The subpower membership problem of 2-nilpotent algebras

Michael Kompatscher
Charles University Prague

12.03.2024

STACS 24 - Clermont-Ferrand

The Subpower Membership Problem

$\underline{A} = (A, f_1, \dots, f_\ell)$ ... finite algebra

SMP($\underline{A}$)

Input: partial operation $A^n \to A$

$$t: \bar{a}_1, \bar{a}_2, \dots, \bar{a}_n \mapsto \bar{b} \in A^k$$

$$\begin{array}{ccccccc} \| & & \| & & \| & & \| \\ \boxed{\begin{array}{c} a_{11} \\ a_{12} \\ \vdots \\ a_{1k} \end{array}} & & \boxed{\begin{array}{c} a_{21} \\ a_{22} \\ \vdots \\ a_{2k} \end{array}} & \begin{array}{c} \dots \\ \dots \\ \\ \dots \end{array} & \boxed{\begin{array}{c} a_{n1} \\ a_{n2} \\ \vdots \\ a_{nk} \end{array}} & \begin{array}{c} \mapsto \\ \mapsto \\ \\ \mapsto \end{array} & \boxed{\begin{array}{c} b_1 \\ b_2 \\ \vdots \\ b_n \end{array}} \end{array}$$

Question: Is there a term of $\underline{A}$ interpolating t?

$\iff$ Is $\bar{b} \in \langle \bar{a}_1, \bar{a}_2, \dots, \bar{a}_n \rangle \leq \underline{A}^k$?

The Subpower Membership Problem

$\underline{A} = (A, f_1, \ldots, f_\ell)$ ... finite algebra

SMP($\underline{A}$)

Input: partial operation $A^n \to A$

$$t: \bar{a}_1, \bar{a}_2, \ldots, \bar{a}_n \mapsto \bar{b} \in A^k$$

$$\begin{array}{ccccccc} \| & & \| & & \| & & \| \\ \boxed{\begin{array}{c} a_{11} \\ a_{12} \\ \vdots \\ a_{1k} \end{array}} & & \boxed{\begin{array}{c} a_{21} \\ a_{22} \\ \vdots \\ a_{2k} \end{array}} & \begin{array}{c} \cdots \\ \cdots \\ \\ \cdots \end{array} & \boxed{\begin{array}{c} a_{n1} \\ a_{n2} \\ \vdots \\ a_{nk} \end{array}} & \begin{array}{c} \mapsto \\ \mapsto \\ \\ \mapsto \end{array} & \boxed{\begin{array}{c} b_1 \\ b_2 \\ \vdots \\ b_n \end{array}} \end{array}$$

$\mathrm{Clo}\,\underline{A} :\Leftrightarrow$ all term operations of $\underline{A}$.

Question: Is there a term of $\underline{A}$ interpolating t?

$$\Leftrightarrow \text{ Is } \bar{b} \in \langle \bar{a}_1, \bar{a}_2, \ldots, \bar{a}_n \rangle \leq \underline{A}^k \,?$$

Examples

- $\underline{A} = (\mathbb{Z}_p, +, 0, -, \cdot, 1)$ Clo $\underline{A}$ ... all operations $\mathbb{Z}_p^n \to \mathbb{Z}_p$
  $\Rightarrow \mathrm{SMP}(\underline{A}) \in P$ (Lagrange interpolation)
- $\underline{A} = (\mathbb{Z}_p, +, 0, -)$ Clo $\underline{A}$ ... all linear maps $\mathbb{Z}_p^n \to \mathbb{Z}_p$
  $\Rightarrow \mathrm{SMP}(\underline{A}) \in P$ (Gauss elimination)
- $\underline{A} = (\{0,1\}, \wedge, \vee, 0, 1)$ Clo $\underline{A}$ ... all monotone maps $\{0,1\}^n \to \{0,1\}$
  $\Rightarrow \mathrm{SMP}(\underline{A}) \in P$ (is input monotone?)

Examples

- $\underline{A} = (\mathbb{Z}_p, +, 0, -, \cdot, 1)$ Clo $\underline{A}$ ... all operations $\mathbb{Z}_p^n \to \mathbb{Z}_p$
  $\Rightarrow \mathrm{SMP}(\underline{A}) \in P$ (Lagrange interpolation)
- $\underline{A} = (\mathbb{Z}_p, +, 0, -)$ Clo $\underline{A}$ ... all linear maps $\mathbb{Z}_p^n \to \mathbb{Z}_p$
  $\Rightarrow \mathrm{SMP}(\underline{A}) \in P$ (Gauss elimination)
- $\underline{A} = (\{0,1\}, \wedge, \vee, 0, 1)$ Clo $\underline{A}$ ... all monotone maps $\{0,1\}^n \to \{0,1\}$
  $\Rightarrow \mathrm{SMP}(\underline{A}) \in P$ (is input monotone?)

SMP in P for
- comm. rings with 1 [BH '17]
- groups [Schreier-Sims '70]
- lattices [folklore]

A tractability conjecture

- $\forall \underline{A}$: $SMP(\underline{A}) \in$ EXPTIME
- $\exists \underline{A}$: $SMP(\underline{A}) \in$ EXPTIME-complete [Kozik'08]
- $\exists \underline{A}$ semigroup: $SMP(\underline{A}) \in$ PSPACE-complete [BKMS'16]

A tractability conjecture

- $\forall \underline{A}$: $SMP(\underline{A}) \in EXPTIME$
- $\exists \underline{A}$: $SMP(\underline{A}) \in EXPTIME$-complete [Kozik'08]
- $\exists \underline{A}$ semigroup: $SMP(\underline{A}) \in PSPACE$-complete [BKMS'16]

$\underline{A}$ has few subpowers $:\Leftrightarrow \exists$ polynomial p:

$$|\{R \leq \underline{A}^n\}| \leq 2^{p(n)}$$

Question [IMMVW'10]

Does few subpowers $\Rightarrow SMP \in P$? (would generalize previous slide!)

we know $\Rightarrow$ $SMP \in NP$ [BMS'19]

(by existence of „canonical" generating sets)

Mal'tsev algebras

$m(x\,y\,z) \in \mathrm{Clo}(\underline{A})$ is a Mal'tsev term

$:\Leftrightarrow \forall x\,y: \; m(y\,x\,x) = m(x\,x\,y) = y$

E.g.

$m(x\,y\,z) = x - y + z$ in rings

$m(x\,y\,z) = x\,y^{-1} \cdot z$ in groups

Mal'tsev $\Rightarrow$ few subpowers

$\boxed{\text{Is } \mathrm{SMP}(\underline{A}) \in P \text{ for } \underline{A} \text{ Mal'tsev?}}$

Mal'tsev algebras

$m(x\,y\,z) \in Clo(\underline{A})$ is a Mal'tsev term $:\Leftrightarrow \forall x\,y: \; m(y\,x\,x) = m(x\,x\,y) = y$

E.g.

$m(x\,y\,z) = x - y + z$ in rings

$m(x\,y\,z) = x\,y^{-1}\cdot z$ in groups

Mal'tsev $\Rightarrow$ few subpowers

$\boxed{\text{Is } SMP(\underline{A}) \in P \text{ for } \underline{A} \text{ Mal'tsev?}}$

$\underline{A}$ is affine $:\Leftrightarrow$

$Clo(\underline{A}, (a)_{a\in A}) = \{ \underbrace{\sum_{i=1}^{n} r_i \cdot x_i + a}_{\text{in a module}} \}$

$SMP(\underline{A}) \in P$ if
- $\underline{A}$ affine
- $\underline{A}$ supernilpotent [M '12]
- $HSP(\underline{A})$ res. finite [BMS '19]

generalizations of affine.

How far can we push this?

Central extensions / wreath products

For $\underline{U}$ Mal'tsev, $\underline{L}$ affine, T

the wreath product $\underline{L} \otimes^T \underline{U} :=$

- Domain $L \times U$
- operations

$$f^{\underline{A}}\left(\begin{pmatrix} l_1 \\ u_1 \end{pmatrix} \dots \begin{pmatrix} l_n \\ u_n \end{pmatrix}\right) = \begin{pmatrix} f^{\underline{L}}(l_1, \dots, l_n) + \hat{f}(u_1, \dots, u_n) \\ f^{\underline{U}}(u_1, \dots, u_n) \end{pmatrix}$$

$\hat{f} : U^n \to L$

$T = (\hat{f})_{f \in F}$

„distortions"

If $\underline{U}$ affine

$\underline{A} \cong \underline{L} \otimes \underline{U}$ is

2-nilpotent

Central extensions / wreath products

For $\underline{U}$ Mal'tsev, $\underline{L}$ affine, T

the wreath product $\underline{L} \otimes^T \underline{U} :=$

-) Domain $L \times U$
-) operations

$$f^{\underline{A}}\left(\begin{pmatrix} l_1 \\ u_1 \end{pmatrix} \cdots \begin{pmatrix} l_n \\ u_n \end{pmatrix}\right) = \begin{pmatrix} f^{\underline{L}}(l_1, \dots, l_n) + \hat{f}(u_1, \dots, u_n) \\ f^{\underline{U}}(u_1, \dots, u_n) \end{pmatrix}$$

$\hat{f} : U^n \to L$

$T = (\hat{f})_{f \in F}$

„distortions"

$$\boxed{\begin{array}{l} \text{If } \underline{U} \text{ affine} \\ \underline{A} \cong \underline{L} \otimes \underline{U} \text{ is} \\ \quad \text{2-nilpotent} \end{array}}$$

Not covered by [M'12] [BMS'19]

-) Is $SMP(\underline{A}) \in P$ for $\underline{A}$ 2-nilpotent?

E.g. $\underline{A} = (\mathbb{Z}_p \times \mathbb{Z}_p, +, 0, -, f(x))$

$$f\begin{pmatrix} l \\ u \end{pmatrix} = \begin{cases} \begin{pmatrix} 1 \\ 0 \end{pmatrix} & \text{if } u = 0 \\ \begin{pmatrix} 0 \\ 0 \end{pmatrix} & \text{else} \end{cases}$$

-) Can we reduce $SMP(\underline{L} \otimes \underline{U})$ to $SMP(\underline{L} \times \underline{U}) + (?)$?

A clone homomorphism

$\underline{A} = \underline{L} \otimes \underline{U}$

Idea 1: Write $t^{A} \in \mathrm{Clo}(\underline{A})$ as "sum" of $t^{\underline{L} \times \underline{U}}$ and $\hat{t}$ [as in CEQV]

Problem: In general $\mathrm{Clo}(\underline{L} \times \underline{U}) \not\subseteq \mathrm{Clo}(\underline{L} \otimes \underline{U})$!

(e.g. dihedral group $\underline{D_4}$)

A clone homomorphism

$\underline{A} = \underline{L} \otimes \underline{U}$

Idea 1: Write $t^{\underline{A}} \in Clo(\underline{A})$ as "sum" of $t^{\underline{L}\times\underline{U}}$ and $\hat{t}$ [as in CEQV]

Problem: In general $Clo(\underline{L}\times\underline{U}) \not\subseteq Clo(\underline{L}\otimes\underline{U})$!

(e.g. dihedral group $\underline{D_4}$)

Idea 2: study map

$$\boxed{\begin{aligned} \xi : \; Clo(\underline{A}) &\longrightarrow Clo(\underline{L}\times\underline{U}) \\ t^{\underline{A}} &\longmapsto t^{\underline{L}\times\underline{U}} \end{aligned}}$$

is a clone homomorphism

(= preserves composition & π_i^n)

$$\begin{pmatrix} t^{\underline{L}}(l_1, \ldots, l_n) + \hat{t}(u_1, \ldots, u_n) \\ t^{u}(u_1, \ldots, u_n) \end{pmatrix} \longmapsto \begin{pmatrix} t^{\underline{L}}(l_1, \ldots, l_n) \\ t^{\underline{U}}(u_1, \ldots, u_n) \end{pmatrix}$$

Difference clonoids (Mayr)

Let $t^{\underline{A}}, s^{\underline{A}} \in \mathrm{Clo}(\underline{A})$: $\xi(t^{\underline{A}}) = \xi(s^{\underline{A}})$

$$t^{\underline{A}} \qquad\qquad\qquad s^{\underline{A}}$$

$$\begin{pmatrix} t^{\underline{L}}(\bar{e}) + \hat{f}(\bar{u}) \\ t^{\underline{U}}(\bar{u}) \end{pmatrix} \qquad \begin{pmatrix} t^{\underline{L}}(\bar{e}) + \hat{s}(\bar{u}) \\ t^{\underline{U}}(\bar{u}) \end{pmatrix}$$

Def The <u>difference</u> $t^{\underline{A}} - s^{\underline{A}}$ is the map $\hat{r}: U^n \to L$

$$\hat{r}(\bar{u}) = \hat{f}(\bar{u}) - \hat{s}(\bar{u})$$

Difference clonoids (Mayr)

Let $t^{\underline{A}}, s^{\underline{A}} \in \mathrm{Clo}(\underline{A})$: $\xi(t^{\underline{A}}) = \xi(s^{\underline{A}})$

$$t^{\underline{A}} \qquad\qquad\qquad\qquad s^{\underline{A}}$$

$$\begin{pmatrix} t^{\underline{L}}(\bar{e}) + \hat{t}(\bar{u}) \\ t^{\underline{U}}(\bar{u}) \end{pmatrix} \qquad \begin{pmatrix} t^{\underline{L}}(\bar{e}) + \hat{s}(\bar{u}) \\ t^{\underline{U}}(\bar{u}) \end{pmatrix}$$

Def The <u>difference</u> $t^{\underline{A}} - s^{\underline{A}}$ is the map $\hat{r}: U^n \to L$

$$\hat{r}(\bar{u}) = \hat{t}(\bar{u}) - \hat{s}(\bar{u})$$

$$\boxed{\mathrm{Diff}(\underline{A}) := \{\hat{r}: U^n \to L \mid \hat{r} = t^{\underline{A}} - s^{\underline{A}}\}}$$

... difference clonoid of $\underline{L} \otimes \underline{U}$

Difference clonoids (Mayr)

Let $t^{\underline{A}}, s^{\underline{A}} \in \mathrm{Clo}(\underline{A})$: $\xi(t^{\underline{A}}) = \xi(s^{\underline{A}})$

$$t^{\underline{A}} \qquad\qquad\qquad s^{\underline{A}}$$

$$\begin{pmatrix} t^{\underline{L}}(\bar{e}) + \hat{f}(\bar{u}) \\ t^{\underline{U}}(\bar{u}) \end{pmatrix} \quad \begin{pmatrix} t^{\underline{L}}(\bar{e}) + \hat{s}(\bar{u}) \\ t^{\underline{U}}(\bar{u}) \end{pmatrix}$$

Def The difference $t^{\underline{A}} - s^{\underline{A}}$ is the map $\hat{r}: U^n \to L$

$$\hat{r}(\bar{u}) = \hat{f}(\bar{u}) - \hat{s}(\bar{u})$$

$$\boxed{\mathrm{Diff}(\underline{A}) := \{\hat{r}: U^n \to L \mid \hat{r} = t^{\underline{A}} - s^{\underline{A}}\}}$$

difference clonoid of $\underline{L} \otimes \underline{U}$

- $\mathrm{Diff}(\underline{A})$ is a clonoid from $\underline{U}$ to $(\underline{L}, 0)$
  - closed under $\mathrm{Clo}(\underline{U})$ (from inside)
  - — " — $\mathrm{Clo}(\underline{L}, 0)$ (from outside)

SMP for clonoids

$\mathrm{SMP}(\underline{A})$

Input: $\bar a_1, \dots \bar a_n, \bar b \in A^k$

Question: $\exists t \in \mathrm{Clo}(\underline{A}) : t(\bar a_1, \dots \bar a_n) = \bar b$?

→ makes also sense for $(\underline{U}, \underline{L})$- clonoids $\mathcal{C}$:

$\mathrm{SMP}(\mathcal{C})$:

$$\exists t \in \mathcal{C} : t(\overset{\in U^k}{\bar u_1 \dots \bar u_n}) = \overset{\in L^k}{\bar l}\ ?$$

SMP for clonoids

$\mathrm{SMP}(\underline{A})$

Input: $\bar{a}_1, \dots \bar{a}_n, \bar{b} \in A^k$

Question: $\exists t \in \mathrm{Clo}(\underline{A}) : t(\bar{a}_1, \dots \bar{a}_n) = \bar{b}$?

→ makes also sense for $(\underline{U}, \underline{L})$-clonoids $\mathcal{C}$:

$\mathrm{SMP}(\mathcal{C})$:

$$\exists t \in \mathcal{C} : t(\underbrace{\bar{u}_1, \dots \bar{u}_n}_{\in U^k}) = \underbrace{\bar{\ell}}_{\in L^k}\,?$$

$\underline{A} = \underline{L} \otimes \underline{U}$, Mal'tsev, finite

Theorem [MK '24]

- If $\mathrm{Clo}(\underline{L} \times \underline{U}) \subseteq \mathrm{Clo}(\underline{A})$:

  $\mathrm{SMP}(\underline{A}) \sim_{p\text{-time}} \mathrm{SMP}(\underline{L} \times \underline{U}) \wedge \mathrm{SMP}(\mathrm{Diff}(\underline{A}))$

- If $\underline{U}$ is affine / supernilpotent:

  $\mathrm{SMP}(\underline{A}) \sim_{p\text{-time}} \mathrm{SMP}(\mathrm{Diff}(\underline{A}))$

SMP of 2-nilpotent algebras

$\boxed{\underline{A} = \underline{L} \otimes \underline{U}\ ,\ \underline{L}, \underline{U} \text{ affine}}$

$\Rightarrow$ reduce to SMP of affine closed clonoids.

$SMP(\underline{A}) \sim_{p\text{-time}} SMP(Diff(\underline{A}))$

In Example $\underline{A} = (\mathbb{Z}_q \times \mathbb{Z}_p, +, 0, -, f(x))$ $p \neq q$ prime

$Diff(\underline{A})$ = all operations $\mathbb{Z}_p^n \longrightarrow \mathbb{Z}_q$ $\Rightarrow SMP(\underline{A}) \in P$.

SMP of 2-nilpotent algebras

$\boxed{\underline{A} = \underline{L} \otimes \underline{U}\,,\ \underline{L}, \underline{U} \text{ affine}}$ $\Rightarrow$ reduce to SMP of affine closed clonoids.

$\mathrm{SMP}(\underline{A}) \sim_{p\text{-time}} \mathrm{SMP}(\mathrm{Diff}(\underline{A}))$

In Example $\underline{A} = (\mathbb{Z}_q \times \mathbb{Z}_p, +, 0, -, f(x))$ $p \neq q$ prime

$\mathrm{Diff}(\underline{A})$ = all operations $\mathbb{Z}_p^n \longrightarrow \mathbb{Z}_q \Rightarrow \mathrm{SMP}(\underline{A}) \in \mathrm{P}$.

Theorem [MK'24]

If $|U| = p$ prime, $p \nmid |L|$

$\mathrm{SMP}(\underline{A}) \in \mathrm{P}$.

SMP of 2-nilpotent algebras

$\boxed{\underline{A} = \underline{L} \otimes \underline{U}\,,\ \underline{L}, \underline{U} \text{ affine}}$

$\Rightarrow$ reduce to SMP of affine closed clonoids.

$\mathrm{SMP}(\underline{A}) \sim_{p\text{-time}} \mathrm{SMP}(\mathrm{Diff}(\underline{A}))$

In Example $\underline{A} = (\mathbb{Z}_q \times \mathbb{Z}_p, +, 0, -, f(x))$ $p \neq q$ prime

$\mathrm{Diff}(\underline{A})$ = all operations $\mathbb{Z}_p^n \longrightarrow \mathbb{Z}_q \Rightarrow \mathrm{SMP}(\underline{A}) \in P$.

Theorem [MK'24]

If $|U| = p$ prime, $p \nmid |L|$

$\mathrm{SMP}(\underline{A}) \in P$.

$\{\hat{r}(\bar{u}_1, \dots, \bar{u}_n) \mid \hat{r} \in \mathrm{Diff}\,\underline{A}\} \leq \underline{L}^k$

is generated by

$\{\hat{f}(u_1, \dots, \bar{u}_n) \mid \hat{f} \in B\}$, s.t. $\mathrm{supp}(\hat{f}) \leq$ 2-dimensional subspace of $\mathbb{Z}_p^k$

[Fioravanti '20] + [MK'24]

Future work

$$\boxed{\underline{A} = \underline{L} \otimes \underline{U}, \ \underline{L}, \underline{U} \text{ affine}}$$

- if $|A| = p^n$

  $SMP(\underline{A}) \in P$ (supernilpotent)

$\Rightarrow$ interesting case: $|L|, |U|$ coprime

Future work

$\boxed{\underline{A} = \underline{L} \otimes \underline{U}, \ \underline{L}, \underline{U} \text{ affine}}$

- if $|A| = p^n$
  $SMP(\underline{A}) \in P$ (supernilpotent)

$\Rightarrow$ interesting case: $|L|, |U|$ coprime

theorem [Mayr, Wynne '23]

If $\underline{U}, \underline{L}$ affine, coprime
$Con(\underline{U})$ distributive (e.g. $\underline{U} = \mathbb{Z}_k$)
$\mathcal{C}$ is $(\underline{U}, \underline{L})$-clonoid

$\Rightarrow$ $\mathcal{C}$ is fin. generated & „nice".

[TO DO]

$SMP(\underline{A}) \in P$

Future work

$\boxed{\underline{A} = \underline{L} \otimes \underline{U} \,,\ \underline{L}, \underline{U} \text{ affine}}$

•) if $|A| = p^n$

$SMP(\underline{A}) \in P$ (supernilpotent)

$\Rightarrow$ interesting case: $|L|, |U|$ coprime

theorem [Mayr, Wynne '23]

If $\underline{U}, \underline{L}$ affine, coprime

$Con(\underline{U})$ distributive (e.g. $\underline{U} = \mathbb{Z}_{k}$)

$\mathcal{C}$ is $(\underline{U}, \underline{L})$-clonoid

$\Rightarrow$ $\mathcal{C}$ is fin. generated & „nice".

Question:

What if

$Con(\underline{U})$ not distributive?

e.g. $\underline{U} = \mathbb{Z}_p \times \mathbb{Z}_p$

$\underline{L} = \mathbb{Z}_q$

[TO DO]

$SMP(\underline{A}) \in P$

Thank you for your attention!

Any questions?