Nilpotent Mal'cev algebras

Michael Kompatscher
Charles University

AAA108
February 7, 2026

Part 1:

Mal'cev algebras

Mal'cev algebras

Def $\underline{A} = (A, f_1, f_2 \dots)$ is **Mal'cev** if it has a **Mal'cev term** $m(x,y,z)$

$\underline{A} \models m(y,x,x) \approx m(x,x,y) \approx y$

Examples

- Rings $(R, +, -, 0, \cdot)$ — $x - y + z$
- Groups $(G, \cdot, 1, ^{-1})$ — $xy^{-1}z$
- BA $(B, \wedge, \vee, \neg, 0, 1)$ — $(x \wedge y \wedge z) \vee (x \wedge \neg y \wedge \neg z) \vee (\neg x \wedge \neg y \wedge z)$
- quasigroups $(G, \cdot, /, \backslash)$ — $(x/(y \backslash y)) \cdot (y \backslash z)$
- Heyting algebras $(H, \wedge, \vee, \to)$ — $[(x \to y) \to z] \wedge [(z \to y) \to x] \wedge (x \vee z)$

Maltsev / Malcev / Mal'tsev / Mal'cev

Malcev algebra

4 languages

Article Talk Read Edit View history Tools

From Wikipedia, the free encyclopedia

For the Lie algebras or groups, see Malcev Lie algebra.

In mathematics, a **Malcev algebra** (or **Maltsev algebra** or **Moufang–Lie algebra**) over a field is a nonassociative algebra that is antisymmetric, so that

$$xy = -yx$$

and satisfies the **Malcev identity**

$$(xy)(xz) = ((xy)z)x + ((yz)x)x + ((zx)x)y.$$

They were first defined by Anatoly Maltsev (1955).

Malcev algebras play a role in the theory of Moufang loops that generalizes the role of Lie algebras in the theory of groups. Namely, just as the tangent space of the identity element of a Lie group forms a Lie algebra, the tangent space of the identity of a smooth Moufang loop forms a Malcev algebra. Moreover, just as a Lie group can be recovered from its Lie algebra under certain supplementary conditions, a smooth Moufang loop can be recovered from its Malcev algebra if certain supplementary conditions hold. For example, this is true for a connected, simply connected real-analytic Moufang loop.[1]

Maltsev / Malcev / Mal'tsev / Mal'cev

Malcev algebra

4 languages

Article Talk Read Edit View history Tools

From Wikipedia, the free encyclopedia

For the Lie algebras or groups, see Malcev Lie algebra.

In mathematics, a **Malcev algebra** (or **Maltsev algebra** or Mo[illegible]ng–Lie **algebra**) over a fie[illegible] a nonassociative algebra that is antisymmetric, so that

$$xy = -yx$$

and satisfies the **Malcev identity**

$$(xy)(xz) = ((xy)z)x + ([illegible])x + ((zx)x)y.$$

They were first defined by Anatoly Maltsev (1955).

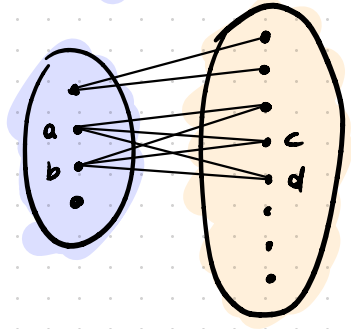
Malcev algebras play a role in the theory of Moufang loops that generalizes the role of Lie algebras in the theory of groups. Namely, just as the tangent space of the identity element of a Lie group forms a Lie algebra, the tangent space of the identity of a smooth Moufang loop forms a Malcev algebra. Moreover, just as a Lie group can be recovered from its Lie algebra under certain supplementary conditions, a smooth Moufang loop can be recovered from its Malcev algebra if certain supplementary conditions hold. For example, this is true for a connected, simply connected real-analytic Moufang loop.[1]

Maltsev / Malcev / Mal'tsev / Mal'cev

Basic properties

$\underline{A}$ is Mal'cev

$\Leftrightarrow$ all $R \leq \underline{A}^n \times \underline{A}^m$ have the **parallelogram property**



$$\frac{(a,c) \in R \quad (a,d) \in R \quad (b,d) \in R}{(b,c) \in R}$$

$\Leftrightarrow$ $\mathrm{HSP}(\underline{A})$ is **congruence permutable** [Mal'cev '54]

$\forall \underline{B} \in \mathrm{HSP}(A)\ \forall \alpha, \beta \in \mathrm{Con}(\underline{B})$: $\alpha \circ \beta = \beta \circ \alpha$

Four Unsolved Problems in Congruence Permutable Varieties

Ross Willard

University of Waterloo, Canada

Nashville, June 2007

Part 2:

Four Unsolved Problems in Congruence Permutable Varieties

~~Ross Willard~~ Michael Kompatscher

~~University of Waterloo, Canada~~

~~Nashville, June 2007~~ Vienna 2026

1) Classification

A ... finite set

Task: Classify all Mal'cev algebras on A up to term equivalence.

finitely many	$\lvert A\rvert = 2$	[Post '41]
	$\lvert A\rvert = 3$	[Bulatov '03]
ω many	$\lvert A\rvert \geq 4$	[AMM '14, Idziak '99]

1) Classification

A ... finite set

Task: Classify all Mal'cev algebras on A up to term equivalence.

finitely many	$\lvert A\rvert = 2$	[Post '41]
	$\lvert A\rvert = 3$	[Bulatov '03]
ω many	$\lvert A\rvert \geq 4$	[AMM '14, Idziak '99]

$Clo(\underline{A}) :=$ clone of term operations

Ex.

$$Clo(\mathbb{Z}_4,+) \subsetneq Clo(\mathbb{Z}_4,+,2x_1x_2) \subsetneq Clo(\mathbb{Z}_4,+,2x_1x_2x_3) \subsetneq \dots$$

$$= \left\{ \sum_i \alpha_i x_i + 2\sum_{i,j,k} \beta_{ijk} x_i x_j x_k \;\middle|\; \begin{matrix} \alpha_i \in \mathbb{Z}_4 \\ \beta_{ijk} \in \mathbb{Z}_2 \end{matrix} \right\}$$

1) Classification

A ... finite set

Task: Classify all Mal'cev algebras on A up to term equivalence.

finitely many	$\lvert A\rvert = 2$	[Post '41]
	$\lvert A\rvert = 3$	[Bulatov '03]
ω many	$\lvert A\rvert \geq 4$	[AHM '14, Idziak '99]

$Clo(\underline{A}) :=$ clone of term operations

Ex.

$$Clo(\mathbb{Z}_4,+) \subsetneq Clo(\mathbb{Z}_4,+,2x_1x_2) \subsetneq Clo(\mathbb{Z}_4,+,2x_1x_2x_3) \subsetneq \dots$$

$$= \left\{ \sum_i \alpha_i x_i + 2\sum_{i,j,k} \beta_{ijk} x_i x_j x_k \;\middle|\; \begin{matrix} \alpha_i \in \mathbb{Z}_4 \\ \beta_{ijk} \in \mathbb{Z}_2 \end{matrix} \right\}$$

Question (Aichinger):
Can there be infinite antichains?

2) Axiomatization

Input: Finite algebra $\underline{A}$

Question: Does $\underline{A}$ have a finite equational basis Σ?

$\Sigma \models t \approx s \Leftrightarrow \underline{A} \models t \approx s$

↳ undecidable! [McKenzie '96]

2) Axiomatization

Input: Finite algebra $\underline{A}$

Question: Does $\underline{A}$ have a finite equational basis Σ?

$\Sigma \models t \approx s \Leftrightarrow \underline{A} \models t \approx s$

↳ undecidable! [McKenzie '96]

Question: But what about Mal'cev algebras?

Ex.

finitely based	$\exists$ non-finitely based
BA	non-associative algebra [Bolin '76]
groups [OP '64]	loop [Vaughan-Lee '79]
rings [Lvov '73]	pointed groups [Bryant '87]

3) Interpolation

$\underline{A}$ ... fixed algebra

SMP($\underline{A}$) subpower membership problem

Input: partial $f : A^n \to A$
Question: $\exists$ extension $f \in Clo(\underline{A})$?

$$f : \begin{pmatrix} a_{11}, \dots, a_{1n} \\ a_{21}, \dots, a_{2n} \\ \vdots \\ a_{m1}, \dots, a_{mn} \end{pmatrix} \mapsto \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}$$

$$\langle \bar{a}_1 \dots \bar{a}_n \rangle_{\underline{A}^m} \overset{?}{\ni} \bar{b}$$

Examples

-) SMP($\mathbb{Z}_2, +, 0, -$) $\in P$ [Gauss elimination]
-) SMP($\{0,1\}, \wedge, \vee, \neg$) $\in P$ [funct. complete]
-) SMP($\underline{A}$) $\in NP$ for Mal'cev [Mayr '12]

Question (Willard): Is SMP($\underline{A}$) $\in P$ for Mal'cev $\underline{A}$?

4) Equivalence

$\underline{A}$ ... fixed algebra

CEQV($\underline{A}$) circuit equivalence problem

Input: $\underline{A}$-circuits t, s
Question: Does $\underline{A} \models t \approx s$?

$\sum_i \alpha_i x_i \approx \sum_i \beta_i x_i \iff \alpha_i \equiv \beta_i \ (2)$

Examples

- CEQV $(\mathbb{Z}_2, +, 0, -) \in$ P
- CEQV $(\{0,1\}, \wedge, \vee, \neg) \in$ coNP-c. ← UNSAT

Question: Complexity of CEQV($\underline{A}$) for Mal'cev $\underline{A}$?

Part 3:

Commutator theory to the rescue!

Abelianness

$\underline{A}$ with Mal'cev term $m(x\,y\,z)$

Def. $\underline{A}$ is *Abelian* $:\Leftrightarrow$ $\left\{ \begin{array}{ccc} x & \text{—} & m(x,y,z) \\ | & & | \\ y & \text{—} & z \end{array} \right\} \leq \underline{A}^4$

Theorem $\underline{A}$ is Abelian $\Leftrightarrow$

[Smith '75] $Clo(\underline{A}, (a)_{a\in A}) = \{ \sum r_i x_i + d \}$ over some module

Abelianness

$\underline{A}$ with Mal'cev term $m(x\,y\,z)$

Def. $\underline{A}$ is **Abelian** $:\Leftrightarrow$ $\left\{ \begin{array}{ccc} x & \text{—} & m(x,y,z) \\ | & & | \\ y & \text{—} & z \end{array} \right\} \leq \underline{A}^4$

Theorem $\underline{A}$ is Abelian $\Leftrightarrow$ [Smith '75]

$$Clo(\underline{A}, (a)_{a\in A}) = \left\{ \sum r_i x_i + d \right\} \text{ over some module}$$

Def. α **centralizes** β $:\Leftrightarrow$ $\alpha, \beta \in Con(\underline{A})$

$$\Delta_{\alpha,\beta} = \left\{ \begin{array}{ccc} x & \text{—} & m(x\,y\,z) \\ | & & | \\ y & \text{—} & z \end{array} \right\} \leq \underline{A}^4$$

[as in group theory]

α is **Abelian** $\Leftrightarrow$ α centralizes α,

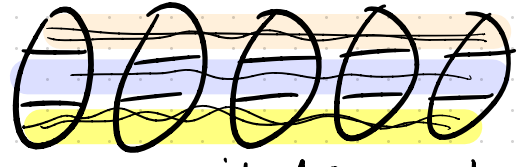
centralizer $(0:\alpha)$ = biggest β centralizing α, ...

Known results

	HSP($\underline{A}$)	classification	fin. based	SMP($\underline{A}$)	CEQV($\underline{A}$)
	Abelian	finite	✓	P	P
	CD	finite	✓	P	coNP-c
$\lvert A\rvert \leq 3$	residually finite	finite [KS '15]	✓ [M '87]	P [BMS '18]	P / coNP-c [IK '18]

HSP($\underline{A}$) is CD $\Leftrightarrow \nexists\ \underline{B} \in HS(\underline{A})$ with Abelian $\alpha \Leftrightarrow \underline{A}$ has majority

HSP($\underline{A}$) is residually finite $\Leftrightarrow \forall B \in HS(\underline{A})$: α Abelian $\Rightarrow (0:\alpha)$ Abelian $\Leftrightarrow \forall$ critical $R \leq \underline{A}^n$



↳ Abelian linked components

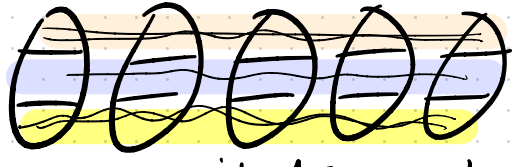
→ [Ross' talk!]

Known results

	HSP($\underline{A}$)	classification	fin. based	SMP($\underline{A}$)	CEQV($\underline{A}$)
	Abelian	finite	✓	P	P
	CD	finite	✓	P	coNP-c
$\lvert A\rvert \leq 3$	residually finite	finite [KS '15]	✓ [M '87]	P [BMS '18]	P / coNP-c [IK '18]

HSP($\underline{A}$) is CD $\Leftrightarrow \nexists\ \underline{B} \in HS(\underline{A})$ with Abelian $\alpha \Leftrightarrow \underline{A}$ has majority

HSP($\underline{A}$) is residually finite $\Leftrightarrow \forall B \in HS(\underline{A})$: α Abelian $\Rightarrow (0:\alpha)$ Abelian $\Leftrightarrow \forall$ critical $R \leq \underline{A}^n$



↳ Abelian linked components

→ [Ross' talk!]

Open case:
What if α Abelian, but $(0:\alpha) = 1_A$ not?

Central extensions

Let $\alpha \in \mathrm{Con}(\underline{A})$ central

$\rightsquigarrow$ "difference algebra"

$\underline{U} := \underline{A}/\alpha$, Abelian $\underline{L} := \alpha/\Delta_{1\alpha}$:

[FM '87] $\Longrightarrow$ $\underline{A} \cong \underline{U} \otimes \underline{L}$, where

$$f^{\underline{U}\otimes\underline{L}}\left(\begin{pmatrix}u_1\\ \ell_1\end{pmatrix},\dots,\begin{pmatrix}u_n\\ \ell_n\end{pmatrix}\right) = \begin{pmatrix} f^{\underline{U}}(u_1,\dots,u_n) \\ f^{\underline{L}}(\ell_1,\dots,\ell_n) + \hat{f}(u_1\dots u_n)\end{pmatrix}$$

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

Central extensions

Let $\alpha \in \mathrm{Con}(\underline{A})$ central

$\rightsquigarrow$ "difference algebra"

$\underline{U} := \underline{A}/\alpha$, Abelian $\underline{L} := \alpha/\Delta_{1\alpha}$:

[FM'87] $\Rightarrow$ $\underline{A} \cong \underline{U} \otimes \underline{L}$, where

$$f^{\underline{U}\otimes\underline{L}}\left(\begin{pmatrix}u_1\\ \ell_1\end{pmatrix},\dots,\begin{pmatrix}u_n\\ \ell_n\end{pmatrix}\right) = \begin{pmatrix} f^{\underline{U}}(u_1,\dots,u_n) \\ f^{\underline{L}}(\ell_1,\dots,\ell_n) + \hat{f}(u_1\dots u_n)\end{pmatrix}$$

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

Example

$\mathbb{Z}_4 \cong \mathbb{Z}_2 \otimes \mathbb{Z}_2$ with $\begin{pmatrix}u_1\\ \ell_1\end{pmatrix} + \begin{pmatrix}u_2\\ \ell_2\end{pmatrix} = \begin{pmatrix}u_1+u_2\\ \ell_1+\ell_2+u_1\cdot u_2\end{pmatrix}$

Central extensions

Let $\alpha \in \mathrm{Con}(\underline{A})$ central

$\rightsquigarrow$ "difference algebra"

$\underline{U} := \underline{A}/\alpha$, Abelian $\underline{L} := \alpha/\Delta_{1\alpha}$:

[FM'87] $\Longrightarrow$ $\underline{A} \cong \underline{U} \otimes \underline{L}$, where

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

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

Example

$\mathbb{Z}_4 \cong \mathbb{Z}_2 \otimes \mathbb{Z}_2$ with $\begin{pmatrix} u_1 \\ l_1 \end{pmatrix} + \begin{pmatrix} u_2 \\ l_2 \end{pmatrix} = \begin{pmatrix} u_1 + u_2 \\ l_1 + l_2 + u_1 \cdot u_2 \end{pmatrix}$

Def. $\underline{A}$ is n-nilpotent $\Leftrightarrow \underline{A} \cong \underline{L}_1 \otimes \underline{L}_2 \otimes \dots \otimes \underline{L}_n$ for $\underline{L}_i$ Abelian

The difference clonoid

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

Def. for terms t, s $\quad t \sim s :\Leftrightarrow t^{\underline{U}} = s^{\underline{U}} \;\&\; t^{\underline{L}} = s^{\underline{L}}$

$$\mathrm{Diff}(\underline{A}) = \{ \hat{t} - \hat{s} \mid t \sim s \}$$

Example $\mathbb{Z}_4 \cong \mathbb{Z}_2 \otimes \mathbb{Z}_2$

$$x_1 + x_2 = \begin{pmatrix} u_1 + u_2 \\ l_1 + l_2 + u_1 u_2 \end{pmatrix} \sim \begin{pmatrix} u_1 + u_2 \\ l_1 + l_2 + u_1 u_2 + u_2 \end{pmatrix} = x_1 + 3x_2$$

$$\Rightarrow (u_1, u_2) \mapsto u_2 \in \mathrm{Diff}(\mathbb{Z}_4)$$

$\cong \{$ linear maps $\mathbb{Z}_2^n \to \mathbb{Z}_2 \}$

$$\underline{A}_k = \left(\mathbb{Z}_4, 2x_1 \dots x_k\right) \curvearrowright \begin{pmatrix} 0 \\ u_1 u_2 \cdots u_k \end{pmatrix}$$

$$\mathrm{Diff}(\underline{A}_k) = \{ f \in \mathbb{Z}_2[u_1, \dots, u_k] \mid \deg(f) \leq k \}$$

The difference clonoid

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

$\hat{d} \in Diff(\underline{A})$, $f \in Clo(\underline{A}) \Rightarrow f + \hat{d} \in Clo(\underline{A})$

$Diff(\underline{A})$ = kernel of clone homomorphism

$$\xi : Clo(\underline{A}) \to Clo(\underline{U} \times \underline{L})$$

$$\begin{pmatrix} t^{\underline{U}} \\ t^{\underline{L}} + \hat{t} \end{pmatrix} \mapsto \begin{pmatrix} t^{\underline{U}} \\ t^{\underline{L}} \end{pmatrix}$$

The difference clonoid

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

$\hat{d} \in Diff(\underline{A})$, $f \in Clo(\underline{A}) \Rightarrow f + \hat{d} \in Clo(\underline{A})$

$Diff(\underline{A})$ = kernel of clone homomorphism

$$\varphi : Clo(\underline{A}) \to Clo(\underline{U} \times \underline{L})$$

$$\begin{pmatrix} t^{\underline{U}} \\ t^{\underline{L}} + \hat{t} \end{pmatrix} \mapsto \begin{pmatrix} t^{\underline{U}} \\ t^{\underline{L}} \end{pmatrix}$$

$C = Diff(\underline{A})$ is a clonoid from $\underline{U}$ to $\underline{L}$

$$C \circ Clo(\underline{U}) \subseteq C$$

$$Clo(\underline{L}) \circ C \subseteq C$$

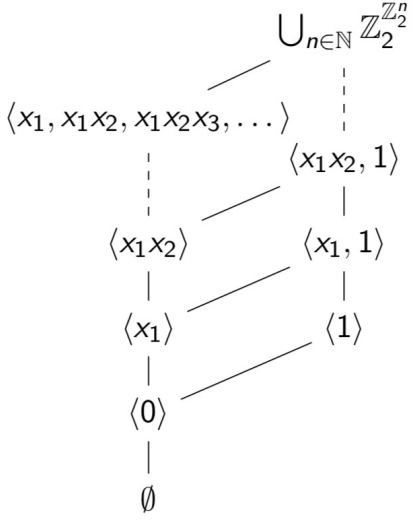
Clonoids

⇝ growing number of clonoid classifications

Cardinalities of (C_1, C_2)-clonoid lattices

	$[J, I]$	$[I^*, \Omega(1)]$	$[V_{01}, V]$ $[\Lambda_{01}, \Lambda]$	$[MU_{01}^{\infty}, MU^{\infty}]$ $[MW_{01}^{\infty}, MW^{\infty}]$	U_{01}^{∞} W_{01}^{∞}	U^{∞} W^{∞}	$[L_{01}, L]$	$[\{SM, MU_{01}^{k}, MW_{01}^{k}\}, \Omega]$
J	U	U	U	U	U	U	C	F
I_0, I_1	U	U	U	U	U	U	C	F
I	U	U	U	F	F	F	C	F
I^*	U	U	U	U	U	U	C	F
$\Omega(1)$	U	U	U	F	F	F	C	F
V_{01}, Λ_{01}	U	U	U	U	U	U	F	F
V_{0*}, Λ_{*1}	U	U	U	F	F	F	F	F
V_{*1}, Λ_{0*}	U	U	U	U	U	U	F	F
V, Λ	U	U	U	F	F	F	F	F
MU_{01}^{k}, MW_{01}^{k}	U	U	U	U	U	U	F	F
MU^{k}, MW^{k}	U	U	U	U	U	U	F	F
U_{01}^{k}, W_{01}^{k}	U	U	U	U	U	U	F	F
U^{k}, W^{k}	U	U	U	U	U	U	F	F
L_{01}	U	U	U	U	U	U	C	F
L_{0*}, L_{*1}	U	U	U	U	U	U	C	F
LS	U	U	U	U	U	U	C	F
L	U	U	U	F	F	F	C	F
SM	U	U	U	U	U	U	F	F
$[M_{01}, M]$	C	C	F	F	F	F	F	F
$[S_{01}, \Omega]$	F	F	F	F	F	F	F	F

[Lehtonen '26]



$(\mathbb{Z}_2, \mathbb{Z}_2)$-clonoids

[Kronecker '19]

Part 4:

Back to Mal'cev clones

1) Classification

Question (Aichinger):
Can there be infinite antichains of Mal'cev clones?

On $|A| = 4$: No!

Proof sketch:

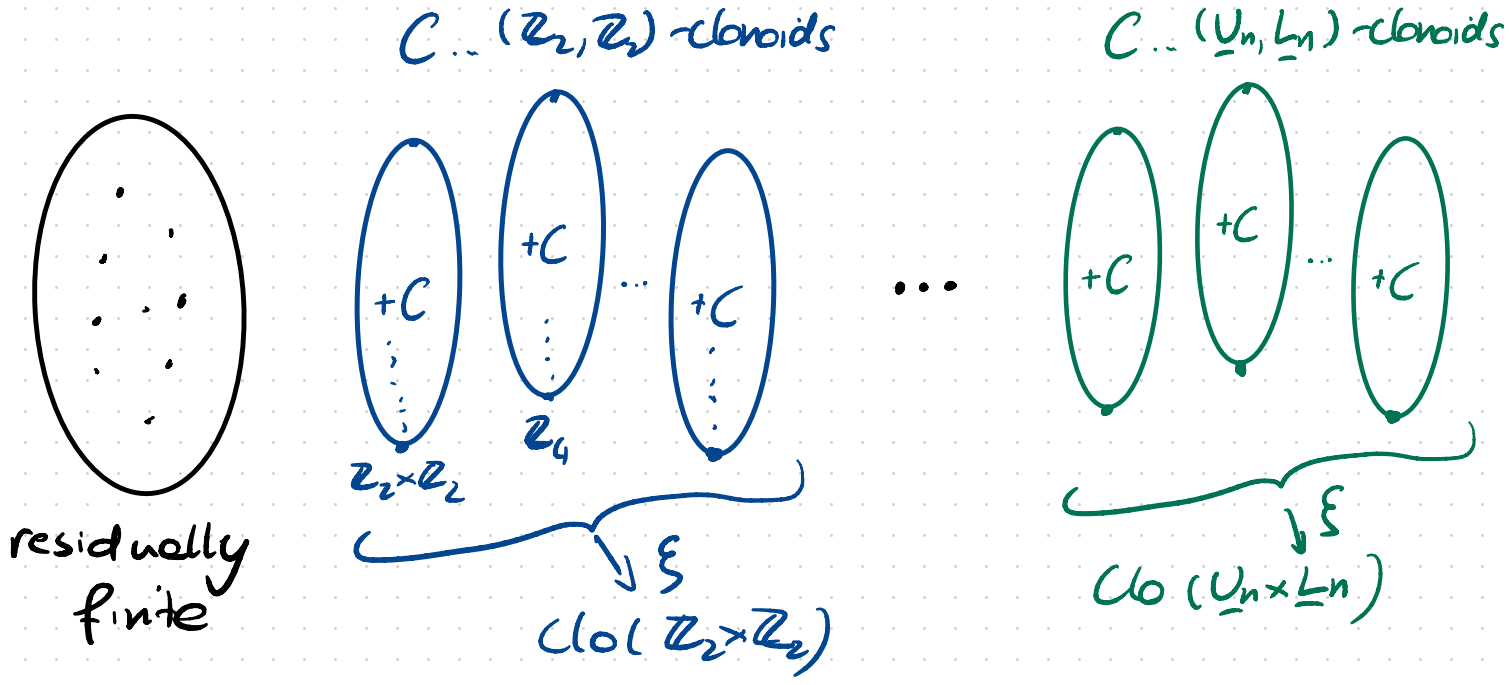
- $\exists^{\leq \text{fin.}}$ $Clo(\underline{A})$ such that $HSP(\underline{A})$ is residually finite.
- else $\underline{A} = \underline{U} \oslash \underline{L}$ $|U| = |L| = 2$, $\underline{L}$ Abelian

$$f : Clo(\underline{A}) \to Clo(\underline{U} \times \underline{L}) \text{ surjective}$$

then $Clo(\underline{A}) = Clo(\underline{A}') + C$ ↪ $(\underline{U}, \underline{L})$-clonoid

↪ minimal as above

$|A| = 4$



By clonoid classification [Kreinecker '19] [CL '24] $\rightsquigarrow$ $\nexists$ antichain in each $\mathcal{O}$

□

More results

$\exists \leq$ finitely many closoids for $(\underline{\cup}, \underline{\leq})$ for:

[Fioravanti '20/21]

$(\mathbb{Z}_p, \mathbb{Z}_q) \Rightarrow$ finitely many extensions of $\mathbb{Z}_p \times \mathbb{Z}_q$

$(\prod_{i \neq j} \mathbb{Z}_{p_i}, \mathbb{Z}_{p_j}) \Rightarrow$ —— " —— $\prod_i \mathbb{Z}_{p_i}$

[MW '24] $\underline{\cup}$ distributive module, $\underline{\leq}$ coprime

[FKR '26] $\underline{\cup}$ vector space, $\underline{\leq}$ coprime

More results

$\exists \leq$ finitely many clonoids for $(\underline{\cup}, \underline{\leq})$ for:

[Fioravanti '20/21]

$(\mathbb{Z}_p, \mathbb{Z}_q) \Rightarrow$ finitely many extensions of $\mathbb{Z}_p \times \mathbb{Z}_q$

$(\prod_{i \neq j} \mathbb{Z}_{p_i}, \mathbb{Z}_{p_j}) \Rightarrow$ —— " —— $\prod_i \mathbb{Z}_{p_i}$

[MW '24] $\underline{\cup}$ distributive module, $\underline{\leq}$ coprime

[FKR '26] $\underline{\cup}$ vector space, $\underline{\leq}$ coprime

Conjecture: $\leq$ fin. $(\underline{\cup}, \underline{\leq})$-clonoids for affine coprime $\underline{\cup}, \underline{\leq}$.

For general nilpotent algebras

Let $\underline{A} = \underline{L}_1 \otimes \underline{L}_2 \otimes \underline{L}_3 \otimes \cdots \otimes \underline{L}_n$ $\qquad (L_i, +) = \mathbb{Z}_{p_i}^{k_i}$

Extension [Aichinger '19]

$$\mathrm{Clo}(\underline{A}) \subseteq \mathrm{Clo}(\underline{A}, +, 0, -) \qquad (A, +) = \prod_{i=1}^{n} (L_i, +)$$

n-nil extended group.

For general nilpotent algebras

Let $\underline{A} = \underline{L}_1 \otimes \underline{L}_2 \otimes \underline{L}_3 \otimes \dots \otimes \underline{L}_n$ $\qquad (L_i,+) = \mathbb{Z}_{p_i}^{k_i}$

Extension [Aichinger '19]

$$Clo(\underline{A}) \leq Clo(\underline{A}, +, 0, -) \qquad (A,+) = \prod_{i=1}^{n} (L_i,+)$$

n-nil extended group.

Reduction

$\exists\ Clo(A,*) \leq Clo(A,0)$ — n-nil loop

for $0 \in A$

$$m(x,0,y) = \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 + \hat{\phi}_2(x, y_1) \\ \vdots \\ x_n + y_n + \hat{\phi}_n(\dots) \end{pmatrix}$$

$!!$

$x * y$

is **loop**

For general nilpotent algebras

Let $\underline{A} = \underline{L}_1 \otimes \underline{L}_2 \otimes \underline{L}_3 \otimes \dots \otimes \underline{L}_n$ $\qquad (L_i,+) = \mathbb{Z}_{p_i}^{k_i}$

Extension [Aichinger '19]

$$\mathrm{Clo}(\underline{A}) \subseteq \mathrm{Clo}(\underline{A}, +, 0, -) \qquad (A,+) = \prod_{i=1}^{n} (L_i,+)$$

n-nil extended group.

Reduction

$\exists\ \mathrm{Clo}(A,*) \subseteq \mathrm{Clo}(A,0)$ — n-nil loop

for $0 \in A$

$$m(x,0,y) = \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 + \hat{\phi}_2(x, y_1) \\ \vdots \\ x_n + y_n + \hat{\phi}_n(\dots) \end{pmatrix}$$

$m(x,0,y) = x * y$ is loop

Theorem: [Mayr, MK '26]

$\exists\ \mathrm{Clo}(A,*') \subseteq \mathrm{Clo}(\underline{A}, 0)$ such that $(A,*') \cong \prod_p (A_p, *')$ (prime power size)

$(A,*')$ is supernilpotent

Part 5:

What about the other problems?

Known results

HSP($\underline{A}$)	classification	fin. based	SMP($\underline{A}$)	CEQV($\underline{A}$)
Abelian	finite	✓	P	P
CD	finite	✓	P	coNP-c
residually finite	finite [KS '15]	✓ [M '87]	P [BMS '18]	P / coNP-c [IK '18]

Known results

HSP(A)	classification	fin. based	SMP(A)	CEQV(A)
Abelian	finite	✓	P	P
CD	finite	✓	P	coNP-c
residually finite	finite [KS '15]	✓ [M '87]	P [BMS '18]	P / coNP-c [IK '18]
super-nilpotent ⇕	finite (for fixed degree n)	✓ [FM '87]	P [Mayr '12]	P [AM '10]

$\forall i : 0 \approx t(x_1 \dots x_{i-1}, 0, x_{i+1}, \dots x_n) \Rightarrow 0 \approx t(x_1 \dots x_n)$

Known results

HSP(A)	classification	fin. based	SMP(A)	CEQV(A)
Abelian	finite	✓	P	P
CD	finite	✓	P	coNP-c
residually finite	finite [KS '15]	✓ [M '87]	P [BMS '18]	P / coNP-c [IK '18]
super-nilpotent ⇕	finite (for fixed degree n)	✓ [FM '87]	P [Mayr '12]	P [AM '10]

$\forall i : 0 \approx t(x_1 \dots x_{i-1}, 0, x_{i+1}, \dots x_n) \Rightarrow 0 \approx t(x_1 \dots x_n)$

focus on ⇝ (2-)nilpotent, not supernilpotent

2) Axiomatization

Example [Mayr, MK '26]

For a 2-nil. loop $\underline{A} = \mathbb{Z}_q \oplus \mathbb{Z}_p$

$\exists$ unary $f\begin{pmatrix} v \\ e \end{pmatrix} = \begin{pmatrix} 0 \\ \hat{f}(v) \end{pmatrix}$: $Clo(\underline{A}) = Clo(\mathbb{Z}_q \times \mathbb{Z}_p, +, f)$

2) Axiomatization

Example [Mayr, MK '26]

For a 2-nil. loop $\underline{A} = \mathbb{Z}_q \oplus \mathbb{Z}_p$

$\exists$ unary $f\binom{u}{e} = \binom{0}{\hat{f}(u)}$: $Clo(\underline{A}) = Clo(\mathbb{Z}_q \times \mathbb{Z}_p, +, f)$

$\rightsquigarrow$ normal forms of terms $\quad t(\bar{x}) \approx \sum_{i=1}^{n} \alpha_i x_i + \sum_{\gamma} \beta_\gamma f(\sum \gamma_i x_i)$

(1) a finite equational basis of $(\mathbb{Z}_q \times \mathbb{Z}_p, +)$,
(2) $f(x + f(y)) = f(x)$,
(3) $f(x + qy) = f(x)$,
(4) $pf(x) = 0$,
(5) all identities of the form (3.1) $\quad f(cx) \approx \sum_{i=0}^{q-1} \beta_i f(ix)$

equational basis

2) Axiomatization

General strategy for 2-nil. [K, unpublished]

$\underline{A} = \underline{U} \otimes \underline{L}$ is finitely based $\iff$ $\mathrm{Diff}(\underline{A})$ is finitely based as many-sorted algebra

Ex. $(\mathbb{Z}_q, \mathbb{Z}_p, \hat{f})$

2) Axiomatization

General strategy for 2-nil. [K, unpublished]

$\underline{A} = \underline{U} \otimes \underline{L}$ is finitely based $\iff$ $\mathrm{Diff}(\underline{A})$ is finitely based as many-sorted algebra

Ex. $(\mathbb{Z}_q, \mathbb{Z}_p, \hat{f})$

Question: For Abelian $\underline{U}, \underline{L}$:
Is $\mathrm{Diff}(\underline{U} \otimes \underline{L})$ always finitely based?

Suspicion: Failure if $\underline{U}$ is not supernilpotent!

3) Interpolation

Theorem [K'23]

$\underline{A} = \underline{U} \otimes \underline{L}$, $\underline{U}$ Abelian / supernilpotent

$\Rightarrow$ SMP($\underline{A}$) reduces to

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

Input : $\bar{u}_1, \bar{u}_2, \dots, \bar{u}_n \in U^m$

Output: generating set of

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

3) Interpolation

Theorem [K'23]

$\underline{A} = \underline{U} \otimes \underline{L}$, $\underline{U}$ Abelian / supernilpotent

$\Rightarrow$ SMP($\underline{A}$) reduces to

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

Input : $\bar{u}_1, \bar{u}_2, \dots, \bar{u}_n \in U^m$

Output: generating set of

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

Example $\underline{A}_K = \mathbb{Z}_2 \otimes \mathbb{Z}_2$

$Diff(\underline{A}_K) =$

$\{ f \in \mathbb{Z}_2[x_1 \dots x_n], \deg(f) \leq k \}$

$\Downarrow$

compute

$\{ \bar{u}_{i_1} \bar{u}_{i_2} \dots \bar{u}_{i_k} \}$ $\mathcal{O}(n^k)$

3) Interpolation

$\mathrm{SMP}(\mathcal{C})$ $\quad$ $\mathcal{C}$ .. $(\underline{U}, \underline{L})$-clonoid

Input : $\bar{u}_1, \bar{u}_2, \dots, \bar{u}_n \in \underline{U}^m$

Output: Generating set of

$$\{ \hat{f}(\bar{u}_1, \dots, \bar{u}_n) \mid \hat{f} \in \mathcal{C} \} \leq \underline{L}^m$$

New results:

$\mathrm{SMP}(\mathcal{C}) \in \mathrm{P}$ for every ($\underline{U}$ (→ vector space), $\underline{L}$)-clonoid $\mathcal{C}$ [FKR'26]

$\mathrm{SMP}(\mathcal{C}) \in \mathrm{P}$ for every ($\mathbb{Z}_p$, $\underline{L}$)-clonoid $\mathcal{C}$

[ongoing work]

⇒ Patrick Wyme's talk!

4) Equivalence

$CEQV(\underline{A})$ circuit equivalence problem

Input: $\underline{A}$-circuits t, s
Question: Does $\underline{A} \models t \approx s$?

$Cl_0(\underline{A}) \leq Cl_0(\underline{A}')$

$\Rightarrow CEQV(\underline{A}) \leq_p CEQV(\underline{A}')$

For $\underline{A} = \underline{L}_1 \oplus \dots \oplus \underline{L}_k$ $\quad CEQV(\underline{A}) \leq CEQV(\underline{A}, +, 0, -)$

Aschinger's extension

4) Equivalence

$CEQV(\underline{A})$ circuit equivalence problem

Input: $\underline{A}$-circuits t, s
Question: Does $\underline{A} \models t \approx s$?

$Clo(\underline{A}) \subseteq Clo(\underline{A}')$
$\Rightarrow CEQV(\underline{A}) \leq_p CEQV(\underline{A}')$

For $\underline{A} = \underline{L}_1 \oplus \cdots \oplus \underline{L}_k$ $\quad CEQV(\underline{A}) \leq CEQV(\underline{A}, +, 0, -)$
Aichinger's extension

Theorem [KKK '24]

$CEQV(\underline{A}) \in P$ if $\underline{A}$ 2-nilpotent. (normal form)

4) Equivalence

$CEQV(\underline{A})$ circuit equivalence problem

Input: $\underline{A}$-circuits t, s
Question: Does $\underline{A} \models t \approx s$?

$Clo(\underline{A}) \leq Clo(\underline{A}') \Rightarrow CEQV(\underline{A}) \leq_p CEQV(\underline{A}')$

For $\underline{A} = \underline{L}_1 \oplus \dots \oplus \underline{L}_k$ $\quad CEQV(\underline{A}) \leq CEQV(\underline{A}, +, 0, -)$
Aichinger's extension

Theorem [KKK '24]
$CEQV(\underline{A}) \in P$ if $\underline{A}$ 2-nilpotent. (normal form)

Theorem [K '22] If (*) then
$CEQV(\underline{A})$ solvable in $\mathcal{O}(n^{(\log n)^d})$

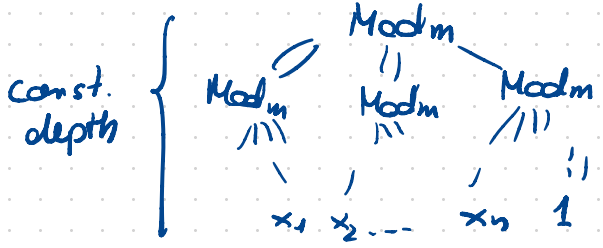
test $t(\bar{x}) = s(\bar{x})$ for all tuples
$\bar{x} = (00\dots0x_1 0\dots x_2 0\dots)$
$\mathcal{O}((\log n)^d)$

4) Equivalence

Theorem [K '22] If (*) then

CEQV ($\underline{A}$) solvable in $\mathcal{O}(n^{(\log n)^d})$

(*) **conjecture**: CC-circuits over $\{0,1\}$:



need size $\Omega(2^{n^d})$ to compute $x_1 \wedge x_2 \wedge \dots \wedge x_n$

(and therefore all $f: \{0,1\}^n \to \{0,1\}$)

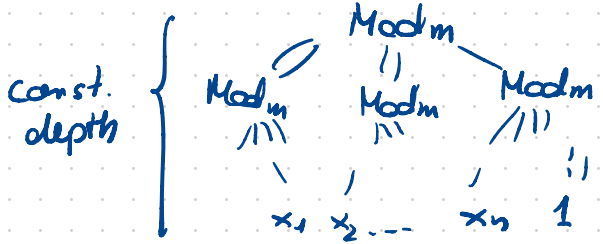
Non-uniform circuit complexity for general $\underline{A}$ → Piotr kawalek talk!

4) Equivalence

Theorem [K '22] If (*) then

CEQV($\underline{A}$) solvable in $\mathcal{O}(n^{(\log n)^d})$

(*) **conjecture**: CC-circuits over $\{0,1\}^*$:



need size $\Omega(2^{n^d})$ to compute $x_1 \wedge x_2 \wedge \dots \wedge x_n$

(and therefore all $f: \{0,1\}^n \to \{0,1\}$)

Non-uniform circuit complexity for general $\underline{A}$ → Piotr kawałek talk!

Theorem [IKK'20] Assuming ETH $\exists\, \underline{A} = \mathbb{Z}_{p_1} \oplus \mathbb{Z}_{p_2} \otimes \dots \otimes \mathbb{Z}_{p_k}$

CEQV($\underline{A}$) needs $\Omega(2^{(g(n))^k})$

4) Equivalence

Summary: For $\underline{A}$ Mal'cev (or from CM variety)

$\mathrm{CEQV}(\underline{A}) \in \mathrm{P}$ if $\underline{A}$ supernilpotent [AM '10]
2-nilpotent [KKK '24]

$\mathrm{CEQV}(\underline{A}) \in \mathrm{coNP\text{-}c}$ if $\underline{A}$ not nilpotent [IKK '16, ...]

under (*), ETH

$\mathrm{CEQV}(\underline{A}) \in \mathrm{QP} \setminus \mathrm{P}$ for some nilpotent $\underline{A}$ [IKK '20, K '22]

4) Equivalence

Summary: For $\underline{A}$ Mal'cev (or from CM variety)

CEQV $(\underline{A}) \in$ P if $\underline{A}$ supernilpotent [AM '10]
2-nilpotent [KKK '24]

CEQV $(\underline{A}) \in$ coNP-c if $\underline{A}$ not nilpotent [IKK '16, ...]

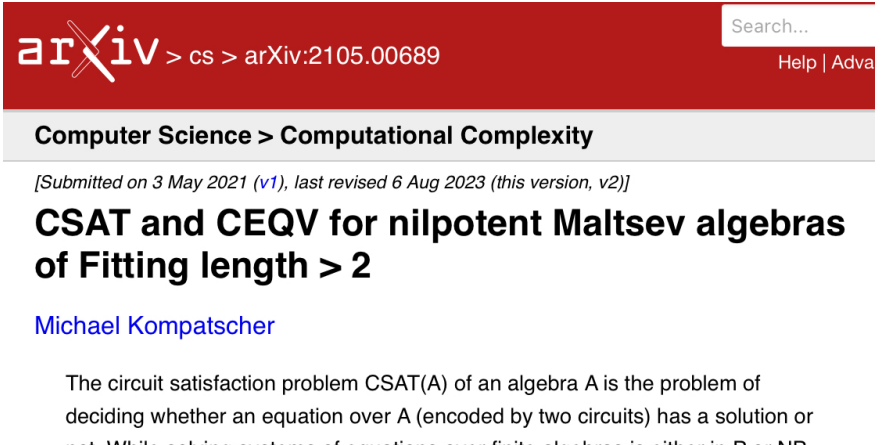
under (*), ETH

CEQV $(\underline{A}) \in$ QP \ P for some nilpotent $\underline{A}$ [IKK '20, K '22]

To fix: CEQV $(\underline{A}) \in$ QP \ P for nilpotent $\underline{A}$ of Hiring length $n \geq 3$

$\exists$ series $1 = \alpha_1 \geq \dots \geq \alpha_n = 0_{\underline{A}}$ s.t. α_i / α_{i+1} supernilpotent

4) Equivalence



contains some gaps / wishful thinking!

What's next ?

What's next ?

13:10 to 14:10	LUNCH			
14:10-14:30		AAA Communications		
14:30 to 15:25		**Michael Kompatscher** Chair: ~~Ross Willard~~		
15:30 to 15:55		**Patrick Wynne** Chair: Stefano Fioravanti	**Piotr Kawałek** Chair: Žaneta Semanišinová	**Pham Ngoc Anh** Chair: Stefan Veldsman
16 to 16:25		**Peter Mayr** Chair: Stefano Fioravanti	**Paul Winkler** Chair: Žaneta Semanišinová	**Heghine Ghumashyan** Chair: Stefan Veldsman
16:30 to 17	Coffee break			
17 to 17:25		**Andrew Moorhead** Chair: Petar Marković	**Juraj Hirjak** Chair: Samir Zahirović	**Chun-Yu Lin** Chair: Ganna Kudryavtseva

Thank you
for your attention!