Synchronization of some DFA

A.N. Trahtman*

Bar-Ilan University, Dep. of Math., 52900, Ramat Gan, Israel

Lecture Notes in Computer Science, 4484(2007), 234-243

Abstract. A word w is called synchronizing (recurrent, reset, directable) word of deterministic finite automaton (DFA) if w brings all states of the automaton to an unique state. Černy conjectured in 1964 that every n-state synchronizable automaton possesses a synchronizing word of length at most $(n-1)^2$. The problem is still open.
It will be proved that the minimal length of synchronizing word is not greater than $(n-1)^2/2$ for every n-state ($n > 2$) synchronizable DFA with transition monoid having only trivial subgroups (such automata are called *aperiodic*). This important class of DFA accepting precisely star-free languages was involved and studied by Schŭtzenberger. So for aperiodic automata as well as for automata accepting only star-free languages, the Černý conjecture holds true.
Some properties of an arbitrary synchronizable DFA and its transition semigroup were established.
http://www.cs.biu.ac.il/∼trakht/syn.html

Keywords: deterministic finite automata, synchronization, aperiodic semigroup, Černy conjecture.

Introduction

The natural problem of synchronization of DFA draws quite often the attention and various aspects of this problem were touched upon the literature. The 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.
An important problem with a long story is the estimation of the shortest length of synchronizing word of DFA. Best known as Černy's conjecture, it was raised independently by distinct authors. Jan Černy found in 1964 [1] an n-state automaton with minimal length synchronizing word of $(n-1)^2$. He conjectured that this is the maximum length of the shortest synchronizing word for any DFA with n states. The conjecture is valid for big list of objects, but in general the question still remains open. The best known upper bound is now equal to $(n^3-n)/6$ [3, 5, 7]. By now, this simple looking conjecture with rich and intriguing story of investigations [4, 7, 10, 12] is one of the most longstanding open problems in the

* Email: trakht@macs.biu.ac.il

theory of finite automata.
The existence of some non-trivial subgroup in the transition semigroup of the automaton is essential in many investigations of Černy conjecture [2, 7, 8]. We use an opposite approach and consider transition semigroups without non-trivial subgroups. This condition distinguishes a wide class of so-called aperiodic automata that, as shown by Schützenberger [11], accept precisely star-free languages (also known as languages of star height 0). Star-free languages play a significant role in the formal language theory.
It will be established that the synchronizable DFA has a synchronizing word of length not greater than $(n-1)^2/2$ $(n > 2)$ for automata with transition semigroup having only trivial subgroups (*aperiodic* automata) and therefore the Černy conjecture holds true for such DFA.
The necessary and sufficient conditions of synchronizability of an arbitrary automaton are presented below in the following form:
An automaton with transition graph Γ is synchronizable iff Γ^2 has sink state.
(see also [1] for another wording). In the case of aperiodic automata holds:

An aperiodic automaton with sink state is synchronizable.

Some properties of an arbitrary synchronizable DFA were found by help of some new concepts such as almost minimal SCC, m-cycle and set of 2-reset words.

Preliminaries

We consider a complete DFA $\mathcal{A}$ with the input alphabet Σ, the transition graph Γ and the transition semigroup S. The elements of S let us consider as words over Σ.
A maximal strongly connected component of a directed graph will be denoted for brevity as **SCC**.
If there exists a path from the state $\mathbf{p}$ to $\mathbf{q}$ and the consecutive transitions of the path are labelled by $\sigma_1, ..., \sigma_k$ then for the word $s = \sigma_1 ... \sigma_k$ let us write $\mathbf{q} = \mathbf{p}s$.
The state $\mathbf{q}$ is called *sink* if for every state $\mathbf{p}$ there exists a word s such that $\mathbf{p}s = \mathbf{q}$.
The binary relation β is called *stable* if for any pair of states $\mathbf{q}, \mathbf{p}$ and any $\sigma \in \Sigma$ from $\mathbf{q}\ \beta\ \mathbf{p}$ follows $\mathbf{q}\sigma\ \beta\ \mathbf{p}\sigma$.
The graph Γ is *complete* if for every $\mathbf{p} \in \mathbf{\Gamma}$ and every $\sigma \in \Sigma$ the state $\mathbf{p}\sigma$ exists.
$|s|$ - the length of the word s in alphabet Σ.
$|P|$ - the size of the set of states of the automaton (of vertices of the graph) P.
Let Ps denote the mapping of the graph (of the automaton) P by help of $s \in \Sigma^*$.
The direct product Γ^2 of two copies of the transition graph Γ over an alphabet Σ consists of pairs $(\mathbf{p}, \mathbf{q})$ and edges $(\mathbf{p}, \mathbf{q}) \to (\mathbf{p}\sigma, \mathbf{q}\sigma)$ labelled by σ. Here $\mathbf{p}, \mathbf{q} \in \Gamma$, $\sigma \in \Sigma$.
A word $s \in \Sigma^+$ is called *synchronizing (reset)* word of an automaton with transition graph Γ if $|\Gamma s| = 1$.
A word w is called *2-reset word* of the pair $\mathbf{p}, \mathbf{q}$ if $\mathbf{p}w = \mathbf{q}w$ and let us denote by $Syn(\mathbf{p}, \mathbf{q})$ the set of all such words w.
Let ϕ be homomorphism of the DFA $\mathcal{A}$. Suppose $\mathbf{q}\ \rho\ \mathbf{p}$ iff $\mathbf{q}\phi = \mathbf{p}\phi$ for the states

$\mathbf{q}$ and $\mathbf{p}$ from $\mathcal{A}$. Then the relation ρ is a *congruence* on $\mathcal{A}$. The ρ-class containing the state $\mathbf{q}$ of $\mathcal{A}$ we denote by $\mathbf{q}^\rho$. The *quotient* $\mathcal{A}/\rho$ is the automaton with the set of states $\mathbf{q}^\rho$ and the transition function defined by the rule $\mathbf{q}^\rho\sigma = \mathbf{q}\sigma^\rho$ for any $\sigma \in \Sigma$.
An *SCC* M from Γ^2 will be called *almost minimal* if for every state $(\mathbf{p}, \mathbf{q})$ $\in M$ and for every $\sigma \in \Sigma$ such that $\mathbf{p}\sigma \neq \mathbf{q}\sigma$ there exists a word s such that $(\mathbf{p}\sigma, \mathbf{q}\sigma)s = (\mathbf{p}, \mathbf{q})$. For every $(\mathbf{p}, \mathbf{q}) \in M$ suppose $\mathbf{p}$ and $\mathbf{q} \in \Gamma(M)$.
Let us define a relation $\succ_M$ for almost minimal *SCC* M. Suppose $\mathbf{p} \succ_M \mathbf{q}$ if $(\mathbf{p}, \mathbf{q}) \in M$ and let $\succ_M$ be the transitive closure of this relation. Let $\succeq_M$ be the reflexive closure and ρ_M be equivalent closure of the relation $\succ_M$.
Let M be almost minimal *SCC*. A non-trivial sequence of states $\mathbf{p}_1, \mathbf{p}_2, ...\mathbf{p}_n = \mathbf{p}_1$ such that $(\mathbf{p}_i, \mathbf{p}_{i+1})$ for $i = 1, ..., n-1$ $(n > 1)$ belong to M let as call *t-cycle*. A *t*-cycle of minimal length let as call *m-cycle*.

1 The graph Γ^2

Lemma 1 *The relation $\succeq_M$ for any almost minimal SCC $M \in \Gamma^2$ is stable. The equivalent closure ρ_M of the relation $\succ_M$ is a congruence.*
If R is a class of the relation ρ_M then for any word w the set Rw is a subset of a class of the relation ρ_M.

Proof. In the case $\mathbf{u} \succeq_M \mathbf{v}$ there exist a sequence of states $\mathbf{u} = \mathbf{p}_1, ..., \mathbf{p}_n = \mathbf{v}$ such that for every integer $i < n$ $(\mathbf{p}_i, \mathbf{p}_{i+1})$ belongs to the almost minimal *SCC* M. One has $(\mathbf{p}_i s, \mathbf{p}_{i+1}s) \in M$ or $\mathbf{p}_i s = \mathbf{p}_{i+1}s$ and therefore $\mathbf{p}_i s \succeq_M \mathbf{p}_{i+1}s$. Consequently, $\mathbf{u}s \succeq_M \mathbf{v}s$.
Suppose $\mathbf{u}$ ρ_M $\mathbf{v}$. Then there exist a sequence of states $\mathbf{u} = \mathbf{p}_1, ..., \mathbf{p}_n = \mathbf{v}$ such that for every integer $i < n$ at least one of the states $(\mathbf{p}_{i+1}, \mathbf{p}_i)$, $(\mathbf{p}_i, \mathbf{p}_{i+1})$ belongs to the almost minimal *SCC* M. Therefore in the sequence of states $\mathbf{u}s = \mathbf{p}_1 s, ..., \mathbf{p}_n s = \mathbf{v}s$ for any two distinct neighbors $\mathbf{p}_i s, \mathbf{p}_{i+1}s$ the state $(\mathbf{p}_i s, \mathbf{p}_{i+1}s)$ or its dual belongs to M. Consequently, $\mathbf{u}s$ ρ_M $\mathbf{v}s$. Therefore for a class R of the relation ρ_M and for any word w the set Rw is a subset of some class of the relation ρ_M.

From the definitions of the almost minimal *SCC* and the relation $\succ_M$ follows

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

Proposition 3 *Synchronizing word of Γ synchronizes also Γ/ρ_M for any M.*

Synchronizing word of Γ is 2-reset word for any pair of states and therefore unites every pair of states from different ρ_M-classes in one sink state.

The following lemma can be also reduced from [1]:

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

Proof. Let s be 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 *Let M be almost minimal SCC of Γ^2. Suppose that for some word s the state $\mathbf{q}s$ is either a maximal element of the order $\succ_M$ or $\mathbf{q}s \notin \Gamma(M)$.*
Then for any state $\mathbf{t}$ such that $\mathbf{t} \succeq_M \mathbf{q}$ holds $\mathbf{t}s = \mathbf{q}s$. The word s unites all ancestors of $\mathbf{q}$.

Proof. By Lemma 1, $\mathbf{t}s \succ_M \mathbf{q}s$ or $\mathbf{q}s = \mathbf{t}s$. The case $\mathbf{t}s \succ_M \mathbf{q}s$ is excluded because the state $\mathbf{q}s$ is a maximal state. In the case $\mathbf{q}s \notin \Gamma(M)$ also $\mathbf{t}s = \mathbf{q}s$ by Proposition 2. Thus the word s is a common synchronizing word for set of all states $\mathbf{t}$ such that $\mathbf{t} \succeq_M \mathbf{q}$.

Theorem 1 *Let M be almost minimal SCC of Γ^2 of n-state synchronizable automaton with transition graph Γ over an alphabet Σ and let the relation ρ_M define homomorphic image Γ/ρ_M of size r. Let the word u syncronize the automaton Γ/ρ_M and let the word v syncronize the ρ_M-class containing Γu. Suppose that the length of the word v is not greater [less] than $c(n-r)(n-1)$ where c is some coefficient.*
Then the automaton has synchronizing word in alphabet Σ of length not greater [less] than $c(n-1)^2$.

Proof. For $r = 1$ the statement of the theorem is a tautology, so let us assume $r > 1$. So $|\Gamma(M)| > 1$ and the relation ρ_M is not trivial. Any synchronizing word of Γ synchronizes also the quotient Γ/ρ_M (Proposition 3) of size less than n. The graph Γ has a synchronizing word uv. In view of $r > 1$, we can use induction, assuming $|u| \le c(|\Gamma/\rho_M| - 1)^2 = c(r-1)^2$. So $|uv| \le c(r-1)^2 + c(n-r)(n-1)$ and in view of
$c(r-1)^2 + c(n-r)(n-1) = c((r-1)^2 + (n-1)^2 - (n-1)(r-1)) = c((n-1)^2 - (r-1)(n-r)) < c(n-1)^2$
one has $|uv| < c(n-1)^2$. So the length of uv in the case $r < n$ or $|v| < c(n-r)(n-1)$ is less than $c(n-1)^2$.

Lemma 6 *For any word w, $Syn(\mathbf{p},\mathbf{q}) \subseteq Syn(\mathbf{r},\mathbf{t})$ implies $Syn(\mathbf{p}w,\mathbf{q}w) \subseteq Syn(\mathbf{r}w,\mathbf{t}w)$. The relation $Syn(\mathbf{p},\mathbf{q})$ is a stable binary relation.*

Proof. Suppose word $u \in Syn(\mathbf{p}w,\mathbf{q}w)$. Therefore the word wu synchronizes the pair of states $\mathbf{p},\mathbf{q}$. From $Syn(\mathbf{p},\mathbf{q}) \subseteq Syn(\mathbf{r},\mathbf{t})$ follows that the word wu synchronizes the pair of states $\mathbf{r},\mathbf{t}$ and $\mathbf{r}wu = \mathbf{t}wu$. Thus the word u from $Syn(\mathbf{p}w,\mathbf{q}w)$ synchronizes also the pair $(\mathbf{r}w,\mathbf{t}w)$, whence $Syn(\mathbf{p}w,\mathbf{q}w) \subseteq Syn(\mathbf{r}w,\mathbf{t}w)$.

Lemma 7 *Let R be ρ_M-class and r be the number of ρ_M - classes of almost minimal SCC M of n-state ($n > 2$) automaton with strongly connected graph Γ. Suppose the relation $\succ_M$ is a partial order.*
Then $|Rs| = 1$ for some word $s \in \Sigma^*$ of length not greater than $(n-r)(n-1)/2$.

Proof. The ρ_M-class R is defined by a state from M, therefore $|R| > 1$. Let Max be the set of all maximal and Min be the set of all minimal states from R according to the order $\succ_M$. Both sets Max and Min are not empty in view of $|R| > 1$. $|Max| \cap |Min| = \emptyset$ because the anti-reflexive relation $\succ_M$ is a partial order. Without loss of generality, let us assume that $|Max| \geq |Min|$. Then $|Min| \leq (n-r)/2$.
For any minimal state $\mathbf{q} \in R$ there exists a word w of length not greater than $n-1$ that maps the state $\mathbf{q}$ in Max. By Lemma 5 the word w maps $\mathbf{q}$ in Max together with all its ancestors. The number of minimal states can be reduced to zero by help of at most $|Min|$ words of length $n-1$. The ρ_M-class without minimal elements is one-element, $|Min| \leq (n-r)/2$, whence for some word s of length not greater than $(n-1)(n-r)/2$ holds $|Rs| = 1$.

2 Transition semigroup of automaton

For definitions of *D*- and *H*-class, ideal, left ideal, idempotent and right zero see [6].

Lemma 8 *Let Γ be strongly connected graph of synchronizing automaton with transition semigroup S. Suppose $\Gamma a = \Gamma b$ for reset words a and b.*
Then $a = b$. Any reset word is an idempotent.

Proof. The elements a and b from S induce equal mappings on the set of states of Γ. S can be embedded into the semigroup of all functions on the set of states under composition [6]. Therefore $a = b$ in S. $\Gamma a = \Gamma a^2$, whence $a = a^2$ for any reset word a and the element $a \in S$ is an idempotent.

Lemma 9 *Let Γ be strongly connected graph of synchronizable automaton with transition semigroup S. Suppose eSe is a group for some idempotent e.*
Then every element s from eSe is a reset word and $|\Gamma s| = 1$.

Proof. Suppose two states $\mathbf{p}$ and $\mathbf{q}$ belong to Γs. The automaton is synchronizable, whence there exists a word $t \in S$ such that $\mathbf{p}t = \mathbf{q}t$. The states $\mathbf{p}$ and $\mathbf{q}$ belong to Γs, therefore $\mathbf{p}e = \mathbf{p}$, $\mathbf{q}e = \mathbf{q}$ and $\mathbf{p}et = \mathbf{q}et$. It implies $\mathbf{p}ete = \mathbf{q}ete$. The element ete belongs to the group eSe with unit e and has an inverse in this group. Consequently, $\mathbf{p}e = \mathbf{q}e$. The states $\mathbf{p}$ and $\mathbf{q}$ belong to $\Gamma s = \Gamma se$. So $\mathbf{p}e = \mathbf{p}$, $\mathbf{q}e = \mathbf{q}$, whence $\mathbf{p} = \mathbf{q}$ in spite of our assumption.

Lemma 10 *Let Γ be strongly connected graph of synchronizable n-state automaton with transition semigroup S.*
Then S contains n distinct reset words and they form a D-class D_r of S. D_r is an ideal of S and a subsemigroup of right zeroes, subgroups of D_r are trivial.

Proof. For every state $\mathbf{p}$ from synchronizable automaton with strongly connected transition graph by Lemma 8 there exists at most one reset word s such that $\Gamma s = \mathbf{p}$. Γ is strongly connected, consequently for any state $\mathbf{q}$ there exists a word t such that $\mathbf{p}t = \mathbf{q}$. Then $\Gamma st = \mathbf{q}$ and st is also a reset word. So for any

state there exists its reset word and all these reset words of distinct states are distinct. Thus there are at least n reset words. From $\Gamma s = \mathbf{p}$ follows $\Gamma us = \mathbf{p}$ for every word $u \in S$, whence by Lemma 8 $us = s$, and in particular $ts = s$. Because for every $t \in S$ st is also reset word and $ts = s$ the set of all reset words is an ideal in S.
For two states $\mathbf{p}$ and $\mathbf{q}$ the corresponding reset words are s and st. So the second word belongs to the left ideal generated by the first. The states $\mathbf{p}$ and $\mathbf{q}$ are arbitrary, whence all reset words create the same left ideal and belong to one D-class D_r. All words from D-class D_r are reset words because from $|\Gamma s| = 1$ follows $|\Gamma vsu| = 1$ for any words u and v. Distinct reset words map Γ on distinct states, so in view of Lemma 8 $|D_r| = n$.
Any H-class of D-class D_r is a group with one idempotent [6] and consists of reset words. By lemma 8 any reset word is an idempotent. Therefore any H-class is trivial and in view of Lemma 9 the set of reset words D_r is a semigroup of right zeroes.

Corollary 11 *Let Γ be transition graph of synchronizable n-state automaton with transition semigroup S. Let Γ have sink strongly connected maximal subgraph T of size k.*
Then S contains k distinct reset words and they all are idempotents, form a subsemigroup of right zeroes and an ideal of S. The difference between the minimal lengths of two distinct reset words is less than k.

Proof. Any reset word of Γ is also a reset word of T. Therefore there are only k distinct reset word and by Lemma 10 they are idempotents, form an ideal of S and a subsemigroup of right zeroes.
Any reset word u maps Γ on some state $\mathbf{p}$ of T. Any other reset word v such that $\Gamma v = \mathbf{q}$ can be obtained as a product ut for t such that $\mathbf{p}t = \mathbf{q}$. $|t| < k$, whence $|v| - |u| < k$.

3 The state outside *t*-cycle

Lemma 12 *Let M be almost minimal SCC from Γ^2 having some t-cycle. Then for any state $(\mathbf{q}, \mathbf{p}) \in M$ the states $\mathbf{q}$ and $\mathbf{p}$ are consecutive states of t-cycle and even of m-cycle.*
If the states $\mathbf{r}$, $\mathbf{s}$ of m-cycle are not consecutive then the state $(\mathbf{r}, \mathbf{s})$ of Γ^2 does not belong to M.

Proof. A t-cycle of minimal length exists because Γ^2 is finite. Let the states $\mathbf{q}_1, \mathbf{p}_1$ be consecutive states of m-cycle C of length m from almost minimal SCC M of Γ^2. So $(\mathbf{q}_1, \mathbf{p}_1) \in M$. For any state $(\mathbf{q}, \mathbf{p})$ from strongly connected component M there exists a word w such that $(\mathbf{q}_1, \mathbf{p}_1)w = (\mathbf{q}, \mathbf{p})$. The word w maps m-cycle C on some t-cycle of length j not greater than m. Because $\mathbf{p} \neq \mathbf{q}$ holds $j > 1$. Therefore $j = m$ and the states $\mathbf{q}, \mathbf{p}$ are consecutive states of m-cycle Cw.
If the state $(\mathbf{r}, \mathbf{s}) \in M$ but the states $\mathbf{r}$, $\mathbf{s}$ are not consecutive states of m-cycle from M then M contains a t-cycle with length less the length of m-cycle. Contradiction.

Theorem 2 *Let the transition graph Γ of an n-state ($n > 2$) synchronizable automaton be strongly connected and let M be almost minimal SCC of Γ^2. Suppose some state $\mathbf{p}$ from Γ does not belong to t-cycle of M.*
Then the automaton has reset word of length not greater than $(n-1)^2/2$.

Proof. The ρ_M-class R is defined by a state from M, therefore $|R| > 1$.
Suppose first that $\mathbf{p} \notin \Gamma(M)$. Then there exists a word w of length not greater than $n - |R| \leq n - 2$ that maps some state from R on $\mathbf{p}$. In virtue of Lemma 1 the class Rw is out of $\Gamma(M)$ and therefore the definition of ρ_M - class implies $Rw = \mathbf{p}$. So $|Rw| = 1$ and $|w| \leq n - 2$.
Let the relation ρ_M define homomorphic image Γ/ρ_M of size r. Let the word u synchronize the automaton Γ/ρ_M. One can suppose by induction that $|u| \leq (r-1)^2/2$. The ρ_M-class $R = \Gamma u$ can be mapped on $\mathbf{p}$ by word w. So
$|uw| \leq n - 2 + (r-1)^2/2 = (n-1)^2/2 - (n-1)^2/2 + n - 2 + (r-1)^2/2 = 0.5((n-1)^2 - (n-1)^2 + (r-1)^2 + 2n - 4) = 0.5((n-1)^2 + (r-n)(r+n-2) + 2(n+r-2) - 2r) = 0.5((n-1)^2 + (r-n+2)(r+n-2) - 2r)$.
In view of $r \leq n - 2$ one has $|uw| < ((n-1)^2/2$.
Let us suppose now that any such $\mathbf{p} \in \Gamma(M)$. If there exists t-cycle in M then by Lemma 12 any state from $\Gamma(M)$ belongs to t-cycle. It contradicts to our assumption that $\mathbf{p}$ does not belong to t-cycle. Therefore we can suppose absence of t-cycles in M. The relation $\succ_M$ is a partial order in such case.
Γ is strongly connected, therefore all its states belong to $\Gamma(M)$. Hence $r = |\Gamma/\rho_M|$ is the number of ρ_M - classes from M. By Lemma 7 any ρ_M - class can be synchronized by a word w of length $(n-r)(n-1)/2$ or less. By induction, Γ/ρ_M can be synchronized by a word u of length $(r-1)^2/2$. So for synchronizing word uw holds
$|uw| \leq (r-1)^2/2 + (n-r)(n-1)/2 = 0.5((n-1)^2 - (n-1)^2 + (r-1)^2 + (n-r)(n-1)) = 0.5((n-1)^2 + (r-n)(r+n-2) - (r-n)(n-1)) = 0.5((n-1)^2 + (r-n)(r-1)) \leq (n-1)^2/2$
So in any case there exists a synchronizing word of length not greater than $(n-1)^2/2$.

4 Aperiodic strongly connected DFA

Let us recall that the transition semigroup S of aperiodic automaton is finite and aperiodic [11] and the semigroup satisfies identity $x^n = x^{n+1}$ for some suitable n. So for any state $\mathbf{p} \in \Gamma$, any $s \in S$ and for some suitable k holds $\mathbf{p}s^k = \mathbf{p}s^{k+1}$.

Lemma 13 *Let $\mathcal{A}$ be an aperiodic automaton. Then the existence of sink state in $\mathcal{A}$ is equivalent to the existence of 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.

Let us go to the key lemma of the proof.

Lemma 14 *Let a DFA with the transition graph Γ be aperiodic.*
Then the graph Γ has no t-cycle, the quasi-order $\succeq_M$ for any almost minimal SCC M is a partial order and no state belongs to t-cycle.

Proof. Suppose the states $\mathbf{p}_1 \succ_M \mathbf{p}_2, .., \mathbf{p}_{m-1} \succ_M \mathbf{p}_m = \mathbf{p}_1$ form t-cycle of the minimal size m for some almost minimal SCC M.
Let us establish that $m > 2$. Indeed, $\mathbf{p}_1 \neq \mathbf{p}_2$ by the definition of the relation $\succ_M$, whence $m > 1$. If $m = 2$ then two states $(\mathbf{p}_1, \mathbf{p}_2)$ and $(\mathbf{p}_2, \mathbf{p}_1)$ belong to common SCC. For some element u from 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 $\mathbf{p}_1 u^2 = \mathbf{p}_1 \neq \mathbf{p}_1 u$. It 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 holds $u^{2k} = u^{2k+1}$, whence $\mathbf{p}_1 u^{2k} = \mathbf{p}_1 u^{2k+1}$. 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 $s \in S$ and for the states $\mathbf{p}_1$, $\mathbf{p}_2$, $\mathbf{p}_3$ from considered t-cycle holds $(\mathbf{p}_1, \mathbf{p}_2)s = (\mathbf{p}_2, \mathbf{p}_3)$. We have

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

For any word $v \in S$ and any state $(\mathbf{p}_i, \mathbf{p}_{i+1})$ from M by Lemma 1 $\mathbf{p}_i v \succeq_M \mathbf{p}_{i+1} v$. Therefore for any word $v \in S$ the non one-element sequence of states $\mathbf{p}_1 v, ..., \mathbf{p}_m v$ forms t-cycle of minimal size m. It is also true for $v = s^i$ for any integer i.
The states $\mathbf{p}_1, \mathbf{p}_1 s, \mathbf{p}_1 s^2$ are distinct. Let us notice that in aperiodic finite semigroup for some l holds $s^l \neq s^{l+1} = s^{l+2}$. Therefore there exists such maximal integer $k \leq l$ such that $\mathbf{p}_1 s^k \neq \mathbf{p}_1 s^{k+1} = \mathbf{p}_1 s^{k+2}$ and in the t-cycle $\mathbf{p}_1 s^k$, $\mathbf{p}_2 s^k = \mathbf{p}_1 s^{k+1}$, $\mathbf{p}_3 s^k = \mathbf{p}_1 s^{k+2}$,..., $\mathbf{p}_m s^k$ holds $\mathbf{p}_1 s^k \neq \mathbf{p}_2 s^k = \mathbf{p}_3 s^k$. So the cardinality of the obtained t-cycle is greater than one and less than m. Contradiction.

Corollary 15 *Let M be almost minimal SCC of aperiodic DFA with transition graph Γ. Then the relation $\succ_M$ is anti-reflexive.*

Theorem 3 *Let the transition graph Γ of an n-state ($n > 2$) synchronizable automaton be strongly connected.*
Then the automaton has reset word of length not greater than $(n-1)^2/2$.

Proof. The case of state outside t-cycle follows from the Theorem 2. In opposite case all states belong to $\Gamma(M)$ of some almost minimal SCC M and therefore the number r of ρ_M - classes of almost minimal SCC M is equal to $|\Gamma/\rho_M|$. By Lemma 14 the relation ρ defines a partial order. Now by Lemma 7 any ρ_M-class can be synchronized by word of length $(n-r)(n-1)/2$. Theorem 1 for $c = 1/2$ finishes the proof.

5 The general case of aperiodic DFA

Lemma 16 *Let Γ be transition graph of synchronizable n-state ($n > 2$) DFA with transition semigroup without non-trivial subgroups. Suppose that SCC Γ_1 of Γ has no ingoing edges from another SCC and $|\Gamma_1| \leq n-2$. Then the automaton has synchronizing word of length not greater than $(n-1)^2/2$.*

Proof. Let us denote $|\Gamma \setminus \Gamma_1| = r$. So $|\Gamma_1| = n - r$ and $r > 1$. By [9] (theorem 6.1), a word of length $(n-r)(n-r+1)/2$ maps Γ in $\Gamma \setminus \Gamma_1$. If $r = 2$ then $\Gamma \setminus \Gamma_1$ has reset word of length 1 and Γ has reset word of length $1 + (n-2)(n-1)/2 = (n-1)^2/2 + (3-n)/2 \leq (n-1)^2/2$ because $n > 2$. In the case $r > 2$ one can assume by induction that the graph $\Gamma \setminus \Gamma_1$ has reset word of length $(r-1)^2/2$. Therefore Γ has reset word v of length $(n-r)(n-r+1)/2 + (r-1)^2/2$. Now from $n > r > 1$ and equality
$(n-r)(n-r+1)+(r-1)^2 = (n-r)^2+n-r+(r-1)^2+2(n-r)(r-1)-2(n-r)(r-1)$
$= (n-r+r-1)^2 + n - r - 2(n-r)(r-1) = (n-1)^2 - (n-r)(2r-3)$
follows that the length of v is not greater than $(n-1)^2/2$.

Lemma 17 *Let Γ be transition graph of synchronizable n-state ($n > 2$) DFA with transition semigroup without non-trivial subgroups. Suppose that Γ is a union of SCC Γ_0 of size $n-1$ and sink $\mathbf{p}$. Then the automaton has synchronizing word of length not greater than $(n-1)^2/2$.*

Proof. Γ has only two SCC, Γ_0 and $\{\mathbf{p}\}$. For any state $\mathbf{t} \in \Gamma_0$ there exists a word $u(t)$ of minimal length such that $\mathbf{t}u(t) = \mathbf{p}$. If we form a reset word $s = s_1...s_{n-1}$ such that $s_i = u(t)$ for $\mathbf{t} \in \Gamma_0 s_1...s_{i-1}$ with minimal $u(t)$ (as in [9]) then $|s| \leq n(n-1)/2 = C_n$. Our aim is to reduce the length $|s|$ to $(n-1)^2/2$.
Let us denote $C_i = i(i-1)/2$. For reset word $s_1...s_{n-1}$ suppose $S_i = s_1...s_i$. Let us denote $\Gamma_i = \Gamma_0 \cap \Gamma_0 S_i$. The size of Γ_i is at most $n-1-i$. For any state $\mathbf{q}$ there exists a letter α such that $\mathbf{q} \neq \mathbf{q}\alpha$ and there exists a minimal integer k such that $\mathbf{q}\alpha^k = \mathbf{q}\alpha^{k+1}$. For letter σ with maximal value of such k suppose $s_i = \sigma$ for $i \leq k$. So $|S_k| = k$.
Let us go now to the values of i after k. If in Γ_i either there exists a state $\mathbf{t}$ with $u(t) \leq i$ or two states $\mathbf{q}$ and $\mathbf{q}\beta^j$ for some β then let us take as s_{i+1} such $u(t)$ or β^i. From $j \leq k \leq i$ and $u(t) \leq i$ follows $|s_{i+1}| \leq i$. Therefore $|S_{i+1}| \leq k + \sum_{j=k+1}^{i} j = k + \sum_{j=1}^{i} j - \sum_{j=1}^{k} j = k + i(i+1)/2 - k(k+1)/2 \leq C_{i+1} - C_k$.
If $|\Gamma_1 S_i| < n-1-i$ then let s_{i+1} be empty word. So $|S_{i+1}| \leq C_{i+1} - C_k$. Thus

$$|S_i| \leq C_i < (i-1)^2/2 \text{ for } i > k$$

For reset word S_{n-1} one has $|S_{n-1}| < (n-1)^2/2$.
Now remains only the case of Γ_i without pairs of states $\mathbf{q}$ and $\mathbf{q}\beta^j$ for some letter β and with $u(t) > i$ for all states $\mathbf{t} \in \Gamma_i$. The existence of the state with $u(t) > i$ implies the existence of at least $|u(t)| - 1 \geq i$ states $\mathbf{q}$ on the path to $\mathbf{p}$ and of at least i states $\mathbf{r}$ with $u(r) \leq i$. Therefore there are at most $n-i-1$ states $\mathbf{t}$ with $u(t) > i$. Obviously, all these states belong to Γ_i.
For any such $\mathbf{t}$ with $u(t) > i$ there exists a letter α such that $\mathbf{t} \neq \mathbf{t}\alpha$. Hence $\mathbf{t}\alpha \notin \Gamma_i$ and $u(t\alpha) \leq i$. Therefore $u(t) \leq i+1$ for all $\mathbf{t} \in \Gamma_i$ and the maximal value of $u(t)$ in Γ_1 is $i+1$. So $n-1-i$ states of Γ_i can be mapped in $\mathbf{p}$ by word

v of length at most $(n-1-i)(i+1)$.
Therefore $S_i v$ is a reset word and
$|S_i v| \leq (n-1-i)(i+1)+C_i-C_k = (n-1-i)(i+1)+i(i-1)/2-C_k = (n-1)(i+1)-i^2-i+i^2/2-0.5i-C_k = (n-1)(i+1)-0.5i^2-i-0.5+0.5-0.5i-C_k = (n-1)^2/2-(n-1)^2/2+(n-1)(i+1)-(i+1)^2/2+0.5-0.5i-C_k = (n-1)^2/2-(n-2-i)^2/2-0.5(i-1)-C_k \leq (n-1)^2/2.$

Theorem 4 *Synchronizable n-state DFA ($n > 2$) with transition semigroup having only trivial subgroups has synchronizing word of length not greater than $(n-1)^2/2$.*

Proof. Let the transition graph Γ of the automaton have SCC C of cardinality r with sink. By Theorem 3 for $\Gamma = C$ the assertion of the theorem is true. So let Γ have several SCC. In the case Γ has more than two SCC or $r > 1$, a synchronizing word of length not greater than $(n-1)^2/2$ exists by Lemma 16. In the case of two SCC and $r = 1$ the graph Γ by Lemma 17 also has synchronizing word of length not greater than $(n-1)^2/2$. Thus a word of length not greater than $(n-1)^2/2$ synchronizes the automaton.

Corollary 18 *The Černy conjecture holds true for DFA with transition semigroup having only trivial subgroups.*

References

1. J. Černy, Poznamka k homogenym eksperimentom s konechnymi automatami, Math.-Fyz. Čas., 14(1964) 208-215.
2. L.Dubuc, Sur le automates circulaires et la conjecture de Černy, RAIRO Inform. Theor. Appl., no 1-3, 32(1998) 21-34.
3. P. Frankl, An extremal problem for two families of sets, Eur. J. Comb., 3(1982) 125-127.
4. J. Kari, Synchronizing finite automata on Eulerian digraphs. Springer, Lect. Notes in Comp. Sci., 2136(2001), 432-438.
5. A.A. Kljachko, 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.
6. G. Lallement, Semigroups and Combinatorial Applications, Wiley, N.Y., 1979.
7. J.E. Pin, On two combinatorial problems arising from automata theory, Annals of Discrete Mathematics 17(1983), 535-548.
8. I.K. Rystsov, Almost optimal bound on recurrent word length for regular automata. Cybernetics and System An. 31, 5(1995) 669-674.
9. I.K. Rystsov, Reset words for commutative and solvable automata. Theoret. Comput. Sci. 172(1997) 273-279.
10. A. Salomaa, Generation of constants and synchronization of finite automata, J. of Univers. Comput. Sci., 8(2) (2002), 332-347.
11. M.P. Schŭtzenberger, On finite monoids having only trivial subgroups. Inf. control, 8(1965) 190-194.
12. A.N. Trahtman, An efficient algorithm finds noticeable trends and examples concerning the Černy conjecture. Lect. Notes in Comp. Sci., Springer, MFCS 2006, 4162(2006), 789-800.