Discrete Mathematics and Theoretical Computer Science DMTCS vol. **15:3**, 2013, 61–72

The Černý conjecture for automata respecting intervals of a directed graph

Mariusz Grech[†] and Andrezj Kisielewicz[‡]

University of Wrocław, Poland

received 11th July 2012, revised 5th Mar. 2013, 30th July 2013, accepted 2nd Aug. 2013.

The Černý's conjecture states that for every synchronizing automaton with n states there exists a reset word of length not exceeding $(n-1)^2$. We prove this conjecture for a class of automata preserving certain properties of intervals of a directed graph. Our result unifies and generalizes some earlier results obtained by other authors.

Keywords: automata, Černý conjecture

In this paper we consider finite (deterministic complete) automata $A = \langle Q, \Sigma, \delta \rangle$ with the state set Q, the input alphabet Σ, and the transition function $\delta : \ Q \times \Sigma \to Q$. The transition function defines the action of the letters in Σ on Q, which, in this paper, is denoted simply by concatenation: $\delta(q, a) = qa$. The action extends in a natural way to the words in Σ^*, and we use the same notation $qw = \delta(q, w)$. Accordingly, we write $Qw = \{qw : \ q \in Q\}$.

The automaton A is called *synchronizing* if there exists a word $w \in \Sigma^*$ such that $|Qw| = 1$ (in other words, w *resets* A sending all the states into one particular state). Such a word w is called *synchronizing* (or a *reset* word) for A. The problem of synchronization is very natural and its various aspects are considered in the literature (see e.g. [6, 8, 13] for general information and further references). The most famous is the following conjecture due to Černý.

Conjecture (Jan Černý 1964, [4]) *If a deterministic finite n-state automaton $A = \langle Q, \Sigma, \delta \rangle$ is synchronizing, then it has a reset word of length $\leq (n-1)^2$.*

This conjecture is considered as one of the most longstanding open problems in the theory of finite automata. The consequent research includes verifying the conjecture for various classes of automata, establishing bounds for the length of reset words, investigating natural algorithmic and complexity questions, and many other related problems. For more detailed discussion we refer the reader to the most recent survey [13] by Volkov. Here, we mention only the most important results proving the conjecture in special cases.

[†]Email: `Mariusz.Grech@math.uni.wroc.pl`. Supported in part by Polish MNiSZW grant N N201 543038.
[‡]Email: `Andrzej.Kisielewicz@math.uni.wroc.pl`.Supported in part by Polish MNiSZW grant N N201 543038

In 1978, Pin [9] proved the conjecture for *circular* automata with a prime number of states (an automaton is *circular* if it has a letter acting as a cyclic permutation of all the states). In 1990, Eppstein [6] proved the conjecture for orientable automata (preserving a given cyclic ordering of all the states). In 1998, Dubuc [5], completing his earlier research, has verified the conjecture for all circular automata. In 2001, Kari [7] verifies the conjecture for *eulerian* automata (whose transition digraph is eulerian). In 2003, Ananichiev and Volkov [2] prove the conjecture for *monotonic* automata (preserving a linear order of the states), and in 2005 they generalize their result to a broader class given by a certain multi-level construction [3]. In 2007, Trahtman [12] demonstrates that the conjecture is true for *aperiodic* automata (ones with the transition monoid having no nontrivial subgroups). In 2008, Almeida, Margolis, Steinberg, and Volkov [1] verify the conjecture for another class of automata related to the formal language theory: those with monoids belonging to **DS** class. In 2009, Volkov [14] proves the conjecture for the so-called *weakly monotonic* automata, a certain strong generalization of generalized monotonic automata including the automata preserving a connected partial order. Most recently, in 2011, Steinberg [10] verifies the conjecture for automata having a letter inducing a connected digraph with the cycle of prime length (thus generalizing the mentioned Pin's result). In addition, various classes of small automata have been verified using computer programs. In particular, Trahtman [11], in 2007, has announced checking all the automata on 2 letters with $n \leq 10$ states.

Some of the above results involve assumptions on preserving by an automaton a certain structure. In this paper, we show that this kind of results may be unified and generalized. We introduce the notions of an *interval* for a directed graph, *respecting the intervals* of a digraph by an automaton, and the congruence induced by such a relation. Then, we prove a reduction theorem of the form that if an automaton A respects intervals of a directed graph and the induced quotient automaton satisfies the Černý conjecture, then so does A. Our result implies that the Černý conjecture is true for a large class of automata that includes, in particular, orientable automata [6], monotonic and generalized monotonic automata [2, 3], aperiodic automata [12], and weakly monotonic automata [14].

1 Preliminaries

There are two structures connected with an automaton $A = \langle Q, \Sigma, \delta \rangle$ giving possibilities of viewing the automaton in various ways. The *transition digraph* $T = T(A)$ is defined on Q by $(q, s) \in T$ if and only if $qa = s$ for some $a \in \Sigma$. The *transition monoid* $M = M(A)$ is one generated by transformations on Q corresponding to letters in Σ. Then, the words in Σ^* correspond to compositions of generating transformations.

Automaton $A = \langle Q, \Sigma, \delta \rangle$ is *strongly connected* if its transition digraph is strongly connected. In general, one can consider strongly connected components of $T(A)$. These are partially ordered by the relation of the existence of a directed edge in $T(A)$ from one component to another. It is clear that if A is synchronizing, then $T(A)$ has to have a unique minimal strongly connected component C. In such a case, the restriction $A|_C$ of A to C forms a reduced automaton. It is easy to prove (and it is considered as a folklore result) that if $A|_C$ satisfies the Černý conjecture, then so does A. Thus, it is enough to consider only strongly connected automata.

In terms of monoids, this is just a reduction to transitive monoids, since it is clear that A is strongly connected if and only if $M(A)$ is transitive. A further natural reduction would be one to transition monoids which are *primitive* in the sense of permutation group theory.

Given $A = \langle Q, \Sigma, \delta \rangle$, an equivalence relation $\sim$ on Q is called a *congruence* (on A) if it is preserved by A. More precisely, $q \sim s$ implies $qa \sim sa$ for all $a \in \Sigma$. If $\sim$ is a congruence, then the *quotient automaton* $A/\sim = \langle Q', \Sigma, \delta' \rangle$ is defined in the natural way: $Q' = Q/\sim$ is the set of the equivalence classes of $\sim$, and $\delta([q]_\sim, a) = [qa]_\sim$, where $[q]_\sim$ denotes the equivalence class containing q. One may conjecture that for all congruences the following equivalence holds: A satisfies the Černý conjecture if and only if the quotient automaton does. If the Černý conjecture is true then, of course, this equivalence is also true. Yet, we see no natural way to prove it, and according to our experience, this problem in general may be as hard as the Černý conjecture itself. Yet, we have attempted to find special kinds of congruences, for which the problem would be more naturally linked to the Černý conjecture and a reduction step would be possible. Here we have one easy and natural result.

Proposition 1.1 *Let $\sim$ be a congruence on a strongly connected automaton $A = \langle Q, \Sigma, \delta \rangle$ such that one of its equivalence class is a singleton. Then, A satisfies the Černý conjecture, whenever $A/\sim$ does.*

Proof: Let $|Q| = n$ and k be the number of the equivalence classes in $\sim$. We may assume that $k < n$, since otherwise the result is trivial. By assumption, there exists a word $w \in \Sigma^*$ of length $\leq (k-1)^2$ resetting $A/\sim$. This word sends all the states of A into one $\sim$-class B.

Let s be the unique element of a singleton $\sim$-class. Since A is strongly connected, there exists a word $u \in \Sigma^*$ that sends a fixed state $q \in B$ into s. Moreover, we may assume that the length $|u| \leq k-1$, since if $u = a_1 \ldots a_t$ is the shortest word with $qu = s$, then the path corresponding to applying successive letters of w visits every $\sim$-class at most once. Indeed, suppose to the contrary that $qa_1 \ldots a_i$ and $qa_1 \ldots a_j$ are in the same $\sim$-class, and $i < j < t$. Then, since $\sim$ is a congruence, $qa_1 \ldots a_i a_{j+1} j \ldots a_t = s$, a contradiction.

It follows that the word u sends all the states of the $\sim$-class B into s, and therefore uw resets A. The length $|uw| \leq (k-1)^2 + k - 1 < (n-1)^2$, as required. $\Box$

In the sequel, the argument used in this proof will be treated as routine.

2 Intervals in digraphs

Apart from the transition digraph $T = T(A)$ determined by the automaton $A\langle Q, \Sigma, \delta \rangle$, we shall consider also another digraph D on the the set of the states Q with the property that certain structures on D, called intervals, are preserved by the transition function δ of A.

Let $D = \langle Q, E \rangle$ be an arbitrary directed graph. We say that a vertex $z \in D$ *lies on a directed path* from x to y (in D) if there is a directed path $x = x_0, x_1, \ldots, x_n = y$ such that $z = x_i$ for some $i = 0, 1, \ldots, n$ and $x, y \notin \{x_1, \ldots, x_{n-1}\}$. In short, we say that the *path xy contains z*. Note that the path in question may have repeated occurrences of vertices except for end vertices x, y each of which occurs only once. In the sequel, we assume that all considered paths have this property. Only if necessary, we stress this calling such paths *singular*. (Note also that we allow trivial paths with $x = y$).

The set of all vertices z lying on a directed path between x and y will be denoted by $[x, y]$. Such a set is called a (directed) *interval* of D. Note, that by definition, if $[x, y] \neq \emptyset$, then $x, y \in [x, y]$. Note also that due to the singularity assumption on paths, even for strongly connected digraphs the intervals $[x, y]$ and $[y, x]$ usually differ from each other. For example, if D is a simple directed cycle, then the intervals yield a division of the cycle into two arcs. If D is acyclic, then one of the intervals $[x, y]$ and $[y, x]$ is empty, and the other one is the usual interval in the induced partial ordering (the transitive closure of D). The interval $[x, x]$, by definition, is the strongly connected component of the vertex x in D. In the sequel, we shall use the abbreviation *sc-component*.

We say that an automaton $A = \langle Q, \Sigma, \delta \rangle$ *respects the intervals* of a digraph D defined on Q, if for every letter $a \in \Sigma$, and all $x, y \in Q$, the following conditions holds:

(i) if $[x, y] \neq \emptyset$, then $[xa, ya] \neq \emptyset$,

(ii) if both $[x, y] \neq \emptyset$ and $[y, x] \neq \emptyset$, then $[x, y]a \subseteq [xa, ya]$,

(iii) if $xa = ya$, then one of the sets $[x, y]a$ or $[y, x]a$ has at most one element.

The first condition means that A preserves existence of a directed path between vertices. The second condition means that in case when there are directed paths between x and y in both directions, $z \in [x, y]$ implies $za \in [xa, ya]$, which means that the relation of lying on a directed path between vertices is preserved. The third condition deals with the special case when the endpoints of the interval are mapped into the same vertex. What is happening with the two intervals $[x, y]$ and $[y, x]$ in such a situation? We assume a sort of continuity: when x approaches y then one of the intervals is getting smaller while the other is getting larger.

We will consider both *strongly connected* digraphs (where for each pair of vertices x, y there exists a directed path from x to y) and *weakly connected* digraphs (where each pair of vertices is connected by some undirected path) (that is the underlying undirected graph is connected). Both the properties induce equivalence relations giving partitions into strongly connected components or weakly connected components, respectively. Note, that the condition (i) above means, in particular, that A preserves both the partition into strongly connected components of D and the partition into weakly connected components of D. Thus the corresponding equivalence relations are congruences, which will be referred to as congruences *induced* by the strongly (or weakly) connected components of D, respectively.

Lemma 2.1 *If $A = \langle Q, \Sigma, \delta \rangle$ respects the intervals of a digraph $D = \langle Q, E \rangle$, then the conditions* (i-iii) *above hold for every word w, as well* (*that is, with a replaced by w, and Σ replaced with Σ^**).

Proof: For the condition (i) the claim is obvious. For (ii), we note that the condition implies that both $[xa, ya]$ and $[ya, xa]$ are nonempty. The claim for $w = a_1 \dots a_n$ follows by successive application of (ii) for letters $a_1, \dots, a_n$. For (iii), if one of $[x, y]$ or $[y, x]$ is empty, then one of $[x, y]w$ or $[y, x]w$ is empty, as well, and thus satisfies (iii). Otherwise, successive application of (ii), yields that $[x, y]u \subseteq [xu, yu]$ for every prefix u of w. Taking u to be the largest prefix of w such that $xu \neq yu$, and applying (iii) for xu and yu, yields the required result for w. $\square$

Example. If D is a simple directed cycle, then respecting intervals means *preserving the orientation* of the cycle. Indeed, the interval $[x, y]$ consists of consecutive vertices on the cycle. Let us make use of the comments after the definition (i)-(iii). If vertices x, y, z occur on the cycle in this very order, then by (i), the relation of lying on a directed path between vertices is preserved. Conversely, if this relation is preserved, then (ii) holds, while (i) and (ii) are trivial for the cycle. If D is an *acyclic* digraph, then respecting intervals means *preserving the partial order* induced by D. Indeed, it is enough to observe that the interval $[x, y]$ is the set of all z such that $x \leq z \leq y$, that is, the usual interval of the induced partial order. If we denote this order by $\leq$, then the condition $[x, y] \neq \emptyset$ is equivalent to $x \leq y$. Thus, the condition $x \leq y$ implies $xa \leq ya$ is equivalent to (i). The condition (ii) is trivial for acyclic digraphs, and

(iii) holds since if $x \neq y$, then one of $[x, y]$ or $[y, x]$ is empty. In the remainder of the paper, we show that these are in fact the extreme cases of a general situation.

Under assumptions as above, let $\sim$ denote the equivalence relation on Q induced by sc-components of D, and let $Q' = Q/\sim$ be the quotient set. Then the relation induced on Q' by D is an acyclic digraph, which we denote by $D' = D/\sim$. The quotient automaton $A/\sim$ respects the intervals of D', that is, in view of the remark above, it preserves the partial order induced by D'. The property of respecting the intervals of a digraph may be now characterized as follows.

Lemma 2.2 *An automaton $A = \langle Q, \Sigma, \delta \rangle$ respects the intervals of a digraph D on Q if and only if $A/\sim$ preserves the partial order induced by $D/\sim$ and for all x, y belonging to the same sc-component of D the conditions* (ii) *and* (iii) *above holds.*

We say that the strongly connected components of a digraph D are *dense*, or that D is *scc-dense*, if for all x, y, z belonging to the same sc-component C of D either $z \in [x, y]$ or $z \in [y, x]$. Note that a simple directed cycle is dense in that sense. The property is not as strong as it may seem at the first sight. Let us call a vertex $z \in C$ a *check-point* for the pair $x, y \in C$ $(x, y \neq z)$ if each directed path from x to y contains z and each directed path from y to x contains z, as well.

Lemma 2.3 *A digraph D is scc-dense if and only if contains no check-point in any sc-component of D.*

Proof: Suppose first D has a check-point z in an sc-component C. So, there are $x, y \in C$ such that any directed singular path between x and y goes through z. It follows that $y \notin [z, x]$ and $y \notin [x, z]$.

Conversely, suppose that $z \notin [x, y]$. Then, one of the following holds: either (a) every path xz contains y, or (b) every path zy contains x.

Similarly, supposing that $z \notin [y, x]$, we have that either (c) every path yz contains x, or (d) every path zx contains y.

Now, (a) and (c) contradicts the fact that there is a path form x to z, while (a) and (d) means that y is a check-point. The situation for the remaining two possibilities is similar. Consequently, there is always a check-point, as required. □

Now we prove a crucial property of the automata respecting the intervals of an scc-dense digraph connected with synchronization. We will be interested in the situation when the image Xw of the subset X of Q under the word w *collapses*, by which we mean that $|Xw| = 1$.

Lemma 2.4 *Let $A = \langle Q, \Sigma, \delta \rangle$ respects the intervals of an scc-dense digraph D on Q. If X is a nonempty subset of Q, $|X| > 1$, contained in an sc-component of D such that $|Xw| = 1$, then there exist different $x, y \in X$ such that $X \subseteq [x, y]$ and the whole interval $[x, y]$ collapses under w.*

Proof: The proof is by induction on the cardinality of X. For $|X| = 2$ the claim follows trivially from the condition (iii) of Lemma 2.1. Otherwise, let us fix $z \in X$. By induction assumption, there are different $x, y \in X \setminus \{z\}$ such that $X \setminus \{z\} \subseteq [x, y]$ and $[x, y]$ collapses under w. If $z \in [x, y]$, then we are done. So, we may assume $z \notin [x, y]$.

Since D is scc-dense, it follows that $z \in [y, x]$. This means that there is a path yx containing z, and consequently, there is a path yz containing no x. This path may be added to every path xy yielding a path from x to z. It follows that $[x, y] \subseteq [x, z]$. Similarly (since there is a path zx containing no y),$[x, y] \subseteq [z, y]$.

If any of $[x, z]$ or $[z, y]$ collapses under w, we are done. Hence, we may assume, by condition (iii) of Lemma 2.1, that both $[z, x]$ and $[y, z]$ collapse under w, that is,

$$|[z, x]w| = |[y, z]w| = 1.$$

We may assume also that there are $t \in [x, z]$ and $s \in [z, y]$ such that $tw \neq zw = xw$ and $sw \neq zw = yw$.

We show that among paths xz containing t there exists one not containing y. Suppose to the contrary that each path xz containing t contains y, as well. If the segment xt of such a path (that is the part from x to t) does not contain y, then neither does the segment tz (otherwise, we would have a path xy containing t, and since by induction hypothesis $|[x, y]w| = 1$, it follows that $tw = xw$, a contradiction). Similarly, if the segment tz of such a path does not contain y, then neither does the segment xt (otherwise, we would have a path yz containing t, and since, by assumption above, $[y, z]$ collapses, we have $tw = zw$, a contradiction). Choose a path xz that contains t. Let yt and ty be the segments of this path that has only one occurrence of y, each. Let xt be a path that does not contain y. Combine it with the segment ty, we have a path from x to y that contains t, and as before, this leads to a contradiction. Similarly, Let tz be a path that does not contain y. Combine it with the segment yt, we have a path from y to z that contains t, and again, a contradiction. It follows that every path xt contains y, and every path tz contains y. Since y is not a check-point, there is a path zt not containing y, and therefore not containing x either. Similarly, there is a path tx not containing y, and therefore not containing z either. This yields a (singular) path zx containing t, which (since $[z, x]$ collapses) yields $tw = zw$, a contradiction.

In a completely analogous way we show that among paths zy containing s there exists one not containing x. Combining it with a path xz containing t and not containing y, we obtain a (singular) path xy containing z, which contradicts the assumption that $z \notin [x, y]$, and thus completes the proof. □

3 Main result

We start from a preliminary result. Let $A = \langle Q, \Sigma, \delta \rangle$ be a synchronizing automaton and let C be a subset of Q. A family $\mathcal{F} = \{X_1, \ldots, X_m\}$ of subsets of Q is called a *Černý family* for C, if for every image $Y = Cu$ by a word $u \in \Sigma^*$ and every $w \in \Sigma^*$ the following implication holds: if $|Y| > 1$ and $|Yw| = 1$, then there exists $i \leq m$ such that $Y \subseteq X_i$ and $|X_i w| = 1$. In other words, if C collapses under uw, then the image Cu, if nontrivial, may be extended to a member of $\mathcal{F}$ that still collapses under w.

Lemma 3.1 *If $\mathcal{F} = \{X_1, \ldots, X_m\}$ is a Černý family for a set $C \subset Q$, $|C| > 1$, then there exists $w \in \Sigma^*$ of length not exceeding $m = |\mathcal{F}|$ such that $|Cw| = 1$.*

Proof: Since A is synchronizing, there is a word $v = a_1 \cdots a_t$ such that C collapses under v. We assume that v is the shortest possible word with this property. Denote $Y_i = Qa_1 \cdots a_i$ for $i \in \{1, \ldots, t-1\}$, and $Y_0 = C$. Then, for all $i \leq t-1$, $|Y_i| > 1$. For each $i \in \{0, \ldots, t-1\}$ choose $Z_i \in \mathcal{F}$ such that $Y_i \subseteq Z_i$ and $|Z_i a_{j+1} \cdots a_t| = 1$. We show that if $i < j$, then $Z_i \neq Z_j$. Indeed, if $i < j$ and $Z_i = Z_j$, then we have $Ca_1 \cdots a_i = Y_i \subseteq Z_j$, and consequently, $|Ca_1 \cdots a_i a_{j+1} \cdots a_t| = 1$, contradicting the fact that v is the shortest word with this property. Thus, $t \leq m$, as required. □

Our main result is the following

Theorem 3.2 *Let $A = \langle Q, \Sigma, \delta \rangle$ be a strongly connected automaton respecting the intervals of an scc-dense digraph D on Q, and let $\sim$ denote the congruence on A induced by weakly connected components of D. Then, if $A/\sim$ satisfies the Černý conjecture, then so does A.*

Proof: Denote by n the number of strongly connected components, and by k the number of weakly connected components (wc-components). If there is a wc-component of D consisting of a single vertex, then by Proposition 1.1 the theorem is true. Hence we may assume that each wc-component has at least two vertices. Assume also that $A/\sim$ is synchronizing and satisfies the Černý conjecture. Recall that, since A respects the intervals, wc-components are mapped by transformations of A into wc-components, and sc-components are mapped into sc-components. We first show that

Claim 1. There exists a word $v \in \Sigma^*$ of length not exceeding $(n-1)^2$ such that Qv is contained in a single sc-component of D.

By assumption on $A/\sim$, there is a word w of the length at most $(k-1)^2$ that resets $A/\sim$. The word w maps all the states of A into one wc-component B of D. Since $A/\sim$ is strongly connected there is a word u of the length at most $k-1$ mapping B on any chosen wc-component B_i. In particular, if there exists a wc-component consisting of a single sc-component, we are done. Indeed, in such a case wu maps Q into a single sc-component and it has length

$$(k-1)^2 + (k-1) = (k-1)k < (n-1)^2.$$

(We note that for $k = 1$ w is simply the empty word and the argument works, as well).

Thus, we may assume that every wc-component of D has at least two sc-components. The sc-components are partially ordered by D, so we may speak of maximal and minimal sc-components. Let $B_1, \ldots, B_k$ denote the wc-components of D (this set includes B defined above). Then, by M_i we denote the number of maximal sc-components in B_i, and by m_i the number of minimal sc-components of B_i. Since each B_i has at least two sc-components, no sc-component is both maximal and minimal. Therefore $\sum_{i=1}^{k}(M_i + m_i) \leq n$. Let us define

$$p = \min\{M_i, m_i : i \in \{1, \ldots, k\}\}.$$

Then, $p \leq n/2k$. To fix attention, we may assume without loss of generality that $p = M_1$, and that the word u of length at most $k-1$, mentioned above, maps B into B_1.

Let $C_1, \ldots, C_p$ denote the maximal sc-components of B_1. We define inductively a sequence of words $u_0, \ldots, u_t$, with $t \leq p$, and such that $B_1 u_t$ is contained in a single sc-component of D. Let u_0 be the empty word. Given the word u_i, we define J_i to be the set of those $j \in \{1, \ldots, p\}$ for which none of the images $C_j u_1, C_j u_2, \ldots, C_j u_i$ is contained in a minimal sc-component of D. Further, let X_i be the set of those sc-components of D that contain $C_j u_i$ for some $j \in J_i$. In particular, we have $J_0 = \{1, 2, \ldots, p\}$ and $X_0 = \{C_1, \ldots, C_p\}$. The word u_{i+1} is now defined as follows.

We look first for a word v_{i+1} that maps at least one sc-component in X_i into some minimal sc-component of D, Such a word exists, since A is strongly connected. We may assume that the length of v_{i+1} is at most $n - (m-1) - |X_i|$, where $m = \sum_{j=1}^{k} m_i$. Indeed, let $I_1, I_2, \ldots, I_r$ be the sequence of images of an sc-component in X_i obtained by applying successive letters of word v_{i+1}. Obviously, each such image is contained in an sc-component, so we have a sequence of corresponding sc-components. We may assume that in this sequence no sc-component appears twice, no sc-component of X_i occurs, and except for the last term, no minimal sc-component occurs. This yields the length bound above. We define $u_{i+1} = u_i v_{i+1}$. Then obviously $|X_{i+1}| < |X_i|$, unless X_i is empty. It follows that X_t is empty for some $t \leq p$, and consequently, for each $j \in \{1, 2, \ldots, p\}$ there exists $i \leq t$ such that $C_j u_i$ is contained in a minimal sc-component of D.

Claim 2. The image $B_1 u_t$ is contained in a single sc-component.

Let $\preceq$ denotes the partial ordering of sc-components in D. Since B_1 is weakly connected, it is enough to show that for every pair of sc-components $Z, Y \in B_1$ such that Z covers Y in $\preceq$, the images Zu_t and Yu_t are contained in the same sc-component. To this end, let $C_j \in X_0$ be the maximal sc-component of B_1 with $Z \preceq C_j$. Now, since for some i, $C_j u_i$ is contained in a minimal sc-component, and A preserves $\preceq$, the images Zu_i and Yu_i are contained in the same minimal sc-component. Since $u_t = w_1 u_i w_2$, for some w_1, w_2, the claim follows.

Thus, the word $v = wuu_t$ maps Q into a single sc-component. Let us denote this component by C. To complete the proof of Claim 1 we need to prove now the following.

Claim 3. The length $|v| \leq (n-1)^2$.

By construction, we have

$$|v| \leq (k-1)^2 + k - 1 + \sum_{i=0}^{p-1}(n - m - p + i + 1) \leq k(k-1) + pn - kp^2 - \frac{p(p-1)}{2}.$$

(In the later inequality, we have used the fact that $m = \sum_{j=1}^{k} m_i \geq kp$).

If $p = 1$, then

$$|v| \leq k(k-2) + n \leq \frac{n}{2}\left(\frac{n}{2} - 2\right) + n \leq (n-1)^2.$$

So, we may assume that $p \geq 2$. Since $2kp \leq n$, we have

$$p(n - kp) \leq \frac{n^2}{2k}.$$

It follows that

$$|v| \leq k(k-1) + \frac{n^2}{2k}.$$

Consider the function $f(k) = k(k-1) + (n^2/2k)$. We know that $1 \leq k \leq n/2$, yet we consider it on the interval $[1, n-1]$. Since $f'(k)$ is continuous and increasing on the interval $[1, n-1]$, $f(k)$ have the maximal value, in this interval, either for $k = 1$ or for $k = n-1$. For $k = 1$, since $n \geq 2kp \geq 4$, we have

$$|v| \leq \frac{n^2}{2} < (n-1)^2.$$

For $k = n-1$, we have

$$|v| \leq (n-1)(n-2) + \frac{n^2}{2(n-1)},$$

and again, using $n \geq 4$,

$$|v| < (n-1)^2.$$

This completes the proofs of Claim 3 and Claim 1.

Now, if all the sc-components in D are trivial (one-element), then the proof of the theorem is finished. Otherwise, let N denote the number of vertices in D (states in A). Then $N > n$. If there is at least one trivial sc-component consisting of a single state q, then there is a word v_0 of length $\leq (n-1)$ mapping the sc-component C containing $B_1 u_t$ onto q. Consequently, the word vv_0 resets A and it has the length not exceeding

$$(n-1)^2 + (n-1) = n(n-1) < (N-1)^2,$$

as required. Hence, we may assume that each sc-component contains at least two vertices. Then $N \geq 2n$.

We show that there exists a small enough Černý family of sets for C. Suppose that $Y = Cu$ is an image of C by a word u. Then, Y is contained in some sc-component of D. Let w be such that $|Yw| = 1$. By Lemma 2.4, there exist $x, y \in Y$ such that $Y \subseteq [x, y]$ and $[x, y]$ collapses under w. This means that the family $\mathcal{F}$ of sets $[x, y]$ with $x \neq y$ belonging to the same sc-component in D forms a Černý family of sets for C. We estimate the cardinality $m = |\mathcal{F}|$ of this family.

Let $c_i = |C_i|$. Then $m = \sum_{i=1}^{n} c_i(c_i - 1)$. Clearly, for a fixed n and N, this sum has the maximal value when c_1 is as large as possible and the remaining values of c_i are as small as possible. Since, by assumption $c_i > 1$, we have

$$m = \sum_{i=1}^{n} c_i(c_i - 1) \leq (N - 2(n-1))(N - 2n + 1) + 2(n-1),$$

and consequently,

$$m \leq N^2 - 4Nn + 4n^2 + 3N - 4n.$$

This may be written as

$$m \leq (N-1)^2 - (n-1)^2 - (4Nn - 5n^2 - 5N + 6n).$$

The latter term in parentheses equals

$$(3N - 5n)(n-1) + Nn - 2N + n,$$

and since $N \geq 2n$ and $n > 1$, it is positive. Therefore,

$$m \leq (N-1)^2 - (n-1)^2.$$

Combining Lemma 3.1 with Claim 1 completes the proof. □

4 Corollaries and applications

First note that if an scc-dense graph D on Q is weakly connected, then $A/\!\sim$ in Theorem 3.2 has one element and trivially satisfies the Černý conjecture (see a remark at the beginning of the proof of Theorem 3.2 concerning the case $k = 1$). Therefore we have the following

Corollary 4.1 *If a strongly connected automaton $A = \langle Q, \Sigma, \delta\rangle$ respects the intervals of an scc-dense weakly connected digraph D on Q, then A satisfies the Černý conjecture.*

Obviously, a (simple directed) cycle is scc-dense, and so, as a particular case of the corollary above, we obtain Eppstein's result [6] that oriented automata (called in [6] *monotonic*) satisfy the Černý conjecture. The following is a natural generalization of the Eppstein result.

Let us call a directed graph D a digraph with *unique return paths*, if whenever there is a path from x to y in D, and there is a return path from y to x, then the latter is unique, and in consequence the former is also unique. Since we allow on paths repeated occurrences of vertices (other than end vertices), it means that on each of the paths every next step is uniquely determined until we reach the end vertex. This leads easily to the conclusion that every two cycles in D are disjoint. Thus, a digraph with unique return paths consists of a collection of disjoint cycles and, possibly, additional edges between them inducing a partial ordering on the cycles. In a sense, this is a class of digraphs next to the acyclic digraphs (and thus a natural generalization of simple cycles). Note that preserving intervals of D in this case means that cycles are mapped into cycles, orientation of vertices on each cycle is preserved and the existence of a directed path between cycles is preserved. We abbreviate it saying that the induced partial order and orientation of cycles are preserved. Then we may formulate the following simple generalization of Eppstein result.

Corollary 4.2 *Let D be a weakly connected digraph on Q with unique return paths. If a strongly connected automaton $A = \langle Q, \Sigma, \delta\rangle$ preserves the partial ordering on the cycles induced by D and orientation of the cycles, then A satisfies the Černý conjecture.*

Now, it is easy to construct examples of automata (using, for instance, Černý automata as components) that are neither orientable nor weakly monotonic and satisfy the Černý conjecture due to the corollary above.

We proceed to show that our results also include all weakly monotonic automata. This leads to a different (and perhaps simpler) way to handle weakly monotonic automata and to a generalization of these constructions. First let us recall the definition from [14]. Given an automaton $A = \langle Q, \Sigma, \delta\rangle$, a binary relation ρ on Q is *stable* if $(p, q) \in \rho$ implies $(pa, qa) \in \rho$ for all $p, q \in Q$ and $a \in \Sigma$. Then, A is called *weakly monotonic of level* $\ell \geq 1$ if there exists a strictly increasing chain of stable binary relations

$$\rho_0 \subset \rho_1 \subset \ldots \subset \rho_\ell,$$

such that ρ_0 is the equality relation, the transitive closure of ρ_ℓ is the universal relation, and for each $i = 0, \ldots, \ell - 1$ the following condition is satisfied:

($*$) the transitive closure π_i of ρ_i is contained in ρ_{i+1} and the relation ρ_{i+1}/π_i induced by ρ_{i+1} on the set of equivalence classes Q/π_i is a partial ordering.

Note that the equivalence classes of the transitive closure of a partial ordering relation τ are just the weakly connected components of any digraph D inducing τ. Recall that if $A = \langle Q, \Sigma, \delta\rangle$ preserves the partial order τ (defined on Q) then the weakly connected components of τ form a congruence on A. It is natural to write simply A/τ to denote the corresponding quotient automaton. Then, we may define weakly monotonic automata by recursion as follows.

(i) The trivial automata with one state are weakly monotonic of level 0;

(ii) for $\ell > 0$, $A = \langle Q, \Sigma, \delta \rangle$ is a weakly monotonic of level ℓ, if there exists a partial order τ on Q, such that A/τ is a weakly monotonic automaton of level $\ell - 1$.

$A = \langle Q, \Sigma, \delta \rangle$ is a weakly monotonic automata of level 1, if if there exists a *weakly connected* partial order τ on Q preserved by A;

It should be clear that in both the definitions the classes of weakly monotonic automata of level not exceeding ℓ coincide. In particular, the weakly monotonic automata of level 1 are just the automata preserving a *connected* partial order. The fact that each strongly connected weakly monotonic automaton of level ℓ satisfies the Černý conjecture follows now by ℓ-fold application of Theorem 3.2. We note, that Volkov [14] proved this result for all (not necessarily strongly connected) weakly monotonic automata. This can be also obtained using the proof of Theorem 3.2 (since the assumption that the automaton in question is strongly connected is necessary only for the case when D has cycles). It should be noted however, that in [14], for strongly connected automata a stronger bound for a reset word is established. It has been also observed in [14] that Trahtman [12] proved that each aperiodic automaton preserves a nontrivial partial order, and therefore each such automaton is weakly monotonic (the latter can be seen immediately from our recursive definition).

These observations may be generalized for strongly connected automata as follows. For an automaton $A = \langle Q, \Sigma, \delta \rangle$ respecting the intervals of a digraph D, by A/D we denote the quotient automaton of the congruence induced by the weakly connected components of D. For an arbitrary class of strongly connected automata $\mathcal{C}$, we define recursively the class $I_\ell(\mathcal{C})$:

(i) $I_0(\mathcal{C}) = \mathcal{C}$;

(ii) for each $\ell > 1$, $I_\ell(\mathcal{C})$ is the class of all strongly connected automata $A = \langle Q, \Sigma, \delta \rangle$ such that, for some digraph D on Q, A respects the intervals of D and $A/D \in I_{\ell-1}(\mathcal{C})$.

Our main result Theorem 3.2 yields

Corollary 4.3 *If $\mathcal{C}$ is a class of strongly connected automata satisfying the Černý conjecture, then every automaton $A \in I_\ell(\mathcal{C})$, for some $\ell \geq 0$, satisfies the Černý conjecture.*

In particular, if $\mathcal{C}_0$ consists of one-element automata, then the class $I_\ell(\mathcal{C}_0)$ contains, in particular, all strongly connected weakly monotonic automata of level ℓ. Yet, one may start from a broader class of automata $\mathcal{C}$ for which the Černý conjecture has been already verified. Then, one may easily construct many new examples of strongly connected automata not covered by the results on the Černý conjecture established so far.

References

[1] J. Almeida, S. W. Margolis, B. Steinberg, and M. V. Volkov, Representation theory of finite semigroups, semigroup radicals and formal language theory Trans. Amer. Math. Soc. 361 (2009), 1429-1461.

[2] D. S. Ananichev, M. V. Volkov, Synchronizing monotonic automata, Theor. Comput. Sci. 327, no.1 (2004), 225-239 (DLT 2003, LNCS 2710 (2003), 111-121).

[3] D. S. Ananichev, M. V. Volkov, Synchronizing generalized monotonic automata, Theor. Comput. Sci. 330(1) (2005), 3-13.

[4] J. Černý. *Poznámka k. homogénnym experimentom s konecnými automatmi*, Mat. fyz. čas SAV 14 (1964) 208-215.

[5] L. Dubuc, Les automates circulaires et la conjecture de Černý, Inform. Theor. Appl. 32 (1998), 21-34.

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

[7] J. Kari. Synchronizing finite automata on Eulerian digraphs, Theor. Comput. Sci. 295 (2003), 223-232 (MFCS 2001, LNCS 2136 (2001), 432-438).

[8] A. Mateescu, A. Salomaa, Many-valued truth functions, Černý's conjecture and road coloring, EATCS Bull. 68(1999), 134-150.

[9] J.-E. Pin, Sur un cas particulier de la conjecture de Černý, Lect. Notes Comput. Sci. 62 (1978), 345-352.

[10] B. Steinberg, The Černý conjecture for one-cluster automata with prime length cycle, Theoret. Comput. Sci. 412(39) (2011), 5487-5491.

[11] A. N. Trahtman, An efficient algorithm finds noticeable trends and examples concerning the Černý conjecture, MFCS 2006, Lect. Notes Comput. Sci. 4162 (2006),789-800.

[12] A. N. Trahtman, The Černý Conjecture for Aperiodic Automata, DMTCS 9(2) (2007), 3-10.

[13] M. V. Volkov, Synchronizing automata and the Černý conjecture, Lect. Notes in Comput. Sci. 5196 (2008), 11-27.

[14] M. V. Volkov, Synchronizing automata preserving a chain of partial orders, Theor. Comput. Sci. 410(37) (2009), 3513-3519 (CIAA 2007, LNCS 4783 (2007), 27-37).