

Characterizing classes of regular languages using prefix codes of bounded synchronization delay

Volker Diekert¹

Universität Stuttgart

MPS2106, Bordeaux, March 21st, 2016

in memoriam: Marcel-Paul Schützenberger

¹Joint work with Tobias Walter

- ① On finite monoids having only trivial subgroups.

Information and Control, 8:190–194, 1965.

$$\text{SF}(A^*) = \mathbf{AP}(A^*)$$

- ① On finite monoids having only trivial subgroups.

Information and Control, 8:190–194, 1965.

$$\text{SF}(A^*) = \mathbf{AP}(A^*) = \text{FO}[<](A^*)$$

- ① On finite monoids having only trivial subgroups.

Information and Control, 8:190–194, 1965.

$$\text{SF}(A^*) = \mathbf{AP}(A^*) = \text{FO}[<](A^*) = \text{LTL}(A^*)$$

Classics of Schützenberger and a generalization

- ① On finite monoids having only trivial subgroups.

Information and Control, 8:190–194, 1965.

$$\text{SF}(A^*) = \mathbf{AP}(A^*) = \text{FO}[<](A^*) = \text{LTL}(A^*)$$

- ② Sur certaines opérations de fermeture dans les langages rationnels.

In *Symposia Mathematica, Vol. XV (Convegno di Informatica Teorica, INDAM, Roma, 1973)*, pages 245–253, 1975.

$$\text{SD}(A^*) = \text{SF}(A^*) = \mathbf{AP}(A^*) = \bar{\mathbf{1}}(A^*)$$

Classics of Schützenberger and a generalization

- ① On finite monoids having only trivial subgroups.

Information and Control, 8:190–194, 1965.

$$\text{SF}(A^*) = \mathbf{AP}(A^*) = \text{FO}[\prec](A^*) = \text{LTL}(A^*)$$

- ② Sur certaines opérations de fermeture dans les langages rationnels.

In *Symposia Mathematica, Vol. XV (Convegno di Informatica Teorica, INDAM, Roma, 1973)*, pages 245–253, 1975.

$$\text{SD}(A^*) = \text{SF}(A^*) = \mathbf{AP}(A^*) = \overline{\mathbf{1}}(A^*)$$

- ③ Sur les monoides finis dont les groupes sont commutatifs.
RAIRO, 8(R-1):55–61, 1974.

$$\text{SD}_{\mathbf{Ab}}(A^*) = \overline{\mathbf{Ab}}(A^*)$$

Theorem (D. and Walter 2016)

$$\text{SD}_{\mathbf{H}}(A^\infty) = \overline{\mathbf{H}}(A^\infty)$$

Notation

- $A =$ finite alphabet

Notation

- A = finite alphabet
- A^* = finite words, A^ω = infinite words, $A^\infty = A^* \cup A^\omega$.

Notation

- A = finite alphabet
- A^* = finite words, A^ω = infinite words, $A^\infty = A^* \cup A^\omega$.
- **Regular languages:** finite subsets & closure under union, concatenation, and Kleene-star
= recognizable by a finite monoid.

Notation

- A = finite alphabet
- A^* = finite words, A^ω = infinite words, $A^\infty = A^* \cup A^\omega$.
- **Regular languages**: finite subsets & closure under union, concatenation, and Kleene-star
= recognizable by a finite monoid.
- **Star-free languages**: finite subsets & closure under union, concatenation, complementation, but **no Kleene-star**
= recognizable by a finite **aperiodic** monoid.

Notation

- A = finite alphabet
- A^* = finite words, A^ω = infinite words, $A^\infty = A^* \cup A^\omega$.
- **Regular languages**: finite subsets & closure under union, concatenation, and Kleene-star
= recognizable by a finite monoid.
- **Star-free languages**: finite subsets & closure under union, concatenation, complementation, but **no Kleene-star**
= recognizable by a finite **aperiodic** monoid.
- $h : A^* \rightarrow M$ **recognizes** $L \subseteq A^*$ if $h^{-1}(h(L)) = L$.

Notation

- A = finite alphabet
- A^* = finite words, A^ω = infinite words, $A^\infty = A^* \cup A^\omega$.
- **Regular languages**: finite subsets & closure under union, concatenation, and Kleene-star
= recognizable by a finite monoid.
- **Star-free languages**: finite subsets & closure under union, concatenation, complementation, but **no Kleene-star**
= recognizable by a finite **aperiodic** monoid.
- $h : A^* \rightarrow M$ **recognizes** $L \subseteq A^*$ if $h^{-1}(h(L)) = L$.
- M is **aperiodic** if all subgroups are trivial.

Notation

- A = finite alphabet
- A^* = finite words, A^ω = infinite words, $A^\infty = A^* \cup A^\omega$.
- **Regular languages**: finite subsets & closure under union, concatenation, and Kleene-star
= recognizable by a finite monoid.
- **Star-free languages**: finite subsets & closure under union, concatenation, complementation, but **no Kleene-star**
= recognizable by a finite **aperiodic** monoid.
- $h : A^* \rightarrow M$ **recognizes** $L \subseteq A^*$ if $h^{-1}(h(L)) = L$.
- M is **aperiodic** if all subgroups are trivial.
- $\mathbf{1} = \{1\}$ = trivial group, \mathbf{Ab} = finite abelian groups,
 \mathbf{Sol} = finite solvable groups, \mathbf{G} = all finite groups,
 \mathbf{Mon} = all finite monoids.

Varieties

A **variety** means here a class of finite monoids which is closed under finite direct products and divisors. A monoid N is a **divisor** of M if N is the homomorphic image of a submonoid of M .

Example

$\mathbf{1}$, \mathbf{Ab} , \mathbf{Sol} , \mathbf{G} are varieties of groups.

If \mathbf{V} is a variety, then we let

$$\mathbf{V}(A^*) = \{L \subseteq A^* \mid L \text{ is recognized by some } M \in \mathbf{V}\}.$$

If \mathbf{H} is a variety of groups, then

$$\overline{\mathbf{H}} = \{M \in \mathbf{Mon} \mid \text{all subgroups of } M \text{ are in } \mathbf{H}\}.$$

Example

$\overline{\mathbf{1}} = \mathbf{AP}$, $\overline{\mathbf{G}} = \mathbf{Mon}$.

Prefix codes of bounded synchronization delay

$K \subseteq A^+$ is called **prefix code** if it is **prefix-free**. That is: $u, uv \in K$ implies $u = uv$.

A prefix-free language K is a code since every word $u \in K^*$ admits a unique factorization $u = u_1 \cdots u_k$ with $k \geq 0$ and $u_i \in K$.

A prefix code K has **bounded synchronization delay** if for some $d \in \mathbb{N}$ and for all $u, v, w \in A^*$ we have:
if $uvw \in K^*$ and $v \in K^d$, then $uv \in K^*$.

Example

Every $B \subseteq A$ yields a prefix code with synchronization delay 0.
If $c \in A \setminus B$, then B^*c is a prefix code with synchr. delay 1.

Application

Assume that Alice sends a message using a prefix code K with synchronization delay d of the form

$$u_1v_1w_1 u_2v_2w_2 u_3v_3w_3 \cdots u_kv_kw_k$$

with $u_i, v_i, w_i \in K^*$, but Bob receives, say due to noise, only a subsequence:

$$?v_1w_1?v_2w_2?v_3w_3 \cdots?v_kw_k$$

such that $v_i \in K^d$. Then Bob can recover a subsequence of the original message corresponding to the subsequence

$$(w_1, w_2, w_3, \dots, w_k) \in (K^*)^k.$$

\mathbf{H} = a variety of groups

Lemma

Let $K \in \overline{\mathbf{H}}(A^*)$ be a prefix code of bounded synchronization delay.
Then: $K^* \in \overline{\mathbf{H}}(A^*)$.

Proof.

We have

$$A^* \setminus K^* = \bigcup_{0 \leq i} (K^i A A^* \setminus K^{i+1} A^*).$$

Now, let d be the synchronization delay of K . Then we can write

$$A^* \setminus K^* = A^* K^d (A A^* \setminus K A^*) \cup \bigcup_{0 \leq i < d} (K^i A A^* \setminus K^{i+1} A^*).$$



Group languages and generalized group languages

Let G be a finite group and \mathcal{C} a class of languages.

$L \subseteq A^*$ is a **group language for G** , if $L = \gamma^{-1}(1)$ for some homomorphism $\gamma : A^* \rightarrow G$.

Group languages and generalized group languages

Let G be a finite group and \mathcal{C} a class of languages.

$L \subseteq A^*$ is a **group language for G** , if $L = \gamma^{-1}(1)$ for some homomorphism $\gamma : A^* \rightarrow G$.

$L \subseteq A^*$ is a **generalized group language for G over \mathcal{C}** , if $L = \gamma^{-1}(1)$ for some homomorphism $\gamma : K^* \rightarrow G$ such that

- 1 $K \subseteq A^+$ is a prefix code of bounded synchronization delay,

Group languages and generalized group languages

Let G be a finite group and \mathcal{C} a class of languages.

$L \subseteq A^*$ is a **group language for G** , if $L = \gamma^{-1}(1)$ for some homomorphism $\gamma : A^* \rightarrow G$.

$L \subseteq A^*$ is a **generalized group language for G over \mathcal{C}** , if $L = \gamma^{-1}(1)$ for some homomorphism $\gamma : K^* \rightarrow G$ such that

- 1 $K \subseteq A^+$ is a prefix code of bounded synchronization delay,
- 2 $(\gamma^{-1}(g) \cap K) \in \mathcal{C}$ for all $g \in G$.

Group languages and generalized group languages

Let G be a finite group and \mathcal{C} a class of languages.

$L \subseteq A^*$ is a **group language for G** , if $L = \gamma^{-1}(1)$ for some homomorphism $\gamma : A^* \rightarrow G$.

$L \subseteq A^*$ is a **generalized group language for G over \mathcal{C}** , if $L = \gamma^{-1}(1)$ for some homomorphism $\gamma : K^* \rightarrow G$ such that

- 1 $K \subseteq A^+$ is a prefix code of bounded synchronization delay,
- 2 $(\gamma^{-1}(g) \cap K) \in \mathcal{C}$ for all $g \in G$.

Proposition (Schützenberger (1974))

Let $L \subseteq A^$ be a generalized group language for G over $\overline{\mathbf{H}}(A^*)$ with $G \in \mathbf{H}$. Then we have $L \in \overline{\mathbf{H}}(A^*)$.*

Schützenberger's $SD_{\mathbf{H}}$ classes

By $SD_{\mathbf{H}}(A^*)$ we denote the set of regular languages which is inductively defined as follows.

Schützenberger's $SD_{\mathbf{H}}$ classes

By $SD_{\mathbf{H}}(A^*)$ we denote the set of regular languages which is inductively defined as follows.

- 1 Finite subsets of A^* are in $SD_{\mathbf{H}}(A^*)$.

Schützenberger's $SD_{\mathbf{H}}$ classes

By $SD_{\mathbf{H}}(A^*)$ we denote the set of regular languages which is inductively defined as follows.

- 1 Finite subsets of A^* are in $SD_{\mathbf{H}}(A^*)$.
- 2 If $L, K \in SD_{\mathbf{H}}(A^*)$, then $L \cup K, L \cdot K \in SD_{\mathbf{H}}(A^*)$

Schützenberger's $SD_{\mathbf{H}}$ classes

By $SD_{\mathbf{H}}(A^*)$ we denote the set of regular languages which is inductively defined as follows.

- 1 Finite subsets of A^* are in $SD_{\mathbf{H}}(A^*)$.
- 2 If $L, K \in SD_{\mathbf{H}}(A^*)$, then $L \cup K, L \cdot K \in SD_{\mathbf{H}}(A^*)$
- 3 If $L \subseteq A^*$ is a generalized group language for G over $SD_{\mathbf{H}}(A^*)$ with $G \in \mathbf{H}$, then $L \in SD_{\mathbf{H}}(A^*)$

Schützenberger's $SD_{\mathbf{H}}$ classes

By $SD_{\mathbf{H}}(A^*)$ we denote the set of regular languages which is inductively defined as follows.

- 1 Finite subsets of A^* are in $SD_{\mathbf{H}}(A^*)$.
- 2 If $L, K \in SD_{\mathbf{H}}(A^*)$, then $L \cup K, L \cdot K \in SD_{\mathbf{H}}(A^*)$
- 3 If $L \subseteq A^*$ is a generalized group language for G over $SD_{\mathbf{H}}(A^*)$ with $G \in \mathbf{H}$, then $L \in SD_{\mathbf{H}}(A^*)$

Proposition (Schützenberger (1974) reformulated)

$$SD_{\mathbf{H}}(A^*) \subseteq \overline{\mathbf{H}}(A^*)$$

Schützenberger's $SD_{\mathbf{H}}$ classes

By $SD_{\mathbf{H}}(A^*)$ we denote the set of regular languages which is inductively defined as follows.

- 1 Finite subsets of A^* are in $SD_{\mathbf{H}}(A^*)$.
- 2 If $L, K \in SD_{\mathbf{H}}(A^*)$, then $L \cup K, L \cdot K \in SD_{\mathbf{H}}(A^*)$
- 3 If $L \subseteq A^*$ is a generalized group language for G over $SD_{\mathbf{H}}(A^*)$ with $G \in \mathbf{H}$, then $L \in SD_{\mathbf{H}}(A^*)$

Proposition (Schützenberger (1974) reformulated)

$$SD_{\mathbf{H}}(A^*) \subseteq \overline{\mathbf{H}}(A^*)$$

Theorem (Schützenberger (1975) and (1974))

$$SD_{\mathbf{1}}(A^*) = \overline{\mathbf{1}}(A^*) = \mathbf{AP}(A^*) \text{ and } SD_{\mathbf{Ab}}(A^*) = \overline{\mathbf{Ab}}(A^*)$$

Extensions of Schützenberger's results (1965 – 1975)

- ① Perrin (1984) generalized $SF(A^*) = \mathbf{AP}(A^*)$ to $SF(A^\omega) = \mathbf{AP}(A^\omega)$, hence he obtained

$$SF(A^\infty) = \mathbf{AP}(A^\infty).$$

- ② D. and Kufleitner (2013) generalized $SD_1(A^*) = \mathbf{AP}(A^*)$ to $SD_1(A^\omega) = \mathbf{AP}(A^\omega)$, hence we obtained

$$SD_1(A^\infty) = \mathbf{AP}(A^\infty).$$

- ③ D. and Walter (2016) generalized $SD_{\mathbf{H}}(A^*) \subseteq \overline{\mathbf{H}}(A^*)$ and $SD_{\mathbf{Ab}}(A^*) = \overline{\mathbf{Ab}}(A^*)$ to $SD_{\mathbf{H}}(A^*) = \overline{\mathbf{H}}(A^*)$ and $SD_{\mathbf{H}}(A^\omega) = \overline{\mathbf{H}}(A^\omega)$, hence we obtained

$$SD_{\mathbf{H}}(A^\infty) = \overline{\mathbf{H}}(A^\infty).$$

Local divisor technique

The **local divisor technique** was established in finite semigroup theory around 2004 as a tool to simplify inductive proofs. (In associative algebra the idea is due to Kurt Meyberg 1972.)

The definition is as follows: Let M be a monoid and $c \in M$. Consider the set $cM \cap Mc$ and define a new multiplication

$$xc \circ cy = xcy.$$

Then $M_c = (cM \cap Mc, \circ, c)$ is monoid: the **local divisor** at c .

Facts

- $\lambda_c : \{x \in M \mid cx \in Mc\} \rightarrow M_c$ given by $\lambda_c(x) = cx$ is a surjective homomorphism. Hence, M_c is a divisor of M .

Local divisor technique

The **local divisor technique** was established in finite semigroup theory around 2004 as a tool to simplify inductive proofs. (In associative algebra the idea is due to Kurt Meyberg 1972.)

The definition is as follows: Let M be a monoid and $c \in M$. Consider the set $cM \cap Mc$ and define a new multiplication

$$xc \circ cy = xcy.$$

Then $M_c = (cM \cap Mc, \circ, c)$ is monoid: the **local divisor** at c .

Facts

- $\lambda_c : \{x \in M \mid cx \in Mc\} \rightarrow M_c$ given by $\lambda_c(x) = cx$ is a surjective homomorphism. Hence, M_c is a divisor of M .
- If c is a unit, then M_c is isomorphic to M .

Local divisor technique

The **local divisor technique** was established in finite semigroup theory around 2004 as a tool to simplify inductive proofs. (In associative algebra the idea is due to Kurt Meyberg 1972.)

The definition is as follows: Let M be a monoid and $c \in M$. Consider the set $cM \cap Mc$ and define a new multiplication

$$xc \circ cy = xcy.$$

Then $M_c = (cM \cap Mc, \circ, c)$ is monoid: the **local divisor** at c .

Facts

- $\lambda_c : \{x \in M \mid cx \in Mc\} \rightarrow M_c$ given by $\lambda_c(x) = cx$ is a surjective homomorphism. Hence, M_c is a divisor of M .
- If c is a unit, then M_c is isomorphic to M .
- If $c = c^2$, then M_c is the standard “local monoid”.

Local divisor technique

The **local divisor technique** was established in finite semigroup theory around 2004 as a tool to simplify inductive proofs. (In associative algebra the idea is due to Kurt Meyberg 1972.)

The definition is as follows: Let M be a monoid and $c \in M$. Consider the set $cM \cap Mc$ and define a new multiplication

$$xc \circ cy = xcy.$$

Then $M_c = (cM \cap Mc, \circ, c)$ is monoid: the **local divisor** at c .

Facts

- $\lambda_c : \{x \in M \mid cx \in Mc\} \rightarrow M_c$ given by $\lambda_c(x) = cx$ is a surjective homomorphism. Hence, M_c is a divisor of M .
- If c is a unit, then M_c is isomorphic to M .
- If $c = c^2$, then M_c is the standard “local monoid”.
- If c is not a unit, then $1 \notin M_c$. Hence, if c is not a unit and if M is finite, then $|M_c| < |M|$.

Baby-step-giant-step induction

Assume we wish to prove a property P for homomorphisms $\varphi : A^* \rightarrow M$ for finite monoids $M \in \mathbf{V}$.

- Base for the induction: prove P for finite groups $G \in \mathbf{V}$.

Baby-step-giant-step induction

Assume we wish to prove a property P for homomorphisms $\varphi : A^* \rightarrow M$ for finite monoids $M \in \mathbf{V}$.

- Base for the induction: prove P for finite groups $G \in \mathbf{V}$.
- If M is not a group choose a letter $c \in A$ such that $\varphi(c) \in M$ is not a unit. Define $B = A \setminus \{c\}$.

Baby-step-giant-step induction

Assume we wish to prove a property P for homomorphisms $\varphi : A^* \rightarrow M$ for finite monoids $M \in \mathbf{V}$.

- Base for the induction: prove P for finite groups $G \in \mathbf{V}$.
- If M is not a group choose a letter $c \in A$ such that $\varphi(c) \in M$ is not a unit. Define $B = A \setminus \{c\}$.
- P holds for $\varphi|_{B^*} : B^* \rightarrow M$ by induction because $|B| < |A|$.
(Baby-step)

Baby-step-giant-step induction

Assume we wish to prove a property P for homomorphisms $\varphi : A^* \rightarrow M$ for finite monoids $M \in \mathbf{V}$.

- Base for the induction: prove P for finite groups $G \in \mathbf{V}$.
- If M is not a group choose a letter $c \in A$ such that $\varphi(c) \in M$ is not a unit. Define $B = A \setminus \{c\}$.
- P holds for $\varphi|_{B^*} : B^* \rightarrow M$ by induction because $|B| < |A|$. (Baby-step)
- P holds for $\psi : T^* \rightarrow M_{\varphi(c)}$ for every finite T by induction because $|M_{\varphi(c)}| < |M|$. (Giant-step)

Baby-step-giant-step induction

Assume we wish to prove a property P for homomorphisms $\varphi : A^* \rightarrow M$ for finite monoids $M \in \mathbf{V}$.

- Base for the induction: prove P for finite groups $G \in \mathbf{V}$.
- If M is not a group choose a letter $c \in A$ such that $\varphi(c) \in M$ is not a unit. Define $B = A \setminus \{c\}$.
- P holds for $\varphi|_{B^*} : B^* \rightarrow M$ by induction because $|B| < |A|$. (Baby-step)
- P holds for $\psi : T^* \rightarrow M_{\varphi(c)}$ for every finite T by induction because $|M_{\varphi(c)}| < |M|$. (Giant-step)
- B^*c is a (prefix) code (of delay 1) and every mapping $\sigma : B^*c \rightarrow T$ can be extended to a homomorphism $\sigma : (B^*c)^+ = A^*c \rightarrow T^+$.

Baby-step-giant-step induction

Assume we wish to prove a property P for homomorphisms $\varphi : A^* \rightarrow M$ for finite monoids $M \in \mathbf{V}$.

- Base for the induction: prove P for finite groups $G \in \mathbf{V}$.
- If M is not a group choose a letter $c \in A$ such that $\varphi(c) \in M$ is not a unit. Define $B = A \setminus \{c\}$.
- P holds for $\varphi|_{B^*} : B^* \rightarrow M$ by induction because $|B| < |A|$. (Baby-step)
- P holds for $\psi : T^* \rightarrow M_{\varphi(c)}$ for every finite T by induction because $|M_{\varphi(c)}| < |M|$. (Giant-step)
- B^*c is a (prefix) code (of delay 1) and every mapping $\sigma : B^*c \rightarrow T$ can be extended to a homomorphism $\sigma : (B^*c)^+ = A^*c \rightarrow T^+$.
- One can choose T and σ such that

$$\varphi(cwc) = \psi\sigma(wc)$$

Baby-step-giant-step induction

Assume we wish to prove a property P for homomorphisms $\varphi : A^* \rightarrow M$ for finite monoids $M \in \mathbf{V}$.

- Base for the induction: prove P for finite groups $G \in \mathbf{V}$.
- If M is not a group choose a letter $c \in A$ such that $\varphi(c) \in M$ is not a unit. Define $B = A \setminus \{c\}$.
- P holds for $\varphi|_{B^*} : B^* \rightarrow M$ by induction because $|B| < |A|$. (Baby-step)
- P holds for $\psi : T^* \rightarrow M_{\varphi(c)}$ for every finite T by induction because $|M_{\varphi(c)}| < |M|$. (Giant-step)
- B^*c is a (prefix) code (of delay 1) and every mapping $\sigma : B^*c \rightarrow T$ can be extended to a homomorphism $\sigma : (B^*c)^+ = A^*c \rightarrow T^+$.
- One can choose T and σ such that

$$\varphi(cwc) = \psi\sigma(wc)$$

and then (hopefully) a miracle happens:

Baby-step-giant-step induction

Assume we wish to prove a property P for homomorphisms $\varphi : A^* \rightarrow M$ for finite monoids $M \in \mathbf{V}$.

- Base for the induction: prove P for finite groups $G \in \mathbf{V}$.
- If M is not a group choose a letter $c \in A$ such that $\varphi(c) \in M$ is not a unit. Define $B = A \setminus \{c\}$.
- P holds for $\varphi|_{B^*} : B^* \rightarrow M$ by induction because $|B| < |A|$. (Baby-step)
- P holds for $\psi : T^* \rightarrow M_{\varphi(c)}$ for every finite T by induction because $|M_{\varphi(c)}| < |M|$. (Giant-step)
- B^*c is a (prefix) code (of delay 1) and every mapping $\sigma : B^*c \rightarrow T$ can be extended to a homomorphism $\sigma : (B^*c)^+ = A^*c \rightarrow T^+$.
- One can choose T and σ such that

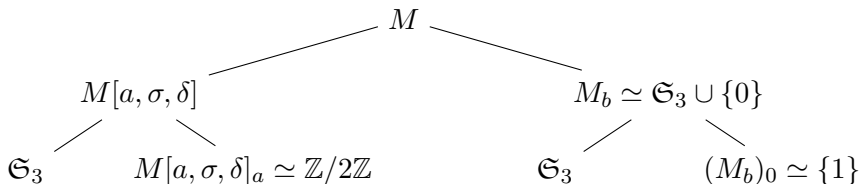
$$\varphi(cwc) = \psi\sigma(wc)$$

and then (hopefully) a miracle happens: P holds for φ .

Example for local divisor decomposition

$M = \{a, b\}^* \times \{\delta, \sigma\}^*$ with a zero 0 modulo defining relations:
 $a^2 = b^2 = ab = ba = 0$, $a\delta = a$, $\delta\sigma = \sigma\delta^2$, $\delta^3 = 1$, and $\sigma^2 = 1$.

The subgroup generated by δ and σ is the symmetric group \mathfrak{S}_3 ; it is solvable but not abelian.



Applications of the local divisor technique

- Simplified proof for $LTL = FO = \mathbf{AP}$ for finite and infinite words and “traces”. D. and Gastin (2006)

Applications of the local divisor technique

- Simplified proof for $LTL = FO = \mathbf{AP}$ for finite and infinite words and “traces”. D. and Gastin (2006)
- “One-page-proof” for $SF = \mathbf{AP}$ for finite (and infinite) words. Kufleitner (2010)

Applications of the local divisor technique

- Simplified proof for $LTL = FO = \mathbf{AP}$ for finite and infinite words and “traces”. D. and Gastin (2006)
- “One-page-proof” for $SF = \mathbf{AP}$ for finite (and infinite) words. Kufleitner (2010)
- Aperiodic languages are Church-Rosser congruential. D., Kufleitner, and Weil (2011)

Applications of the local divisor technique

- Simplified proof for $LTL = FO = \mathbf{AP}$ for finite and infinite words and “traces”. D. and Gastin (2006)
- “One-page-proof” for $SF = \mathbf{AP}$ for finite (and infinite) words. Kufleitner (2010)
- Aperiodic languages are Church-Rosser congruential. D., Kufleitner, and Weil (2011)
- Regular languages are Church-Rosser congruential. D., Kufleitner, Reinhardt, and Walter (2012)

Applications of the local divisor technique

- Simplified proof for $LTL = FO = \mathbf{AP}$ for finite and infinite words and “traces”. D. and Gastin (2006)
- “One-page-proof” for $SF = \mathbf{AP}$ for finite (and infinite) words. Kufleitner (2010)
- Aperiodic languages are Church-Rosser congruential. D., Kufleitner, and Weil (2011)
- Regular languages are Church-Rosser congruential. D., Kufleitner, Reinhardt, and Walter (2012)
- Simplified proof for the Krohn-Rhodes Theorem. D., Kufleitner, and Steinberg (2012)

Applications of the local divisor technique

- Simplified proof for $LTL = FO = \mathbf{AP}$ for finite and infinite words and “traces”. D. and Gastin (2006)
- “One-page-proof” for $SF = \mathbf{AP}$ for finite (and infinite) words. Kufleitner (2010)
- Aperiodic languages are Church-Rosser congruential. D., Kufleitner, and Weil (2011)
- Regular languages are Church-Rosser congruential. D., Kufleitner, Reinhardt, and Walter (2012)
- Simplified proof for the Krohn-Rhodes Theorem. D., Kufleitner, and Steinberg (2012)
- $SD(A^\omega) = \mathbf{AP}(A^\omega)$. D. and Kufleitner (2013)

Applications of the local divisor technique

- Simplified proof for $LTL = FO = \mathbf{AP}$ for finite and infinite words and “traces”. D. and Gastin (2006)
- “One-page-proof” for $SF = \mathbf{AP}$ for finite (and infinite) words. Kufleitner (2010)
- Aperiodic languages are Church-Rosser congruential. D., Kufleitner, and Weil (2011)
- Regular languages are Church-Rosser congruential. D., Kufleitner, Reinhardt, and Walter (2012)
- Simplified proof for the Krohn-Rhodes Theorem. D., Kufleitner, and Steinberg (2012)
- $SD(A^\omega) = \mathbf{AP}(A^\omega)$. D. and Kufleitner (2013)
- New interpretation of Green’s Lemma: Schützenberger categories. Costa and Steinberg (2014)

Applications of the local divisor technique

- Simplified proof for $LTL = FO = \mathbf{AP}$ for finite and infinite words and “traces”. D. and Gastin (2006)
- “One-page-proof” for $SF = \mathbf{AP}$ for finite (and infinite) words. Kufleitner (2010)
- Aperiodic languages are Church-Rosser congruential. D., Kufleitner, and Weil (2011)
- Regular languages are Church-Rosser congruential. D., Kufleitner, Reinhardt, and Walter (2012)
- Simplified proof for the Krohn-Rhodes Theorem. D., Kufleitner, and Steinberg (2012)
- $SD(A^\omega) = \mathbf{AP}(A^\omega)$. D. and Kufleitner (2013)
- New interpretation of Green’s Lemma: Schützenberger categories. Costa and Steinberg (2014)
- $SD_{\mathbf{H}}(A^\infty) = \overline{\mathbf{H}}(A^\infty)$. D. and Walter (2016)

Main steps in showing $\overline{\mathbf{H}}(A^*) \subseteq \text{SD}_{\mathbf{H}}(A^*)$

Starting point: $\varphi : A^* \rightarrow M$, all subgroups of M are divisors of $G \in \mathbf{H}$. Wlog. M is not a group. Choose $c \in A$ such that $\varphi(c)$ is not a unit. We write $[w] = \varphi^{-1}(w)$ and $T = \{[u] \mid u \in B^*\}$ becomes a finite alphabet.

Let $M_c = M_{\varphi(c)}$ the local divisor at $\varphi(c)$. Define

$$\psi : T^* \rightarrow M_c, \quad [u] \mapsto \varphi(cuc).$$

Then

$$\begin{aligned} \psi([u_1] \cdots [u_n]) &= \varphi(cu_1c) \circ \cdots \circ \varphi(cu_nc) \\ &= \varphi(cu_1c \cdots cu_nc) = \varphi(c) \cdot \varphi(u_1c \cdots u_nc). \end{aligned}$$

Define $\sigma : (B^*c)^* \rightarrow T^*$ with $\sigma(u_c) = [u]$. Then

$$\forall w \in A^* : \varphi(cwc) = \psi\sigma(wc).$$

“Essentially” it remains to show

$$\sigma^{-1}(\text{SD}_G(T^*)) \subseteq \text{SD}_G(A^*).$$

$$\sigma^{-1}(\text{SD}_G(T^*)) \subseteq \text{SD}_G(A^*)$$

We have to show $\sigma^{-1}(K) \in \text{SD}_G(A^*)$ for all $K \in \text{SD}_G(T^*)$. This is done by structural induction.

The key observation is;

$$\sigma^{-1}(\text{SD}_G(T^*)) \subseteq \text{SD}_G(A^*)$$

We have to show $\sigma^{-1}(K) \in \text{SD}_G(A^*)$ for all $K \in \text{SD}_G(T^*)$. This is done by structural induction.

The key observation is; if $K \in \text{SD}_G(T^*)$ be a prefix code of synchronization delay d , then $\sigma^{-1}(K)$ is a prefix code of synchronization delay $d + 1$. (Exercise.)

Concluding remarks

- The corresponding result for infinite words is more demanding.

Concluding remarks

- The corresponding result for infinite words is more demanding.
- For $\mathbf{H} = \mathbf{Sol}_q$ we obtain via a result of Straubing, Thérien, and Thomas the characterization:
 $(\text{FO} + \text{MOD}_q)[<](A^\infty) = \text{SD}_{\mathbf{Sol}_q}(A^\infty).$

Concluding remarks

- The corresponding result for infinite words is more demanding.
- For $\mathbf{H} = \mathbf{Sol}_q$ we obtain via a result of Straubing, Thérien, and Thomas the characterization:
 $(\text{FO} + \text{MOD}_q)[<](A^\infty) = \text{SD}_{\mathbf{Sol}_q}(A^\infty).$
- The monoid decomposition along proper submonoids and local divisors leads a purely algebraic description using “local” Rees extension. Answering thereby a recent question of Almeida and Klíma about “bullet varieties”.

Concluding remarks

- The corresponding result for infinite words is more demanding.
- For $\mathbf{H} = \mathbf{Sol}_q$ we obtain via a result of Straubing, Thérien, and Thomas the characterization:
 $(\text{FO} + \text{MOD}_q)[<](A^\infty) = \text{SD}_{\mathbf{Sol}_q}(A^\infty)$.
- The monoid decomposition along proper submonoids and local divisors leads a purely algebraic description using “local” Rees extension. Answering thereby a recent question of Almeida and Klíma about “bullet varieties”.
- Straubing (1979) gave a description of the “star-free” closure of a variety in terms of Mal’cev products. Is there a way to use a characterization with prefix codes of bounded synchronization delay?

Concluding remarks

- The corresponding result for infinite words is more demanding.
- For $\mathbf{H} = \mathbf{Sol}_q$ we obtain via a result of Straubing, Thérien, and Thomas the characterization:
 $(\text{FO} + \text{MOD}_q)[<](A^\infty) = \text{SD}_{\mathbf{Sol}_q}(A^\infty)$.
- The monoid decomposition along proper submonoids and local divisors leads a purely algebraic description using “local” Rees extension. Answering thereby a recent question of Almeida and Klíma about “bullet varieties”.
- Straubing (1979) gave a description of the “star-free” closure of a variety in terms of Mal’cev products. Is there a way to use a characterization with prefix codes of bounded synchronization delay?

MERCI

Concluding remarks

- The corresponding result for infinite words is more demanding.
- For $\mathbf{H} = \mathbf{Sol}_q$ we obtain via a result of Straubing, Thérien, and Thomas the characterization:
 $(\text{FO} + \text{MOD}_q)[<](A^\infty) = \text{SD}_{\mathbf{Sol}_q}(A^\infty)$.
- The monoid decomposition along proper submonoids and local divisors leads a purely algebraic description using “local” Rees extension. Answering thereby a recent question of Almeida and Klíma about “bullet varieties”.
- Straubing (1979) gave a description of the “star-free” closure of a variety in terms of Mal’cev products. Is there a way to use a characterization with prefix codes of bounded synchronization delay?

MERCI à Marcel-Paul

Concluding remarks

- The corresponding result for infinite words is more demanding.
- For $\mathbf{H} = \mathbf{Sol}_q$ we obtain via a result of Straubing, Thérien, and Thomas the characterization:
 $(\text{FO} + \text{MOD}_q)[<](A^\infty) = \text{SD}_{\mathbf{Sol}_q}(A^\infty)$.
- The monoid decomposition along proper submonoids and local divisors leads a purely algebraic description using “local” Rees extension. Answering thereby a recent question of Almeida and Klíma about “bullet varieties”.
- Straubing (1979) gave a description of the “star-free” closure of a variety in terms of Mal’cev products. Is there a way to use a characterization with prefix codes of bounded synchronization delay?

MERCI

à Marcel-Paul

et au LaBRI