Semisimple Synchronizing Automata and the Wedderburn-Artin Theory

Emanuele Rodaro
Joint work with J. Almeida

Centro de Matemática, University of Porto
CMUP

DLT 2014

Notation

- A deterministic finite automaton (DFA) is a triple $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ (more appropriate to call semiautomaton), Q set of states, Σ finite alphabet, $\delta : Q \times \Sigma \to Q$ is transition function
- Equivalently, δ describes an action for each $a \in \Sigma$: $q \cdot a = \delta(q, a)$.
- This action extends naturally on the free monoid Σ^*:

$$q \cdot (a_1 \ldots a_n) = (q \cdot a_1 \ldots a_{n-1}) \cdot a_n$$

This action extends also on 2^Q, for $S \subseteq Q$ and $w \in \Sigma^*$:

$$S \cdot w = \{q \cdot w \mid q \in S\}$$

- An automata congruence: equivalence relation $\rho \subseteq Q \times Q$ such that $q \rho q'$ implies $(q \cdot a) \rho (q' \cdot a)$ for all $a \in \Sigma$.
  - The quotient automaton $\mathscr{A}/\rho$ is defined as usual.
  - If the only congruences of $\mathscr{A}$ are the identity $1_{\mathscr{A}}$ and the universal relation $\omega_{\mathscr{A}}$, then $\mathscr{A}$ is called simple.

Notation

- A deterministic finite automaton (DFA) is a triple $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ (more appropriate to call semiautomaton), Q set of states, Σ finite alphabet, $\delta : Q \times \Sigma \to Q$ is transition function
- Equivalently, δ describes an action for each $a \in \Sigma$: $q \cdot a = \delta(q, a)$.
- This action extends naturally on the free monoid Σ^*:

$$q \cdot (a_1 \dots a_n) = (q \cdot a_1 \dots a_{n-1}) \cdot a_n$$

This action extends also on 2^Q, for $S \subseteq Q$ and $w \in \Sigma^*$:

$$S \cdot w = \{q \cdot w \mid q \in S\}$$

- An automata congruence: equivalence relation $\rho \subseteq Q \times Q$ such that $q \rho q'$ implies $(q \cdot a) \rho (q' \cdot a)$ for all $a \in \Sigma$.
  - The quotient automaton $\mathscr{A}/\rho$ is defined as usual.
  - If the only congruences of $\mathscr{A}$ are the identity $1_{\mathscr{A}}$ and the universal relation $\omega_{\mathscr{A}}$, then $\mathscr{A}$ is called simple.

Notation

- A deterministic finite automaton (DFA) is a triple $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ (more appropriate to call semiautomaton), Q set of states, Σ finite alphabet, $\delta : Q \times \Sigma \to Q$ is transition function
- Equivalently, δ describes an action for each $a \in \Sigma$: $q \cdot a = \delta(q, a)$.
- This action extends naturally on the free monoid Σ^*:

$$q \cdot (a_1 \dots a_n) = (q \cdot a_1 \dots a_{n-1}) \cdot a_n$$

This action extends also on 2^Q, for $S \subseteq Q$ and $w \in \Sigma^*$:

$$S \cdot w = \{q \cdot w \mid q \in S\}$$

- An automata congruence: equivalence relation $\rho \subseteq Q \times Q$ such that $q \rho q'$ implies $(q \cdot a) \rho (q' \cdot a)$ for all $a \in \Sigma$.
  - The quotient automaton $\mathscr{A}/\rho$ is defined as usual.
  - If the only congruences of $\mathscr{A}$ are the identity $1_{\mathscr{A}}$ and the universal relation $\omega_{\mathscr{A}}$, then $\mathscr{A}$ is called simple.

Notation

- A deterministic finite automaton (DFA) is a triple $\mathscr{A} = \langle Q, \Sigma, \delta\rangle$ (more appropriate to call semiautomaton), Q set of states, Σ finite alphabet, $\delta : Q \times \Sigma \to Q$ is transition function
- Equivalently, δ describes an action for each $a \in \Sigma$: $q \cdot a = \delta(q, a)$.
- This action extends naturally on the free monoid Σ^*:

$$q \cdot (a_1 \dots a_n) = (q \cdot a_1 \dots a_{n-1}) \cdot a_n$$

  This action extends also on 2^Q, for $S \subseteq Q$ and $w \in \Sigma^*$:

$$S \cdot w = \{q \cdot w \mid q \in S\}$$

- An automata congruence: equivalence relation $\rho \subseteq Q \times Q$ such that $q\rho q'$ implies $(q \cdot a)\rho(q' \cdot a)$ for all $a \in \Sigma$.
  - The quotient automaton $\mathscr{A}/\rho$ is defined as usual.
  - If the only congruences of $\mathscr{A}$ are the identity $1_{\mathscr{A}}$ and the universal relation $\omega_{\mathscr{A}}$, then $\mathscr{A}$ is called simple.

Synchronizing Automata & Cerny's conjecture

- A DFA $\mathscr{A} = \langle Q, \Sigma, \delta \rangle$ is called *synchronizing* if there is a word w whose action *resets* $\mathscr{A}$, that is, leaves the automaton in one particular state no matter which state in Q we start at: $\delta(q, w) = \delta(q', w)$ for all $q, q' \in Q$. Equivalently, $|Q \cdot w| = 1$.
- Any such w is called *synchronizing* or *reset* word for $\mathscr{A}$. The set of resets words is denoted by $\mathrm{Syn}(\mathscr{A})$.
- Mostly know for the following conjecture stated by Jan Černý around 1964:

Cerny's conjecture

Any synchronizing automaton with n states has a reset word of length at most $(n-1)^2$.

Cerny's automata

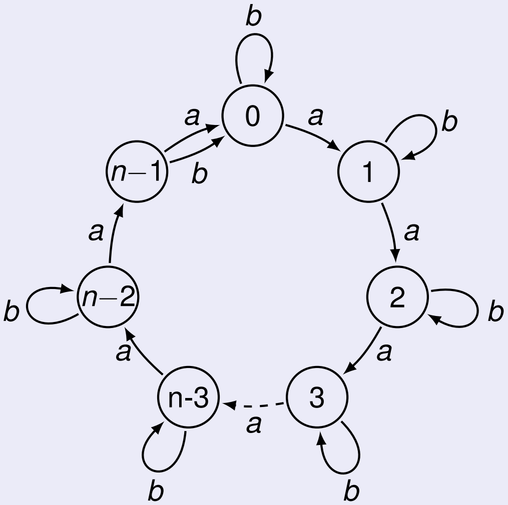
Properties:

-Reach the bound via

$$(ba^{n-1})^{n-2}b$$

-It is simple!

Cerny's series



Cerny's automata

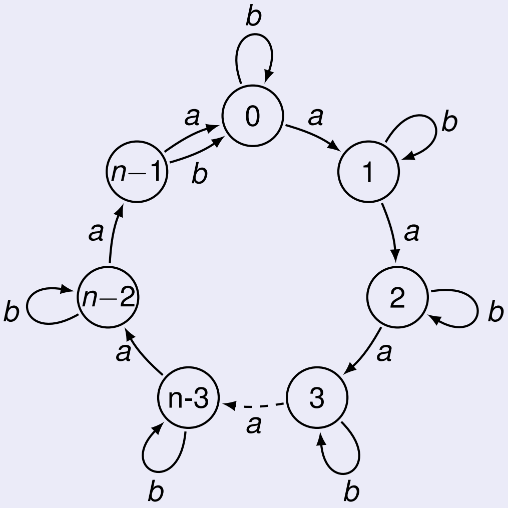
Properties:

-Reach the bound via

$$(ba^{n-1})^{n-2}b$$

-It is simple!

Cerny's series



The importance of being simple

- In an hypothetical proof of Cerny's conjecture by induction on the number of states it is the (non-trivial) base case!
- Automata having letters that act like a primitive group are simple. Primitive: no equivalence relation preserved by the group.
- Many slowly synchronizing automata appear to be simple: Wielandt automata $\mathcal{W}_n$, $\mathcal{D}'_n$, Cerny's series...

Question

Let $\rho \neq \omega_{\mathscr{A}}, 1_{\mathscr{A}}$ be a congruence of $\mathscr{A}$, what is the relation between shortest reset words in $\mathscr{A}$ and $\mathscr{A}/\rho$?

The importance of being simple

- In an hypothetical proof of Cerny's conjecture by induction on the number of states it is the (non-trivial) base case!
- Automata having letters that act like a primitive group are simple. Primitive: no equivalence relation preserved by the group.
- Many slowly synchronizing automata appear to be simple: Wielandt automata $\mathcal{W}_n$, $\mathcal{D}'_n$, Cerny's series...

The importance of being simple

- In an hypothetical proof of Cerny's conjecture by induction on the number of states it is the (non-trivial) base case!
- Automata having letters that act like a primitive group are simple. Primitive: no equivalence relation preserved by the group.
- Many slowly synchronizing automata appear to be simple: Wielandt automata $\mathcal{W}_n$, $\mathcal{D}'_n$, Cerny's series...

Question

Is there a connection between simplicity and "slow" synchronization?

The Wedderburn-Artin approach

- The representation perspective: if $|Q| = n$ each $a \in \Sigma$ can be represented by the incidence matrix of the graph pinpointed by the edges labelled by a in $\mathscr{A}$.
- This gives a representation $\pi : \Sigma^* \to M_n(\mathbb{C}) = \mathrm{End}(\mathbb{C}^n)$.
- Easy exercise to check that Σ^* acts on the subspace

$$Q^{\perp} = \{v \in \mathbb{C}^n : \langle v | (1, \ldots, 1) \rangle = 0\}$$

  giving a representation

$$\varphi : \Sigma^* / \mathrm{Syn}(\mathscr{A}) \hookrightarrow \mathrm{End}(Q^{\perp}) \simeq \mathrm{End}(\mathbb{C}^{n-1}) \simeq M_{n-1}(\mathbb{C})$$

- Consider the monoid $\mathscr{A}^* = \varphi(\Sigma^* / \mathrm{Syn}(\mathscr{A}))$, idea to apply Wedderburn-Artin Theory to the subalgebra $\mathcal{R}$ of $\mathrm{End}(Q^{\perp})$ (finitely) generated by $\mathscr{A}^*$.

The Wedderburn-Artin approach

- The representation perspective: if $|Q| = n$ each $a \in \Sigma$ can be represented by the incidence matrix of the graph pinpointed by the edges labelled by a in $\mathscr{A}$.
- This gives a representation $\pi : \Sigma^* \to M_n(\mathbb{C}) = \mathrm{End}(\mathbb{C}^n)$.
- Easy exercise to check that Σ^* acts on the subspace

$$Q^{\perp} = \{v \in \mathbb{C}^n : \langle v|(1, \ldots, 1)\rangle = 0\}$$

giving a representation

$$\varphi : \Sigma^*/\,\mathrm{Syn}(\mathscr{A}) \hookrightarrow \mathrm{End}(Q^{\perp}) \simeq \mathrm{End}(\mathbb{C}^{n-1}) \simeq M_{n-1}(\mathbb{C})$$

- Consider the monoid $\mathscr{A}^* = \varphi(\Sigma^*/\,\mathrm{Syn}(\mathscr{A}))$, idea to apply Wedderburn-Artin Theory to the subalgebra $\mathcal{R}$ of $\mathrm{End}(Q^{\perp})$ (finitely) generated by $\mathscr{A}^*$.

The Wedderburn-Artin approach

- The representation perspective: if $|Q| = n$ each $a \in \Sigma$ can be represented by the incidence matrix of the graph pinpointed by the edges labelled by a in $\mathscr{A}$.
- This gives a representation $\pi : \Sigma^* \to M_n(\mathbb{C}) = \mathrm{End}(\mathbb{C}^n)$.
- Easy exercise to check that Σ^* acts on the subspace

$$Q^\perp = \{v \in \mathbb{C}^n : \langle v|(1,\dots,1)\rangle = 0\}$$

giving a representation

$$\varphi : \Sigma^*/\mathrm{Syn}(\mathscr{A}) \hookrightarrow \mathrm{End}(Q^\perp) \simeq \mathrm{End}(\mathbb{C}^{n-1}) \simeq M_{n-1}(\mathbb{C})$$

- Consider the monoid $\mathscr{A}^* = \varphi(\Sigma^*/\mathrm{Syn}(\mathscr{A}))$, idea to apply Wedderburn-Artin Theory to the subalgebra $\mathcal{R}$ of $\mathrm{End}(Q^\perp)$ (finitely) generated by $\mathscr{A}^*$.

The Wedderburn-Artin approach

- The representation perspective: if $|Q| = n$ each $a \in \Sigma$ can be represented by the incidence matrix of the graph pinpointed by the edges labelled by a in $\mathscr{A}$.
- This gives a representation $\pi : \Sigma^* \to M_n(\mathbb{C}) = \mathrm{End}(\mathbb{C}^n)$.
- Easy exercise to check that Σ^* acts on the subspace

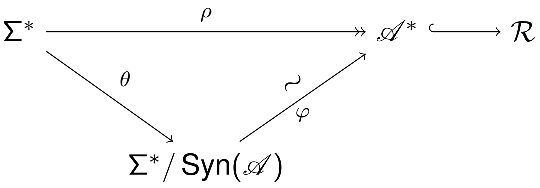
$$Q^\perp = \{v \in \mathbb{C}^n : \langle v|(1,\ldots,1)\rangle = 0\}$$

giving a representation

$$\varphi : \Sigma^*/\,\mathrm{Syn}(\mathscr{A}) \hookrightarrow \mathrm{End}(Q^\perp) \simeq \mathrm{End}(\mathbb{C}^{n-1}) \simeq M_{n-1}(\mathbb{C})$$

- Consider the monoid $\mathscr{A}^* = \varphi(\Sigma^*/\,\mathrm{Syn}(\mathscr{A}))$, idea to apply Wedderburn-Artin Theory to the subalgebra $\mathcal{R}$ of $\mathrm{End}(Q^\perp)$ (finitely) generated by $\mathscr{A}^*$.

The radical of a synchronizing automaton



- Consider the Jacobson radical $\mathrm{Rad}(\mathcal{R})$, then the radical of the automaton $\mathscr{A}$ is the two-sided ideal of Σ^*

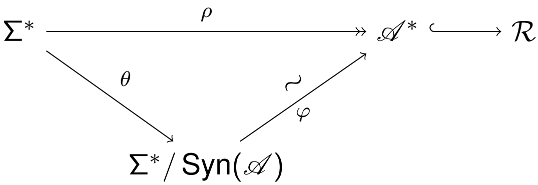
$$\mathrm{Rad}(\mathscr{A}) = \rho^{-1}\left(\mathrm{Rad}(\mathcal{R}) \cap \mathscr{A}^*\right)$$

- An element of $\mathrm{Rad}(\mathscr{A})$ is called a radical word.

Proposition

$\mathrm{Syn}(\mathscr{A}) \subseteq \mathrm{Rad}(\mathscr{A})$, and $\mathrm{Rad}(\mathscr{A}) / \mathrm{Syn}(\mathscr{A})$ is the largest nilpotent left (right) ideal of $\Sigma^* / \mathrm{Syn}(\mathscr{A})$.

The radical of a synchronizing automaton



- Consider the Jacobson radical $\mathrm{Rad}(\mathcal{R})$, then the radical of the automaton $\mathscr{A}$ is the two-sided ideal of Σ^*

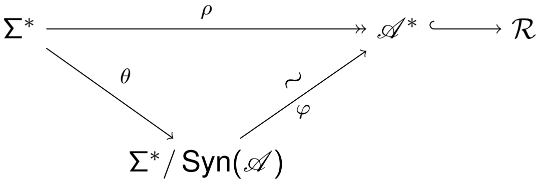
$$\mathrm{Rad}(\mathscr{A}) = \rho^{-1}\left(\mathrm{Rad}(\mathcal{R}) \cap \mathscr{A}^*\right)$$

- An element of $\mathrm{Rad}(\mathscr{A})$ is called a radical word.

Proposition

$\mathrm{Syn}(\mathscr{A}) \subseteq \mathrm{Rad}(\mathscr{A})$, and $\mathrm{Rad}(\mathscr{A}) / \mathrm{Syn}(\mathscr{A})$ is the largest nilpotent left (right) ideal of $\Sigma^* / \mathrm{Syn}(\mathscr{A})$.

The radical of a synchronizing automaton



- Consider the Jacobson radical $\mathrm{Rad}(\mathcal{R})$, then the radical of the automaton $\mathscr{A}$ is the two-sided ideal of Σ^*

$$\mathrm{Rad}(\mathscr{A}) = \rho^{-1}(\mathrm{Rad}(\mathcal{R}) \cap \mathscr{A}^*)$$

- An element of $\mathrm{Rad}(\mathscr{A})$ is called a radical word.

Proposition

$\mathrm{Syn}(\mathscr{A}) \subseteq \mathrm{Rad}(\mathscr{A})$, *and* $\mathrm{Rad}(\mathscr{A}) / \mathrm{Syn}(\mathscr{A})$ *is the largest nilpotent left (right) ideal of* $\Sigma^* / \mathrm{Syn}(\mathscr{A})$.

The importance of radical words

- Looking for radical words gives information on the synchronizing words (a suitable power of the radical word is a reset word).
- In particular, upper bounds on radical words give upper bound on the reset words.
- We call $\mathscr{A}$ semisimple whenever $\text{Rad}(\mathscr{A}) = \text{Syn}(\mathscr{A})$. Thus in this case looking for radical words is the same as looking for reset words.
- Factoring the problem using the Wedderburn-Artin theory.

The importance of radical words

- Looking for radical words gives information on the synchronizing words (a suitable power of the radical word is a reset word).
- In particular, upper bounds on radical words give upper bound on the reset words.
- We call $\mathscr{A}$ semisimple whenever $\mathrm{Rad}(\mathscr{A}) = \mathrm{Syn}(\mathscr{A})$. Thus in this case looking for radical words is the same as looking for reset words.
- Factoring the problem using the Wedderburn-Artin theory.

Weak Cerny's conjecture/Radical conjecture

Every synchronizing automaton with n states has a radical word of length at most $(n-1)^2$.

The importance of radical words

- Looking for radical words gives information on the synchronizing words (a suitable power of the radical word is a reset word).
- In particular, upper bounds on radical words give upper bound on the reset words.
- We call $\mathscr{A}$ semisimple whenever $\mathrm{Rad}(\mathscr{A}) = \mathrm{Syn}(\mathscr{A})$. Thus in this case looking for radical words is the same as looking for reset words.
- Factoring the problem using the Wedderburn-Artin theory.

The importance of radical words

- Looking for radical words gives information on the synchronizing words (a suitable power of the radical word is a reset word).
- In particular, upper bounds on radical words give upper bound on the reset words.
- We call $\mathscr{A}$ semisimple whenever $\mathrm{Rad}(\mathscr{A}) = \mathrm{Syn}(\mathscr{A})$. Thus in this case looking for radical words is the same as looking for reset words.
- Factoring the problem using the Wedderburn-Artin theory.

Theorem

A synchronizing automaton which is simple is also semisimple.

The importance of radical words

- Looking for radical words gives information on the synchronizing words (a suitable power of the radical word is a reset word).
- In particular, upper bounds on radical words give upper bound on the reset words.
- We call $\mathscr{A}$ semisimple whenever $\mathrm{Rad}(\mathscr{A}) = \mathrm{Syn}(\mathscr{A})$. Thus in this case looking for radical words is the same as looking for reset words.
- Factoring the problem using the Wedderburn-Artin theory.

Theorem

A synchronizing automaton which is simple is also semisimple.

Factoring the problem via the Wedderburn-Artin theorem

- Using this theorem we have:

$$\mathcal{R}/\,\mathsf{Rad}(\mathcal{R}) \simeq \mathbb{M}_{n_1}(\mathbb{C}) \times \ldots \times \mathbb{M}_{n_k}(\mathbb{C})$$

  for some (uniquely determined) positive integers $n_1, \ldots, n_k$.

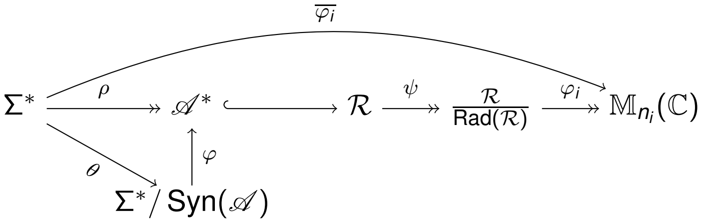
- Thus the problem of looking for radical words is “factorized” into the sub-problems of looking for words that are “zeros” in each component.

Factoring the problem via the Wedderburn-Artin theorem

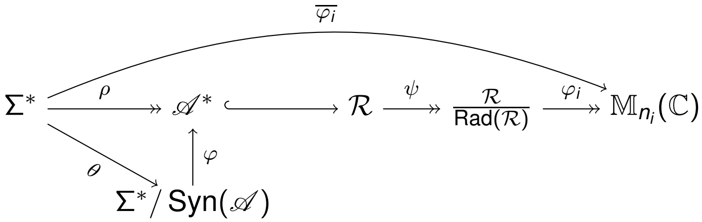
- Using this theorem we have:

$$\mathcal{R}/\,\mathrm{Rad}(\mathcal{R}) \simeq \mathbb{M}_{n_1}(\mathbb{C}) \times \ldots \times \mathbb{M}_{n_k}(\mathbb{C})$$

  for some (uniquely determined) positive integers $n_1, \ldots, n_k$.
- Thus the problem of looking for radical words is "factorized" into the sub-problems of looking for words that are "zeros" in each component.

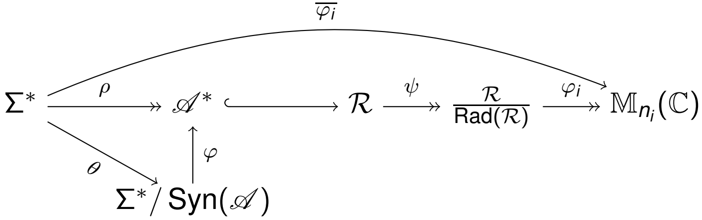


Factoring the problem via the Wedderburn-Artin theorem



- Strategy: for each $i = 1, \ldots k$ find "small" words w_i such that $\overline{\varphi_i}(w_i) = 0_i$ in $\mathbb{M}_{n_i}(\mathbb{C})$.
- Then concatenate: $w_1 \ldots w_k \in \mathrm{Rad}(\mathscr{A})$. In particular, if $\mathscr{A}$ is semisimple then $w_1 \ldots w_k \in \mathrm{Syn}(\mathscr{A})$.

Factoring the problem via the Wedderburn-Artin theorem



- Strategy: for each $i = 1, \ldots k$ find "small" words w_i such that $\overline{\varphi_i}(w_i) = 0_i$ in $\mathbb{M}_{n_i}(\mathbb{C})$.
- Then concatenate: $w_1 \ldots w_k \in \mathrm{Rad}(\mathscr{A})$. In particular, if $\mathscr{A}$ is semisimple then $w_1 \ldots w_k \in \mathrm{Syn}(\mathscr{A})$.

A working case

- Consider the i-th factor monoid $\mathcal{M}_i = \overline{\varphi_i}(\Sigma^*)$.

Lemma

$\mathcal{M}_i$ has a unique 0-minimal ideal $\mathcal{I}_i$ which is a 0-simple semigroup. Furthermore, $\mathcal{M}_i$ acts faithfully on the right and left of $\mathcal{I}_i$.

- An interesting case: $\mathcal{I}_i \setminus \{0\}$ is subsemigroup of $\mathcal{M}_i$. With some technical work one can prove:

Theorem

Consider an ideal I of $\mathcal{R}/\operatorname{Rad}(\mathcal{R}) \simeq \mathbb{M}_{n_1}(\mathbb{C}) \times \ldots \times \mathbb{M}_{n_k}(\mathbb{C})$ of the form

$$I = \mathbb{M}_{n_{i_1}}(\mathbb{C}) \times \ldots \times \mathbb{M}_{n_{i_m}}(\mathbb{C})$$

for some choices $i_1, \ldots, i_m$ of $\{1, \ldots, k\}$, such that the associated 0-minimal ideals $\mathcal{I}_{i_j} \setminus \{0\}$, are semigroups. Then there is a word $u \in \Sigma^*$ with $|u| \leq (n-1)^2$ such that $\overline{\varphi_{i_j}}(u) = 0_{i_j}$ for all $j = 1, \ldots, m$.

A working case

- Consider the i-th factor monoid $\mathcal{M}_i = \overline{\varphi_i}(\Sigma^*)$.

Lemma

$\mathcal{M}_i$ has a unique 0-minimal ideal $\mathcal{I}_i$ which is a 0-simple semigroup. Furthermore, $\mathcal{M}_i$ acts faithfully on the right and left of $\mathcal{I}_i$.

- An interesting case: $\mathcal{I}_i \setminus \{0\}$ is subsemigroup of $\mathcal{M}_i$. With some technical work one can prove:

Theorem

Consider an ideal I of $\mathcal{R}/\operatorname{Rad}(\mathcal{R}) \simeq \mathbb{M}_{n_1}(\mathbb{C}) \times \ldots \times \mathbb{M}_{n_k}(\mathbb{C})$ of the form

$$I = \mathbb{M}_{n_{i_1}}(\mathbb{C}) \times \ldots \times \mathbb{M}_{n_{i_m}}(\mathbb{C})$$

for some choices $i_1, \ldots, i_m$ of $\{1, \ldots, k\}$, such that the associated 0-minimal ideals $\mathcal{I}_{i_j} \setminus \{0\}$, are semigroups. Then there is a word $u \in \Sigma^*$ with $|u| \leq (n-1)^2$ such that $\overline{\varphi_{i_j}}(u) = 0_{i_j}$ for all $j = 1, \ldots, m$.

A working case

- Consider the i-th factor monoid $\mathcal{M}_i = \overline{\varphi_i}(\Sigma^*)$.

Lemma

$\mathcal{M}_i$ has a unique 0-minimal ideal $\mathcal{I}_i$ which is a 0-simple semigroup. Furthermore, $\mathcal{M}_i$ acts faithfully on the right and left of $\mathcal{I}_i$.

- An interesting case: $\mathcal{I}_i \setminus \{0\}$ is subsemigroup of $\mathcal{M}_i$. With some technical work one can prove:

Theorem

Consider an ideal I of $\mathcal{R}/\operatorname{Rad}(\mathcal{R}) \simeq \mathbb{M}_{n_1}(\mathbb{C}) \times \ldots \times \mathbb{M}_{n_k}(\mathbb{C})$ of the form

$$I = \mathbb{M}_{n_{i_1}}(\mathbb{C}) \times \ldots \times \mathbb{M}_{n_{i_m}}(\mathbb{C})$$

for some choices $i_1, \ldots, i_m$ of $\{1, \ldots, k\}$, such that the associated 0-minimal ideals $\mathcal{I}_{i_j} \setminus \{0\}$, are semigroups. Then there is a word $u \in \Sigma^*$ with $|u| \leq (n-1)^2$ such that $\overline{\varphi_{i_j}}(u) = 0_{i_j}$ for all $j = 1, \ldots, m$.

A working case

- Consider the i-th factor monoid $\mathcal{M}_i = \overline{\varphi_i}(\Sigma^*)$.

Lemma

$\mathcal{M}_i$ has a unique 0-minimal ideal $\mathcal{I}_i$ which is a 0-simple semigroup. Furthermore, $\mathcal{M}_i$ acts faithfully on the right and left of $\mathcal{I}_i$.

- An interesting case: $\mathcal{I}_i \setminus \{0\}$ is subsemigroup of $\mathcal{M}_i$. With some technical work one can prove:

Theorem

Consider an ideal I of $\mathcal{R}/\operatorname{Rad}(\mathcal{R}) \simeq \mathbb{M}_{n_1}(\mathbb{C}) \times \ldots \times \mathbb{M}_{n_k}(\mathbb{C})$ of the form

$$I = \mathbb{M}_{n_{i_1}}(\mathbb{C}) \times \ldots \times \mathbb{M}_{n_{i_m}}(\mathbb{C})$$

for some choices $i_1, \ldots, i_m$ of $\{1, \ldots, k\}$, such that the associated 0-minimal ideals $\mathcal{I}_{i_j} \setminus \{0\}$, are semigroups. Then there is a word $u \in \Sigma^*$ with $|u| \leq (n-1)^2$ such that $\overline{\varphi_{i_j}}(u) = 0_{i_j}$ for all $j = 1, \ldots, m$.

A less abstract case: strongly semisimple

- Unfortunately we could not prove Cerny's conjecture for semisimple synchronizing automata, this would be probably a major breakthrough to this conjecture.
- A stronger condition: strongly semisimple. We recall the root of a (regular) language

$$\mathrm{root}(L) = \{u \in \Sigma^* : \exists m \geq 1, u^m \in L\}$$

- By previous proposition if $u \in \mathrm{Rad}(\mathscr{A})$ then $u^\ell \in \mathrm{Syn}(\mathscr{A})$ (actually $\ell \leq |Q| - 1$), if $\mathrm{Syn}(\mathscr{A})$ is closed by taking roots, then $\mathrm{Syn}(\mathscr{A}) = \mathrm{Rad}(\mathscr{A})$, i.e. it is semisimple!

A less abstract case: strongly semisimple

- Unfortunately we could not prove Cerny's conjecture for semisimple synchronizing automata, this would be probably a major breakthrough to this conjecture.
- A stronger condition: strongly semisimple. We recall the root of a (regular) language

$$\mathrm{root}(L) = \{u \in \Sigma^* : \exists m \geq 1, u^m \in L\}$$

- By previous proposition if $u \in \mathrm{Rad}(\mathscr{A})$ then $u^\ell \in \mathrm{Syn}(\mathscr{A})$ (actually $\ell \leq |Q| - 1$), if $\mathrm{Syn}(\mathscr{A})$ is closed by taking roots, then $\mathrm{Syn}(\mathscr{A}) = \mathrm{Rad}(\mathscr{A})$, i.e. it is semisimple!

A less abstract case: strongly semisimple

- Unfortunately we could not prove Cerny's conjecture for semisimple synchronizing automata, this would be probably a major breakthrough to this conjecture.
- A stronger condition: strongly semisimple. We recall the root of a (regular) language

$$\mathrm{root}(L) = \{u \in \Sigma^* : \exists m \geq 1, u^m \in L\}$$

- By previous proposition if $u \in \mathrm{Rad}(\mathscr{A})$ then $u^\ell \in \mathrm{Syn}(\mathscr{A})$ (actually $\ell \leq |Q| - 1$), if $\mathrm{Syn}(\mathscr{A})$ is closed by taking roots, then $\mathrm{Syn}(\mathscr{A}) = \mathrm{Rad}(\mathscr{A})$, i.e. it is semisimple!

Definition (strongly semisimple)

$\mathscr{A}$ is called strongly semisimple if $\mathrm{Syn}(\mathscr{A})$ is closed by taking roots.

A less abstract case: strongly semisimple

- Unfortunately we could not prove Cerny's conjecture for semisimple synchronizing automata, this would be probably a major breakthrough to this conjecture.
- A stronger condition: strongly semisimple. We recall the root of a (regular) language

$$\text{root}(L) = \{u \in \Sigma^* : \exists m \geq 1, u^m \in L\}$$

- By previous proposition if $u \in \text{Rad}(\mathscr{A})$ then $u^\ell \in \text{Syn}(\mathscr{A})$ (actually $\ell \leq |Q| - 1$), if $\text{Syn}(\mathscr{A})$ is closed by taking roots, then $\text{Syn}(\mathscr{A}) = \text{Rad}(\mathscr{A})$, i.e. it is semisimple!

Proposition

$\text{Syn}(\mathscr{A}) \subseteq \text{Rad}(\mathscr{A})$, *and* $\text{Rad}(\mathscr{A}) / \text{Syn}(\mathscr{A})$ *is the largest nilpotent left (right) ideal of* $\Sigma^* / \text{Syn}(\mathscr{A})$.

Cyclic ideal languages

- Syn($\mathscr{A}$) is a two-sided ideal (regular) language, for shor ideal.
- Given an ideal I, it is called cyclic whenever root(I) $= I$.
- The name "cyclic" comes from the fact that I is also a cyclic language (studied by Béal, Carton, Reutenauer).
- We have found a characterization of cyclic ideal languages. First we need a couple of notations.
- For a language L, $\sqrt{L} = \{u \in \Sigma^* : u^2 \in L\}$. Let $x, y \in \Sigma^*$ with $x = vx'$ and $y = y'v$, where $v \in \Sigma^*$ is the maximal prefix of x which is also a suffix of y, we define the concatenation with overlap as $y \circ x = y'vx'$.

Cyclic ideal languages

- Syn($\mathscr{A}$) is a two-sided ideal (regular) language, for shor ideal.
- Given an ideal I, it is called cyclic whenever root(I) $= I$.
- The name "cyclic" comes from the fact that I is also a cyclic language (studied by Béal, Carton, Reutenauer).
- We have found a characterization of cyclic ideal languages. First we need a couple of notations.
- For a language L, $\sqrt{L} = \{u \in \Sigma^* : u^2 \in L\}$. Let $x, y \in \Sigma^*$ with $x = vx'$ and $y = y'v$, where $v \in \Sigma^*$ is the maximal prefix of x which is also a suffix of y, we define the concatenation with overlap as $y \circ x = y'vx'$.

Cyclic ideal languages

- Syn($\mathscr{A}$) is a two-sided ideal (regular) language, for shor ideal.
- Given an ideal I, it is called cyclic whenever $\mathrm{root}(I) = I$.
- The name "cyclic" comes from the fact that I is also a cyclic language (studied by Béal, Carton, Reutenauer).
- We have found a characterization of cyclic ideal languages. First we need a couple of notations.
- For a language L, $\sqrt{L} = \{u \in \Sigma^* : u^2 \in L\}$. Let $x, y \in \Sigma^*$ with $x = vx'$ and $y = y'v$, where $v \in \Sigma^*$ is the maximal prefix of x which is also a suffix of y, we define the concatenation with overlap as $y \circ x = y'vx'$.

Cyclic ideal languages

- Syn($\mathscr{A}$) is a two-sided ideal (regular) language, for shor ideal.
- Given an ideal I, it is called cyclic whenever $\text{root}(I) = I$.
- The name "cyclic" comes from the fact that I is also a cyclic language (studied by Béal, Carton, Reutenauer).
- We have found a characterization of cyclic ideal languages. First we need a couple of notations.
- For a language L, $\sqrt{L} = \{u \in \Sigma^* : u^2 \in L\}$. Let $x, y \in \Sigma^*$ with $x = vx'$ and $y = y'v$, where $v \in \Sigma^*$ is the maximal prefix of x which is also a suffix of y, we define the concatenation with overlap as $y \circ x = y'vx'$.

Cyclic ideal languages

- Syn($\mathscr{A}$) is a two-sided ideal (regular) language, for shor ideal.
- Given an ideal I, it is called cyclic whenever $\mathrm{root}(I) = I$.
- The name "cyclic" comes from the fact that I is also a cyclic language (studied by Béal, Carton, Reutenauer).
- We have found a characterization of cyclic ideal languages. First we need a couple of notations.
- For a language L, $\sqrt{L} = \{u \in \Sigma^* : u^2 \in L\}$. Let $x, y \in \Sigma^*$ with $x = vx'$ and $y = y'v$, where $v \in \Sigma^*$ is the maximal prefix of x which is also a suffix of y, we define the concatenation with overlap as $y \circ x = y'vx'$.

Cyclic ideal languages

Theorem

Given an ideal language I, the following are equivalent.

i) $\mathrm{root}(I) = I$;

ii) $\sqrt{I} \subseteq I$;

iii) *for any $u \in I$ and any factorization $u = xy$, for some $x, y \in \Sigma^*$, then $y \circ x \in I$;*

iv) *$I = \eta^{-1}(0)$ where $\eta : \Sigma^* \to S$ is a morphism onto a finite monoid with 0 satisfying the condition $x^2 = 0 \Rightarrow x = 0$.*

Cerny's conjecture for strongly semisimple

- Existence for such automata, i.e., synchronizing automata $\mathscr{A}$ having Syn($\mathscr{A}$) which is a cyclic ideal.
- Given an a cyclic ideal I, the minimal DFA recognizing I is synchronizing with a sink state. However, Cerny's conjecture holds for such class. It is well know that the difficult case is when the synchronizing automaton is strongly connected.
- For these cases Cerny's conjecture holds.

Cerny's conjecture for strongly semisimple

- Existence for such automata, i.e., synchronizing automata $\mathscr{A}$ having Syn($\mathscr{A}$) which is a cyclic ideal.
- Given an a cyclic ideal I, the minimal DFA recognizing I is synchronizing with a sink state. However, Cerny's conjecture holds for such class. It is well know that the difficult case is when the synchronizing automaton is strongly connected.
- For these cases Cerny's conjecture holds.

Cerny's conjecture for strongly semisimple

- Existence for such automata, i.e., synchronizing automata $\mathscr{A}$ having Syn($\mathscr{A}$) which is a cyclic ideal.
- Given an a cyclic ideal I, the minimal DFA recognizing I is synchronizing with a sink state. However, Cerny's conjecture holds for such class. It is well know that the difficult case is when the synchronizing automaton is strongly connected.
- For these cases Cerny's conjecture holds.

Theorem (Reis, R.)

Let I be an ideal language on a non-unary alphabet, then there is a strongly connected synchronizing automaton having I as the set of synchronizing words.

Cerny's conjecture for strongly semisimple

- Existence for such automata, i.e., synchronizing automata $\mathscr{A}$ having Syn($\mathscr{A}$) which is a cyclic ideal.
- Given an a cyclic ideal I, the minimal DFA recognizing I is synchronizing with a sink state. However, Cerny's conjecture holds for such class. It is well know that the difficult case is when the synchronizing automaton is strongly connected.
- For these cases Cerny's conjecture holds.

Theorem

A strongly semisimple synchronizing automaton $\mathscr{A}$ satisfies the Cerny conjecture.


The End