the Černý conjecture.

This paper is a contribution to this form of the Černý-Pin conjecture. To state our main result, we recall the notion of a variety of finite monoids [13]. A *variety of finite monoids* is a class of finite monoids closed under taking finite products, submonoids and homomorphic images [13]. There is a bijection between varieties

⋆ The first author was supported, in part, by FCT through CMUP and also through the project PTDC/MAT/65481/2006, which is partly funded by the European Community Fund FEDER.
⋆⋆ The second author was supported in part by NSERC and the DFG.

of finite monoids and varieties of languages [13]. Recall that the variety **DS** [1,32], introduced by Schützenberger [38], consists of all finite monoids whose regular $\mathscr{J}$-classes are subsemigroups. The variety **EDS** consists of all monoids whose idempotents generate a submonoid belonging to **DS**. For example, this variety contains all monoids with commuting idempotents. It is known that **EDS** is the largest variety of finite monoids that does not contain the syntactic monoid of the language $\{a,b\}^*ab\{a,b\}^*$ and that a monoid belongs to **EDS** if and only if it cannot recognize the language $\{a,b\}^*ab\{a,b\}^*$ (cf. [32, Chapter 7]). We show that, for an n-state automaton of rank r whose transition monoid belongs to **EDS**, there is a word of length at most $(n-r)(n-r+1)/2$ which acts as a transformation of rank r. This bound is tight for this class since Rystsov gave an example of an n-state synchronizing automaton whose transition monoid has commuting idempotents and whose minimal length reset word has length $n(n-1)/2$ [34]. As most papers just focus on the original Černý conjecture, this result gives the widest class of monoids for which the more general Černý-Pin conjecture is known to hold.

We also give a tight bound of $n-1$ on the length of reset words for n-state synchronizing automata with transition monoid in the pseudovariety **DS** [1, 32], improving the result of [2] and answering a question of Volkov [43]. Our techniques are a continuation of the representation theoretic approach to the Černý conjecture initiated in [2,6,39], and also are an elaboration on an idea of Rystsov [35].

The key notion in this paper is that of a mortality function for a finite monoid S. A mortality function measures the lengths of zero words under matrix representations of S. We estimate mortality functions by reducing to the case of irreducible representations and using the theory of Munn, Ponizovsky, Rhodes and Zalcstein [9, 15, 23, 24, 33]. These results are then applied to a particular representation coming from an automaton. The paper ends with a universal mortality function that relies on the effective solution to the Burnside problem for matrix semigroups [7, 14, 17, 22, 25, 40].

A journal version of this paper is under preparation that extends the results to a much more general class of automata, which is a bit more technical to define.

2 Mortality Functions

In this paper, all monoids are assumed finite except free monoids and full matrix monoids. We use Σ^* to denote the free monoid on a set Σ. If Σ is a generating set for a monoid S, we will abuse notation and not distinguish between $w \in \Sigma^*$ and the element of S represented by w. All actions of monoids are on the right. Denote by $\mathbb{N}$ the set of positive integers. By a *representation* of a monoid S of *degree* n, we mean a monoid homomorphism $\varphi\colon S \to M_n(\mathbb{Q})$ where $M_n(\mathbb{Q})$ is the monoid of $n \times n$ matrices over the field of rational numbers $\mathbb{Q}$. If $v \in \mathbb{Q}^n$ and $s \in S$, then $v\varphi(s)$ will be abbreviated to vs.

Definition 2.1 (Mortality function). *Let S be a monoid. By a* ***mortality function*** *for S, we mean a function $f\colon \mathbb{N} \to \mathbb{N}$ such that, for all representations*

$\varphi\colon S \to M_n(\mathbb{Q})$ of degree n with $0 \in \varphi(S)$ and all generating sets Σ of S, there is a word $w \in \Sigma^*$ of length at most $f(n)$ so that $\varphi(w) = 0$.

The terminology mortality comes from [26]. The reader is referred to [10, 11] for basic notions and definitions from representation theory. Notice that a mortality function is non-decreasing since if $\varphi\colon S \to M_n(\mathbb{Q})$ is a representation with $0 \in \varphi(S)$ and $\psi\colon S \to \mathbb{Q}$ is the degree 1 representation sending the group of units of S to 1 and all other elements to 0, then $\varphi \oplus \psi$ has degree $n+1$ and contains 0, so from this it follows that $f(n) \leq f(n+1)$. Also note that $f(n) = |S| - 1$ is a mortality function for S and so we are really interested in mortality functions with "good" constants, rather than in asymptotics. Most of the time we are interested in degrees that are significantly smaller than $|S|$. Also, we want mortality functions that are valid for whole classes of monoids and not just for a single monoid. We remark that if $\varphi\colon S \to T$ is an onto homomorphism and f is a mortality function for S, then f is also a mortality function for T.

There is a connection between mortality under matrix representations and the Černý-Pin problem due to Rystsov [35]. To state the Černý-Pin conjecture, we need a few definitions. The *rank* of a transformation is the size of its image. An automaton (Q, Σ) has *rank* r if r is the minimal rank of an element of its transition monoid S. Notice that the set of elements of minimal rank in S is an ideal and hence contains the minimal ideal. We now state the Černý-Pin (or Rank) conjecture.

Conjecture 2.2 (Černý-Pin). An automaton of rank r has a word of length at most $(n-r)^2$ representing a transformation of rank r.

The Černý conjecture is the special case when $r = 1$; the general statement is a variation on a conjecture of Pin. An automaton of rank 1 is called *synchronizing* and a word representing a transformation of rank 1 is often termed a *reset word*.

A function $f\colon \mathbb{N} \to \mathbb{N}$ is called *superadditive* if, for all $m, n \in \mathbb{N}$, one has that $f(m) + f(n) \leq f(m+n)$. We are mostly interested in superadditive mortality functions. The following is a variant on a result of Rystsov [35].

Proposition 2.3. *Let (Q, Σ) be an n-state automaton of rank r with transition monoid S. Let f be a supperadditive mortality function for S. Then there is a word $w \in \Sigma^*$ of length at most $f(n-r)$ so that $|Qw| = r$.*

Proof. Without loss of generality, assume $Q = \{1, \ldots, n\}$. Linearize the action of S on Q to a matrix representation $\varphi\colon S \to M_n(\mathbb{Q})$ by setting $e_i s = e_{is}$ where $e_1, \ldots, e_n$ is the standard basis for $\mathbb{Q}^n$.

Assume first that S acts transitively on Q, that is, the automaton (Q, Σ) is strongly connected. If $X \subseteq Q$, let $\overline{X}$ denote the characteristic vector of X. Let $\mathscr{C}$ be the set of images of rank r elements of S. Notice that S acts on $\mathscr{C}$. Indeed, the elements of rank r in S form an ideal and so if $t \in S$ has rank r, then $|Qts| = r$ for all $s \in S$ and so $Qt \in \mathscr{C}$ implies $Qts \in \mathscr{C}$. Let V be the subspace of $\mathbb{Q}^n$ spanned by the elements $\overline{X} - \overline{Y}$ such that $X, Y \in \mathscr{C}$. It is easy to see that V is S-invariant. We claim that $Vs = 0$, for $s \in S$, if and only if s has rank r.

First note that if s has rank r, then for any $X \in \mathscr{C}$ one has $Xs = Qs$ since both sets have size r. Thus $(\overline{X} - \overline{Y})s = 0$. For the converse, suppose that s has rank greater than r. Let $X \in \mathscr{C}$ and choose $q \in Qs \setminus Xs$. Choose $p \in Q$ so that $ps = q$ and let $Y \in \mathscr{C}$ such that $p \in Y$. Such a Y exists as S acts transitively on Q. Then $(\overline{X} - \overline{Y})s \neq 0$ since $\overline{X}s$ has 0 in the q-coordinate while $\overline{Y}s$ has 1 in this coordinate.

Next we show that $\dim V \leq n - r$. First of all let $s \in S$ have rank r and let $P_1, \ldots, P_r$ be the equivalence classes of the kernel of s. Since these sets are disjoint, it is immediate that their characteristic vectors are linearly independent. Let W be the subspace spanned by the $\overline{P_i}$, $i = 1, \ldots, r$. Then $\dim W = r$ and hence $\dim W^{\perp} = n - r$. Suppose now that $X \in \mathscr{C}$. Since $|Xs| = |X| = r$, it follows that $|X \cap P_i| = 1$ all i. In other words, $\overline{X} \cdot \overline{P_i} = 1$ for all i. Thus if $X, Y \in \mathscr{C}$, then $\overline{X} - \overline{Y} \perp \overline{P_i}$, for all i. We conclude that $V \subseteq W^{\perp}$ and hence $\dim V \leq n - r$. The result now follows in the transitive case.

Now suppose that S does not act transitively on Q. The S-invariant subsets of Q are ordered by inclusion. Let $C_1, \ldots, C_\ell$ be the minimal S-invariant subsets of Q, that is, the minimal strongly connected components of the automaton (Q, Σ). Then the C_i are disjoint and S acts transitively on each C_i by minimality. First suppose that $Q = C_1 \cup \ldots \cup C_\ell$. Let $n_i = |C_i|$ and let r_i be the rank of (C_i, Σ). Plainly $n = n_1 + \cdots + n_\ell$ and, moreover, one easily verifies that $r = r_1 + \cdots + r_\ell$ (consider an element of the minimal ideal of S). Since the transition monoid of (C_i, Σ) is a quotient of S, it admits f as a mortality function. It now follows from the previous case that we have, for each i, a word w_i of length at most $f(n_i - r_i)$ with $|C_i w_i| = r_i$. Then $w = w_1 \cdots w_\ell$ represents a transformation of Q of rank r and the length of w is at most $\sum_{i=1}^{\ell} f(n_i - r_i) \leq f(n - r)$ by superadditivity.

Next suppose that $C = C_1 \cup \cdots \cup C_\ell \neq Q$. Since C contains all the minimal S-invariant subsets, it is easy to see that $qS \cap C \neq \emptyset$ for all $q \in Q \setminus C$. Consequently, the set $\{s \in S \mid Qs \subseteq C\}$ is a non-empty ideal of S and hence contains the minimal ideal. Thus r is also the rank of (C, Σ). Indeed, if $s \in S$ belongs to the minimal ideal, then $Qs \subseteq C$ and hence $Qs = Qs^2 \subseteq Cs$ (the equality $Qs = Qs^2$ follows from minimality of the rank of s).

Now S acts by partial transformations on $X = Q \setminus C$ by restriction; moreover, the elements of the minimal ideal of S act via the empty transformation by the above paragraph. Thus by linearizing this partial transformation action of S on X, we obtain a representation $\rho \colon S \to M_{|X|}(\mathbb{Q})$ with $0 \in \rho(S)$. Hence there is a word w of length at most $f(n - |C|)$ representing the empty transformation on X, i.e., so that $Qw \subseteq C$. Because the transition monoid of (C, Σ) is a quotient of S, it has f as a mortality function, so by the previous case there is a word u of length at most $f(|C| - r)$ so that $|Cu| = r$. Then $r \leq |Qwu| \leq |Cu| = r$ so wu represents a transformation of rank r. Since f is superadditive,

$$|wu| \leq f(n - |C|) + f(|C| - r) \leq f(n - r)$$

as required. □

It is natural to try to obtain a mortality function for S by reducing to the case of an irreducible representation: a representation of S is called *irreducible* if there are no proper, non-zero S-invariant subspaces. To do this, we need to deal with composition series.

Lemma 2.4. *Let $\varphi\colon S \to M_n(\mathbb{Q})$ be a representation and let*

$$0 = V_k \subseteq V_{k-1} \subseteq \cdots \subseteq V_0 = \mathbb{Q}^n$$

be a tower of S-invariant subspaces. Suppose that, for $i = 0, \ldots, k-1$, there are elements $s_i \in S$ with $V_i s_i \subseteq V_{i+1}$. Then $\varphi(s_0 s_1 \cdots s_{k-1}) = 0$.

Proof. Straightforward induction shows that $V_0 s_0 \cdots s_i \subseteq V_{i+1}$, from which the result follows as $V_k = 0$. □

The above lemma lets us enact our reduction to the case of irreducible representations.

Proposition 2.5. *Let $f\colon \mathbb{N} \to \mathbb{N}$ be a superadditive function and suppose that, for all irreducible representations $\rho\colon S \to M_d(\mathbb{Q})$ with $0 \in \rho(S)$ and for all generating sets Σ of S, there exists $w \in \Sigma^*$ so that $|w| \leq f(d)$ and $\rho(w) = 0$. Then f is a mortality function for S.*

Proof. Let $\varphi\colon S \to M_n(\mathbb{Q})$ be a representation so that $0 \in \varphi(S)$ and fix a generating set Σ for S. Let $0 = V_k \subseteq V_{k-1} \subseteq \cdots \subseteq V_0 = \mathbb{Q}^n$ be a composition series for $\mathbb{Q}^n$, that is, an unrefinable tower of S-invariant subspaces. Let $\rho_i\colon S \to \mathrm{End}(V_i/V_{i+1})$ be the associated irreducible representation. Since $0 \in \varphi(S)$, it follows immediately that $0 \in \rho_i(S)$. Thus, by assumption, we can find words w_i, for $0 \leq i \leq k-1$, with $V_i w_i \subseteq V_{i+1}$ and $|w_i| \leq f(d_i)$ where d_i is the dimension of V_i/V_{i+1}. Now $d_0 + \cdots + d_{k-1} = n$ and $\varphi(w_0 w_1 \cdots w_{k-1}) = 0$ by Lemma 2.4. Since f is superadditive, $|w_0 w_1 \cdots w_{k-1}| \leq f(d_0) + \cdots + f(d_{k-1}) \leq f(n)$. This completes the proof. □

It was proved in [2] that if $S \in \mathbf{DS}$, $\varphi\colon S \to M_n(\mathbb{Q})$ is an irreducible representation with $0 \in \varphi(S)$ and Σ is a generating set of S, then there is an element of Σ which is mapped to the zero matrix. Since the function $f(n) = n$ is superadditive, it now follows from Proposition 2.5 that $f(n) = n$ is a mortality function for S. Putting it all together, we obtain:

Theorem 2.6. *Let S be a monoid in $\mathbf{DS}$. Then $f(n) = n$ is a mortality function for S. Hence, if (Q, Σ) is a synchronizing automaton with transition monoid in $\mathbf{DS}$, then it has a reset word of length at most $n-1$ and moreover this bound is tight. More generally, if (Q, Σ) is an automaton of rank r with transition monoid in $\mathbf{DS}$, then there is a word $w \in \Sigma^*$ of length at most $n - r$ so that $|Qw| = r$.*

Proof. In light of Proposition 2.3, the argument before the theorem statements proves everything except the tightness. For tightness, just use an n-state counter-free automaton over a unary alphabet. □

The above theorem generalizes Rystsov's result for the case of commutative monoids [34] and answers a question raised by Volkov [43]. The following lemma is due to Rystsov [34] and will be used later to obtain our main result.

Lemma 2.7. *Let S be a monoid acting by partial transformations on an n element set and suppose that some element of S acts as the empty function. Let Σ be a generating set for S. Then there is a word $w \in \Sigma^*$ of length at most $n(n+1)/2$ acting as the empty function.*

Rystsov shows in [34] that the bound in the above lemma is tight. The monoid in his example is an inverse semgroup.

3 The Structure of Monoids in EDS

We briefly recall here some structural results concerning monoids in **EDS**. The reader is referred to [32, Appendix A] or [1, 9, 21] for the basic structure theory of finite monoids. Let us denote by $\mathrm{Reg}(S/\mathscr{J})$ the set of regular $\mathscr{J}$-classes of a monoid S. We write J_s for the $\mathscr{J}$-class of s and use similar notation for $\mathscr{L}$-classes and $\mathscr{R}$-classes.

Let J be a regular $\mathscr{J}$-class of a monoid S. Then there is an isomorphism $J^0 \cong \mathscr{M}^0(G, A, B, C)$ of the principal factor J^0 with a Rees matrix semigroup with sandwich matrix $C\colon B \times A \to G^0$ [9,21,32] where G is the maximal subgroup of J, A is the set of $\mathscr{R}$-classes of J and B is the set of $\mathscr{L}$-classes of J. It follows from Graham's Theorem [16] (cf. [32, Theorem 4.13.34]) that S belongs to **EDS** if and only if, for each regular $\mathscr{J}$-class J of S, we can always choose the sandwich matrix C to have a block diagonal form

$$C = \begin{bmatrix} C_1 & 0 & \cdots & 0 \\ 0 & C_2 & 0 & \vdots \\ \vdots & 0 & \ddots & 0 \\ 0 & \cdots & 0 & C_r \end{bmatrix} \tag{3.1}$$

where each C_i is a matrix over G (with no zero entries). We define r to be the *rank* of J, which we denote by $\mathrm{rk}(J)$. It can be defined independently of the Rees matrix representation in the following way. Continuing to denote the set of $\mathscr{L}$-classes of J by B, define an equivalence relation on B by setting $L_1 \sim_L L_2$ if, for all $\mathscr{R}$-classses R of J, one has $R \cap L_1$ contains an idempotent if and only if $R \cap L_2$ contains an idempotent. Observing that $C_{ba} \neq 0$ if and only if the $\mathscr{H}$-class $b \cap a$ contains an idempotent, it follows that r is the number of blocks of the partition associated to $\sim_L$. (The journal version of this article will define the rank of a regular $\mathscr{J}$-class for arbitrary finite monoids.)

The monoid S acts by partial functions on the right of J by right multiplication, where rs is undefined if $r \in J$, $s \in S$, but $rs \notin J$. Moreover, it is easy to see that s acts as the empty function on J if and only if $J_s \not\geq_{\mathscr{J}} J$. Indeed, if $J_s \not\geq_{\mathscr{J}} J$, trivially s acts as the empty function. Conversely, if $usv \in J$

with $u, v \in S^1$, then since J is regular we can find an idempotent e so that $eusv = usv \in J$. Thus $eu, eus \in J$ and so the action of s on $eu \in J$ is defined. Define an equivalence relation $\equiv$ on J by putting $s \equiv t$ if $L_s \sim_L L_t$. Denote by $[r]$ the $\equiv$-class of r.

Proposition 3.1. *There is a well defined action of S on $J/\equiv$ by partial functions given by*

$$[r]s = \begin{cases} [rs] & rs \in J \\ \textit{undefined} & \textit{else.} \end{cases}$$

Moreover, $s \in S$ acts as the empty function on $J/\equiv$ if and only if $J_s \not\geq_{\mathscr{J}} J$.

Proof. Let us begin with the following claim.

Claim. Suppose $t_1 \equiv t_2$. Then, for all $x \in J$, one has $t_1 x \in J$ if and only if $t_2 x \in J$.

Proof. If $E(J)$ denotes the set of idempotents of J, then standard finite semigroup theory [1, 9, 21, 32] yields

$$\begin{aligned} t_1 x \in J &\iff L_{t_1} \cap R_x \cap E(J) \neq \emptyset \\ &\iff L_{t_2} \cap R_x \cap E(J) \neq \emptyset \\ &\iff t_2 x \in J. \end{aligned}$$

□

Suppose now that $t_1 \equiv t_2$ and let $s \in S$. We first establish that $t_1 s \in J$ if and only if $t_2 s \in J$. Indeed, if $t_1 s \in J$, we can find an idempotent $e \in E(J)$ so that $t_1 se = t_1 s \in J$ by regularity of J. Thus $se \in J$ and so by the claim $t_2 se \in J$, whence $t_2 s \in J$. The reverse implication is proved in an identical manner.

Next assume that $t_1 s, t_2 s \in J$. We establish that if R' is an $\mathscr{R}$-class of J, then

$$R' \cap L_{t_1 s} \cap E(J) \neq \emptyset \iff R' \cap L_{t_2 s} \cap E(J) \neq \emptyset.$$

Suppose that $e \in R' \cap L_{t_1 s}$ is an idempotent. Then $t_1 se = t_1 s \in J$ and $se \in J$. Thus the claim implies $t_2 se \in J$. It follows that $R' \cap L_{t_2 s}$ contains an idempotent. The reverse implication is proved in the same fashion. We conclude that the action of S on $J/\{\equiv\}$ is well defined. Verifying the axioms of an action is straightforward and left to the reader.

By the definition of the action, it is clear that $s \in S$ acts as the empty function on $J/\equiv$ if and only if it acts as the empty function on J. The final statement now follows from the discussion before the proposition. □

The above proposition is valid for regular $\mathscr{J}$-classes of any monoid, not just those in **EDS**. However, one can verify that $S \in$ **EDS** if and only if the above action is by partial injective functions for each regular $\mathscr{J}$-class J. Since we do not need this result, we do not prove it here.

The following proposition will be used to estimate mortality bounds for monoids in **EDS**.

Proposition 3.2. *Let $S \in$ **EDS** and suppose that J is a regular $\mathscr{J}$-class of S other than the minimal ideal. Given a generating set Σ for S, there is a word $w \in \Sigma^*$ of length at most $\mathrm{rk}(J)(\mathrm{rk}(J)+1)/2$ so that $J_w \not\geq_{\mathscr{J}} J$.*

Proof. The result follows from applying Lemma 2.7 to the action of S on $J/\equiv$ by partial functions and using Proposition 3.1. □

4 A Mortality Function for EDS

We begin with some basic facts concerning the representation theory of monoids. We take a minimalist approach, stating exactly what we need in order to prove our main result. Details can be found in [9,15,24,30,33]. To fix notation, if S is a monoid, we use $\mathrm{Irr}(S)$ to denote the set of equivalence classes of irreducible representations of S. The reader should verify that every irreducible representation of a group is by invertible maps.

Let S be a monoid. Fix a maximal subgroup G_J for each regular $\mathscr{J}$-class J of S. Then the theory of Munn and Ponizovsky says that $\mathrm{Irr}(S)$ is in bijection with $\coprod_{J \in \mathrm{Reg}(S/\mathscr{J})} \mathrm{Irr}(G_J)$. Following Munn, if ρ^* is the irreducible representation of S corresponding to an irreducible representation ρ of G_J, then the $\mathscr{J}$-class J is called the *apex* of ρ^*. Suppose that d is the degree of ρ. Let $C\colon B \times A \to G_J^0$ be the sandwich matrix for J and denote by $\rho \otimes C$ the $d|B| \times d|A|$ matrix obtained by applying ρ entrywise to C (where we take $\rho(0)$ to be the $d \times d$ zero matrix). The following result can be extracted from [33] and [9, Chapter 5]; see also [30] and [31, Chapter 15] for a summary without proofs or [15, 23] for module-theoretic statements and proofs.

Theorem 4.1 (Munn, Ponizovsky). *Suppose that S is a finite monoid. Let $\rho^*\colon S \to M_n(\mathbb{Q})$ be an irreducible representation with apex J corresponding to an irreducible representation $\rho\colon G_J \to M_d(\mathbb{Q})$ of the maximal subgroup of J. Let $C\colon B \times A \to G_J^0$ be the sandwich matrix of J. Then:*

1. *The degree of ρ^* is the rank of the matrix $\rho \otimes C$;*
2. *For $s \in S$, one has $\rho^*(s) = 0$ if and only if $J_s \not\geq_{\mathscr{J}} J$.*

Now we are ready to prove that $f(n) = n(n+1)/2$ is a superadditive mortality function for monoids in **EDS**.

Theorem 4.2. *Let $S \in$ **EDS**. Then $f(n) = n(n+1)/2$ is a superadditive mortality function for S.*

Proof. It is routine to verify that f is superadditive. Thus it suffices to consider irreducible representations by Proposition 2.5. So let $\varphi\colon S \to M_n(\mathbb{Q})$ be an irreducible representation with $0 \in \varphi(S)$ and let Σ be a generating set for S. Let $J \in \mathrm{Reg}(S/\mathscr{J})$ be the apex of φ; note that J is not the minimal ideal of S. Suppose that $\varphi = \rho^*$ where $\rho\colon G_J \to M_d(\mathbb{Q})$ is an irreducible representation of the maximal subgroup G_J of J. Putting $r = \mathrm{rk}(J)$, we can find by Proposition 3.2 a word w of length at most $r(r+1)/2$ with $J_w \not\geq_{\mathscr{J}} J$ and hence with $\varphi(w) = 0$

by Theorem 4.1. It thus suffices to prove that $r \leq n$. Since $S \in \mathbf{EDS}$, we can place C in the block form (3.1) where the C_i are matrices over G_J (with no zero entries). Then evidently,

$$\rho \otimes C = \begin{bmatrix} \rho \otimes C_1 & 0 & \cdots & 0 \\ 0 & \rho \otimes C_2 & 0 & \vdots \\ \vdots & 0 & \ddots & 0 \\ 0 & \cdots & 0 & \rho \otimes C_r \end{bmatrix}.$$

Since $\rho(g)$ is invertible for all $g \in G$, it now follows that the rank of $\rho \otimes C$ is at least r. But this rank is the degree n of φ by Theorem 4.1. This completes the proof of the theorem. □

We can now resolve the Černý-Pin conjecture for automata with transition monoid in **EDS**.

Corollary 4.3. *Every synchronizing automaton with transition monoid in* **EDS** *has a reset word of length at most* $n(n-1)/2$ *and this bound is sharp. More generally, if* (Q, Σ) *is an automaton of rank* r *whose transition monoid is in* **EDS**, *then there is a word of length at most* $(n-r)(n-r+1)/2$ *representing a transformation of rank* r.

Proof. The upper bound is a direct consequence of Proposition 2.3 and Theorem 4.2. The sharpness follows from an example of Rystsov [34] of an n-state synchronizing automaton whose transition monoid has commuting idempotents with shortest reset word of length $n(n-1)/2$. □

5 A Universal Mortality Function

It is natural to ask whether there is a single function that is a mortality function for every finite monoid.

Definition 5.1 (Universal mortality function). *A* ***universal mortality function*** *is a function* $f\colon \mathbb{N} \to \mathbb{N}$ *which is a mortality function for all finite monoids.*

It is not *a priori* clear that there exist universal mortality functions. In fact, a famous result of Paterson [26] asserts that it is undecidable whether the monoid generated by a finite collection of 3×3 integer matrices contains the zero matrix and so there can be no 'universal' mortality function if one lifts the restriction on finiteness. A result proved independently by Mandel and Simon [22] and by Jacob [17] (see also [7, Chapter IX]) easily implies that one can find a simultaneous mortality function for all finitely generated monoids with at most k generators for any given k. But this is not good enough for our purposes.

We use the methods from the solution of the Burnside problem for matrix semigroups [7, 14, 25, 40] to establish the existence of a universal mortality function. More precisely, we show that the function $f\colon \mathbb{N} \to \mathbb{N}$ given by

$$f(n) = \begin{cases} 1 & n = 1 \\ (2n-1)^{n^2} - 1 & n > 1 \end{cases} \tag{5.1}$$

is a superadditive universal mortality function. The journal version of the paper will contain a slightly better bound.

The proof of the following elementary proposition is left to the reader.

Proposition 5.2. *The function f from* (5.1) *is superadditive.*

So to prove that f is a universal mortality function, it suffices to consider irreducible representations. Let us say that a submonoid S of $M_n(\mathbb{Q})$ is *irreducible* if the inclusion map $S \hookrightarrow M_n(\mathbb{Q})$ is an irreducible representation.

Recall that a subalgebra $\mathfrak{A} \subseteq M_n(\mathbb{Q})$ is said to be *irreducible* if the only $\mathfrak{A}$-invariant subspaces of $\mathbb{Q}^n$ are $\{0\}$ and $\mathbb{Q}^n$. An algebra is *simple* if it has no ideals. We shall need the following well-known result (cf. [9, Theorem 5.7]) going back to Burnside.

Theorem 5.3. *An irreducible subalgebra of $M_n(\mathbb{Q})$ is simple.*

If $a \in M_n(\mathbb{Q})$, then $\operatorname{tr} a$ denotes the trace of a. Our next lemma relies on a little bit of algebraic number theory.

Lemma 5.4. *Let $a \in M_n(\mathbb{Q})$ have finite order, that is, $|\langle a \rangle| < \infty$. Then $\operatorname{tr} a \in \mathbb{Z}$ and $|\operatorname{tr} a| \leq n$. Moreover, if $|\operatorname{tr} a| = n$, then a is invertible.*

Proof. By assumption, $a^m = a^{m+k}$ for some $m, k > 0$. Thus the minimal polynomial of a divides $x^m(x^k - 1)$ and so each non-zero eigenvalue is a k^{th}-root of unity. Thus $\operatorname{tr} a$ is an algebraic integer, being a sum of algebraic integers. But $\operatorname{tr} a \in \mathbb{Q}$ and hence $\operatorname{tr} a \in \mathbb{Z}$ as the rational algebraic integers are precisely the integers. Suppose $\lambda_1, \ldots, \lambda_n$ are the complex eigenvalues of a listed with multiplicity. Then

$$|\operatorname{tr} a| = \left| \sum_{i=1}^{n} \lambda_i \right| \leq \sum_{i=1}^{n} |\lambda_i| \leq n$$

since each λ_i is zero or a root of unity. Moreover, if $|\operatorname{tr} a| = n$, then no $\lambda_i = 0$ and so a is invertible. □

The following lemma uses traces to bound mortality. The essential idea goes back to Burnside [10]. We use the well-known and easy to prove fact that if S is a monoid with n elements generated as a monoid by a set Σ, then each element of S can be represented by a word of length at most $n - 1$.

Lemma 5.5. *Let $\Sigma \subseteq M_n(\mathbb{Q})$ be such that $S = \langle \Sigma \rangle$ is a finite irreducible submonoid, $0 \in S$ and $S \setminus \{0\}$ contains a singular matrix. Let J be the apex of the irreducible representation $S \hookrightarrow M_n(\mathbb{Q})$ and let G be a maximal subgroup of J. Suppose that $|\{\operatorname{tr} g \mid g \in G\} \cup \{0\}| = m$. Then there is a word $w \in \Sigma^*$ of length at most $m^{n^2} - 1$ mapping to the zero matrix in S.*

Proof. Let $\mathfrak{A}$ be the subalgebra of $M_n(\mathbb{Q})$ spanned by S; then $\mathfrak{A}$ is irreducible and hence simple by Theorem 5.3. Let $I = J \cup \{0\}$; it is the unique 0-minimal ideal of S as a consequence of Theorem 4.1. The span of I is a non-zero ideal of $\mathfrak{A}$ and hence $\mathfrak{A}$, being simple, is spanned by I. Thus there exists a basis $\{s_1, \ldots, s_d\}$ for $\mathfrak{A}$ consisting of elements of J; note that $d = \dim \mathfrak{A} \leq n^2$.

Consider now the trace form $(a, b) \mapsto \operatorname{tr}(ab)$ on $\mathfrak{A}$. The associativity of multiplication in $\mathfrak{A}$ and the linearity of the trace functional immediately yield that the trace form is a (symmetric) bilinear form on $\mathfrak{A}$. Since the identity matrix I_n is in $S \subseteq \mathfrak{A}$ and $\operatorname{tr} I_n = n$, it follows that the trace form is not identically 0 on $\mathfrak{A}$. Thus the radical of the trace form is a proper ideal of $\mathfrak{A}$, and hence zero by the simplicity of $\mathfrak{A}$. Thus the trace form is non-degenerate on $\mathfrak{A}$. Consequently, if $a \in \mathfrak{A}$, then a is determined by the d rational numbers $\operatorname{tr}(as_i)$, for $i = 1, \ldots, d$.

In particular, consider $s \in S$. Then $ss_i \in I$, for $i = 1, \ldots, d$. Let

$$A = \{\operatorname{tr} g \mid g \in G\} \cup \{0\}.$$

We claim that $\operatorname{tr}(ss_i) \in A$. This is evident if $ss_i = 0$. If $ss_i \in J$, but not in a maximal subgroup, then $(ss_i)^2 = 0$ and hence $\operatorname{tr}(ss_i) = 0$ (since it has only 0 as an eigenvalue). Finally, suppose ss_i belongs to some maximal subgroup of J. Then we can find by Green-Rees Theory [32, Appendix A] elements $x, x' \in J$ so that $xx'x = x, x'xx' = x'$, $x'xss_i = ss_i$ and $xss_ix' \in G$. Then

$$\operatorname{tr}(ss_i) = \operatorname{tr}(x'xss_i) = \operatorname{tr}(xss_ix') \in A$$

establishing the claim. As a consequence, $\operatorname{tr}(ss_i)$ takes on at most $m = |A|$ values for $s \in S$ and so S has at most m^d elements. Thus there is a word $w \in \Sigma^*$ of length at most $m^d - 1$ representing 0 in S. As $d \leq n^2$, this provides the desired result. □

We are now ready to prove the main theorem of this section.

Theorem 5.6. *The function f from* (5.1) *is a universal mortality function.*

Proof. Because f is superadditive, it suffices by Proposition 2.5 to show that if $\Sigma \subseteq M_n(\mathbb{Q})$ is such that $S = \langle \Sigma \rangle$ is a finite irreducible submonoid and $0 \in S$, then there exists a word $w \in \Sigma^*$ with $|w| \leq f(n)$ and $w = 0$ in S. If $S \setminus \{0\}$ contains only invertible elements, then $0 \in \Sigma$ and there is nothing to prove. So assume that S contains non-zero singular matrices (and hence $n > 1$).

Let J be the apex of $S \hookrightarrow M_n(\mathbb{Q})$ and let G be a maximal subgroup of J. Then since S is finite and G consists of singular matrices, it follows from Lemma 5.4 that $\{|\operatorname{tr}(g)| \mid g \in G\} \cup \{0\} \subseteq \{0, \ldots, n-1\}$ and hence has at most $2n - 1$ elements. Thus Lemma 5.5 yields the desired result. □

This leaves open an obvious question:

Question 5.7. Is there a polynomial universal mortality function? How about an exponential one?

Rystsov [35] conjectured that n^2 would be a universal mortality function, but he also conjectured this bound should hold over all finite fields, which is impossible given the undecidability of matrix mortality for integer matrices [26]. However, the best known lower bound to our knowledge is n^2 coming from the lower bound for the Černý problem.

Let us prove that for aperiodic monoids, we can find a better mortality function than (5.1). Recall that a monoid is *aperiodic* if all its maximal subgroups are trivial. The journal version of this paper deals with further classes of monoids.

Theorem 5.8. *The superadditive function $k(n) = 2^{n^2} - 1$ is a mortality function for all aperiodic monoids.*

Proof. Routine computation shows that k is superadditive. So it suffices by Proposition 2.5 to deal with irreducible representations $\rho\colon S \to M_n(\mathbb{Q})$. Without loss of generality we may assume that S is an irreducible aperiodic submonoid of $M_n(\mathbb{Q})$ and ρ is the inclusion. If $S \setminus \{0\}$ contains only invertible elements, then $0 \in \Sigma$ and there is nothing to prove. So assume that S contains non-zero singular matrices (and hence $n > 1$).

Let J be the apex of ρ and let G be a maximal subgroup of J; then $G = \{e\}$ where e is an idempotent. Set $V = \mathbb{Q}^n$. Then $\operatorname{tr} e = \dim Ve$. But the theory of Munn and Ponizovsky implies that the restriction of the action of G to Ve gives an irreducible representation of G [9,15,30,33]. Since G is the trivial group, this implies $\dim Ve = 1$ and so $\operatorname{tr} e = 1$. Thus $|\{\operatorname{tr} g \mid g \in G\} \cup \{0\}| = 2$ from which Lemma 5.5 yields the desired result. □

References

1. J. Almeida. *Finite semigroups and universal algebra*, volume 3 of *Series in Algebra*. World Scientific Publishing Co. Inc., River Edge, NJ, 1994. Translated from the 1992 Portuguese original and revised by the author.
2. J. Almeida, S. Margolis, B. Steinberg, and M. Volkov. Representation theory of finite semigroups, semigroup radicals and formal language theory. *Trans. Amer. Math. Soc.*, 361(3):1429–1461, 2009.
3. D. S. Ananichev and M. V. Volkov. Some results on Černý type problems for transformation semigroups. In *Semigroups and languages*, pages 23–42. World Sci. Publ., River Edge, NJ, 2004.
4. D. S. Ananichev and M. V. Volkov. Synchronizing generalized monotonic automata. *Theoret. Comput. Sci.*, 330(1):3–13, 2005.
5. D. S. Ananichev, M. V. Volkov, and Y. I. Zaks. Synchronizing automata with a letter of deficiency 2. *Theoret. Comput. Sci.*, 376(1-2):30–41, 2007.
6. F. Arnold and B. Steinberg. Synchronizing groups and automata. *Theoret. Comput. Sci.*, 359(1-3):101–110, 2006.
7. J. Berstel and C. Reutenauer. *Rational series and their languages*, volume 12 of *EATCS Monographs on Theoretical Computer Science*. Springer-Verlag, Berlin, 1988.
8. J. Černý. A remark on homogeneous experiments with finite automata. *Mat.-Fyz. Časopis Sloven. Akad. Vied*, 14:208–216, 1964.

9. A. H. Clifford and G. B. Preston. *The algebraic theory of semigroups. Vol. I.* Mathematical Surveys, No. 7. American Mathematical Society, Providence, R.I., 1961.
10. C. W. Curtis and I. Reiner. *Representation theory of finite groups and associative algebras.* Wiley Classics Library. John Wiley & Sons Inc., New York, 1988. Reprint of the 1962 original, A Wiley-Interscience Publication.
11. L. Dornhoff. *Group representation theory. Part A: Ordinary representation theory.* Marcel Dekker Inc., New York, 1971. Pure and Applied Mathematics, 7.
12. L. Dubuc. Sur les automates circulaires et la conjecture de Černý. *RAIRO Inform. Théor. Appl.*, 32(1-3):21–34, 1998.
13. S. Eilenberg. *Automata, languages, and machines. Vol. B.* Academic Press, New York, 1976. With two chapters ("Depth decomposition theorem" and "Complexity of semigroups and morphisms") by Bret Tilson, Pure and Applied Mathematics, Vol. 59.
14. A. Freedman, R. N. Gupta, and R. M. Guralnick. Shirshov's theorem and representations of semigroups. *Pacific J. Math.*, (Special Issue):159–176, 1997. Olga Taussky-Todd: in memoriam.
15. O. Ganyushkin, V. Mazorchuk, and B. Steinberg. On the irreducible representations of a finite semigroup. *Proc. Amer. Math. Soc.*, to appear.
16. R. L. Graham. On finite 0-simple semigroups and graph theory. *Math. Systems Theory*, 2:325–339, 1968.
17. G. Jacob. Un algorithme calculant le cardinal, fini ou infini, des demi-groupes de matrices. *Theoret. Comput. Sci.*, 5(2):183–204, 1977/78.
18. J. Kari. A counter example to a conjecture concerning synchronizing words in finite automata. *Bull. Eur. Assoc. Theor. Comput. Sci. EATCS*, (73):146, 2001.
19. J. Kari. Synchronizing finite automata on Eulerian digraphs. *Theoret. Comput. Sci.*, 295(1-3):223–232, 2003. Mathematical foundations of computer science (Mariánské Lázně, 2001).
20. A. A. Klyachko, I. C. Rystsov, and M. A. Spivak. On an extremal combinatorial problem connected with an estimate for the length of a reflexive word in an automaton. *Kibernetika (Kiev)*, (2):16–20, 25, 132, 1987.
21. K. Krohn, J. Rhodes, and B. Tilson. *Algebraic theory of machines, languages, and semigroups.* Edited by Michael A. Arbib. With a major contribution by Kenneth Krohn and John L. Rhodes. Academic Press, New York, 1968. Chapters 1, 5–9.
22. A. Mandel and I. Simon. On finite semigroups of matrices. *Theoret. Comput. Sci.*, 5(2):101–111, 1977/78.
23. S. W. Margolis and B. Steinberg. The quiver of an algebra associated to the Mantaci-Reutenauer descent algebra and the homology of regular semigroups. *Algebr. Represent. Theory*, to appear.
24. D. B. McAlister. Characters of finite semigroups. *J. Algebra*, 22:183–200, 1972.
25. R. McNaughton and Y. Zalcstein. The Burnside problem for semigroups. *J. Algebra*, 34:292–299, 1975.
26. M. S. Paterson. Unsolvability in 3×3 matrices. *Studies in Appl. Math.*, 49:105–107, 1970.
27. J.-E. Pin. Sur un cas particulier de la conjecture de Cerny. In *Automata, languages and programming (Fifth Internat. Colloq., Udine, 1978)*, volume 62 of *Lecture Notes in Comput. Sci.*, pages 345–352. Springer, Berlin, 1978.
28. J.-E. Pin. Le problème de la synchronisation et la conjecture de Černý. In *Noncommutative structures in algebra and geometric combinatorics (Naples, 1978)*, volume 109 of *Quad. "Ricerca Sci."*, pages 37–48. CNR, Rome, 1981.

29. J.-E. Pin. On two combinatorial problems arising from automata theory. In *Combinatorial mathematics (Marseille-Luminy, 1981)*, volume 75 of *North-Holland Math. Stud.*, pages 535–548. North-Holland, Amsterdam, 1983.
30. M. S. Putcha. Complex representations of finite monoids. II. Highest weight categories and quivers. *J. Algebra*, 205(1):53–76, 1998.
31. L. E. Renner. *Linear algebraic monoids*, volume 134 of *Encyclopaedia of Mathematical Sciences*. Springer-Verlag, Berlin, 2005. Invariant Theory and Algebraic Transformation Groups, V.
32. J. Rhodes and B. Steinberg. *The q-theory of finite semigroups*. Springer Monographs in Mathematics. Springer, New York, 2009.
33. J. Rhodes and Y. Zalcstein. Elementary representation and character theory of finite semigroups and its application. In *Monoids and semigroups with applications (Berkeley, CA, 1989)*, pages 334–367. World Sci. Publ., River Edge, NJ, 1991.
34. I. Rystsov. Reset words for commutative and solvable automata. *Theoret. Comput. Sci.*, 172(1-2):273–279, 1997.
35. I. C. Rystsov. On the rank of a finite automaton. *Kibernet. Sistem. Anal.*, (3):3–10, 187, 1992.
36. I. K. Rystsov. Quasioptimal bound for the length of reset words for regular automata. *Acta Cybernet.*, 12(2):145–152, 1995.
37. I. K. Rystsov. On the length of reset words for automata with simple idempotents. *Kibernet. Sistem. Anal.*, (3):32–39, 187, 2000.
38. M. P. Schützenberger. Sur le produit de concaténation non ambigu. *Semigroup Forum*, 13(1):47–75, 1976/77.
39. B. Steinberg. Černý's conjecture and group representation theory. Preprint, 2008.
40. B. Steinberg. Yet another solution to the burnside problem for matrix semigroups. *Canad. Math. Bull.*, to appear.
41. A. N. Trahtman. An efficient algorithm finds noticeable trends and examples concerning the Černy conjecture. In *Mathematical foundations of computer science 2006*, volume 4162 of *Lecture Notes in Comput. Sci.*, pages 789–800. Springer, Berlin, 2006.
42. A. N. Trahtman. The Černý conjecture for aperiodic automata. *Discrete Math. Theor. Comput. Sci.*, 9(2):3–10 (electronic), 2007.
43. M. V. Volkov. Synchronizing automata and the Černý conjecture. In C. Martín-Vide, F. Otto, and H. Fernau, editors, *Language and Automata Theory and Applications Second International Conference, LATA 2008, Tarragona, Spain, March 13-19, 2008.*, volume 5196 of *Lecture Notes in Computer Science*, pages 11–27, Berlin / Heidelberg, 2008. Springer.