On the membership problem for pseudovarieties

K. Auinger

NBSAN, Edinburgh, July 2014

All semigroups/monoids/categories are finite!

A *pseudovariety* is a class of semigroups/monoids closed under P_f, S and H.

The collection of all pseudovarieties forms a complete lattice.

Join operation $\vee$:

$$\mathbf{V} \vee \mathbf{W} = \mathrm{HS}\{V \times W \mid V \in \mathbf{V}, W \in \mathbf{W}\}$$

Other operations: semidirect product $*$:

$$\mathbf{V} * \mathbf{W} = \mathrm{HS}\{V \rtimes W \mid V \in \mathbf{V}, W \in \mathbf{W}\}$$

Similarly defined operations: ⓜ, $**$, $\diamondsuit_n$, $\diamondsuit$, $\mathfrak{P}$

Notation

- $\mathbf{G}$: pseudovariety of all groups
- $\mathbf{A}$: pseudovariety of all aperiodic semigroups/monoids
- $\mathbf{J}$: pseudovariety of all $\mathcal{J}$-trivial semigroups/monoids

Open problems

- (Schützenberger) Decide membership in $\mathbf{A} \vee \mathbf{G}$.
- (Krohn–Rhodes) Decide membership in $(\mathbf{A} * \mathbf{G})^n * \mathbf{A}$ for $n = 1, 2, \ldots$.
- (Pin–Straubing) Decide membership in $\mathfrak{P}\mathbf{J} = \Diamond\mathbf{J}$.

Result (Albert, Baldinger, Rhodes, 1992)

There exists a finite set E of semigroup identities such that the pseudovariety join $[\![E]\!] \vee \mathbf{Com}$ has undecidable membership.

$\mathbf{Com}$ = commutative semigroups
$[\![E]\!]$ = semigroups satisfying E

Result (Rhodes, 1999)

The operations $*$, $**$ and ⓜ do not preserve decidability of membership.

Different approach to such results:
decompose the set $\mathbb{P}$ of all primes into two disjoint infinite recursive subsets A and B, for example

- $A = \{2, 5, 11, p_7, p_9, \dots\}$
- $B = \{3, 7, 13, p_8, p_{10}, \dots\}$

Choose an injective, recursive function $f : A \to B$ for which $C := f(A)$ is not recursive.
For $D := B \setminus C$ we have

$$\mathbb{P} = (A \cup C) \cup D,$$

where $A \cup C$ is r.e. but not recursive, D is not r.e.
For $p \in \mathbb{P}$ let

- $\mathbf{G}_p$ = the pseudovariety of all p-groups
- $\mathbf{Ab}_p$ = the pseudovariety of all abelian p-groups

For $p \in A$ let $\mathbf{U}_p := \mathbf{G}_p * \mathbf{Ab}_{f(p)}$
Our main object is the pseudovariety defined by:

$$\mathbf{U} := \bigvee_{p \in A} \mathbf{U}_p \vee \bigvee_{p \in D} \mathbf{Ab}_p.$$

Then

$$\mathbf{U} = \mathrm{P}_f\Big(\bigcup_{p \in A} \mathbf{U}_p \cup \bigcup_{p \in D} \mathbf{Ab}_p \Big).$$

Decidability of membership of $\mathbf{U}$: let G be a group and $a_1, \ldots, a_k$ be those prime divisors of $|G|$ which are in A and $b_1 \ldots, b_n$ those which are in $B \setminus \{f(a_1), \ldots, f(a_k)\}$;
then

$$G \in \mathbf{U} \Leftrightarrow G \in \mathrm{P}_f\Big(\bigcup_{i=1}^{k} \mathbf{U}_{a_i} \cup \bigcup_{j=1}^{n} \mathbf{Ab}_{b_j} \Big).$$

Intuitive idea of the construction of **U**:
Let $p \in \mathbb{P}$ and G be an abelian p-group; then:

1. either: there exists a prime q such that **every** co-extension of G by any q-group belongs to **U**
2. or: **every** co-extension of G in **U** is of the form $H \times K$ for a p'-group H and an abelian p-group K

The two cases are in sharp contrast to each other but are not recursively separable. In other words, if we are given an abelian p-group, we can't decide whether case (1) or case (2) applies.

The pseudovariety **U** contains all abelian groups, is solvable and does not satisfy any non-trivial group identity. One can modify the construction to get a similar pseudovariety which is metabelian.

Definition

- $C_{2,1} := \langle a \mid a^2 = 0 \rangle = \{1, a, a^2 = 0\}$
- $\mathbf{C}_{2,1} = \mathrm{HSP}_f(C_{2,1})$

Theorem

No pseudovariety in the interval $[\mathbf{C}_{2,1} \vee \mathbf{U}, \mathbf{A} \vee \mathbf{U}]$ has decidable membership. In particular, the two joins $\mathbf{C}_{2,1} \vee \mathbf{U}$ and $\mathbf{A} \vee \mathbf{U}$ have undecidable membership.

For each prime p let $C_p := \langle x \mid x^p = 1 \rangle$ be the cyclic group of order p. We define the monoid M_p as follows:

$$M_p = C_p \cup (C_p \times C_p) \cup \{0\}$$

where $(C_p \times C_p) \cup \{0\}$ is a null semigroup and an ideal of M_p and C_p is the group of units of M_p acting on $(C_p \times C_p) \cup \{0\}$ by

$$x(y,z) = (xy, z), \quad (y,z)x = (y, zx), \quad x0 = 0x = 0.$$

The claim follows from the facts:
if $p \in A$ then M_p divides $C_{2,1} \times (\mathbb{F}_p^{C_p \times C_p} \rtimes C_p) \in \mathbf{C}_{2,1} \vee \mathbf{U}_p$
if $p \in C$ then M_p divides $C_{2,1} \times (\mathbb{F}_{f^{-1}(p)}^{C_p \times C_p} \rtimes C_p) \in \mathbf{C}_{2,1} \vee \mathbf{U}_{f^{-1}(p)}$
let $p \in D$; suppose there exist $A \in \mathbf{A}$, $G \in \mathbf{U}$, $M \leq A \times G$ and $\varphi : M \twoheadrightarrow M_p$;
then $G = H \times K$ with H a p'-group and K an abelian p-group;
let $a = (m, h, k) \in x\varphi^{-1}$ where x is a generating element of C_p
then there exists a positive integer $n \equiv 1 \pmod{p}$ such that
$a^n = c = (e, 1, k^n)$, $e^2 = e$ and $c\varphi = x$;
for each $b \in M$ then $c^2bc = cbc^2$ but for $b \in (1,1)\varphi^{-1}$,
$(c^2bc)\varphi = (x^2, x) \neq (x, x^2) = (cbc^2)\varphi$.

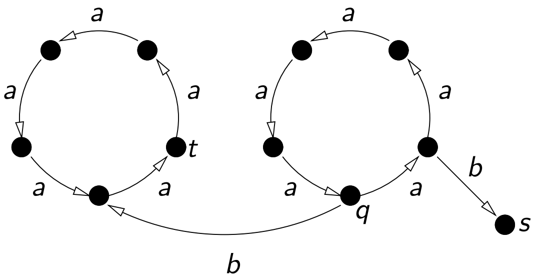
Corollary

The join $\mathbf{Com} \vee \mathbf{U}$ *has undecidable membership.*

because

$$\mathbf{Com} \vee \mathbf{U} = \mathbf{ACom} \vee \mathbf{Ab} \vee \mathbf{U} = \mathbf{ACom} \vee \mathbf{U} \in [\mathbf{C}_{2,1} \vee \mathbf{U}, \mathbf{A} \vee \mathbf{U}].$$

For each prime p define an inverse automaton $\mathcal{A}_p$ as depicted for $p = 5$:



- if $p \in A$ then $\mathcal{A}_p$ embeds in the Cayley graph of $C_p \wr C_p \in \mathbf{U}_p$
- if $p \in C$ then $\mathcal{A}_p$ embeds in the Cayley graph of $C_{f^{-1}(p)} \wr C_p \in \mathbf{U}_{f^{-1}(p)}$
- if $p \in D$ then $\mathcal{A}_p$ does not embed in any permutation automaton with transition group in $\mathbf{U}$

Definition

- For a prime p denote by I_p the inverse monoid defined by the automaton $\mathcal{A}_p$.
- For a group pseudovariety $\mathbf{H}$ denote by $\mathbf{SI} \circ \mathbf{H}$ the inverse monoid pseudovariety of all inverse monoids which have an E-unitary cover over a group in $\mathbf{H}$.

Corollary

- *if* $p \in A$ *then* $I_p \in \mathbf{SI} \circ \mathbf{U}_p$
- *if* $p \in C$ *then* $I_p \in \mathbf{SI} \circ \mathbf{U}_{f^{-1}(p)}$
- *if* $p \in D$ *then* $I_p \notin \mathbf{SI} \circ \mathbf{U}$.

No inverse monoid pseudovariety in $\mathbf{V}$ *for which* $\bigvee_{p \in A} \mathbf{SI} \circ \mathbf{U}_p \subseteq \mathbf{V} \subseteq \mathbf{SI} \circ \mathbf{U}$ *has decidable membership.*

For a group pseudovariety $\mathbf{H}$, the inverse semigroups/monoids in $\mathbf{J} * \mathbf{H}$ are exactly those of the semigroup/monoid pseudovariety $\mathbf{SI} * \mathbf{H}$ which are exactly those of $\mathbf{SI} \circ \mathbf{H}$. Consequently,

- if $p \in A \cup C$ then $I_p \in \bigvee_{q \in A} \mathbf{SI} * \mathbf{U}_q$
- if $p \in D$ then $I_p \notin \mathbf{J} * \mathbf{U}$

Theorem

No semigroup/monoid pseudovariety in the interval

$$\Big[\bigvee_{q \in A} \mathbf{SI} * \mathbf{U}_q, \mathbf{J} * \mathbf{U} \Big]$$

has decidable membership. In particular, $\mathbf{SI} * \mathbf{U}$ *has undecidable membership.*

Since $\mathbf{SI} * \mathbf{U} = \mathbf{SI} \, ⓜ \, \mathbf{U} = \mathbf{SI} ** \mathbf{U}$, we have

Corollary

None of the operations $*$, ⓜ, $**$ preserves the decidability of membership.

Since

$$\mathbf{SI} ** \mathbf{U} = \diamondsuit_2\mathbf{U} \subseteq \cdots \subseteq \diamondsuit_n\mathbf{U} \subseteq \cdots \bigcup \diamondsuit_n\mathbf{U} = \diamondsuit\mathbf{U} = \mathbf{J} * \mathbf{U}$$

and, for each $p \in A$,

$$\mathbf{J} * \mathbf{U}_p = \mathfrak{P}\mathbf{U}_p \subseteq \mathfrak{P}\mathbf{U} \subseteq \mathbf{J} * \mathbf{U}$$

each of $\diamondsuit_n\mathbf{U}$ (all $n \geq 2$), $\diamondsuit\mathbf{U}$ and $\mathfrak{P}\mathbf{U}$ have undecidable membership,

Corollary

None of the operators $\diamondsuit_n$ (all $n \geq 2$), $\diamondsuit$ and $\mathfrak{P}$ preserves the decidability of membership.

Tilson used categories to establish his decomposition result for monoid (pseudo)varieties:

Theorem

Let $\mathbf{V}, \mathbf{W}$ *be pseudovarieties of monoids; a monoid* M *belongs of* $\mathbf{V} * \mathbf{W}$ *iff there exists* $N \in \mathbf{W}$ *and a relational morphism* $\varphi : M \to N$ *for which the derived category* D_φ *belongs to* $g\mathbf{V}$.

$g\mathbf{V}$, the *global* of $\mathbf{V}$, is the smallest pseudovariety of categories containing $\mathbf{V}$, i.e. the class of all category divisors of members of $\mathbf{V}$
membership in $g\mathbf{V}$ is essential to Tilson's theory

Problem

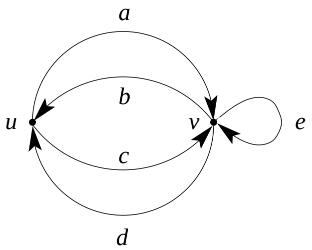
Can decidability of membership in $g\mathbf{V}$ *be reduced to decidability of membership in* $\mathbf{V}$*?*

No! Let $D\mathbf{U}$ be the pseudovariety of monoids all of whose regular $\mathcal{D}$-classes are members of $\mathbf{U}$.

Theorem

Membership in $D\mathbf{U}$ is decidable while membership in $gD\mathbf{U}$ is undecidable.

We start with the graph Γ:



and let Γ^* be the free category generated by Γ. For each prime p let $\Gamma_p = \Gamma/{\equiv_p}$ where $\equiv_p$ is a congruence defined by a certain set of identities. It can be shown that Γ_p is finite and computable.

Some very deep results of Kad'ourek then imply

- if $p \in A$ then $\Gamma_p \in gD\mathbf{U}_p \subseteq gD\mathbf{U}$
- if $p \in C$ then $\Gamma_p \in gD\mathbf{U}_{f^{-1}(p)} \subseteq gD\mathbf{U}$
- if $p \in D$ then $\Gamma_p \notin gD(\mathbf{G}_{p'} \vee \mathbf{Ab}_p) \supseteq gD\mathbf{U}$

Papers:

- K. A., B. Steinberg, On the extension problem for partial permutations, PAMS 131, 2693-2703 (2003)
- K. A., On the decidability of membership in the global of a monoid pseudovariety, IJAC 20, 181-188 (2010).

Thanks!