Clonoids and Nilpotent Algebras

Patrick Wynne
Joint work with Peter Mayr

University of Colorado Boulder
PALS 2023, Boulder, CO

October 24, 2023

Function Class Composition

A, B, C nonempty sets

$f\colon B^n \to C,\ g_1, \ldots, g_n\colon A^m \to B.$

The composition $f(g_1, \ldots, g_n)\colon A^m \to C$ is given by

$$f(g_1, \ldots, g_n)(\mathbf{x}) = f(g_1(\mathbf{x}), \ldots, g_n(\mathbf{x})).$$

For $F \subseteq \bigcup_{n\in\mathbb{N}} C^{B^n}$ and $K \subseteq \bigcup_{n\in\mathbb{N}} B^{A^n}$, we define the composition FK by

$$FK = \{f(g_1, \ldots, g_n) \ : \ n, m \in \mathbb{N}, f \in F^{(n)}, g_1, \ldots, g_n \in K^{(m)}\}.$$

For $D \subseteq \bigcup_{n\in\mathbb{N}} A^{A^n}$, we say D is a clone on A if $J_A \subseteq D$ and $DD \subseteq D$.

Algebras and Clones

$\mathbb{A}$ algebra, $g_1, g_2, \ldots$ basic operations, $g_i : A^{n_i} \to A$.
Form *term functions* via composition of basic operations:

$$h : A^k \to A$$

$$h(x_1, \ldots, x_k) = f(g_1(x_1, \ldots, x_k), \ldots, g_n(x_1, \ldots, x_k))$$

$\mathrm{Clo}(\mathbb{A})$ is the *clone* of term functions of the algebra $\mathbb{A}$.

Example: $\mathbb{A} = (\mathbb{F}^n,\ +, -, 0, \mathbb{F})$

$$\mathrm{Clo}(\mathbb{A}) = \{\alpha_1 x_1 + \ldots + \alpha_k x_k \ : \ k \in \mathbb{N}, \alpha_1, \ldots, \alpha_k \in \mathbb{F}\}.$$

Example: $\mathbb{B} = (\mathbb{Z},\ +, -, 0, \cdot, 1)$

$$\mathrm{Clo}(\mathbb{B}) = \mathbb{Z}[x_1, x_2, \ldots]$$

Clonoids

Clonoid

For $C \subseteq \bigcup_{n \in \mathbb{N}} B^{A^n}$ we say that C is a **clonoid** from algebra $\mathbb{A}$ to algebra $\mathbb{B}$ if

$$C\,\mathrm{Clo}(\mathbb{A}) \subseteq C \qquad \& \qquad \mathrm{Clo}(\mathbb{B})C \subseteq C$$

- C is closed under precomposition with term functions of $\mathbb{A}$, and
- C is closed under postcomposition with term functions of $\mathbb{B}$;

Example: $\mathbb{A} = (\mathbb{Z}_3, +, -, 0)$, $\mathbb{B} = (\{0,1\}, \wedge, \vee)$, C clonoid from $\mathbb{A}$ to $\mathbb{B}$. If $f : A^2 \to B$ is in C then

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

$$\text{and so} \quad g(x_1, x_2, x_3) = f(x_1 + x_2, 0) \wedge f(2x_1, 2x_2 + x_3) \in C.$$

Notation: $\langle f \rangle$ is the clonoid from $\mathbb{A}$ to $\mathbb{B}$ generated by $f : A^k \to B$.

Polymorphisms and Clonoids

Clones are determined by relations via the Pol – Inv Galois connection. Clonoids are determined by pairs of relations.

Definition

For $R \subseteq A^n, S \subseteq B^n$, let

$$\mathrm{Pol}(R, S) = \bigcup_{k \in \mathbb{N}} \{f \colon A^k \to B \mid f(R, \ldots, R) \subseteq S\}$$

denote the set of **polymorphisms** of the relational pair (R, S).

Theorem (Couceiro, Foldes 2009)

Let $\mathbb{A}$ and $\mathbb{B}$ be algebras with $|A|$ finite. Let $C \subseteq \bigcup_{n \in \mathbb{N}} B^{A^n}$. The following are equivalent.

1. C is a clonoid from $\mathbb{A}$ to $\mathbb{B}$.
2. $C = \bigcap_{i \in I} \mathrm{Pol}(R_i, S_i)$ where $R_i \leq \mathbb{A}^{m_i}, S_i \leq \mathbb{B}^{m_i}$ are subalgebras.

Example:

- $\mathbb{A} = (\mathbb{Z}_9, +)$ $\qquad$ $\mathbb{B} = (\mathbb{Z}_2, +)$
- $\text{Pol}(3\mathbb{Z}_9, 0)$ is the clonoid of functions from $\mathbb{A}$ to $\mathbb{B}$ that are constant zero on $3\mathbb{Z}_9$.

Example:

- $\mathbb{A} = (\mathbb{Z}_9, +)$ $\qquad$ $\mathbb{B} = (\mathbb{Z}_2, +)$
- $\text{Pol}(\equiv_3, =)$ is the clonoid of functions from $\mathbb{Z}_9$ to $\mathbb{Z}_2$ that are constant on blocks modulo 3.

Clonoids from $\mathbb{A}$ to $\mathbb{B}$ form a lattice, $\mathcal{L}(\mathbb{A}, \mathbb{B})$, with

$$C \wedge D = C \cap D \text{ and } C \vee D = \langle C \cup D \rangle.$$

An upper bound on the number of clonoids

In some cases, we need just one relational pair to determine a clonoid.

Theorem (Aichinger, Mayr 2018)

If $\mathbb{A}$ is a finite algebra and $\mathbb{B}$ is a finite Mal'cev algebra then clonoids from $\mathbb{A}$ to $\mathbb{B}$ are finitely related (i.e. determined by a single relational pair).

Since modules are Mal'cev algebras (with Mal'cev term $x - y + z$),

Upper Bound

If $\mathbb{A}$ and $\mathbb{B}$ are finite modules then the lattice of clonoids from $\mathbb{A}$ to $\mathbb{B}$ is countable.

Obtaining the upper bound

Theorem (Mayr, W. 2023)

Let $\mathbb{A}$ and $\mathbb{B}$ be finite modules whose orders are not coprime. Then the lattice of clonoids from $\mathbb{A}$ to $\mathbb{B}$ is countably infinite, and not all clonoids are finitely generated.

Proof idea:

- Let p be a prime and $\mathbb{A} = (\mathbb{Z}_p, ; +) = \mathbb{B}$.
- For $n \in \mathbb{N}$ let $f_n(x_1, \ldots, x_n) = x_1 \cdot x_2 \cdot \ldots \cdot x_n$.
- Then $\langle f_1 \rangle \subsetneq \langle f_1, f_2 \rangle \subsetneq \langle f_1, f_2, f_3 \rangle \subsetneq \cdots$.
- f_n is zero-absorbing. If some $x_i = 0$ then $f_n(x_1, \ldots, x_n) = 0$.
- But the only zero-absorbing functions in $\langle f_1, \ldots, f_n \rangle$ of arity greater than n are the constant zero functions.

Upper bound not attained

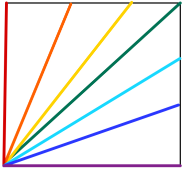
Theorem (Fioravanti, 2020)

Let p be a prime, $\mathbb{A} = (\mathbb{Z}_p, +)$ and let $\mathbb{B}$ be a finite abelian group with order coprime to p. Then every clonoid from $\mathbb{A}$ to $\mathbb{B}$ is generated by its unary functions.

Proof idea:

- $f : \mathbb{Z}_p^k \to \mathbb{Z}_q$ can be interpolated on lines in $\mathbb{Z}_p^k$ passing through $\mathbf{0}$.
- For $v \in \mathbb{Z}_p^k$, unary functions generated by f generate $f_v : \mathbb{Z}_p^k \to \mathbb{Z}_q$,

$$f_v(x) = \begin{cases} f(x) & \text{if } x \in \text{span}(v) \\ 0 & \text{otherwise .} \end{cases}$$



- $f = \sum f_v$ for v's generating distinct lines.

Modules of Coprime Order

Question

Given $\mathbb{A}$ and $\mathbb{B}$ finite modules of coprime order, is the lattice of clonoids from $\mathbb{A}$ to $\mathbb{B}$ finite?

A partial answer...

A module is distributive if its submodule lattice is a distributive lattice.

Theorem (Mayr, W. 2023)

Let $\mathbb{A}$ be a finite distributive $\mathbf{R}$-module, and let $\mathbb{B}$ be a finite $\mathbf{S}$ module such that $|A|$ and $|B|$ are coprime. Let n be the nilpotence degree of the Jacobson radical of $\mathbf{R}$.

- Every clonoid from $\mathbb{A}$ to $\mathbb{B}$ is generated by its subset of n-ary functions.
- $\mathcal{L}(\mathbb{A}, \mathbb{B})$ is finite.

Example

$$\mathbb{A} = (\mathbb{Z}_2, +), \;\; \mathbb{B} = (\mathbb{Z}_3, +), \qquad f : (\mathbb{Z}_2)^2 \to \mathbb{Z}_3$$

- f is generated by its unary minors.
- Unary minors of f include $f(x,x), f(0,x), f(x,0),$ and $f(0,0)$.

$$\begin{aligned} f(x_1,x_2) = & f(0,0) \\ & + 2^{-1}[f(x_1,0) + f(x_1+x_2,0) - f(0,0) - f(x_2,0) \\ & + f(0,x_2) + f(0,x_1+x_2) - f(0,0) - f(0,x_1) \\ & + f(x_1,x_1) + f(x_2,x_2) - f(0,0) - f(x_1+x_2,x_1+x_2)]. \end{aligned}$$

Note that this formula holds independently of the choice of f.

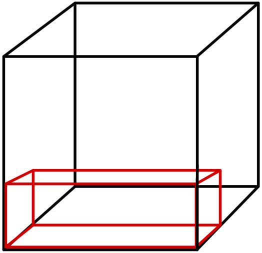
Theorem (Mayr, W. 2023)

Let $\mathbb{A} = (\mathbb{Z}_{p^n}, +)$ for a prime p and $n \geq 1$. Let $\mathbb{B}$ be a finite abelian group with order coprime to p. Then every clonoid from $\mathbb{A}$ to $\mathbb{B}$ is generated by its subset of n-ary functions.

Proof idea: For $f : A^k \to B$, we show f is generated by its n-ary *minors*.

- Reduce to the case that $f(p\mathbb{A}, p\mathbb{A}, \ldots, p\mathbb{A}) = 0$.
- n-ary minors of f generate $f' : A^k \to B$,

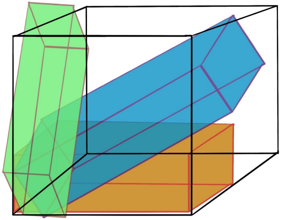
$$f'(x) = \begin{cases} f(x) & \text{if } x \in A \times (pA)^{k-1}, \\ 0 & \text{else.} \end{cases}$$



- Let $N \leq \mathbb{A}^k$ such that $(pA)^k \leq N$ and $N/pA^k \cong \mathbb{A}/pA$.
- Interpolate f on N.
- n-ary minors of f generate $f_N : A^k \to B$,

$$f_N(x) = \begin{cases} f(x) & \text{if } x \in N, \\ 0 & \text{else.} \end{cases}$$

- Cover A^k by subgroups of this form.



- Then $f = \sum_N f_N$.

Uniform Generation

For ring $\mathbf{R}$ and $r \in R^{k \times k}$, we define the inner rank of r as the least ℓ such that the right $\mathbf{R}$-submodule of R^k that is generated by the columns of r is contained in an ℓ-generated module.

Lemma (Mayr, W. 2023)

Let $\mathbb{A}$ be a finite distributive $\mathbf{R}$-module, and let $\mathbb{B}$ be a finite $\mathbf{S}$-module such that $|A|$ and $|B|$ are coprime. Let n be the nilpotence degree of the Jacobson radical of $\mathbf{R}$.
For all $k \in \mathbb{N}$ there exists $s\colon \{r \in R^{k \times k} \;:\; \operatorname{rank}(r) \leq n\} \to S$ such that for all $f\colon A^k \to B$ and all $x \in A^k$

$$f(x) = \sum_{r \in R^{k \times k}, \operatorname{rank}(r) \leq n} s(r) f(rx).$$

For $k \in \mathbb{N}$, the set $\{f\colon A^k \to B\}$ is *uniformly generated* by n-ary minors.

From Modules to Abelian Mal'cev Algebras

$\mathbb{A}$ algebra with Mal'cev term $m(x,y,z)$.
$\mathbb{A}$ is abelian if $[1_{\mathbb{A}}, 1_{\mathbb{A}}] = 0_{\mathbb{A}}$.

Theorem (Herrmann, 1979)

An algebra $\mathbb{A}$ in a congruence modular variety is abelian if and only if $\mathbb{A}$ is polynomially equivalent to a module over a ring.

- Ring: $\mathbf{R}_{\mathbb{A}} := \{r \in \mathrm{Clo}(\mathbb{A})^{(2)} \ : \ r(z,z) = z \ \forall z \in A\}$.

$$r(x,z) + s(x,z) := m(r(x,z), z, s(x,z)),$$
$$-r(x,z) := m(z, r(x,z), z)$$
$$r(x,z) \cdot s(x,z) := r(s(x,z), z)$$

  Neutral elements z, x for $+$ and $\cdot$ respectively.
- Addition: $a + b := m(a, 0, b), \quad -a := m(0, a, 0)$ for fixed $0 \in A$
- Scalar Multiplication: $ra := r(a, 0)$

Clonoids Between Abelian Mal'cev Algebras

We extend our main theorem from modules to Abelian Mal'cev algebras.

Theorem (Mayr, W. 2023)

Let $\mathbb{A}$ be polynomially equivalent to a finite distributive $\mathbf{R}_{\mathbb{A}}$-module and $\mathbb{B}$ polynomially equivalent to a finite $\mathbf{R}_{\mathbb{B}}$-module such that $|A|$ and $|B|$ are coprime. Let n be the nilpotence degree of the Jacobson radical of $\mathbf{R}_{\mathbb{A}}$.

- Every clonoid from $\mathbb{A}$ to $\mathbb{B}$ is generated by its $(n+1)$-ary functions.
- $\mathcal{L}(\mathbb{A}, \mathbb{B})$ is finite.

Change from n to $n+1$ due to extra variable in place of constant.

Uniform Generation

Like in the module case, functions from $\mathbb{A}$ to $\mathbb{B}$ are uniformly generated.

Lemma (Mayr, W. 2023)

For all $k \in \mathbb{N}$ there exists $s\colon \{r \in R_{\mathbb{A}}^{k\times k} \ : \ \text{rank}(r) \leq n\} \to R_{\mathbb{B}}$ such that for all $f, b\colon A^{k+1} \to B$ and all $x \in A^k, z \in A$

$$f(x,z) = \sum_{r \in R_{\mathbb{A}}^{k\times k}, \text{rank}(r) \leq n} s(r) *_{b(x,z)} f(r *_z x, z)$$

where the sum is taken pointwise with respect to $+_{b(x,z)}$ in $\mathbb{B}$.

Central Extensions

Denote the center of an algebra $\mathbb{A}$ in a congruence modular variety by $\zeta_{\mathbb{A}}$.
$\zeta_{\mathbb{A}}$ is the largest congruence α on $\mathbb{A}$ such that $[\alpha, 1_{\mathbb{A}}] = 0_{\mathbb{A}}$.

Theorem (Freese & McKenzie, 1987)

For an algebra $\mathbb{A}$ in a congruence modular variety $\mathcal{V}$, let $\mathbb{U} = \mathbb{A}/\zeta_{\mathbb{A}}$.
There exists an abelian algebra $\mathbb{L} \in \mathcal{V}$ such that $\mathbb{A} \cong \mathbb{L} \otimes \mathbb{U}$.

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

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

where $\hat{f} : U^k \to L$.
We call $\mathbb{L} \otimes \mathbb{U}$ a central extension of $\mathbb{L}$ by $\mathbb{U}$.

For central extension $\mathbb{L} \otimes \mathbb{U}$, every k-ary term is of the form

$$t^{\mathbb{L}\otimes\mathbb{U}}(\ell, u) = (t^{\mathbb{L}}(\ell) + \hat{t}(u), t^{\mathbb{U}}(u)),$$

for some $\hat{t}\colon L^k \to U$.
Example: $\mathbb{L} \times \mathbb{U}$ is a central extension of $\mathbb{L}$ by $\mathbb{U}$ with $\hat{t} = 0$ for all terms t.
We compare arbitrary central extensions to the direct product.

Lemma (Mayr, W. 2023)

For $\mathbb{L} \otimes \mathbb{U}$ in a congruence modular variety, with $0 \in L$ such that $\{0\} \leq \mathbb{L}$,

$$\xi\colon \mathrm{Clo}(\mathbb{L} \otimes \mathbb{U}) \to \mathrm{Clo}(\mathbb{L} \times \mathbb{U}),\ f^{\mathbb{L}\otimes\mathbb{U}} \mapsto f^{\mathbb{L}\times\mathbb{U}}.$$

is a surjective clone homomorphism.
Moreover, ξ is injective if and only if $\mathbb{L} \otimes \mathbb{U} \cong \mathbb{L} \times \mathbb{U}$.

Difference Clonoid

We define the *difference clonoid* of a central extension to capture the situation where ξ is not injective.

Difference Clonoid

$$D(\mathbb{L}\otimes\mathbb{U}) := \{e\colon U^k \to L \ :\ (x_1^{\mathbb{L}} + e(u_1, \ldots, u_k),\ x_1^{\mathbb{U}}) \in \mathrm{Clo}_k(\mathbb{L}\otimes\mathbb{U}), k \in \mathbb{N}\}.$$

- $D(\mathbb{L} \otimes \mathbb{U})$ is a clonoid from $\mathbb{U}$ to $\mathbb{L}$.
- $f + e \in \mathrm{Clo}(\mathbb{L} \otimes \mathbb{U})$ for all $f \in \mathrm{Clo}(\mathbb{L} \otimes \mathbb{U})$ and $e \in D(\mathbb{L} \otimes \mathbb{U})$.
- $(f, f + e) \in \ker \xi$ for all $f \in \mathrm{Clo}(\mathbb{L} \otimes \mathbb{U})$ and $e \in D(\mathbb{L} \otimes \mathbb{U})$.

Here, $(f + e)(\ell, u) = (f^{\mathbb{L}}(\ell) + \hat{f}(u) + e(u), f^{\mathbb{U}}(u))$.

Generators of Term Clones

Theorem (Mayr, W. 2023)

Let $\mathcal{V}$ be a CM variety with difference term d and $\mathbb{L} \otimes \mathbb{U} \in \mathcal{V}$.

- Let $G \subseteq \mathrm{Clo}(\mathbb{L} \otimes \mathbb{U})$ such that $\xi(G)$ generates $\mathrm{Clo}(\mathbb{L} \times \mathbb{U})$.
- Let E be a generating set of the clonoid $D(\mathbb{L} \otimes \mathbb{U})$.

Then

$$\mathrm{Clo}(\mathbb{L} \otimes \mathbb{U}) = \langle \{d^{\mathbb{L} \otimes \mathbb{U}}\} \cup G \cup x_1 + E \rangle.$$

$\mathbb{L} \in \mathcal{V}$ abelian implies $\mathbb{L}$ is term equivalent to an algebra with basic operations of arity at most 3,
i.e. $\mathrm{Clo}(\mathbb{L})$ is generated by ternary functions.
If $\mathbb{U} \in \mathcal{V}$ is also abelian, $\mathrm{Clo}(\mathbb{L} \times \mathbb{U})$ is generated by ternary functions.
We investigate this case next.

Number of Nilpotent Mal'cev Algebras

For $\mathbb{A} \in \mathcal{V}$ a congruence modular variety, $\mathbb{A}$ is 2-nilpotent if

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

Theorem (Freese & McKenzie, 1987)

An algebra $\mathbb{A}$ in a congruence modular variety is 2-nilpotent if and only if $\mathbb{A} \cong \mathbb{L} \otimes \mathbb{U}$ for abelian algebras $\mathbb{L}$ and $\mathbb{U}$.

Theorem (Mayr, W. 2023)

Let $\mathbb{L} \otimes \mathbb{U}$ be a finite 2-nilpotent algebra in a congruence modular variety.

- If $D(\mathbb{L} \otimes \mathbb{U})$ is finitely generated then $\mathrm{Clo}(\mathbb{L} \otimes \mathbb{U})$ is finitely generated.
- If $|L|$ and $|U|$ are coprime and $\mathbb{U}$ is polynomially equivalent to a distributive module over a ring whose Jacobson radical has nilpotence degree n then $\mathrm{Clo}(\mathbb{L} \otimes \mathbb{U})$ is generated by its functions of arity $\max(3, n+1)$.

Theorem (Mayr, W. 2023)

Let $\mathbb{L} \otimes \mathbb{U}$ be a finite 2-nilpotent algebra in a congruence modular variety.

- If $D(\mathbb{L} \otimes \mathbb{U})$ is finitely generated then $\text{Clo}(\mathbb{L} \otimes \mathbb{U})$ is finitely generated.
- If $|L|$ and $|U|$ are coprime and $\mathbb{U}$ is polynomially equivalent to a distributive module over a ring whose Jacobson radical has nilpotence degree n then $\text{Clo}(\mathbb{L} \otimes \mathbb{U})$ is generated by its functions of arity $\max(3, n+1)$.

Proof:

- $\mathbb{L} \otimes \mathbb{U}$ is 2-nilpotent, so $\mathbb{L}$ and $\mathbb{U}$ are abelian.
- Hence $\text{Clo}(\mathbb{L} \times \mathbb{U})$ is generated by its ternary functions.
- If $D(\mathbb{L} \otimes \mathbb{U})$ is finitely generated then $\text{Clo}(\mathbb{L} \otimes \mathbb{U})$ is finitely generated.
- For $\mathbb{U}$ distributive and $|L|, |U|$ coprime, every clonoid from $\mathbb{U}$ to $\mathbb{L}$ is generated by its $(n+1)$-ary functions.

Corollary

Let $m \in \mathbb{N}$ squarefree. The number of 2-nilpotent Mal'cev algebras of order m (up to term equivalence) is finite.

Proof: Let $\mathbb{L} \otimes \mathbb{U}$ be a 2-nilpotent Mal'cev algebra.

- Since m is squarefree, $|L|$ and $|U|$ are coprime.
- $\mathbb{U}$ is abelian and squarefree, so $\mathrm{Con}(\mathbb{U})$ is distributive.
- So $\mathbb{U}$ is polynomially equivalent to a distributive module.
- $\mathrm{Clo}(\mathbb{L} \otimes \mathbb{U})$ is generated by its functions of arity $\max(3, n+1)$.

Corollary

Let $m \in \mathbb{N}$ non-squarefree. The number of 2-nilpotent Mal'cev algebras of order m (up to term equivalence) is infinite.

This result was already known, but can be proven with clonoids as well.

Ongoing Work and Questions

We are on our way to proving...
2-nilpotent Mal'cev algebras of squarefree order

- are finitely based,
- and have tractable Subpower Membership Problem.

Question

Is every clonoid between finite abelian Mal'cev algebras of coprime order finitely generated (i.e. can we drop the distributivity assumption)?

Question

For m squarefree, is the number of k-nilpotent Mal'cev algebras of order m (up to term equivalence) finite for $k > 2$?

This likely requires understanding of clonoids from nilpotent algebras to abelian algebras.

Mayr & Wynne, “Clonoids between modules” Arxiv link

Thanks!