The Subpower Membership Problem for 2-Nilpotent Mal'cev Algebras

Patrick Wynne

University of Colorado Boulder

BLAST 2025

May 21, 2025

The Subpower Membership Problem

$\mathbb{A} = (A, f_1, \ldots, f_n)$ with $|A|$ finite and $f_i \colon A^{k_i} \to A$ basic operations.

A term function of $\mathbb{A}$ is a finitary function on A built from composition of basic operations of $\mathbb{A}$ (and projections).

$\mathrm{Clo}(\mathbb{A})$ is the set of term functions of $\mathbb{A}$.

Problem: Given a *partial function*

$$p \colon A^k \to A,$$

determine if p can be interpolated by a k-ary term function of $\mathbb{A}$.

An equivalent formulation:

Problem: Given $a_1, \ldots, a_k \in A^n$ and $b \in A^n$ determine if

$$b \in \langle a_1, \ldots, a_k \rangle_{\mathbb{A}^n}.$$

The Subpower Membership Problem

SMP$(\mathbb{A})$:

Input: $a_1, \ldots, a_k, b \in A^n$.

Problem: Decide if b is in the subalgebra of $\mathbb{A}^n$ generated by $a_1, \ldots, a_k$.

$$t \begin{pmatrix} a_{11} & \ldots & a_{k1} \\ \vdots & \ddots & \vdots \\ a_{1n} & \ldots & a_{kn} \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$

A solution: Enumerate all elements of $\langle a_1, \ldots, a_k \rangle_{\mathbb{A}^n}$
and determine if b is among them.

Theorem (Kozik)

There exists a finite algebra $\mathbb{A}$ of finite type such that SMP$(\mathbb{A})$ is EXPTIME-complete.

Tractable SMP

Let p be a prime and let $\mathbb{A} = (\mathbb{Z}_p, +)$.
On input $a_1, \ldots, a_k, b \in \mathbb{Z}_p^n$, the Subpower Membership Problem asks:
Does there exist $(x_1, \ldots, x_k) \in \mathbb{Z}_p^k$ such that

$$\begin{pmatrix} a_{11} & \ldots & a_{k1} \\ \vdots & \ddots & \vdots \\ a_{1n} & \ldots & a_{kn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}?$$

So we can decide SMP($\mathbb{A}$) via **Gaussian Elimination**.
This can be done in polynomial time in the input size.

Theorem (Sims)

The subgroup membership problem is solvable in polynomial time.

Theorem (Willard)

If $\mathbb{A}$ is a finite group, ring, module then SMP($\mathbb{A}$) $\in$ P.

Mal'cev Algebras

An algebra $\mathbb{A}$ is called *Mal'cev* if there is a ternary term m of $\mathbb{A}$ such that

$$m(x, x, y) = y = m(y, x, x)$$

for all $x, y \in A$.
Ex: Groups (and their expansions) are Mal'cev algebras with Mal'cev term

$$m(x, y, z) = xy^{-1}z.$$

Question (Willard)

Is $\mathrm{SMP}(\mathbb{A}) \in \mathrm{P}$ for every finite Mal'cev algebra $\mathbb{A}$?

Theorem (Mayr)

$\mathrm{SMP}(\mathbb{A}) \in \mathrm{NP}$ for every finite Mal'cev algebra $\mathbb{A}$.

Abelian Mal'cev Algebras

For Mal'cev algebras we generalize the commutator from groups to a binary operator on the congruence lattice of $\mathbb{A}$.

$$[\_\_, \_\_]\colon \mathrm{Con}(\mathbb{A})^2 \to \mathrm{Con}(\mathbb{A})$$

We say that $\mathbb{A}$ is abelian if $[1_\mathbb{A}, 1_\mathbb{A}] = 0_\mathbb{A}$ where $0_\mathbb{A}$ and $1_\mathbb{A}$ are the least and greatest congruences on $\mathbb{A}$, respectively.

Theorem (Herrmann)

An algebra $\mathbb{A}$ in a congruence modular variety is abelian if and only if $\mathbb{A}$ is *polynomially equivalent* to a module over a ring.

Nilpotent Mal'cev Algebras

A Mal'cev algebra is 2-step nilpotent if

$$[1_{\mathbb{A}}, [1_{\mathbb{A}}, 1_{\mathbb{A}}]] = 0_{\mathbb{A}}$$

and *k*-step nilpotent if

$$[1_{\mathbb{A}}, [1_{\mathbb{A}}, \ldots, [1_{\mathbb{A}}, 1_{\mathbb{A}}] \ldots]] = 0_{\mathbb{A}}$$

where $0_{\mathbb{A}}$ and $1_{\mathbb{A}}$ are the least and greatest congruences on $\mathbb{A}$, respectively.

Theorem (Freese & McKenzie)

A Mal'cev algebra $\mathbb{A}$ is 2-nilpotent if and only if $\mathbb{A} \cong \mathbb{L} \otimes \mathbb{U}$ for abelian Mal'cev algebras $\mathbb{L}$ and $\mathbb{U}$.

Theorem (Freese & McKenzie)

A Mal'cev algebra $\mathbb{A}$ is 2-nilpotent if and only if $\mathbb{A} \cong \mathbb{L} \otimes \mathbb{U}$ for abelian Mal'cev algebras $\mathbb{L}$ and $\mathbb{U}$.

$\mathbb{L} \otimes \mathbb{U}$ is an algebra with universe $L \times U$ and basic operations

$$f^{\mathbb{L}\otimes\mathbb{U}}((\ell_1, u_1), \ldots, (\ell_k, u_k)) \\ = (f^{\mathbb{L}}(\ell_1, \ldots, \ell_k) + \hat{f}(u_1, \ldots, u_k), f^{\mathbb{U}}(u_1, \ldots, u_k))$$

where $\hat{f} : U^k \to L$.

We call $\mathbb{L} \otimes \mathbb{U}$ a central extension of $\mathbb{L}$ by $\mathbb{U}$.

Theorem (Mayr)

If $\mathbb{A}$ is a finite nilpotent Mal'cev algebra **and** $\mathbb{A}$ factors into the product of nilpotent algebras of prime power order then $\mathrm{SMP}(\mathbb{A}) \in \mathrm{P}$.

Unlike for finite nilpotent groups, some finite nilpotent Mal'cev algebras do not factor into the product of nilpotent algebras of prime power order.

Clonoids

Clonoid

For $C \subseteq \bigcup_{n \in \mathbb{N}} L^{U^n}$ we say that C is a **clonoid** from $\mathbb{U}$ to $\mathbb{L}$ if

$$C \circ \mathrm{Clo}(\mathbb{U}) \subseteq C \qquad \& \qquad \mathrm{Clo}(\mathbb{L}) \circ C \subseteq C$$

- C is closed under precomposition with term functions of $\mathbb{U}$, and
- C is closed under postcomposition with term functions of $\mathbb{L}$.

Example: $\mathbb{U} = (\mathbb{Z}_3, +, -, 0)$, $\mathbb{L} = (\{0,1\}, \wedge, \vee)$, C clonoid from $\mathbb{U}$ to $\mathbb{L}$.

If $f : U^2 \to L$ is in C then

$$f(x_1 + x_2, 0) \in C \text{ and } f(2x_1, x_1 - x_2 + x_3) \in C,$$

and so $g(x_1, x_2, x_3) = f(x_1 + x_2, 0) \wedge f(2x_1, x_1 - x_2 + x_3) \in C.$

Generation of Clonoids

Theorem (Mayr, W.)

Let $\mathbb{U}$ and $\mathbb{L}$ be finite abelian Mal'cev algebras of coprime order.
Suppose $\mathbb{U}$ is the direct product of pairwise non-isomorphic simple abelian Mal'cev algebras.
Every clonoid from $\mathbb{U}$ to $\mathbb{L}$ is uniformly generated by its binary functions.

$\mathbb{U}$ is (polynomially equivalent to) an **R**-module.
$\mathbb{L}$ is (polynomially equivalent to) an **S**-module.

There exists $s\colon R^{k\times k} \to S$ such that for all $f\colon U^k \to L$

$$f(x) \quad = \sum_{r\in R^{k\times k}, \mathrm{rank}(r)\leq 2} s(r) f(rx).$$

Let $\Delta := \{(z, \dots, z) \in U^k \ : \ z \in U\}$ and

$$V := \{N \leq \mathbb{U}^k \ : \ \Delta \leq N,\ N \cong \mathbb{U}^2\}.$$

Then for each $N \in V$ and for each $f \colon U^k \to L$ the functions

$$f'(x_1, \dots, x_k) := f(x_1, \dots, x_k) - f(x_k, \dots, x_k)$$
$$f'_N(x_1, \dots, x_k) := \begin{cases} f'(x_1, \dots, x_k) & \text{if } (x_1, \dots, x_k) \in N \\ 0 & \text{else,} \end{cases}$$

are $\mathbb{U}, \mathbb{L}$-minors of f, and

$$f(x_1, \dots, x_k) = f(x_k, \dots, x_k) + \sum_{N \in V} f'_N(x_1, \dots, x_k).$$

Compact Representations

Let $\mathbb{A}$ be a finite Mal'cev algebra and $R \subseteq \mathbb{A}^n$.

Define $\mathrm{Sig}(R)$ as the set of triples $(i, a, b) \in \{1, 2, \ldots, n\} \times A^2$ such that

- there exist $t_a, t_b \in R$ with $t_a(j) = t_b(j)$ for all $j < i$,
- and $t_a(i) = a$, $t_b(i) = b$.

If $S \subset R$ and $\mathrm{Sig}(S) = \mathrm{Sig}(R)$ we say S is a representation of R.
If moreover $|S| \leq 2|\mathrm{Sig}(R)|$ we say S is a compact representation of R.

Note: Every $R \subset \mathbb{A}^n$ has a compact representation S.
For each $(i, a, b) \in \mathrm{Sig}(R)$ include in S two tuples t_a and t_b witnessing this.

Theorem (Bulatov & Dalmau)

For $\mathbb{A}$ Mal'cev, $\mathrm{SMP}(\mathbb{A})$ is polynomial time reducible to $\mathrm{CompRep}(\mathbb{A})$.

Difference Clonoid

We decompose the term functions of $\mathbb{A} = \mathbb{L} \otimes \mathbb{U}$ using a clonoid.

Difference Clonoid

$$D(\mathbb{L} \otimes \mathbb{U}) := \{e \colon U^k \to L \ : \ e = s^{\mathbb{L} \otimes \mathbb{U}} - t^{\mathbb{L} \otimes \mathbb{U}} \text{ for } s^{\mathbb{L} \times \mathbb{U}} = t^{\mathbb{L} \times \mathbb{U}}\}.$$

- $D(\mathbb{L} \otimes \mathbb{U})$ is a clonoid from $\mathbb{U}$ to $(L, +, -, 0)$.
- $t + e = (t^{\mathbb{L}} + \hat{t} + e, t^{\mathbb{U}}) \in \mathrm{Clo}(\mathbb{L} \otimes \mathbb{U})$
for all $t \in \mathrm{Clo}(\mathbb{L} \otimes \mathbb{U})$ and $e \in D(\mathbb{L} \otimes \mathbb{U})$.

Understand $\mathbb{L} \otimes \mathbb{U}$ by understanding $\mathbb{L}$, $\mathbb{U}$, and $D(\mathbb{L} \otimes \mathbb{U})$.

Compact Representations for Clonoids

Let $\mathbb{U}$ and $\mathbb{L}$ be finite Mal'cev algebras and C a clonoid from $\mathbb{U}$ to $\mathbb{L}$.

CompRep(C) :

Input: $a_1, \ldots, a_k \in U^n$.

Output: A compact representation of

$$C(a_1, \ldots, a_k) := \{f(a_1, \ldots, a_k) \ : \ f \in C^{(k)}\} \leq \mathbb{L}^n.$$

Theorem (Kompatscher)

Let $\mathbb{A} = \mathbb{L} \otimes \mathbb{U}$ be a finite Mal'cev algebra such that $\mathbb{U}$ is supernilpotent. Then SMP($\mathbb{A}$) reduces in polynomial time to CompRep($D(\mathbb{L} \otimes \mathbb{U})$).

So to solve SMP($\mathbb{L} \otimes \mathbb{U}$) efficiently it suffices to efficiently compute a compact representation for the difference clonoid.

Lemma

Let $\mathbb{U}$ and $\mathbb{L}$ be finite abelian Mal'cev algebras of coprime order such that $\mathbb{U}$ is a product of simple abelian Mal'cev algebras.
Let C be a clonoid from $\mathbb{U}$ to $\mathbb{L}$.
Given $a_1, \dots, a_k \in U^n$, we can compute a set of generators for

$$C^{(k)}(a_1, \dots, a_k) := \{f(a_1, \dots, a_k) \ : \ f \in C^{(k)}\} \leq \mathbb{L}^n$$

in time polynomial in n and k.

Proof idea: Let $\mathbb{U} = (\mathbb{Z}_p, +)$.

For each $f \in C^{(k)}$ we need to compute $f \begin{pmatrix} a_{11} & \dots & a_{k1} \\ \vdots & \ddots & \vdots \\ a_{1n} & \dots & a_{kn} \end{pmatrix}$.

Each $f \in C^{(k)}$ can be decomposed as

$$f(x_1, \dots, x_k) = f(x_k, \dots, x_k) + \sum_{\Delta \leq N \leq \mathbb{A}^k, N \cong \mathbb{A}^2} f'_N(x_1, \dots, x_k).$$

Each f'_N has support N (a dimension 2 subspace of $\mathbb{A}^n$).

$q_N \colon A^2 \to N$ parameterizes N by $\mathbb{A}^2$ via term functions.

$g_N := f' \circ q_N \in C^{(2)}$ and $g_N \circ q_N^{-1} = f'_N|_N$.

So instead of computing $f'_N(a_{1j}, \dots, a_{kj})$ we can compute $gq_N^{-1}(a_{1j}, \dots, a_{kj})$ for $g \in C^{(2)}$.

Each non-constant $(a_{1j}, \dots, a_{kj})$ is contained in exactly one N so we need only compute (at most) n many q_N^{-1}.

$|C^{(2)}| \leq |B|^{|A|^2}$ is independent of n and k (the input size).

So generators for $C^{(k)}(a_1, \dots, a_k)$ can be computed in polynomial time. $\square$

From this generating set we can compute a compact representation of $C^{(k)}(a_1, \dots, a_k)$ in polynomial time.

Hence ...

Tractable Subpower Membership Problem

Theorem (W.)

If $\mathbb{A}$ is a 2-nilpotent Mal'cev algebra of squarefree order then $\mathrm{SMP}(\mathbb{A}) \in \mathrm{P}$.

Proof: $\mathbb{A} = \mathbb{L} \otimes \mathbb{U}$ for abelian Mal'cev algebras $\mathbb{L}$ and $\mathbb{U}$.
$|A|$ squarefree implies $|L|$ and $|U|$ are squarefree and coprime.
$\mathbb{U}$ abelian implies $\mathbb{U}$ is a product of abelian algebras of prime order.
$\mathrm{CompRep}(D(\mathbb{L} \otimes \mathbb{U}))$ has a polynomial time algorithm.
By Kompatscher's reduction, $\mathrm{SMP}(\mathbb{A})$ has a polynomial time algorithm.
More generallly,

Theorem (W.)

Let $\mathbb{A} = \mathbb{L} \otimes \mathbb{U}$ be a finite 2-nilpotent Mal'cev algebra of finite type such that $|L|$ and $|U|$ are relatively prime. Further assume that $\mathbb{U}$ is the direct product of pairwise non-isomorphic simple abelian Mal'cev algebras.
Then $\mathrm{SMP}(\mathbb{A}) \in \mathrm{P}$.

Questions

Q: Does every finite 2-nilpotent Mal'cev algebra have tractable SMP?

What if $\mathbb{A} = \mathbb{L} \otimes \mathbb{U}$ and $D(\mathbb{L} \otimes \mathbb{U})$ is uniformly generated?

Q: Does every finite Mal'cev algebra have tractable SMP?

Thank you!

- Clonoid results $\rightarrow$ Mayr & Wynne: "Clonoids between modules"
- SMP results $\rightarrow$ Wynne: "Clonoids and Nilpotent Mal'cev Algebras"