Finitely based 2-nilpotent Maltsev algebras

Michael Kompatscher, Peter Mayr, Patrick Wynne
Charles University Prague   CU Boulder

AAA 102
University of Szeged, 24.06.2022

European Research Council
Established by the European Commission

CoCoSym: Symmetries in Computational Complexity
This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant No 771005)

Maltsev algebras and finite eq. bases

$\underline{A} = (A, f_1, \dots, f_n)$ ... finite algebra $(|A| < \infty)$

$\underline{A}$ is Maltsev if $\exists$ term m: $m(yxx) \approx m(xxy) \approx y$

Ex. rings $x - y + z$, groups $x y^{-1} z$, loops $(x/y)z$, BA, ...

$\boxed{\mathrm{Id}(\underline{A})}$ ... identities holding in $\underline{A}$

$\underline{A}$ is finitely based if $\exists \Sigma \subseteq \mathrm{Id}(\underline{A})$: $\boxed{|\Sigma| < \infty,\ \Sigma \models \mathrm{Id}(\underline{A})}$

Ex. $\mathbb{Z}_n$ is finitely based:

$\mathrm{Id}(\mathbb{Z}_n, +, 0, -) \dashv \{$ Abelian group axioms, $n \cdot x \approx 0 \}$

Finitely based Maltsev algebras

$\exists$ non-finitely based Maltsev $\underline{A}$ ($(G,\cdot,1,^{-1},c)$ '82 Bryant)

→ Which Maltsev algebras $\underline{A}$ are finitely based?

rewriting approach

↳ modulo some Σ every term has a normal form.

- affine $\underline{A}$ (e.g. $\mathbb{Z}_n$)
- groups (Oates, Powell '64)
- rings (L'vov/Kruse '73)
- supernilpotent $\underline{A}$ (Vaughan-Lee '83)

$HSP(\underline{A})$ is residually finite

↳ non-constructive

↳ also if $HSP(\underline{A})$ has difference term (KSW '16)

$\not\Leftarrow$

←?— nilpotent $\underline{A}$

2-nilpotent Maltsev algebras

- $\underline{A}$ is affine if $Clo(\underline{A}, (a)_{a \in A}) = \{ c + \sum \alpha_i \cdot x_i \}$ w.r.t. a module
- $\underline{A}$ is 2-nilpotent $\iff \exists \underline{L}, \underline{U}$ affine [Freese McKenzie '87]

$\boxed{\underline{A} \simeq \underline{L} \otimes^T \underline{U}}$ $\quad A = L \times U$, $\forall t \in Clo(\underline{A})$:

$$t^{A}((l_1,u_1),\dots,(l_n,u_n)) = \underbrace{(t^{L}(\bar{l}), t^{U}(\bar{u}))}_{\text{affine part}} + \underbrace{(\hat{t}(\bar{u}), 0)}_{\text{'distortion'}}$$

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

In particular:

$x * y := m(x, 0, y) = x + y + \hat{t}(x_U, y_U)$ is Loop

2-nilpotent Maltsev algebras

$\underline{A}$ is 2-nilpotent $\boxed{\underline{A} \simeq \underline{L} \otimes^T \underline{U}}$

$$t^{\underline{A}}((l_1,u_1),\dots,(l_n,u_n)) = \underbrace{(t^{\underline{L}}(\bar{l}), t^{\underline{U}}(\bar{u}))}_{\text{affine part}} + \underbrace{(\hat{t}(\bar{u}), 0)}_{\text{'distortion'}\ \hat{t}: U^n \to L}$$

rewriting approach (idea)

? 1) Seperate affine and distortion part.

✓ 2) $\Sigma_{aff.}$ $\models$ normal forms of affine terms

? 3) $\hat{\Sigma}$, to describe normal forms in the clonoid $\mathrm{Clo}\,\underline{L} \circ \{\hat{t} : U^n \to L\} \circ \mathrm{Clo}\,\underline{U}$

2-nilpotent loops of size $p \cdot q$

$p \neq q$ ... primes, $\underline{A}$ nilpotent loop $|A| = p \cdot q$

Then wlog. $\underline{A} \,\hat{=}\, \mathbb{Z}_q \otimes \mathbb{Z}_p = (\mathbb{Z}_q \times \mathbb{Z}_p, *, 0, /, \backslash)$

Lemma (→ Peter's talk)

$\underline{A}$ is term equivalent to $(\mathbb{Z}_q \times \mathbb{Z}_p, +, 0, -, \hat{r})$

$$\boxed{\begin{aligned} \hat{r}(x,y) &:= (x*y)^p / (x^p * y^p) \\ x+y &:= (x*y)/r(x,y) \end{aligned}}$$

distortion $\mathbb{Z}_p^2 \to \mathbb{Z}_q$

Abelian group

$(\mathbb{Z}_p, \mathbb{Z}_q)$ - clonoids

•) $\sum_j \lambda_j \hat{r}\left(\sum_{i=1}^{n} \alpha_i x_i, \sum_{i=1}^{n} \beta_i x_i\right)$ form a $(\mathbb{Z}_p, \mathbb{Z}_q)$-clonoid $\mathcal{C}$

Theorem (Fioravanti '19) → Patrick's talk

1) $\mathcal{C}$ is generated by unaries $\mathcal{C}^{(1)} = \{\hat{f}(x) \in \mathcal{C}\} \leq \mathbb{Z}_q^{\mathbb{Z}_p}$

2) $\hat{f} \in \mathcal{C} \iff \hat{f}(\alpha_1 x, \alpha_2 x, \ldots, \alpha_n x) \in \mathcal{C}^{(1)} \quad \forall \bar{\alpha} \in \mathbb{Z}_p^n$

3) Already one $\hat{g} \in \mathcal{C}^{(1)}$ generates $\mathcal{C}$

↳ $\underline{A}$ is term equivalent to $(\mathbb{Z}_q \times \mathbb{Z}_p, +, 0, -, \hat{g})$

⇒ full classification of 2-nil. $\underline{A}$, $|A| = pq$, with constant.

$(\mathbb{Z}_p, \mathbb{Z}_q)$ - clonoids

For $\bar{a} = (0,\dots,0,1,a_i,\dots,a_n) \in \mathbb{Z}_p^n$, $f \in \mathcal{C}^{(1)}$, let $f^{\bar{a}}(\bar{x}) := \begin{cases} f(x) & \text{if } \bar{x} = (a_1 x, \dots, a_n x) \\ 0 & \text{else} \end{cases}$

Corollary (Fioravanti '19)

If B is basis of $\mathcal{C}^{(1)}$, then

1) $B_1^n = \{ f^{\bar{a}} \mid f \in B \}$
2) $B_2^n = \{ f(\bar{a} \cdot \bar{x}) \mid f \in B \}$.

$\Big\}$ is a basis of $\mathcal{C}^{(n)} = \{ f : \mathbb{Z}_p^n \to \mathbb{Z}_q \mid f \in \mathcal{C} \}$

Subpower membership of $\underline{A}$ is in $\underline{P}$: (Peter's talk)

$$Sg_{\underline{A}^n}(\bar{a}_1, \dots, \bar{a}_k) = Sg_{(A_1^n,+)}(\bar{a}_1, \dots, \bar{a}_k) + Sg_{(A_1^n,+)}\big(\underbrace{B_1^n(\bar{a}_1, \dots, \bar{a}_k)}\big)$$

can be computed in $|B| \cdot n$

A finite basis

Summary $\underline{A} = (\mathbb{Z}_q \times \mathbb{Z}_p, +, 0, -, \underbrace{\hat{f}_1, \dots, \hat{f}_n}_{B \text{ basis of } C^{(1)}})$

- $t \in \mathrm{Clo}\,\underline{A}$ has a normal form

$$t(x_1, \dots, x_n) = \underbrace{\sum_i \beta_i x_i}_{\text{affine}} + \underbrace{\sum_{f \in B, \bar{\alpha}} \lambda_{f,\bar{\alpha}} f(\bar{\alpha} \cdot \bar{x})}_{\text{lin. com. over } B_2^n}$$

Rewriting using

- $+$ is Abelian group, $[pq] \cdot x \approx 0$ $\quad \Sigma_{\text{aff}}$
- $q \cdot \hat{f}_i(x) \approx 0$, $\hat{f}_i(x + p \cdot y) \approx \hat{f}_i(x)$, $\hat{f}_i(x + \hat{f}_j(y)) \approx \hat{f}_i(x)$
- $\hat{f}_i(c \cdot x) \approx \sum_{f \in B} \lambda_j f_j(x)$ for all $c \in \mathbb{Z}_p$

$\Big] \; \hat{\Sigma}$

$\Rightarrow$ $\underline{A}$ is finitely based

What I was hoping to tell you...

For general $\underline{A} = (\mathbb{Z}_q \times \mathbb{Z}_p, m(x,y,z), f_1 \dots f_n))$

rewriting approach

1) Seperate affine and distortion part

✓ 2) $\Sigma_{aff} \models$ normal forms of affine term

✓ 3) $\hat{\Sigma}$ to describe normal forms in the clonoid

$$\mathcal{C} = \mathrm{Clo}(\mathbb{Z}_q, +) \circ \{\hat{t} : U \to L\} \circ \mathrm{Clo}(\mathbb{Z}_p, x - y + z)$$

↳ $\mathcal{C}$ generated by $\mathcal{C}^{(2)}$

↳ $x - y + z \in \mathrm{Clo}\,\underline{A}$?

We don't know!!

→ Peter's talk

The clonoid part

Let $\mathcal{C}$ be a $((\mathbb{Z}_p, x-y+z), (\mathbb{Z}_q, +))$-clonoid

* s.t. $\hat{f}(x \dots x) \simeq 0 \quad \forall \hat{f} \in \mathcal{C}$

Theorem (Wyme... ?)

1) $\mathcal{C}$ is generated by binary $\mathcal{C}^{(2)} \leq \mathbb{Z}_q^{\mathbb{Z}_p^2}$

2) $\hat{f} \in \mathcal{C} \iff \hat{f}(\underbrace{\alpha_1 x + (1-\alpha_1) y, \dots, \alpha_n x + (1-\alpha_n) y}_{\text{2-dim subspaces} \leq \mathbb{Z}_p^n \text{ containing } (x x \dots x)}) \in \mathcal{C}^{(2)}$

If B ... basis of $\mathcal{C}^{(2)}$, then

3) $B_1^{(n)} = \{ f^{\bar{\alpha}} \mid f \in B \}$ is basis of $\mathcal{C}^{(n)}$

4) $B_2^{(n)} = \{ f(x_1, \bar{\alpha} \cdot \bar{x}) \mid f \in B \}$

Do we actually need $x-y+z$?

For $\underline{A} = (\mathbb{Z}_q \times \mathbb{Z}_p, m(xyz), f_1 \dots f_n)$

For $t, s \in \mathrm{Clo}\,\underline{A}$ define $t \sim s :\Leftrightarrow t_{aff} = s_{aff}$

$\mathcal{C} := \{ t - s \mid t \sim s \}$ is $((\mathbb{Z}_p, x-y+z), (\mathbb{Z}_q, +))$-clonoid

obs.: If $f \in \mathrm{Clo}\,\underline{A}, \hat{r} \in \mathcal{C} \Rightarrow f + \hat{r} \in \mathcal{C}$

Rewriting strategy:

~ •) Find normal forms $t = t_m + \hat{t}$, $t_m \in \mathrm{Clo}(A, m)$, $\hat{t} \in \mathcal{C}$

not affine

✓ •) Finite identities computing $\hat{t}$

~ •) Finite identities for computing t_m (e.g. $m(xyz) \approx m(zyx) + \hat{r}(xyz)$, $\hat{r} \in \mathcal{C}$)

Thank you!

Any questions?