The length of a minimal synchronizing word and the Černy conjecture

A.N. Trahtman

Abstract. A word $w$ of letters on edges of underlying graph $Γ$ of deterministic finite automaton (DFA) is called synchronizing if $w$ sends all states of the automaton to a unique state. J. Černy 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 the Černy conjecture, claims that it is also precise upper bound on the length of such a word for a complete DFA. The hypothesis was formulated in 1966 by Starke. The problem has motivated great and constantly growing number of investigations and generalizations.

To prove the conjecture, we use algebra with non-standard operations on a special class of matrices (row monomial), induced by words in the alphabet of labels on edges. These matrices generate a space with respect to the mentioned operation.

The proof is based on connection between length of words $u$ and dimension of the space generated by solutions $L_x$ of matrix equation $M_uL_x = M_s$ for synchronizing word $s$, as well as on the relation between ranks of $M_u$ and $L_x$.

Keywords: deterministic finite automaton, synchronizing word, Černy conjecture.

Introduction

The problem of synchronization of DFA is a natural one and various aspects of this problem have been touched in the literature. Prehistory of the term, the connections with the early coding theory, first efforts to estimate the length of synchronizing word [22], [23], different problems of synchronization one can find in surveys [15], [18], [39], [38].

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.

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

J. Černy in 1964 [7] 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:

**Conjecture 1** The deterministic complete n-state synchronizing automaton over alphabet \( \Sigma \) has synchronizing word in \( \Sigma \) of length at most \((n - 1)^2\) \[29\] (Starke, 1966).

The problem can be reduced to automata with a strongly connected graph \[7\]. An attempt to prove this hypothesis is proposed below.

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 \[36\].

Moreover, two conferences ”Workshop on Synchronizing Automata” (Turku, 2004) and ”Around the Černý conjecture” (Wrocław, 2008) were dedicated to this longstanding conjecture. The problem is discussed in ”Wikipedia” - the popular Internet Encyclopedia and on many other sites.

As well as the Road Coloring problem \[1\], \[13\], \[34\], this simple-looking conjecture was arguably the most longstanding and famous open combinatorial problems in the theory of finite automata \[15\], \[25\], \[26\], \[29\], \[30\], \[38\].

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 \( \Gamma \). We call them matrices of word.

The matrix \( M_u \) of word \( u \) belongs to the class of matrices with one unit in every row and rest zeros (row monomial). Row monomial matrices also can be considered as matrices of word of some suitable graph.

There are no examples of automata such that the length of the shortest synchronizing word is greater than \((n - 1)^2\). 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 Rosenaurova \[10\] of 1971 for \( |\Sigma| = 2 \), the next such examples were found by Kari \[16\] in 2001 for \( n = 6 \) and \( |\Sigma| = 2 \) and by Roman \[28\] for \( n = 5 \) and \( |\Sigma| = 3 \) in 2004.

The package TESTAS \[34\], \[37\] 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 \((n - 1)^2\) with \( n \leq 4 \).

Don and Zantema present in \[11\] an ingenious method of designing 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 exactly 12 DFA for \( n = 4 \) with shortest synchronizing word of length \((n - 1)^2\). The authors of \[11\] support the hypothesis from \[32\] 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 \[2\], \[4\], \[6\], \[11\], \[32\] 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], [9], [17], [19], [33].

Initially found upper bound for the minimal length of synchronizing word was very big and has been consistently improved over the years by different authors. The upper bound found by Frankl in 1982 [12] is equal to \((n^3 - n)/6\). The result was reformulated in terms of synchronization in [27] and repeated independently in [20].

The cubic estimation of the bound exists since 1982. Attempts to improve Frankl’s result were unsuccessful.

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

Our work uses a special class of matrices \( M_u \) of mapping induced by words \( u \) in the alphabet of letters on edges of the underlying graph (row monomial) with properties of corresponding space.

We study the rational series \((S, u)\) (see [3]). This approach for synchronizing automata supposed first by Béal [3] proved to be fruitful [4], [6], [8].

We consider the equation \( M_uL_x = M_s \) for synchronizing word \( s \) and the space generated by a sort of its row monomial solutions \( L_x \).

A connection between the set of nonzero columns of matrix of word, subsets of states of automaton and our kind \( L_x \) of solutions of \( (3) \) is revealed in Remarks.

There are no examples of automata such that the length of the shortest synchronizing word is greater than \((n - 1)^2\). 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 [10] of 1971 for \(|\Sigma| = 2\), the next such examples were found by Kari [16] in 2001 for \( n = 6 \) and \(|\Sigma| = 2\) and by Roman [28] for \( n = 5 \) and \(|\Sigma| = 3\) in 2004.

The package TESTAS [34], [37] 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 \((n - 1)^2\) with \( n \leq 4\).

Don and Zantema present in [11] an ingenious method of designing 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 exactly 12 DFA for \( n = 4 \) with shortest synchronizing word of length \((n - 1)^2\). The authors of [11] support the hypothesis from [32] 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], [4], [8], [11], [32] 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], [9], [17], [19], [33].

Initially found upper bound for the minimal length of synchronizing word was very big and has been consistently improved over the years by different authors. The upper bound found by Frankl in 1982 [12] is equal to \((n^3 - n)/6\). The result
was reformulated in terms of synchronization in [27] and repeated independently in [20].

The cubic estimation of the bound exists since 1982. Attempts to improve Frankl’s result were unsuccessful.

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

Our work uses a special class of matrices $M_u$ of mapping induced by words $u$ in the alphabet of letters on edges of the underlying graph (row monomial) with properties of corresponding space.

We study the rational series $(S, u)$ (see [5]). This approach for synchronizing automata supposed first by Béal [3] proved to be fruitful [4], [6], [8].

We consider the equation $M_u L_x = M_s$ (3) for synchronizing word $s$ and the space generated by a sort of its row monomial solutions $L_x$.

A connection between the set of nonzero columns of matrix of word, subsets of states of automaton and our kind $L_x$ of solutions of (3) is revealed in Remarks.

Theorems 1, 2 finish our attempt to prove the Černý conjecture. Theorem 3 and some corollaries contain certain consequences.

We consider the equation $M_u L_x = M_s$ (3) for synchronizing word $s$ and the space generated by a sort of its row monomial solutions $L_x$.

A connection between the set of nonzero columns of matrix of word, subsets of states of automaton and our kind $L_x$ of solutions of (3) is revealed in Remarks.

The ideas of the proof are illustrated on examples of automata with a maximal length of synchronizing word from [16], [7], [28].

**Preliminaries**

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

The restriction on strongly connected graphs is based on [7]. The states of the automaton $A$ are considered also as vertices of the graph $Γ$.

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 $σ_1, ..., σ_k$, then for $s = σ_1...σ_k ∈ Σ^+$ let us write $q = ps$.

Let $Px$ be the set of states $q = px$ for all $p$ from the subset $P$ of states and $x ∈ Σ^+$. Let $Ax$ denote the set $Px$ for the set $P$ of all states of the automaton.

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

The problem can be reduced to automata with a strongly connected graph [7].

The states of the automaton are enumerated with number one for the 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 (row monomial).

We connect a mapping of the set of states of the automaton made by a word $u$ with an $n \times n$-matrix $M_u$ such that for an element $m_{i,j} \in M_u$ takes place

$$m_{i,j} = \begin{cases} 1, & q_i u = q_j; \\ 0, & \text{otherwise}. \end{cases}$$

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.

$M_u M_v = M_{uv}$. \[1\]

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 proper subword $v$ of $u$ $M_u \neq M_v$.

The minimal synchronizing word and all its subwords are irreducible.

Zero matrix is considered as a matrix of empty word.

The subset of states $A u$ is denoted as $c_u$ 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 \[21\], \[24\].

1 **Mappings induced by a word and subword**

**Remark 1** The invertible matrix $M_a$ does not change the number of units of every column of $M_u$ in its image of the product $M_u M_a$.

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

**Remark 2** The columns of the matrix $M_a M_u$ are obtained by permutation of columns $M_u$. Some columns can be merged (units of columns are moved along row to a common column) with $|R(ua)| < |R(u)|$.

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

**Lemma 1** The number of nonzero columns $|R(b)|$ is equal to the rank of $M_b$.

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

\[ R(au) \subseteq R(u). \]

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

For the set of states of deterministic finite automaton \( A \) and any words \( u \)
and \( a \) \( Aua \subseteq Aa. \)

Nonzero columns of \( M_{ua} \) have units also in \( M_a. \)

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

The matrix \( M_a \) in the product \( M_u M_a \) shifts column of \( M_u \) to columns
of \( M_u M_a \) without changing the column itself by Remark 2 or merging. some
columns of \( M_u. \)

In view of possible merged columns, \( |R(ua)| \leq |R(u)|. \)

Some rows of \( M_u \) can be replaced in \( M_u M_a \) by another row and therefore
some rows from \( M_u \) may be changed, but zero columns of \( M_u \) remain in \( M_u M_a \)
(Remark 1).

Hence \( R(au) \subseteq R(u) \) and \( |R(ua)| \leq |R(u)|. \)

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

From \( R(ua) \subseteq R(a) \) follows \( Aua \subseteq Aa. \)

Nonzero columns of \( M_{ua} \) have units also in \( M_a \) in view of \( R(ua) \subseteq R(a). \)

Corollary 1 The invertible matrix \( M_a \) keeps the number of units of any column
of \( M_u \) in corresponding column of the product \( M_u M_a. \)

Corollary 2 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.

Lemma 2 Suppose that for row monomial matrices \( M_i \) and \( M \)

\[ M = \sum_{i=1}^{k} \lambda_i M_i, \]  

(1)

with coefficients \( \lambda \) from \( Q. \)

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 (1) also is equal to one.

If \( \sum_{i=1}^{k} \lambda_i M_i = 0 \) 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 \( \{\text{zero}\} \) then \( \sum_{i=1}^{k} \lambda_i M_i \) is not a
row monomial matrix.

Proof. The nonzero matrices \( M_i \) have \( n \) cells with unit in the cell. Therefore,
the sum of values in all cells of the matrix \( \lambda_i M_i \) is \( n \lambda_i. \)

For nonzero \( M \) the sum is \( n. \) So one has in view of \( M = \sum_{i=1}^{k} \lambda_i M_i \)

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

whence \( 1 = \sum_{i=1}^{k} \lambda_i. \)
Let us consider the row $j$ of matrix $M_j$ in (1) and let $1_j$ be unit in the row $j$. The sum of values in a row of the sum (1) is equal to unit in the row of $M$. So $1 = \sum_{i=1}^{k} \lambda_i 1_i = \sum_{i=1}^{k} \lambda_i$.

$\sum_{i=1}^{k} \lambda_i M_i = 0$ implies $S_j = \sum_{i=1}^{k} \lambda_i 1_i = \sum_{i=1}^{k} \lambda_i = 0$ for every row $j$.

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

The set of row monomial matrices is closed with respect to the considered operation and together with zero matrix generates a space.

**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 only 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,

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

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 only value of $m$ 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 from the set $V$ is a span of $(k - 1)n + 1$ 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 3** The set of all row monomial \( n \times (n - 1) \)-matrices of words (or \( n \times n \)-matrices with zeros in a fixed column) has \((n - 1)^2\) linear independent matrices.

The set of row monomial \( n \times n \)-matrices has at most \( n(n - 1) + 1 \) linear independent matrices.

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

**Corollary 4** Suppose the vertex \( p \notin A\alpha \) 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 \( p \) because \( p \notin A\alpha \). So we have \( n \times n \)-matrices with zeros in a fixed column and due to Corollary 3 there are at most \((n - 1)^2\) linear independent matrices \( M_u \).

**Corollary 5** There are at most \( n(n - 1) + 1 \) linear independent matrices of words in the set of \( n \times n \)-matrices.

**Lemma 4** Distributivity from left.

For every words \( b \) and \( x_i \)

\[
M_b \sum \tau_i M_{x_i} = \sum \tau_i M_b M_{x_i}.
\]

If \( \sum \tau_i M_{x_i} \) is a matrix of word then also \( \sum \tau_i M_b M_{x_i} \) is a matrix of word.

Proof. The matrix \( M_b \) shifts rows of every \( M_{x_i} \) 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 \( M_b M_{x_i} \) and the sum \( \sum \tau_i M_b M_{x_i} \) has the origin rows with one unit from \( M_{x_i} \) and from its linear combination \( \sum \tau_i M_{x_i} \), maybe in another order.

If the matrix \( \sum \tau_i M_{x_i} \) is a matrix of word then also the matrix \( M_b \sum \tau_i M_{x_i} = \sum \tau_i M_b M_{x_i} \) is a matrix of word with unit in every row.

Let us notice that from right it is sometimes wrong.

## 2 Rational series

The section follows ideas and definitions from [5] and [3]. 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 \( K \) [5], [6].

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 [8], we denote by $S$ the rational series depending on the set $P$ defined by:

$$(S, u) = CM_uP^t - CP^t = C(M_u - E)P^t.$$  \hspace{1cm} (2)

**Remark 3** 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 \([2]\) added to $(S, u)$ the value of $k - 1$.

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

**Lemma 5** Let $S$ be a rational series depending on the set $P$ of an automaton $A$. Let $M_u = \sum_{j=1}^{n} \lambda_j M_{uj}$. 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 \((2)\)

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

where $C$ is a row of units and $P^t$ is a characteristic column of units and zeros.

Due to Lemma \([2]\)

$$\sum_{j=1}^{k} \lambda_j M_{uj} - E = \sum_{j=1}^{k} \lambda_j M_{uj} - \sum_{j=1}^{k} \lambda_j E = \sum_{j=1}^{k} \lambda_j (M_{uj} - E).$$

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

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 \([2]\).

From Lemma \([5]\) 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 \([8]\) 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 $V$.

### 2.1 The equivalence for the state $q$, rational series $S_q$

**Definition 1** Two matrices $M_u$ and $M_v$ of word are called $q$-equivalent if the columns of the state $q$ of both matrices are equal. We denote it as
\[ M_u \sim_q M_v. \]

If the set of cells with units in the column \( q \) of the matrix \( M_v \) is a subset of the analogous set of the matrix \( M_u \), then we write
\[ M_v \sqsubseteq_q M_u. \]

Let rational series \( S_q \) depend only on the set \( P = \{ q \} \) for the state \( q \) of number one.

Of course, for \( A_s = q \) and rational series depending on the set \( P = \{ q \} \) for matrices of words in the alphabet \( \Sigma \).

**Remark 4** The matrix \( M_u \) has \( (S_q, u) + 1 \) units in the column \( q \).

\[(S_q, u) = (S_q, v) \text{ if } M_u \sim_q M_v \text{ and} \]
\[(S_q, v) \leq (S_q, u) \text{ if } M_v \sqsubseteq_q M_u \]

**Lemma 6** For matrices \( M_a, M_u, M_v \) of words \( u, v \)
\[ M_u \sim_q M_v \rightarrow M_{au}M_u = M_{au}M_v = M_{av}, \]
\[ M_v \sqsubseteq_q M_u \rightarrow M_{av}M_v \sqsubseteq_q M_{au}M_u. \]

**Proof.** Suppose \( M_u \sim_q M_v \) and element \( a_{i,r} = 1 \) in \( M_a \). For an element \( u_{r,q} \) in the column \( q \) of \( M_u \) and \( t_{i,q} \in M_t = M_aM_u \)
\[ t_{i,q} = \sum_{m=1}^n a_{i,m}u_{m,q} = a_{i,r}u_{r,q} \]

because \( a_{i,m} = 0 \) for \( m \neq r \) in the matrix \( M_a \) of word \( a \) (Remark 1). Analogously, in the matrix \( Z = M_{av} \) \( z_{i,q} = a_{i,r}v_{r,q} \).

Therefore \( z_{i,q} = a_{i,r}v_{r,q} = a_{i,r}u_{r,q} = t_{i,q} \) because \( v_{r,q} = u_{r,q} \) for every cell \((i, q)\) of the column \( q \) of \( M_u \) and \( M_v \).

Thus matrices \( M_{au} \) and \( M_{av} \) have common columns \( q \). So \( M_u \sim_q M_v \) implies \( M_{au} \sim_q M_{av} \).

Suppose now \( M_v \sqsubseteq_q M_u \). For the matrix \( T = M_{av} \) with \( t_{i,q} = 1 \) one has \( t_{i,q} = a_{i,r}v_{r,q} = 1 \) for some \( v_{r,q} = 1 \) and \( a_{i,r} = 1 \) as well as before. From \( v_{r,q} = 1 \) and \( M_v \sqsubseteq_q M_u \) follows \( 1 = v_{r,q} = u_{r,q} \). So for the matrix \( W = M_{au} \) one has \( w_{i,q} = a_{i,r}u_{r,q} = 1 \), whence \( t_{i,q} = 1 \) implies \( w_{i,q} = 1 \) for every \( i \).

Thus \( M_v \sqsubseteq_q M_u \) implies \( M_{av}M_v \sqsubseteq_q M_{au}M_u \).

From Lemma 6 follow

**Corollary 8** For \( A_s = q \) and \( M_u \sim_q M_v \)
\[ M_s \sim_q M_t \rightarrow M_s = M_tM_u = M_tM_v. \]

For \( M_v \sqsubseteq_q M_u \)
\[ M_s = M_{1M_v} \rightarrow M_s = M_{1M_u}. \]
\[ M_vL_u \sim_L M_{vu} \text{ for any words } u, v. \]

In the following example \( V_1 \sim_q V_2 \) for the first column \( q \). \( M_s = M_a V_1 = M_a V_2 \).

\[
M_a = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}, \quad V_1 = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}, \quad V_2 = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad M_{aV_1} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}.
\]
3 The equation with unknown $L_x$

Rational series $S_q$ depends on the state $q$. $A s = q$ for irreducible synchronizing word $s$.

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 $q$.

**Lemma 7** Every equation $M_u L_x = M_s$ (3) has solutions $L_x$ with $n > (S_q, x) \geq 0$.

$|R(u)| - 1 = (S_q, x)$ for $L_x$ with minimal $(S_q, x)$ (a minimal solution), every matrix $L_y$ satisfies the equation (3) iff $L_x \subseteq_q L_y$.

There exists one-to-one correspondence between units in the column $q$ of minimal solution $L_x$ and the set $c_u$ of states. Every set $c \supset c_u$ is presented by units of column $q$ of some not minimal solution $L_y$ of the equation.

**Proof.** The matrix $M_s$ of rank one has nonzero column of the state $q$. For every nonzero column $j$ of $M_u$ with elements $u_{i,j} = 1$ 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 $L_x$.

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

Therefore by Remark 3 for rational series $S$ that depends on the state $q$ the minimal solution $L_x$ has in the column $q$ $(S_q, x) + 1$ units, whence $(S_q, x) = |R(u)| - 1$.

So to the column $q$ of every solution belong at least $(S_q, x) + 1$ units. The remaining units of the solution $L_x$ belong to the next columns, one unit in a row. The remaining cells obtain zero.

Lastly every solution $L_x$ is a matrix of word.

Zeros in the column $q$ of minimal $L_x$ correspond zero columns of $M_u$. Therefore for matrix $L_y$ such that $L_x \subseteq_q L_y$ we have $M_u L_y = M_s$. On the other hand, every solution $L_y$ must have units in cells of column $q$ that correspond nonzero columns of $M_u$.

Thus $L_x$ has minimal $(S_q, x)$ and the equality $M_u L_x = M_u L_y = M_s$ is equivalent to $L_x \subseteq_q L_y$.

The matrix $M_u$ has set $R(u)$ of nonzero columns and maps the automaton on the set $c_u$ of states and on the set of units in the column $q$ of minimal $L_x$. Units in the column $q$ of $L_y$ correspond some set of states $c \supset c_u$.

**Lemma 7** explains the following

**Remark 5** Every permutation and shift of $m$ nonzero columns $M_u$ induces corresponding permutation of the set of $m$ units in the column $q$ of minimal solution $L_x$ of (3), and vice versa.
Definition 2 Let us call the matrix $M_a^-$ of word a left \textit{generalized inverse 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 arbitrarily in such row of the matrix $M_a^-$ of word.

For invertible matrix $M_a$ we have $M_a^- = M_a^{-1}$, for singular $M_a$ there are some generalized inverse matrices, including invertible.

3.1 Right pseudoinverse matrices

Definition 8 Let us call the matrix $M_a^-$ of word a right \textit{pseudoinverse matrix} of the matrix $M_a$ of 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.

In still zero rows of $M_a^-$ is added one unit arbitrarily in such row. Zeros fill rest of cells. So it is a matrix of word.

For instance,

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

Remark 6 For invertible matrix $M_a$ (with $|R(a)| = n$) we have a special case $M_a^- = M_a^{-1}$, for singular $M_a$ there are some pseudoinverse matrices, even some invertible.

The product $M_a M_a^-$ does not depend on arbitrary adding of units in rows of $M_a^-$ corresponding zero columns of $M_a$ in view of Remark 7 because the nonzero product needs at least one nonzero cell in corresponding column of $M_a$.

Remark 7 Some matrix $M_a^-$ with $A_s = q$ defines set of paths of $s$ from the state $q$ in opposite direction to every state.

Some matrix $M_a^-$ defines several paths of $a$ from the state $q$ in opposite direction to the set of corresponding states $c_a$.

By Definition 8 and Lemma 7 for $M_b^-$ and $M_a^- = \sum \lambda_i M_{a_i}$ one has

$$M_b^- M_a^- = M_{ab}^- \quad \text{and} \quad M_b^- M_a^- = M_b^- \sum \lambda_i M_{a_i} = \sum \lambda_i M_b^- M_{a_i}.$$}

Lemma 9 For every equation $M_u L_x = M_s$ and every letter $\beta$ the equation

$$M_u \beta L_y = M_s$$

has solution $L_y$. For minimal solutions $L_x$ of (3) and $L_y$ one has $(S_q, y) \leq (S_q, x)$. $R(y) \geq R(x)$ is possible for some $L_y$.

For every solution $L_x$ of equation (3) and suitable $M_{\beta}^-$, even invertible,

$$M_s = M_u M_{\beta} M_{\beta}^- L_x$$
for solution $M^{-}_{\beta}L_{x}$ of the equation $[4]$. Let $|R(u)| = |R(u_\beta)|$. Then $(S_q, y) = (S_q, x)$ for minimal solutions $L_y$, $L_x$ and maximal ranks $|R(y)| = |R(x)|$ for invertible $M^{-}_{\beta}$. $R(y) = R(x)$ for invertible $M^{-}_{\beta}$ anyway.

For $|R(u)| \neq |R(u_\beta)|$ and singular $M_\beta$- there exists solution $L_y$ of the equation $M_\alpha M_\beta L_y = M_\alpha L_y = M_\alpha$ such that $(S_q, y) < (S_q, x)$ for minimal solutions and $|R(y)| > |R(x)|$ for maximal ranks. Thus for some $L_y$ one has $R(x) \subseteq R(y)$ and $|R(y)| = |R(x)| + |R(u)| - |R(u_\beta)|$. $|R(u)| + |R(x)| = n + 1$ for last considered word $u$ and corresponding minimal solution $L_x$.

Proof. The equality in $[4]$ is correct for some $L_y$. By Lemma $1$ $|R(u)| \geq |R(u_\beta)|$.

Therefore by Corollary $9$ $(S_q, y) \leq (S_q, x)$ for minimal solutions $L_x$ and $L_y$. Hence in view of arbitrary placing $n - (S_q, y)$ units in $L_y$ outside column $q$ (Lemma $7$), $R(x) \subseteq R(y)$ is possible for some minimal $L_y$.

The matrix $M^{-}_{\beta}$ returns the set of nonzero columns from $R(u_\beta)$ to $R(u)$ (or to its part) in view of Definition $8$.

Arbitrary placing of units in some rows of $M^{-}_{\beta}$ does not change the product $M_\beta M^{-}_{\beta}$ by Remark $5$. Therefore $|R(u)M_\beta M^{-}_{\beta}| \leq |R(u)|$, whence $(S_q, x) \geq (S_q, y)$. Hence the equality in $M_\alpha M_\beta M^{-}_{\beta}L_x = M_\alpha M^{-}_{\beta}L_x = M_\alpha M_\beta L_y = M_\alpha$

is correct for some $L_y = M^{-}_{\beta}L_x$ with $R(x) \subseteq R(y)$ and free placing only of $(S_q, x) - (S_q, y)$ units in $L_y$ (see Lemma $7$).

In the case $|R(u)| = |R(u_\beta)|$ the matrix $M_\beta$ does not merge some columns of $M_\alpha$ and by Lemma $7$ $(S_q, y) = (S_q, x)$ for minimal solutions $L_y$ and $L_x$. So $R(y) = R(x)$ in view of $R(x) \subseteq R(y)$ and Lemma $7$ for invertible matrix $M^{-}_{\beta}$.

From $|R(u)| \neq |R(u_\beta)|$ due to Lemma $1$ follows $|R(u_\beta)| < |R(u)|$, whence for some solution $L_y$ of the equation $M_\alpha M_\beta L_y = M_\alpha (S_q, y) < (S_q, x)$ for both such minimal solutions by Lemma $7$.

After filling by units nonzero columns of $R(x)$ by units from $R(y)$. $R(x)$ can be extended by new columns using arbitrary addition of $|R(y)| - |R(x)|$ units and $R(y) \supseteq R(x)$.

The possible equalities $|R(x)| = n - (S_q, x)$ and $|R(u)| - 1 = (S_q, x)$ (Lemma $7$) imply for minimal $L_y$ and $L_x$ and maximal ranks $|R(u)| + |R(x)| = n + 1$, $|R(y)| - |R(x)| = (S_q, x) - (S_q, y)$ and $|R(y)| = n - (S_q, y) = |R(x)| + (S_q, x) - (S_q, y) = |R(x)| + |R(u)| - |R(u_\beta)|$.

Corollary 9 Let $M_\alpha L_x = M_\alpha$ and $|a| < n$ for words $a$.

A set of $m \leq n$ linear independent matrices $L_y = M^{-}_{\beta}L_x$ with $(S_q, y) = (S_q, x)$ can be created by help of invertible generalized inverse matrix $M^{-}_{\alpha}$.

From Lemma $9$ follows

Corollary 10 A set of linear independent solutions $L_x$ of $[3]$ with constant $(S_q, x)$ and fixed $R(x)$ can be expanded by help of invertible matrices $M^{-}_{\beta}$ (and words of them) with the same $(S_q, x)$ and common set $R(x)$. 
Proof. The invertible matrix $M^{-1}_{\beta}$ does not change $(S_q, x)$ and $R(x)$ of matrix $L_x$ in the equation (4) by Corollary 1.

Anyway we have a space generated by row monomial matrices with one unit in every row and with rest of zeros.

**Remark 8** Not minimal solutions $L_y$ of (4) with $(S_q, y) > (S_q, x)$ and $R(y) \subset R(x)$ also are useful sometimes for extending subspace $V_k$ of greater $(S_q, y) = n - k$. Arbitrary placing of units in $L_y$ is preferable in nonzero columns of matrices of $V_k$.

**Lemma 10** Let the space $W$ be generated by matrix $M_s$ of minimal synchronizing word $s$ and solutions $L_x$ of the equation $M_uL_x = M_s$ (3) with $(S_q, x) > 0$ of words $u$. All generators $W$ have common zero column.

Then there exist a word $u$ in equation (3) such that the solution $L_x \in W$ and a letter $\beta$ such that the solution $L_y \notin W$ of the equation $M_{u\beta}L_y = M_s$.

Proof. Assume the contrary: for every word $u$ of (3) with solution $L_x \in W$ and every letter $\beta$ the equation $M_{u\beta}L_y = M_s$ has every solution $L_y \in W$.

The space $W$ is not changed by the assumption and has the same basis. The matrices in $W$ have the same zero column.

The solution $L_y$ is a linear combination of matrices from basis of $W$ and therefore $L_y$ can replace one matrix from this linear combination thereby creating a new basis of $W$ with $L_y$.

By assumption, every solution $L_y$ of equation $M_uL_y = M_s$ belongs to $W$ for the word $v = u\beta$ with $|v| \leq |u| + 1$.

Let us consider the word $u\beta\delta = v\delta$ of length $|u| + 2 = |v| + 1$ for arbitrary letter $\delta$ and solution $L_z$ of equation $M_{u\delta}L_z = M_sM_{\delta}L_z = M_s$ for the word $v\delta$.

By assumption, the solution $L_z$ of equation $M_{\delta}L_z = M_s$ also belongs to $W$.

By induction it is true for the word $u$ from (3) and $v$ of every length, whence every solution $L_z$ has the common zero column. $L_x$ with $(S_q, x) > 0$ also belongs to some basis of $W$ as a solution of (3).

The considered automaton is synchronizing, therefore for every word $u$ exists a synchronizing continuation $v$ of $u$ with $|R(uv)| = 1$ of synchronizing matrix $M_{uv}$. Now $(S_q, x) = 0$ by Lemma 7 in spite of $(S_q, x) > 0$ above.

Therefore the existence of common zero column in all solutions $L_x$ of (3) contradicts the emergence of minimal solution $L_x$ with $(S_q, x) = 0$ on some step of expanding of words $u$.

4 The sequence of spaces of solutions $L_x$ for words $u$ of growing length

We are going to define a sequence of spaces $W_j$ which is is generated by $M_s$ of word $s$ and $j$ linear independent solutions $L_x$ of equations $M_uL_x = M_s$ (3) with $|u| \leq j$.

The space $W_0$, in particular, is generated by minimal synchronizing matrix $M_s$, a trivial solution of every equation (3): $\dim(W_0) = 1$. The matrix $M_s$ and
the minimal solution $L_x$ of equation $M_\alpha L_x = M_\alpha$ for the left letter $\alpha$ of minimal $s$ generate the subspace $W_1$. $\dim(W_1) = 2$.

We consider for every $W_j$ the set of solutions $L_x$ of equation (3) for $|u| \leq j + 1$. We choose a solution $L_x \not\subset W_j$ for minimal such $|u|$ following Lemmas 7 and 9. The existence of such $L_x$ is studied in Lemma 10. Then $L_x$ is added to the space $W_j$ turning it into the space $W_{j+1}$ with corresponding growth of $j$.

The solutions $L_x$ of equations $M_\alpha L_x = M_\alpha$ with fixed $(S_\alpha, x) = n - i$ generate subspace $V_i \subset W_j$ with the same $(S_\alpha, x)$ by Corollary 11. $V_i$ can be extended by help of invertible matrices $M_\beta$ of letters with keeping by Corollary 9 the same rank $|R(x)|$. In view of Lemma 3 the set of nonzero columns in matrices $V_i$ does not change because $M_\beta$ is invertible.

We can extend $V_i$ following Corollary 9 or reduce $(S_\beta, x) = i$.

The space $W_j$ is created by generators $L_x$ of subspaces $V_i$ by decrease of $i$ from $i = n - 1$ until $i = 1$. So $(S_\beta, x) > 0$ for all generators $L_x$ of $W_j$ because for $i > 0$ $L_x$ have common zero column.

With decreasing of $(S_\beta, x)$ and increasing $|R(x)|$, we can add to the set of nonzero columns of matrices $L_x$ new columns due to $R(y) \supset R(x)$ and $|R(y)| = |R(x)| + (S_\beta, x) - (S_\beta, y)$ (Lemma 9).

The set of nonzero columns in matrices $W_j$ is a union of nonzero columns of matrices from $V_i$ and in view of $(S_\beta, x) > 0$ there is common zero column in matrices $W_j$.

One can extend the rank $|R(x)|$ and reduce $(S_\beta, x)$ of minimal solution $L_x$ of (3) only by decreasing $|R(u)|$ (Lemma 9, Corollary 10).

We follow conditions of Lemma 9 with a view to obtain $(S_\beta, x) = 0$ for solution $L_x$ of (3). It’s unavoidable after $\dim(W_j) > (n - 1)^2$ (or before) in view of Corollary 10 and Lemma 10.

The distinct linear independent solutions can be added consistently extending the dimension of $W_j$ and upper bound $j$ of the length of the word $u$. So

$$\dim(W_j) = j + 1 \quad |u| \leq j.$$  \hspace{1cm} (5)

5 \hspace{1cm} Theorems

**Theorem 1** The deterministic complete $n$-state synchronizing automaton $A$ with strongly connected underlying graph over alphabet $\Sigma$ has synchronizing word in $\Sigma$ of length at most $(n - 1)^2$.

Proof. The introduction to the former section considers a growing sequence of spaces $W_j$ (an ascending chain by dimension $j + 1$) generated by linear independent solutions $L_x$ of the equations (3) for $|u| \leq j$ by help of Lemmas 7 and 9 with Corollaries.

By Lemma 10 any space $W$ generated by solutions $L_x$ of the equation $M_\alpha L_x = M_\alpha$ with common zero column and of restricted length $|u| \leq j$ has a solution $L_x \not\subset W$ for some word $u$ of length at most $j + 1$.

$$\dim(W_j) \leq n(n - 2) + 1 = (n - 1)^2$$ for $W_j$ with matrices having units in at most $n - 1$ column by Corollary 3 of Lemma 8.
So inevitably at least one solution \( L_y \notin W_j \) of equation (4) has corresponding word \( v \) with \( |v| = j + 1 > (n - 1)^2 \) and minimal \( (S_q, y) = 0 \).

By Lemma 7, for \( L_x \) with minimal \( (S_q, x) \) of equation (3) \( |R(u)| - 1 = (S_q, x) \).

We reach finally a minimal \( (S_q, y) = 0 \) for path of length \( |v| \leq n(n - 2) + 1 \). So

Consequently the matrix \( M_v \) of rank one in equation \( M_v \) has the matrix of synchronizing word \( v \) of length at most \( n(n - 2) + 1 = (n - 1)^2 \).

**Corollary 11** For every integer \( k < n \) of deterministic complete \( n \)-state synchronizing automaton \( A \) with strongly connected underlying graph over alphabet \( \Sigma \) there exists a word \( v \) of length at most \( n(k - 1) + 1 \) such that \( |Av| \leq n - k \).

**Corollary 12** For every set \( P \) of states from deterministic complete \( n \)-state synchronizing automaton over alphabet \( \Sigma \) there exists a word \( s \) of length at most \( (n - 1)^2 \) such that \( |Ps| = 1 \).

**Corollary 13** The graph \( \Gamma^2 \) of pairs of states for deterministic complete \( n \)-state synchronizing automaton with underlying graph \( \Gamma \) and \( \Gamma s = q \) for minimal word \( s \) has a set of paths to the pair \( (q, q) \) of length at most \( (n - 1)^2 \) defined by \( s \).

Every pair of distinct states belongs to a path from the set.

**Theorem 2** The deterministic complete \( n \)-state synchronizing automaton \( A \) with underlying graph over alphabet \( \Sigma \) has synchronizing word in \( \Sigma \) of length at most \( (n - 1)^2 \).

Follows from Theorem 1 because the restriction for strongly connected graphs can be omitted due to 7.

**Theorem 3** Suppose that \( |\Gamma \alpha| < |\Gamma| - 1 \) for a letter \( \alpha \in \Sigma \) in deterministic complete \( n \)-state synchronizing automaton \( A \) with underlying graph \( \Gamma \) over alphabet \( \Sigma \).

Then the minimal length of synchronizing word of the automaton is less than \( (n - 1)^2 \).

Proof. We follow the proof of Theorem 1.

The difference is that at the beginning of the proof the equation (3) has at least two linear independent nontrivial solutions for the matrix \( M_\alpha \) of a letter \( \alpha \) equal to the first word \( u \) of length one.

Hence we obtain finally synchronizing word of length less than \( (n - 1)^2 \).

Let us go to the case of not strongly connected underlying graph with \( n - |I| > 0 \) states outside minimal strongly connected ideal \( I \).

This ideal has synchronizing word of length at most \((|I| - 1)^2 \) (Theorem 1).

There is a word \( p \) of length at most \((n - |I|)(n - |I| + 1)/2 \) such that \( Ap \subset I \).

\((|I| - 1)^2 + (n - |I|)(n - |I| + 1)/2 < (n - 1)^2 \). Thus, the restriction for strongly connected automata can be omitted.

**Theorem 4** Every road coloring of edges of \( n \)-state strongly connected directed graph with constant outdegree and gcd=1 of length of all its cycles has synchronizing word of length at most \( (n - 1)^2 \).
Proof follows from Theorem 1 and work [34].

**Theorem 5** Suppose that $|\Gamma \alpha| < |\Gamma| - 1$ for a letter $\alpha \in \Sigma$ in deterministic complete $n$-state synchronizing automaton $A$ with underlying graph $\Gamma$ over alphabet $\Sigma$.

Then the minimal length of synchronizing word of the automaton is less than $(n - 1)^2$.

**Proof.** We follow the proof of Theorem 1.

The difference is that at the beginning of the proof there are at least two linear independent matrices ($L_\alpha$ and $L_v$) such that $L_\alpha \subseteq_q L_v$ for the letter $\alpha = u$.

So for the first word $u$ of length one there are at least two linear independent matrices with $\dim(W_1) > 2$, i.e. $\dim(W_j) > j$ for $j = 1$.

Hence following the proof of Lemma 10 and Theorem 1 we obtain synchronizing word of length less than $(n - 1)^2$.

Let us go to the case of not strongly connected underlying graph with $n - |I| > 0$ states outside minimal strongly connected ideal $I$.

This ideal has synchronizing word of length at most $(|I| - 1)^2$ (Theorem 1). There is a word $p$ of length at most $(n - |I|)(n - |I| + 1)/2$ such that $Ap \subset I$.

$(|I| - 1)^2 + (n - |I|)(n - |I| + 1)/2 < (n - 1)^2$. Thus the restriction for strongly connected automata can be omitted.

6 Examples

J. Kari [16] discovered the following example of $n$-state automaton with minimal synchronizing word of length $(n - 1)^2$ for $n = 6$.

```
| 1 | 2 | 0 |
|---|---|---|
| b | a | a |
| b | b | 2 |
| b | a | b |
```

The minimal synchronizing word $s = ba^2 bababa^2 b^2 aba^2 ba^2 baba^2 b$ has the length at the Černy border.

Every line below presents a pair (word $u$, $n$-vector $c_u$) of linear independent matrices $L_u$ from the sequence.

- $(b, 111110)$ $R(u) = 5$
- $(ba, 111011)$
- $(ba^2, 111010)$
- $(ba^2b, 111000)$ $R(u) = 4$
- $(ba^2ba, 111010)$
- $(ba^2bab, 011110)$
- $(ba^2baba, 101111)$ $R(v) = 5$ (101011 of $L_u$)
- $(ba^2babab, 101110)$ $R(u) = 4$
(ba^2 bababa, 110101)
(ba^2 bababa^2, 011101)
(ba^2 bababa^2 b, 111000) R(u) = 3
(ba^2 bababa^2 b^2, 011100)
(ba^2 bababa^2 b^2 a, 110111) R(v) = 5 (101010 of L_u)
(ba^2 bababa^2 b^2 ab, 001110) R(u) = 3
(ba^2 bababa^2 b^2 aba, 100011)
(ba^2 bababa^2 b^2 aba^2, 011111) R(v) = 5 (010101 of L_u)
(ba^2 bababa^2 b^2 aba^2 b, 110000) R(u) = 2
(ba^2 bababa^2 b^2 aba^2 ba, 011000)
(ba^2 bababa^2 b^2 aba^2 ba^2, 101000)
(ba^2 bababa^2 b^2 aba^2 ba^2 b, 001101) R(v) = 3 (001100 of L_u)
(ba^2 bababa^2 b^2 aba^2 ba^2 ba, 100110) R(u) = 2
(ba^2 bababa^2 b^2 aba^2 ba^2 bab, 000110)
(ba^2 bababa^2 b^2 aba^2 ba^2 bab^2, 001011) R(v) = 3 (000011 of L_u)
(ba^2 bababa^2 b^2 aba^2 ba^2 bab^2, 000101) R(u) = 2
(ba^2 bababa^2 b^2 aba^2 ba^2 bab^2 b = s, 100000) R(s) = 1

By the bye, the matrices of right subwords of s are simply linear independent.

For the Černy sequence of n-state automata [7], [22], [23] 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 baabaabaab with pairs of word u and n-vector c_u of linear independent matrices L_u below.

(b, 0111) R(u) = 3
(ba, 1011)
(baa, 1101)
(baaa, 1110)
(baaba, 1010) R(u) = 2
(baaaba, 0011)
In the example of Roman \[28\]

the minimal synchronizing word
\[s = ab(ca)^2 c bca^2 c abca\]

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

\[
\begin{align*}
(a, 10111) & \quad R(u) = 4 \\
(ab, 11011) & \\
(abc, 11110) & \\
(abca, 10110) & \quad R(u) = 3 \\
(abca, 10011) & \\
(abca, 01111) & \quad R(v) = 4 \ (00111 \text{ of } L_u) \\
(abca, 10101) & \quad R(u) = 3 \\
(abca, 1001) & \\
(abca, 01101) & \\
(abca, 10010) & \quad R(u) = 2 \\
(abca^2, 00110) & \\
(abca^2 c, 10001) & \\
(abca^2 c a^2, 11011) & \quad R(v) = 4 \ (00101 \text{ of } L_u) \\
(abca^2 c ab, 01001) & \quad R(u) = 2 \\
(abca^2 c abc, 01100) & \\
(abca^2 c abc = s, 10000) & \quad R(s) = 1
\end{align*}
\]

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.

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, Lect. Notes in Comp. Sci., 6281(2010), 55-65.
3. M.-P. Béal, A note on Černy Conjecture and rational series, technical report, Inst. Gaspar Monge, Univ. de Marne-la-Vallee, 2003.
4. 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.
5. J. Berstel, C. Reutenauer, Rational series and their languages, Springer, 1988.
6. A. Carpi, F. D’Alessandro, Strongly transitive automata and the Černý conjecture. Acta Informatica, 46(2009), 591-607.
7. J. Černý, Poznamka k homogeným eksperimentom s konečnými automatami, Math.-Fyz. Čas., 14(1964), 208-215.
8. A. Carpi, F. D’Alessandro, On the Hybrid Černý-Road coloring problem and Hamiltonian paths. LNCS, 6224(2010), 124-135.
9. K. Chmieleń, A. Roman. COMPAS - A Computing Package for Synchronization. LNCS, Impl. and Appl. of Automata, 6482(2011), 79-86, 2011.
10. J. Černý, A. Piricka, B. Rosenaurova. On directable automata, Kybernetika 7(1971), 289-298.
11. H. Don, H. Zantema, Finding DFAs with maximal shortest synchronizing word length. arXiv:1609.06853, 2016.
12. P. Frankl, An extremal problem for two families of sets, Eur. J. Comb., 3(1982), 125-127.
13. J. Friedman. On the road coloring problem, Proc. of the Amer. Math. Soc. 110(1990), 1133-1135.
14. F. Gonze, R. M. Jungerman, A.N. Trahtman. A Note on a Recent Attempt to Improve the Pin-Frankl Bound. DM & TCS, 1(17), 2015, 307-308.
15. H. Jurgensen, Synchronization. Inf. and Comp. 206(2008), 9-10, 1033-1044.
16. J. Kari, A counter example to a conjecture concerning synchronizing word in finite automata, EATCS Bulletin, 73(2001), 146-147.
17. J. Kari, Synchronizing finite automata on Eulerian digraphs. Springer, LNCS, 2136(2001), 432-438.
18. J. Kari, M. V. Volkov, Černý’s conjecture and the road coloring problem. Handbook of Automata, 2013.
19. A. Kisielewicz, J. Kowalski, M. Szykula. Computing the shortest reset words of synchronizing automata, J. Comb. Optim., Springer, 29(2015), 88-124.
20. 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.
21. P. Lankaster, Theory of matrices, Acad. Press, 1969.
22. 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.
23. 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.
24. A. I. Malcev, Foundations of linear algebra, San Francisco, Freeman, 1963. (Nauka, 1970, in Russian.)
25. A. Mateescu and A. Salomaa, Many-Valued Truth Functions, Černý’s conjecture and road coloring, Bulletin EATCS, 68 (1999), 134-148.
26. D. Perrin, M.-P. Schützenberger. Synchronizing prefix codes and automata and the road coloring problem. Symbolic dynamics and its applications , 135 (1992), 295-318.
27. J.-E. Pin, On two combinatorial problems arising from automata theory, Annals of Discrete Math., 17(1983), 535-548.
28. A. Roman, Experiments on Synchronizing Automata. Schedae Informaticae, 19(2010), 35-51.
29. P. H. Starke. Eine Bemerkung ueber homogene Experimente. Elektronische Informationverarbeitung und Kybernetik, 2(1966), 257-259.
30. B. Steinberg, The Averaging Trick and the Cerny Conjecture. Developments in Language Theory, Springer, NY, LNCS, 6224(2010), 423-431.
31. M. Szykula. Improving the Upper Bound on the Length of the Shortest Reset Words. STACS 2018 v. 96, 56:1–56:13.
32. A.N. Trahtman. Notable trends concerning the synchronization of graphs and automata, CTW06, El. Notes in Discrete Math., 25(2006), 173-175.
33. A.N. Trahtman. The Cerny Conjecture for Aperiodic Automata. Discr. Math. Theoret. Comput. Sci. v. 9, 2(2007), 3-10.
34. A.N. Trahtman. The Road Coloring and Cerny Conjecture. Proc. of Prague Stringology Conference, 2008, 1-12.
35. A.N. Trahtman. Modifying the upper bound on the length of minimal synchronizing word. LNCS, 6914(2011), 173-180, arXiv:1104.2409.
36. A.N. Trahtman. Bibliography, http://u.cs.biu.ac.il/~trakht/syn.html
37. A.N. Trahtman. Synchronization, http://u.cs.biu.ac.il/~trakht/readme.html
38. 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.
39. M. V. Volkov, Lecture Notes on Synchronizing Automata, M, V. Volkov, 2016 [http://csseminar.kadm.usu.ru/Hunter/lectures.pdf]