The Holonomy Decomposition of some Circular Semi-Flower Automata

Shubh N. Singh[*] and Kanduru V. Krishna[†]

Abstract

Using holonomy decomposition, the absence of certain types of cycles in automata has been characterized. In the direction of studying the structure of automata with cycles, this paper focuses on a special class of semi-flower automata and establish the holonomy decomposition of certain circular semi-flower automata. In particular, we show that the transformation monoid of a circular semi-flower automaton with at most two bpis divides a wreath product of cyclic transformation groups with adjoined constant functions.

Keywords: transformation monoids, semi-flower automata, holonomy decomposition

1 Introduction

Usefulness of a decomposition method for any given system does not require any justification. The primary decomposition theorem due to Krohn and Rhodes has been considered as one of the fundamental results in the theory of automata and monoids [13]. Eilenberg has given a slight generalization of the primary decomposition called the holonomy decomposition [8]. Here, Eilenberg established that every finite transformation monoid divides a wreath product of its holonomy permutation-reset transformation monoids. The holonomy decomposition of an automaton is considered to be the holonomy decomposition of the transformation monoid of the automaton. The holonomy decomposition is also used to study the structural properties of certain algebraic structures [11, 12]. The holonomy decomposition method appears to be relatively efficient and has been implemented computationally [4, 5]. One can use the computer algebra package, SgpDec [7] to obtain the holonomy decomposition of a given finite transformation monoid.

In order to ascertain the structure of an automaton, the holonomy decomposition considers the monoid of automaton and looks for groups induced by the

---

[*]Department of Mathematics, Central University of South Bihar, Patna, India, E-mail: `shubh@cub.ac.in`

[†]Department of Mathematics, IIT Guwahati, Guwahati, India, E-mail: `kvk@iitg.ac.in`

monoid permuting some set of subsets of the state set. These groups are called the holonomy groups, which are building blocks for the components of the holonomy decomposition. Using the holonomy decomposition, Egri-Nagy and Nehaniv characterized the absence of certain types of cycles in automata [6]. In fact, they proved that an automaton is algebraically cyclic-free if and only if the holonomy groups are trivial. On the other hand, the structure of automata with cycles is much more complicated.

In the direction of studying the structure of automata with cycles, this work concentrates on a special class of semi-flower automata (SFA) [9, 15]. Using SFA, the rank and intersection problem of certain submonoids of a free monoid have been studied [10, 16, 17].

In this paper, we consider circular semi-flower automata (CSFA) classified by their bpi(s) – branch point(s) going in – and obtain the holonomy decomposition of CSFA with at most two bpis. We present some preliminary concepts and results in Section 2. The main work of the paper is presented in Section 3. Finally, Section 4 concludes the paper.

2 Preliminaries

This section has two subsections on the holonomy decomposition and automata to present necessary background materials on these topics.

2.1 The Holonomy Decomposition

In this subsection, we provide brief details on the holonomy decomposition which will be useful in this paper. For more details one may refer [2, 4, 8].

We fix our notation regarding functions. Let $f : X \to Y$ be a function from X into Y. We write an argument $x \in X$ of f on its left so that xf is the value of f at x. The *rank* of f, denoted $\mathrm{rank}(f)$, is the cardinality of its image set Xf. The set of all functions from X into Y is denoted by Y^X. The composition of functions is designated by concatenation, with the leftmost function understood to apply first so that $xfg = (xf)g$.

A *transformation monoid* is a pair (P, M) consists of a nonempty finite set P and a submonoid M of $\mathscr{T}(P)$, where $\mathscr{T}(P)$ is the monoid of all functions on P with respect to composition of functions. Note that there is an action of submonoid M on set P. Let us denote the action of $m \in M$ on $p \in P$ as pm. If M is a subgroup of $\mathscr{T}(P)$, then (P, M) is called a *transformation group*.

A transformation monoid (P, M) *divides* a transformation monoid (Q, N), denoted $(P, M) \prec (Q, N)$, if there exists a partial surjective function $\varphi : Q \to P$ and, for every $m \in M$, an element $n \in N$ such that $(q\varphi)m = (qn)\varphi$ for each $q \in \mathrm{Dom}(\varphi)$. The *wreath product* of two transformation monoids (P, M) and (Q, N), denoted $(P, M) \wr (Q, N)$, is the transformation monoid $(P \times Q, W)$, where $W = \{(f, n) \mid f \in M^Q \ \text{and} \ n \in N\}$ is the monoid with operation given by

$$(f, n)(g, k) = (h, nk), \quad qh = (qf)((qn)g) \ \text{for every} \ q \in Q,$$

and the action of $(f, n) \in W$ on an element $(p, q) \in P \times Q$ is given by

$$(p, q)(f, n) = (p(qf), qn).$$

The wreath product is an associative operation on transformation monoids.

Let (P, M) be a transformation monoid. For $p \in P$, let $\widetilde{p}$ be the constant function on P which takes the value p. The semigroup of all these constant functions on P is denoted by $\widetilde{P}$. The *closure* of (P, M) is the transformation monoid $\overline{(P, M)} = (P, M \cup \widetilde{P})$. The *skeleton* of (P, M) is $\mathscr{J} = \{Pm \mid m \in M\} \cup \bigcup_{p \in P} \{\{p\}\}$ with the subduction relation $\leq$ on $\mathscr{J}$ given by $R \leq S$ if and only if $R \subseteq Sm$ for some $m \in M$. The subduction relation is a preorder relation. Consequently, there is an equivalence relation $\sim$ on $\mathscr{J}$ given by $R \sim S$ if and only if $R \leq S$ and $S \leq R$. We write $\mathscr{J}_i$ to denote the set of all elements of $\mathscr{J}$ of cardinality i (for $i \geq 1$), i.e.,

$$\mathscr{J}_i = \{T \in \mathscr{J} \mid |T| = i\}.$$

Let (P, M) be a transformation monoid. The *height* of $T \in \mathscr{J}$ is given by the function $\eta : \mathscr{J} \to \mathbb{Z}$, which is defined by $T\eta = 0$ if $|T| = 1$, and for $|T| > 1$, $T\eta$ is the length of the longest subduction chain(s) in the skeleton starting from a non-singleton set and ending in T. The *height* of (P, M) is defined as $P\eta$. For $T \in \mathscr{J}$ with $|T| > 1$, put $K(T) = \{m \in M \mid Tm = T\}$. The *paving of* T, denoted $B(T)$, is the set of maximal subsets of T that are contained in $\mathscr{J}$, i.e.,

$$B(T) = \{R \in \mathscr{J} \mid R \subsetneq T \text{ and if } S \in \mathscr{J} \text{ with } R \subseteq S \subseteq T, \text{ then } S = R \text{ or } S = T\}.$$

The set $G(T)$ of all distinct permutations on $B(T)$ induced by elements of $K(T)$ is called the *holonomy group* of T, and $(B(T), G(T))$ is a transformation group. We denote an element of $G(T)$ by $\breve{m}$ which is induced by $m \in K(T)$. For $T, T' \in \mathscr{J}$ with $|T| > 1, |T'| > 1$, if $T \sim T'$, then $(B(T), G(T))$ is isomorphic to $(B(T'), G(T'))$.

The *holonomy decomposition theorem* due to Eilenberg states that every finite transformation monoid divides a wreath product of its holonomy permutation-reset transformation monoids, as presented in the following:

Theorem 2.1 ([8])**.** *If (P, M) is a finite transformation monoid of height n, then*

$$(P, M) \prec \overline{\mathscr{H}_1} \wr \overline{\mathscr{H}_2} \wr \ldots \wr \overline{\mathscr{H}_n},$$

where, for $1 \leq i \leq n$,

$$\mathscr{H}_i = \left(\prod_{j=1}^{k_i} B(T_{ij}), \prod_{j=1}^{k_i} G(T_{ij}) \right),$$

in which k_i is the number of equivalence classes at height i and $\{T_{ij} \mid 1 \leq j \leq k_i\}$ is the set of representatives of equivalence classes at height i.

2.2 Automata

This subsection is devoted for essential preliminaries on automata and monoids. For more details one may refer [1, 9, 15].

Let A be a nonempty finite set called *alphabet* with its elements as *symbols*. The free monoid over A is denoted by A^* whose elements are called words, and ε denotes the empty word – the identity element of A^*.

By an *automaton*, we mean a quintuple $\mathcal{A} = (Q, A, \delta, q_0, F)$, where Q is a nonempty finite set called the set of *states*, A is alphabet, $q_0 \in Q$ called the *initial* state, $F \subseteq Q$ called the set of *final* states, and $\delta : Q \times A \to Q$ called the transition function. Clearly, by denoting the states as vertices and the transitions as labeled directed edges, an automaton can be represented by a digraph in which the initial state and final states shall be distinguished appropriately. A path in a digraph is an alternating finite sequence $v_0, e_1, v_1, e_2, v_2, \ldots v_{k-1}, e_k, v_k$ of vertices and labeled directed edges such that, for $1 \leq i \leq k$, the tail and the head of the edge e_i are v_{i-1} and v_i, respectively. A *path* in an automaton is a path in its digraph. For $p_i \in Q$ ($0 \leq i \leq k$) and $a_j \in A$ ($1 \leq j \leq k$), let

$$p_0 \xrightarrow{a_1} p_1 \xrightarrow{a_2} p_2 \xrightarrow{a_3} \cdots \xrightarrow{a_{k-1}} p_{k-1} \xrightarrow{a_k} p_k$$

be a path in $\mathcal{A}$. The word $a_1 \cdots a_k \in A^*$ is called the *label of the path*. A *null path* is a path from a state to itself labeled by the empty word ε. A path that starts and ends at the same state is called as a *cycle*, if it is not a null path.

Given an automaton $\mathcal{A}$, we can inductively extend the transition function for words by, for all $u \in A^*, a \in A$ and $q \in Q$,

$$\delta(q, \varepsilon) = q, \quad \text{and} \quad \delta(q, au) = \delta(\delta(q, a), u).$$

We write qu instead of $\delta(q, u)$. There is a natural way to associate a finite monoid to $\mathcal{A}$. For each $x \in A^*$, we define a function $\delta_x : Q \to Q$ by $q\delta_x = qx$ for all $q \in Q$. The set of functions, $M(\mathcal{A}) = \{\delta_x \mid x \in A^*\}$, forms a monoid under the composition of functions. If $M(\mathcal{A})$ is a group, then $\mathcal{A}$ is called a *permutation* automaton. Note that the monoid $M(\mathcal{A})$ is generated by the functions defined by symbols. Further, for all $x, y \in A^*$, we have $\delta_{xy} = \delta_x \delta_y$ and δ_ε is the identity function on Q.

Let $\mathcal{A}$ be an automaton. A state q is called a *branch point going in*, in short *bpi*, if the number of transitions coming into q (i.e. the indegree of q – the number of edges coming into q – in the digraph of $\mathcal{A}$) is at least two. We write $BPI(\mathcal{A})$ to denote the set of all bpis of $\mathcal{A}$. A state q is *accessible* (respectively, *coaccessible*) if there is a path from the initial state to q (respectively, a path from q to a final state). An automaton $\mathcal{A}$ is called a *trim* automaton if all the states of $\mathcal{A}$ are accessible and coaccessible. An automaton $\mathcal{A}$ is called a *semi-flower automaton* (in short, SFA) if it is a trim automaton with a unique final state that is equal to the initial state such that all the cycles in $\mathcal{A}$ visit the unique initial-final state q_0.

Let $X = \{p_1, \ldots, p_r\}$ be a finite set and $Y \subseteq X$. A *Y-cycle* is a permutation f_Y on X such that f_Y induces a cyclic ordering on Y ($= \{p_{i_1}, \ldots, p_{i_s}\}$, say) and f_Y is identity on $X \setminus Y$, i.e., for $1 \leq j < s$ and $p \in X \setminus Y$,

$$p_{i_j} f_Y = p_{i_{j+1}}, \ p_{i_s} f_Y = p_{i_1}, \quad \text{and} \quad pf_Y = p.$$

A *circular permutation* on X is an X-cycle. It is well known that for every permutation f on X, there exists a partition $\{Y_1, \ldots, Y_t\}$ of X such that $f = f_{Y_1} f_{Y_2} \cdots f_{Y_t}$, a composition of (disjoint) Y_i-cycles.

An automaton $\mathcal{A}$ is called a *circular* automaton if there exists a symbol $a \in A$ such that δ_a is a circular permutation on Q. Circular automata have been studied in various contexts. Pin proved the Černý conjecture for circular directable automata with a prime number of states [14]. Further, Dubuc showed that the Černý conjecture is true for any circular directable automata [3].

In order to investigate the holonomy decomposition of circular semi-flower automata, we consider these automata classified by their number of bpis and complete the task for the automata with at most two bpis.

3 Main Results

We present results of the paper in three subsections. In Subsection 3.1, we obtain some properties of circular semi-flower automata (CSFA) which are useful in the work. We investigate the holonomy decomposition of CSFA with at most one bpi and two bpis in subsections 3.2 and 3.3, respectively.

In what follows, $\mathcal{A} = (Q, A, \delta, q_0, q_0)$ is an SFA such that $|Q| = n$ ($n > 1$). Further, for $1 \leq m \leq n$, $\mathscr{C}_m$ denotes a transformation group (X, C_m) for some set $X \subseteq Q$ with $|X| = m$ and C_m is the cyclic group generated by circular permutation induced by a word on the set X.

3.1 Circular Semi-Flower Automata

In this subsection, we first ascertain that there is a unique circular permutation induced by symbols on the state set of CSFA and then we proceed to obtain certain properties pertaining to the bpis of CSFA.

Proposition 3.1. *Let $\mathcal{A}$ be an SFA and $a, b \in A$.*

(i) *If δ_a is a permutation on Q, then δ_a is circular permutation on Q.*

(ii) *If δ_a and δ_b are permutations on Q, then $\delta_a = \delta_b$.*

Proof.

(i) Write $\delta_a = f_{Q_1} \cdots f_{Q_t}$, a composition of Q_i-cycles for some partition $\{Q_1, \ldots, Q_t\}$ of Q. Let $q_0 \in Q_r$ for some $r \in \{1, \ldots, t\}$. If $Q_r = Q$, then $t = r = 1$ and so that δ_a is circular permutation on Q. Otherwise, there exists $q \in Q \setminus Q_r$ and $s \in \{1, \ldots, t\} \setminus \{r\}$ such that $q \in Q_s$. Note that the Q_s-cycle induces a cycle in $\mathcal{A}$ that does not pass through the initial-final state q_0; a contradiction.

(ii) On the contrary, let us assume that $\delta_a \neq \delta_b$. From Proposition 3.1 (i), the permutations δ_a and δ_b are circular permutations on Q. Let cyclic orderings

on Q with respect to δ_a and δ_b be as shown below.

$$\delta_a : q_0, q_{i_1}, q_{i_2}, \ldots, q_{i_{n-1}}$$
$$\delta_b : q_0, q_{j_1}, q_{j_2}, \ldots, q_{j_{n-1}}$$

Since $\delta_a \neq \delta_b$, let k be the least number such that $q_{i_k} \neq q_{j_k}$. Note that there exists $s > k$ such that $q_{i_k} = q_{j_s}$ and also there exists $r > k$ such that $q_{j_k} = q_{i_r}$. The path

$$q_{i_k} \xrightarrow{a^{r-k}} q_{i_r} = q_{j_k} \xrightarrow{b^{s-k}} q_{j_s} = q_{i_k}$$

is a cycle in $\mathcal{A}$ labeled by the word $a^{r-k}b^{s-k}$ that does not pass through the initial-final state q_0; a contradiction.

$\square$

Corollary 3.1. *There is a unique circular permutation induced by symbols on the state set of a CSFA.*

Proposition 3.2. *Let $\mathcal{A}$ be an SFA; then*

$$BPI(\mathcal{A}) = \varnothing \iff |A| = 1.$$

Proof. In an n-state automaton,

the total indegree of all states = the total number of transitions = $n|A|$.

Since $\mathcal{A}$ is accessible, indegree of each state is at least one. Consequently,

$$BPI(\mathcal{A}) = \varnothing \iff \text{the total indegree of all states } = n \iff |A| = 1.$$

$\square$

In what follows, $\mathcal{B} = (Q, A, \delta, q_0, q_0)$ stands for an CSFA with $|Q| = n$ ($n > 1$). If the number of bpis in $\mathcal{B}$ is less than the number of states in $\mathcal{B}$, then there is a unique symbol induces a permutation on Q. For the rest of the paper we fix the following regarding $\mathcal{B}$. Assume that the symbol $a \in A$ induces a circular permutation δ_a on Q. Accordingly,

$$\delta_a : q_0, q_1, \ldots, q_{n-1}$$

is the cyclic ordering on Q with respect to δ_a.

Proposition 3.3. *If $\mathcal{B}$ has at least one bpi, then its initial-final state q_0 is a bpi.*

Proof. Since $\mathcal{B}$ has at least one bpi, by Proposition 3.2, we have $|A| \geq 2$. We claim that $q_{n-1}\delta_b = q_0$ for all $b \in A \setminus \{a\}$ and so that q_0 is a bpi.

On the contrary, let us assume that $q_{n-1}\delta_c \neq q_0$ for some $c \in A \setminus \{a\}$. Then $q_{n-1}\delta_c = q_i$ for some i (with $1 \leq i < n$). Note that $q_i\delta_{a^{n-i-1}c} = q_i$. Therefore there is a cycle in $\mathcal{B}$ from q_i to q_i labeled by the word $a^{n-i-1}c$ that does not pass through the initial-final state q_0; a contradiction. Hence $q_{n-1}\delta_b = q_0$ for all $b \in A \setminus \{a\}$. $\square$

Proposition 3.4. *For $1 \leq m < n$, if $|BPI(\mathcal{B})| = m$, then any non-permutation function in $M(\mathcal{B})$ has rank at most m.*

Proof. Since $|BPI(\mathcal{B})| = m \geq 1$, by Proposition 3.2, we have $|A| \geq 2$. Note that the permutation δ_a contributes one to the indegree of each state of $\mathcal{B}$.

For $x \in A^*$, let δ_x be a non-permutation function in $M(\mathcal{B})$. The nonempty word x contains at least one symbol of $A \setminus \{a\}$. We claim that $|Q\delta_b| \leq m$ for all $b \in A \setminus \{a\}$ and so that the rank of δ_x is at most m. On the contrary, let us assume that $|Q\delta_c| > m$ for some $c \in A \setminus \{a\}$. This implies that $|BPI(\mathcal{B})| > m$; a contradiction. Hence $|Q\delta_b| \leq m$ for all $b \in A \setminus \{a\}$. $\square$

In view of Proposition 3.3, we have the following corollary of Proposition 3.4.

Corollary 3.2. *If $\mathcal{B}$ has a unique bpi, then $Q\delta_b = \{q_0\}$ for all $b \in A \setminus \{a\}$.*

3.2 Circular Semi-Flower Automata with at most one bpi

In this subsection, we obtain the holonomy decomposition of an SFA which is permutation automaton or has no bpis or circular automaton with a unique bpi. We first prove the following result.

Proposition 3.5. *Let $\mathcal{A}$ be an SFA. If $\mathcal{A}$ is permutation automaton or has no bpis, then $M(\mathcal{A})$ is a cyclic group.*

Proof.

Case ($\mathcal{A}$ is permutation): The monoid $M(\mathcal{A})$ is a group. All elements in $M(\mathcal{A})$ induced by words are permutation functions on Q. Note that $M(\mathcal{A})$ is generated by the functions induced by symbols. Also $\mathcal{A}$ is an SFA, all the permutations on Q induced by symbols are equal (cf. Proposition 3.1). Therefore $M(\mathcal{A})$ is a cyclic group.

Case ($\mathcal{A}$ has no bpis): Here $|A| = 1$ (cf. Proposition 3.2). Clearly the function induced by the symbol is a circular permutation on Q, and so $\mathcal{A}$ is permutation SFA. Therefore, by the previous case, the monoid $M(\mathcal{A})$ is a cyclic group.

$\square$

Theorem 3.1. *Let $\mathcal{A}$ be an SFA. If $\mathcal{A}$ is permutation automaton or has no bpis or circular automaton with a unique bpi, then $(Q, M(\mathcal{A})) \prec \overline{\mathscr{C}_n}$.*

Proof.

Case ($\mathcal{A}$ is permutation or has no bpis): Here $M(\mathcal{A})$ is a group (cf. Proposition 3.5). Therefore $|Q\delta_x| = n$ for all $\delta_x \in M(\mathcal{A})$.

Case ($\mathcal{A}$ is circular with a unique bpi): Since $\mathcal{A}$ has a unique bpi, we have $Q\delta_b = \{q_0\}$ for all $b \in A \setminus \{a\}$ (cf. Corollary 3.2). This implies that $\delta_b = \delta_c$ for all $b, c \in A \setminus \{a\}$, and so that $M(\mathcal{A})$ is generated by the set $\{\delta_a, \delta_b\}$ of functions induced by the symbols a and b. For $\delta_x \in M(\mathcal{A})$, by Proposition 3.4, we have either $|Q\delta_x| = n$ or $|Q\delta_x| = 1$.

In all the cases, the skeleton of the transformation monoid $(Q, M(\mathcal{A}))$ is $\mathscr{J} = \{Q\} \cup \mathscr{J}_1$. Clearly $B(Q) = \mathscr{J}_1$ and so that $|B(Q)| = n$. Note that $K(Q) = \{\delta_{a^i} \mid 1 \le i \le n\}$. The holonomy group $G(Q)$ is

$$G(Q) = \{\check{\delta}_{a^i} \mid 1 \le i \le n\}.$$

For $1 \le i \le n$, since $\delta_{a^i} = (\delta_a)^i$, we have $\check{\delta}_{a^n} = (\check{\delta}_a)^n = \check{\delta}_\varepsilon$. The holonomy group $G(Q)$ is cyclic group of order n generated by $\check{\delta}_a$. Thus, in each case, the holonomy decomposition of $(Q, M(\mathcal{A}))$ is

$$(Q, M(\mathcal{A})) \prec \overline{\mathscr{C}_n}.$$

$\square$

3.3   Circular Semi-Flower Automata with two bpis

In this subsection, we investigate the holonomy decomposition of CSFA with two bpis. Here $\mathcal{B} = (Q, A, \delta, q_0, q_0)$ denotes a CSFA with two bpis. Note that, by Proposition 3.2, we have $|A| \ge 2$. If $|Q| = 2$, then the holonomy decomposition of $\mathcal{B}$ follows directly from Theorem 3.1. Therefore, let us assume that $|Q| > 2$. By Proposition 3.3, the initial-final state q_0 of $\mathcal{B}$ is always a bpi. Let q_m, where $1 \le m < n$, be the other bpi of $\mathcal{B}$ so that $BPI(\mathcal{B}) = \{q_0, q_m\}$. Note that there is only one symbol $a \in A$ which induces the permutation on Q.

Lemma 3.1.   *Let $\mathcal{B} = (Q, A, \delta, q_0, q_0)$ be a CSFA with two bpis.*

(i) *For a symbol $b \in A$, if $rank(\delta_b) = 2$, then $Q\delta_b = BPI(\mathcal{B})$.*

(ii) *There exists a symbol $b \in A \setminus \{a\}$ such that $Q\delta_b = BPI(\mathcal{B})$.*

Proof. We note that δ_a contributes one to the indegree of each state of $\mathcal{B}$. Since $BPI(\mathcal{B}) = \{q_0, q_m\}$, we have $Q\delta_b \subseteq \{q_0, q_m\}$ for all $b \in A \setminus \{a\}$ (cf. Proposition 3.4).

(i) Straightforward from the above statement.

(ii) By Lemma 3.1(i), it is sufficient to prove that $rank(\delta_b) = 2$ for some $b \in A \setminus \{a\}$. On the contrary, let us assume that $rank(\delta_b) \neq 2$ for all $b \in A \setminus \{a\}$. Then $rank(\delta_b) = 1$ for all $b \in A \setminus \{a\}$ (cf. Proposition 3.4). This implies that either $Q\delta_b = \{q_0\}$ or $Q\delta_b = \{q_m\}$ for all $b \in A \setminus \{a\}$. If $Q\delta_b = \{q_m\}$ for some $b \in A \setminus \{a\}$, then there is a loop at q_m; which is not possible. Consequently $Q\delta_b = \{q_0\}$ for all $b \in A \setminus \{a\}$, and so that $BPI(\mathcal{B}) = \{q_0\}$; a contradiction. Hence $rank(\delta_b) = 2$ for some $b \in A \setminus \{a\}$.

$\square$

The following lemma provides the skeleton of the transformation monoid $(Q, M(\mathcal{B}))$.
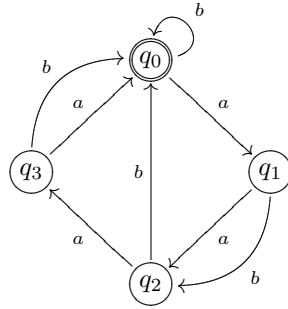
Figure 1: CSFA $\mathcal{B}_1$ with two bpis

Lemma 3.2. *Let $\mathcal{B}$ be a CSFA with $BPI(\mathcal{B}) = \{q_0, q_m\}$. Then the skeleton of transformation monoid $(Q, M(\mathcal{B}))$ is given by*

$$\mathscr{J} = \{Q\} \cup \mathscr{J}_2 \cup \mathscr{J}_1,$$

where $\mathscr{J}_2 = \big\{\{q_0, q_m\}\delta_{a^i} \mid 1 \le i \le n\big\}$.

Proof. In view of Proposition 3.4, other than Q and singletons, the skeleton $\mathscr{J}$ can have some sets of size two. Therefore it is sufficient to determine $\mathscr{J}_2$.

By Lemma 3.1(ii), there exists a symbol $b \in A \setminus \{a\}$ such that $Q\delta_b = \{q_0, q_m\}$. Therefore, for $1 \le i \le n$, the image set $Q\delta_{ba^i} = \{q_0, q_m\}\delta_{a^i} \in \mathscr{J}_2$, and so that

$$\big\{\{q_0, q_m\}\delta_{a^i} \mid 1 \le i \le n\big\} \subseteq \mathscr{J}_2.$$

Let us assume that $Q\delta_w \in \mathscr{J}_2$ for some nonempty word $w \in A^*$. Then w is of the form

$$w = a^{i_1} b_1 a^{i_2} b_2 \cdots a^{i_k} b_k a^{i_{k+1}},$$

for $i_j \ge 0$ $(1 \le j \le k+1)$ and $b_t \in A$ $(1 \le t \le k)$ such that the rank of each function δ_{b_t} is two (cf. Proposition 3.4). Write $w = a^{i_1} b_1 u b_k a^{i_{k+1}}$, where $u = a^{i_2} b_2 \cdots a^{i_k}$. Since $\mathrm{rank}(\delta_{b_1 u b_k}) = \mathrm{rank}(\delta_{b_k}) = 2$, we have

$$Q\delta_{b_1 u b_k} = Q\delta_{b_k} = \{q_0, q_m\},$$

by Lemma 3.1(i). Therefore $Q\delta_w = Q\delta_{a^{i_1} b_1 u b_k a^{i_{k+1}}} = \{q_0, q_m\}\delta_{a^{i_{k+1}}}$, and consequently

$$\mathscr{J}_2 = \big\{\{q_0, q_m\}\delta_{a^i} \mid 1 \le i \le n\big\}.$$

$\square$

Remark 3.1. As shown in Example 3.1, the cardinality of $\mathscr{J}_2$ is not necessarily n.

Example 3.1. The 4-state automaton $\mathcal{B}_1$ given in the Figure 1 is CSFA with $BPI(\mathcal{B}_1) = \{q_0, q_2\}$. We observe that

$$\{q_0, q_2\}\delta_a = \{q_1, q_3\}, \quad \{q_0, q_2\}\delta_{a^2} = \{q_0, q_2\}, \quad \text{and so that } |\mathscr{J}_2| = 2.$$

Lemma 3.3. *Let $\mathcal{B}$ be a CSFA with $BPI(\mathcal{B}) = \{q_0, q_m\}$. Then there is a nonempty word $x \in A^*$ such that $q_0\delta_x = q_m$ and $q_m\delta_x = q_0$.*

Proof. If there exists a symbol $b \in A \setminus \{a\}$ such that $q_0\delta_b \neq q_0$, then clearly the word $x = b$ will serve the purpose. Otherwise we have $q_0\delta_b = q_0$ for all $b \in A \setminus \{a\}$. However, by Lemma 3.1(ii), there exists a symbol $c \in A \setminus \{a\}$ such that $Q\delta_c = \{q_0, q_m\}$.

Note that the permutation δ_a induces the cyclic ordering $q_0, q_1, \ldots, q_{n-1}$ of the state set Q. Since $q_0\delta_c = q_0$ and the state q_m is the other bpi of $\mathcal{B}$, there exists a state q_i (with $1 \leq i < m$) such that $q_i\delta_c = q_m$. Let t (with $1 \leq t < m$) be the least integer such that $q_t\delta_c = q_m$. Choose the word $x = a^t c$ and observe that $q_0\delta_x = q_m$. We claim that $q_m\delta_x = q_0$.

On the contrary, let us assume that $q_m\delta_x \neq q_0$. Since $BPI(\mathcal{B}) = \{q_0, q_m\}$, we have $q_m\delta_x = q_m$ and so that there is a cycle in $\mathcal{B}$ from q_m to q_m labeled by the word x. Since $\mathcal{B}$ is SFA, the cycle must pass through q_0. Since $q_0\delta_c = q_0$, there exist t_1 and t_2 $(1 \leq t_1, t_2 < t)$ with $t_1 + t_2 = t$ such that

$$q_m\delta_{a^{t_1}} = q_0 \quad \text{and} \quad q_0\delta_{a^{t_2}c} = q_m.$$

Note that $q_0\delta_{a^{t_2}c} = q_{t_2}\delta_c = q_m$. This contradicts the choice of t, as $t_2 < t$. Thus we have $q_m\delta_x = q_0$. $\square$

Theorem 3.2. *If $\mathcal{B}$ is an n-state CSFA with $BPI(\mathcal{B}) = \{q_0, q_m\}$, then*

$$(Q, M(\mathcal{B})) \prec \overline{\mathscr{C}_2} \wr \overline{\mathscr{C}_r},$$

where r (with $1 < r \leq n$) is the smallest integer such that $\{q_0, q_m\}\delta_{a^r} = \{q_0, q_m\}$.

Further, if n is an odd number, then

$$(Q, M(\mathcal{B})) \prec \overline{\mathscr{C}_2} \wr \overline{\mathscr{C}_n}.$$

Proof. From Lemma 3.2, the skeleton of $(Q, M(\mathcal{B}))$ is given by

$$\mathscr{J} = \{Q\} \cup \mathscr{J}_2 \cup \mathscr{J}_1$$

in which all the elements of $\mathscr{J}_2$ are equivalent to each other.

For $1 \leq i \leq n$, note that δ_{a^i} permutes the elements of Q. Also, for $x \in A^*$, if $\delta_x \neq \delta_{a^i}$ for any i (with $1 \leq i \leq n$), then δ_x is not a permutation on Q (cf. Proposition 3.1). Consequently we have $K(Q) = \{\delta_{a^i} \mid 1 \leq i \leq n\}$. Since the elements of $\mathscr{J}_2$ are maximal in Q, we have $B(Q) = \mathscr{J}_2$. Let r (with $1 < r \leq n$) be the smallest integer such that $\{q_0, q_m\}\delta_{a^r} = \{q_0, q_m\}$ so that $|B(Q)| = r$. The holonomy group of Q is

$$G(Q) = \{\check{\delta}_{a^i} \mid 1 \leq i \leq r\}.$$

For $1 \le i \le r$, since $\delta_{a^i} = (\delta_a)^i$, we have $\check{\delta}_{a^r} = (\check{\delta}_a)^r = \check{\delta}_\varepsilon$. The holonomy group $G(Q)$ is cyclic group of order r generated by $\check{\delta}_a$, and so that $(B(Q), G(Q)) = \mathscr{C}_r$.

Let $P = \{q_0, q_m\}$ be representative in $\mathscr{J}_2$. Clearly $B(P) = \{\{q_0\}, \{q_m\}\}$. By Lemma 3.3, there exists a nonempty word $x \in A^*$ such that $q_0\delta_x = q_m$ and $q_m\delta_x = q_0$. This implies that $K(P) = \{\delta_x, \delta_\varepsilon\}$. Therefore the holonomy group $G(P)$ is cyclic group of order two generated by $\check{\delta}_x$, and so that $(B(P), G(P)) = \mathscr{C}_2$. Thus the holonomy decomposition of $(Q, M(\mathcal{B}))$ is

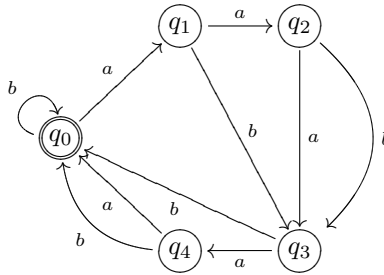$$(Q, M(\mathcal{B})) \prec \overline{\mathscr{C}_2} \wr \overline{\mathscr{C}_r}.$$

If n is an odd number, we claim that $r = n$. On the contrary, let us assume that $r < n$. Since $\{q_0, q_m\}\delta_{a^r} = \{q_0, q_m\}$ and δ_a is circular permutation on Q. It follows that $q_0\delta_{a^r} = q_m$ and $q_m\delta_{a^r} = q_0$. This implies that $q_0\delta_{a^{2r}} = q_0$ and $q_m\delta_{a^{2r}} = q_m$ with $1 < 2r < 2n$. Therefore $2r = n$; which is a contradiction. Thus the holonomy decomposition of $(Q, M(\mathcal{B}))$ is

$$(Q, M(\mathcal{B})) \prec \overline{\mathscr{C}_2} \wr \overline{\mathscr{C}_n}.$$

$\square$

Figure 2: CSFA $\mathcal{B}_2$ with two bpis

Example 3.2. The 4-state automaton $\mathcal{B}_1$ given in the Figure 1 is CSFA with $BPI(\mathcal{B}_1) = \{q_0, q_2\}$. Using [18], we find the skeleton of $(Q, M(\mathcal{B}_1))$ as

$$\mathscr{J} = \{Q\} \cup \mathscr{J}_2 \cup \mathscr{J}_1,$$

where $\mathscr{J}_2 = \{\{q_0, q_2\}\delta_{a^i} \mid 1 \le i \le 4\}$. Clearly $B(Q) = \mathscr{J}_2$. The smallest integer r (with $1 < r \le 4$) such that $\{q_0, q_2\}\delta_{a^r} = \{q_0, q_2\}$ is two, and therefore $|B(Q)| = 2$. The holonomy group $G(Q)$ is cyclic group of order two generated by $\check{\delta}_a$, and so that $(B(Q), G(Q)) = \mathscr{C}_2$.

We observe that the elements of $\mathscr{J}_2$ are equivalent to each other. Let $P = \{q_0, q_2\}$ be representative in $\mathscr{J}_2$. Clearly $B(P) = \{\{q_0\}, \{q_2\}\} \subseteq \mathscr{J}_1$. The holonomy group $G(P)$ is cyclic group of order two generated by $\check{\delta}_{ab}$, and so that $(B(P), G(P)) = \mathscr{C}_2$. Thus the holonomy decomposition of $(Q, M(\mathcal{B}_1))$ is

$$(Q, M(\mathcal{B}_1)) \prec \overline{\mathscr{C}_2} \wr \overline{\mathscr{C}_2}.$$

If the cardinality of the state set is an odd number, the following example illustrates Theorem 3.2.

Example 3.3. The 5-state automaton $\mathcal{B}_2$ given in the Figure 2 is CSFA with $BPI(\mathcal{B}_2) = \{q_0, q_3\}$. Using [18], we find the skeleton of $(Q, M(\mathcal{B}_2))$ as

$$\mathscr{J} = \{Q\} \cup \mathscr{J}_2 \cup \mathscr{J}_1,$$

where $\mathscr{J}_2 = \big\{\{q_0, q_3\}\delta_{a^i} \ \big| \ 1 \leq i \leq 5\big\}$. Clearly $B(Q) = \mathscr{J}_2$. The smallest integer r (with $1 < r \leq 5$) such that $\{q_0, q_3\}\delta_{a^r} = \{q_0, q_3\}$ is five, and therefore $|B(Q)| = 5$. The holonomy group $G(Q)$ is cyclic group of order five generated by $\check{\delta}_a$, and so that $(B(Q), G(Q)) = \mathscr{C}_5$.

We observe that the elements of $\mathscr{J}_2$ are equivalent to each other. Let $P = \{q_0, q_3\}$ be representative in $\mathscr{J}_2$. Clearly $B(P) = \big\{\{q_0\}, \{q_3\}\big\} \subseteq \mathscr{J}_1$. The holonomy group $G(P)$ is cyclic group of order two generated by $\check{\delta}_{ab}$, and so that $(B(P), G(P)) = \mathscr{C}_2$. Thus the holonomy decomposition of $(Q, M(\mathcal{B}_2))$ is

$$(Q, M(\mathcal{B}_2)) \prec \overline{\mathscr{C}_2} \wr \overline{\mathscr{C}_5}.$$

We conclude the paper by looking at two examples that exhibit that the study on the holonomy decomposition of CSFA with more than two bpis is much more complicated.
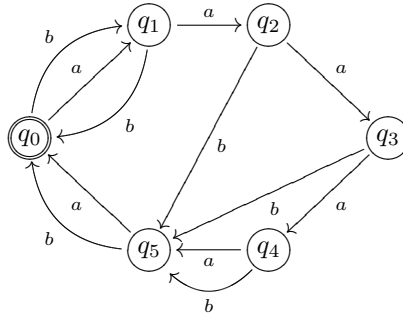

Figure 3: CSFA $\mathcal{B}_3$ with three bpis

Example 3.4. The 6-state automaton $\mathcal{B}_3$ given in the Figure 3 is CSFA with $BPI(\mathcal{B}_3) = \{q_0, q_1, q_5\}$. Using [18], we find the skeleton of $(Q, M(\mathcal{B}_3))$ as

$$\mathscr{J} = \{Q\} \cup \mathscr{J}_3 \cup \mathscr{J}_2 \cup \mathscr{J}_1,$$

where $\mathscr{J}_3 = \big\{\{q_0, q_1, q_5\}\delta_{a^i} \ \big| \ 1 \leq i \leq 6\big\}$, and $\mathscr{J}_2 = \big\{\{q_0, q_1, q_5\}\delta_{ba^i} \ \big| \ 1 \leq i \leq 6\big\}$. Clearly $B(Q) = \mathscr{J}_3$ and $|\mathscr{J}_3| = 6$. The holonomy group $G(Q)$ is cyclic group of order six generated by $\check{\delta}_a$, and so that $(B(Q), G(Q)) = \mathscr{C}_6$.

We observe that the elements of $\mathscr{J}_3$ are equivalent to each other. Let $P = \{q_0, q_1, q_5\}$ be representative in $\mathscr{J}_3$. Clearly $B(P) = \big\{\{q_0, q_1\}, \{q_0, q_5\}\big\} \subseteq \mathscr{J}_2$.

The holonomy group $G(P)$ is cyclic group of order two generated by $\check{\delta}_{ab}$, and so that $(B(P), G(P)) = \mathscr{C}_2$.

We further observe that all six elements of $\mathscr{J}_2$ are equivalent to each other. Let $T = \{q_0, q_1\}$ be representative in $\mathscr{J}_2$. Clearly $B(T) = \{\{q_0\}, \{q_1\}\} \subseteq \mathscr{J}_1$. The holonomy group $G(T)$ is cyclic group of order two generated by $\check{\delta}_b$, and so that $(B(T), G(T)) = \mathscr{C}_2$. Thus the holonomy decomposition of $(Q, M(\mathcal{B}_3))$ is

$$(Q, M(\mathcal{B}_3)) \prec \overline{\mathscr{C}_2} \wr \overline{\mathscr{C}_2} \wr \overline{\mathscr{C}_6}.$$
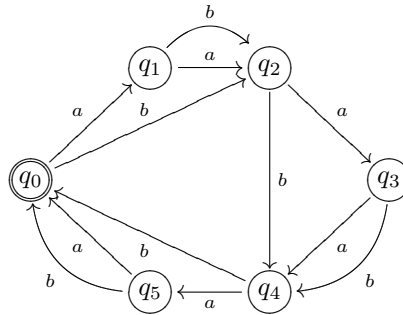

Figure 4: CSFA $\mathcal{B}_4$ with three bpis

Example 3.5. The 6-state automaton $\mathcal{B}_4$ given in the Figure 4 is CSFA with $BPI(\mathcal{B}_4) = \{q_0, q_2, q_4\}$. Using [18], we find the skeleton of $(Q, M(\mathcal{B}_4))$ as

$$\mathscr{J} = \{Q\} \cup \mathscr{J}_3 \cup \mathscr{J}_1,$$

where $\mathscr{J}_3 = \{\{q_0, q_2, q_4\}, \{q_1, q_3, q_5\}\}$. Clearly $B(Q) = \mathscr{J}_3$. The holonomy group $G(Q)$ is cyclic group of order two generated by $\check{\delta}_a$, and so that $(B(Q), G(Q)) = \mathscr{C}_2$.

We observe that the elements of $\mathscr{J}_3$ are equivalent to each other. Let $P = \{q_0, q_2, q_4\}$ be representative in $\mathscr{J}_3$. Clearly $B(P) = \{\{q_0\}, \{q_2\}, \{q_4\}\} \subseteq \mathscr{J}_1$. The holonomy group $G(P)$ is cyclic group of order three generated by $\check{\delta}_b$, and so that $(B(P), G(P)) = \mathscr{C}_3$. Thus the holonomy decomposition of $(Q, M(\mathcal{B}_4))$ is

$$(Q, M(\mathcal{B}_4)) \prec \overline{\mathscr{C}_3} \wr \overline{\mathscr{C}_2}.$$

4 Conclusion

In this paper we have initiated the investigations on the holonomy decomposition of circular semi-flower automata (CSFA) classified by their number of bpis. In fact, we have ascertained the holonomy decomposition of CSFA with at most two bpis. Our experiments for the holonomy decomposition of CSFA with more than two bpis over numerous examples exhibit that their structure is much more complicated.

However, we feel that the approach adopted in the paper may be useful to target the holonomy decomposition of CSFA having arbitrary number of bpis. In general, one can look for the holonomy decomposition of semi-flower automata.

Acknowledgements

References

[1] Berstel, J. and Perrin, D. *Theory of codes*, volume 117 of *Pure and Applied Mathematics*. Academic Press Inc., 1985.

[2] Dömösi, P. and Nehaniv, C. L. *Algebraic theory of automata networks: An introduction*, volume 11 of *SIAM Monographs on Discrete Mathematics and Applications*. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 2005.

[3] Dubuc, L. Sur les automates circulaires et la conjecture de Černý. *RAIRO Inform. Théor. Appl.*, 32(1-3):21–34, 1998.

[4] Egri-Nagy, A. *Algebraic Hierarchical Decomposition of Finite State Automata– A Computational Approach*. PhD thesis, University of Hertfordshire, England, 2005.

[5] Egri-Nagy, A. and Nehaniv, C. L. Algebraic hierarchical decomposition of finite state automata: Comparison of implementations for Krohn-Rhodes theory. In *CIAA*, pages 315–316, 2004.

[6] Egri-Nagy, A. and Nehaniv, C. L. Cycle structure in automata and the holonomy decomposition. *Acta Cybernet.*, 17(2):199–211, 2005.

[7] Egri-Nagy, A. and Nehaniv, C. L. *SgpDec – software package for hierarchical coordinatization of groups and semigroups, implemented in the GAP computer algebra system*. https://github.com/gap-packages/sgpdec, 2010.

[8] Eilenberg, S. *Automata, languages, and machines. Vol. B*. Academic Press [Harcourt Brace Jovanovich Publishers], New York, 1976.

[9] Giambruno, L. *Automata-theoretic Methods in Free Monoids and Free Groups*. PhD thesis, Universit degli Studi di Palermo, Palermo, Italy, 2007.

[10] Giambruno, L. and Restivo, A. An automata-theoretic approach to the study of the intersection of two submonoids of a free monoid. *Theor. Inform. Appl.*, 42(3):503–524, 2008.

[11] Holcombe, M. Holonomy decompositions of near-rings. *Proc. Edinburgh Math. Soc. (2)*, 23(1):43–47, 1980.

[12] Krishna, K. V. and Chatterjee, N. Holonomy decomposition of seminearrings. *Southeast Asian Bull. Math.*, 31(6):1113–1122, 2007.

[13] Krohn, K. and Rhodes, J. Algebraic theory of machines. I. Prime decomposition theorem for finite semigroups and machines. *Trans. Amer. Math. Soc.*, 116:450–464, 1965.

[14] Pin, J.-E. Sur un cas particulier de la conjecture de Černý. In *Automata, languages and programming (Fifth Internat. Colloq., Udine, 1978)*, volume 62 of *Lecture Notes in Comput. Sci.*, pages 345–352. Springer, Berlin, 1978.

[15] Singh, S. N. *Semi-Flower Automata*. PhD thesis, IIT Guwahati, India, 2012.

[16] Singh, S. N. and Krishna, K. V. The rank and Hanna Neumann property of some submonoids of a free monoid. *Ann. Math. Inform.*, 40:113–123, 2012.

[17] Singh, S. N. and Krishna, K. V. A sufficient condition for the Hanna Neumann property of submonoids of a free monoid. *Semigroup Forum*, 86(3):537–554, 2013.

[18] The GAP Group. *GAP–Groups, Algorithms, and Programming, Version 4.8.4.* http://www.gap-system.org, 2016.