Automata Specialities:

Černý Automata

David Casas

Departamento de Matemáticas
Universidad Nacional de Colombia

J. Andrés Montoya

Departamento de Matemáticas
Universidad Nacional de Colombia

Copyright © 2018 David Casas and J. Andrés Montoya. This article is distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Abstract

We study the following question: what does make Černý automata such a singular set of automata? We give some partial answers.

Mathematics Subject Classification: 68R01

Keywords: Automata synchronization

1 Introduction

We have been interested in automata synchronization for a long period of time. We have tried different approaches in order to attack the famous Černý Conjecture [6]. Most of those approaches have led us to nothing. The few remaining approaches have showed us that Černý automata are very much more special than it was originally conjectured. We want to tell a part of this story in this paper. We refer the reader to [18] for a pedagogical introduction to automata synchronization and Černý conjecture.

Organization of the work. This work is organized into four sections. In section 1 we introduce the basic notions of automata synchronization. In
section 2 we introduce Černý automata and we discuss some special properties of them. In section 3 we study the holonomy decomposition of Černý automata [14]. We finish in section 4 with some concluding remarks.

2 Synchronization of Automata and The Černý Conjecture

Let us begin with the basic definition of deterministic finite state automata (DFA’s).

Definition 2.1 A finite state automaton is a triple $A = (Q, \Sigma, \delta)$ such that:

1. $Q$ is a finite set, the set of states of $A$.
2. $\Sigma$ is a finite alphabet, the input alphabet of $A$.
3. $\delta$, the transition function of $A$, is a function from $Q \times \Sigma$ in $Q$.

We use the symbol $\hat{\delta}$ to denote the transitive closure of $\delta$, which is the extension of function $\delta$ to the set $Q \times \Sigma^*$. Function $\hat{\delta}$ is recursively defined by

\begin{align*}
\hat{\delta}(p, w_1) &= \delta(p, w_1), \\
\hat{\delta}(p, w_1 \cdots w_n) &= \hat{\delta}(\delta(p, w_1), w_2 \cdots w_n).
\end{align*}

We say that automaton $A$ is synchronizing, if and only if, there exists a string $w$ such that for all $p, q \in Q$ the equality

$$\hat{\delta}(p, w) = \hat{\delta}(q, w)$$

holds. We say in the latter case that $w$ is a reset word for $A$.

The question about the length of the minimal reset words seems to be a very hard question. Jan Černý published in 1964 the first of a series of papers related to this question [5]. He constructed a sequence $\{C_n\}_{n \geq 1}$ of synchronizing automata such that for all $n \geq 1$ the shortest reset length of the $n$-state automaton $C_n$ is equal to $(n - 1)^2$. The aforementioned series of works finished with the paper [6], published in 1971, and which contains the first formulation of the famous Černý Conjecture. The latter conjecture states that the synchronizing time (the shortest reset length) of any $n$-state synchronizing automaton is upperbounded by $(n - 1)^2$. The best (known) upper bound for the shortest reset length, registered in the literature, is the cubic bound of Pin, which is equal to $\frac{n^3 - n}{6}$, and which was proved in 1983 [16]. It has been proved since then that quadratic upper bounds hold for many different classes
of automata, as for example Eulerian [13], circular [7], and aperiodic automata [17]. The interested reader can consult the excellent survey by Volkov [18]. Černý Conjecture states that the automata in the sequence \( \{C_n\}_{n \geq 1} \) are the hardest to synchronize synchronizing automata. Notice that the conjecture is pointing out an extremal (unproved) property of those automata which makes them a very a special set of automata. The status of the conjecture has been open for almost fifty years, and we only know that the sequence \( \{C_n\}_{n \geq 1} \) is the only known sequence of automata achieving the worst known synchronizing times. We think that the latter fact makes Černý automata a very special sequence of extremal automata, but we think that those automata are very much more special than that.

3 Where Do Černý Automata Come From?

Černý conjectured that the automata in the sequence \( \{C_n\}_{n \geq 1} \) are the hardest to synchronize automata. It is natural to ask: where do those automata come from? How did Černý arrive to the definition (construction) of those automata? We cannot give a conclusive answer to the latter two questions, but we think that the origin of Černý automata is related to the following facts.

Given a \( n \)-state synchronizing automaton \( M \), one can synchronize it using a naive strategy that we call pair synchronization. The latter strategy reduces the synchronization of \( M \) to a sequence of no more than \( n - 1 \) rounds, at each round he focuses on synchronizing two states. Given \( p,q \in Q \) we use the symbol \( st(p,q,M) \) to denote the synchronizing time of the pair \( p,q \). The synchronizing time of \( M \), denoted by \( st(M) \), satisfies the inequalities

\[
st_2(M) \leq st(M) \leq (n - 1) \cdot st_2(M),
\]

where \( st_2(M) \) is equal to \( \max_{p,q \in Q} \{ st(p,q,M) \} \). The latter fact has an important consequence: if one wants to construct a sequence of slowly synchronizing automata [1], he must think of constructing a sequence of automata that contain many hard to synchronize pairs of states. It is easy to prove that for any \( n \)-state synchronizing automaton the inequality

\[
st_2(M) \leq \frac{n(n - 1)}{2}
\]

holds [15]. Can one construct a sequence of automata meeting the above upper bound? Suppose that \( M \) is a \( n \)-state automaton \( M_n \) satisfying the equality
we have that $\mathcal{M}$ must exhibit the following singular feature:

there exists a pair of states that is transformed in all the other pairs before it gets synchronized. We think that the canonical construction of a $n$-state automaton exhibiting such a singular feature is the following one:

- Use the $n$ states labelled $1,\ldots,n$ to built a directed cycle of length $n$, whose arrows are colored with the letter $a$, and which are directed according to the cyclic order $1 \leq \cdots \leq n \leq 1$.

- Add a loop colored with the letter $b$ to any node in the set $\{2,\ldots,n\}$. Add an arrow $(1,2)$ and color it with the same letter $b$.

We use the symbol $\mathcal{C}_n$ to denote the synchronizing automaton that is obtained from the above construction, and which is equal to the $n$-th Černý automaton [5].

Observe that the synchronization of any pair of states of $\mathcal{C}_n$ can only be achieved by a careful alternation of $a$-rotations and $b$-collapses. The $b$-collapses are used to reduce, by one, the distance between the pair of states that is being synchronized. The $a$-rotations are used to lead the automaton towards a configuration for which a $b$-collapse can effectively reduce the latter distance. Any pair of states of $\mathcal{C}_n$ is determined by the distance between its two states and the position of the state that is clockwise closest to $1$. We have, for instance, that the pair $\{2,\lceil \frac{n}{2} \rceil + 1\}$ is completely determined by the parameters $\lceil \frac{n}{2} \rceil$ and $1$. Notice that $\lceil \frac{n}{2} \rceil$ is the largest possible distance between a pair of states. Suppose that one wants to synchronize the pair $\{2,\lceil \frac{n}{2} \rceil + 1\}$. We observe that:

- The distance between the above two states must be decreased from the maximum possible distance to 0 (the pair must visit all the possible distances before it gets synchronized).

- After one (useful) application of letter $b$ the distance between the pair gets decreased by one, and the clockwise closest state becomes equal to $2$. Then, if one wants to decrease the latter distance, once again, he is forced to transform state $2$ into state $1$, and it requires a full clockwise rotation. Along this rotation the clockwise closest parameter assumes all the possible values.

We can conclude, from the above two facts, that

$$st_2 \left( \mathcal{M}_n, \mathcal{C}_n \right) = \frac{n(n-1)}{2}.$$
the hardest possible pairs. However, it seems that this was not the origin of Černý automata, because it seems that Černý was not aware of the inequality 

\[ st_2 (\mathcal{M}) \leq \frac{n(n-1)}{2} \]

We are strongly convinced of the canonicity of the above construction, so much so that once upon a time we conjectured that it was the only possible construction

**Conjecture 3.1** Let \( \mathcal{M} \) be \( n \)-state binary automaton satisfying the equality 

\[ st_2 (\mathcal{M}) = \frac{n(n-1)}{2} \]

then the automaton \( \mathcal{M} \) is isomorphic to \( C_n \).

### 3.1 Towards a Proof of the Conjecture, and a Refutation of it

**Notation 3.2** Given a set \( A \), and given \( i \leq |A| \) we use the symbol \( \mathcal{P}^{=i} (A) \) to denote the collection of all the subsets of \( A \) whose size is equal to \( i \).

We strongly believed in the true of our conjecture and we began to work hard on it. To begin with, we observed that:

Given a \( n \)-state binary automaton \( \mathcal{M} \) such that 

\[ st_2 (\mathcal{M}) = \frac{n(n-1)}{2} \]

a pair \( p, q \in Q \) such that 

\[ st_2 (p, q, \mathcal{M}) = \frac{n(n-1)}{2} \]

and given \( w \in \{a, b\}^{\frac{n(n-1)}{2}} \) a shortest reset word for the pair \( p, q \), we could define a bijection \( f_w : \{1, ..., \frac{n(n-1)}{2}\} \rightarrow \mathcal{P}^{=2} (Q) \) as follows

\[ f_w (i) = \left\{ \tilde{\delta} \left( p, w[1, ..., i-1] \right), \tilde{\delta} \left( q, w[1, ..., i-1] \right) \right\}. \]

Notice that \( f_w \) induces a linear order over the set \( \mathcal{P}^{=2} (Q) \), a linear order that ranks the pairs of states of \( \mathcal{M} \) according to their synchronizing time. Let \( \{r, s\} = f_w \left( \frac{n(n-1)}{2} \right) \). We have that \( \{r, s\} \) is the only pair of states that can be synchronized with the application of only one letter. We got that there is only one state of \( \mathcal{M} \) which has more than one ingoing edges labeled with the same letter.

The beginning seemed to be promising. We had that the transition graph of one of the two actions (letters) was a disjoint union of cycles. And we had that the transition graph of the second action was almost the same, except that this graph also contains a cycle with a path (tail) appended to it. We feel, at that point, that we was already close to Černý automata (to the proof of our conjecture). We also feel that we had to study in more detail the cyclic structure of the transformation semigroup of \( \mathcal{M} \). The analysis of those cyclic structures led us to discover the theory of Krohn-Rhodes (see [14]) as well as a counterexample to our conjecture. The counterexample is a binary automaton \( \mathcal{M} \) whose set of states is equal to \( \{1, 2, 3, 4\} \). Moreover, we have that the letter \( a \) induces a permutation that acts cyclically over the set \( \{1, 2, 4\} \) and fixes the
state 3, while the letter b fixes the state 1, sends 2 to 3, and acts cyclically over the pair \{3, 4\}. We have that \(\mathcal{M}\) is not circular, and as a consequence, it cannot be isomorphic to \(C_4\). It is easy to check that

\[
st_2(2, 3, \mathcal{M}) = 6 = \frac{4(3)}{2}.
\]

There are only five examples, registered in the literature, of binary automata that are not isomorphic to a Černý automaton and which achieve Černý bound for the synchronizing time (see [18] and the references therein). We realized, soon, that \(\mathcal{M}\) was one of those five automata. We checked the remaining four examples, and none of them is a counterexample. It seems that automaton \(\mathcal{M}\) is, up to the date, the only known counterexample to our conjecture. We have to ask: are there infinite many counterexamples? We also ask:

**Solution 3.3** Does the equality \(st_2(\mathcal{M}) = \frac{n(n-1)}{2}\) imply that \(st(\mathcal{M}) = (n-1)^2\)?

## 4 Krohn-Rhodes Theory and Černý Automata

As we said before, we have been interested in automata synchronization for long time, and we have tried many different approaches to study the synchronizing times of different classes of automata. One of those approaches was related to Krohn-Rhodes Theory (KR-theory, for short).

One of the most basic and ubiquitous ideas in mathematics is the idea of prime decomposition. It tells us that one can try to represent a complex structure as an amalgamation (product) of simpler (prime) objects, and that he can study the factors of such a construction in order to deduce some structural properties of the decomposed structure. There are many examples of this:

- Any natural number is a prime or a product of prime numbers, and some of the properties of the composite numbers can be deduced from their prime factors.

- Any finite abelian group is isomorphic to a Cartesian product of finite cyclic groups, and some of the properties of the non-cyclic groups can be deduced from the structure of its cyclic factors.

Keneth Krohn and John Rhodes proved in 1968 a structure theorem for semigroups (and hence for automata) [14]. The KR-Theorem is not as simple as the aforementioned examples, but given the lack of structure in semigroups
it is a big and (possibly) helpful achievement. We considered the following question: can one use KR-theory to study the synchronizing time of automata? The latter question was the motivating question behind the research work developed by the first author in his master degree thesis [4]. We discover that Černý automata can be used to illustrate KR-theory. It happens that the holonomy decompositions of Černý automata have a very pleasant structure, and it also happens that those decompositions are easy to compute. We argue that the latter fact is not a minor one. The reader must take into account that KR-theory is a demanding chapter of automata theory, a chapter that is not easy to survey because of several reasons: the intermediate constructions are hard to grasp, and the decompositions are hard to compute and give place to very large structures.

There are many different formulations of the KR-Theorem (see for example [10]). We have chosen to work with the alternative presentation given by Egri-Nagy and Nehaniv [9], which is related to the development of a software tool, implemented in the computer algebra system GAP (see [11]), and which can be used to effectively compute the decomposition of moderately large semigroups and automata. The aforementioned algorithmic tool is called SgpDec (see reference [8]).

4.1 Automata and the Wreath Products of Semigroups

We say that a pair $X = (Q, S)$ is a transformation semigroup, if and only if, $Q$ is a finite set of states and $S$ is a semigroup that acts on $Q$. We represent the action of $s \in S$ over $q \in Q$, as $q \cdot s$.

Let $A = (Q, \Sigma, \delta)$ be a DFA. Notice that $(\Sigma^*, \circ)$ is a semigroup, where $\circ$ denotes the concatenation operation. The transition function of $A$ allows us to think of the pair $(Q, (\Sigma^*, \delta))$ as a transformation semigroup, the transformation semigroup of automaton $A$ that is defined by the following action:

Given $p \in Q$ and given $w \in \Sigma^*$, the action $p \cdot w$ is defined as $\hat{\delta}(p, w)$.

We use the symbol $S_A$ to denote the latter transformation semigroup.

**Remark 4.1** We denote the action of $w$ on $p$ by the symbol $p \cdot w$, and given $A = \{q_1, ..., q_n\}$ we use the symbol $A \cdot w$ to denote the set $\{q_1 \cdot w, ..., q_n \cdot w\}$

From now on we study the Holonomy decomposition of finite state automata [9]. Let us begin introducing some basic concepts of the theory of transformation semigroups.

**Definition 4.2** Let $A = (Q, S)$ and $B = (P, T)$ be two transformation semigroups, we say that $A$ divides $B$ ($A \mid B$, for short), if and only if, there is a subset $R \subseteq P$ and a sub-semigroup $U \subseteq T$ such that:
• \((R, U)\) is a transformation semigroup i.e. for all \(r \in R\) and \(u \in U\) we have that \(u \cdot r \in R\).

• There are two surjective functions \(\theta : R \to Q\) and \(\phi : U \to S\) such that \(\phi\) is a semigroup homomorphism, and both mappings preserve the action i.e. for all \(r \in R\) and for all \(u \in U\) the equality \(\theta(r \cdot u) = \theta(r) \cdot \phi(u)\) holds.

It is important to remark that most automata are not isomorphic to their KR-decompositions. The theorem states (see below) that any automaton divides its decomposition, and it happens that those decompositions can be very much larger than the decomposed automata. This latter fact is a serious drawback of the theorem.

**Definition 4.3** Let \(((Q_1, S_1), ..., (Q_n, S_n))\) be a finite tuple of transformation semigroups. Given \(i \in \{1, ..., n\}\), we say that \(d_i\) is a dependency function of level \(i\), if and only if, \(d_i\) is a function from \(Q_1 \times \cdots \times Q_{i-1}\) to \(S_i\). If \(i = 1\), we have that \(d_1\) is a function from \(\emptyset\) to \(S_1\). A tuple \((d_1, ..., d_n)\) of dependency functions is called a cascade. Let \(V\) be a set of cascades, the cascade product determined by \(V\) is the transformation semigroup \((Q_1, S_1) \wr V \cdots \wr V (Q_n, S_n)\) defined by:

• The set of states is the set \(Q_1 \times \cdots \times Q_n\).

• The set of functions acting on \(Q_1 \times \cdots \times Q_n\) is a set \(\hat{V}\) that is determined by \(V\). Before defining the set \(\hat{V}\) we have to define the action of a cascade \((d_1, ..., d_n) \in V\). Let \((q_1, ..., q_n)\) be a state, we set

\[
(q_1, ..., q_n) \cdot (d_1, ..., d_n) = (q_1 \cdot d_1(\emptyset), q_2 \cdot d_2(q_1), ..., q_n \cdot d_n(q_1, ..., q_{n-1})).
\]

The composition of two cascades corresponds to sequential composition: first acts the cascade on the left, and then the cascade on the right. The set \(\hat{V}\) is the closure (under compositions) of the set \(V\).

If \(V\) is the set of all the possible cascades we say that the later cascade product is the full wreath product of the semigroups \((Q_1, S_1), ..., (Q_n, S_n)\).

Let us begin to introduce some of the concepts that are specific of the KR-theory, we use the special case of Černý automata to illustrate those concepts. To begin with we fix an automaton \(A = (Q, \Sigma, \delta)\).

**Definition 4.4** The set

\[
I_A := \{Q \cdot s : s \in \Sigma^*\} \cup \{Q\} \cup \{\{q\} : q \in Q\},
\]

is called the extended set of images of \(A\).
Example 4.5 It is easy to check that $I_{cn}$ is equal to $\{Q \cdot s : s \in \Sigma^*\}$ (see below), and it is easy to check that the latter set is equal to the set constituted by all the non-empty subsets of $\{1, \ldots, n\}$. The latter feature of Černý automata is not a minor one, it tells us that Černý automata are examples of completely reachable automata (see [3]), and it will have important consequences in the computation of the KR-decompositions.

Definition 4.6 The subduction relation determined by $A$ is a binary relation $\leq_A \subset \mathcal{P}(Q) \times \mathcal{P}(Q)$ that is defined by

$$H \leq_A K, \text{ if and only if, there exists } s \in \Sigma^* \text{ such that } H \subseteq K \cdot s.$$ 

Example 4.7 It can be proved (see below) that given $A, B \subseteq \{0, \ldots, n - 1\}$, the relation $A \leq_{cn} B$ holds, if and only if, $|A| \leq |B|$.

Let $\approx_A$ be the binary relation given by

$$H \approx_A K, \text{ if and only if, } H \leq_A K \text{ and } K \leq_A H,$$

we have that $\approx_A$ is an equivalence relation.

Example 4.8 We have that $A \approx_{cn} B$, if and only if, the equality $|A| = |B|$ holds. Thus, given $k \leq n$, we have that all the subsets of size $k$ are equivalent for the relation $\approx_{cn}$. The latter fact implies that the holonomy transformation semigroup of level $k$ is small (constituted by a small number of pieces), see below.

Definition 4.9 Let $H, K \in I_A$, and suppose that $H \subseteq K$, we say that $H$ is a tile of $K$, if and only if, it is a maximal proper subset of $K$ in $I_A$, that is: $K \in I_A$, and given $L \in I_A$ such that $H \subseteq L \subseteq K$, we have that $H = L$. We use the symbol $T^A_K$ to denote the set of tiles of $K$.

Example 4.10 Given $K \in I_{cn}$, the set of tiles of $K$ is constituted by all the maximal subsets of $K$.

Notation 4.11 We use the symbol $M_A$ to denote the transformation monoid that is generated from $A$ by adding an identity transformation.

The notion of stabilizer used in the KR-theory is similar to the notion that is used in group theory.

Definition 4.12 Let $K \in I_A$, the stabilizer of $K$, denoted with the symbol $St^A_K$, is the subset of $M_A$ constituted by the strings that preserve the tiles of $K$, that is: if $w \in St^A_K$ and $H \in T^A_K$, then $H \cdot w \in St^A_K$. 
Suppose that \( w \in \text{St}^A_K \), string \( w \) acts as a permutation on \( \mathcal{T}^A_K \). We use the symbol \( G^A_K \) to denote the group of permutations of \( \mathcal{T}^A_K \) that is generated by \( \text{St}^A_K \). The transformation group \( (\mathcal{T}^A_K, G^A_K) \) is called the holonomy transformation group of \( K \). It is important to observe that \( G^A_K \) is a subgroup of \( \mathcal{M}_A \).

**Example 4.13** Let \( K = \{2, 3, 4\} \), we know that \( \mathcal{T}^C_K \) contains the tiles
\[
\{2, 3\}, \{2, 4\}, \{3, 4\}.
\]

Notice that
\[
\{2, 3\} \cdot ab = \{3, 4\}, \quad \{3, 4\} \cdot ab = \{2, 4\} \quad \text{and} \quad \{2, 4\} \cdot ab = \{2, 3\}.
\]

It is easy to check that the holonomy group of \( K \) is generated by \( ab \), and it is isomorphic to \( \mathbb{Z}_3 \).

**Definition 4.14** Let \( h_A : I_A \to \mathbb{N} \) be the function defined by:

1. \( h_A (\{q\}) = 0 \) for all \( q \in Q \).
2. If \( |K| > 1 \) then \( h_A (K) \) is defined as
\[
\max \{ k \in \mathbb{N} : \text{there exists a sequence } K_1 <_A \cdots <_A K_k = K \land |K_1| > 1 \}.
\]

The function \( h_A \) is called the height of \( A \).

**Example 4.15** Recall that the subduction relation in \( I_C_n \) is equal to the containment relation. Therefore, we have that for all \( 3 \leq k \leq n \) and for all \( K \in \mathcal{P}^=k (\{1, \ldots, n\}) \) the equality \( h_{C_n} (K) = k - 1 \) holds.

Let \( A(k) \) be the subset of \( I_A \) constituted by the elements of height \( k \). Suppose that \( \frac{A(k)}{\approx_A} = \{B_1, \ldots, B_{j_k}\} \), which means that \( B_1, \ldots, B_{j_k} \) is a full list of representatives of the set \( A(k) \). Set
\[
\mathcal{H}^A_k = \left( \mathcal{T}^A_{B_1} \sqcup \cdots \sqcup \mathcal{T}^A_{B_{j_k}} \sqcup \{*\} ; \mathcal{G}^A_{B_1} \sqcup \cdots \sqcup \mathcal{G}^A_{B_{j_k}} \right),
\]

where given a subset \( W \) of \( \pm^* \), the symbol \( W \) denotes the transformation semigroup that is generated by \( W \) after adding to it all the constant transformations. The action of \( \alpha \in \mathcal{G}^A_{B_j} \) on \( v \in \mathcal{T}^A_{B_1} \sqcup \cdots \sqcup \mathcal{T}^A_{B_{j_k}} \sqcup \{*\} \) is defined by
\[
v \cdot a = \begin{cases} v \cdot a, & \text{if } v \in \mathcal{T}^A_{B_j} \\ v, & \text{otherwise} \end{cases}.
\]
The semigroup $H_k^A$ is called the \textit{holonomy transformation semigroup of level $k$}.

We have already introduced all the concepts that must be introduced before stating the chosen version of the Krohn-Rhodes Theorem (the version that was worked out by Egry-Nagy and Nehaniv [9]). We would like to observe that all the concepts introduced so far can be suitably illustrated when one considers the special case of Černý automata.

**Theorem 4.16** Let $A$ be a DFA, automaton $A$ divides a cascade product of the holonomy transformation semigroups $H_k^A,...,H_1^A$.

**Definition 4.17** Let $A$ be an automaton, and let $H_k^A,...,H_1^A$ be its holonomy semigroups. The full wreath product of $A$, denoted with the symbol $F(A)$, is the full wreath product of the semigroups $H_k^A,...,H_1^A$.

**Example 4.18** It can be easily checked that $F(C_3) \simeq ([3], \mathbb{Z}_3) \wr ([2], \mathbb{Z}_2)$.

### 4.2 The Full Wreath Product of Černý Automata.

Computing the holonomy decomposition of $A$ demands the construction of its full wreath product. This is a first major obstacle for the teaching, and for the effective application of the theory, given that most of those products are neither easy to compute nor can be succinctly described. This is not the case if $A$ is a Černý automaton.

Let $n \geq 2$ and let $K \subseteq \{1,...,n\}$, we have that $h_{C_n}(K) = |K| - 1$. Moreover, we have that all the subsets of height $k$ are equivalent under the relation $\approx_A$ if $|K| = k$, we can represent $K$ as the set $\{1,...,k\}$. Furthermore, we have that $T_{K_{C_n}}$ contains all the subsets of $K$ of size $k - 1$. Notice that each one of those subsets can be represented by the excluded element, and it means that $T_{K_{C_n}}$ can be represented by the set $\{1,...,k\}$. It can be checked that $G_{K_{C_n}}$ is isomorphic to $\mathbb{Z}_k$ (see below). We get that

$$H_k^A = ([k+1], \mathbb{Z}_{k+1}),$$

where $[i]$ is equal to the set $\{1,...,i\}$. We get that the full wreath product of $C_n$ is equal to the full wreath product of the transformation semigroups $([n], \mathbb{Z}_n),...,([2], \mathbb{Z}_2)$. The latter fact answers a question posed by Berstel et al [2], who observed that for $n = 2,3,4,5$ the equality

$$F(C_n) = ([n], \mathbb{Z}_n) \wr \cdots \wr ([2], \mathbb{Z}_2)$$

holds, they asked if this equality holds for all $n \geq 2$. We answer the latter question in the affirmative.
Notation 4.19 An action on \(\{1,\ldots,n\}\) is represented by a tuple \([t_1,\ldots,t_n]\) indicating that state \(i\) is sent to state \(t_i\).

Proposition 4.20 For all \(n\), the set \(\mathcal{I}_{\mathcal{C}_n}\) is equal to \(\mathcal{P}([n]) \setminus \emptyset\).

Proof. We must show that for all nonempty subset \(A \subset [n]\) there is a word \(w_A\) such that \([n] \cdot w_A = A\).

To begin with we notice that, given \(k \leq n\), it is fairly easy to transform the set \(\{1,\ldots,n\}\) into the set \(\{1,\ldots,k\}\). Suppose \(k < n\). First at all we apply letter \(b\), obtaining in this way the set \(\{2,\ldots,n\}\). Then, we apply the word \(a^{n-1}\) and we get the set \(\{1,\ldots,n-1\}\). We can continue in a similar way until we get the set \(\{1,\ldots,k\}\). Thus, it is enough to prove that for all \(A, B \subset \{1,\ldots,n\}\) such that \(|A| = |B| = k\) there exists a string \(w_{AB}\) for which \(A \cdot w_{AB} = B\). Let us suppose that \(A = \{q_1,\ldots,q_k\}\) and \(B = \{p_1,\ldots,p_k\}\). We can also suppose, without loss of generality, that \(p_1 < \ldots < p_k\). Observe that if there exists a permutation \(\pi \in S_k\) such that for all \(1 < j < k\) the equality

\[p_j - p_{j-1} \equiv (q_{\pi(j)} - q_{\pi(j-1)}) \mod n\]

holds, then there exists \(t \leq n\) such that for all \(i \leq k\) the equality \(q_{\pi(i)} \cdot a^t = q_i\) also holds. We get that, in this special case, the equality \(A \cdot a^t = B\) holds.

Now we suppose that the latter permutation does not exist. We can suppose that \(q_1 < \ldots < q_k\). Let \(q_i\) be the first element such that \(p_i - p_{i-1} \neq q_i - q_{i-1}\). If \(p_i - p_{i-1} < q_i - q_{i-1}\), we can find a string \(u\) such that

\[p_i - p_{i-1} = q_i \cdot u - p_{i-1} \cdot u,
\]

However, we have to take into account that the application of \(u\) alters the distance between \(q_{i-1}\) and \(q_{i-2}\) (if possible) by increasing it. We can fix this problem by repeating the previous process. Now, it is clear how to proceed in order to go back to the previous situation, that is: there exists \(w\) such that

\[p_i - p_{i-1} \equiv (q_i \cdot w - q_{i-1} \cdot w) \mod n.
\]

Thus, there exists \(t \leq n\) such that \(A \cdot wa^t\) is equal to \(B\). 

We observe that the above proof allows us to get some additional results:

1. The subduction relation is equal to the subset relation for the special case of Černý’s automata.
2. Given \(K \subset \{1,\ldots,n\}\), we have that \(h_{\mathcal{C}_n}(K) = |K| - 1\).
3. The tiles of \(K\) are all its subsets of size \(|K| - 1\)
4. Two sets of the same size are \(\approx_{C_n}\)-equivalent, and it implies that there
is only one representative for each height level.

For all \(k \leq n - 1\) we can choose the set \(\{1, ..., k + 1\}\) as the representative
of height \(k\). We know that the set of tiles of \(\{1, ..., k + 1\}\) is equal to the set
\[
P^=_{k}([k + 1]) = \{A \subseteq \{1, ..., k + 1\} : |A| = k\}.
\]

Observe that the size of \(P^=_{k}([k + 1])\) is equal to \(k + 1\). Moreover, there
exists a natural correspondence between \(P^=_{k}([k + 1])\) and \([k + 1]\) : given \(A \in P^=_{k}([k + 1])\) we identify the set \(A\) with its hole, where the hole of \(A\) is equal
to \([k + 1] \setminus A\). Thus, we have that the holonomy semigroup at level \(k\) is equal
to \(\left([k + 1] \cup \{*\}, G_{C_n}^{\{1, ..., k+1\}}\right)\), where \(G_{C_n}^{\{1, ..., k+1\}}\) is the stabilizer of the set of
tiles of \(\{1, ..., k + 1\}\). It remains to compute the transformation semigroup
\(G_{C_n}^{\{1, ..., k+1\}}\).

**Theorem 4.21** \(G_{P^=_{k}([k + 1])}^{C_n}\) is isomorphic to \(\mathbb{Z}_{k+1}\) and the transformation semigroup
\[
\left(\left(P^=_{k}([k + 1]) \cup \{*\}, G_{C_n}^{\{1, ..., k+1\}}\right)\right)
\]
is isomorphic to \(\left([k + 1] \cup \{*\}, \mathbb{Z}_{k+1}\right)\).

We split the proof of the above theorem into a series of lemmata.

Let \(f\) be an action that belongs to \(G_{C_n}^{\{1, ..., k+1\}}\), it follows from the definition
of stabilizer that there exists a string \(w_f\) representing this action, and which
acts as a permutation on the set of tiles of \(\{1, ..., k + 1\}\). Thus, If one wants
to compute the semigroup \(G_{C_n}^{\{1, ..., k+1\}}\), he has to determine the set of strings
fulfilling the latter condition as well as the actions that are represented by
those strings. Let us use the term \([k + 1]-\)strings to denote those strings. It follows from the definition of the stabilizer that \(w\) is a \([k + 1]-\)string, if and only if, the equality \(\{1, ..., k + 1\} \cdot w = \{1, ..., k + 1\}\) holds.

**Example 4.22** String \(a^n\) is a \([k + 1]-\)string that represents the identity
action on \(\{1, ..., k + 1\}\).

Let \(S_{k+1}\) be the (shift) action defined by:

\[
S_{k+1}(1) = 2, \ S_{k+1}(2) = 3, ..., S_{k+1}(k) = k + 1 \text{ and } S_{k+1}(k + 1) = 1.
\]

**Lemma 4.23** There exists a string \(w_{S_{k+1}}\) such that for all \(i \leq k + 1\) the
equality \(i \cdot w_{S_{k+1}} = S_{k+1}(i)\) holds.
Proof. It is easy to check that string \( a^{n-k+1}(ba^{n-1})^{n-k} \) works, that is: for all \( i \leq k + 1 \) the equality \( i \cdot (a^{n-k+1}(ba^{n-1})^{n-k}) = S_{k+1}(i) \) holds. Let us use the symbol \( w_{S_{k+1}} \) to denote the string \( a^{n-k+1}(ba^{n-1})^{n-k} \), and let us use the symbol \( S_{k+1}^{(j)} \) to denote the action \( S_{k+1} \circ \cdots \circ S_{k+1} \) \( j \) times. Notice that for all \( i, j \leq k + 1 \) the equality
\[
i \cdot (w_{S_{k+1}})^j = S_{k+1}^{(j)}(i) = (i + j) \mod (k + 1)
\]
holds. We have:

1. \( \langle S_{k+1} \rangle \), the transformation semigroup generated by \( S \), is isomorphic to \( \mathbb{Z}_{k+1} \).

2. \( \langle S_{k+1} \rangle \) is embedded into \( G_{\{1, \ldots, k+1\}} \).

It only remains to be proved that for all \([k + 1]\)-string \( w \) there exists \( j \leq k + 1 \) such that \( S_{k+1}^{(j)} \) is equal to the action exerted by \( w \) on the set \( \{1, \ldots, k + 1\} \).

Next lemma can be easily proved by induction on string-length.

Lemma 4.24 For all \( 1 \leq p < q < r < s \leq k + 1 \) there does not exist a string \( w \) such that \( p \cdot w < r \cdot w < q \cdot w < q \cdot w \).

It follows easily from the above lemma that for all \([k + 1]\)-string \( w \) there exists at most one \( i \in \{1, \ldots, k\} \) such that \( i \cdot w > (i + 1) \cdot w \). The last fact implies that for all \([k + 1]\)-string \( w \) there exists \( j \leq k + 1 \) such that action represented by \( w \) is equal to \( S_{k+1}^{(j)} \). Given the latter we claim that the theorem is proved, and we get as a corollary that

Corollary 4.25 For all \( n \geq 2 \) the equality
\[
F(C_n) = ([n], \mathbb{Z}_n) \lesssim \cdots \lesssim ([2], \mathbb{Z}_2)
\]
holds.

The KR-decomposition of an automaton \( M \) is constituted by two main objects: the full wreath product of its holonomy semigroups and the embedding of \( M \) into the latter product. We have surveyed the construction of the first object, the full wreath product of transformation semigroups, and we have used Černý automata to illustrate most of the concepts and related constructions. The construction of the embedding also requires of the introduction of several concepts that are not easy to grasp. One can use Černý automata to illustrate those concepts. The interested reader can consult the master degree thesis of the first author [4]. In this paper we focussed on their decomposability,
but we could focus on several other interesting properties (see for instance [12] and [15]) because Černý automata are real peculiarities.

Acknowledgements. The second author thanks the support provided by Universidad Nacional de Colombia Hermes research project 32083.

References


Received: July 17, 2018; Published: August 9, 2018