Valence automata over E-unitary inverse semigroups

Erzsi Dombi

30 May 2018

Outline

Motivation

Chomsky-Schützenberger Theorem (1963):
Let L be a language. Then the following are equivalent:

- L is context-free;
- L is accepted by a polycyclic monoid automaton of rank 2;
- L is accepted by a free group automaton of rank 2.

Greibach (1968): Let L be a language. Then the following are equivalent:

- L is accepted by a bicyclic monoid automaton;
- L is accepted by a partially-blind one-counter automaton.

Motivation

Aims:

- To understand these theorems from a structure theoretical point of view.
- To introduce the notion of a partially blind group automaton with respect to a submonoid.
- To describe language classes accepted by automata over bisimple F-inverse monoids with the help of partially blind automata over their maximal group homomorphic image with respect to a submonoid.
- To describe language classes accepted by automata over bisimple strongly F^*-inverse monoids with the help of partially blind automata over their *universal group* homomorphic image with respect to a submonoid.

Notation

Σ: finite set of symbols called an *alphabet*.

Σ^*: set of finite sequences of symbols elements of which are called *words*.

$L \subseteq \Sigma^*$: *language* over Σ.

$|w|_a$: number of occurrences of the letter a in the word w.

Notation

M: Inverse monoid

$\leq$: Natural partial order on M:

$$s \leq t \quad \iff \quad s = et,\ e \in E(M).$$

σ: Minimum group congruence

$$s\sigma t \quad \iff \quad \exists u \in M \text{ such that } u \leq s \text{ and } u \leq t.$$

$W(M, \alpha)$: Let A be a choice of generators for a monoid M with $\alpha : A^* \to M$. The *identity language* for M with respect to A is

$$W(M, \alpha) = \{w \in A^* \mid \alpha(w) = 1\}.$$

E-unitary and F-inverse monoids

An inverse monoid M is *E-unitary* if

$$e \leq s, \ e \in E(M) \implies s \in E(M).$$

It is well known that

$$M \text{ is } E\text{-unitary} \iff \mathrm{Ker}\sigma = E(M).$$

An inverse monoid M is *F-inverse* if each σ-class contains a unique maximal element.

Strongly E^*-unitary monoids

Szendrei:
An inverse monoid M is *E^*-unitary* if and only if

$$e \leq s,\ 0 \neq e \in E(M) \implies s \in E(M).$$

Bullman-Fleming, Fountain, Gould [1999]:
An inverse monoid M with zero is *strongly E^*-unitary* if and only if there exists a function $\theta : S \to G^0$ such that

- $s\theta = 0 \iff s = 0;$
- $s\theta = 1 \iff s \in E(M);$
- if $st \neq 0$, then $(st)\theta = s\theta t\theta$.

We call θ an 0-restricted idempotent-pure pre-homomorphism.

Strongly E^*-unitary monoids

Bullman-Fleming, Fountain, Gould [1999]:
Let S be an inverse semigroup with zero. Then S is strongly E^*-unitary if and only if $S \cong \mathcal{M}_0(G, \mathcal{X}, \mathcal{Y})$.

Strongly F^*-inverse monoids

An inverse monoid M is *F^*-inverse* if for each $0 \neq s \in M$, there exists a unique element $m \in M$ such that $s \leq m$.

An inverse monoid M is *strongly F^*-inverse* if M is F^*-inverse and strongly E^*-unitary.

Finite state automata

Definition

A *Finite State Automaton* $\mathcal{A}$ is a tuple $\mathcal{A} = (Q, \Sigma, \delta, q_0, F)$, where

- Q is a finite set of *states*;
- Σ is an *alphabet;*
- $\delta : Q \times (\Sigma \cup \{\epsilon\}) \to \mathcal{P}(Q)$ *transition relation*;
- $q_0 \in Q$ is the *initial state*;
- $F \subseteq Q$ is the set of *final states*.

Finite state automata

We can think of a FSA as a finite directed graph, where

- the set of vertices Q are the states of the automaton;
- q_0 is a distinguished vertex called an initial state;
- $F \subseteq Q$ terminal states;
- edges are labelled by elements of $\Sigma \cup \{\epsilon\}$.

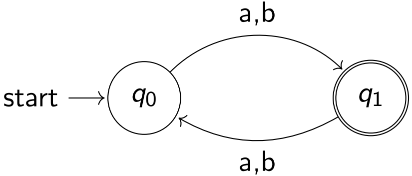
A word $w \in \Sigma^*$ is accepted by the automaton $\mathcal{A}$ if there exists a path from the initial vertex to a final vertex whose label is w. The language accepted by $\mathcal{A}$ is

$$L(\mathcal{A}) = \{w \in \Sigma^* \mid w \text{ is accepted by } \mathcal{A}\}.$$

Finite state automata

Example

Consider $\mathcal{A} = (\{q_0, q_1\}, \{a, b\}, \delta, q_0, \{q_1\})$:



Then

$$L(\mathcal{A}) = \{w \in \{a, b\}^+ \mid |w| = 2k + 1\}.$$

Extended finite automata - Valence automata - M-automata

A *extended finite automaton* over M is a finite state automaton $\mathcal{A}_M$ whose edges are labelled by elements of $\Sigma^* \times M$.

A word is accepted by $\mathcal{A}_M$ if there exists a path from the initial vertex to a final vertex, whose label is $(w, 1)$.

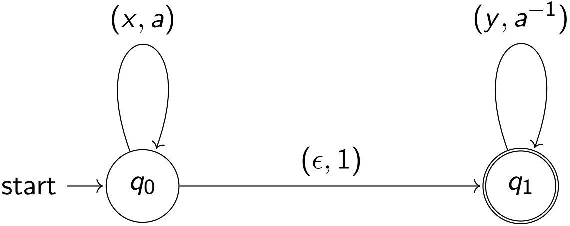
The language $L_{\mathcal{A}}(M)$ in Σ^* accepted by $\mathcal{A}_M$ consists of all words $w \in \Sigma^*$ that are accepted by $\mathcal{A}_M$.

We let $\mathcal{L}(M)$ denote the family of languages that are accepted by M-automata.

M-automata

Example

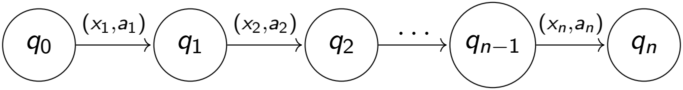
Let $M = \mathbb{Z} =< a >$, $\Sigma = \{x, y\}$ and $\mathcal{A}_M$:



$$L_{\mathcal{A}}(M) = \{x^n y^n \mid n \geq 0\}.$$

Partially blind one-counter automata: Greibach 1968

Consider a path p in a $\mathbb{Z}$-automaton:



Let

$$l_2(p_i) = a_1 + a_2 + \ldots + a_i, \quad (1 \leq i \leq n)$$

A word is accepted by a partially blind automaton, if there exists a path p from the initial vertex to a final vertex whose label is $(w, 0)$ and is such that $l_2(p_i) \geq 0$ for all $1 \leq i \leq |p|$.

In case the counter would go negative, no further transitions are defined and the machine is blocked.

Partially blind one-counter automata: Greibach 1968

We will denote the family of languages accepted by a partially blind one-counter automaton $\mathcal{A}$ by $\mathcal{L}(\mathbb{Z}|\mathbb{Z}^+)$.

General results

Proposition[Kambites 2009]
Let M and N be monoids and assume that M is generated by a finite set X. Then $W(M, X) \in \mathcal{L}(N)$ if and only if $\mathcal{L}(N) \subseteq \mathcal{L}(M)$.

Proposition[Render, Kambites 2010]
For every monoid M there is a simple or 0-simple monoid N such that $\mathcal{L}(M) = \mathcal{L}(N)$.

Proposition[Render, Kambites 2010]
Let M be a monoid. Then either $\mathcal{L}(M) = \mathcal{L}(G)$, where G is a group or $\mathcal{L}(M)$ contains the partially blind one-counter languages.

Examples

monoid M	$\mathcal{L}(M)$
finite monoid	regular
bicyclic monoid P_1	partially blind languages
polycylic monoid P_n, $n \geq 2$	context free languages
free group F_n, $n \geq 2$	context free languages
$\mathbb{Z}^n$	blind n-counter languages

Bicyclic and polycyclic monoids

Bicylic monoid: P_1	Polycyclic monoid: P_2
bisimple	0-bisimple
F-inverse	strongly F^*-inverse
$\sigma : P_1 \to \mathbb{Z}$	$\phi : P_2 \to F_2^0$ suitable homomorphism
$\mathcal{L}(P_1) = \mathcal{L}(\mathbb{Z}\|\mathbb{Z}^+)$	$\mathcal{L}(P_2) = \mathcal{L}(F_2)$

Kambites: "The polycyclic monoid automaton apparently makes fundamental use of its ability to fail, by reaching a zero configuration of the register monoid. Since the free group has no zero, the free group automaton seems to have no such capability, and appears to be *blind* in a much more fundamental way."

Partially blind automata over G with respect to M

Let G be a group and M be a submonoid of G.

A *partially blind automaton* $\mathcal{A}$ *over* G *with respect to* M is a G-automaton in which a word w is accepted if

- there exists a path p from the initial vertex to a final vertex, whose label is $(w, 1)$
- $l_2(p_i) \in M$ for all $1 \leq i \leq |p|$.

We let

$$L_{\mathcal{A}}(G|M)$$

denote the language accepted by such an automaton.
We let $\mathcal{L}(G|M)$ denote the family of languages accepted by partially blind automata over G with respect to M.

Example: Bicyclic monoid

The *bicyclic monoid* is given by the monoid presentation

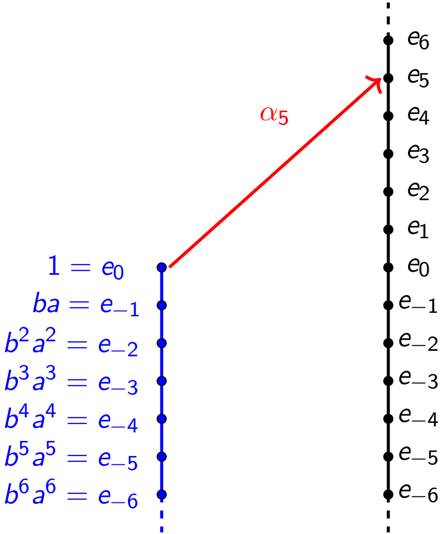
$$P_1 =< a, b : ab = 1 > .$$

The identity language of P_1 is:

$$W(P_1) = \{w \in \{a, b\}^+ : |w|_a = |w|_b, \text{ if } w = uv \text{ then } |u|_a \geq |u|_b\}.$$

Bicyclic monoid: P-representation

Let $G = \mathbb{Z}$, $\mathcal{X} = \mathbb{Z}$ and $\mathcal{Y} = \mathbb{Z}^-$. Let $\alpha_m : e_k \to e_{k+m}$.



Bicyclic monoid: P-representation

$$P(\mathbb{Z}, \mathcal{X}, \mathcal{Y}) = \{(e, g) \in \mathcal{Y} \times G \mid {}^{g^{-1}}e \in \mathcal{Y}\}$$

$$\varphi : P_1 \to P(\mathbb{Z}, \mathcal{X}, \mathcal{Y});\ a \mapsto (e_0, 1)\ b \mapsto (e_{-1}, -1)$$

Bicyclic monoid: Identity language

Observation: Let

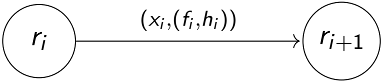
$$w \equiv (f_0, h_0)(f_1, h_1)\dots(f_n, h_n),$$

where $(f_i, h_i) \in \{(e_0, 1), (e_{-1}, -1)\}$.
Then

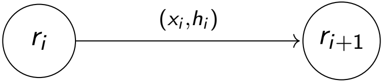
$$\begin{aligned} w = (e, 0) \iff & f_0 = e_0 \\ & h_0 + \dots + h_n = 0 \\ & h_0 + \dots + h_i \in \mathbb{Z}^+ \quad (1 \leq i \leq n-1) \end{aligned}$$

Bicyclic monoid: $\mathcal{L}(P_1) = \mathcal{L}(\mathbb{Z}|\mathbb{Z}^+)$

Replace each arrow



with



and vica versa.

Bisimple E-unitary inverse semigroups

Theorem [Clifford,Reilly,McAlister 1968]
Let S be an E-unitary bisimple inverse monoid and R be the $\mathcal{R}$-class of 1. Then

- $S = R^{-1}R$;
- R is a cancellative submonoid;
- principal left-ideals of R form a semilattice under intersection;
- R can be embedded in S/σ.

Bisimple E-unitary inverse semigroups

Theorem [McAlister 1974]
Let S be an E-unitary bisimple inverse monoid and R be the $\mathcal{R}$-class of 1. Let $G = S/\sigma$. Let

$$\mathcal{X} = \{Rg \mid g \in G\} \qquad \text{and} \qquad \mathcal{Y} = \{Ra \mid a \in R\}$$

and define a transitive action of G on $\mathcal{Y}$ by ${}^{h}Rg = Rgh^{-1}$. Let

$$P(G, \mathcal{X}, \mathcal{Y}) = \{(Ra, g) \in \mathcal{Y} \times G \mid Rag \in \mathcal{Y}\}$$

with

$$(Ra, g)(Rb, h) = (Ra \cap {}^{g}Rb, gh).$$

Then

$$S \cong P(G, \mathcal{X}, \mathcal{Y}); \quad a^{-1}b \mapsto (Ra, a^{-1}b).$$

Bisimple E-unitary inverse semigroups

Observation:

$$(R,1) = (Ra_1, g_1)(Ra_2, g_2)\ldots(Ra_n, g_n) \Longrightarrow \begin{array}{l} 1 = a_1 \\ 1 = g_1 \ldots g_n \\ g_1 \ldots g_i \in R \\ (1 \leq i \leq n) \end{array}$$

Conjecture [P Davidson, ED]: Let S is a bisimple F-inverse semigroup and let R denote the $\mathcal{R}$-class of 1. Then $\mathcal{L}(S) = \mathcal{L}(S/\sigma | R/\sigma)$.

Polycyclic monoids

The polycyclic monoid of rank 2 is defined by the monoid presentation

$$P_2 =< a, b, a^{-1}, b^{-1} \mid aa^{-1} = bb^{-1} = 1,\ ab^{-1} = ba^{-1} = 0 \text{ for } i \neq j > .$$

Properties of P_2:

- combinatorial;
- 0-bisimple;
- strongly F^*-unitary;
- $\theta : P_2 \to F_2^0$ idempotent pure pre-homomorphism;
- $\theta : u^{-1}v \mapsto \mathrm{red}(u^{-1}v), 0 \mapsto 0$.

We let $\Sigma = \{a, b\}$.

Polycyclic monoid: identity language

Proposition [Schützenberger, Chomsky, Corson]
For all nonempty word $w \in A^*$, if $w \in W(P_2)$, then either

- $w = uv$, where $u, v \in W \setminus \{\emptyset\}$, or
- $w = aWa^{-1}$ or $w = bWb^{-1}$.

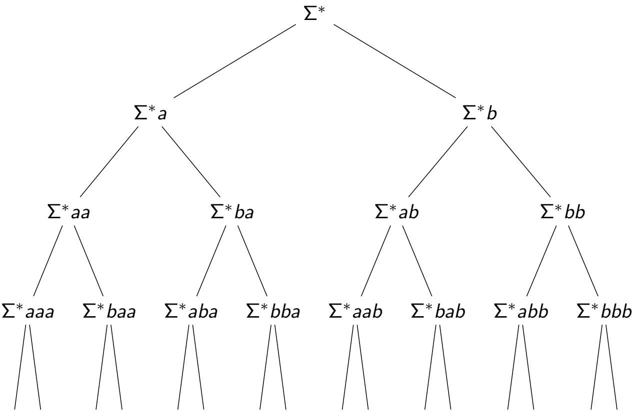
Note: W is the language of properly matched arrangements of parenthesis and brackets:

$$a = (\qquad a^{-1} =) \qquad b = [\qquad b^{-1} =]$$

(restricted Dyck language)

Polycyclic monoids: P^*-representation

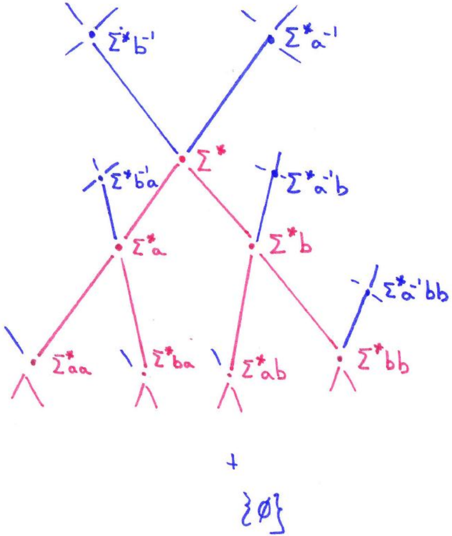
$\mathcal{Y}$:



$$+\{\emptyset\}$$

Polycyclic monoids: P^*-representation

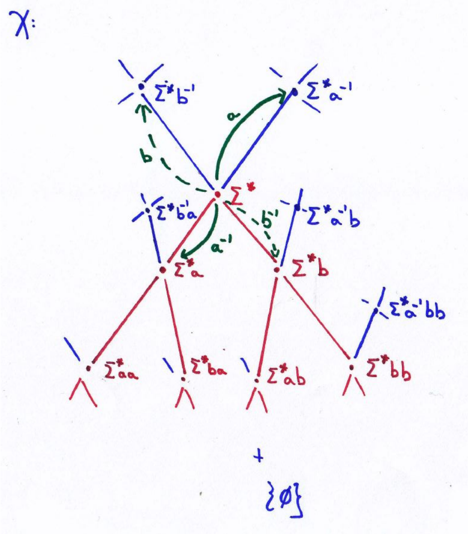
χ:



Polycyclic monoids: P^*-representation

Action of G on $\mathcal{X}$:

$$^{g}\Sigma^* u = \Sigma^* u g^{-1}.$$



Polycyclic monoids: P^*-representation

McAlister 0-triple:

$$(F_2,\ \mathcal{X},\ \mathcal{Y}):$$

- $\mathcal{X}$ is a partially ordered set;
- $\mathcal{Y}$ is a subsemilattice and order ideal of $\mathcal{X}$;
- $G\mathcal{Y} = \mathcal{X}$;
- $g\mathcal{Y} \cap \mathcal{Y} \neq \emptyset$ for all $g \in G$;
- $\mathcal{X}$ has a smallest element: $\emptyset$.

$$P(G, \mathcal{X}, \mathcal{Y}) = \{(A, g) \in \mathcal{Y} \times G : Ag \in \mathcal{Y}\}.$$

Polycyclic monoids: P^*-representation

$$\varphi : P_2 \to P_0(G, \mathcal{X}, \mathcal{Y}) = P(G, \mathcal{X}, \mathcal{Y})/(\{\emptyset\} \times G)$$

$$u^{-1}v \mapsto (\Sigma^* u, u^{-1}v), \quad 0 \mapsto 0$$

$$a \mapsto (\Sigma^*, a), \quad b \mapsto (\Sigma^*, b)$$

$$a^{-1} \mapsto (\Sigma^* a, a^{-1}), \quad b^{-1} \mapsto (\Sigma^* b, b^{-1})$$

Polycyclic monoid: Identity language

Observation: Let

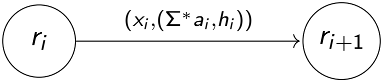
$$w \equiv (f_0, h_0)(f_1, h_1) \dots (f_n, h_n),$$

where $(f_i, h_i) \in \{(\Sigma^*, a), (\Sigma^*, b), (\Sigma^* a, a^{-1}), (\Sigma^* b, b^{-1})\}$.
Then

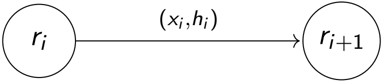
$$w = (\Sigma^*, 1) \iff \begin{aligned} & f_0 = \Sigma^* \\ & h_0 h_1 \dots h_n = 1 \\ & h_0 \dots h_i \in \Sigma^* \quad (1 \leq i \leq n-1) \end{aligned}$$

Polycylic monoid: $\mathcal{L}(P_2) = \mathcal{L}(F_2|\Sigma^*)$

Replace each arrow



with



and vica versa.

0-bisimple strongly E^*-unitary inverse semigroups

Theorem [Lawson 1999]
Let S be a 0-bisimple strongly E^*-unitary inverse monoid and R be the $\mathcal{R}$-class of 1.Then

- $S^* = R^{-1}R$;
- R is a cancellative submonoid;
- principal left-ideals of R are either disjoint or intersect in a principal left ideal;
- R can be embedded in a group.

0-bisimple strongly E^*-unitary inverse semigroups

Theorem [Jiang]
Let M be an 0-bisimple strongly E^*-unitary inverse monoid and R be the $\mathcal{R}$-class of 1. Let $\theta : M \to G^0$ be a suitable homomorphism. Let

$$\mathcal{Y} = \{Ra \mid a \in R\} \cup \{\emptyset\} \qquad \text{and} \qquad \mathcal{X} = \{Ag \mid A \in \mathcal{Y}, g \in G\} \cup \{\emptyset\}$$

and define a transitive action of G on $\mathcal{X}$ by ${}^{h}Ag = Agh^{-1}$. Then $(G, \mathcal{X}, \mathcal{Y})$ is a McAlister 0-triple and we can construct

$$P(G, \mathcal{X}, \mathcal{Y}) = \{(Ra, g) \in \mathcal{Y} \times G \mid Rag \in \mathcal{Y}\}$$

with

$$(Ra, g)(Rb, h) = (Ra \cap {}^{g}Rb, gh).$$

Then

$$S \cong P_0(G, \mathcal{X}, \mathcal{Y}); \quad a^{-1}b \mapsto (Ra, a^{-1}b).$$

0-bisimple strongly E^*-unitary inverse semigroups

Observation:

$$(R, 1) = (Ra_1, g_1)(Ra_2, g_2)\dots(Ra_n, g_n) \Longrightarrow \begin{array}{l} 1 = a_1 \\ 1 = g_1 \dots g_n \\ g_1 \dots g_i \in R \\ (1 \leq i \leq n) \end{array}$$

Conjecture [P Davidson, ED]: Let S be a 0-bisimple strongly F^*-inverse monoid and let R denote the $\mathcal{R}$-class of 1. Let G be a fundamental group of M. Then $\mathcal{L}(S) = \mathcal{L}(G|R)$.

Semidirect products

Observation: Let Y be a semilattice and G be a group acting on Y on the left by automorphisms. Assume that $S = Y \rtimes G$ is finitely generated. Then, for any maximal element $e \in Y$, we have that $\mathcal{L}(S, \{e\}) = \mathcal{L}(G)$.

Further questions

- Understand the relationship between the language classes $\mathcal{L}(G)$ and $\mathcal{L}(G|M)$.
- Understand properties of languages in $\mathcal{L}(G|M)$.
- Understand the relationship between $\mathcal{L}(S)$ and $\mathcal{L}(S/\sigma)$, where S is an E-unitary or strongly E^*-unitary inverse semigroup.
- Understand if $\mathcal{L}(S)$ can be described in terms of $\mathcal{L}(S/\sigma|M)$ for arbitrary E-unitary inverse semigroups.

Thank you for listening!