Matrix approach to synchronizing automata

A.N. Trahtman*

22.10.2019

Abstract. A word \( w \) of letters on edges of underlying graph \( \Gamma \) of deterministic finite automaton (DFA) is called synchronizing if \( w \) sends all states of the automaton to a unique state.

J. Černý discovered in 1964 a sequence of \( n \)-state complete DFA possessing a minimal synchronizing word of length \( (n - 1)^2 \). The hypothesis, well known today as Černý conjecture, claims that \( (n - 1)^2 \) is a precise upper bound on the length of such a word over alphabet \( \Sigma \) of letters on edges of \( \Gamma \) for every complete \( n \)-state DFA. The hypothesis was formulated distinctly in 1966 by Starke.

A special classes of matrices induced by words in the alphabet of labels on edges of the underlying graph of DFA are used for the study of synchronizing automata.

Keywords deterministic finite automata, synchronizing word, Černý conjecture.

Introduction

The problem of synchronization of DFA is a natural one and various aspects of this problem have been touched in the literature. The connections with the early coding theory and first efforts to estimate the length of synchronizing word look in the works [28], [29]. Prehistory of the topic, the emergence of the term, different problems of synchronization one can find in surveys [21], [23], [35], [44].

Synchronization makes the behavior of an automaton resistant against input errors since, after detection of an error, a synchronizing word can reset the automaton back to its original state, as if no error had occurred. The synchronizing word limits the propagation of errors for a prefix code. Deterministic finite automaton is a tool that helps to recognise language in a set of DNA strings.

A problem with a long story is the estimation of the minimal length of synchronizing word.

J. Černý in 1964 [9] found the sequence of \( n \)-state complete DFA with shortest synchronizing word of length \( (n - 1)^2 \) for an alphabet of size two. The hypothesis, well known today as the Černý’s conjecture, claims that this lower bound on the length of the synchronizing word of aforementioned automaton is also the upper bound for the shortest synchronizing word of any \( n \)-state complete DFA:

* Email: avraham.trakhtman@gmail.com
Conjecture 1 The deterministic complete $n$-state synchronizing automaton over alphabet $\Sigma$ has synchronizing word in $\Sigma$ of length at most $(n - 1)^2$ (Starke, 1966).

The problem can be reduced to automata with a strongly connected graph [9].

This famous conjecture is true for a lot of automata, but in general the problem still remains open although several hundreds of articles consider this problem from different points of view [12]. Moreover, two conferences ”Workshop on Synchronizing Automata” (Turku, 2004) and ”Around the Černý conjecture” (Wroclaw, 2008) were dedicated to this longstanding conjecture. The problem is discussed on many sites on the Internet.

Together with the Road Coloring problem [31], [15], [32], this simple-looking conjecture was arguably the most longstanding and famous open combinatorial problems in the theory of finite automata [24], [33], [35], [36], [44].

The road coloring problem to find a labelling of the edges that turns the graph into a deterministic finite automaton possessing a synchronizing word was stated in 1970 [1] and solved in 2008 [40], [41].

Examples of automata such that the length of the shortest synchronizing word is greater than $(n - 1)^2$ are unknown for today. Moreover, the examples of automata with shortest synchronizing word of length $(n - 1)^2$ are infrequent. After the sequence of Černý and the example of Černý, Piricka and Rosenauerova [12] of 1971 for $|\Sigma| = 2$, the next such examples were found by Kari [22] in 2001 for $n = 6$ and $|\Sigma| = 2$ and by Roman [34] for $n = 5$ and $|\Sigma| = 3$ in 2004.

The package TESTAS [37], [43] studied all automata with strongly connected underlying graph of size $n \leq 11$ for $|\Sigma| = 2$, of size $n \leq 8$ for $|\Sigma| \leq 3$ and of size $n \leq 7$ for $|\Sigma| \leq 4$ and found five new examples of DFA with shortest synchronizing word of length $(n - 1)^2$ for $n \leq 4$.

Don and Zantema present in [13] an ingenious method of designing several new automata from existing examples of size three and four and proved that for $n \geq 5$ the method does not work. So there are up to isomorphism exactly 15 DFA for $n = 3$ and 12 DFA for $n = 4$ with shortest synchronizing word of length $(n - 1)^2$. The authors of [13] support the hypothesis from [37] that all automata with shortest synchronizing word of length $(n - 1)^2$ are known, of course, with essential correction found by themselves for $n = 3, 4$.

There are several reasons [2], [5], [8], [13], [37] to believe that the length of the shortest synchronizing word for remaining automata with $n > 4$ (except the sequence of Černý and two examples for $n = 5, 6$) is essentially less and the gap grows with $n$. For several classes of automata, one can find some estimations on the length in [2], [13], [11], [24], [25], [38].

Initially found upper bound for the minimal length of synchronizing word was big and has been consistently improved over the years by different authors. The upper bound found by Frankl in 1982 [14] is equal to $(n^3 - n)/6$. The result was reformulated in terms of synchronization in [33] and repeated independently in [26].
The mentioned results for \((n^3 - n)/6\) successfully use the matrix approach and the dimension of the arising spaces. See also, for instance, \[5\], \[3\], \[6\], \[24\], \[20\], \[17\], \[16\] for this approach.

Nevertheless, the cubic estimation of the bound exists since 1982.

The considered deterministic automaton \(A\) can be presented by a complete underlying graph with edges labelled by letters of an alphabet.

We consider a special class of matrices \(M_u\) of mapping induced by words \(u\) in the alphabet of letters on edges of the underlying graph. \(M_u\) has one unit in every row and rest zeros. The matrix of synchronizing word has units only in one column.

Our proof used some lemmas from \[39\]. For a complete picture of the proof, these lemmas after some modification are included in the proposed work.

Help Lemmas \[2\] and \[1\] state that the size of the set \(R(u)\) of nonzero columns of the matrix \(M_u\) is equal to the rank of \(M_u\), \(R(bu) \subseteq R(u)\) and \(|R(ub)| \leq |R(u)|\) for every word \(b\).

Lemma \[3\] estimates the dimension of the space generated by matrices of words: The set of all \(n \times k\)-matrices of words for \(k < n\) has at most \(\frac{n(k - 1) + 1}{2}\) linear independent matrices.

In particular, the set of \(n \times (n-1)\)-matrices of words has at most \((n-2)^2\) linear independent matrices. The famous value from the Černý hypothesis appears here.

Lemma \[4\] studied the nontrivial linear combination of matrices of words:

\[
M_u = \sum_{i=1}^{k} \lambda_i M_{u_i} \rightarrow \sum_{i=1}^{k} \lambda_i = 1. \quad \sum_{i=1}^{k} \lambda_i M_{u_i} = 0 \rightarrow \sum_{i=1}^{k} \lambda_i = 0. \quad (1)
\]

Lemma \[5\] notes distributivity by multiplication matrix from left on linear combination of matrices of word.

We study the rational series \((S, u)\) for matrix \(M_u\) (see \[7\]), \[4\]. This approach for synchronizing automata supposed first by Béal \[4\] proved to be fruitful \[5\], \[8\], \[10\].

Lemma \[6\] and its Corollary \[6\] establish some algebraic properties of rational series of matrices of words, for instance:

the matrices \(M_u\) with constant \((S, u) = i\) generate a space \(V\) with \((S, t) = i\) for every nonzero matrix \(M_t \in V\).

We consider the equations \(M_u L_x = M_s \quad (4)\) for synchronizing word \(s = ux\) and solutions \(L_x\) (Definition \[2\]) in Lemma \[7\].

A connection between the set of nonzero columns of matrix of word, subsets of states of automaton and of solutions \(L_x\) of \((4)\) is revealed in Remarks \[2\], \[5\].

Lemmas \[8\], \[9\] consider pseudoinverse matrices \[9\] and their connection with equation \((4)\).

The ideas of the approach are illustrated on examples of automata with a maximal length of synchronizing word from \[22\], \[9\], \[34\]. A sequence of words \(u\) of growing length together with corresponding \(n\)-vector of subset of states obtained by mapping of \(u\) presents column \(q\) of solutions from \((4)\). Some connection between the sequence of linear independent solutions (\(n\)-vector of subset of states) and subwords of the minimal synchronizing word is easy to detect.
Preliminaries

We consider a complete $n$-state DFA with strongly connected underlying graph $\Gamma$ and transition semigroup $S$ over a fixed finite alphabet $\Sigma$ of labels on edges of $\Gamma$ of an automaton $A$. The trivial cases $n \leq 2$, $|\Sigma| = 1$ and $|A\sigma| = 1$ for $\sigma \in \Sigma$ are excluded.

The restriction on strongly connected graphs is based on [9]. The states of the automaton $A$ are considered also as vertices of the graph $\Gamma$.

If there exists a path in an automaton from the state $p$ to the state $q$ and the edges of the path are consecutively labelled by $\sigma_1, \ldots, \sigma_k$, then for $s = \sigma_1 \ldots \sigma_k \in \Sigma^+$ let us write $q = ps$.

Let $P \times$ be the set of states $q = px$ for all $p$ from the subset $P$ of states and $x \in \Sigma^+$. Let $Ax$ denote the set $P \times$ for the set $P$ of all states of the automaton.

A word $s \in \Sigma^+$ is called a synchronizing (reset, magic, recurrent, homing, directable) word of an automaton $A$ with underlying graph $\Gamma$ if $|As| = 1$. The word $s$ below denotes minimal synchronizing word such that for a state $q As = q$.

The states of the automaton are enumerated with number one for the fixed state $q$.

An automaton (and its underlying graph) possessing a synchronizing word is called synchronizing.

Let us consider a linear space generated by $n \times n$-matrices $M$ with one unit in any row of the matrix and zeros everywhere else.

We connect a mapping of the set of states of the automaton made by a word $u$ of $n \times n$-matrix $M_u$ such that for an element $m_{i,j} \in M_u$ takes place $m_{i,j} = 1$ if the word $u$ maps $q_i$ on $q_j$ and 0 otherwise.

Any mapping of the set of states of the automaton $A$ can be presented by some word $u$ and by a corresponding matrix $M_u$. For instance,

$$M_u = \begin{pmatrix} 0 & 0 & 1 & \ldots & 0 \\ 1 & 0 & 0 & \ldots & 0 \\ 0 & 0 & 0 & \ldots & 1 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 1 & 0 & \ldots & 0 \\ 1 & 0 & 0 & \ldots & 0 \end{pmatrix}$$

Let us call the matrix $M_u$ of the mapping induced by the word $u$, for brevity, the matrix of word $u$, and vice versa, $u$ is the word of matrix $M_u$.

Every square matrix with one unit in every row and zeros in remaining cells will be also considered as a matrix of word.

$M_u M_v = M_{uv}$ [4].

The set of nonzero columns of $M_u$ (set of second indexes of its elements) of $M_u$ is denoted as $R(u)$.

The word $u$ of the matrix $M_u$ is called irreducible if for every word $v$ obtained by removing some subword of $u$ $M_u \neq M_v$.

The minimal synchronizing word and all its subwords are irreducible.

The right word $x$ of synchronizing word $ux$ let us call right synchronizing continuation of $u$.

Zero matrix is a matrix of empty word.
The subset of states $A_u$ of the set of all states of $A$ is denoted $c_u$ with number of states $|c_u|$. In $n$-vector $c_u$ the coordinate $j$ has unit if the state $j \in c_u$ and zero in opposite case.

For linear algebra terminology and definitions, see [27], [30].

1 Mappings induced by a word and subword

**Remark 1** For every cell of $n \times n$-matrix of words in strongly connected automaton there is a matrix with unit in the cell.

Every unit in the product $M_u M_a$ is the product of two units, first unit from a row of $M_u$ and second unit from nonzero column of $M_a$.

The unit in the cell $(i, j)$ of the matrix of letter denotes the edge from the state $i$ to the state $j$, for matrix of word, such unit denotes the path from $i$ to $j$.

The set $R(u)$ of nonzero columns of matrix $M_u$ corresponds the set of states $c_u$ of the automaton.

**Lemma 1** For the set of states of deterministic finite automaton and any words $u$ and $w$, $A_u \subseteq A_w$.

For every word $w$, $R(u) \subseteq R(v)$ implies $R(uw) \subseteq R(vw)$.

For the state $p \not\in A_w$ takes place $p \not\in A_{uw}$. Nonzero columns of $M_{uw}$ have units also in $M_w$.

The number of nonzero columns $|R(b)|$ is equal to the rank of $M_b$.

**Proof.** The properties of $A_u \subseteq A$, $M_w$ and $M_{uw}$ follow from the definition of the matrix of word.

The set of nonzero columns of matrix defines a set of states. The mapping by word $w$ of a set of states [columns $R(v)$] induces a mapping of its subset [columns $R(u)$].

For any word $u$ and the zero column of $M_w$ the corresponding column of $M_{uw}$ also consist of zeros. Hence nonzero columns of $M_{uw}$ have units also in $M_w$.

The matrix $M_b$ has submatrix with only one unit in every row and every nonzero column with nonzero determinant. Therefore $|R(b)|$ is equal to the rank of $M_b$.

**Corollary 1** The matrix $M_s$ of word $s$ is synchronizing if and only if $M_s$ has zeros in all columns except one and units in the residuary column.

All matrices of right subwords of $s$ also have at least one unit in this column.

**Remark 2** The rows of the matrix $M_u M_a$ are obtained by permutation of rows of the matrix $M_a$. Some of these rows may disappear and replaced by another rows of $M_u$.

The invertible matrix $M_a$ does not change the number of units of every column of $M_u$ in its image of the product $M_a M_u$.

The columns of the matrix $M_u M_a$ are obtained by permutation of columns $M_u$. Some columns can be merged with $|R(ua)| < |R(u)|$. 
Lemma 2 For every words $a$ and $u$

$$|R(ua)| \leq |R(u)|$$ and

$$R(au) \subseteq R(u).$$

The matrix $M_a$ with $m$ units in column $r$ replicates row $r$ of $M_u$ $m$ times in $M_a M_u$.

For invertible matrix $M_a$ $R(au) = R(u)$ and $|R(ua)| = |R(u)|$.

Proof. The matrix $M_a$ in the product $M_a M_u$ shifts column of $M_u$ to columns of $M_a M_u$ without changing the column itself (Remark 2).

$M_a$ also can merge columns of $M_a$. In view of possible merged columns, $|R(ua)| \leq |R(u)|$.

The zero columns $j$ of $M_a$ changes the row $j$ of $M_u$ in the product $M_a M_u$.

Let $M_a$ have $m$ units in column $r$. These units and unit in row $r$ of $M_u$ create $m$ units in the product $M_a M_u$ in different rows of common column. Therefore the matrix $M_a$ replicates the row $r$ of $M_u$ $m$ times in $M_a M_u$.

So some rows of $M_u$ can be replaced in $M_a M_u$ by row $r$ and therefore some rows from $M_u$ may disappear (Remark 2).

Hence $R(au) \subseteq R(u)$ (See also Lemma 1).

For invertible matrix $M_a$ in view of existence $M_a^{-1}$ we have $|R(ua)| = |R(u)|$ and $R(au) = R(u)$.

2 The set of linear independent matrices of words

Remark 3 The space generated by matrices of words has zero matrix of empty word.

Lemma 3 The set $V$ of all $n \times k$-matrices of words (or $n \times n$-matrices with zeros in fixed $n - k$ columns for $k < n$) has $n(k - 1) + 1$ linear independent matrices.

Proof. Let us consider distinct $n \times k$-matrices of word with at most one nonzero cell outside the last nonzero column $k$.

Let us begin from the matrices $V_{i,j}$ with unit in $(i, j)$ cell ($j < k$) and units in $(m, k)$ cells for all $m$ except $i$. The remaining cells contain zeros. So we have $n - 1$ units in the $k$-th column and only one unit in remaining $k - 1$ columns of the matrix $V_{i,j}$. Let the matrix $K$ have units in the $k$-th column and zeros in the other columns. There are $n(k - 1)$ matrices $V_{i,j}$. Together with $K$ they belong to the set $V$. So we have $n(k - 1) + 1$ matrices. For instance,

$$V_{1,1} = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ 0 & 0 & 0 & \ldots & 1 \\ 0 & 0 & 0 & \ldots & 1 \\ \ldots \\ 0 & 0 & 0 & \ldots & 1 \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix}, \quad V_{3,2} = \begin{pmatrix} 0 & 0 & 0 & \ldots & 1 \\ 0 & 0 & 0 & \ldots & 1 \\ 0 & 1 & 0 & \ldots & 0 \\ \ldots \\ 0 & 0 & 0 & \ldots & 1 \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix}, \quad K = \begin{pmatrix} 0 & 0 & 0 & \ldots & 1 \\ 0 & 0 & 0 & \ldots & 1 \\ 0 & 0 & 0 & \ldots & 1 \\ \ldots \\ 0 & 0 & 0 & \ldots & 1 \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix}$$

The first step is to prove that the matrices $V_{i,j}$ and $K$ generate the space with the set $V$. For arbitrary matrix $T$ of word from $V$ for every $t_{i,j} \neq 0$ and
\( j < k \), let us consider the matrices \( V_{i,j} \) with unit in the cell \((i,j)\) and the sum of them \( \sum V_{i,j} = Z \).

The first \( k - 1 \) columns of \( T \) and \( Z \) coincide. Hence in the first \( k - 1 \) columns of the matrix \( Z \) there is at most only one unit in any row. Therefore in the cell of \( k \)-th column of \( Z \) one can find at most two values which differ by unit, say \( m \) or \( m - 1 \). The value of \( m \) appears if there are only zeros in other cells of the considered row. Therefore \( \sum V_{i,j} - (m - 1)K = T \).

Thus, every matrix \( T \) from the set \( V \) is a span of above-mentioned \((k-1)n+1\) matrices from \( V \). It remains now to prove that the set of matrices \( V_{i,j} \) and \( K \) is a set of linear independent matrices.

If one excludes a certain matrix \( V_{i,j} \) from the set of these matrices, then it is impossible to obtain a nonzero value in the cell \((i,j)\) and therefore to obtain the matrix \( V_{i,j} \). So the set of matrices \( V_{i,j} \) is linear independent. Every non-trivial linear combination of the matrices \( V_{i,j} \) equal to a matrix of word has at least one nonzero element in the first \( k - 1 \) columns. Therefore, the matrix \( K \) could not be obtained as a linear combination of the matrices \( V_{i,j} \). Consequently the set of matrices \( V_{i,j} \) and \( K \) forms a basis of the set \( V \).

**Corollary 2** The set of all \( n \times (n-1) \)-matrices of words (or \( n \times n \)-matrices with zeros in a fixed column) has \((n-1)^2\) linear independent matrices.

Proof. For \( k = n - 1 \) it follows from \( n(n - 1 - 1) + 1 = (n - 1)^2 \).

**Corollary 3** Suppose the vertex \( p \not\in A\alpha \) and let words \( u \) of matrices \( M_u \) have the last letter \( \alpha \).

Then there are at most \((n-1)^2\) linear independent matrices \( M_u \).

Proof. All matrices \( M_u \) have common zero column \( p \) by Lemma 1. So we have \( n \times n \)-matrices with zeros in a fixed column and due to Corollary 2 there are at most \((n-1)^2\) linear independent matrices \( M_u \).

**Corollary 4** There are at most \( n(n-1) + 1 \) linear independent matrices of words in the set of \( n \times n \)-matrices.

**Corollary 5** There are at most \( n + 1 \) linear independent matrices of words in the set of matrices with 2 nonzero columns.

**Lemma 4** Suppose that for nonzero matrices \( M_u \) of word \( u \) and \( M_{u_i} \) of words \( u_i \)

\[
M_u = \sum_{i=1}^{k} \lambda_i M_{u_i}. \tag{2}
\]

Then the sum \( \sum_{i=1}^{k} \lambda_i = 1 \) and the sum \( S_j \) of values in every row \( j \) of the sum in (2) also is equal to one.

If \( \sum_{i=1}^{k} \lambda_i M_{u_i} = 0 \) then \( \sum_{i=1}^{k} \lambda_i = 0 \) and \( S_j = 0 \) for every \( j \) with \( M_u = 0 \).

If the sum \( \sum_{i=1}^{k} \lambda_i \) in every row is not unit [zero] then \( \sum_{i=1}^{k} \lambda_i M_{u_i} \) is not a matrix of word.
Proof. The nonzero matrices $M_u$ and $M_{ui}$ have $n$ cells with unit in the cell. Therefore, the sum of values in all cells of the matrix $\lambda_i M_{ui}$ is $n \lambda_i$.

For nonzero $M_u$ the sum is $n$. So one has in view of $M_u = \sum_{i=1}^{k} \lambda_i M_{ui}$,

$$n = n \sum_{i=1}^{k} \lambda_i,$$

whence $1 = \sum_{i=1}^{k} \lambda_i = 0$ for every row $j$.

If the matrix $M = \sum_{i=1}^{k} \lambda_i M_{ui}$ is a matrix of word or zero matrix then $\sum_{i=1}^{k} \lambda_i \notin \{0, 1\}$ or the sum is not the same in every row then we have opposite case.

Lemma 5 Distributivity from left.

For every words $b$ and $x_i$,

$$M_b \sum_{i=1}^{k} \tau_i M_{xi} = \sum_{i=1}^{k} \tau_i M_b M_{xi}. $$

Proof. The matrix $M_b$ shifts rows of every $M_{xi}$ and of the sum of them in the same way according to Remark 2. $M_b$ removes common row of them and replace also by common row (Remark 2).

Therefore the matrices $M_b M_{xi}$ has the origin rows of $M_{xi}$, maybe in another order, and the rows of the sum $\sum_{i=1}^{k} \tau_i M_b M_{xi}$ repeat rows of $\sum_{i=1}^{k} \tau_i M_{xi}$ also in the same order.

Note that this is not always true on the right.

3 Rational series

The section follows ideas and definitions from [7] and [4]. We recall that a formal power series with coefficients in a field $K$ and variables in $\Sigma$ is a mapping of the free monoid $\Sigma^*$ into $K$ [7], [8].

We consider an $n$-state automaton $A$. Let $P$ denote the subset of states of the automaton with the characteristic column vector $P^t$ of $P$ of length $n$ having units in coordinates corresponding to the states of $P$ and zeros everywhere else. Let $C$ be a row of units of length $n$. Following [4], we denote by $S$ the rational series depending on the set $P$ defined by:

$$(S, u) = C M_u P^t - C P^t = C (M_u - E) P^t. \quad (3)$$

Remark 4 Let $S$ be a rational series depending on the set $P$.

If the cell $i$ in $P^t$ has zero then $(S, u)$ does not depend on column $i$ of $M_u$. If this cell $i$ has unit then the column $i$ of $M_u$ with $k$ units from $S$ added to $(S, u)$ the value of $k - 1$.

For $k$ units in the column $q$ of $n \times n$-matrix $M_u$ and $P = \{q\}$ $(S, u) = k - 1$.

For $P$ nonzero columns of $n \times n$-matrix $M_u$ $(S, u) = n - |P|$. 

Lemma 6 Let $S$ be a rational series depending on the set $P$ of an automaton $A$. Let $M_u = \sum_{j=1}^{k} \lambda_j M_{u_j}$. Then $(S, u) = \sum_{j=1}^{k} \lambda_j (S, u_j)$.

If $(S, u_j) = i$ for every $j$ then also $(S, u) = i$.

Proof. One has in view of (3)
$$(S, u) = C(\sum_{j=1}^{k} \lambda_j M_{u_j} - E)P^t$$
where $C$ is a row of units and $P^t$ is a characteristic column of units and zeros.

Due to Lemma 4
$$\sum_{j=1}^{k} \lambda_j M_{u_j} - E = \sum_{j=1}^{k} \lambda_j M_{u_j} - \sum_{j=1}^{k} \lambda_j E = \sum_{j=1}^{k} \lambda_j (M_{u_j} - E).$$

So
$$(S, u) = C(M_{u_j} - E)P^t = C(\sum_{j=1}^{k} \lambda_j M_{u_j} - E)P^t = C(\sum_{j=1}^{k} \lambda_j (M_{u_j} - E))P^t = \sum_{j=1}^{k} \lambda_j C(M_{u_j} - E)P^t = \sum_{j=1}^{k} \lambda_j (S, u_j).$$

Thus, $(S, u) = \sum_{j=1}^{k} \lambda_j (S, u_j)$.

If $\forall j (S, u_j) = i$, then $(S, u) = \sum_{j=1}^{k} \lambda_j i = i \sum_{j=1}^{k} \lambda_j = i$ by Lemma 4.

From Lemma 6 follows

Corollary 6 Let $S$ be a rational series depending on the set $P$ of an automaton $A$.

The matrices $M_u$ with constant $(S, u) = i$ generate a space $V$ such that for every nonzero matrix $M_t \in V$ of word $t, (S, t) = i$.

Corollary 7 Let $S$ be a rational series depending on the set $P$ of size one of $n$-state automaton.

Then the set $V$ of matrices $M_u$ with two fixed nonzero columns and fixed nonnegative $(S, u) < n - 1$ has at most $n$ linear independent matrices.

Proof. By lemma 3 for $k = 2$ there are at most $n + 1$ linear independent matrices. There is a matrix $M_w$ in a space for $k = 2$ with one nonzero column and $(S, w) \neq (S, u)$. Therefore fixed $(S, u) < n - 1$ excludes the matrix $M_w$ from space generated by $V$.

4 Matrix $L_x$ of word $x$ with common column $q$ of $M_x$.

Let $S_q$ below be a rational series depending on the set $P = \{q\}$ of size one with number one for the column $q$.

By Remark 4 the matrix $M_x$ has $(S_q, x) + 1$ units in the column $q$.

Definition 1 If the set of cells with units in the column $q$ of the matrix $M_u$ is a subset of the analogous set of the matrix $M_u$ then we write
$$(S_q, x) + 1$$

Definition 2 The matrix $L_x$ has column $q$ of $M_x$. For $(S_q, x) = n - i$ with $0 < i \leq n$, $L_x$ has $n - i + 1$ units in the column one of the state $q$ and remaining $i - 1$ units in next nearest columns, as usual one unit in the column.
The set of matrices \( L_x \) with nonzero column \( q \) is a subset of the set of matrices of word, having in every row one unit and the rest of zeros.

Many results concerning matrices \( M_x \) are valid for \( L_x \) because they use only matrix properties and existence of one unit in a row. For instance, Lemma 4, Corollary 5 of Lemma 3, Corollary 6 of Lemma 6 directly related to the set of matrices \( L_x \).

### 4.1 The equation with unknown \( L_x \)

The solution \( L_x \) of the equation

\[
M_u L_x = M_s
\]

for synchronizing matrix \( M_s \) and arbitrary \( M_u \) must have units in the column of the state \( q \).

In general, there are several solutions \( L_x \) of synchronizing continuations \( x \) of the word \( u \).

**Lemma 7** Every equation \( M_u L_x = M_s \) has a solutions \( L_x \) with \( (S_q, x) \geq 0 \).

\(|R(u)| - 1 = (S_q, x)\) for \( L_x \) with minimal \( (S_q, x) \) (a minimal solution), every matrix \( L_y \) satisfies the equation (4) iff \( L_x \subseteq L_y \).

Distinct solutions \( L_x \) are different in rows corresponding zero columns of \( M_u \).

The rank \( |R(x)| \leq n - (S_q, x) \).

There exists one-to-one correspondence between nonzero columns of \( M_u \), units in the column \( q \) of minimal solution \( L_x \) and the set of states \( c_u = A_x \) of automaton \( A \).

**Proof.** The matrix \( M_s \) of rank one has column of units of the state \( q \). For every nonzero column \( j \) of \( M_u \) with elements \( u_{ij} = 1 \) and \( s_{i,q} = 1 \) in the matrix \( M_s \) let the cell \((j, q)\) have unit in the matrix \( L_x \). So the unit in the column \( q \) of matrix \( M_s \) is a product of every unit from the column \( j \) of \( M_u \) and unit in the cell \( j \) of column \( q \) of \( L_x \).

Therefore by Remark 4 for rational series \( S_q \) the minimal solution \( L_x \) has in the column \( q \) \( (S_q, x) + 1 \) units, whence \( (S_q, x) = |R(u)| - 1 \).

The set \( R(u) \) of nonzero columns of \( M_u \) corresponds the set of cells of the column \( q \) with unit of minimal \( L_x \).

So to the column \( q \) of every solution belong at least \( (S_q, x) + 1 \) units. The units outside column \( q \) of the solution \( L_x \) belong to the next columns, one unit in a row. Units in rows corresponding zero columns of \( M_u \) do not imply on result in (4) (Remark 4) and therefore can be placed arbitrarily. The remaining cells obtain zero.
Lastly every solution $L_x$ of (4) has one unit with rest of zeros in every row and is a matrix of word.

Zeros in the cells of column $q$ of minimal $L_x$ correspond zero columns of $M_a$. Therefore for the matrix $L_y$ such that $L_x \subseteq_q L_y$ we have $M_aL_y = M_x$.

Every solution $L_y$ must have units in cells of column $q$ that correspond $|R(u)| = (S_q, x) + 1$ nonzero columns of $M_a$. Therefore $R(x)$ in (3) has at most $n - (S_q, x) - 1$ nonzero columns besides $q$, whence the rank $|R(x)| \leq n - (S_q, x)$.

Thus, the equality $M_aL_x = M_aL_y = M_s$ is equivalent to $L_x \subseteq_q L_y$ for the minimal $L_x$.

The matrix $M_a$ with set $R(u)$ of nonzero columns maps the automaton on the set $c_u$ of states and on the set of units in the column $q$ of minimal $L_x$.

**Corollary 8** For minimal solution $L_x$ of the equation $M_aL_x = M_s$ and minimal solution $L_y$ of the equation $M_aL_y = M_s$ one has $(S_q, y) \leq (S_q, x)$ in view of $|R(ut)| \leq |R(u)|$ (Lemma 7).

Lemma 7 explains the following

**Remark 5** Every permutation and shift of nonzero columns $M_a$ induces corresponding permutation of the set of units in the column $q$ of minimal solution $L_x$ of (4), and vice versa.

## 5 Right pseudoinverse matrices

**Definition 3** Let us call the matrix $M_{a^-}$ of word right pseudoinverse matrix of the matrix $M_a$ of a word $a$ if for precisely one element $a_{i,j} = 1$ of every nonzero column $j$ of $M_a$ the cell $(j, i)$ of $M_{a^-}$ has unit.

If in $M_{a^-}$ still are zero rows then unit is added arbitrary in every such row of the matrix $M_{a^-}$ of word.

Let $E_a$ denote $M_aM_{a^-}$.

For instance,

$$M_a = \begin{pmatrix}
0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0
\end{pmatrix},
M_{a^-} = \begin{pmatrix}
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{pmatrix},
M_{a^-} = \begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1
\end{pmatrix}$$

**Remark 6** For invertible matrix $M_a$ with $|R(a)| = n$ we have $M_{a^-} = M_a^{-1}$, for singular $M_a$ there are some generalized inverse matrices, including invertible.

Pseudoinverse matrices can be considered as matrices of word in the alphabet $\Gamma^-$. 

**Lemma 8** The product $M_bM_{b^-} = E_b$ does not depend on any arbitrary placing of units in $M_{b^-}$ in empty rows. The rank of $E_b$ is restricted by $|R(b)|$.

In the case $|R(u)| = |R(ub)|$ the product $M_aE_b$ returns all images of nonzero columns of $M_u$ to its origin place in $M_u$. $M_uL_x = M_s \rightarrow M_aM_bM_{b^-}L_x = M_s$. 

Proof. For nonzero column \(i\) of \(M_b\) there exists a unit in corresponding row \(i\) of \(M_b^\circ\).

The rows with free placing of units in \(M_b^-\) correspond zero columns of \(M_b\) and therefore could imply on the product \(M_b M_{b^-} = E_b\). Besides, all \(n\) units of columns \(M_b\) are moved to \(E_b\), whence units of the arbitrary placing could not imply on \(E_b = M_b M_{b^-}\).

By Lemma 2 the rank of \(M_b M_{b^-}\) is not greater than the rank \(|R(b)|\) of \(M_b\). Consequently rank of \(E_b\) is restricted by \(|R(b)|\).

In the case \(|R(u)| = |R(u\beta)|\) the matrix \(M_u\) does not merge columns of \(M_u\) and therefore the product \(M_u E_b\) returns all columns of \(M_u E_b\) to its origin place in \(M_u\), whence \(M_u L_x = M_s\) for every \(M_u M_{b^-} L_x = M_s\).

Lemma 9 For every equation \(M_u L_x = M_s\) and every letter \(\beta\)

\[
M_{u\beta} L_y = M_s
\]  
(5)

for minimal solutions \(L_y\) and \(L_x\) with \((S_q, y) \leq (S_q, x)\).

For \(|R(u)| \neq |R(u\beta)|\) and every letter \(\beta\) there exists solution \(L_y\) of the equation \(M_u M_{\beta^-} L_y = M_{\beta^-} L_y = M_s\) such that \((S_q, y) < (S_q, x)\) for minimal solutions.

For some \(L_y\), there exists a matrix \(M_{\beta^-}\) such that \(L_y = M_{\beta^-} L_x\).

\(|R(u)| = |R(u\beta)|\) implies \((S_q, y) = (S_q, x)\) for minimal solutions \(L_y\) and \(L_x\). The invertible matrix \(M_{\beta^-}\) does not change number of units of \(L_x\) in every column of \(L_y = M_{\beta^-} L_x\). \(M_u L_x = M_s\) for minimal solutions by Lemma 7.

In the case \((S_q, y) < (S_q, x)\) for minimal solutions \(L_x\) and \(L_y\) the column \(i\) of the matrix \(M_{\beta^-}\) merges some columns \(k_1, \ldots, k_m\) of \(M_u\). Then let us paste in pseudoinvers matrix \(M_{\beta^-}\) for every \(i\) unit in the cell \(k_1, i\) and units in the cells \((k_r, j)\) \(r > 1\) for distinct zero columns \(j\) of \(M_u\). Therefore the matrix \(E_{\beta^-}\) returns a part of nonzero columns from \(R(u)\) to the origin place in the matrix \(M_u M_{\beta^-}\). This part has all nonzero columns of \(M_u M_{\beta^-}\), whence \(M_u L_x = M_s\) for minimal solutions by Lemma 7.

Let \(|R(u)| = |R(u\beta)|\).

According to Definition 3 the units in the matrix \(M_{\beta^-}\) in some rows can be disposed arbitrarily. But they could not imply on the product \(M_{\beta^-} M_{\beta^-} = E_{\beta^-}\) by Lemma 2. \(E_{\beta^-}\) returns nonzero columns from \(R(u)\) to the origin place also due to Lemma 8. Hence the equality in

\[
M_u M_{\beta^-} M_{\beta^-} L_x = M_u M_{\beta^-} L_x = M_u L_y = M_s
\]

is correct in such case for every matrix \(M_{\beta^-}\) and solution \(L_y = M_{\beta^-} L_x\).

Moreover, the invertible matrix \(M_{\beta^-} = M_{\beta^-}\) keeps the number of units of every column of \(L_x\) in \(L_y = M_{\beta^-} L_x\) by Remark 2. Whence also for column \(q\) one has \((S_q, y) = (S_q, x)\) for minimal solutions \(L_y\) and \(L_x\).
Corollary 9 A set of linear independent solutions \( L_y = M_a - L_x \) of (4) and \( L_x \) with constant \((S_q, y) = (S_q, x)\) (and therefore \( R(y) = R(x) \)) can be created by help of invertible matrices \( M_a \) by words \( a \) of restricted length (Lemma 4, Remark 6).

So such invertible matrices \( M_a \) can create even a maximal subset of linear independent matrices \( L_y \) with fixed \((S_q, y) = (S_q, x)\) and greater in a space.

6 Examples

The coordinate \( j \) in \( n \)-vector of subset of states \( c_u \) has unit if the state \( j \in c_u \) and zero in opposite case. For instance, \((011011)\) means that the subset has states \( \{2, 3, 5, 6\} \).

Units in \( c_u \) correspond nonzero columns from \( R(u) \) of matrix \( M_u \). The vector \( c_u \) is equal to column \( q \) of solution \( L_x \) of equation \( M_u L_x = M_s \).

The matrices \( L_x \) corresponding word \( u \) of \( M_u \) (or \( L_v \) where \( L_x \subseteq q L_v \)) of fixed \((S_q, x)\) in lines of examples below are linear independent.

J. Kari [22] discovered the following example of \( n \)-state automaton with minimal synchronizing word of length \((n - 1)^2 \) for \( n = 6 \).

![Diagram of an automaton](image)

The minimal synchronizing word

\[ s = ba^2bababa^2b^2aba^2baba^2b \]

has the length at the Černy border.

Every line below presents a pair (word \( u \), \( n \)-vector \( c_u \)) of the word \( u \).

\((b, 111110) \ | R(u) | = 5 \)

\((ba, 111011) \)

\((ba^2, 111101) \)

\((ba^2b, 111100) \ | R(u) | = 4 \)

\((ba^2ba, 111010) \)

\((ba^2bab, 011110) \)

\((ba^2baba, 101111) \ | R(v) | = 5 \ (101111 of \( c_u \subset c_v \) \)

\((ba^2babab, 101110) \ | R(u) | = 4 \)

\((ba^2bababa, 110101) \)

\((ba^2bababa^2, 011101) \)

\((ba^2bababa^2b, 111000) \ | R(u) | = 3 \)

\((ba^2bababa^2b^2, 011100) \)

\((ba^2bababa^2b^2a, 110111) \ | R(v) | = 5 \ (101110 of \( c_u \subset c_v \) \)

\((ba^2bababa^2b^2ab, 001110) \ | R(u) | = 3 \)

\((ba^2bababa^2b^2aba, 100011) \)

\((ba^2bababa^2b^2aba^2, 011111) \ | R(v) | = 5 \ (010101 of \( c_u \subset c_v \) \)
By the bye, the matrices of right subwords of \( s \) are simply linear independent. It is possible that this property is by no means rare for minimal synchronizing word.

For the Černy sequence of \( n \)-state automata [9], [28], [29] the situation is more pure.

The minimal synchronizing word

\[ s = b(a^{n-1}b)^{n-2} \]

of the automaton also has the length at the Černy border.

For \( n = 4 \)

and synchronizing word \( baabaabab \) with pairs of word \( u \) and \( n \)-vector \( c_u \) of linear independent matrices \( L_u \) below.

\[
\begin{align*}
(b, 0111) & \mid |R(u)| = 3 \\
(ba, 1011) \\
(baa, 1101) \\
(baa, 1110) & \mid |R(u)| = 2 \\
(baaba, 0011) \\
(baaaba, 1001) \\
(baaaba, 1100) & \mid |u| = 8 \\
(baaabaab = s, 0100) & \mid |R(s)| = 1
\end{align*}
\]

In the example of Roman [34]
the minimal synchronizing word

\[ s = ab(ca)^2c bca^2c abca \]

The line below presents a pair \((\text{word } u, \text{n-vector } c_u)\) of the word \(u\).

\[(a, 10111) |R(u)| = 4\]
\[(ab, 11011)\]
\[(abc, 11110)\]
\[(abca, 10111) |R(u)| = 3\]
\[(abca, 10101) |R(u)| = 3\]
\[(abca, 11001)\]
\[(abca, 01110)\]
\[(abca, 10010) |R(u)| = 2\]
\[(abca, 00110)\]
\[(abca, 10001)\]
\[(abca, 11001) |R(u)| = 2\]
\[(abca, 00101)\]

Acknowledgments

I would like to express my gratitude to Francois Gonze, Dominique Perrin, Marie Béal, Akihiro Munemasa, Wit Forys, Benjamin Weiss, Mikhail Volkov and Mikhail Berlinkov for fruitful and essential remarks throughout the study.

References

1. R.L. Adler, B. Weiss: Similarity of automorphisms of the torus, Memoirs of the Amer. Math. Soc., 98, Providence, RI, 1970.
2. D. S. Ananichev, V. V. Gusev, and M. V. Volkov. Slowly synchronizing automata and digraphs. Springer, LNCS, 6281(2010), 55-65.
3. J Almeida, B Steinberg. Matrix Mortality and the Černy-Pin Conjecture. DLT 2009, LNCS, 5583(2009), Monographs in Math. Springer, 67-80.
4. M.-P. Béal, A note on Černy Conjecture and rational series, technical report, Inst. Gaspard Monge, Univ. de Marne-la-Vallee, 2003.
5. M.-P. Béal, M.V. Berlinkov, D. Perrin. A quadratic upper bound on the size of a synchronizing word in one-cluster automata, Int. J. Found. Comput. Sci. 22(2), 2011, 277-288.
6. M.V. Berlinkov, M Szykula. Algebraic synchronization criterion and computing reset words. Information Sciences, 2016. Elsevier Volume 369, 2016, 718-730.
7. J. Berstel, C. Reutenauer, *Rational series and their languages*, Springer, 1988.
8. A. Carpi, F. D’Alessandro, *Strongly transitive automata and the Černý conjecture*. Acta Informatica, 46(2009), 591-607.
9. J. Černý, *Poznamka k homogeným eksperimentom s konečnými automatami*, Math.-Fyz. Čas., 14(1964), 208-215.
10. A. Carpi, F. D’Alessandro, *On the Hybrid Černý-Road coloring problem and Hamiltonian paths*. LNCS, 6224(2010), 124-135.
11. K. Chmial, A. Roman. *COMPAS - A Computing Package for Synchronization*. LNCS, Impl. and Appl. of Automata, 6482(2011), 79-86, 2011.
12. J. Černý, A. Piricka, B. Rosenauerova. *On directable automata*, Kybernetika 7(1971), 289-298.
13. H. Don, H. Zantema, *Finding DFAs with maximal shortest synchronizing word length*. arXiv:1609.06853, 2016.
14. P. Frankl, *An extremal problem for two families of sets*. Eur. J. Comb., 3(1982), 125-127.
15. J. Friedman. *On the road coloring problem*. Proc. of the Amer. Math. Soc., 110(1990), 1133-1135.
16. B. Gerencser, V. V. Gusev, and R. M. Jungers. *Primitive sets of nonnegative matrices and synchronizing automata*. SIAM J. Matrix Analysis and Applications, 39 (1):83(98), 2018.
17. F. Gonze and R. M. Jungers. *On the synchronizing probability function and the triple rendezvous time for synchronizing automata*. SIAM J. Discrete Math., 30(2):995(1014), 2016.
18. F. Gonze, R. M. Jungers, A.N. Trahtman. *A Note on a Recent Attempt to Improve the Pin-Frankl Bound*. DM & TCS, 1(17), 2015, 307-308.
19. F. Gonze, V. V. Gusev, B. Gerencser, R. M. Jungers, M. V. Volkov. On the interplay between Babai and Černý’s conjectures. LNCS, v. 10396, 185-197.
20. R. M. Jungers. *The synchronizing probability function of an automaton*. SIAM Journal on Discrete Mathematics, 26(1):177(192), 2012.
21. H. Jurgensen, *Synchronization*. Inf. and Comp. 206(2008), 9-10, 1033-1044.
22. J. Kari, *A counter example to a conjecture concerning synchronizing word in finite automata*, EATCS Bulletin, 73(2001), 146-147.
23. J. Kari, *finite automata on Eulerian digraphs*. LNCS, 2136(2001), Springer, 432-438.
24. J. Kari, M. V. Volkov, Černý’s conjecture and the road coloring problem. Handbook of Automata, 2013.
25. A. Kisielewicz, J. Kowalski, M. Szykula. *Computing the shortest reset words of synchronizing automata*. J. Comb. Optim., Springer, 29(2015), 88-124.
26. A.A. Klijachko, I.K. Rystsov, M.A. Spivak, *An extremely combinatorial problem connected with the bound on the length of a recurrent word in an automata*. Kybernetika, 2(1987), 16-25.
27. P. Lankaster, *Theory of matrices*, Acad. Press, 1969.
28. A. E. Laemmel. *Study on application of coding theory*. Technical Report PIBMRI-895. Dept. Electrophysics, Microwave Research Inst., Polytechnic Inst., Brooklyn, NY, 5-63, 1963.
29. C. L. Liu. *Determination of the final state of an automaton whose initial state is unknown*. IEEE Transactions on Electronic Computers, EC-12(5):918-920, 1963.
30. A. I. Malcev, *Foundations of linear algebra*, San Francisco, Freeman, 1963. (Nauka, 1970, in Russian.)
31. A. Mateescu and A. Salomaa, *Many-Valued Truth Functions, Černý’s conjecture and road coloring*, Bulletin EATCS, 68 (1999), 134-148.
32. D. Perrin, M.-P. Schutzenberger. *Synchronizing prefix codes and automata and the road coloring problem*. Symbolic dynamics and its applications, 135 (1992), 295-318.

33. J.-E. Pin, *On two combinatorial problems arising from automata theory*. Annals of Discrete Math., 17(1983), 535-548.

34. A. Roman, *Experiments on Synchronizing Automata*. Schedae Informaticae, Versita, Warsaw, 19(2010), 35-51.

35. P. H. Starke. *Eine Bemerkung ueber homogene Experimente*. Elektronische Informationverarbeitung und Kybernetik, 2(1966), 257-259.

36. B. Steinberg, *The Averaging Trick and the Cerny Conjecture*. DLT, Springer, NY, LNCS, 6224(2010), 423-431.

37. A.N. Trahtman, *Notable trends concerning the synchronization of graphs and automata*. CTW06. El. Notes in Discrete Math., 25(2006), 173-175.

38. A.N. Trahtman, *The Cerny Conjecture for Aperiodic Automata*. Discr. Math. Theoret. Comput. Sci. 9, 2(2007), 3-10.

39. A.N. Trahtman, *Matrix approach to synchronizing automata*, [http://arxiv.org/abs/1904.07694](http://arxiv.org/abs/1904.07694).

40. A.N. Trahtman, *The Road Coloring and Cerny Conjecture*. Proc. of Prague Stringology Conference, 2008, 1-12.

41. A.N. Trahtman, *The Road Coloring*. Israel J. of Mathematics, 172, 1(2009), 51-60.

42. A.N. Trahtman, *Bibliography*, [http://u.cs.biu.ac.il/~trakht/syn.html](http://u.cs.biu.ac.il/~trakht/syn.html).

43. A.N. Trahtman, *Synchronization*, [http://u.cs.biu.ac.il/~trakht/readme.html](http://u.cs.biu.ac.il/~trakht/readme.html).

44. M. V. Volkov, *Synchronizing automata and the Cerny conjecture*, in: C.Martin-Vide, F. Otto, H. Fernau eds., Language and Automata Theory and Applications, LATA 2008, Springer, LNCS, 5196(2008), 11-27.

45. M. V. Volkov, *Lecture Notes on Synchronizing Automata*, M. V. Volkov, 2016, [http://csseminar.kadm.usu.ru/Hunter/lectures.pdf](http://csseminar.kadm.usu.ru/Hunter/lectures.pdf).