Operators on varieties of monoids related to polynomial operators on classes of regular languages

Ondřej Klíma and Libor Polák

Department of Mathematics and Statistics Masaryk University Brno

SSAOS 2009

The polynomial operator assigns to each class of languages \mathscr{V} the class of all (positive) boolean combinations of the languages of the form

$$L_0 a_1 L_1 a_2 \dots a_\ell L_\ell , \qquad (*)$$

where A is an alphabet, $a_1, \ldots, a_\ell \in A, L_0, \ldots, L_\ell \in \mathscr{V}(A)$ (i.e. they are over A).

The resulting classes are denoted by $\mathsf{PPol}\mathscr{V}$ and $\mathsf{BPol}\mathscr{V}$, respectively.

In the restricted case we fix a natural number k and we allow only $\ell \leq k$ in (*). We get the classes $\text{PPol}_k \mathscr{V}$ and $\text{BPol}_k \mathscr{V}$, respectively.

The polynomial operator assigns to each class of languages \mathscr{V} the class of all (positive) boolean combinations of the languages of the form

$$L_0 a_1 L_1 a_2 \dots a_\ell L_\ell , \qquad (*)$$

where A is an alphabet, $a_1, \ldots, a_\ell \in A, L_0, \ldots, L_\ell \in \mathscr{V}(A)$ (i.e. they are over A).

The resulting classes are denoted by $PPol \mathscr{V}$ and $BPol \mathscr{V}$, respectively.

In the restricted case we fix a natural number k and we allow only $\ell \leq k$ in (*). We get the classes $\text{PPol}_k \mathscr{V}$ and $\text{BPol}_k \mathscr{V}$, respectively.

The polynomial operator assigns to each class of languages \mathscr{V} the class of all (positive) boolean combinations of the languages of the form

$$L_0 a_1 L_1 a_2 \dots a_\ell L_\ell , \qquad (*)$$

where A is an alphabet, $a_1, \ldots, a_\ell \in A, L_0, \ldots, L_\ell \in \mathscr{V}(A)$ (i.e. they are over A).

The resulting classes are denoted by $PPol \mathscr{V}$ and $BPol \mathscr{V}$, respectively.

In the restricted case we fix a natural number k and we allow only $\ell \leq k$ in (*). We get the classes $\text{PPol}_k \mathscr{V}$ and $\text{BPol}_k \mathscr{V}$, respectively.

1. Let $\mathscr{T}(A) = \{\emptyset, A^*\}$ for each finite set *A*. Then PPol \mathscr{T} is level 1/2 of the Straubing-Thérien hierarchy and BPol $\mathscr{T} = \mathscr{V}_1$ is level 1, i.e. the piecewise testable languages.

Result (Simon - 1972): Decidability of the membership problem for the class \mathscr{V}_1 .

Open problem: Decidability of the membership problem for the class BPol $\mathscr{V}_1 = \mathscr{V}_2$.

2. Let $\mathscr{S}^+(A)$ be the set of all finite unions of the languages of the form B^* , where $B \subseteq A$, for each finite set A.

Result (Pin, Straubing): BPOL $\mathcal{S}^{+} = \mathcal{V}_{2}$

Open problem – reformulation:

Is it decidable whether a given regular language $L \subseteq A^*$ can be expressed as a boolean combination languages of the form $B_0^*a_1B_1^*a_2\dots a_\ell B_\ell^*$, where $a_1,\dots,a_\ell \in A, B_0,\dots,B_\ell \subseteq A$. 1. Let $\mathscr{T}(A) = \{\emptyset, A^*\}$ for each finite set *A*. Then PPol \mathscr{T} is level 1/2 of the Straubing-Thérien hierarchy and BPol $\mathscr{T} = \mathscr{V}_1$ is level 1, i.e. the piecewise testable languages.

Result (Simon - 1972): Decidability of the membership problem for the class \mathscr{V}_1 .

Open problem: Decidability of the membership problem for the class $\mathsf{BPol}\,\mathscr{V}_1=\mathscr{V}_2.$

2. Let $\mathscr{S}^+(A)$ be the set of all finite unions of the languages of the form B^* , where $B \subseteq A$, for each finite set A. **Result** (Pin, Straubing): BPol $\mathscr{S}^+ = \mathscr{V}_2$. **Open problem – reformulation:** Is it decidable whether a given regular language $L \subseteq A^*$ can be expressed as a boolean combination languages of the form $B_0^*a_1B_1^*a_2...a_\ell B_\ell^*$, where $a_1,...,a_\ell \in A$, $B_0,...,B_\ell \subseteq A$. 1. Let $\mathscr{T}(A) = \{\emptyset, A^*\}$ for each finite set *A*. Then PPol \mathscr{T} is level 1/2 of the Straubing-Thérien hierarchy and BPol $\mathscr{T} = \mathscr{V}_1$ is level 1, i.e. the piecewise testable languages.

Result (Simon - 1972): Decidability of the membership problem for the class \mathscr{V}_1 .

Open problem: Decidability of the membership problem for the class $\mathsf{BPol}\,\mathscr{V}_1=\mathscr{V}_2.$

2. Let $\mathscr{S}^+(A)$ be the set of all finite unions of the languages of the form B^* , where $B \subseteq A$, for each finite set A.

Result (Pin, Straubing): BPol $\mathscr{S}^+ = \mathscr{V}_2$.

Open problem – reformulation:

Is it decidable whether a given regular language $L \subseteq A^*$ can be expressed as a boolean combination languages of the form $B_0^*a_1B_1^*a_2\ldots a_\ell B_\ell^*$, where $a_1,\ldots,a_\ell \in A$, $B_0,\ldots,B_\ell \subseteq A$.

3. Let $\mathscr{S}(\underline{A})$ be the set of all finite unions of the languages of the form \overline{B} , where $B \subseteq A$, for each finite set A. Here \overline{B} is the set of all words over A containing exactly the letters from B.

4. Let *m* be a fixed natural number. Let $\mathscr{A}_m(A)$ be the set of all boolean combinations of the languages of the form $L(a,r) = \{ u \in A^* \mid |u|_a \equiv r \pmod{m} \}$, where $a \in A$ and $0 \leq r < m$, for each finite set *A*.

Notice that the classes $\mathcal{T}, \mathcal{S}, \mathcal{A}_m$ are boolean varieties and \mathcal{S}^+ is a positive variety.

3. Let $\mathscr{S}(\underline{A})$ be the set of all finite unions of the languages of the form \overline{B} , where $B \subseteq A$, for each finite set A. Here \overline{B} is the set of all words over A containing exactly the letters from B.

4. Let *m* be a fixed natural number. Let $\mathscr{A}_m(A)$ be the set of all boolean combinations of the languages of the form $L(a,r) = \{ u \in A^* \mid |u|_a \equiv r \pmod{m} \}$, where $a \in A$ and $0 \leq r < m$, for each finite set *A*.

Notice that the classes $\mathcal{T}, \mathcal{S}, \mathcal{A}_m$ are boolean varieties and \mathcal{S}^+ is a positive variety.

3. Let $\mathscr{S}(\underline{A})$ be the set of all finite unions of the languages of the form \overline{B} , where $B \subseteq A$, for each finite set A. Here \overline{B} is the set of all words over A containing exactly the letters from B.

4. Let *m* be a fixed natural number. Let $\mathscr{A}_m(A)$ be the set of all boolean combinations of the languages of the form $L(a,r) = \{ u \in A^* \mid |u|_a \equiv r \pmod{m} \}$, where $a \in A$ and $0 \leq r < m$, for each finite set *A*.

Notice that the classes $\mathcal{T}, \mathcal{S}, \mathcal{A}_m$ are boolean varieties and \mathcal{S}^+ is a positive variety.

A boolean variety of languages \mathscr{V} associates to every finite alphabet *A* a class $\mathscr{V}(A)$ of regular languages over *A* in such a way that

- 𝒱(A) is closed under finite unions, finite intersections and complements (in particular, Ø, A* ∈ 𝒱(A)),
- $\mathscr{V}(A)$ is closed under derivatives, i.e. $L \in \mathscr{V}(A), u, v \in A^*$ implies $u^{-1}Lv^{-1} = \{ w \in A^* \mid uwv \in L \} \in \mathscr{V}(A),$
- \mathscr{V} is closed under inverse morphisms, i.e. $f: B^* \to A^*, \ L \in \mathscr{V}(A)$ implies $f^{-1}(L) = \{ v \in B^* \mid f(v) \in L \} \in \mathscr{V}(B).$

To get the notion of a **positive** variety of languages, we use in the first item only intersections and unions (not complements).

A boolean variety of languages \mathscr{V} associates to every finite alphabet *A* a class $\mathscr{V}(A)$ of regular languages over *A* in such a way that

- 𝒱(A) is closed under finite unions, finite intersections and complements (in particular, Ø, A* ∈ 𝒱(A)),
- $\mathscr{V}(A)$ is closed under derivatives, i.e. $L \in \mathscr{V}(A), u, v \in A^*$ implies $u^{-1}Lv^{-1} = \{ w \in A^* \mid uwv \in L \} \in \mathscr{V}(A),$
- \mathscr{V} is closed under inverse morphisms, i.e. $f: B^* \to A^*, \ L \in \mathscr{V}(A)$ implies $f^{-1}(L) = \{ v \in B^* \mid f(v) \in L \} \in \mathscr{V}(B).$

To get the notion of a **positive** variety of languages, we use in the first item only intersections and unions (not complements).

A pseudovariety of finite (ordered) monoids is a class of finite monoids closed under submonoids, morphic images and products of finite families. Similarly for ordered monoids. When defining a variety of (ordered) monoids we use arbitrary products.

The pseudovarieties of ordered monoids can be characterized by pseudoidentities. The pseudovarieties we consider here are equational – they are given by identities, or equivalently, they are of the form Fin**V** where **V** is a variety of (ordered) monoids. A pseudovariety of finite (ordered) monoids is a class of finite monoids closed under submonoids, morphic images and products of finite families. Similarly for ordered monoids. When defining a variety of (ordered) monoids we use arbitrary products.

The pseudovarieties of ordered monoids can be characterized by pseudoidentities. The pseudovarieties we consider here are equational – they are given by identities, or equivalently, they are of the form Fin V where V is a variety of (ordered) monoids. For a regular language $L \subseteq A^*$, we define the relations \sim_L and \preceq_L on A^* as follows: for $u, v \in A^*$ we have

 $u \sim_L v$ if and only if $(\forall p, q \in A^*) (puq \in L \iff pvq \in L)$,

 $u \preceq_L v$ if and only if $(\forall p, q \in A^*) (pvq \in L \Longrightarrow puq \in L).$

The relation \sim_L is the syntactic congruence of L on A^* . It is of finite index (i.e. there are finitely many classes), the quotient structure $M(L) = A^*/\sim_L$ is called the syntactic monoid of L. The relation \preceq_L is the syntactic quasiorder of L and we have $\preceq_L \cap \succeq_L = \sim_L$. Hence \preceq_L induces an order on $M(L) = A^*/\sim_L$, namely: $u \sim_L \leq v \sim_L$ if and only if $u \preceq_L v$. We speak about the syntactic ordered monoid of L; we denote the structure by O(L) For a regular language $L \subseteq A^*$, we define the relations \sim_L and \preceq_L on A^* as follows: for $u, v \in A^*$ we have

 $u \sim_L v$ if and only if $(\forall p, q \in A^*) (puq \in L \iff pvq \in L)$,

 $u \preceq_L v$ if and only if $(\forall p, q \in A^*)$ $(pvq \in L \Longrightarrow puq \in L)$.

The relation \sim_L is the syntactic congruence of *L* on *A*^{*}. It is of finite index (i.e. there are finitely many classes), the quotient structure $M(L) = A^* / \sim_L$ is called the syntactic monoid of *L*. The relation \preceq_L is the syntactic quasiorder of *L* and we have $\preceq_L \cap \succeq_L = \sim_L$. Hence \preceq_L induces an order on $M(L) = A^* / \sim_L$, namely: $u \sim_L \leq v \sim_L$ if and only if $u \preceq_L v$. We speak about the syntactic ordered monoid of *L*; we denote the structure by O(L).

Result (Eilenberg, Pin)

Boolean varieties (positive varieties) of languages correspond to pseudovarieties of finite monoids (ordered monoids). The correspondence, written $\mathscr{V} \longleftrightarrow \mathbf{V}$ ($\mathscr{P} \longleftrightarrow \mathbf{P}$), is given by the following relationship: for $L \subseteq A^*$ we have

 $L \in \mathscr{V}(A)$ if and only if $M(L) \in \mathbf{V}$

 $(L \in \mathscr{P}(A) \text{ if and only if } O(L) \in \mathbf{P}).$

Pseudovarieties of (ordered) monoids corresponding to the classes $\mathcal{T}, \mathcal{S}^+, \mathcal{S}, \mathcal{A}_m$ consist exactly of all finite members of the following varieties:

$$T = Mod(x = y), S^+ = Mod(x^2 = x, xy = yx, 1 \le x),$$

$$S = Mod(x^2 = x, xy = yx), A_m = Mod(xy = yx, x^m = 1)$$
.

The names for the (ordered) monoids of the pseudovarieties T, S^+, S, A_m are trivial monoids (semilattices with the smallest element 1, semilattices and abelian groups of index *m*, respectively)

Let $X = \{x_1, x_2, ...\}$. A relation γ on X^* is a finite characteristic if it satisfies the following conditions: (i) γ is a quasiorder on X^* ; (ii) γ is compatible with the multiplication, i.e. for each $u, v, w \in X^*$ we have

 $u \gamma v$ implies $uw \gamma vw$, $wu \gamma wv$;

(iii) γ is fully invariant, i.e. for each morphism $\varphi : X^* \to X^*$ and each $u, v \in X^*$ we have

$$u \gamma v$$
 implies $\varphi(u) \gamma \varphi(v)$;

(iv) for each finite subset *Y* of the set *X*, the set *Y*^{*} intersects only finitely many classes of $X^*/\gamma \cap \gamma^{-1}$.

Positive varieties of languages having all $\mathscr{V}(A)$ finite correspond to finite characteristics. Namely $\mathscr{V} \mapsto \operatorname{Id} \mathbf{V}$ and $L \in \mathscr{V}(A)$ iff $\gamma \mid A^* \times A^* \subseteq \preceq_L$.

The classes of languages in our basic examples have the following finite characteristics: 1. Id $\mathbf{T} = X^* \times X^*$. 2. Id $\mathbf{S}^+ = \{(u, v) \in X^* \times X^* \mid \mathbf{c}(u) \subseteq \mathbf{c}(v)\}$. 3. Id $\mathbf{S} = \{(u, v) \in X^* \times X^* \mid \mathbf{c}(u) = \mathbf{c}(v)\}$. 4. Id $\mathbf{A}_m = \{(u, v) \in X^* \times X^* \mid (\forall x \in X) \mid u|_x \equiv |v|_x \pmod{m}\}$.

Positive varieties of languages having all $\mathscr{V}(A)$ finite correspond to finite characteristics. Namely $\mathscr{V} \mapsto \operatorname{Id} \mathbf{V}$ and $L \in \mathscr{V}(A)$ iff $\gamma \mid A^* \times A^* \subseteq \preceq_L$.

The classes of languages in our basic examples have the following finite characteristics:

1. Id
$$\mathbf{T} = X^* \times X^*$$
.
2. Id $\mathbf{S}^+ = \{(u, v) \in X^* \times X^* \mid c(u) \subseteq c(v)\}.$
3. Id $\mathbf{S} = \{(u, v) \in X^* \times X^* \mid c(u) = c(v)\}.$
4. Id $\mathbf{A}_m = \{(u, v) \in X^* \times X^* \mid (\forall x \in X) \mid u|_x \equiv |v|_x \pmod{m}\}.$

Let *k* be a fixed natural number and γ be a finite characteristic. For a word $u \in X^*$, we say that

 $f = (u_0, a_1, u_1, a_2, \dots, a_\ell, u_\ell)$

is a factorization of *u* of length ℓ if $u_0, u_1, \ldots, u_\ell \in X^*$,

 $a_1, a_2, ..., a_\ell \in X$ and $u_0 a_1 u_1 ... a_\ell u_\ell = u$.

The set of all factorizations of lengths at most *k* of the word *u* is denoted by $Fact_k(u)$.

For a factorization $f = (u_0, a_1, u_1, ..., a_\ell, u_\ell)$ of a word $u \in X^*$ and a factorization $g = (v_0, b_1, v_1, ..., b_m, v_m)$ of a word $v \in X^*$, we write $f \leq_{\gamma} g$ if

• $\ell = m$,

- $a_i = b_i$ for every $i \in \{1, \ldots, \ell\}$,
- $u_i \gamma v_i$ for every $i \in \{0, 1, \ldots, \ell\}$.

We define the relation $p_k(\gamma)$ on the set X^* as follows: for $u, v \in X^*$, we have $(u, v) \in p_k(\gamma)$ iff

 $(\forall g \in \operatorname{Fact}_k(v)) (\exists f \in \operatorname{Fact}_k(u)) f \leq_{\gamma} g.$

Theorem

Let \mathscr{V} be a locally finite positive variety of languages and γ be a finite characteristic of \mathscr{V} . Then $\operatorname{PPol}_k \mathscr{V}$ is a locally finite positive variety of languages with the finite characteristic $p_k(\gamma)$ and $\operatorname{BPol}_k \mathscr{V}$ is a locally finite boolean variety of languages with the finite characteristic $p_k(\gamma) \cap (p_k(\gamma))^{-1}$.

 $\cap, \cup \quad \cap, \cup, \text{ compl.}$ $\mathscr{S} \quad \overline{B_0}a_1\overline{B_1}a_2...a_{\ell}\overline{B_{\ell}} \quad \mathsf{PPol}_k(\mathscr{S}) \subseteq \mathsf{BPol}_k(\mathscr{S})$ $\cup | \qquad \cup |$ $\mathscr{S}^+ \quad B_0^*a_1B_1^*a_2...a_{\ell}B_{\ell}^* \quad \mathsf{PPol}_k(\mathscr{S}^+) \subseteq \mathsf{BPol}_k(\mathscr{S}^+)$ $\ell \leq k, \ a_1,...,a_{\ell} \in A, \ B_0,...,B_{\ell} \subseteq A$

Proposition

A positive variety \mathscr{V} is generated by a finite number of languages if and only if the corresponding psedovariety **V** of ordered monoids is generated by a single ordered monoid.

Proposition

For each k, the positive variety $PPol_k \mathscr{S}^+$ is generated by a finite number of languages.

Propositior

The positive variety $PPol_1 \mathscr{S}$ is generated by a finite number of languages.

Proposition

Proposition

A positive variety \mathscr{V} is generated by a finite number of languages if and only if the corresponding psedovariety **V** of ordered monoids is generated by a single ordered monoid.

Proposition

For each k, the positive variety $PPol_k \mathscr{S}^+$ is generated by a finite number of languages.

Proposition

The positive variety $PPol_1 \mathscr{S}$ is generated by a finite number of languages.

Proposition

Proposition

A positive variety \mathscr{V} is generated by a finite number of languages if and only if the corresponding psedovariety **V** of ordered monoids is generated by a single ordered monoid.

Proposition

For each k, the positive variety $PPol_k \mathscr{S}^+$ is generated by a finite number of languages.

Proposition

The positive variety $PPol_1 \mathscr{S}$ is generated by a finite number of languages.

Proposition

Proposition

A positive variety \mathscr{V} is generated by a finite number of languages if and only if the corresponding psedovariety **V** of ordered monoids is generated by a single ordered monoid.

Proposition

For each k, the positive variety $PPol_k \mathscr{S}^+$ is generated by a finite number of languages.

Proposition

The positive variety $PPol_1 \mathscr{S}$ is generated by a finite number of languages.

Proposition

The hierarchies $PPol_k(\mathcal{S}^+)$, $PPol_k(\mathcal{S})$, $BPol_k(\mathcal{S}^+)$ and $BPol_k(\mathcal{S})$ are strict.

Proposition

For each k, the varieties $PPol_k(\mathscr{S}^+)$, $PPol_k(\mathscr{S})$, $BPol_k(\mathscr{S}^+)$ and $BPol_k(\mathscr{S})$ are pairwise different.

Theorem

The only non-trivial inclusions are

 $BPol_1(\mathscr{S}) \subseteq PPol_2(\mathscr{S}), BPol_2(\mathscr{S}^+), PPol_3(\mathscr{S}^+)$

and

$$\mathsf{BPol}_1(\mathscr{S}^+) \subseteq \mathsf{PPol}_2(\mathscr{S}^+)$$

The hierarchies $PPol_k(\mathscr{S}^+)$, $PPol_k(\mathscr{S})$, $BPol_k(\mathscr{S}^+)$ and $BPol_k(\mathscr{S})$ are strict.

Proposition

For each k, the varieties $\text{PPol}_k(\mathscr{S}^+)$, $\text{PPol}_k(\mathscr{S})$, $\text{BPol}_k(\mathscr{S}^+)$ and $\text{BPol}_k(\mathscr{S})$ are pairwise different.

Theorem

The only non-trivial inclusions are

 $BPol_1(\mathscr{S}) \subseteq PPol_2(\mathscr{S}), BPol_2(\mathscr{S}^+), PPol_3(\mathscr{S}^+)$

and

$$\mathsf{BPol}_1(\mathscr{S}^+) \subseteq \mathsf{PPol}_2(\mathscr{S}^+)$$

The hierarchies $PPol_k(\mathcal{S}^+)$, $PPol_k(\mathcal{S})$, $BPol_k(\mathcal{S}^+)$ and $BPol_k(\mathcal{S})$ are strict.

Proposition

For each k, the varieties $\text{PPol}_k(\mathscr{S}^+)$, $\text{PPol}_k(\mathscr{S})$, $\text{BPol}_k(\mathscr{S}^+)$ and $\text{BPol}_k(\mathscr{S})$ are pairwise different.

Theorem

The only non-trivial inclusions are

```
BPol_1(\mathscr{S}) \subseteq PPol_2(\mathscr{S}), BPol_2(\mathscr{S}^+), PPol_3(\mathscr{S}^+)
```

and

$$\mathsf{BPol}_1(\mathscr{S}^+) \subseteq \mathsf{PPol}_2(\mathscr{S}^+)$$

Let *x*, *y* be two different letters from *X* and $u \in X^*$ be a word which contains both *x* and *y*, i.e. $x, y \in c(u)$. The "identity"

$$uxyx = uyx$$
, where $x, y \in c(u)$ (1)

is equivalent to a pair of identities: we distinguish two cases $u = u_1 x u_2 y u_3$ and $u = u_1 y u_2 x u_3$ for some $u_1, u_2, u_3 \in X^*$, so the identity (1) is equivalent to the identities

$$x_1 x x_2 y x_3 \cdot x y x = x_1 x x_2 y x_3 \cdot y x$$
,

$$x_1 y x_2 x x_3 \cdot x y x = x_1 y x_2 x x_3 \cdot y x$$
.

We have also the dual version of the identity (1)

$$xyxu = xyu$$
 where $x, y \in c(u)$.

Consider also

$$uxyv = uyxv$$
, where $x, y \in c(u) \cap c(v)$. (2)

Note that this identity represents in fact four identities.

$$yuyx \le yuxyx$$
 and $xyuy \le xyxuy$ (3)

$$xuxvx \leq xuvx$$
. (4)

Propositior

(i) The identities (1) and (2) form a finite basis of identities for the variety of monoids corresponding to $BPol_1(\mathscr{S}^+)$. (ii) The identities (2), (3) and (4) form a finite basis of identities for the variety of ordered monoids corresponding to $PPol_1(\mathscr{S}^+)$

Consider also

$$uxyv = uyxv$$
, where $x, y \in c(u) \cap c(v)$. (2)

Note that this identity represents in fact four identities.

$$yuyx \le yuxyx$$
 and $xyuy \le xyxuy$ (3)

$$xuxvx \leq xuvx$$
. (4)

Proposition

(i) The identities (1) and (2) form a finite basis of identities for the variety of monoids corresponding to $\text{BPol}_1(\mathscr{S}^+)$. (ii) The identities (2), (3) and (4) form a finite basis of identities for the variety of ordered monoids corresponding to $\text{PPol}_1(\mathscr{S}^+)$.

(i) The variety of monoids corresponding to BPol₁(*S*) has a finite basis of identities.
(ii) The variety of ordered monoids corresponding to PPol₁(*S*) has a finite basis of identities.