Polynomials and Structure of Universal Algebras

Erhard Aichinger

Department of Algebra
Johannes Kepler University Linz, Austria

January 2012

Polynomials

Definition

$\mathbf{A} = \langle A, F \rangle$ an algebra, $n \in \mathbb{N}$. $\mathrm{Pol}_k(\mathbf{A})$ is the subalgebra of

$$\mathbf{A}^{A^k} = \langle \{f : A^k \to A\}, \text{“}F \text{ pointwise”} \rangle$$

that is generated by

- $(x_1, \ldots, x_k) \mapsto x_i \ (i \in \{1, \ldots, k\})$
- $(x_1, \ldots, x_k) \mapsto a \ (a \in A)$.

Proposition

$\mathbf{A}$ be an algebra, $k \in \mathbb{N}$. Then $\mathbf{p} \in \mathrm{Pol}_k(\mathbf{A})$ iff there exists a term t in the language of $\mathbf{A}$, $\exists m \in \mathbb{N}$, $\exists a_1, a_2, \ldots, a_m \in A$ such that

$$\mathbf{p}(x_1, x_2, \ldots, x_k) = \mathbf{t}^{\mathbf{A}}(a_1, a_2, \ldots, a_m, x_1, x_2, \ldots, x_k)$$

for all $x_1, x_2, \ldots, x_k \in A$.

Function algebras – Clones

$\mathcal{O}(A) := \bigcup_{k \in \mathbb{N}} \{f \mid f : A^k \to A\}$.

Definition of Clone

$\mathcal{C} \subseteq \mathcal{O}(A)$ is a clone on A iff

1. $\forall k, i \in \mathbb{N}$ with $i \leq k$: $\big((x_1, \ldots, x_k) \mapsto x_i\big) \in \mathcal{C}$,
2. $\forall n \in \mathbb{N}, m \in \mathbb{N}, f \in \mathcal{C}^{[n]}, g_1, \ldots, g_n \in \mathcal{C}^{[m]}$:

$$f(g_1, \ldots, g_n) \in \mathcal{C}^{[m]}.$$

$\mathcal{C}^{[n]}$ ... the n-ary functions in $\mathcal{C}$.

$\mathrm{Pol}(\mathbf{A}) := \bigcup_{k \in \mathbb{N}} \mathrm{Pol}_k(\mathbf{A})$ is a clone on A.

Functional Description of Clones

A algebra.

$\mathrm{Pol}(\mathbf{A})$ ... the smallest clone on A that contains all projections, all constant operations, all basic operations of **A**.

$\mathrm{Clo}(\mathbf{A})$ ... the smallest clone on A that contains all projections, and all basic operations of **A** = clone of term functions of **A**.

Clones vs. term functions

Proposition

Every clone is the set of term functions of some algebra.

Proposition

Let $\mathcal{C}$ be a clone on A. Define $\mathbf{A} := \langle A, \mathcal{C} \rangle$. Then $\mathcal{C} = \mathrm{Clo}(\mathbf{A})$.

Definition

A clone is *constantive* or *a polynomial clone* if it contains all unary constant functions.

Proposition

Every constantive clone is the set of polynomial functions of some algebra.

Relational Description of Clones

Definition

I a finite set, $\rho \subseteq A^I$, $f : A^n \to A$. f preserves ρ ($f \rhd \rho$) if $\forall v_1, \ldots, v_n \in \rho$:

$$\langle f(v_1(i), \ldots, v_n(i)) \,|\, i \in I \rangle \in \rho.$$

Remark

$f \rhd \rho \iff \rho$ is a subuniverse of $\langle A, f \rangle^I$.

Definition (Polymorphisms)

Let R be a set of finitary relations on A, $\rho \in R$.

$$\begin{aligned} \mathrm{Polym}(\{\rho\}) &:= \{f \in \mathcal{O}(A) \,|\, f \rhd \rho\}, \\ \mathrm{Polym}(R) &:= \textstyle\bigcap_{\rho \in R} \mathrm{Polym}(\{\rho\}). \end{aligned}$$

Relational Descriptions of Clones

Theorem

Let ρ be a finitary relation on A. Then $\mathrm{Polym}(\{\rho\})$ is a clone.

Theorem (testing clone membership), [Pöschel and Kalužnin, 1979, Folgerung 1.1.18]

Let $\mathcal{C}$ be a clone on A, $n \in \mathbb{N}$, $f : A^n \to A$. The set $\rho := \mathcal{C}^{[n]}$ is a subset of A^{A^n}, hence a relation on A with index set $I := A^n$. Then $f \in \mathcal{C} \iff f \rhd \rho$.

Theorem (testing whether a relation is preserved) [Pöschel and Kalužnin, 1979, Satz 1.1.19]

Let $\mathcal{C}$ be a clone on A, ρ a finitary relation on A with m elements. Then

$$(\forall c \in \mathcal{C} : c \rhd \rho) \iff (\forall c \in \mathcal{C}^{[m]} : c \rhd \rho).$$

Finite Description of Clones

Definition

A clone is finitely generated if it is generated by a finite set of finitary functions.

Definition

A clone $\mathcal{C}$ is finitely related if there is a finite set of finitary relations R with $\mathcal{C} = \mathrm{Polym}(R)$.

Open and probably very hard

Given a finite $F \subseteq \mathcal{O}(A)$ and a finitary relation ρ on A. Decide whether F generates $\mathrm{Polym}(\{\rho\})$.

Mal’cev operations

A a set. A function $d : A^3 \to A$ is a Mal’cev operation if

$$d(a,a,b) = d(b,a,a) = b \text{ for all } a, b \in A.$$

Typical example: $d(x,y,z) := x - y + z$.

An algebra is a *Mal’cev algebra* if it has a Mal’cev operation in its ternary term functions. (Algebra with a Mal’cev term should be used if the notion *Mal’cev algebra* causes confusion.)

A clone is a *Mal’cev clone* if it has a Mal’cev operation in its ternary functions.

Theorem [Mal'cev, 1954]

An algebra **A** is a Mal'cev algebra if for all $\mathbf{B} \in \mathbb{HSP}\,\mathbf{A}$:
$\forall \alpha, \beta \in \operatorname{Con} \mathbf{B} : \alpha \circ \beta = \beta \circ \alpha$.

A characterization of Mal'cev clones

Theorem ([Berman et al., 2010])

Let A be a finite set, $\mathcal{C}$ a clone on A. For $n \in \mathbb{N}$, let

$$i(n) := \max\{|X| \mid X \text{ is an independent subset } of \langle A, \mathcal{C}\rangle^n\}.$$

Then $\mathcal{C}$ is a Mal'cev clone if and only if $\exists \alpha \in \mathbb{N}$ such that

$$\forall n \in \mathbb{N} : i(n) \leq 2^{\alpha n}.$$

Functionally complete algebras

Theorem (cf. [Hagemann and Herrmann, 1982]), forerunner in [Istinger et al., 1979]

Let **A** be a finite algebra, $|A| \geq 2$. Then $\mathrm{Pol}(\mathbf{A}) = \mathcal{O}(\mathbf{A})$ if and only if $\mathrm{Pol}_3(\mathbf{A})$ contains a Mal'cev operation, and **A** is simple and nonabelian.

A is nonabelian iff $[1_A, 1_A] \neq 0_A$. Here, $[.,.]$ is the *term condition commutator*.
This describes finite algebras with

$$\mathrm{Pol}(\mathbf{A}) = \mathrm{Polym}(\emptyset).$$

Affine complete algebras

Definition of affine completeness

An algebra **A** is affine complete if $\mathrm{Pol}(\mathbf{A}) = \mathrm{Polym}(\mathrm{Con}\,(\mathbf{A}))$.

Theorem [Hagemann and Herrmann, 1982, Idziak and Słomczyńska, 2001, Aichinger, 2000]

Let **A** be a finite Mal'cev algebra. Then the following are equivalent:

1. Every $\mathbf{B} \in \mathbb{H}(\mathbf{A})$ is affine complete.
2. For all $\alpha \in \mathrm{Con}\,(\mathbf{A})$, we have $[\alpha, \alpha] = \alpha$.

Open and probably still very hard

Is affine completeness a decidable property of $\mathbf{A} = \langle A, F \rangle$ (of finite type)?

Other concepts of polynomial completeness

Concepts of Polynomial completeness

1. weak polynomial richness:
   [Idziak and Słomczyńska, 2001],
   [Aichinger and Mudrinski, 2009] (expanded groups)
2. polynomial richness: [Idziak and Słomczyńska, 2001],
   [Aichinger and Mudrinski, 2009] (expanded groups)

Conclusion about completeness properties

Completeness provides relations

Completeness results often provide a finite set R of relations on A such that

$$\mathrm{Pol}(\mathbf{A}) = \mathrm{Polym}(R).$$

E.g., for every affine complete algebra, we have

$$\mathrm{Pol}(\mathbf{A}) = \mathrm{Polym}(\mathrm{Con}\,(\mathbf{A})).$$

Polynomially equivalent algebras

Definition

The algebras **A** and **B** are polynomially equivalent if $A = B$ and $\mathrm{Pol}\,(\mathbf{A}) = \mathrm{Pol}\,(\mathbf{B})$.

Task

Classify finite algebras modulo polynomial equivalence.

Task

$\mathbf{A} = \langle A, F \rangle$ algebra.

- Classify all expansions $\langle A, F \cup G \rangle$ of **A** modulo polynomial equivalence.
- Determine all clones $\mathcal{C}$ with $\mathrm{Pol}(\mathbf{A}) \subseteq \mathcal{C} \subseteq \mathcal{O}(A)$.

Polynomially inequivalent expansions

Examples

- $\langle \mathbb{Z}_p, + \rangle$, p prime, has exactly 2 polynomially inequivalent expansions.
- [Aichinger and Mayr, 2007] $\langle \mathbb{Z}_{pq}, + \rangle$, p, q primes, $p \neq q$, has exactly 17 polynomially inequivalent expansions.
- [Mayr, 2008] $\langle \mathbb{Z}_n, + \rangle$, n squarefree, has finitely many polynomially inequivalent expansions.
- [Kaarli and Pixley, 2001] Every finite Mal'cev algebra **A** with $\mathrm{typ}(\mathbf{A}) = \{\mathbf{3}\}$ has finitely many polynomially inequivalent expansions. (Semisimple rings with 1, groups without abelian principal factors)

Finitely many expansions $\Longrightarrow$ finitely related

Proposition, cf. [Pöschel and Kalužnin, 1979, Charakterisierungssatz 4.1.3]

If **A** has only finitely many polynomially inequivalent expansions, $\mathrm{Pol}(\mathbf{A})$ is finitely related.

Examples where $\mathrm{Pol}(\mathbf{A})$ is finitely related

Theorem

$\mathrm{Pol}(\mathbf{A})$ is finitely related for the following algebras:

- expansions of groups of order p^2 (p a prime) [Bulatov, 2002],
- Mal'cev algebras with congruence lattice of height at most 2 [Aichinger and Mudrinski, 2010],
- supernilpotent Mal'cev algebras [Aichinger and Mudrinski, 2010],
- finite groups all of whose Sylow subgroups are abelian [Mayr, 2011],
- finite commutative rings with 1 [Mayr, 2011].

Often, we obtain concrete bounds for the arity of the relations.

Algebras with many expansions

Examples

- [Bulatov, 2002] $\langle Z_p \times \mathbb{Z}_p, +\rangle$, p prime, has countably many polynomially inequivalent expansions.
- [Ágoston et al., 1986] $\langle \{1, 2, 3\}, \emptyset \rangle$ has $2^{\aleph_0}$ many polynomially inequivalent expansions.

Main Questions on Polynomial Equivalence

Question [Bulatov and Idziak, 2003, Problem 8]

- A a finite set. How many polynomially inequivalent Mal'cev algebras are there on A?
- Equivalent question: A finite set. How many clones on A contain all constant operations and a Mal'cev operation?
- *Does there exist a finite set with uncountably many polynomial Mal'cev clones?*

Known before 2009 [Idziak, 1999]

$|A| \leq 3$: finite, $|A| \geq 4$: $\aleph_0 \leq x \leq 2^{\aleph_0}$.

Conjectures on the number of constantive Mal'cev clones

Wild conjecture

On a finite set A , there are at most $\aleph_0$ constantive Mal'cev clones.

Wilder conjecture 1 [Idziak, oral communication, 2006]

For every constantive Mal'cev clone $\mathcal{C}$ on a finite set, there is a finite set of relations R such that $\mathcal{C} = \mathrm{Polym}(R)$.

Wilder conjecture 2

Every Mal'cev clone on a finite set is generated by finitely many functions.

Situation of these conjectures

Situation of these conjectures

Known before August 2009:

- WC 1 $\Rightarrow$ WC, since the number of finite subsets of A^* is countable.
- WC 2 $\Rightarrow$ WC, since the number of finite subsets of $\mathcal{O}(\mathbf{A})$ is countable.
- WC 2 is wrong [Idziak, 1999]
  On $\mathbb{Z}_2 \times \mathbb{Z}_4$, $\mathrm{Polym}(\mathrm{Con}(\langle \mathbb{Z}_2 \times \mathbb{Z}_4, + \rangle))$ is not f.g.

Finitely related Mal'cev clones

Wilder conjecture 1

For every constantive Mal'cev clone $\mathcal{C}$ on a finite set, there is a finite set of relations R such that $\mathcal{C} = \mathrm{Polym}(R)$.

Finite relatedness vs. DCC

Suppose $\mathcal{C}$ is not finitely related. Then there is a sequence of clones

$$\mathcal{C}_1 \supset \mathcal{C}_2 \supset \mathcal{C}_3 \supset \cdots$$

such that $\bigcap_{i \in \mathbb{N}} \mathcal{C}_i = \mathcal{C}$. Hence, it is sufficient for WC 1 to prove:

Claim

The set of Mal'cev clones on a finite set has no infinite descending chains.

How to represent a Mal'cev clone

Example: $\mathcal{C} = \mathrm{Pol}(\langle \mathbb{Z}_2, + \rangle)$.
$c(\mathbf{0}) = 0 \Rightarrow c(\mathbf{x} + \mathbf{y}) = c(\mathbf{x}) + c(\mathbf{y})$.

The ternary functions of this clone

$$\begin{array}{lrcl}
000 & \{c(000) \mid c \in \mathcal{C}\} & = & \{0,1\} \\
001 & \{c(001) \mid c \in \mathcal{C}, c(000) = 0\} & = & \{0,1\} \\
010 & \{c(010) \mid c \in \mathcal{C}, c(000) = c(001) = 0\} & = & \{0,1\} \\
011 & \{c(011) \mid c \in \mathcal{C}, c(000) = c(001) = c(010) = 0\} & = & \{0\} \\
100 & \{c(100) \mid c \in \mathcal{C}, c(000) = \cdots = c(011) = 0\} & = & \{0,1\} \\
101 & \{c(101) \mid c \in \mathcal{C}, c(000) = \cdots = c(100) = 0\} & = & \{0\} \\
110 & \{c(110) \mid c \in \mathcal{C}, c(000) = \cdots = c(101) = 0\} & = & \{0\} \\
111 & \{c(111) \mid c \in \mathcal{C}, c(000) = \cdots = c(110) = 0\} & = & \{0\}
\end{array}$$

Abstract from $\mathbb{Z}_2$:
Clones on $A = \{0, \dots, t-1\}$ with group operation $+$ and neutral element 0:

Splittings at $\mathbf{a}$

For $\mathbf{a} \in A^n$, let

$$\varphi(\mathcal{C}, \mathbf{a}) := \{f(\mathbf{a}) \,|\, f(\mathbf{z}) = 0 \text{ for all } \mathbf{z} \in A^n \text{ with } \mathbf{z} <_{\mathrm{lex}} \mathbf{a}\}.$$

Theorem

Let $\mathcal{C}, \mathcal{D}$ clones on A with $+$ and 0. If $\mathcal{C} \subseteq \mathcal{D}$ and $\varphi(\mathcal{C}, \mathbf{a}) = \varphi(\mathcal{D}, \mathbf{a})$ for all $\mathbf{a} \in A^*$, then $\mathcal{C} = \mathcal{D}$.

Consequence

From a linearly ordered set of clones with the same binary group operation $+$, the mapping

$$\mathcal{C} \mapsto \langle \varphi(\mathcal{C}, \mathbf{a}) \,|\, \mathbf{a} \in A^* \rangle$$

is injective.

Higman's Theorem

Word embedding

hen $\leq_e$ achievement,   austria $\leq_e$ australia

Higman's Theorem [Higman, 1952]

Let A be a finite set. Then $\langle A^*, \leq_e \rangle$ has no infinite antichain.

Corollary

The set of upward closed subsets of A^* has no infinite ascending chain with respect to $\subseteq$.

The key observation

$\mathbf{a} \leq_e \mathbf{b} \Rightarrow \varphi(\mathcal{C}, \mathbf{b}) \subseteq \varphi(\mathcal{C}, \mathbf{a})$

$\mathcal{C}$ ... clone on $\mathbb{Z}_2$ containing $+$. We observe $0110 \leq_e 0011101$.
Claim:

$$\varphi(\mathcal{C}, 0011101) \subseteq \varphi(\mathcal{C}, 0110).$$

Proof

Let $a \in \varphi(\mathcal{C}, 0011101)$,
$f \in \mathcal{C}^{[7]}$ such that $f(0011101) = a$, $f(\mathbf{z}) = 0$ for all $\mathbf{z} \in \{0,1\}^7$ with $\mathbf{z} <_{\text{lex}} 0011101$.
Define

$$g(x_1, x_2, x_3, x_4) := f(0, x_1, x_2, 1, x_3, x_4, 1).$$

Then $g(0110) = f(0011101) = a$ and $g(\mathbf{z}) = 0$ for $\mathbf{z} \in \{0,1\}^4$ with $\mathbf{z} <_{\text{lex}} 0110$. Thus $a \in \varphi(\mathcal{C}, 0110)$.

Abstract from $\mathbb{Z}_2$:
Clones on $A = \{0, \ldots, t-1\}$ with group operation $+$ and neutral element 0:

Theorem

Let $\mathcal{C}$ be a constantive clone on A with $+$. $\mathbf{a}, \mathbf{b} \in A^*$ with $\mathbf{a} \leq_e \mathbf{b}$.
Then $\varphi(\mathcal{C}, \mathbf{b}) \subseteq \varphi(\mathcal{C}, \mathbf{a})$.

Consequence

For every subset S of A, the set $\{\mathbf{x} \in A^* \mid \varphi(\mathcal{C}, \mathbf{x}) \subseteq S\}$ is an upward closed subset of $\langle A^*, \leq_e \rangle$.

Applying Higman's Theorem

Let $\mathbb{L}$ be an infinite descending chain of Mal'cev clones. Then the mapping

$$\begin{array}{rcccl} r & : & \mathbb{L} & \longrightarrow & (\mathcal{U}(A^*, \leq_e))^{2^A} \\ & & \mathcal{C} & \longmapsto & \langle \{\mathbf{x} \in A^* \mid \varphi(\mathcal{C}, \mathbf{x}) \subseteq S\} \mid S \subseteq A \rangle \end{array}$$

is injective and inverts the ordering.

Hence it produces an infinite ascending chain in $(\mathcal{U}(A^*, \leq_e))^{2^A}$, and hence in $\mathcal{U}(A^*, \leq_e)$. Contradiction.

Splitting pairs ("indices and witnesses" in [Bulatov and Dalmau, 2006], [Aichinger, 2000])

Let $\mathbf{a} \in A^n$. In a Mal'cev clone $\mathcal{C}$, the role of

$$\varphi(\mathcal{C}, \mathbf{a}) = \{c(\mathbf{a}) \,|\, c \in \mathcal{C}^{[n]}, c(\mathbf{z}) = 0 \text{ for all } \mathbf{z} \in A^n \text{ with } \mathbf{z} <_{\mathrm{lex}} \mathbf{a}\}$$

is taken by the relation

$$\{(f(\mathbf{a}), g(\mathbf{a})) \,|\, f, g \in \mathcal{C}^{[n]}, \forall \mathbf{z} \in A^n : \mathbf{z} <_{\mathrm{lex}} \mathbf{a} \Rightarrow f(\mathbf{z}) = g(\mathbf{z})\}.$$

Constantive Mal'cev clones on finite sets are finitely related

Theorem [Aichinger, 2010]

Let A be a finite set, and let $\mathcal{M}$ be the set of all constantive Mal'cev clones on A. Then we have:

1. There is no infinite descending chain in $(\mathcal{M}, \subseteq)$.
2. For every constantive Mal'cev clone $\mathcal{C}$, there is a finitary relation ρ on A such that $\mathcal{C} = \mathrm{Polym}(\{\rho\})$.
3. The set $\mathcal{M}$ is finite or countably infinite.

Is the assumption “constantive” needed?

The constantive place in the proof

Let $a \in \varphi(\mathcal{C}, 0011101)$, $f \in \mathcal{C}^{[7]}$ such that $f(0011101) = a$, $f(\mathbf{z}) = 0$ for all $\mathbf{z} \in \{0,1\}^7$ with $\mathbf{z} <_{\text{lex}} 0011101$. Define

$$g(x_1, x_2, x_3, x_4) := f(0, x_1, x_2, 1, x_3, x_4, 1).$$

Then $g(0110) = f(0011101) = a$ and $g(\mathbf{z}) = 0$ for $\mathbf{z} \in \{0,1\}^4$ with $\mathbf{z} <_{\text{lex}} 0110$. Thus $a \in \varphi(\mathcal{C}, 0110)$.

Repair

$g(x_1, x_2, x_3, x_4) := f(x_1, x_1, x_2, x_2, x_3, x_4, x_2)$.

Limitations

- $010 \leq_e 0210$,
- $012 \leq_e 2012$, $g(x_1, x_2, x_3) := f(x_3, x_1, x_2, x_3)$, $003 <_{\text{lex}} 012$, not $3003 <_{\text{lex}} 2012$.

Generalization 1

How to get rid of “constantive”

We need:

- a new ordering $\leq_E$ that replaces $\leq_e$,
- a proof that $\langle A^*, \leq_E \rangle$ has DCC and no infinite antichains,
- a proof of $\mathbf{a} \leq_E \mathbf{b} \Rightarrow \varphi(\mathcal{C}, \mathbf{b}) \subseteq \varphi(\mathcal{C}, \mathbf{a})$.

Mal'cev clones on finite sets are finitely related

Theorem [Aichinger, Mayr, McKenzie, 2009]

Let A be a finite set, and let $\mathcal{M}$ be the set of all Mal'cev clones on A. Then we have:

1. There is no infinite descending chain in $(\mathcal{M}, \subseteq)$.
2. For every Mal'cev clone $\mathcal{C}$, there is a finitary relation ρ on A such that $\mathcal{C} = \mathrm{Polym}(\{\rho\})$.
3. The set $\mathcal{M}$ is finite or countably infinite.

The theorem in full generality

Definition

Let $k \geq 2$. Then $t : A^{k+1} \to A$ is a *k-edge operation* if for all $x, y \in A$ we have

$$t(y, y, x, \dots, x) = t(y, x, y, x, \dots, x) = x$$

and for all $i \in \{4, \dots, k+1\}$ and for all $x, y \in A$, we have

$$t(x, \dots, x, y, x, \dots, x) = x, \text{ with } y \text{ in position } i.$$

Examples of edge operations

1. d Mal'cev $\Rightarrow t(x, y, z) := d(y, x, z)$ is 2-edge.
2. m majority $\Rightarrow t(x_1, x_2, x_3, x_4) := m(x_2, x_3, x_4)$ is 3-edge.

Algebras with few subpowers

Theorem ([Berman et al., 2010])

Let **A** be a finite algebra. The following are equivalent:

1. **A** has *few subpowers*, i.e., $\exists p \, \forall n \, |Sub(\mathbf{A}^n)| \leq 2^{p(n)}$;
2. There is $k \in \mathbb{N}$ such that **A** has a k-edge term.

The Finitely-related-theorem in full generality

"Constantive" has been dropped. Do we need "Mal'cev"?

Theorem (Aichinger, Mayr, McKenzie)

Let A be a finite set, let $k \in \mathbb{N}$, $k > 1$, and let $\mathcal{M}_k$ be the set of all clones on A that contain a k-edge operation. Then we have:

1. For every clone $\mathcal{C}$ in $\mathcal{M}_k$, there is a finitary relation R on A such that $\mathcal{C} = \mathrm{Pol}(A, \{R\})$.
2. There is no infinite descending chain in $(\mathcal{M}_k, \subseteq)$.
3. The set $\mathcal{M}_k$ is finite or countably infinite.

Consequences

Mal'cev algebras

1. Up to term equivalence and renaming of elements, there are only countably many finite Mal'cev algebras.
2. Every finite Mal'cev algebra can be represented by a single finitary relation.

Corollary – The clone lattice above a Mal'cev clone

Let $\mathcal{C}$ be a Mal'cev clone on a finite set A.

1. The interval $\mathbb{I}[\mathcal{C}, \mathcal{O}(A)]$ has finitely many atoms [Pöschel and Kalužnin, 1979],
2. every clone $\mathcal{D}$ with $\mathcal{C} \subset \mathcal{D}$ contains one of these atoms,
3. If $\mathbb{I}[\mathcal{C}, \mathcal{O}(A)]$ is infinite, it contains a clone that is not f.g. (cf. König's Lemma).

A consequence on groups

Corollary

Let G be a finite group, $|G| > 1$. Then there exists $k \in \mathbb{N}$ and $H \leq G^k$ such that for every $n \in \mathbb{N}$, $S \leq G^n$, there are $l, m \in \mathbb{N}$, $\sigma : \underline{m} \times \underline{k} \to \underline{l}$, $\tau : \underline{n} \to \underline{l}$ such that

$$S = \{ \begin{array}{l} (g_1, \ldots, g_n) \in G^n \,|\, \exists a_1, \ldots, a_l \in G : \\ \bigwedge_{i \in \underline{m}} (a_{\sigma(i,1)}, \ldots, a_{\sigma(i,k)}) \in H \\ \wedge \\ g_1 = a_{\tau(1)} \wedge \ldots \wedge g_n = a_{\tau(n)} \}. \end{array}$$

A consequence on groups

Theorem

Let G be a finite group. Then there is $k \in \mathbb{N}$, $H \leq G^k$ such that $\mathcal{S} := \bigcup_{n\in\mathbb{N}} \mathrm{Sub}(G^n)$ is the smallest set such that

- $H \in \mathcal{S}$;
- $\forall m, n \in \mathbb{N}, A \in \mathcal{S}^{[m]}, \sigma : \underline{n} \to \underline{m}$ we have $\{(h_{\sigma(1)}, \ldots, h_{\sigma(n)}) \mid (h_1, \ldots, h_m) \in A\} \in \mathcal{S}^{[n]}$;
- $\forall m, n \in \mathbb{N}, A \in \mathcal{S}^{[n]}, \sigma : \underline{n} \to \underline{m}$ we have $\{(h_1, \ldots, h_m) \mid (h_{\sigma(1)}, \ldots, h_{\sigma(n)}) \in A\} \in \mathcal{S}^{[n]}$;
- $\forall n \in \mathbb{N}, A, B \in \mathcal{S}^{[n]} : A \cap B \in \mathcal{S}^{[n]}$.

Absorbing polynomials and Supernilpotence

Definition

$\mathbf{V} = \langle V, +, -, 0, f_1, f_2, \ldots \rangle$ expanded group, $p \in \mathrm{Pol}_n \mathbf{V}$. p is *absorbing* $:\Leftrightarrow \forall \mathbf{x} : 0 \in \{x_1, \ldots, x_n\} \Rightarrow p(x_1, \ldots, x_n) = 0$.

Definition

$\mathbf{V}$ expanded group. $\mathbf{V}$ is k*-supernilpotent* $: \Leftrightarrow$ the zero-function is the only $(k+1)$-ary absorbing polynomials.

Lemma

A group $\mathbf{G}$ is k-supernilpotent if and only if it is nilpotent of class $\leq k$.

Supernilpotent expanded groups

Proposition

$\mathbf{FZ}_6 := \langle \mathbb{Z}_6, +, f \rangle$ with $f(0) = f(3) = 3$, $f(1) = f(2) = f(4) = f(5) = 0$ is 2-step nilpotent and not supernilpotent.

Theorem [Berman and Blok, 1987, Theorem 2], [Freese and McKenzie, 1987, Chapter VII]

Let $\mathbf{V}$ be a nilpotent expanded group of finite type with $|V|$ a prime power. Then $\mathbf{V}$ is supernilpotent.

Theorem (Aichinger, Mudrinski)

Let $k, m \in \mathbb{N}$, $m \geq 2$, and let $\mathbf{V}$ be a multilinear expanded group with degree m of nilpotence class k. Then $\mathbf{V}$ is m^{k-1}-supernilpotent.

Direct decomposition of expanded groups

Theorem [Kearnes, 1999]

Let **V** be a finite supernilpotent expanded group. Then **V** is isomorphic to a direct product of expanded groups of prime power order.

Theorem [Aichinger]

Let **V** be a supernilpotent expanded group whose ideal lattice is of finite height. Then **V** is isomorphic to a direct product of finitely many π-monochromatic expanded groups.

Height 2

Lemma

Let **R** be a ring with unit, and let **M** be an **R**-module such that **M** has exactly three submodules; let Q be the submodule different from 0 and M. Then the exponents of the groups $\langle M/Q, +\rangle$ and $\langle Q, +\rangle$ are equal.

Lemma

Let **V** be a finite expanded group whose ideal lattice is a three element chain $\{0\} < Q < V$. We assume that the exponents of the groups $\langle Q, +\rangle$ and $\langle V/Q, +\rangle$ are different, and that $[V, V] = Q$, $[V, Q] = 0$. Then **V** is not supernilpotent.

Ágoston, I., Demetrovics, J., and Hannák, L. (1986).
On the number of clones containing all constants (a problem of R. McKenzie).
In *Lectures in universal algebra (Szeged, 1983)*, volume 43 of *Colloq. Math. Soc. János Bolyai*, pages 21–25. North-Holland, Amsterdam.

Aichinger, E. (2000).
On Hagemann's and Herrmann's characterization of strictly affine complete algebras.
Algebra Universalis, 44:105–121.

Aichinger, E. (2010).
Constantive Mal'cev clones on finite sets are finitely related.
Proc. Amer. Math. Soc., 138(10):3501–3507.

Aichinger, E. and Mayr, P. (2007).
Polynomial clones on groups of order *pq*.
Acta Math. Hungar., 114(3):267–285.

Aichinger, E. and Mudrinski, N. (2009).
Types of polynomial completeness of expanded groups.
Algebra Universalis, 60(3):309–343.

Aichinger, E. and Mudrinski, N. (2010).
Polynomial clones of Mal'cev algebras with small congruence lattices.
Acta Math. Hungar., 126(4):315–333.

Berman, J. and Blok, W. J. (1987).
Free spectra of nilpotent varieties.
Algebra Universalis, 24(3):279–282.

Berman, J., Idziak, P., Marković, P., McKenzie, R., Valeriote, M., and Willard, R. (2010).
Varieties with few subalgebras of powers.
Transactions of the American Mathematical Society, 362(3):1445–1473.

Bulatov, A. and Dalmau, V. (2006).
A simple algorithm for Mal'tsev constraints.

SIAM J. Comput., 36(1):16–27 (electronic).

Bulatov, A. A. (2002).
Polynomial clones containing the Mal'tsev operation of the groups $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p \times \mathbb{Z}_p$.
Mult.-Valued Log., 8(2):193–221.

Bulatov, A. A. and Idziak, P. M. (2003).
Counting Mal'tsev clones on small sets.
Discrete Math., 268(1-3):59–80.

Freese, R. and McKenzie, R. N. (1987).
Commutator Theory for Congruence Modular varieties, volume 125 of *London Math. Soc. Lecture Note Ser.*
Cambridge University Press.

Hagemann, J. and Herrmann, C. (1982).
Arithmetical locally equational classes and representation of partial functions.
In *Universal Algebra, Esztergom (Hungary)*, volume 29, pages 345–360. Colloq. Math. Soc. János Bolyai.

Higman, G. (1952).
Ordering by divisibility in abstract algebras.
Proc. London Math. Soc. (3), 2:326–336.

Idziak, P. M. (1999).
Clones containing Mal'tsev operations.
Internat. J. Algebra Comput., 9(2):213–226.

Idziak, P. M. and Słomczyńska, K. (2001).
Polynomially rich algebras.
J. Pure Appl. Algebra, 156(1):33–68.

Istinger, M., Kaiser, H. K., and Pixley, A. F. (1979).
Interpolation in congruence permutable algebras.
Colloq. Math., 42:229–239.

Kaarli, K. and Pixley, A. F. (2001).
Polynomial completeness in algebraic systems.
Chapman & Hall / CRC, Boca Raton, Florida.

Kearnes, K. A. (1999).
Congruence modular varieties with small free spectra.

Algebra Universalis, 42(3):165–181.

Mal'cev, A. I. (1954).
On the general theory of algebraic systems.
Mat. Sb. N.S., 35(77):3–20.

Mayr, P. (2008).
Polynomial clones on squarefree groups.
Internat. J. Algebra Comput., 18(4):759–777.

Mayr, P. (2011).
Mal'cev algebras with supernilpotent centralizers.
Algebra Universalis, 65:193–211.

Pöschel, R. and Kalužnin, L. A. (1979).
Funktionen- und Relationenalgebren, volume 15 of *Mathematische Monographien [Mathematical Monographs]*.

VEB Deutscher Verlag der Wissenschaften, Berlin.
Ein Kapitel der diskreten Mathematik. [A chapter in discrete mathematics].