Computations in direct powers

Peter Mayr

JKU Linz, Austria
peter.mayr@jku.at

Novi Sad, June 5, 2015

Supported by the Austrian Science Fund (FWF): P24285

JOHANNES KEPLER UNIVERSITY LINZ | JKU

FWF Der Wissenschaftsfonds.

Joint work with

- Andrei Bulatov (Vancouver)
- Jakub Bulin (Krakow)
- Markus Steindl (Linz)
- Ágnes Szendrei (Boulder)

Question

How to represent a family of finitary relations $R_1, R_2, \ldots$ over a set A?

Question

How to represent a family of finitary relations $R_1, R_2, \dots$ over a set A?

If A is finite, we can list the elements of relations (space intensive).

Question

How to represent a family of finitary relations $R_1, R_2, \dots$ over a set A?

If A is finite, we can list the elements of relations (space intensive).

Algebraic approach

1. Consider the polymorphisms F of $R_1, R_2, \dots,$ i.e., the operations on A that preserve every R_i.
2. Then $R_1, R_2, \dots$ are subalgebras of powers (**subpowers**) of the algebra $\mathbf{A} := (A, F)$ and can be represented by their generating sets.
3. In general more space efficient but:
   How to check that a tuple is in a relation given by generators?

Main problem

Fix a finite algebraic structure $\mathbf{A} = (A, F)$ with finite set of operations F (e.g., a group, ring, lattice, ...).

Subpower Membership Problem $\mathrm{SMP}(\mathbf{A})$ (Willard, 2007)

Input	$a_1, \ldots, a_k, b \in A^n$
Problem	Is b in the subalgebra of $\mathbf{A}^n$ that is generated by $a_1, \ldots, a_k$?

Main problem

Fix a finite algebraic structure $\mathbf{A} = (A, F)$ with finite set of operations F (e.g., a group, ring, lattice, ...).

Subpower Membership Problem $\mathrm{SMP}(\mathbf{A})$ (Willard, 2007)

Input	$a_1, \ldots, a_k, b \in A^n$
Problem	Is b in the subalgebra of $\mathbf{A}^n$ that is generated by $a_1, \ldots, a_k$?

What is its complexity in terms of k and n?

1. For vector spaces, the problem is in P (Gaussian elimination).
2. Elements of $B := \langle a_1, \ldots, a_k \rangle$ can be enumerated by a closure algorithm. Since $|B| \leq |A|^n$, this puts $\mathrm{SMP}(\mathbf{A})$ in $\mathrm{EXPTIME}$.

Complexity hierarchy

Goal

Given **A**, what is the complexity of $\mathrm{SMP}(\mathbf{A})$ within the range

$$\mathrm{P} \subseteq \mathrm{NP} \subseteq \mathrm{PSPACE} \subseteq \mathrm{EXPTIME}$$

Convention

All algebras will be finite and have finitely many basic operations.

EXPTIME

SMP and term functions

Clone Membership for $\mathbf{A} = (A, F)$

Input	$g\colon A^k \to A$ by its graph
Problem	Is g a term function on $\mathbf{A}$?

SMP and term functions

Clone Membership for $\mathbf{A} = (A, F)$

Input	$g\colon A^k \to A$ by its graph
Problem	Is g a term function on $\mathbf{A}$?

Note

1. SMP generalizes Clone Membership: $g\colon A^k \to A$ is a term function iff g is in the subalgebra of $\mathbf{A}^{A^k}$ that is generated by projection maps.

SMP and term functions

Clone Membership for $\mathbf{A} = (A, F)$

Input	$g\colon A^k \to A$ by its graph
Problem	Is g a term function on $\mathbf{A}$?

Note

1. SMP generalizes Clone Membership: $g\colon A^k \to A$ is a term function iff g is in the subalgebra of $\mathbf{A}^{A^k}$ that is generated by projection maps.
2. SMP asks: Is a given partial operation a term function?

$$b \in \langle a_1, \ldots, a_k \rangle$$

iff $g(a_1, \ldots, a_k) = b$ for some term function g

iff $\begin{cases} g(a_{11}, \ldots, a_{k1}) = b_1, \\ \vdots \\ g(a_{1n}, \ldots, a_{kn}) = b_n \end{cases}$ defines the restriction of a term function.

As hard as it gets

Theorem (Kozik, 2008)

There exists $\mathbf{A}$ for which Clone Membership (and hence SMP) is $\mathrm{EXPTIME}$-complete.

P

Classical results

Theorem (Furst, Hopcroft, Luks, 1980)

SMP is in P for groups.

Proof.

Uses Sims' stabilizer chains. □

Theorem (Baker, Pixley, 1975)

For $\mathbf{A}$ with d-ary near unanimity term, $\mathrm{SMP}(\mathbf{A})$ is in P.

Proof

1. $b \in \langle a_1, \ldots, a_k \rangle \leq \mathbf{A}^n$ iff $\pi_S(b) \in \langle \pi_S(a_1), \ldots, \pi_S(a_k) \rangle$ for all $S \subseteq [n], |S| \leq d-1$.
2. Need $\leq n^{d-1}$ membership tests in $\mathbf{A}^{d-1}$ at cost $O(k)$ each. □

Theorem (Mayr, 2012)

SMP is in P for algebras of size 2.

Theorem (Mayr, 2012)

SMP is in P for algebras of size 2.

Proof.

By Post's classification (1941) either **A**

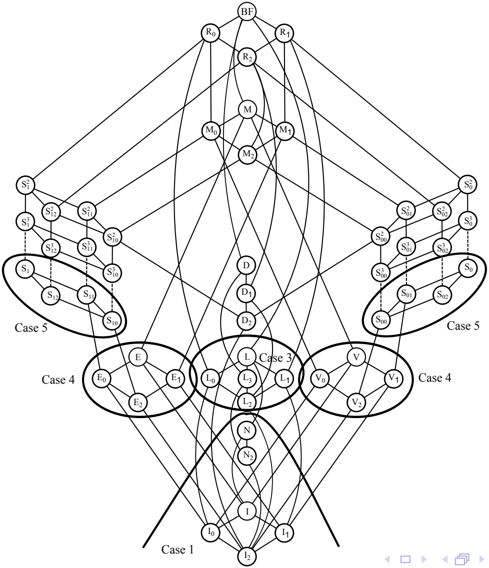
1. is unary,
2. has a near unanimity term,
3. is polynomially equivalent to $(\mathbb{Z}_2, +)$,
4. is polynomially equivalent to a semilattice,
5. is one of 4 reducts of the implication algebra with term $x \vee (y \wedge z)$ (or their duals).

In case 5, **A** has a term

$$w \vee \underbrace{(x \wedge y) \vee (x \wedge z) \vee (y \wedge z)}_{\text{majority operation}}$$

and membership can be checked by an adaptation of Baker-Pixley. □

Post's lattice



Algebras for which all subpowers have small generating sets

$\mathbf{A}$ has **few subpowers** if $\exists$ polynomial p $\forall n \in \mathbb{N}$: $|\{B \leq \mathbf{A}^n\}| \leq 2^{p(n)}$.

Algebras for which all subpowers have small generating sets

A has **few subpowers** if $\exists$ polynomial p $\forall n \in \mathbb{N}$: $|\{B \leq \mathbf{A}^n\}| \leq 2^{p(n)}$.

Theorem (Berman, Idziak, Markovic, McKenzie, Valeriote, Willard, 2010)

TFAE for **A**:

1. **A** has few subpowers.
2. $\exists$ polynomial q $\forall n \in \mathbb{N}$ $\forall B \leq \mathbf{A}^n$: B is generated by $\leq q(n)$ elements.
3. **A** has an edge (cube, parallelogram) term.

Algebras for which all subpowers have small generating sets

$\mathbf{A}$ has **few subpowers** if $\exists$ polynomial p $\forall n \in \mathbb{N}$: $|\{B \leq \mathbf{A}^n\}| \leq 2^{p(n)}$.

Theorem (Berman, Idziak, Markovic, McKenzie, Valeriote, Willard, 2010)

TFAE for $\mathbf{A}$:

1. $\mathbf{A}$ has few subpowers.
2. $\exists$ polynomial q $\forall n \in \mathbb{N}$ $\forall B \leq \mathbf{A}^n$: B is generated by $\leq q(n)$ elements.
3. $\mathbf{A}$ has an edge (cube, parallelogram) term.

Example

Algebras with group operation (Mal'cev term) or lattice operation (near unanimity term) have few subpowers. Equivalently, their subpowers have generating sets whose size is polynomial in the length of tuples.

Kearnes, Szendrei (2012)

A $(d+3)$-ary term operation p on $\mathbf{A}$ is a $(1, d-1)$-**parallelogram term** if

$$p\left(\begin{array}{ccc|cccccc} x & x & y & z & y & \dots & \dots & y \\ y & x & x & y & \ddots & \ddots & & \vdots \\ \vdots & \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \vdots & \vdots & \vdots & & \ddots & \ddots & y \\ y & x & x & y & \dots & \dots & y & z \end{array}\right) \approx \begin{pmatrix} y \\ \vdots \\ \vdots \\ \vdots \\ y \end{pmatrix}.$$

Equivalent problems

For $\mathbf{A}$ with few subpowers, every $B \leq \mathbf{A}^n$ has a **compact representation** (a generating set of particular form and size polynomial in n, Berman, et al, 2010).

Equivalent problems

For **A** with few subpowers, every $B \leq \mathbf{A}^n$ has a **compact representation** (a generating set of particular form and size polynomial in n, Berman, et al, 2010).

Lemma (Idziak, Markovic, McKenzie, Valeriote, Willard, 2010)

For **A** with few subpowers and $B \leq \mathbf{A}^n$ given by compact representation, deciding membership in B is in P.

Equivalent problems

For **A** with few subpowers, every $B \leq \mathbf{A}^n$ has a **compact representation** (a generating set of particular form and size polynomial in n, Berman, et al, 2010).

Lemma (Idziak, Markovic, McKenzie, Valeriote, Willard, 2010)

For **A** with few subpowers and $B \leq \mathbf{A}^n$ given by compact representation, deciding membership in B is in P.

Lemma (Mayr, 2014)

For **A** with few subpowers the following are equivalent under polynomial reduction:

1. SMP.
2. Given a subpower B by arbitrary generators, determine a compact representation of B.
3. Given subpowers B, C by generators, determine generators of $B \cap C$.

Results

Lemma (Mayr, 2014)

SMP is in NP for algebras with few subpowers.

Proof.

Uses compact representations. $\square$

Theorem (Mayr, 2012)

SMP is in P for expansions of p-groups (more generally, of nilpotent Mal'cev algebras of prime power size).

Proof.

Uses structure of nilpotent Mal'cev algebras (Freese, McKenzie, 1987) and group representation theory. □

Reduction lemmas

Lemma (Bulatov, Mayr, Szendrei, 2014)

For $\mathbf{A}$ with few subpowers, $\mathrm{SMP}(\mathbf{A})$ reduces to membership problems for $B \leq_{sd} \mathbf{B}_1 \times \cdots \times \mathbf{B}_n$ where for all $i \neq j$:

1. $\mathbf{B}_i \in HS(\mathbf{A})$ is subdirectly irreducible with abelian monolith μ_i,
2. $\pi_{ij}(B)/(0 : \mu_i) \times (0 : \mu_j)$ is the graph of an isomorphism.

Reduction lemmas

Lemma (Bulatov, Mayr, Szendrei, 2014)

For **A** with few subpowers, $\mathrm{SMP}(\mathbf{A})$ reduces to membership problems for $B \leq_{sd} \mathbf{B}_1 \times \cdots \times \mathbf{B}_n$ where for all $i \neq j$:

1. $\mathbf{B}_i \in HS(\mathbf{A})$ is subdirectly irreducible with abelian monolith μ_i,
2. $\pi_{ij}(B)/(0 : \mu_i) \times (0 : \mu_j)$ is the graph of an isomorphism.

Proof.

Uses critical relations (Kearnes, Szendrei, 2012). □

Reduction lemmas

Lemma (Bulatov, Mayr, Szendrei, 2014)

For $\mathbf{A}$ with few subpowers, $\mathrm{SMP}(\mathbf{A})$ reduces to membership problems for $B \leq_{sd} \mathbf{B}_1 \times \cdots \times \mathbf{B}_n$ where for all $i \neq j$:

1. $\mathbf{B}_i \in HS(\mathbf{A})$ is subdirectly irreducible with abelian monolith μ_i,
2. $\pi_{ij}(B)/(0 : \mu_i) \times (0 : \mu_j)$ is the graph of an isomorphism.

Proof.

Uses critical relations (Kearnes, Szendrei, 2012). □

Lemma (Bulatov, Mayr, Szendrei, 2014)

Membership for B as above reduces to membership for $C \leq_{sd} \mathbf{C}_1 \times \cdots \times \mathbf{C}_m$ with $\mathbf{C}_1, \ldots, \mathbf{C}_m$ subdirectly irreducible with central monoliths and with edge term.

Proof.

Blocks for centralizers $(0 : \mu_i)$ are turned into algebras $\mathbf{C}_j$. □

Main result

Theorem (Bulatov, Mayr, Szendrei, 2014)

Let $\mathbf{A}$ with few subpowers such that every subdirectly irreducible $\mathbf{B} \in HS(\mathbf{A})$ has a monolith with supernilpotent centralizer. Then $\mathrm{SMP}(\mathbf{A})$ is in P.

Proof.

By our Reduction Lemmas $\mathrm{SMP}(\mathbf{A})$ reduces to membership problems for $C \leq_{sd} \mathbf{C}_1 \times \cdots \times \mathbf{C}_m$ with supernilpotent Mal'cev algebras $\mathbf{C}_1, \ldots, \mathbf{C}_m$. These are in P by Mayr, 2012. □

Consequences

Corollary (Bulatov, Mayr, Szendrei, 2014)

SMP is in P for algebras with few subpowers in a residually finite variety.

Consequences

Corollary (Bulatov, Mayr, Szendrei, 2014)

SMP is in P for algebras with few subpowers in a residually finite variety.

Corollary (Bulatov, Mayr, Szendrei, 2014)

$\mathrm{SMP}(\mathbf{A})$ is in P for Mal'cev algebras $\mathbf{A}$ with $|A| \leq 3$.

Can we compute efficiently with generators of subpowers?

Question (Willard, 2007; Idziak, et al, 2010)

Is SMP in P for every algebra with few subpowers?

Still open in general, even for Mal'cev algebras, expansions of groups.

NP

Semigroups are hard

Example (Bulatov, 2014)

The semigroup $\mathbf{S}^1 := (\{0, a, 1\}, \cdot)$ with

$\cdot$	0	a	1
0	0	0	0
a	0	0	a
1	0	a	1

has NP-complete SMP.

Proof.

Since $\mathbf{S}^1$ is commutative, $\mathrm{SMP}(\mathbf{S}^1)$ is in NP.
For NP-hardness, we reduce the following NP-complete problem to SMP.

Set Covering Problem

Input	subsets $T_1, \ldots, T_k$ of $[n] = \{1, \ldots, n\}$
Problem	Is $[n]$ a disjoint union of some of the $T_1, \ldots, T_k$?

Proof.

Since $\mathbf{S}^1$ is commutative, $\mathrm{SMP}(\mathbf{S}^1)$ is in NP.
For NP-hardness, we reduce the following NP-complete problem to SMP.

Set Covering Problem

Input	subsets $T_1, \ldots, T_k$ of $[n] = \{1, \ldots, n\}$
Problem	Is $[n]$ a disjoint union of some of the $T_1, \ldots, T_k$?

For $T \subseteq [n]$, consider its **characteristic function** $a_T \in (S^1)^n$,

$$a_T(i) := \begin{cases} a & \text{if } i \in T, \\ 1 & \text{else.} \end{cases}$$

Recall $a^2 = 0$.
Then $[n] = T_{i_1} \dot\cup \cdots \dot\cup T_{i_\ell}$ iff $a_{[n]} = a_{T_{i_1}} \cdots a_{T_{i_\ell}}$. □

A dichotomy for commutative semigroups

Theorem (Bulatov, Mayr, Steindl, 2015)

Let **S** be a commutative semigroup. Then $\mathrm{SMP}(\mathbf{S})$ is in P if **S** embeds into a direct product of a nilpotent semigroup and a Clifford semigroup; NP-complete otherwise.

PSPACE

Semigroups are PSPACE-easy

Theorem (Bulatov, Mayr, Steindl, 2015)

SMP for semigroups is in PSPACE.

Semigroups are PSPACE-easy

Theorem (Bulatov, Mayr, Steindl, 2015)

SMP for semigroups is in PSPACE.

Proof

1. If $b \in \langle a_1, \ldots, a_k \rangle$, then $b = a_{i_1} \ldots a_{i_m}$ for $i_1, \ldots, i_m \in [k]$.
2. A nondeterministic Turing machine can guess factors a_{i_j} one by one saving only the last partial product $a_{i_1} \ldots a_{i_j}$ until it reaches b. This takes space $O(n)$.
3. Hence SMP is in NPSPACE (which is equal to PSPACE by Savitch's Theorem). □

PSPACE-hard semigroup

Theorem (Bulatov, Mayr, Steindl, 2015)

SMP for the full transformation semigroup $\mathbf{T}_5$ on 5 letters is PSPACE-complete.

PSPACE-hard semigroup

Theorem (Bulatov, Mayr, Steindl, 2015)

SMP for the full transformation semigroup $\mathbf{T}_5$ on 5 letters is PSPACE-complete.

Proof

We reduce Quantified SAT (which is PSPACE-complete) to SMP. Given an instance of 3QSAT

$$\Phi := \forall x_1 \exists y_1 \dots \forall x_n \exists y_n \left(\bigvee C_1\right) \wedge \dots \wedge \left(\bigvee C_m\right)$$

with clauses $C_1, \dots, C_m$ of length 3, define an instance of $\mathrm{SMP}(\mathbf{T}_5)$ such that

$$\Phi \text{ is true iff } e \in \langle G \rangle.$$

Recall $\Phi = \forall x_1 \exists y_1 \dots \forall x_n \exists y_n \, (\bigvee C_1) \wedge \cdots \wedge (\bigvee C_m)$

$G := \{a, a_1, \dots, a_n, b_1^{-1/0/+1}, \dots, b_n^{-1/0/+1}, c, d\}$ and e are in T_5^{3n+m}

Recall $\Phi = \forall x_1 \exists y_1 \ldots \forall x_n \exists y_n \, (\bigvee C_1) \wedge \cdots \wedge (\bigvee C_m)$

$$G := \{a, a_1, \ldots, a_n, b_1^{-1/0/+1}, \ldots, b_n^{-1/0/+1}, c, d\} \text{ and } e \text{ are in } T_5^{3n+m}$$

Basic ideas:

1. The first $2n$ coordinates encode assignments $0, 1$ of the variables, the next m give the number $0, 1, 2, 3$ of literals satisfied in each clause, the rest governs the order of multiplication of generators.

Recall $\Phi = \forall x_1 \exists y_1 \dots \forall x_n \exists y_n \; (\bigvee C_1) \wedge \cdots \wedge (\bigvee C_m)$

$G := \{a, a_1, \dots, a_n, b_1^{-1/0/+1}, \dots, b_n^{-1/0/+1}, c, d\}$ and e are in T_5^{3n+m}

Basic ideas:

1. The first $2n$ coordinates encode assignments $0, 1$ of the variables, the next m give the number $0, 1, 2, 3$ of literals satisfied in each clause, the rest governs the order of multiplication of generators.
2. a_i changes universal variables, $b_i^{-1/0/+1}$ changes existential variables.

Recall $\Phi = \forall x_1 \exists y_1 \ldots \forall x_n \exists y_n \ (\bigvee C_1) \wedge \cdots \wedge (\bigvee C_m)$

$G := \{a, a_1, \ldots, a_n, b_1^{-1/0/+1}, \ldots, b_n^{-1/0/+1}, c, d\}$ and e are in T_5^{3n+m}

Basic ideas:

1. The first $2n$ coordinates encode assignments $0, 1$ of the variables, the next m give the number $0, 1, 2, 3$ of literals satisfied in each clause, the rest governs the order of multiplication of generators.
2. a_i changes universal variables, $b_i^{-1/0/+1}$ changes existential variables.
3. $e \in \langle G \rangle$ iff $g_1 \ldots g_\ell = e$ for some $g_1, \ldots, g_\ell \in G$ with partial products encoding satisfying assignments for the existential variables for all 2^n choices for the universal variables. □

Product of automata

Automata Intersection Problem

Input	$F_1, \ldots, F_n$ deterministic finite state automata with common alphabet Σ
Problem	Is there a word in Σ^* that is accepted by all of $F_1, \ldots, F_n$?

Product of automata

Automata Intersection Problem

Input	$F_1, \ldots, F_n$ deterministic finite state automata with common alphabet Σ
Problem	Is there a word in Σ^* that is accepted by all of $F_1, \ldots, F_n$?

Theorem (Kozen, 1977)

The Automata Intersection Problem is PSPACE-complete.

Note

PSPACE-complete even if $F_1, \ldots, F_n$ have only 4 states (Bulatov, Mayr, Steindl, 2015).

Conclusion

$$\mathrm{P} \subseteq \mathrm{NP} \subseteq \mathrm{PSPACE} \subseteq \mathrm{EXPTIME}$$

1. $\mathrm{SMP}(\mathbf{A})$ is always in $\mathrm{EXPTIME}$ and is $\mathrm{EXPTIME}$-complete for some **A**.
2. SMP for **A** with few subpowers is in NP, not known to be in P in general.
3. There are semigroups for which SMP is in P, NP-complete, or PSPACE-complete.