Discrete Mathematics and Theoretical Computer Science DMTCS vol. **9:2**, 2007, 3–10

The Černý Conjecture for Aperiodic Automata

A. N. Trahtman†

Bar-Ilan University, Department of Mathematics
52900, Ramat Gan, Israel

received 6 Jan 2005, *revised 23 Apr 2005*, *accepted 23 May 2005*.

A word w is called a *synchronizing* (*recurrent, reset, directable*) word of a deterministic finite automaton (DFA) if w brings all states of the automaton to some specific state; a DFA that has a synchronizing word is said to be *synchronizable.* Černý conjectured in 1964 that every n-state synchronizable DFA possesses a synchronizing word of length at most $(n-1)^2$. We consider automata with aperiodic transition monoid (such automata are called *aperiodic*). We show that every synchronizable n-state aperiodic DFA has a synchronizing word of length at most $n(n-1)/2$. Thus, for aperiodic automata as well as for automata accepting only star-free languages, the Černý conjecture holds true.

Keywords: deterministic finite automaton, synchronizing word, star-free language

Introduction

The problem of synchronization of DFA is natural and various aspects of this problem were touched upon the literature. We pay attention to the problem of the existence and of the length of a synchronizing word.

An important problem with a long story is estimating the shortest length of a synchronizing word. Best known as the Černý conjecture, it was proposed independently by several authors. Černý found in 1964 [2] an n-state DFA whose shortest synchronizing word was of length $(n-1)^2$. He conjectured that this is the maximum length of the shortest synchronizing word for any DFA with n states. The conjecture has been verified for several partial cases [1, 3, 4, 6, 10, 8] but in general the question still remains open. By now, this simply looking conjecture is arguably one of the most longstanding open problems in the theory of finite automata. The best upper bound for the length of the shortest synchronizing word for DFA with n states known so far is equal to $(n^3-n)/6$ [5, 7, 9]. For the rich and intriguing story of investigations in this area see [12].

The existence of some non-trivial subgroup in the transition semigroup of the automaton is essential in many investigations of the Černý conjecture, see, e.g., [3, 8]. We use another approach and consider transition semigroups without non-trivial subgroups. This condition distinguishes

†Email: trakht@macs.biu.ac.il

a wide class of so-called aperiodic automata that, as shown by Schützenberger [13], accept precisely star-free languages (also known as languages of star height 0). Star-free languages play a significant role in formal language theory.

We prove that every n-state aperiodic DFA with a state that is accessible from every state of the automaton has a synchronizing word of length not greater than $n(n-1)/2$, and therefore, for aperiodic automata as well as for automata accepting only star-free languages, the Černý conjecture holds true.

In the case when the underlying graph of the aperiodic DFA is strongly connected, this upper bound has been recently improved by Volkov who has reduced the estimation to $n(n+1)/6$.

1 Preliminaries

We consider a complete DFA $\mathcal{A}$ with the input alphabet Σ. The transition graph of $\mathcal{A}$ is denoted by Γ and the transition semigroup of $\mathcal{A}$ is denoted by S.

Let $\mathbf{p}$ and $\mathbf{q}$ be two (not necessarily distinct) states of the automaton $\mathcal{A}$. If there exists a path in $\mathcal{A}$ from the state $\mathbf{p}$ to the state $\mathbf{q}$ and the transitions of the path are consecutively labelled by $\sigma_1, \dots, \sigma_k \in \Sigma$ then for $s = \sigma_1 \dots \sigma_k$ we write $\mathbf{q} = \mathbf{p}s$. We call a state $\mathbf{q}$ a *sink* if for every state $\mathbf{p}$ of $\mathcal{A}$ there exists a word s such that $\mathbf{p}s = \mathbf{q}$. For a set P of states and $s \in \Sigma^*$, let Ps denote the set $\{\mathbf{p}s \mid \mathbf{p} \in P\}$. A word $s \in \Sigma^+$ is called a *synchronizing word for* P if $|Ps| = 1$, that is, $\mathbf{p}s = \mathbf{q}s$ for all states $\mathbf{p}, \mathbf{q} \in P$. A word is said to be a *synchronizing word of the automaton* $\mathcal{A}$ (*of the graph* Γ) if it is synchronizing for the set of all states of $\mathcal{A}$ (the set of all vertices of Γ).

A binary relation β on the state set of $\mathcal{A}$ is called *stable* if, for any pair of states $\mathbf{q}, \mathbf{p}$ and any $\sigma \in \Sigma$, from $\mathbf{q}\,\beta\,\mathbf{p}$ it follows $\mathbf{q}\sigma\,\beta\,\mathbf{p}\sigma$. Recall that a stable equivalence relation on the state set of $\mathcal{A}$ is called a *congruence* of $\mathcal{A}$. If ρ is a congruence of $\mathcal{A}$, we denote by $[\mathbf{q}]_\rho$ the ρ-class containing the state $\mathbf{q}$. The *quotient* $\mathcal{A}/\rho$ is the automaton with the states $[\mathbf{q}]_\rho$ and the transition function defined by the rule $[\mathbf{q}]_\rho\sigma = [\mathbf{q}\sigma]_\rho$ for any $\sigma \in \Sigma$.

For a word s over the alphabet Σ, we denote its length by $|s|$.

2 The graph Γ^2

The direct square Γ^2 of the transition graph Γ has as vertices all pairs $(\mathbf{p}, \mathbf{q})$, where $\mathbf{p}, \mathbf{q}$ are vertices of Γ. The edges of the graph Γ^2 have the form $(\mathbf{p}, \mathbf{q}) \to (\mathbf{p}\sigma, \mathbf{q}\sigma)$ where $\sigma \in \Sigma$; such an edge is labelled by σ.

For brevity, a strongly connected component of a directed graph is referred to as an **SCC**. An **SCC** M of the graph Γ^2 is called *almost minimal* if, for every pair $(\mathbf{p}, \mathbf{q}) \in M$, one has $\mathbf{p} \neq \mathbf{q}$ and, for every $\sigma \in \Sigma$ such that $\mathbf{p}\sigma \neq \mathbf{q}\sigma$, there exists a word $s \in \Sigma^*$ such that $(\mathbf{p}\sigma, \mathbf{q}\sigma)s = (\mathbf{p}, \mathbf{q})$. We observe that then $(\mathbf{p}\sigma, \mathbf{q}\sigma) \in M$ by the definition of an **SCC**. By $\Gamma(M)$ we denote the set of states that appear as components in the pairs from the almost minimal **SCC** M.

If M is an almost minimal **SCC**, we define the relation $\succ_M$ as the transitive closure of M (where M is treated as a relation on the state set of our automaton). So $\mathbf{r} \succ_M \mathbf{q}$ if there exists a sequence of states $\mathbf{r} = \mathbf{p}_1, \dots, \mathbf{p}_n = \mathbf{q}$ such that $n > 1$ and $(\mathbf{p}_i, \mathbf{p}_{i+1}) \in M$ for all $i = 1, \dots, n-1$. Let $\succeq_M$ be the reflexive closure and ρ_M the equivalent closure of the relation $\succ_M$.

Lemma 1 *For any almost minimal **SCC** M, the relation $\succeq_M$ is stable and the relation ρ_M is a congruence.*

Proof: Suppose $\mathbf{u}\,\rho_M\,\mathbf{v}$. Then there exists a sequence of states

$$\mathbf{u} = \mathbf{p}_1, \ldots, \mathbf{p}_n = \mathbf{v} \tag{1}$$

such that for every integer $i < n$ at least one of the pairs $(\mathbf{p}_{i+1}, \mathbf{p}_i)$, $(\mathbf{p}_i, \mathbf{p}_{i+1})$ belongs to the almost minimal **SCC** M. Therefore in the sequence of states $\mathbf{r}s = \mathbf{p}_1 s, \ldots, \mathbf{p}_n s = \mathbf{q}s$, for any two distinct neighbors $\mathbf{p}_i s, \mathbf{p}_{i+1} s$, the pair $(\mathbf{p}_i s, \mathbf{p}_{i+1} s)$ or its dual belongs to M. Hence $\mathbf{r}s\ \rho_M\ \mathbf{q}s$.

If $\mathbf{u} \succeq_M \mathbf{v}$, then there exists a sequence (1) such that for every integer $i < n$ the pair $(\mathbf{p}_i, \mathbf{p}_{i+1})$ belongs to M. Then either $(\mathbf{p}_i s, \mathbf{p}_{i+1} s) \in M$ or $\mathbf{p}_i s = \mathbf{p}_{i+1} s$, and therefore, $\mathbf{p}_i s \succeq_M \mathbf{p}_{i+1} s$ in any case. Hence $\mathbf{u}s \succeq_M \mathbf{v}s$. □

From the definition of the relation $\succ_M$ and Lemma 1, we obtain

Corollary 2 *If $\mathbf{r} \succ_M \mathbf{q}$ and $\mathbf{r}s \notin \Gamma(M)$ for some word s, then $\mathbf{r}s = \mathbf{q}s$.*

We also observe the following obvious property:

Corollary 3 *Each state $\mathbf{p}$ from $\Gamma(M)$ belongs to a ρ_M-class of size at least two.*

Let us present the following new formulation of a result from [2]:

Lemma 4 *An automaton $\mathcal{A}$ with the transition graph Γ is synchronizing if and only if the graph Γ^2 has a sink.*

Proof: Let s be a synchronizing word of $\mathcal{A}$. Then the unique pair of the set $\Gamma^2 s$ is a sink of Γ^2. Conversely, the components of a sink of Γ^2 obviously are equal. Let $(\mathbf{t}, \mathbf{t})$ be a sink. For any pair $(\mathbf{p}, \mathbf{q})$, there exists a word s such that $(\mathbf{p}, \mathbf{q})s = (\mathbf{t}, \mathbf{t})$, that is, $\mathbf{p}s = \mathbf{q}s = \mathbf{t}$. Some product of such words s taken for all pairs of distinct states from Γ is a synchronizing word of the graph Γ. □

Lemma 5 *The sets of synchronizing words of the graphs Γ and Γ^2 coincide.*

Proof: Let s be a synchronizing word of the graph Γ. Then there is a state $\mathbf{q}$ from Γ such that $\mathbf{p}s = \mathbf{q}$ for every state $\mathbf{p}$. Therefore for every pair $(\mathbf{p}, \mathbf{r})$ one has $(\mathbf{p}, \mathbf{r})s = (\mathbf{q}, \mathbf{q})$. Thus, s is a synchronizing word of the graph Γ^2.

Now let t be a synchronizing word of the graph Γ^2. Then there is a pair $(\mathbf{q}, \mathbf{v})$ such that $(\mathbf{p}, \mathbf{r})t = (\mathbf{q}, \mathbf{v})$ for every pair $(\mathbf{p}, \mathbf{r})$. Therefore $\mathbf{p}t = \mathbf{q}$ for an arbitrary state $\mathbf{p}$ from Γ and $\mathbf{r}t = \mathbf{v}$ for an arbitrary state $\mathbf{r}$ from Γ. Consequently, $\mathbf{v} = \mathbf{q}$ and t is a synchronizing word of the graph Γ. □

3 Aperiodic automata

A semigroup without non-trivial subgroups is called *aperiodic*. A DFA with aperiodic transition semigroup is called *aperiodic* too.

Let us recall that the syntactic semigroup of a star-free language is finite and aperiodic [13] and the semigroup satisfies the identity $x^n = x^{n+1}$ for some suitable n. Therefore, for any state $\mathbf{p} \in \Gamma$, any $s \in S$ and for some suitable k, one has $\mathbf{p}s^k = \mathbf{p}s^{k+1}$.

Lemma 6 *Let $\mathcal{A}$ be an aperiodic DFA. Then the existence of a sink in $\mathcal{A}$ is equivalent to the existence of a synchronizing word.*

Proof: It is clear that, for any DFA, the existence of a synchronizing word implies the existence of a sink.

Now suppose that $\mathcal{A}$ has at least one sink. For any state $\mathbf{p}$ and any sink $\mathbf{p_0}$, there exists an element s from the transition semigroup S such that $\mathbf{p}s = \mathbf{p_0}$. The semigroup S is aperiodic, whence for some positive integer m we have $s^m = s^{m+1}$. Therefore $\mathbf{p}s^m = \mathbf{p}s^{m+1} = \mathbf{p_0}s^m$, whence the element s^m brings both $\mathbf{p}$ and $\mathbf{p_0}$ to the same state $\mathbf{p_0}s^m$ which is a sink again. We repeat the process reducing the number of states on each step. Then some product of all elements of the form s^m arising on each step brings all states of the automaton to some sink. Thus, we obtain in this way a synchronizing word. $\square$

Let M be an almost minimal **SCC**. A *t-cycle* for M is a sequence of states

$$\mathbf{p}_1, \mathbf{p}_2, \ldots, \mathbf{p}_{m-1}, \mathbf{p}_m = \mathbf{p}_1 \tag{2}$$

such that $n > 1$ and $(\mathbf{p}_i, \mathbf{p}_{i+1}) \in M$ for all $i = 1, \ldots, m-1$. The next observation is the key ingredient of the proof.

Lemma 7 *Let $\mathcal{A}$ be an aperiodic DFA and let M be an almost minimal **SCC**. Then there is no t-cycle for M and the quasi-order $\succeq_M$ is a partial order.*

Proof: Suppose that (2) is a t-cycle of minimum size m among all t-cycles for the almost minimal **SCC** M. Let us first establish that $m > 2$. Indeed, $\mathbf{p}_1 \neq \mathbf{p}_2$, whence $m > 1$. If $m = 2$ then the two pairs $(\mathbf{p}_1, \mathbf{p}_2)$ and $(\mathbf{p}_2, \mathbf{p}_1)$ belong to the **SCC** M. For some element u from the transition semigroup S, we have $(\mathbf{p}_1, \mathbf{p}_2)u = (\mathbf{p}_2, \mathbf{p}_1)$. Therefore $\mathbf{p}_1 u = \mathbf{p}_2$, $\mathbf{p}_2 u = \mathbf{p}_1$, whence $\mathbf{p}_1 u^2 = \mathbf{p}_1 \neq \mathbf{p}_1 u$. This implies $\mathbf{p}_1 u^{2k} = \mathbf{p}_1 \neq \mathbf{p}_1 u = \mathbf{p}_1 u^{2k+1}$ for any integer k. However, semigroup S is finite and aperiodic, and therefore, for some k we have $u^{2k} = u^{2k+1}$, whence $\mathbf{p}_1 u^{2k} = \mathbf{p}_1 u^{2k+1}$, a contradiction.

Thus, we can assume that $m > 2$ and suppose that the states $\mathbf{p}_1, \mathbf{p}_2, \mathbf{p}_3$ are distinct. For some element $s \in S$, we have $(\mathbf{p}_1, \mathbf{p}_2)s = (\mathbf{p}_2, \mathbf{p}_3)$. Hence

$$\mathbf{p}_2 = \mathbf{p}_1 s, \ \ \mathbf{p}_3 = \mathbf{p}_1 s^2.$$

For any element $u \in S$ and any pair $(\mathbf{p}_i, \mathbf{p}_{i+1})$ from M, we have either $\mathbf{p}_i u = \mathbf{p}_{i+1} u$ or $(\mathbf{p}_i u, \mathbf{p}_{i+1} u) \in M$. Therefore, for any element $u \in S$, the sequence of states $\mathbf{p}_1 u, \ldots, \mathbf{p}_m u$ either reduces to just one element repeated m times or forms a t-cycle of size m (because of the minimality of m).

The states $\mathbf{p}_1, \mathbf{p}_1 s, \mathbf{p}_1 s^2$ are distinct. Since S is an aperiodic finite semigroup, there exists some integer ℓ such that $s^\ell \neq s^{\ell+1} = s^{\ell+2}$. Therefore there exists an $k \leq \ell$ such that $\mathbf{p}_1 s^k \neq \mathbf{p}_1 s^{k+1} = \mathbf{p}_1 s^{k+2}$ the sequence $\mathbf{p}_1 s^k$, $\mathbf{p}_2 s^k = \mathbf{p}_1 s^{k+1}$, $\mathbf{p}_3 s^k = \mathbf{p}_1 s^{k+2}$,..., $\mathbf{p}_m s^k$ has more than 1 but less than m distinct elements. This contradicts the conclusion of the previous paragraph applied to the element $u = s^k$.

It is easy to see that if the quasi-order $\succeq_M$ is not antisymmetric that there exists a t-cycle for M. Hence $\succeq_M$ is a partial order. $\square$

4 The Černý conjecture

Lemma 8 *Let $\mathcal{A}$ be an aperiodic DFA with n states and strongly connected graph, M an almost minimal **SCC**. Let r be the number of ρ_M-classes and let R be a ρ_M-class. Then $|Rs| = 1$ for some word $s \in \Sigma^*$ of length ar most $(n-r+1)(n-1)/2$.*

Proof: Suppose $|R| > 1$. Let Max be the set of all maximal and Min the set of all minimal states from R with respect to the order $\succ_M$. Observe that there is no ambiguity here: since the order $\succ_M$ is contained in the congruence ρ_M, maximal (minimal) states of the ordered set $(R, \succ_M)$ are precisely those maximal (minimal) states of the automaton $\mathcal{A}$ that belong to R. Further, $Max \cap Min = \emptyset$ because the congruence ρ_M is the equivalent closure of the order $\succ_M$ whence for every state $\mathbf{q} \in R$ there must be a state $\mathbf{p} \in R$ such that either $\mathbf{q} \succ_M \mathbf{p}$ or $\mathbf{p} \succ_M \mathbf{q}$. Without loss of generality, we may assume that $|Max| \geq |Min|$. Then $|Min| \leq |R|/2 \leq (n-r+1)/2$.

We need three properties of ordered sets of the form $(Rs, \succ_M)$ where s is a word. Let Max_s (Min_s) stand for the set of all maximal (respectively all minimal) states in $(Rs, \succ_M)$.

Claim 1. If $|Rs| > 1$, then $Min_s \cap Max_s = \emptyset$.

Proof: Take an arbitrary state $\mathbf{p}' \in Min_s$ and let $\mathbf{q}'$ be any state in $Rs \setminus \{\mathbf{p}'\}$. Consider some preimages $\mathbf{p}, \mathbf{q} \in R$ of $\mathbf{p}'$ and respectively $\mathbf{q}'$. Since R is a ρ_M-class, there is a sequence of states $\mathbf{q}_0, \mathbf{q}_1, \ldots, \mathbf{q}_k \in R$ such that $\mathbf{p} = \mathbf{q}_0$, $\mathbf{q}_k = \mathbf{q}$, and for each $i = 1, \ldots, k$ either $\mathbf{q}_{i-1} \succeq_M \mathbf{q}_i$ or $\mathbf{q}_i \succeq_M \mathbf{q}_{i-1}$. Let ${\mathbf{q}'}_i = \mathbf{q}_i s \in Rs$, $i = 0, \ldots, k$. Since the order $\succeq_M$ is stable (Lemma 1), we conclude that there is a sequence of states ${\mathbf{q}'}_0, {\mathbf{q}'}_1, \ldots, {\mathbf{q}'}_k \in Rs$ such that $\mathbf{p}' = {\mathbf{q}'}_0$, ${\mathbf{q}'}_k = \mathbf{q}'$, and for each $i = 1, \ldots, k$ either ${\mathbf{q}'}_{i-1} \succeq_M {\mathbf{q}'}_i$ or ${\mathbf{q}'}_i \succeq_M {\mathbf{q}'}_{i-1}$. Since $\mathbf{p}' \neq \mathbf{q}'$, some of these inequalities must be strict. Let j be the least index such that ${\mathbf{q}'}_{j-1} \neq {\mathbf{q}'}_j$. Then $\mathbf{p}' = {\mathbf{q}'}_0 = \ldots = {\mathbf{q}'}_{j-1}$ whence either $\mathbf{p}' \succ_M {\mathbf{q}'}_j$ or ${\mathbf{q}'}_j \succ_M \mathbf{p}'$. As the first inequality would contradict the assumption that $\mathbf{p}'$ is a minimal element of $(Rs, \succ_M)$, we conclude that the second inequality holds true whence $\mathbf{p}'$ is not a maximal element of $(Rs, \succ_M)$. Thus, no state in Min_s can belong to Max_s. $\square$

Claim 2. If $s, t \in \Sigma^*$ are two arbitrary words, then $Min_{ts} \subseteq Min_t\, s$.

Proof: Take an arbitrary state $\mathbf{p}' \in Min_{ts}$ and consider its arbitrary preimage $\mathbf{p} \in Rt$. There exists a state $\mathbf{q} \in Min_t$ such that $\mathbf{p} \succeq_M \mathbf{q}$. Since the order $\succeq_M$ is stable (Lemma 1), we then have $\mathbf{p}' = \mathbf{p}\, s \succeq_M \mathbf{q}\, s = \mathbf{q}'$. The state $\mathbf{q}'$ belongs to the set Rts, and therefore, $\mathbf{q}' = \mathbf{p}'$ because $\mathbf{p}'$ has been chosen to be a minimal element in this set. Thus, we have found a preimage for $\mathbf{p}'$ in Min_t whence $Min_{ts} \subseteq Min_t\, s$. $\square$

Claim 3. For any word $t \in \Sigma^*$, there exists a word $s \in \Sigma^*$ of length at most $n-1$ such that either $|Rst| = 1$ or $|Min_{ts}| < |Min_t|$.

Proof: Now take arbitrary state $\mathbf{q} \in Min_t$. Since the graph Γ is strongly connected, there exists a word that maps $\mathbf{q}$ to an element of Max. If s is a word of minimum length with this property then the path labelled s does not visit any state of $\mathcal{A}$ twice whence $|s| \leq n-1$. Observe that since $\mathbf{q}s \in Max$, we also have $\mathbf{q}s \in Max_{ts}$. Therefore either $|Rst| = 1$ or, by Claim 1 above, $\mathbf{q}s \notin Min_{ts}$. Since $\mathbf{q}s \in Min_t\, s$, we conclude from Claim 2 that $Min_{ts} \subset Min_t\, s$. Thus, $|Min_{ts}| < |Min_t\, s| \leq |Min_t|$. $\square$

Using Claim 3, we can easily complete the proof of the lemma. Indeed, applying it to the case when t is the empty word, we can find a word s_1 of length at most $n-1$ such that either $|Rs_1| = 1$ or $|Min_{s_1}| < |Min|$. In the latter case, applying Claim 3 again, we can find a word s_2 of length at most $n-1$ such that either $|Rs_1s_2| = 1$ or $|Min_{s_1s_2}| < |Min_{s_1}|$, and so on. Clearly, the process will stop after at most $|Min|$ steps yielding a word $s = s_1s_2\cdots s_k$ (with $k \leq |Min|$ and $|s_i| \leq n-1$ for each $i = 1, \dots, k$) such that $|Rs| = 1$. Since $|Min| \leq (n-r+1)/2$, we have $|s| \leq (n-r+1)(n-1)/2$ as required. □

Theorem 9 *If the transition graph Γ of an aperiodic DFA $\mathcal{A}$ with n states is strongly connected, then $\mathcal{A}$ has a synchronizing word of length at most $(n-1)n/2$.*

Proof: All states of a DFA whose transition graph is strongly connected are sinks. Therefore the automaton is synchronizable (Lemma 6).

There exists at least one almost minimal **SCC** M in Γ^2 because the number of **SCC**'s is finite and the set of **SCC**'s is partially ordered under the attainability relation. Consider the congruence ρ_M (Lemma 1) and the quotient Γ/ρ_M.

It is clear that any synchronizing word of Γ synchronizes also Γ/ρ_M and that Γ/ρ_M is aperiodic and strongly connected. Therefore the graph Γ has a synchronizing word uv where u is a synchronizing word of Γ/ρ_M and v is a synchronizing word of the preimage R of the singleton set $(\Gamma/\rho_M)\,u$. By Corollary 3, ρ_M is not trivial, therefore $r = |\Gamma/\rho_M| < n$ and we can use induction assuming $|u| \leq (r-1)r/2$. By Lemma 8, a word v of length at most $(n-r+1)(n-1)/2$ synchronizes R. Therefore $|uv| \leq \frac{r(r-1)}{2} + \frac{(n-r+1)(n-1)}{2} \leq \frac{(r-1)(n-1)}{2} + \frac{(n-r+1)(n-1)}{2} \leq \frac{n(n-1)}{2}$ as required. □

Let us go to the general case.

Theorem 10 *Let $\mathcal{A}$ be an aperiodic DFA with n states. Then the existence of a sink in $\mathcal{A}$ is equivalent to the existence of a synchronizing word of length at most $n(n-1)/2$.*

Proof: It is clear that the existence of a synchronizing word implies the existence of a sink.

For the converse, let us consider a DFA with at least one sink. By Lemma 6, the automaton is synchronizable. We may assume in view of Theorem 9 that the transition graph Γ of $\mathcal{A}$ is not strongly connected.

It is clear that the collection C of all sinks of Γ forms a **SCC** of Γ which is the least **SCC** with respect to the attainability order. Let $r < n$ stand for the cardinality of C. Let Γ_i $(i = 1, 2, \dots, k)$ be all other **SCC**'s of Γ. We may assume that Γ_i are numbered so that $i \leq j$ whenever there is a path in Γ from Γ_i to Γ_j. Let r_i be the cardinality of Γ_i. It easily follows from [11, Theorem 6.1] that there exists a word s_i of length at most $r_i(r_i+1)/2$ such that $\Gamma_i s_i \cap \Gamma_i$ is empty. Then the product $s_1 \cdots s_k$ of maps Γ into the **SCC** C. By Theorem 9, C has a synchronizing word s of length at most $r(r-1)/2$. Therefore the word $s_1 \cdots s_k s$ synchronizes Γ and

$$|s_1 \dots s_k s| \leq \sum_{i=1}^{k} \frac{r_i(r_i+1)}{2} + \frac{r(r-1)}{2}. \tag{3}$$

Using the equality $\sum_{i=1}^{k} r_i + r = n$, it is easy to calculate that the right-hand side of the inequality 3 does not exceed $(n-1)n/2$. □

Corollary 11 *The Černý conjecture holds for aperiodic automata.*

Acknowledgments

I am very grateful to M. V. Volkov for helpful and detailed comments that proved to be highly useful in improving the presentation and style of the paper.

References

[1] D. S. Ananichev, M. V. Volkov, *Some results on Černý type problems for transformation semigroups*, In I. Araujo, M. Branco, V. H. Fernandes, and G. M. S. Gomes (eds.), Semigroups and Languages, World Scientific, Singapore, 2004, 23–42.

[2] J. Černý, Poznamka k homogenym eksperimentom s konechnymi automatami, *Math.-Fyz. Čas.* 14(1964), 208–215.

[3] L. Dubuc, Sur le automates circulaires et la conjecture de Černý, *RAIRO Inform. Theor. Appl.* 32(1998), 21–34.

[4] D. Eppstein, Reset sequences for monotonic automata, *SIAM J. Comput.* 19(1990), 500–510.

[5] P. Frankl, An extremal problem for two families of sets, *Eur. J. Comb.* 3(1982), 125–127.

[6] J. Kari, *Synchronizing finite automata on Eulerian digraphs*, Springer, Lect. Notes in Comp. Sci. 2136(2001), 432–438.

[7] A. A. Kljachko, I. K. Rystsov, M. A. Spivak, An extremal combinatorial problem connected with the bound on the length of a recurrent word in an automata, *Kybernetika* (1987), no.2, 16–25.

[8] J.-E. Pin, *Sur un cas particulier de la conjecture de Černý*, Springer, Lect. Notes Comp. Sci. 62(1978), 345–352.

[9] J.-E. Pin, On two combinatorial problems arising from automata theory, *Ann. Discrete Math.* 17(1983), 535–548.

[10] I. K. Rystsov, Almost optimal bound on recurrent word length for regular automata, *Cybernetics and System Analysis* 31(1995), 669–674.

[11] I. K. Rystsov, Reset words for commutative and solvable automata, *Theoret. Comput. Sci.* 172(1997), 273–279.

[12] A. Salomaa, Generation of constants and synchronization of finite automata, *J. Univers. Comput. Sci.* 8(2002), 332–347.

[13] M. P. Schützenberger, On finite monoids having only trivial subgroups, *Inf. Control* 8(1965) 190–194.