Theoretical Computer Science 410 (2009) 3513–3519

Contents lists available at ScienceDirect

Theoretical Computer Science

journal homepage: www.elsevier.com/locate/tcs

Synchronizing automata preserving a chain of partial orders☆

M.V. Volkov

Department of Mathematics and Mechanics, Ural State University, 620083 Ekaterinburg, Russia

ARTICLE INFO

Keywords:
Synchronizing automata
Aperiodic automata
Weakly monotonic automata

ABSTRACT

We present a new class of automata which strictly contains the class of aperiodic automata and shares with the latter certain synchronization properties. In particular, every strongly connected automaton in this new class is synchronizing and has a synchronizing word of length $\left\lfloor \frac{n(n+1)}{6} \right\rfloor$ where n is the number of states of the automaton.

0. Background and motivation

Let $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ be a *deterministic finite automaton* (DFA), where Q is the state set, Σ stands for the input alphabet, and $\delta : Q \times \Sigma \to Q$ is the transition function defining an action of the letters in Σ on Q. The action extends in a unique way to an action $Q \times \Sigma^* \to Q$ of the free monoid Σ^* over Σ; the latter action is still denoted by δ. The DFA $\mathscr{A}$ is called *synchronizing* if there exists a word $w \in \Sigma^*$ whose action resets $\mathscr{A}$, that is to leave the automaton in one particular state no matter which state in Q it starts at: $\delta(q, w) = \delta(p, w)$ for all $q, p \in Q$. Any such word w is said to be a *synchronizing word* for the DFA.

It is rather natural to ask how short a synchronizing word for a given synchronizing automaton may be. The question is not easy: given a DFA $\mathscr{A}$ and a positive integer ℓ, the problem whether or not $\mathscr{A}$ has a synchronizing word of length at most ℓ is known to be NP-complete (see [5] or [8] or [14]). On the other hand, there are some upper bounds on the minimum length of synchronizing words for synchronizing automata with a given number of states. The best such bound known so far is due to Pin [12] (it is based on a combinatorial theorem conjectured by Pin and then proved by Frankl [6]): for each synchronizing automaton with n states, there exists a synchronizing word of length at most $\frac{n^3-n}{6}$. In 1964, Černý [3] constructed for each $n > 1$ a synchronizing automaton with n states whose shortest synchronizing word has length $(n-1)^2$. Soon after that he conjectured that those automata represent the worst possible case, that is, every synchronizing automaton with n states can be reset by a word of length $(n-1)^2$. By now this simple looking conjecture is arguably the most longstanding open problem in the combinatorial theory of finite automata. The reader is referred to the survey [17] for historical notes and a summary of the current state-of-the-art. Also the survey [10] gives an interesting overview of the area and its relations to multiple-valued logic and symbolic dynamics; applications of synchronizing automata to robotics are discussed in [5,7]. The survey [15] contains a detailed account of algorithmic and complexity issues in the field but unfortunately omits some important references.

While the Černý conjecture remains open in general, some progress has been achieved for various restricted classes of synchronizing automata. For instance, in Kari's elegant paper [9] the conjecture has been verified for automata with Eulerian underlying digraphs. Dubuc [4] has proved the conjecture under the assumption that there is a letter which acts on the state set Q as a cyclic permutation of order $|Q|$. Eppstein [5] has confirmed the conjecture for automata whose states can be arranged in some cyclic order which is preserved by the action of each letter in Σ.

☆ Supported by the Russian Foundation for Basic Research, grant 05-01-00540. The paper has been completed during the author's stay at the University of Turku under the Finnish Mathematical Society International Visitors Program 2006–2007 "Algorithmic and Discrete Mathematics".

E-mail address: Mikhail.Volkov@usu.ru.

0304-3975/$ – see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.tcs.2009.03.021

Recently some attention has been paid to the synchronization issues within the class **Ap** of *aperiodic automata*. Recall that a DFA is called *aperiodic* (or *counter-free*) if its transition monoid has only singleton subgroups. Aperiodic automata play a distinguished role in many aspects of formal language theory and its connections to logic, see the classic monograph [11]. Thus, studying synchronization of aperiodic automata appears to be well justified, especially if one takes into account that the problem of finding short synchronizing words is known to remain difficult when restricted to **Ap**. Indeed, inspecting the reductions from 3-SAT used in [5] or [8] or [14], one can observe that in each case the construction results in an aperiodic automaton, and therefore, the question of whether or not a given aperiodic automaton admits a synchronizing word whose length does not exceed a given positive integer, is NP-complete.

Trahtman [16] has proved that every synchronizing aperiodic automaton with n states admits a synchronizing word of length at most $\frac{n(n-1)}{2}$. Thus, the Černý conjecture holds true for synchronizing aperiodic automata. However, the problem of establishing a precise bound for the minimum length of synchronizing words for synchronizing aperiodic automata with n states still remains open, and moreover, we do not even have a reasonably justified conjecture for this case. Indeed, in all concrete examples of synchronizing aperiodic automata the minimum length of synchronizing words is bounded by a linear function of the number of states, namely, by $n + \lfloor \frac{n}{2} \rfloor - 2$. (A series of examples reaching this bound for $n \geq 7$ appeared in [1].) This phenomenon creates a feeling, first, that the upper bound $\frac{n(n-1)}{2}$ is rather rough, and second, that some arguments from [16] may apply to a larger class of automata.

In Section 1 we define such a new class of automata which we call *weakly monotonic*. Their definition resembles one of the generalized monotonic automata introduced and motivated in [2] and is in fact obtained by a slight relaxation of the latter notion. But, while generalized monotonic automata form a proper subclass of the class **Ap** of aperiodic automata [2], the class of weakly monotonic automata can be shown to strictly contain **Ap**, see Propositions 1.1 and 1.2.

In Section 2 we discuss synchronization properties of weakly monotonic automata. Here we restrict ourselves to the case when the underlying digraph of the automaton in question is strongly connected (for brevity, we refer to such automata as *strongly connected*). The restriction is rather natural since it is known (and easy to verify, see the discussion following Proposition 2.1) that the Černý conjecture readily reduces to this case. We prove, and this is the main result of the paper, that every strongly connected weakly monotonic automaton is synchronizing and has a synchronizing word of length $\left\lfloor \frac{n(n+1)}{6} \right\rfloor$ where n is the number of states of the automaton. This upper bound is new even for the aperiodic case.

1. Weakly monotonic automata

Let X be a set and $\rho \subseteq X \times X$ a binary relation on X. We denote by $\mathrm{Eq}(\rho)$ the *equivalence closure* of ρ, that is, the least equivalence relation containing ρ. It is well known and easy to see that a pair $(x, y) \in X \times X$ belongs to $\mathrm{Eq}(\rho)$ if and only if there exist elements $x_0, x_1, \ldots, x_k \in X$ such that $x = x_0, x_k = y$, and for each $i = 1, \ldots, k$ either $x_{i-1} = x_i$ or $(x_{i-1}, x_i) \in \rho$ or $(x_i, x_{i-1}) \in \rho$.

A binary relation ρ on the state set Q of a DFA $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ is said to be *stable* if $(p, q) \in \rho$ implies $\big(\delta(p, a), \delta(q, a)\big) \in \rho$ for all states $p, q \in Q$ and all letters $a \in \Sigma$. From the above description of the equivalence closure it easily follows that $\mathrm{Eq}(\rho)$ is stable whenever ρ is.

Recall that a stable equivalence π on the state set of a DFA is called a *congruence*. Given a congruence π of $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ and a state $q \in Q$, we denote by $[q]_\pi$ the π-class containing q. The *quotient* $\mathscr{A}/\pi$ is the DFA $\langle Q/\pi, \Sigma, \delta_\pi \rangle$ where $Q/\pi = \big\{[q]_\pi \mid q \in Q\big\}$ and the transition function δ_π is defined by the rule $\delta_\pi([q]_\pi, a) = [\delta(q, a)]_\pi$ for all $q \in Q$ and $a \in \Sigma$. Observe that every stable relation $\rho \subseteq Q \times Q$ containing π induces a stable relation on Q/π, namely, the relation $\rho/\pi = \big\{\big([p]_\pi, [q]_\pi\big) \mid (p, q) \in \rho\big\}$.

We call a DFA $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ *weakly monotonic of level* ℓ if it has a strictly increasing chain of stable binary relations

$$\rho_0 \subset \rho_1 \subset \cdots \subset \rho_\ell \tag{1}$$

satisfying the following conditions:

(WM1) ρ_0 is the equality relation $\{(q, q) \mid q \in Q\}$;
(WM2) for each $i = 1, \ldots, \ell$, the congruence $\pi_{i-1} = \mathrm{Eq}(\rho_{i-1})$ is contained in ρ_i and the relation ρ_i/π_{i-1} is a (partial) order on Q/π_{i-1};
(WM3) π_ℓ is the universal relation $Q \times Q$.

Slightly abusing terminology, we refer to any chain of the form (1) satisfying WM1–WM3 as a *chain of partial orders preserved by* $\mathscr{A}$. (It should be clear that in fact the ρ_i's with $i > 1$ are preorders on Q but not orders as they cannot be antisymmetric.)

First of all, since the definition of a weakly monotonic automaton is rather involved, we illustrate it by a transparent example. Consider the DFA in the left part of Fig. 1; we denote it by $\mathscr{E}$. We want to show that $\mathscr{E}$ is weakly monotonic of level 2. Let ρ_0 be the equality relation. Then so is $\pi_0 = \mathrm{Eq}(\rho_0)$, of course. We define $\rho_1 = \pi_0 \cup \{(1, 2), (3, 4)\}$. Then it is easy to check that ρ_1 is a stable partial order and the congruence $\pi_1 = \mathrm{Eq}(\rho_1)$ is the partition of $\{1, 2, 3, 4\}$ into 2 classes $Q_1 = \{1, 2\}$ and $Q_2 = \{3, 4\}$ (the partition is shown in Fig. 1 by the dashed line). The quotient $\mathscr{E}/\pi_1$ is shown in Fig. 1 on the right. Next, we define $\rho_2 = \pi_1 \cup Q_1 \times Q_2$. Then we immediately see that ρ_2/π_1 is a stable order with respect to the quotient $\mathscr{E}/\pi_1$ and $\pi_2 = \mathrm{Eq}(\rho_2)$ is the universal relation.

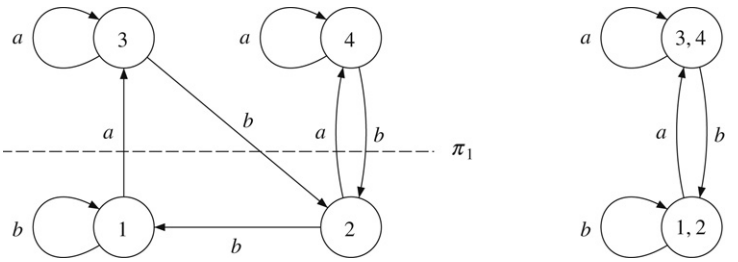

Fig. 1. An example of a weakly monotonic automaton.

We mention in passing that one can show that $\mathscr{E}$ is in fact weakly monotonic of level 1. (For this, one should check that the partial order

$$\pi_0 \cup \{(1, 2), (1, 3), (1, 4), (2, 4), (3, 4)\}$$

also is stable with respect to $\mathscr{E}$.)

Now we give two mass examples of weakly monotonic automata. The first of them constitutes our main motivation for considering this class.

Proposition 1.1. *Every aperiodic automaton is weakly monotonic.*

Proof. Let $\mathscr{A} = \langle Q, \Sigma, \delta\rangle$ be an aperiodic automaton. We use induction on $|Q|$ and, since the claim is trivial for $|Q| = 1$, we assume that $|Q| > 1$. We have to construct a strictly increasing chain of stable relations satisfying the conditions WM1–WM3. In [16, Lemma 7] it is shown that every non-trivial aperiodic automaton admits a non-trivial stable partial order. Let ρ_1 be such an order with respect to $\mathscr{A}$ and $\pi_1 = \mathrm{Eq}(\rho_1)$. The quotient automaton $\mathscr{A}/\pi_1$ is aperiodic again because its transition monoid is a quotient of the transition monoid of $\mathscr{A}$. Thus, $\mathscr{A}/\pi_1$ preserves a chain of partial orders by the induction assumption. Lifting this chain back to Q, we obtain, for some ℓ, a chain of stable relations $\rho'_0 \subset \rho'_1 \subset \cdots \subset \rho'_\ell$ satisfying WM2 and WM3 and such that $\rho'_0 = \pi_1$. Now it is easy to see that the chain $\rho_0 \subset \rho_1 \subset \rho'_1 \subset \cdots \subset \rho'_\ell$, in which ρ_0 is the equality relation on Q, satisfies WM1–WM3. □

The second group of examples shows, in particular, that the converse of Proposition 1.1 is not true. Recall that a state s of a DFA $\mathscr{A} = \langle Q, \Sigma, \delta\rangle$ is called a *sink* if $\delta(s, a) = s$ for all $a \in \Sigma$.

Proposition 1.2. *Every DFA with a unique sink is weakly monotonic.*

Proof. Let $\mathscr{A} = \langle Q, \Sigma, \delta\rangle$ be a DFA with a unique sink $s \in Q$. We define a partial order ρ_1 on the set Q by letting the sink s be less than each state in $Q \setminus \{s\}$ and leaving all states in $Q \setminus \{s\}$ incomparable. It is easy to see that ρ_1 is preserved by all the transformations $\delta(\sqcup, a)$ where $a \in \Sigma$ and that $\mathrm{Eq}(\rho_1) = Q \times Q$. Thus, the chain $\rho_0 \subset \rho_1$, in which ρ_0 is the equality on Q, satisfies WM1–WM3, and $\mathscr{A}$ is weakly monotonic of level 1. □

Of course, a DFA $\mathscr{A}$ with a unique sink need not be aperiodic. For instance, some of the input letters of $\mathscr{A}$ can act as a cyclic permutation of the non-sink states thus inducing a non-singleton cyclic subgroup in the transition monoid of $\mathscr{A}$.

2. Strongly connected weakly monotonic automata

In this section, when dealing with a fixed automaton $\mathscr{A} = \langle Q, \Sigma, \delta\rangle$, we will simply write $q.w$ instead of $\delta(q, w)$ for $q \in Q$ and $w \in \Sigma^*$. For $S \subseteq Q$, we denote the set $\{q.w \mid q \in S\}$ by $S.w$.

First, we explain why one may concentrate on strongly connected automata when studying synchronization issues such as the minimum length of synchronizing words for automata with a given number of states.

Proposition 2.1. *Let* $\mathbf{C}$ *be any class of automata closed under taking subautomata and quotients, and let* $\mathbf{C}_n$ *stand for the class of all automata with* n *states in* $\mathbf{C}$*. Further, let* $f : \mathbb{Z}^+ \to \mathbb{N}$ *be any function such that*

$$f(n) \geq f(n - m + 1) + f(m) \quad \text{whenever } n \geq m \geq 1. \tag{2}$$

If each synchronizing automaton in $\mathbf{C}_n$ *which either is strongly connected or possesses a unique sink has a synchronizing word of length* $f(n)$*, then the same holds true for all synchronizing automata in* $\mathbf{C}_n$*.*

Proof. Let $\mathscr{A} = \langle Q, \Sigma, \delta\rangle$ be a synchronizing automaton in $\mathbf{C}_n$. Consider the set S of all states to which the automaton $\mathscr{A}$ can be synchronized and let $m = |S|$. If $q \in S$, then there exists a synchronizing word $w \in \Sigma^*$ such that $Q.w = \{q\}$. Then wa also is a synchronizing word and $Q.wa = \{q.a\}$ whence $q.a \in S$. This means that, restricting the transition function δ to $S \times \Sigma$, we get a subautomaton $\mathscr{S}$ with the state set S. Obviously, $\mathscr{S}$ is synchronizing and strongly connected and, since the class $\mathbf{C}$ is closed under taking subautomata, we have $\mathscr{S} \in \mathbf{C}$. Hence, $\mathscr{S}$ has a synchronizing word v of length $f(m)$.

Now consider the partition π of Q into $n - m + 1$ classes one of which is S and all others are singletons. It is easy to see that π is a congruence of the automaton $\mathscr{A}$. Clearly, the quotient $\mathscr{A}/\pi$ is synchronizing and has S as a unique sink. Since the class $\mathbf{C}$ is closed under taking quotients, we have $\mathscr{A}/\pi \in \mathbf{C}$. Hence, $\mathscr{A}/\pi$ has a synchronizing word u of length $f(n - m + 1)$.

Since $Q.u \subseteq S$ and $S.v$ is a singleton, we conclude that also $Q.uv \subseteq S.v$ is a singleton. Thus, uv is synchronizing word for $\mathscr{A}$, and the length of this word does not exceed $f(n - m + 1) + f(m) \leq f(n)$ according to (2). □

It is easy to check that the function $f(n) = (n-1)^2$ satisfies (2). Thus, applying Proposition 2.1 to the class of all automata, we see that it suffices to prove the Černý conjecture for strongly connected automata and for automata with a unique sink. It is known (see, e.g., [13]) that every synchronizing automaton with a unique sink has a synchronizing word of length $\frac{n(n-1)}{2} \leq (n-1)^2$, whence only the strongly connected case remains open.

Similarly, applying Proposition 2.1 to the class **Ap** of all aperiodic automata and to the function $f(n) = \frac{n(n-1)}{2}$, we see that Trahtman's upper bound [16] for the length of synchronizing words for synchronizing aperiodic automata follows from its restriction to strongly connected automata.

In view of Proposition 1.2, weak monotonicity does not impose any extra restriction on automata with a unique sink. In contrast, we will prove that strongly connected weakly monotonic automata are rather specific from the synchronization viewpoint.

Theorem 2.2. *Every strongly connected weakly monotonic automaton $\mathscr{A} = \langle Q, \Sigma, \delta\rangle$ is synchronizing and has a synchronizing word of length $\lfloor \frac{n(n+1)}{6} \rfloor$ where $n = |Q|$.*

Proof. We proceed by induction on n and observe that the case $n = 1$ is obvious. Thus, we assume that $n > 1$.

By the definition of weakly monotonic automata there exists a non-trivial stable partial order relation ρ_1 on Q. For $S \subseteq Q$, we denote by $\min(S)$ and $\max(S)$ the sets of the minimal and the maximal elements of S with respect to the order ρ_1.

It is convenient to isolate the following observation.

Lemma 2.3. *For every word $v \in \Sigma^*$, one has $\min(S.v) \subseteq \min(S).v$.*

Proof. In order to improve readability, we write $\leq$ instead of ρ_1. Take any state $p' \in \min(S.v)$ and consider its arbitrary preimage $p \in S$. There exists $q \in \min(S)$ such that $q \leq p$. Since the order $\leq$ is stable, we then have $q' = q.v \leq p.v = p'$. The state q' belongs to the set $S.v$, and therefore, $q' = p'$ because p' has been chosen to be a minimal element in this set. Thus, we have found a preimage for p' in $\min(S)$ whence $\min(S.v) \subseteq \min(S).v$. □

We say that a subset $T \subseteq Q$ is *linked* if for every pair $(q, p) \in T \times T$ there exist states $q_0, q_1, \ldots, q_k \in T$ such that $q = q_0$, $q_k = p$, and for each $i = 1, \ldots, k$ either $(q_{i-1}, q_i) \in \rho_1$ or $(q_i, q_{i-1}) \in \rho_1$. (This simply means that the Hasse diagram of the poset $\langle T, \rho_1\rangle$ is connected as a graph.) Let $\pi_1 = \mathrm{Eq}(\rho_1)$. It is clear that each π_1-class is a linked set and that any linked set is contained in a single π_1-class. Further, since the order ρ_1 is stable, we immediately get the following observation:

Lemma 2.4. *If $T \subseteq Q$ is linked, then for every word $v \in \Sigma^*$ the set $T.v$ is linked.*

We will often use the following property of linked sets:

Lemma 2.5. *If T is linked and $|T| > 1$, then $\min(T) \cap \max(T) = \varnothing$.*

Proof. Again, we write $\leq$ instead of ρ_1. Take any state $q \in \min(T)$, and let p be any state in $T \setminus \{q\}$. Since T is linked, there is a sequence of states $q_0, q_1, \ldots, q_k \in T$ such that $q = q_0$, $q_k = p$, and for each $i = 1, \ldots, k$ either $q_{i-1} \leq q_i$ or $q_i \leq q_{i-1}$. If we choose $q_0, q_1, \ldots, q_k$ to be such a sequence of minimum length, then no adjacent states can be equal, in particular, $q_0 \neq q_1$. Therefore either $q_0 \lneqq q_1$ or $q_1 \lneqq q_0$. As the latter inequality would contradict the fact that $q_0 = q \in \min(T)$, we conclude that $q = q_0 \lneqq q_1$ whence q is not a maximal element of T. Thus, no minimal element of T can be at the same time a maximal element. □

The core of our argument is contained in the following

Lemma 2.6. *Let $T \subseteq Q$ be a linked set, $\ell = |\min(T) \setminus \max(T)|$ and $k = |\max(Q)|$. Then there exists a word $w \in \Sigma^*$ of length at most $b(\ell, k) = \ell(n-k+1) - \frac{\ell(\ell+1)}{2}$ such that $|T.w| = 1$.*

Proof. We proceed by induction on ℓ. If $\ell = 0$, then $b(\ell, k) = 0$. Besides that, from the definition of ℓ it follows that in T each minimal element is in the same time a maximal element. By Lemma 2.5 this is only possible if T is a singleton. Then the empty word can play the role of w.

Let $\ell > 0$. By Lemma 2.5 we then have $\ell = |\min(T)|$. Since the DFA $\mathscr{A}$ is strongly connected, there is a directed path from $\min(T)$ to $\max(Q)$ in its underlying digraph. Choose such a path of minimum length. This path cannot visit any state twice, only its first state can belong to $\min(T)$ and only its last state can lie in $\max(Q)$. Therefore the number of the edges in the path cannot exceed $|Q \setminus \big(\min(T) \cup \max(Q)\big)| + 1$. From Lemma 2.5 it follows that $\min(T) \cap \max(Q) = \varnothing$ whence the cardinality of the set $Q \setminus \big(\min(T) \cup \max(Q)\big)$ is equal to $n - \ell - k$ (in particular, $n - \ell - k \geq 0$). Thus, if u is the word that labels a path of minimum length from $\min(T)$ to $\max(Q)$, then the length of u does not exceed $n - \ell - k + 1$.

Observe that

$$b(\ell-1, k) + (n-\ell-k+1) = (\ell-1)(n-k+1) - \frac{(\ell-1)\ell}{2} + (n-\ell-k+1) = \ell(n-k+1) - \frac{\ell(\ell+1)}{2} = b(\ell, k). \tag{3}$$

Since $n - \ell - k \geq 0$, this implies that $b(\ell, k) > b(\ell-1, k)$ whenever $\ell > 0$.

Now consider the set $T.u$. It is linked by Lemma 2.4. By Lemma 2.3 $\min(T.u) \subseteq \min(T).u$. Let $q \in \min(T)$ be the state at which the path labelled u starts. If $q' = q.u \notin \min(T.u)$, then

$$|\min(T.u)| < |\min(T).u| \leq |\min(T)| = \ell,$$

and the induction assumption applies to the set $T.u$. We have observed that the number $b(\ell, k)$ increases with ℓ, and therefore, we may assume that there is a word $v \in \Sigma^*$ of length at most $b(\ell - 1, k)$ such that $|(T.u).v| = 1$. Then we can let $w = uv$: we have $T.w = (T.u).v$ whence $|T.w| = 1$ and (3) ensures that the length of w does not exceed $b(\ell, k)$.

It remains to consider the case when $q' = q.u \in \min(T.u)$. Recall that by the choice of our path $q' \in \max(Q)$. Thus, the state q' which is minimal in $T.u$ is also maximal in Q whence it is of course maximal in $T.u$ as well. By Lemma 2.5 this implies that $|T.u| = 1$, and we can let $w = u$. The fact that the length of u (which does not exceed $n - \ell - k + 1$) is less than or equal to $b(\ell, k)$ follows from the equality (3) if one takes into account that $b(\ell - 1, k) \geq 0$. □

We will also use the following arithmetical observation:

Lemma 2.7. *If $0 \leq \ell \leq k$, then $b(\ell, k) \leq \lfloor \frac{n(n+1)}{6} \rfloor$.*

Proof. Considering the expression $\frac{n(n+1)}{6} + \frac{1}{24} - b(\ell, k)$ as a quadratic polynomial of n, one readily sees that its discriminant $\frac{2}{3}\ell(\ell - k)$ is non-positive whenever $0 \leq \ell \leq k$. Therefore $b(\ell, k) \leq \frac{n(n+1)}{6} + \frac{1}{24}$. Since $b(\ell, k)$ is an integer, we also have $b(\ell, k) \leq \lfloor \frac{n(n+1)}{6} + \frac{1}{24} \rfloor$, and it remains to observe that

$$\left\lfloor \frac{n(n+1)}{6} + \frac{1}{24} \right\rfloor = \left\lfloor \frac{n(n+1)}{6} \right\rfloor$$

for every integer n. □

Now we can return to the proof of Theorem 2.2. Since π_1 is not the equality relation on Q, the number m of π_1-classes is strictly less than n. We subdivide the proof into 3 cases depending on m.

Case 1: $m = 1$. In this case the whole set Q forms a π_1-class, and therefore, it is linked. Let $\ell = |\min(Q)|$, $k = \max(Q)$. If $\ell \leq k$, then, applying Lemma 2.6 for $T = Q$, we get a synchronizing word of length at most $b(\ell, k)$, and by Lemma 2.7 we obtain the desired upper bound. If $\ell > k$, we may apply the dual of Lemma 2.6 in which we interchange the roles of minimal and maximal elements. This gives a synchronizing word of length at most $b(k, \ell)$, and again a reference to Lemma 2.7 concludes the proof.

Thus, for the rest of the proof we may assume that $m > 1$. The quotient automaton $\mathscr{A}/\pi_1$ is weakly monotonic and strongly connected. Applying the induction hypothesis, we obtain that $\mathscr{A}/\pi_1$ possesses a synchronizing word u of length at most $\lfloor \frac{m(m+1)}{6} \rfloor$. This means that in the automaton $\mathscr{A}$ we have $Q.u \subseteq T$ where T is a π_1-class.

Case 2: $m > \frac{n}{2}$. It is easy to calculate that in this case the congruence π_1 has at least $2m - n$ singleton classes and at most $n - m$ non-singleton classes. Since the automaton $\mathscr{A}/\pi_1$ is strongly connected, there is a path from the class T to a singleton class, and the length of the shortest path with this property does not exceed the number of non-singleton classes. Let v be the word of length at most $n - m$ labelling such a path. Since $|T.v| = 1$, we have $|Q.uv| = 1$, that is, uv is a synchronizing word for $\mathscr{A}$ of length at most $\lfloor \frac{m(m+1)}{6} \rfloor + (n - m)$. It is not hard to check that for all n and m satisfying $n > m > \frac{n}{2}$ the latter sum does not exceed $\lfloor \frac{n(n+1)}{6} \rfloor$. Indeed, consider the difference

$$\frac{n(n+1)}{6} - \frac{m(m+1)}{6} - (n - m) = \frac{1}{6}(n - m)(n + m - 5). \tag{4}$$

Clearly, $n = 3$ and $m = 2$ are the only admissible values of n and m such that (4) is equal to 0, and for all other n and m satisfying $n > m > \frac{n}{2}$ the difference (4) is positive. Thus, if $(n, m) \neq (3, 2)$, then

$$\left\lfloor \frac{m(m+1)}{6} \right\rfloor + (n - m) \leq \frac{m(m+1)}{6} + (n - m) < \frac{n(n+1)}{6}.$$

Since the left-hand side of this inequality is an integer, we conclude that

$$\left\lfloor \frac{m(m+1)}{6} \right\rfloor + (n - m) \leq \left\lfloor \frac{n(n+1)}{6} \right\rfloor,$$

and the latter inequality also holds for the exceptional pair $(n, m) = (3, 2)$.

Case 3: $2 \leq m \leq \frac{n}{2}$. This is the most complicated case whose proof involves a combination of the ideas from the two previous cases with some extra twists.

Denote the π_1-classes by $T_1, \ldots, T_m$. For each $i = 1, \ldots, m$ we consider the numbers $\ell_i = |\min(T_i)|$ and $k_i = |\max(T_i)|$. Let ℓ be the least number in the set $\{\ell_1, \ldots, \ell_m, k_1 \ldots, k_m\}$.

We partition the set of the π_1-classes into 4 subsets:

$$M_{00} = \{T_i \mid \ell_i = \ell,\ k_i = \ell\}, \qquad M_{01} = \{T_i \mid \ell_i = \ell,\ k_i > \ell\},$$
$$M_{10} = \{T_i \mid \ell_i > \ell,\ k_i = \ell\}, \qquad M_{11} = \{T_i \mid \ell_i > \ell,\ k_i > \ell\}.$$

Some of these subsets may be empty but at least one of the subsets M_{00}, M_{01} and M_{10} has to be non-empty by the choice of the number ℓ. Let m_{st} denote the cardinality of the set M_{st}, $s, t \in \{0, 1\}$. Using, if necessary, the up–down symmetry, we can always assume that $m_{01} \geq m_{10}$. Observe that this assumption implies that $M_{00} \cup M_{01} \neq \varnothing$. Indeed, if $M_{00} \cup M_{01} = \varnothing$, then $m_{00} = m_{01} = 0$ and from the assumed inequality $m_{01} \geq m_{10}$ it would also follow that $m_{10} = 0$. Then all the three subsets M_{00}, M_{01} and M_{10} would be empty, a contradiction.

Each π_1-class $T_i \in M_{00} \cup M_{01}$ has exactly ℓ minimal elements. Since every π_1-class is a linked set, we may apply Lemma 2.6 to each such π_1-class. Thus, letting $k = |\max(Q)|$, we obtain that for every $T_i \in M_{00} \cup M_{01}$ there exists a word $w_i \in \Sigma^*$ of length at most $b(\ell, k) = \ell(n - k + 1) - \frac{\ell(\ell+1)}{2}$ such that $|T_i.w_i| = 1$.

Since the congruence π_1 is the equivalence closure of the order ρ_1, any two ρ_1-comparable states always belong to the same π_1-class. In particular, the set $\max(Q)$ of all maximal elements of Q is a disjoint union of the sets of all maximal elements of the π_1-classes, and the cardinality k of $\max(Q)$ is equal to the sum $k_1 + \cdots + k_m$. Recall that $k_i = \ell$ if $T_i \in M_{00} \cup M_{10}$ and $k_i \geq \ell + 1$ if $T_i \in M_{01} \cup M_{11}$. Therefore $k \geq \ell m + m_{01} + m_{11}$. As $b(\ell, k)$ is a decreasing function of k, we can conclude that $b(\ell, \ell m + m_{01} + m_{11}) \geq b(\ell, k)$.

Recall that there is a word u of length at most $\lfloor \frac{m(m+1)}{6} \rfloor$ such that $Q.u \subseteq T$ where T is a certain π_1-class. Since the automaton $\mathscr{A}/\pi_1$ is strongly connected, there is a path from T to a class $T_i \in M_{00} \cup M_{01}$, and the length of the shortest path with this property does not exceed $m_{10} + m_{11}$. Let v be a word that labels such a shortest path. Then $Q.uv = (Q.u).v \subseteq T.v \subseteq T_i$ whence the product uvw_i is a synchronizing word for the automaton $\mathscr{A}$. Its length does not exceed

$$\left\lfloor \frac{m(m+1)}{6} \right\rfloor + (m_{10} + m_{11}) + b(\ell, \ell m + m_{01} + m_{11}), \tag{5}$$

and it remains to verify that this sum does not exceed $\lfloor \frac{n(n+1)}{6} \rfloor$.

To start with, consider the sum of the second and the third summands:

$$\begin{aligned}(m_{10} + m_{11}) + b(\ell, \ell m + m_{01} + m_{11}) &= (m_{10} + m_{11}) + \ell(n - \ell m - m_{01} - m_{11} + 1) - \frac{\ell(\ell+1)}{2} \\ &= (m_{10} + m_{11}) + b(\ell, \ell m) - \ell(m_{01} + m_{11}).\end{aligned}$$

Since $\ell \geq 1$ and $m_{01} \geq m_{10}$, we see that it does not exceed $b(\ell, \ell m)$. Now considering $b(\ell, \ell m) = \ell(n - \ell m + 1) - \frac{\ell(\ell+1)}{2}$ as a quadratic polynomial of ℓ, one sees that its maximum value is $\frac{(2n+1)^2}{8(2m+1)}$. Thus,

$$b(\ell, \ell m) < \frac{(2n+1)^2}{8(2m+1)} \leq \frac{(2n+1)^2}{40}. \tag{6}$$

Here the first inequality is strict because $b(\ell, \ell m)$ is an integer while $\frac{(2n+1)^2}{8(2m+1)}$ is not, and the second inequality follows from the fact that $m \geq 2$ in the case under consideration.

On the other hand, we have

$$\left\lfloor \frac{m(m+1)}{6} \right\rfloor \leq \frac{m(m+1)}{6} \leq \frac{n(n+2)}{24}. \tag{7}$$

Here the first inequality is clear and the second follows from another condition of the case, namely, $m \leq \frac{n}{2}$. From (6) and (7) we conclude that the sum (5) is strictly less than the sum

$$\frac{n(n+2)}{24} + \frac{(2n+1)^2}{40}$$

which can be easily seen to be strictly less than $\frac{n(n+1)}{6}$ for all $n \geq 2$. Since the sum (5) is an integer, it does not exceed $\lfloor \frac{n(n+1)}{6} \rfloor$, as required. □

As an immediate consequence of Proposition 1.1 and Theorem 2.2 we get

Corollary 2.8. *Every strongly connected aperiodic automaton is synchronizing and has a synchronizing word of length* $\lfloor \frac{n(n+1)}{6} \rfloor$ *where n is the number of states of the automaton.*

The fact that strongly connected aperiodic automata are synchronizing is known [16] but our upper bound for the minimum length of synchronizing words is considerably better than the bound $\frac{n(n-1)}{2}$ established in [16]. However, we strongly believe that our bound can be further improved.

References

[1] D.S. Ananichev, The mortality threshold for partially monotonic automata, in: C. De Felice, A. Restivo (Eds.), Developments in Language Theory, in: Lect. Notes Comput. Sci., vol. 3572, Springer-Verlag, Berlin, Heidelberg, 2005, pp. 112–121.
[2] D.S. Ananichev, M.V. Volkov, Synchronizing generalized monotonic automata, Theoret. Comput. Sci. 330 (2005) 3–13.
[3] J. Černý, Poznámka k homogénnym eksperimentom s konečnými automatami, Mat.-Fyz. Čas. Slovensk. Akad. Vied. 14 (1964) 208–216 (in Slovak).
[4] L. Dubuc, Sur les automates circulaires et la conjecture de Černý, RAIRO Inform. Theor. Appl. 32 (1998) 21–34 (in French).
[5] D. Eppstein, Reset sequences for monotonic automata, SIAM J. Comput. 19 (1990) 500–510.
[6] P. Frankl, An extremal problem for two families of sets, European. J. Combin. 3 (1982) 125–127.
[7] K. Goldberg, Orienting polygonal parts without sensors, Algorithmica 10 (1993) 201–225.
[8] P. Goralčik, V. Koubek, Rank problems for composite transformations, Internat. J. Algebra Comput. 5 (1995) 309–316.
[9] J. Kari, Synchronizing finite automata on Eulerian digraphs, Theoret. Comput. Sci. 295 (2003) 223–232.
[10] A. Mateescu, A. Salomaa, Many-valued truth functions, Černý's conjecture and road coloring, EATCS Bull. 68 (1999) 134–150.
[11] R. McNaughton, S.A. Papert, Counter-Free Automata, MIT Press, 1971.
[12] J.-E. Pin, On two combinatorial problems arising from automata theory, Ann. Discrete Math. 17 (1983) 535–548.
[13] I. Rystsov, Reset words for commutative and solvable automata, Theoret. Comput. Sci. 172 (1997) 273–279.
[14] A. Salomaa, Composition sequences for functions over a finite domain, Theoret. Comput. Sci. 292 (2003) 263–281.
[15] S. Sandberg, Homing and synchronizing sequences, in: M. Broy, et al. (Eds.), Model-Based Testing of Reactive Systems, in: Lect. Notes Comput. Sci., vol. 3472, Springer-Verlag, Berlin, Heidelberg, 2005, pp. 5–33.
[16] A.N. Trahtman, The Černý conjecture for aperiodic automata, Discrete Math. Theoret. Comp. Sci. 9 (2) (2007) 3–10.
[17] M.V. Volkov, Synchronizing automata and the Černý conjecture, in: C. Martín-Vide, et al. (Eds.), Language and Automata Theory and Applications, in: Lect. Notes Comput. Sci., vol. 5196, Springer-Verlag, Berlin, Heidelberg, 2008, pp. 11–27.