The Subpower Membership Problem via Clonoids

Patrick Wynne
Joint work with Stefano Fioravanti and Michael Kompatscher

TU Wien
AAA 108

February 7, 2026

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.

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.

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.

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

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

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

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

An equivalent formulation:

Problem: Given a *partial function*

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

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

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 $a_1, \ldots, a_k$.

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

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.

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

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

Tractable SMP

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.

Tractable SMP

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.

Tractable SMP

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

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 $x, y \in A$.

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

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

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 $\mathbb{A}$?

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 $\mathbb{A}$.

Nilpotent Mal'cev Algebras

A Mal'cev algebra is 2-step nilpotent if

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

Nilpotent Mal'cev Algebras

A Mal'cev algebra is 2-step nilpotent if

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

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

Nilpotent Mal'cev Algebras

A Mal'cev algebra is 2-step nilpotent if

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

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 $\mathbb{A} \cong \mathbb{U} \otimes \mathbb{L}$ for abelian Mal'cev algebras $\mathbb{U}$ and $\mathbb{L}$.

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

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

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

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

A finite nilpotent Mal'cev algebra $\mathbb{A}$ is *supernilpotent* if $\mathbb{A}$ splits into the direct product of algebras of prime power order.

A finite nilpotent Mal'cev algebra $\mathbb{A}$ is *supernilpotent* if $\mathbb{A}$ splits into the direct product of algebras of prime power order.

Groups: nilpotent implies supernilpotent.
In general, no.

A finite nilpotent Mal'cev algebra $\mathbb{A}$ is *supernilpotent* if $\mathbb{A}$ splits into the direct product of algebras of prime power order.

Groups: nilpotent implies supernilpotent.
In general, no.

Theorem (Mayr)

If $\mathbb{A}$ is a finite supernilpotent Mal'cev algebra then $\mathrm{SMP}(\mathbb{A}) \in \mathrm{P}$.

What to do when $\mathbb{A}$ is not supernilotent?

Clonoids

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 $\mathbb{L}$.

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 $\mathbb{L}$.

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

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

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

Difference Clonoid

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

Difference Clonoid

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

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

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

SMP for Clonoids

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

SMP(C) :

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

Output: A polynomial size generating set of

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

SMP for Clonoids

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

SMP(C) :

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

Output: A polynomial size generating set of

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

Theorem (Kompatscher)

Let $\mathbb{U} \otimes \mathbb{L}$ be a finite 2-nilpotent Mal'cev algebra. Then SMP($\mathbb{U} \otimes \mathbb{L}$) reduces in polynomial time to SMP($\mathbb{U} \times \mathbb{L}$) and SMP($D(\mathbb{U} \otimes \mathbb{L})$).

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

SMP(C) :

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

Output: A polynomial size generating set of

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

Theorem (Kompatscher)

Let $\mathbb{U} \otimes \mathbb{L}$ be a finite 2-nilpotent Mal'cev algebra. Then SMP($\mathbb{U} \otimes \mathbb{L}$) reduces in polynomial time to SMP($\mathbb{U} \times \mathbb{L}$) and SMP($D(\mathbb{U} \otimes \mathbb{L})$).

Since $\mathbb{U}$ and $\mathbb{L}$ are abelian, SMP($\mathbb{U} \times \mathbb{L}$) $\in$ P.

Theorem

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

Theorem

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

Proof idea: For $\mathbb{A} = \mathbb{U} \times \mathbb{L}$ show that for $a_1, \ldots, a_k \in U^m$ we can compute a generating set of

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

in time polynomial in m and k.

Theorem

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

Proof idea: For $\mathbb{A} = \mathbb{U} \times \mathbb{L}$ show that for $a_1, \ldots, a_k \in U^m$ we can compute a generating set of

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

in time polynomial in m and k.
Let C satisfy $f(0, \ldots, 0) = 0$ for all $f \in C$.
For $g \in C^{(1)}$ and for $c \in U^k \setminus 0$ there is a function $g^c \in C^{(k)}$ with

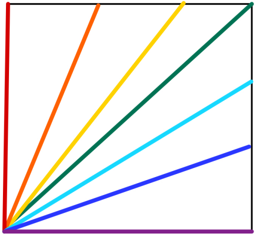
$$g^c(x) = \begin{cases} g(y) & \text{if } x = yc, \\ 0 & \text{else.} \end{cases}$$

Example: For $c = (1, 0)$ and $g \in C^{(1)}$ we have

$$g^c(x_1, x_2) = \sum_{a \in \mathbb{Z}_p} g(x_1 + a x_2) - g(a x_2).$$

Let $\Omega \subset U^k \setminus 0$ such that $\langle c \rangle \cap \langle d \rangle = 0$ for $c \neq d \in \Omega$.

$$f = \sum_{g \in C^{(1)}, c \in \Omega} g^c.$$



Instead of

$$f \begin{pmatrix} a_{11} & \dots & a_{k1} \\ \vdots & \ddots & \vdots \\ a_{1n} & \dots & a_{kn} \end{pmatrix}$$

compute

$$g^c \begin{pmatrix} a_{11} & \dots & a_{k1} \\ \vdots & \ddots & \vdots \\ a_{1n} & \dots & a_{kn} \end{pmatrix}$$

for linearly many c's.

Goal

Let $\mathbb{U} = (\mathbb{Z}_{p^n}, +)$ and $\mathbb{L}$ be a coprime abelian Mal'cev algebra.
Then $\mathrm{SMP}(\mathbb{U} \otimes \mathbb{L}) \in \mathrm{P}$.

Goal

Let $\mathbb{U} = (\mathbb{Z}_{p^n}, +)$ and $\mathbb{L}$ be a coprime abelian Mal'cev algebra.
Then $\mathrm{SMP}(\mathbb{U} \otimes \mathbb{L}) \in \mathrm{P}$.

Main step: Let $C = D(\mathbb{U} \otimes \mathbb{L})$.
Given $a_1, \ldots, a_k \in U^m$, we can compute a set of generators for

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

in time polynomial in n and k.

Goal

Let $\mathbb{U} = (\mathbb{Z}_{p^n}, +)$ and $\mathbb{L}$ be a coprime abelian Mal'cev algebra.
Then $\mathrm{SMP}(\mathbb{U} \otimes \mathbb{L}) \in \mathrm{P}$.

Main step: Let $C = D(\mathbb{U} \otimes \mathbb{L})$.
Given $a_1, \ldots, a_k \in U^m$, we can compute a set of generators for

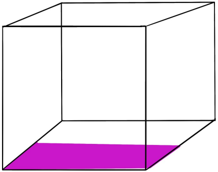
$$C^{(k)}(a_1, \ldots, a_k) := \{f(a_1, \ldots, a_k) \ : \ f \in C^{(k)}\} \leq \mathbb{L}^m$$

in time polynomial in n and k.

With~~out~~ loss of generality,

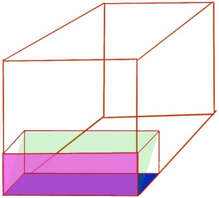
$$f(pA, \ldots, pA) = 0 \text{ for all } f \in C.$$

Interpolate f on "slices" isomorphic to $A \times pA \times p^2A \times \cdots \times p^{n-1}A$.

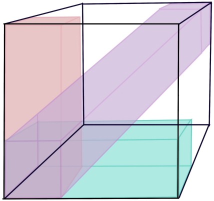


For $g \in C^{(n)}$ there exists $f \in C^{(k)}$ with

$$f(x) = \begin{cases} g(x_1, \ldots, x_n) & \text{if } x_i \in p^{i-1}A \text{ for } i \leq k, \\ 0 & \text{else.} \end{cases}$$



Next, cover $A \times pA \times \ldots pA$ with such slices.



Finally cover A^k with blocks isomorphic to

$$A \times pA \times \cdots \times pA.$$

Each "slice" is parametrized by $c = (c_1, \dots, c_n) \in (A^k)^n$.
Let Ω be a collection of all such slices. For $g \in C^{(n)}$ and $c \in \Omega$ we have

$$g^c(x) = \begin{cases} g(y_1, \dots, y_n) & \text{if } x = y_1 c_1 + \dots + y_n c_n \text{ and } y_i \in p^{i-1}A \\ 0 & \text{else.} \end{cases}$$

For all $f \in C^{(k)}$,

$$f = \sum_{g \in C^{(n)}, c \in \Omega} g^c.$$

Instead of

$$f \begin{pmatrix} a_{11} & \dots & a_{k1} \\ \vdots & \ddots & \vdots \\ a_{1n} & \dots & a_{kn} \end{pmatrix}$$

compute

$$g^c \begin{pmatrix} a_{11} & \dots & a_{k1} \\ \vdots & \ddots & \vdots \\ a_{1n} & \dots & a_{kn} \end{pmatrix}$$

for linearly many c's.

Tractable Subpower Membership Problem

Goal:

Let $\mathbb{U} = (\mathbb{Z}_{p^n}, +)$ and $\mathbb{L}$ a coprime module. Then $\mathrm{SMP}(\mathbb{U} \otimes \mathbb{L}) \in \mathrm{P}$.

Tractable Subpower Membership Problem

Goal:

Let $\mathbb{U} = (\mathbb{Z}_{p^n}, +)$ and $\mathbb{L}$ a coprime module. Then $\mathsf{SMP}(\mathbb{U} \otimes \mathbb{L}) \in \mathsf{P}$.

Still to do: Reduce to $D(\mathbb{U} \otimes \mathbb{L}) \subseteq \mathrm{Pol}(pA, 0)$.
For $n = 1, 2$ done.
For $n > 2$ ... plan for next week.

Tractable Subpower Membership Problem

Goal:

Let $\mathbb{U} = (\mathbb{Z}_{p^n}, +)$ and $\mathbb{L}$ a coprime module. Then $\mathrm{SMP}(\mathbb{U} \otimes \mathbb{L}) \in \mathrm{P}$.

Still to do: Reduce to $D(\mathbb{U} \otimes \mathbb{L}) \subseteq \mathrm{Pol}(pA, 0)$.
For $n = 1, 2$ done.
For $n > 2$ ... plan for next week.

Conjecture

Let $\mathbb{U} \otimes \mathbb{L}$ be a finite 2-nilpotent Mal'cev algebra. Then $\mathrm{SMP}(\mathbb{U} \otimes \mathbb{L}) \in \mathrm{P}$.

Still to do: Study clonoids between abelian algebras in remaining cases.

- Are they finitely generated?
- Can we use the interpolation arguments to solve SMP like here?

Questions

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

Questions

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

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

Questions

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

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

- What about 2-nilpotent?

Questions

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

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

- What about 2-nilpotent?
- What if $D(\mathbb{U} \otimes \mathbb{L})$ is uniformly generated?

Thank you!