On the Subpower Membership Problem

Jakub Bulín

Charles University in Prague & Jagiellonian University in Kraków

SSAOS 2014

joint work with

Peter Mayr (JKU Linz),

supported by
Austrian Science Fund project P24285

Subpower membership problem

Fix a finite, finitely presented algebra $\mathbf{A} = (A; f_1, \ldots, f_m)$.

Subpower membership problem for $\mathbf{A}$ (Willard '07)

INPUT: $\mathbf{a_1}, \ldots, \mathbf{a_k}, \mathbf{b} \in A^n$
QUESTION: Is $\mathbf{b} \in \langle \mathbf{a_1}, \ldots, \mathbf{a_k} \rangle$*?*

- equivalently: does a partial operation (n-ary, defined on k inputs) extend to a term operation of $\mathbf{A}$?
- size of the input: $n \cdot (k+1) \cdot \log |A| \sim O(nk)$
- SMP($\mathbf{A}$) is in EXPTIME (naive algorithm: generate all elements of $\langle \mathbf{a_1}, \ldots, \mathbf{a_k} \rangle$)
- $\mathbf{A}$ polynomially evaluable := SMP($\mathbf{A}$) is in P

Subpower membership problem

Fix a finite, finitely presented algebra $\mathbf{A} = (A; f_1, \ldots, f_m)$.

Subpower membership problem for $\mathbf{A}$ (Willard '07)

INPUT: $\mathbf{a_1}, \ldots, \mathbf{a_k}, \mathbf{b} \in A^n$
QUESTION: Is $\mathbf{b} \in \langle \mathbf{a_1}, \ldots, \mathbf{a_k} \rangle$*?*

- equivalently: does a partial operation (n-ary, defined on k inputs) extend to a term operation of $\mathbf{A}$?
- size of the input: $n \cdot (k+1) \cdot \log |A| \sim O(nk)$
- SMP($\mathbf{A}$) is in EXPTIME (naive algorithm: generate all elements of $\langle \mathbf{a_1}, \ldots, \mathbf{a_k} \rangle$)
- $\mathbf{A}$ polynomially evaluable := SMP($\mathbf{A}$) is in P

Fix a finite, finitely presented algebra $\mathbf{A} = (A; f_1, \ldots, f_m)$.

Subpower membership problem for $\mathbf{A}$ (Willard '07)

INPUT: $\mathbf{a_1}, \ldots, \mathbf{a_k}, \mathbf{b} \in A^n$
QUESTION: Is $\mathbf{b} \in \langle \mathbf{a_1}, \ldots, \mathbf{a_k} \rangle$*?*

- equivalently: does a partial operation (n-ary, defined on k inputs) extend to a term operation of $\mathbf{A}$?
- size of the input: $n \cdot (k+1) \cdot \log |A| \sim O(nk)$
- SMP($\mathbf{A}$) is in EXPTIME (naive algorithm: generate all elements of $\langle \mathbf{a_1}, \ldots, \mathbf{a_k} \rangle$)
- $\mathbf{A}$ polynomially evaluable := SMP($\mathbf{A}$) is in P

A subproblem of SMP:

Clone membership problem

INPUT: an operation $f : A^k \to A$
QUESTION: Is $f \in \mathrm{Clo}(\mathbf{A})$ *(the clone of term functions)?*

Reduction: write f and the projection operations $p_i^k(x_1, \ldots, x_k) = x_i$ $(1 \leq i \leq k)$ as $|A|^k$-ary tuples, test if $f \in \langle p_1^k, \ldots, p_k^k \rangle$.

Theorem (Kozik '08)

There exists $\mathbf{A}$ *such that CLOMEM(*$\mathbf{A}$*) (and thus also SMP(*$\mathbf{A}$*)) is EXPTIME-complete.*

- idea: model computation of an alternating Turing machine
- $\mathbf{A}$ is not nice (HSP($\mathbf{A}$) admits TCT type 1)

A subproblem of SMP:

Clone membership problem

INPUT: an operation $f : A^k \to A$
QUESTION: Is $f \in \mathrm{Clo}(\mathbf{A})$ *(the clone of term functions)?*

Reduction: write f and the projection operations $p_i^k(x_1, \ldots, x_k) = x_i$ $(1 \leq i \leq k)$ as $|A|^k$-ary tuples, test if $f \in \langle p_1^k, \ldots, p_k^k \rangle$.

Theorem (Kozik '08)

There exists $\mathbf{A}$ *such that CLOMEM(*$\mathbf{A}$*) (and thus also SMP(*$\mathbf{A}$*)) is EXPTIME-complete.*

- idea: model computation of an alternating Turing machine
- $\mathbf{A}$ is not nice (HSP($\mathbf{A}$) admits TCT type 1)

A subproblem of SMP:

Clone membership problem

INPUT: an operation $f : A^k \to A$
QUESTION: Is $f \in \mathrm{Clo}(\mathbf{A})$ *(the clone of term functions)?*

Reduction: write f and the projection operations $p_i^k(x_1, \ldots, x_k) = x_i$ $(1 \leq i \leq k)$ as $|A|^k$-ary tuples, test if $f \in \langle p_1^k, \ldots, p_k^k \rangle$.

Theorem (Kozik '08)

There exists $\mathbf{A}$ *such that CLOMEM(*$\mathbf{A}$*) (and thus also SMP(*$\mathbf{A}$*)) is EXPTIME-complete.*

- idea: model computation of an alternating Turing machine
- $\mathbf{A}$ is not nice (HSP($\mathbf{A}$) admits TCT type 1)

A subproblem of SMP:

Clone membership problem

INPUT: an operation $f : A^k \to A$
QUESTION: Is $f \in \mathrm{Clo}(\mathbf{A})$ *(the clone of term functions)?*

Reduction: write f and the projection operations $p_i^k(x_1, \ldots, x_k) = x_i$ $(1 \leq i \leq k)$ as $|A|^k$-ary tuples, test if $f \in \langle p_1^k, \ldots, p_k^k \rangle$.

Theorem (Kozik '08)

There exists $\mathbf{A}$ *such that CLOMEM(*$\mathbf{A}$*) (and thus also SMP(*$\mathbf{A}$*)) is EXPTIME-complete.*

- idea: model computation of an alternating Turing machine
- $\mathbf{A}$ is not nice (HSP($\mathbf{A}$) admits TCT type 1)

An NP-complete semigroup

(Bulatov '13): The following semigroup has an NP-complete SMP.

$*$	0	1	∞
0	0	1	∞
1	1	∞	∞
∞	∞	∞	∞

- in NP: commutative semigroup $\rightarrow$ normal form for terms
- NP-hard: reduction from the Exact cover problem:
  - given $\mathcal{S} = \{S_1, \ldots, S_k\} \subseteq \mathcal{P}(X)$, can X be exactly covered by a subset of $\mathcal{S}$?
  - set $\mathbf{a}_i = \chi_{S_i}$ $(1 \leq i \leq k)$ and $\mathbf{b} = (1, 1, \ldots, 1)$

(Steindl '14): work towards a characterization of some classes of semigroups wrt. complexity of SMP

An NP-complete semigroup

(Bulatov '13): The following semigroup has an NP-complete SMP.

$*$	0	1	∞
0	0	1	∞
1	1	∞	∞
∞	∞	∞	∞

- in NP: commutative semigroup $\rightarrow$ normal form for terms
- NP-hard: reduction from the Exact cover problem:
  - given $\mathcal{S} = \{S_1, \ldots, S_k\} \subseteq \mathcal{P}(X)$, can X be exactly covered by a subset of $\mathcal{S}$?
  - set $\mathbf{a}_i = \chi_{S_i}$ $(1 \leq i \leq k)$ and $\mathbf{b} = (1, 1, \ldots, 1)$

(Steindl '14): work towards a characterization of some classes of semigroups wrt. complexity of SMP

An NP-complete semigroup

(Bulatov '13): The following semigroup has an NP-complete SMP.

$*$	0	1	∞
0	0	1	∞
1	1	∞	∞
∞	∞	∞	∞

- in NP: commutative semigroup $\rightarrow$ normal form for terms
- NP-hard: reduction from the Exact cover problem:
  - given $\mathcal{S} = \{S_1, \ldots, S_k\} \subseteq \mathcal{P}(X)$, can X be exactly covered by a subset of $\mathcal{S}$?
  - set $\mathbf{a}_i = \chi_{S_i}$ $(1 \leq i \leq k)$ and $\mathbf{b} = (1, 1, \ldots, 1)$

(Steindl '14): work towards a characterization of some classes of semigroups wrt. complexity of SMP

(Bulatov '13): The following semigroup has an NP-complete SMP.

$*$	0	1	∞
0	0	1	∞
1	1	∞	∞
∞	∞	∞	∞

- in NP: commutative semigroup $\rightarrow$ normal form for terms
- NP-hard: reduction from the Exact cover problem:
  - given $\mathcal{S} = \{S_1, \ldots, S_k\} \subseteq \mathcal{P}(X)$, can X be exactly covered by a subset of $\mathcal{S}$?
  - set $\mathbf{a}_i = \chi_{S_i}$ $(1 \leq i \leq k)$ and $\mathbf{b} = (1, 1, \ldots, 1)$

(Steindl '14): work towards a characterization of some classes of semigroups wrt. complexity of SMP

A near-unanimity operation:
$f(x, \dots, x, y) \approx \cdots \approx f(y, x, \dots, x) \approx x$.

Theorem (Baker, Pixley '75)

If there exists an $(r+1)$-ary NU $f \in \mathrm{Clo}(\mathbf{A})$, then all subpowers of $\mathbf{A}$ are determined by projections to r-element subsets of coordinates.

- in our setting: $\mathbf{b} \in \langle \mathbf{a_1}, \dots, \mathbf{a_k} \rangle$ iff for all $S \subseteq [n]$, $|S| \leq r$ we have $\mathrm{pr}_S \mathbf{b} \in \langle \mathrm{pr}_S \mathbf{a_1}, \dots, \mathrm{pr}_S \mathbf{a_k} \rangle$.
- this gives an $O((nk)^r)$ algorithm for SMP($\mathbf{A}$), since we can find the NU (Maróti '09), in constant time!
- lattices have ternary NU: $(x \wedge y) \vee (y \wedge z) \vee (z \wedge x)$

Corollary

Lattices (and their extensions) are polynomially evaluable.

A near-unanimity operation:
$f(x, \dots, x, y) \approx \cdots \approx f(y, x, \dots, x) \approx x$.

Theorem (Baker, Pixley '75)

If there exists an $(r+1)$-ary NU $f \in \mathrm{Clo}(\mathbf{A})$, then all subpowers of $\mathbf{A}$ are determined by projections to r-element subsets of coordinates.

- in our setting: $\mathbf{b} \in \langle \mathbf{a_1}, \dots, \mathbf{a_k} \rangle$ iff for all $S \subseteq [n]$, $|S| \leq r$ we have $\mathrm{pr}_S \mathbf{b} \in \langle \mathrm{pr}_S \mathbf{a_1}, \dots, \mathrm{pr}_S \mathbf{a_k} \rangle$.
- this gives an $O((nk)^r)$ algorithm for SMP($\mathbf{A}$), since we can find the NU (Maróti '09), in constant time!
- lattices have ternary NU: $(x \wedge y) \vee (y \wedge z) \vee (z \wedge x)$

Corollary

Lattices (and their extensions) are polynomially evaluable.

A near-unanimity operation:
$f(x, \dots, x, y) \approx \cdots \approx f(y, x, \dots, x) \approx x$.

Theorem (Baker, Pixley '75)

If there exists an $(r+1)$-ary NU $f \in \mathrm{Clo}(\mathbf{A})$, then all subpowers of $\mathbf{A}$ are determined by projections to r-element subsets of coordinates.

- in our setting: $\mathbf{b} \in \langle \mathbf{a_1}, \dots, \mathbf{a_k} \rangle$ iff for all $S \subseteq [n]$, $|S| \leq r$ we have $\mathrm{pr}_S \mathbf{b} \in \langle \mathrm{pr}_S \mathbf{a_1}, \dots, \mathrm{pr}_S \mathbf{a_k} \rangle$.
- this gives an $O((nk)^r)$ algorithm for SMP($\mathbf{A}$), since we can find the NU (Maróti '09), in constant time!
- lattices have ternary NU: $(x \wedge y) \vee (y \wedge z) \vee (z \wedge x)$

Corollary

Lattices (and their extensions) are polynomially evaluable.

A near-unanimity operation:
$f(x, \dots, x, y) \approx \cdots \approx f(y, x, \dots, x) \approx x$.

Theorem (Baker, Pixley '75)

If there exists an $(r+1)$*-ary NU* $f \in \mathrm{Clo}(\mathbf{A})$*, then all subpowers of* $\mathbf{A}$ *are determined by projections to* r*-element subsets of coordinates.*

- in our setting: $\mathbf{b} \in \langle \mathbf{a_1}, \dots, \mathbf{a_k} \rangle$ iff for all $S \subseteq [n]$, $|S| \leq r$ we have $\mathrm{pr}_S \mathbf{b} \in \langle \mathrm{pr}_S \mathbf{a_1}, \dots, \mathrm{pr}_S \mathbf{a_k} \rangle$.
- this gives an $O((nk)^r)$ algorithm for SMP($\mathbf{A}$), since we can find the NU (Maróti '09), in constant time!
- lattices have ternary NU: $(x \wedge y) \vee (y \wedge z) \vee (z \wedge x)$

Corollary

Lattices (and their extensions) are polynomially evaluable.

A near-unanimity operation:
$f(x, \dots, x, y) \approx \cdots \approx f(y, x, \dots, x) \approx x$.

Theorem (Baker, Pixley '75)

If there exists an $(r+1)$*-ary NU* $f \in \mathrm{Clo}(\mathbf{A})$*, then all subpowers of* $\mathbf{A}$ *are determined by projections to* r*-element subsets of coordinates.*

- in our setting: $\mathbf{b} \in \langle \mathbf{a_1}, \dots, \mathbf{a_k} \rangle$ iff for all $S \subseteq [n]$, $|S| \leq r$ we have $\mathrm{pr}_S \mathbf{b} \in \langle \mathrm{pr}_S \mathbf{a_1}, \dots, \mathrm{pr}_S \mathbf{a_k} \rangle$.
- this gives an $O((nk)^r)$ algorithm for SMP($\mathbf{A}$), since we can find the NU (Maróti '09), in constant time!
- lattices have ternary NU: $(x \wedge y) \vee (y \wedge z) \vee (z \wedge x)$

Corollary

Lattices (and their extensions) are polynomially evaluable.

2-element algebras are polynomially evaluable

Theorem (Post '41)

Every two-element algebra is term-equivalent to one of the following:

1. *an essentially unary algebra*
2. *a semilattice with no, one or two constants*
3. *an algebra with $x \wedge (y \vee z)$ or its dual*
4. *an algebra with a near-unanimity operation*
5. *an algebra with a Maltsev operation $x + y + z$*

Corollary

Every two-element algebra is polynomially evaluable.

2-element algebras are polynomially evaluable

Theorem (Post '41)

Every two-element algebra is term-equivalent to one of the following:

1. *an essentially unary algebra*
2. *a semilattice with no, one or two constants*
3. *an algebra with $x \wedge (y \vee z)$ or its dual*
4. *an algebra with a near-unanimity operation*
5. *an algebra with a Maltsev operation $x + y + z$*

Corollary

Every two-element algebra is polynomially evaluable.

An interesting class: Maltsev algebras

A Maltsev algebra: $\varphi \in \mathrm{Clo}_3(\mathbf{A})$ with $\varphi(x,x,y) \approx y \approx \varphi(y,x,x)$; equivalently, $\mathrm{HSP}(\mathbf{A})$ is *congruence permutable*.

Problem (Willard '07)

Are all (finite) Maltsev algebras polynomially evaluable?

- (Mayr '12): SMP is in NP for all Maltsev algebras
- (Newton 1670): finite fields
- (Sims '71; Furst, Hopcroft, Luks '80): groups
- (Willard '07): expansions of groups by multilinear operations, eg. rings, modules, nonassociative rings, ...
- abelian Maltsev algebras
- (Mayr '12): algebras of prime power order with a nilpotent reduct, eg. expansions of p-groups; so-called supernilpotence

An interesting class: Maltsev algebras

A Maltsev algebra: $\varphi \in \mathrm{Clo}_3(\mathbf{A})$ with $\varphi(x,x,y) \approx y \approx \varphi(y,x,x)$; equivalently, $\mathrm{HSP}(\mathbf{A})$ is *congruence permutable*.

Problem (Willard '07)

Are all (finite) Maltsev algebras polynomially evaluable?

- (Mayr '12): SMP is in NP for all Maltsev algebras
- (Newton 1670): finite fields
- (Sims '71; Furst, Hopcroft, Luks '80): groups
- (Willard '07): expansions of groups by multilinear operations, eg. rings, modules, nonassociative rings, ...
- abelian Maltsev algebras
- (Mayr '12): algebras of prime power order with a nilpotent reduct, eg. expansions of p-groups; so-called supernilpotence

An interesting class: Maltsev algebras

A Maltsev algebra: $\varphi \in \mathrm{Clo}_3(\mathbf{A})$ with $\varphi(x,x,y) \approx y \approx \varphi(y,x,x)$; equivalently, $\mathrm{HSP}(\mathbf{A})$ is *congruence permutable*.

Problem (Willard '07)

Are all (finite) Maltsev algebras polynomially evaluable?

- (Mayr '12): SMP is in NP for all Maltsev algebras
- (Newton 1670): finite fields
- (Sims '71; Furst, Hopcroft, Luks '80): groups
- (Willard '07): expansions of groups by multilinear operations, eg. rings, modules, nonassociative rings, ...
- abelian Maltsev algebras
- (Mayr '12): algebras of prime power order with a nilpotent reduct, eg. expansions of p-groups; so-called supernilpotence

Let $\mathbf{A}$ be a finite algebra with a Maltsev term φ and $R \subseteq A^n$.

- a pair $\mathbf{x}, \mathbf{y} \in A^n$ witnesses a fork (a, b) at i-th coordinate, if

$$\mathbf{x} = (x_1, x_2, \ldots, x_{i-1}, a, ?, ?, \ldots, ?)$$
$$\mathbf{y} = (x_1, x_2, \ldots, x_{i-1}, b, ?, ?, \ldots, ?)$$

- a signature of R: $\operatorname{Sig} R \subseteq A^2 \times [n]$ . . . forks witnessed by tuples from R
- a compact representation of R: $R' \subseteq R$ such that

$$\operatorname{Sig} R' = \operatorname{Sig} R \;\&\; |R'| \leq 2 \cdot |\operatorname{Sig} R|$$

Theorem (Bulatov, Dalmau '06)

If R' is a compact representation of R, then $\langle R' \rangle_\varphi = R$.

Let $\mathbf{A}$ be a finite algebra with a Maltsev term φ and $R \subseteq A^n$.

- a pair $\mathbf{x}, \mathbf{y} \in A^n$ witnesses a fork (a, b) at i-th coordinate, if

$$\mathbf{x} = (x_1, x_2, \ldots, x_{i-1}, a, ?, ?, \ldots, ?)$$
$$\mathbf{y} = (x_1, x_2, \ldots, x_{i-1}, b, ?, ?, \ldots, ?)$$

- a signature of R: $\operatorname{Sig} R \subseteq A^2 \times [n]$ . . . forks witnessed by tuples from R
- a compact representation of R: $R' \subseteq R$ such that

$$\operatorname{Sig} R' = \operatorname{Sig} R \;\&\; |R'| \leq 2 \cdot |\operatorname{Sig} R|$$

Theorem (Bulatov, Dalmau '06)

If R' is a compact representation of R, then $\langle R' \rangle_\varphi = R$.

Let $\mathbf{A}$ be a finite algebra with a Maltsev term φ and $R \subseteq A^n$.

- a pair $\mathbf{x}, \mathbf{y} \in A^n$ witnesses a fork (a, b) at i-th coordinate, if

$$\mathbf{x} = (x_1, x_2, \ldots, x_{i-1}, a, ?, ?, \ldots, ?)$$
$$\mathbf{y} = (x_1, x_2, \ldots, x_{i-1}, b, ?, ?, \ldots, ?)$$

- a signature of R: $\operatorname{Sig} R \subseteq A^2 \times [n]$ . . . forks witnessed by tuples from R
- a compact representation of R: $R' \subseteq R$ such that

$$\operatorname{Sig} R' = \operatorname{Sig} R \;\&\; |R'| \leq 2 \cdot |\operatorname{Sig} R|$$

Theorem (Bulatov, Dalmau '06)

If R' is a compact representation of R, then $\langle R' \rangle_\varphi = R$.

Let $\mathbf{A}$ be a finite algebra with a Maltsev term φ and $R \subseteq A^n$.

- a pair $\mathbf{x}, \mathbf{y} \in A^n$ witnesses a fork (a, b) at i-th coordinate, if

$$\mathbf{x} = (x_1, x_2, \ldots, x_{i-1}, a, ?, ?, \ldots, ?)$$
$$\mathbf{y} = (x_1, x_2, \ldots, x_{i-1}, b, ?, ?, \ldots, ?)$$

- a signature of R: $\operatorname{Sig} R \subseteq A^2 \times [n]$ . . . forks witnessed by tuples from R
- a compact representation of R: $R' \subseteq R$ such that

$$\operatorname{Sig} R' = \operatorname{Sig} R \;\&\; |R'| \leq 2 \cdot |\operatorname{Sig} R|$$

Theorem (Bulatov, Dalmau '06)

If R' is a compact representation of R, then $\langle R' \rangle_\varphi = R$.

Let $\mathbf{A}$ be a finite algebra with a Maltsev term φ and $R \subseteq A^n$.

- a pair $\mathbf{x}, \mathbf{y} \in A^n$ witnesses a fork (a, b) at i-th coordinate, if

$$\mathbf{x} = (x_1, x_2, \ldots, x_{i-1}, a, ?, ?, \ldots, ?)$$
$$\mathbf{y} = (x_1, x_2, \ldots, x_{i-1}, b, ?, ?, \ldots, ?)$$

- a signature of R: $\operatorname{Sig} R \subseteq A^2 \times [n]$ . . . forks witnessed by tuples from R
- a compact representation of R: $R' \subseteq R$ such that

$$\operatorname{Sig} R' = \operatorname{Sig} R \;\&\; |R'| \leq 2 \cdot |\operatorname{Sig} R|$$

Theorem (Bulatov, Dalmau '06)

If R' is a compact representation of R, then $\langle R' \rangle_\varphi = R$.

Some (useful??) observations

- SMP($\mathbf{A}$) is equivalent to the following problem: given generators of $R \leq \mathbf{A}^n$ and $a, b \in A$, decide if the fork (a, b) at the n-th coordinate is witnessed in R (no need to produce the witnessing tuples)
- we can assume that R is subdirect and the projections are SI algebras ("multisorted" compact representations)
- if all SI factors of $\mathbf{A}$ are simple, then $\mathbf{A}$ is polynomially evaluable
- we do not know how to "climb up the congruence lattice"

Some (useful??) observations

- SMP($\mathbf{A}$) is equivalent to the following problem: given generators of $R \leq \mathbf{A}^n$ and $a, b \in A$, decide if the fork (a, b) at the n-th coordinate is witnessed in R (no need to produce the witnessing tuples)
- we can assume that R is subdirect and the projections are SI algebras ("multisorted" compact representations)
- if all SI factors of $\mathbf{A}$ are simple, then $\mathbf{A}$ is polynomially evaluable
- we do not know how to "climb up the congruence lattice"

Some (useful??) observations

- SMP($\mathbf{A}$) is equivalent to the following problem: given generators of $R \leq \mathbf{A}^n$ and $a, b \in A$, decide if the fork (a, b) at the n-th coordinate is witnessed in R (no need to produce the witnessing tuples)
- we can assume that R is subdirect and the projections are SI algebras ("multisorted" compact representations)
- if all SI factors of $\mathbf{A}$ are simple, then $\mathbf{A}$ is polynomially evaluable
- we do not know how to "climb up the congruence lattice"

Some (useful??) observations

- SMP($\mathbf{A}$) is equivalent to the following problem: given generators of $R \leq \mathbf{A}^n$ and $a, b \in A$, decide if the fork (a, b) at the n-th coordinate is witnessed in R (no need to produce the witnessing tuples)
- we can assume that R is subdirect and the projections are SI algebras ("multisorted" compact representations)
- if all SI factors of $\mathbf{A}$ are simple, then $\mathbf{A}$ is polynomially evaluable
- we do not know how to "climb up the congruence lattice"

theorem

All 3-element Maltsev algebras are polynomially evaluable.

Our proof uses ideas from Bulatov: "Three-element Mal'tsev algebras" and a particular trick:

Let $\mathbf{A} = (\{0,1,2\}; \mathcal{F})$ and $\alpha = \{0 \mid 1,2\} \in \mathrm{Con}(\mathbf{A})$.

For every $f \in \mathcal{F}$ (say n-ary) and $S \subseteq \{1,\ldots,n\}$ let f_S be the operation obtained from f by plugging 0's in coordinates from S, eg. for $n = 7$ and $S = \{2,5,6,7\}$:

$$f_S(x,y,z) = f(x,0,y,z,0,0,0).$$

Then we can reduce SMP($\mathbf{A}$) to SMP($\mathbf{B}$), where

$$\mathbf{B} = (\{1,2\}; \{f_S \mid \{1,2\} \text{ is closed under } f_S\}).$$

theorem

All 3-element Maltsev algebras are polynomially evaluable.

Our proof uses ideas from Bulatov: "Three-element Mal'tsev algebras" and a particular trick:

Let $\mathbf{A} = (\{0,1,2\}; \mathcal{F})$ and $\alpha = \{0 \mid 1,2\} \in \mathrm{Con}(\mathbf{A})$.

For every $f \in \mathcal{F}$ (say n-ary) and $S \subseteq \{1,\ldots,n\}$ let f_S be the operation obtained from f by plugging 0's in coordinates from S, eg. for $n = 7$ and $S = \{2,5,6,7\}$:

$$f_S(x,y,z) = f(x,0,y,z,0,0,0).$$

Then we can reduce SMP($\mathbf{A}$) to SMP($\mathbf{B}$), where

$$\mathbf{B} = (\{1,2\}; \{f_S \mid \{1,2\} \text{ is closed under } f_S\}).$$

theorem

All 3-element Maltsev algebras are polynomially evaluable.

Our proof uses ideas from Bulatov: "Three-element Mal'tsev algebras" and a particular trick:

Let $\mathbf{A} = (\{0,1,2\}; \mathcal{F})$ and $\alpha = \{0 \mid 1,2\} \in \mathrm{Con}(\mathbf{A})$.

For every $f \in \mathcal{F}$ (say n-ary) and $S \subseteq \{1,\ldots,n\}$ let f_S be the operation obtained from f by plugging 0's in coordinates from S, eg. for $n = 7$ and $S = \{2,5,6,7\}$:

$$f_S(x,y,z) = f(x,0,y,z,0,0,0).$$

Then we can reduce SMP($\mathbf{A}$) to SMP($\mathbf{B}$), where

$$\mathbf{B} = (\{1,2\}; \{f_S \mid \{1,2\} \text{ is closed under } f_S\}).$$

theorem

All 3-element Maltsev algebras are polynomially evaluable.

Our proof uses ideas from Bulatov: "Three-element Mal'tsev algebras" and a particular trick:

Let $\mathbf{A} = (\{0,1,2\}; \mathcal{F})$ and $\alpha = \{0 \mid 1,2\} \in \mathrm{Con}(\mathbf{A})$.

For every $f \in \mathcal{F}$ (say n-ary) and $S \subseteq \{1,\ldots,n\}$ let f_S be the operation obtained from f by plugging 0's in coordinates from S, eg. for $n = 7$ and $S = \{2,5,6,7\}$:

$$f_S(x,y,z) = f(x,0,y,z,0,0,0).$$

Then we can reduce SMP($\mathbf{A}$) to SMP($\mathbf{B}$), where

$$\mathbf{B} = (\{1,2\}; \{f_S \mid \{1,2\} \text{ is closed under } f_S\}).$$

theorem

All 3-element Maltsev algebras are polynomially evaluable.

Our proof uses ideas from Bulatov: "Three-element Mal'tsev algebras" and a particular trick:

Let $\mathbf{A} = (\{0,1,2\}; \mathcal{F})$ and $\alpha = \{0 \mid 1,2\} \in \mathrm{Con}(\mathbf{A})$.

For every $f \in \mathcal{F}$ (say n-ary) and $S \subseteq \{1,\ldots,n\}$ let f_S be the operation obtained from f by plugging 0's in coordinates from S, eg. for $n = 7$ and $S = \{2,5,6,7\}$:

$$f_S(x,y,z) = f(x,0,y,z,0,0,0).$$

Then we can reduce SMP($\mathbf{A}$) to SMP($\mathbf{B}$), where

$$\mathbf{B} = (\{1,2\}; \{f_S \mid \{1,2\} \text{ is closed under } f_S\}).$$

An open loop

Complexity of SMP is widely open even for loops.
Is the following 2-nilpotent loop polynomially evaluable?

$*$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	1	4	3	6	5
3	3	4	5	6	1	2
4	4	3	6	5	2	1
5	5	6	2	1	3	4
6	6	5	1	2	4	3

An open loop

Complexity of SMP is widely open even for loops.
Is the following 2-nilpotent loop polynomially evaluable?

$*$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	1	4	3	6	5
3	3	4	5	6	1	2
4	4	3	6	5	2	1
5	5	6	2	1	3	4
6	6	5	1	2	4	3

An abelian extension of $\mathbb{Z}_2$ by $\mathbb{Z}_3$ over a loop cocycle.

An open loop

Complexity of SMP is widely open even for loops.
Is the following 2-nilpotent loop polynomially evaluable?

$+$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$	$(0,2)$	$(1,2)$
$(0,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$	$(0,2)$	$(1,2)$
$(1,0)$	$(1,0)$	$(0,0)$	$(1,1)$	$(0,1)$	$(1,2)$	$(0,2)$
$(0,1)$	$(0,1)$	$(1,1)$	$(0,2)$	$(1,2)$	$(0,0)$	$(1,0)$
$(1,1)$	$(1,1)$	$(0,1)$	$(1,2)$	$(0,2)$	$(1,0)$	$(0,0)$
$(0,2)$	$(0,2)$	$(1,2)$	$(0+1,0)$	$(1+1,0)$	$(0,1)$	$(1,1)$
$(1,2)$	$(1,2)$	$(0,2)$	$(1+1,0)$	$(0+1,0)$	$(1,1)$	$(0,1)$

An abelian extension of $\mathbb{Z}_2$ by $\mathbb{Z}_3$ over a loop cocycle,
add $+1$ if $[x]_\alpha = 2$ and $[y]_\alpha = 1$.

A finite algebra has few subpowers if $|S(\mathbf{A}^n)| \leq 2^{p(n)}$ for some polynomial $p(x)$; equivalently, $\mathbf{A}$ has an *edge term*

- a common generalization of Maltsev and NU
- (Barto '12) few subpowers = fin. related + congr. modular
- compact representations: witness forks and projections to small ($<$ arity of the edge term) subsets of coordinates
- SMP is in NP (similar argument as in the Maltsev case)

Problem (Idziak, Marković, McKenzie, Valeriote, Willard '10)

Are all algebras with few subpowers polynomially evaluable?

Thank you for your attention!