Algebras with few subpowers are finitely related

Erhard Aichinger, Peter Mayr, Ralph McKenzie

CAUL, Lisbon, Portugal
JKU Linz, Austria
stein@cii.fc.ul.pt

Praha, June 2010

What is the number of algebras on a finite set?

On A finite, $|A| \geq 2$, there are:

- ω distinct finitary operations,
- 2^ω distinct algebraic structures.

Many, like the Boolean lattice $\langle A, \wedge, \vee, \neg \rangle$ and the Boolean ring $\langle A, +, \cdot, 1 \rangle$, have the same term functions. They are **term equivalent**.

Fact

On A finite, there are:

- ω term inequivalent algebras if $|A| = 2$ (Post, 1941),
- 2^ω term inequivalent algebras if $|A| \geq 3$ (Yanov, Muchnik, 1959).

Question (McKenzie, Rosenberg 1988)

How many finite, term inequivalent algebras generate a congruence permutable (CP) variety?

Clones of term functions

Definition

$\mathrm{Clo}(\mathbf{A})$... **all finitary term functions** on an algebra $\mathbf{A} := \langle A, F \rangle$

Remark

$\mathrm{Clo}(\mathbf{A})$ contains all finitary projections on A and is closed under composition. Such a set of functions is called a **clone** on A.

Example

$\mathrm{Clo}(\mathbb{Z}_5, +) \ldots (x_1, x_2, x_3) \mapsto 2x_1 + 3x_2$
$\mathrm{Clo}(\{0,1\}, \wedge, \vee) \ldots (x_1, x_2, x_3) \mapsto (x_1 \wedge x_2) \vee x_3$

Describing functions by invariant relations

$\mathbb{S}(\mathbf{A})$ ... subuniverses of **A**

Fact

1. Every $f \in \mathrm{Clo}(\mathbf{A})$ preserves every $R \in \mathbb{S}(\mathbf{A}^n)$.
2. If A is finite and $f : A^k \to A$ preserves every $R \in \mathbb{S}(\mathbf{A}^n)$ for every $n \in \mathbb{N}$, then $f \in \mathrm{Clo}(\mathbf{A})$.

Definition

$R \subseteq A^n$ ... *n-ary relation*
$\mathcal{R}$ ... set of finitary relations on A
$\mathrm{Pol}(\mathcal{R})$ ... functions that preserve every $R \in \mathcal{R}$ (*polymorphisms*)
A (resp. $\mathrm{Clo}(\mathbf{A})$)is **finitely related** if $\exists$ finite $\mathcal{R}$: $\mathrm{Clo}(\mathbf{A}) = \mathrm{Pol}(\mathcal{R})$.

Theorem (Baker, Pixley, 1975)

Lattices (more general, algebras with NU-term) are finitely related.

Are Malcev algebras finitely related?

Theorem (Malcev, 1954)

$\mathbb{HSP}(\mathbf{A})$ is CP iff $\exists m \in \mathrm{Clo}_3(\mathbf{A})\ \forall x, y \in A$:

$$m(x,y,y) = m(y,y,x) = x \text{ } (\textbf{Malcev term}).$$

Example

For a group $\langle G, +, -, 0\rangle$ consider $m(x,y,z) := x - y + z$.

Question (McKenzie, Rosenberg 1988, Idziak 1999)

Let C be a clone with Malcev operation on a finite set. Is C fin. related? Verified in special cases, eg. Idziak 1999, Bulatov 2001, Kearnes, Szendrei 2005, Aichinger, Mudrinski 2008, M 2008.

2009: Yes, if C contains all constants (Aichinger, to appear Proc. AMS).

An overview of Malcev conditions

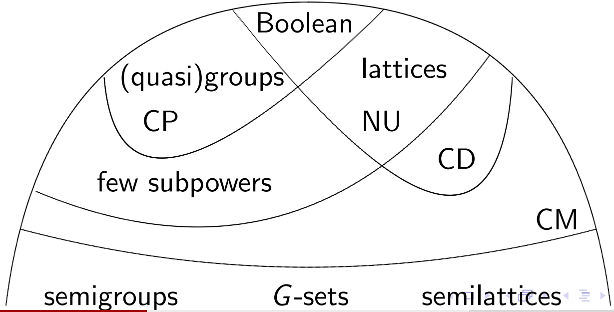
Definition

A, finite, has **few subpowers** if $\exists$ polynomial $p\ \forall n \in \mathbb{N}$: $|\mathbb{S}(\mathbf{A}^n)| \leq 2^{p(n)}$.

The set $\mathbf{A} := \langle A, \emptyset \rangle$ has many subpowers, $|\mathbb{S}(\mathbf{A}^n)| = 2^{|A|^n}$.

Fact (Idziak, Markovic, McKenzie, Valeriote, Willard, 2007)

If **A** has few subpowers, then $CSP(\mathbf{A})$ is tractable.



The result

Theorem (Aichinger, M, McKenzie, manuscript 2009)

Every finite algebra with few subpowers is finitely related.

This applies to algebras with Malcev term and generalizes the Baker-Pixley Theorem for algebras with NU-term.

Corollary

On A finite, there exist at most countably many term inequivalent algebras with few subpowers (in particular, with Malcev term).

How to represent functions on a group

Let C be a clone on $A := \{0, \dots, n-1\}$.
$\leq_{lex}$ ... lexicographical order on A^k
$f \in C_k$ **jumps to** c **at** $\bar{a} \in A^k$ if $\forall \bar{x} <_{lex} \bar{a}: \; f(\bar{x}) = 0$ and $f(\bar{a}) = c$.

Lemma 1

Let $G \subseteq C_k$ such that $\forall f \in C_k \forall \bar{a} \in A^k \forall c \in A$: if f jumps to c at $\bar{a}$, then $\exists g \in G$ that jumps to c at $\bar{a}$.
If C contains a group operation $+$, then G generates C_k as subgroup of $\langle A, + \rangle^{A^k}$.

Problem: What is the connection between jumpy functions in C_k and C_l?

Embedding order on words

Definition

$\bar{a}, \bar{b} \in A^+ \ldots$ words over A
$\bar{a} \leq_E \bar{b}$ if $\bar{b}$ is obtained from $\bar{a}$ by inserting letters after their first occurence in $\bar{a}$.

Example

hedgo $\leq_E$ hedgehog
an $\not\leq_E$ ant

Lemma 2 (cf. Higman's Theorem, 1952)

Let A finite. Then $\langle A^+, \leq_E \rangle$ is partially ordered with (DCC) and without infinite antichains (i.e., *well partially ordered*).

Ordering jumps

Lemma 3

Let C be a clone on $\{0, \dots, n-1\}$.
If $f \in C$ jumps to c at $\bar{b}$, then $\forall \bar{a} \leq_E \bar{b} \, \exists f' \in C$ that jumps to c at $\bar{a}$.

Example

Let $\bar{a} := (h, e, d, g, o)$, $\bar{b} := (h, e, d, g, e, h, o, g)$.

$$f'(x_1, x_2, x_3, x_4, x_5) := f(x_1, x_2, x_3, x_4, x_2, x_1, x_5, x_4)$$

satisfies $f'(\bar{a}) = f(\bar{b})$.
If $(x_1, x_2, x_3, x_4, x_5) <_{lex} \bar{a}$, then $(x_1, x_2, x_3, x_4, x_2, x_1, x_5, x_4) <_{lex} \bar{b}$ and $f'(x_1, x_2, x_3, x_4, x_5) = 0$.

A finite representation of all jumps

Let C be a clone on $A := \{0, \dots, n-1\}$. For $c \in A$, let

$$\lambda(c) := \{\bar{a} \in A^+ \mid \nexists f \in C\colon f \text{ jumps to } c \text{ at } \bar{a}\}.$$

1. $\lambda(c)$ is upward closed wrt. $\leq_E$ (Lemma 3).
2. $\lambda(c)$ is determined by its finitely many minimal elements (Lemma 2).
3. Then

$$m := \max_{c \in A}\{|\bar{a}| \mid \bar{a} \text{ is minimal wrt. } \leq_E \text{ in } \lambda(c)\}$$

is finite.

C_m determines C

Recall

$$\begin{aligned} \lambda(c) &= \{\bar{a} \in A^+ \mid \nexists f \in C \colon f \text{ jumps to } c \text{ at } \bar{a}\} \\ m &= \max_{c \in A}\{|\bar{a}| \mid \bar{a} \text{ is minimal wrt. } \leq_E \text{ in } \lambda(c)\} \end{aligned}$$

Claim

If C contains a group operation, then C is equal to the greatest clone D on A with $D_m = C_m$ (Note $C \subseteq D = \mathrm{Pol}(\{C_m\})$).

1. If $\bar{b} \in \lambda(c)$, then $\exists \bar{a} \in \lambda(c) \colon \bar{a} \leq_E \bar{b}$ and $|\bar{a}| \leq m$ (Lemma 3). Since $D_m = C_m$, $\nexists f \in D$ that jumps to c at $\bar{a}$ (or at $\bar{b}$).
2. Conversely, all jumps in D are already witnessed in C.
3. Hence $C = D$ (Lemma 1), and C is finitely related.

Combining NU and Malcev operations

Definition

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

$$t \begin{pmatrix} y & y & x & x & \cdots & x \\ y & x & y & x & & x \\ x & x & x & y & & x \\ \vdots & & & & \ddots & \vdots \\ x & x & x & x & \cdots & y \end{pmatrix} = \begin{pmatrix} x \\ x \\ x \\ \vdots \\ x \end{pmatrix}.$$

Example

If f is k-NU, then $t(x_1, \dots, x_{k+1}) := f(x_2, \dots, x_k)$ is k-edge.
t is a 2-edge operation iff $m(x, y, z) := t(y, x, z)$ is Malcev.

Theorem (Berman, Idziak, Markovic, McKenzie, Valeriote, Willard, 2008)

A finite algebra **A** has few subpowers iff **A** has an edge term.

How to represent functions on an algebra with few subpowers

Let C be a clone on $A := \{0, \dots, n-1\}$.
(c, d) is a **splitting pair at** $\bar{a} \in A^m$ in C_m if $\exists f, g \in C_m \, \forall \bar{x} <_{lex} \bar{a}$:
$f(\bar{x}) = g(\bar{x})$ and $(f(\bar{a}), g(\bar{a})) = (c, d)$.

Lemma (Berman, Idziak, Markovic, McKenzie, Valeriote, Willard, 2008)

Let C be a clone with k-edge term t, let $G \subseteq C_m$ such that

1. $\forall T \subseteq A^m, |T| < k$: $G|_T = C_m|_T$, and
2. $\forall \bar{a} \in A^m$: every splitting pair at $\bar{a}$ in C^m is a splitting pair at $\bar{a}$ in G.

Then G generates C_m as subalgebra of $\langle A, t \rangle^{A^m}$.

Problems

Question

1. Given a clone C with Malcev operation on A, finite. Find a relation R such that $C = \mathrm{Pol}(\{R\})$.
   Possible in special cases by "constructive pre-AMM proofs".
2. Given functions $f_1, \ldots, f_n$ on A and a relation R on A, finite.
   Is $\mathrm{Clo}(\langle A, f_1, \ldots, f_n \rangle) = \mathrm{Pol}(\{R\})$ decidable?
3. (Valeriote) Let $\mathbf{A}$ finite in a CM variety with $\mathrm{Clo}(\mathbf{A})$ finitely related.
   Does $\mathbf{A}$ have few subpowers?
   Barto, 2009: Yes, if $\mathbb{HSP}(\mathbf{A})$ is CD (Zadori's conjecture).