Supernilpotent reducts of nilpotent algebras

Peter Mayr

June 24, 2022

Mathematics
UNIVERSITY OF COLORADO **BOULDER**

A is a **Mal'cev algebra** if it has a term $m(x, y, z)$ such that $m(x, x, y) = m(y, x, x) = y$.
Examples: (expansions of) groups, loops with $m(x, y, z) = (x/y)z$

Definition

1. **A** is **nilpotent** if $[.[[1, 1], 1], \dots, 1] = 0$ for some iteration of the binary commutator.
2. **A** is **supernilpotent** if $[1, \dots, 1] = 0$ for some **higher commutator**.

Theorem (Aichinger, Mudrinski 2010)

TFAE for a finite Mal'cev algebra **A** of finite type:

1. **A** is supernilpotent;
2. **A** is nilpotent and a direct product of prime power order algebras.

For groups: nilpotent = supernilpotent

Supernilpotence is super

Theorem

Every finite supernilpotent Mal'cev algebra of finite type has ...

1. a **finite basis** for its equational theory (Vaughan–Lee 1983, Freese, McKenzie 1987);
2. **subpower membership problem** in P (M 2012);
3. **polynomial equation/circuit satisfiability** in P (Kompatscher 2018, Idziak, Krzaczkowski 2018).

Proofs are syntactic and use that supernilpotent **A** has a bound on the arity of commutator terms.

Open

Is 'super' necessary in 1 , 2 ?

Nilpotent $\neq$ supernilpotent

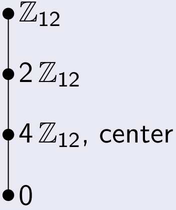
Example (Vaughan–Lee 1983)

Let $\mathbf{L} := (\mathbb{Z}_{12}, x + y + t(x,y))$ with

$$t(x,y) := \begin{cases} 4 & \text{if } (x,y) \equiv_4 (1,3), (3,1), \\ 0 & \text{else.} \end{cases}$$

	0	2	1	3
0				
2				
1				4
3			4	

L is a loop with normal subloops



L is nilpotent but not supernilpotent.

Main results

(A, T) is a (polynomial) reduct of $\mathbf{A} = (A, F)$ if T is a set of (polynomial) term functions of $\mathbf{A}$.

Theorem (Kompatscher, M, Wynne 2022)

Every finite nilpotent loop has a supernilpotent loop reduct.

Corollary (Kompatscher, M, Wynne 2022)

Every finite nilpotent Mal'cev algebra has a polynomial reduct that is supernilpotent and Mal'cev.

$x * y := m(x, 0, y)$ is a loop multiplication for $\mathbf{A}$ nilpotent, $0 \in A$.

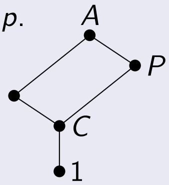
Loops

Main Lemma

Let p be a prime and $\mathbf{A}$ a finite loop with central subloop C of p-power order and $\mathbf{A}/C$ supernilpotent.
Then $\mathbf{A}$ has a normal subloop P with $|P|$ a p-power, $|\mathbf{A}/P|$ coprime to p, and a supernilpotent reduct isomorphic to $\mathbf{P} \times \mathbf{A}/P$.

Proof.

1. $\mathbf{A}/C \cong \mathbf{U} \times \mathbf{V}$ for $|U|$ a p-power and $|V|$ coprime to p.
2. Let $P \trianglelefteq \mathbf{A}$ such that $\mathbf{A}/P = \mathbf{V}$.
   $|P| = |C||U|$ is the maximal p-power dividing $|A|$.



Proof, continued.

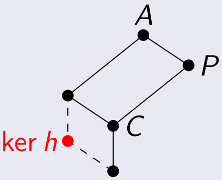
3. Since **P** and **A**$/P$ are coprime, there exists $n \geq 1$ such that

$$x^n := \underbrace{(.(xx)x \ldots)x}_{n \text{ times}} = x \text{ for all } x \in P, \quad x^n \in P \text{ for all } x \in A.$$

4. $h\colon A \to A,\ x \mapsto x^n$, is a homomorphism on $\mathbf{A}' := (A, *)$ with

$$x * y := (xy) \,/\, [(xy)^n/(x^n y^n)].$$

5. Since $h(\mathbf{A}') = \mathbf{P}$ and $\mathbf{A}'/P = \mathbf{A}/P$ are coprime quotients of $\mathbf{A}'$, $\mathbf{A}' \cong \mathbf{P} \times \mathbf{A}/P$ is supernilpotent.



□

Example

Vaughan–Lee's loop **L** is an extension of $P = C \cong (\mathbb{Z}_3 +)$ by $(\mathbb{Z}_4, +)$, hence has a reduct isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_4$, in fact $* = +$ on $\mathbb{Z}_{12}$.

Proving the main result

Main Lemma

Let $\mathbf{A}$ be a finite loop with central subloop C of prime power order and $\mathbf{A}/C$ supernilpotent. Then $\mathbf{A}$ has a supernilpotent loop reduct.

Theorem

Every finite nilpotent loop $\mathbf{A}$ has a supernilpotent loop reduct.

Proof.

Use the Main Lemma inductively down a central series of $\mathbf{A}$ with factors of prime power order. □

Normal forms for term functions of Vaughan–Lee's loop **L**

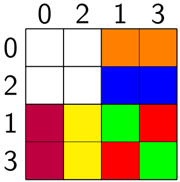
$\mathrm{Clo}(\mathbf{A})$ ... clone of term functions of an algebra **A**

Lemma (M, 2022)

$\mathrm{Clo}_k(\mathbf{L}) = \mathrm{Clo}_k(\mathbb{Z}_{12}, +) \oplus W_k$ for

$$W_k := \{w\colon \mathbb{Z}_{12}^k \to 4\,\mathbb{Z}_{12} \mid \begin{array}{l} w(2\,\mathbb{Z}_{12}^k) = 0, \\ w(x + 4\,\mathbb{Z}_{12}^k) = w(x), \\ w(x) = w(-x) \text{ for all } x \in \mathbb{Z}_{12}^k \end{array} \}.$$

W_2 = functions that are constant with values $\{0, 4, 8\}$ on any colored line segment, 0 else



Note

$W := \bigcup_{k \in \mathbb{N}} W_k$ is a set of finitary functions from $\mathbb{Z}_{12}$ to $4\,\mathbb{Z}_{12}$ that is closed under $+$ on domain and codomain.

W is no clone but a **clonoid** (→ P. Wynne's talk).

Subpower membership for Vaughan–Lee's loop **L**

SMP(A)

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

Question: Is $b \in \langle a_1, \ldots, a_k \rangle \leq \mathbf{A}^n$?

$\mathrm{SMP}(\mathbf{A})$ is in EXPTIME for any finite **A**.

Theorem (M, 2022)

$\mathrm{SMP}(\mathbf{L})$ is in P.

Proof.

1. $b \in \langle a_1, \ldots, a_k \rangle$ iff $b = f(a_1, \ldots, a_k)$ for some $f \in \mathrm{Clo}_k(\mathbf{L})$.
2. The additive normal form of term functions of **L** yields a polytime reduction of $\mathrm{SMP}(\mathbf{L})$ to $\mathrm{SMP}(\mathbb{Z}_{12}, +)$. □

Finite basis for Vaughan–Lee's loop **L**

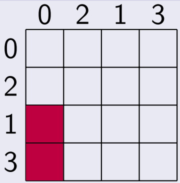
Theorem (M, 2022)

L is finitely based.

Proof.

1. **L** is term equivalent to $\mathbf{A} := (\mathbb{Z}_{12}, +, f)$ for

$$f(x, y) := \begin{cases} 4 & \text{if } x \equiv_4 1, 3, \ \ y \equiv_4 0, \\ 0 & \text{else.} \end{cases}$$



2. **L** is finitely based iff **A** is finitely based.

Proof, continued

3. Every term s of $\mathbf{A}$ can be transformed into a unique normal form s_0 using the identities of $(\mathbb{Z}_{12}, +)$ and
    1. $f(x + 2u, y + 4v) \approx f(x, y)$
    2. $3f(x, y) \approx 0$
    3. $f(0, y) \approx 0$
    4. $f(x + y, z) \approx$
       $f(x, 2x + 2y + 2z) + f(x, 2y + z) - f(x, 2y) + f(x, 2z) + f(y, z)$
    5. $f(x, 2x + y) \approx f(x, 2y) - f(x, y)$
    6. $f(x, 2y + z) \approx f(x, z) - f(y, z) + f(y, 2x + z)$
4. $\mathbf{A}$ satisfies $s \approx t$ iff $s_0 = t_0$.
5. Hence the identities above are a finite basis for $\mathbf{A}$. □

Advertisements

More about . . .

- clonoids ($\to$ P. Wynne's talk)
- nilpotent algebras ($\to$ M. Kompatscher's talk)