Algebras from congruences

Peter Mayr

AAA 100, Krakow, February 7, 2021

Mathematics
UNIVERSITY OF COLORADO **BOULDER**

Content

1. A functor $\mathfrak{C}$ that makes "algebras from congruences"
   - Motivation
   - History
   - New signature
2. Algebraic properties preserved by $\mathfrak{C}$
   - The kitchen sink
3. Applications
   - Characterizing supernilpotent congruences
   - Reductions for subpower membership
   - Relations for polynomial clones

A question

Question

Given a congruence α of a finite algebra $\mathbf{A}$, is it decidable if α is supernilpotent, i.e. $\exists k \in \mathbb{N} : [\underbrace{\alpha, \ldots, \alpha}_{k+1}] = 0$?

Note

- There is no a priori bound on the supernilpotence class k of α.
- For α the total congruence on $\mathbf{A}$ and mild assumptions, supernilpotence can be decided.

Theorem (Hobby, McKenzie '88, Kearnes '99, Aichinger, Mudrinski 2010)

For a finite algebra $\mathbf{A}$ of finite signature in a variety omitting type 1 TFAE:

1. $\mathbf{A}$ is supernilpotent.
2. $\mathbf{A}$ is a direct product of nilpotent algebras of prime power order.

Can we relativize this structural result from $\mathbf{A}$ to α?

Making congruences into algebras

Goal

For $\alpha \in \mathrm{Con}(\mathbf{A})$ with $\mathbf{A}/\alpha$ finite, build an algebra $\mathbf{A}^{\mathfrak{C}}$ such that:

- $\mathrm{Con}(\mathbf{A}^{\mathfrak{C}})$ is isomorphic to the interval $\{\beta \in \mathrm{Con}(\mathbf{A}) \mid \beta \leq \alpha\}$.
- This isomorphism preserves (higher) commutators and TCT-types.
- $\mathbf{A}^{\mathfrak{C}}$ has finite signature if $\mathbf{A}$ has finite signature.
- $\mathbf{A}^{\mathfrak{C}}$ inherits idempotent Mal'cev conditions from $\mathbf{A}$.

Note

Then α is supernilpotent iff $\mathbf{A}^{\mathfrak{C}}$ is supernilpotent.

This construction is not new

Elements of the following construction appear, e.g. in

- heterogeneous algebras (Novotný 1982)
- making many-sorted algebras one-sorted (Gardner 1989)
- modules from abelian congruences (Freese, McKenzie 1987)
- wreath decomposition of algebras (VanderWerf 1994)
- matrix powers (McKenzie 1996)
- homogenization of multisorted algebras (Mućka, Romanowska, Smith 2013)

1. Construction

Fix throughout:

- $\mathcal{F}$ a signature without nullary symbols,
- $[m] := \{1, \dots, m\}$,
- $\mathbf{I} := ([m], \mathcal{F})$ a finite $\mathcal{F}$-algebra.

Definition

For an $\mathcal{F}$-algebra $\mathbf{A}$ with onto homomorphism $\chi\colon \mathbf{A} \twoheadrightarrow \mathbf{I}$, define an algebra

$$\mathfrak{C}(\mathbf{A}, \chi) := (\, \chi^{-1}(1) \times \cdots \times \chi^{-1}(m),\, \mathcal{F}_{\mathbf{I}} \,)$$

with

- **universe** $A^{\mathfrak{C}}$ the product of congruence classes $\chi^{-1}(i)$ of the kernel of χ,
- **signature** $\mathcal{F}_I := \{f_i \mid f \in \mathcal{F}, i \in [m]^{\mathrm{arity}(f)}\} \cup \{d\}$.

Write elements in $A^{\mathfrak{C}} = \chi^{-1}(1) \times \cdots \times \chi^{-1}(m)$ as columns.

- $d \in F_{\mathbf{I}}$ is the m-**ary diagonal operation**

$$d \colon (A^{\mathfrak{C}})^m \to A^{\mathfrak{C}}, \quad \left(\begin{bmatrix} x_1^{(1)} \\ \vdots \\ x_1^{(m)} \end{bmatrix}, \ldots, \begin{bmatrix} x_m^{(1)} \\ \vdots \\ x_m^{(m)} \end{bmatrix} \right) \mapsto \begin{bmatrix} x_1^{(1)} \\ \vdots \\ x_m^{(m)} \end{bmatrix}$$

Recall: Write elements in $A^{\mathfrak{C}} = \chi^{-1}(1) \times \cdots \times \chi^{-1}(m)$ as columns.

- For k-ary $f \in \mathcal{F}$ and $i = (i_1, \ldots, i_k) \in [m]^k$

$$f_i \colon (A^{\mathfrak{C}})^k \to A^{\mathfrak{C}}$$

is the restriction of f to $\chi^{-1}(i_1) \times \cdots \times \chi^{-1}(i_k) \to \chi^{-1}(f(i))$ padded with projections:

$$f_i\left(\begin{bmatrix} x_1^{(1)} \\ \vdots \\ x_1^{(i_1)} \\ \vdots \\ x_1^{(m)} \end{bmatrix}, \begin{bmatrix} \\ x_2^{(i_2)} \\ \\ \\ \\ \end{bmatrix}, \ldots, \begin{bmatrix} \\ \\ \\ \\ x_k^{(i_k)} \end{bmatrix}\right) := \begin{bmatrix} x_1^{(1)} \\ \vdots \\ x_1^{(f(i)-1)} \\ f(x_1^{(i_1)}, \ldots, x_k^{(i_k)}) \\ x_1^{(f(i)+1)} \\ \vdots \\ x_1^{(m)} \end{bmatrix}$$

Or: f_i is the k-ary first projection with $f(x_1^{(i_1)}, \ldots, x_k^{(i_k)})$ in entry $f(i)$.

Note

- $\mathbf{A}$ and $\mathfrak{C}(\mathbf{A}, \chi)$ have different signatures $\mathcal{F}$ and $\mathcal{F}_{\mathbf{I}}$, respectively.
- E.g., for $\mathbf{A} = (A, \cdot)$ a semigroup, $\chi \colon \mathbf{A} \twoheadrightarrow \mathbf{I}$ with $|I| = m$: $\mathfrak{C}(\mathbf{A}, \chi)$ is not a semigroup but has m^2 binary operations $\cdot_i$ and an m-ary diagonal operation.
- E.g. for $\mathbf{A}$ a group, $\mathfrak{C}(\mathbf{A}, \chi)$ encodes $\ker \chi$ but is **not** a normal subgroup of $\mathbf{A}$.

What can d do for you (1)?

$\mathcal{F}_I$-terms are products of $\mathcal{F}$-terms restricted to ker χ-classes.

Lemma

T is a k-ary term function of $\mathfrak{C}(\mathbf{A}, \chi)$ iff $\exists mk$-ary term functions $t^{(1)}, \ldots, t^{(m)}$ of $\mathbf{A}$ such that

$$t^{(i)} \begin{pmatrix} 1 & \ldots & 1 \\ 2 & \ldots & 2 \\ \vdots & & \vdots \\ m & \ldots & m \end{pmatrix} = i,$$

and

$$T \underbrace{\left(\begin{bmatrix} x_1^{(1)} \\ \vdots \\ x_1^{(m)} \end{bmatrix}, \ldots, \begin{bmatrix} x_k^{(1)} \\ \vdots \\ x_k^{(m)} \end{bmatrix} \right)}_{=X} = \begin{bmatrix} t^{(1)}(X) \\ \vdots \\ t^{(m)}(X) \end{bmatrix}$$

What can d do for you (2)?

Lemma

The functor $\mathfrak{C}$ is an isomorphism

- from the category of $\mathcal{F}$-algebras $\mathbf{A}$ with onto homomorphism $\chi\colon \mathbf{A} \twoheadrightarrow \mathbf{I}$
- to the category of $\mathcal{F}_{\mathbf{I}}$-algebras satisfying the obvious identities between d and f_i.

Proof.

For an $\mathcal{F}_{\mathbf{I}}$-algebra $\mathbf{B}$, d yields a product decomposition

$$B \cong B_1 \times \cdots \times B_m$$

and an $\mathcal{F}$-algebra $\mathbf{A}$ with universe $B_1 \cup \cdots \cup B_m$ such that $\mathfrak{C}(\mathbf{A}, \chi) = \mathbf{B}$. □

2. Properties of $\mathfrak{C}$

Morphisms

Lemma

Let $\chi\colon \mathbf{A} \twoheadrightarrow \mathbf{I}$ and $\xi\colon \mathbf{B} \twoheadrightarrow \mathbf{I}$. Then

$$\begin{array}{rccl} {}^{\mathfrak{C}}\colon \{\varphi\colon \mathbf{A} \to \mathbf{B} \mid \chi = \xi\varphi\} & \to & \{\mathfrak{C}(\mathbf{A},\chi) \to \mathfrak{C}(\mathbf{B},\xi)\}, \\ \varphi & \mapsto & \varphi^{\mathfrak{C}}, \end{array}$$

with $\varphi^{\mathfrak{C}}\left(\begin{bmatrix} x^{(1)} \\ \vdots \\ x^{(m)} \end{bmatrix}\right) := \begin{bmatrix} \varphi(x^{(1)}) \\ \vdots \\ \varphi(x^{(m)}) \end{bmatrix}$ is a bijection.

Subalgebras

Lemma

Let $\chi\colon \mathbf{A} \twoheadrightarrow \mathbf{I}$. Then

$$\begin{aligned} {}^{\mathfrak{C}}\colon \{\mathbf{B} \leq \mathbf{A} \mid \chi(B) = I\} &\to \mathbb{S}(\mathfrak{C}(\mathbf{A}, \chi)), \\ \mathbf{B} &\mapsto \mathfrak{C}(\mathbf{B}, \chi|_B), \end{aligned}$$

is a $\vee$-semilattice isomorphism.

Note $\chi(B_1), \chi(B_2) \neq \emptyset$ does not imply $\chi(B_1 \cap B_2) \neq \emptyset$ in general.

Products

Lemma

For $j \in J$, let $\chi_j \colon \mathbf{A}_j \twoheadrightarrow \mathbf{I}$ and consider the **fiber product**

$$\prod_{j\in J}^{\mathbf{I}} \mathbf{A}_j := \{a \in \prod_{j\in J} \mathbf{A}_j \mid \exists i \in [m] \forall j \in J : \ \chi_j(a_j) = i\}.$$

Then

$$\mathfrak{C}(\prod_{j\in J}^{\mathbf{I}} \mathbf{A}_j, \prod_{j\in J} \chi_j) \cong \prod_{j\in J} \mathfrak{C}(\mathbf{A}_j, \chi_j).$$

Congruences

Lemma

Let $\chi\colon \mathbf{A} \twoheadrightarrow \mathbf{I}$. Then

$$\begin{aligned} {}^{\mathfrak{C}}\colon \{\alpha \in \mathrm{Con}(\mathbf{A}) \mid \alpha \leq \ker\chi\} &\to \mathrm{Con}(\mathfrak{C}(\mathbf{A},\chi)), \\ \alpha &\mapsto \alpha^{\mathfrak{C}} \end{aligned}$$

with $\begin{bmatrix} x^{(1)} \\ \vdots \\ x^{(m)} \end{bmatrix} \alpha^{\mathfrak{C}} \begin{bmatrix} y^{(1)} \\ \vdots \\ y^{(m)} \end{bmatrix}$ if $x^{(i)} \alpha y^{(i)}$ for all $i \in [m]$ is a lattice isomorphism.

Lemma

For $\alpha \leq \ker\chi$,

$$\mathfrak{C}(\mathbf{A}/\alpha, \chi/\alpha) \cong \mathfrak{C}(\mathbf{A},\chi)/\alpha^{\mathfrak{C}}.$$

Commutators

Lemma

Let $\chi\colon \mathbf{A} \twoheadrightarrow \mathbf{I}$ and $\alpha_1, \dots, \alpha_k \leq \ker \chi$. Then

$$[\alpha_1, \dots, \alpha_k]^{\mathfrak{C}} = [\alpha_1^{\mathfrak{C}}, \dots, \alpha_k^{\mathfrak{C}}].$$

Proof.

Uses the definition of (higher) commutators via subpowers $M_{\mathbf{A}}(\alpha_1, \dots, \alpha_k) \leq \mathbf{A}^{2^k}$. □

Varieties

Lemma

Let V be a variety of $\mathcal{F}$-algebras. Then

$$V^{\mathfrak{C}} := \mathbb{I}(\mathfrak{C}(\mathbf{A}, \chi) \mid \mathbf{A} \in V, \chi \colon \mathbf{A} \twoheadrightarrow \mathbf{I})$$

is a variety of $\mathcal{F}_{\mathbf{I}}$-algebras.

Proof.

$V^{\mathfrak{C}}$ inherits closure under $\mathbb{HSP}$ from V by the previous observations. □

Free algebras

Lemma

For $X \neq \emptyset$,

$$\mathbf{Free}_{V^{\mathfrak{C}}}(X) \cong \mathfrak{C}(\,\mathbf{Free}_V(X \times [m]),\, \mathrm{proj}_2\,).$$

Proof.

Check the universal property in $V^{\mathfrak{C}}$. □

Terms

Corollary

Up to equivalence k-ary $\mathcal{F}_\mathbf{I}$-terms T of $V^{\mathfrak{C}}$ are of the form

$$\underbrace{T\left(\begin{bmatrix} x_1^{(1)} \\ \vdots \\ x_1^{(m)} \end{bmatrix}, \dots, \begin{bmatrix} x_k^{(1)} \\ \vdots \\ x_k^{(m)} \end{bmatrix}\right)}_{=X} = \begin{bmatrix} t^{(1)}(X) \\ \vdots \\ t^{(m)}(X) \end{bmatrix}$$

for mk-ary $\mathcal{F}$-terms $t^{(1)}, \dots, t^{(m)}$ of V such that

$$t^{(i)}\begin{pmatrix} 1 & \dots & 1 \\ 2 & \dots & 2 \\ \vdots & & \vdots \\ m & \dots & m \end{pmatrix} = i.$$

Idempotent Mal'cev conditions

Corollary

$V^{\mathfrak{C}}$ inherits every idempotent Mal'cev condition from V.

Proof.

$$t(x_1, \dots, x_k) \mapsto t\left(\begin{bmatrix} x_1^{(1)} \\ \vdots \\ x_1^{(m)} \end{bmatrix}, \dots, \begin{bmatrix} x_k^{(1)} \\ \vdots \\ x_k^{(m)} \end{bmatrix}\right)$$

is a clone homomorphism between idempotent terms of V and idempotent terms of $V^{\mathfrak{C}}$. □

Note

$V^{\mathfrak{C}}$ may satisfy more Mal'cev conditions than V.
E.g. if $V(\mathbf{A})$ is congruence modular and $\chi\colon \mathbf{A} \twoheadrightarrow \mathbf{I}$ has abelian kernel, then $V(\,\mathfrak{C}(\mathbf{A}, \chi)\,)$ is congruence permutable (cf. Freese, McKenzie 1987).

TCT-types

Lemma

Let $\chi\colon \mathbf{A} \twoheadrightarrow \mathbf{I}$ and $\alpha \prec \beta \leq \ker \chi$.
Then the TCT-type of β/α in $\mathbf{A}$ is the same as that of $\beta^{\mathfrak{C}}/\alpha^{\mathfrak{C}}$ in $\mathfrak{C}(\mathbf{A}, \chi)$.

Proof.

Like term functions, polynomial functions on $\mathfrak{C}(\mathbf{A}, \chi)$ are assembled from restrictions of polynomial functions on $\mathbf{A}$ to $\ker \chi$-classes. □

Finiteness conditions

Corollary

Let $\chi\colon \mathbf{A} \twoheadrightarrow \mathbf{I}, \mathbf{A}^{\mathfrak{C}} := \mathfrak{C}(\mathbf{A}, \chi)$ and $\alpha \leq \ker \chi$. Then

- $\mathbf{A}, \alpha, \mathrm{Clo}(\mathbf{A})$, respectively, are finitely generated iff $\mathbf{A}^{\mathfrak{C}}, \alpha^{\mathfrak{C}}, \mathrm{Clo}(\mathbf{A}^{\mathfrak{C}})$ are.
- $\mathbf{A}$ is residually finite iff $\mathbf{A}^{\mathfrak{C}}$ is.
- $\mathbf{A}$ is finitely presented in V iff $\mathbf{A}^{\mathfrak{C}}$ is finitely presented in $V^{\mathfrak{C}}$.
- V is locally finite iff $V^{\mathfrak{C}}$ is.

What is not preserved by $\mathfrak{C}$?

- signature $\mathcal{F}$
- non-idempotent Mal'cev conditions
- finite equational basis (?)

Applications

1. Supernilpotence

Theorem (M, Szendrei 2019, Idziak, Kawałek, Kraczkowski 2020)

For a congruence α of a finite algebra $\mathbf{A}$ of finite signature in a variety omitting type 1 TFAE:

1. α is supernilpotent.
2. $\mathfrak{C}(\mathbf{A}, \chi)$ for the natural projection $\chi\colon \mathbf{A} \to \mathbf{A}/\alpha$ is supernilpotent.
3. α is nilpotent, and $\exists \beta_1, \dots, \beta_\ell \leq \alpha$ such that $\forall i \leq \ell$:
   - $\exists$ prime p_i: every α/β_i-block in A/β_i has p_i-power size,
   - $(\beta_1 \wedge \cdots \wedge \beta_{i-1}) \circ \beta_i = \beta_i \circ (\beta_1 \wedge \cdots \wedge \beta_{i-1}) = \alpha$,
   - $\beta_1 \wedge \cdots \wedge \beta_\ell = 0_A$.

Note

Condition 3 is clearly decidable.

2. Subpower membership

Let K be a finite set of finite algebras of finite signature.

$\mathrm{SMP}(K)$

Input: $a_1, \dots, a_k, b \in \prod_{i=1}^{n} \mathbf{A}_i$ with $\mathbf{A}_i \in K$
Question: Is b in the algebra generated by $a_1, \dots, a_k$?

Note

- $\mathrm{SMP}(K)$ is in ExpTime.
- There exist K with SMP ExpTime-complete (Kozik 2008), PSpace- or NP-complete (Bulatov, Kozik, M, Steindl 2016).
- $\mathrm{SMP}(K)$ for K with cube term is in NP (Bulatov, M, Szendrei 2019).

SMP for algebras with cube term

It suffices to solve SMP for sets of SI algebras with central monoliths.

Theorem (M, Szendrei 2019)

Let K be a finite set of algebras in a variety V with cube term.
Then $\mathrm{SMP}(K)$ is polytime reducible to $\mathrm{SMP}(K_1^{\mathfrak{C}}), \ldots, \mathrm{SMP}(K_\ell^{\mathfrak{C}})$ where

- $K_1, \ldots, K_\ell$ are the similarity classes of the SI algebras with abelian monoliths in $\mathbb{HS}(K)$,
- $K_i^{\mathfrak{C}}$ is the set of algebras from centralizers of monoliths of $\mathbf{A} \in K_i$ (a set of SIs with central monoliths in a variety $V_i^{\mathfrak{C}}$ with cube term).

Reduction lemmas

Lemma (Bulatov, M, Szendrei, 2019)

$\mathrm{SMP}(K)$ above reduces to membership problems for $\mathbf{A} \leq_{\mathrm{sd}} \mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ where for all $i \neq j$:

- $\mathbf{A}_i \in \mathbb{HS}(K)$ is SI with abelian monolith μ_i,
- $\mathbf{A}_i, \mathbf{A}_j$ are similar, $\mathbf{A}_i/(0:\mu_i) \cong \mathbf{A}_j/(0:\mu_j)$,
- $\mathrm{proj}_{ij}(\mathbf{A})/(0:\mu_i) \times (0:\mu_j)$ is the graph of an isomorphism.

Proof.

Uses critical relations (Kearnes, Szendrei, 2012). □

Lemma (M, Szendrei, 2019)

Membership for $\mathbf{A}$ as above reduces to membership for $\mathbf{A}^{\mathfrak{C}} \leq_{\mathrm{sd}} \mathbf{A}_1^{\mathfrak{C}} \times \cdots \times \mathbf{A}_n^{\mathfrak{C}}$ where $\mathbf{A}_i^{\mathfrak{C}}$ is the algebra from $(0:\mu_i)$ in $\mathbf{A}_i$.

Corollary (M, Szendrei 2019)

Let K be a finite set of algebras in a variety with cube term such that

every SI $\mathbf{A} \in \mathbb{HS}(K)$ has a monolith with supernilpotent centralizer.

Then $\mathrm{SMP}(K)$ is in P.

Proof.

- $\mathrm{SMP}(K)$ reduces to several SMPs for supernilpotent algebras by the previous Theorem.
- The latter are in P (M, 2012).

3. Polynomial clones

Theorem (Aichinger, M, McKenzie, 2014)

For every finite algebra $\mathbf{A}$ with cube term there exists a subpower (invariant relation) R of $\mathbf{A}$ such that

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

Question

How to find R from $\mathbf{A}$? Proof is not constructive.

Reducing to SIs with central monolith again

Let $P(\mathbf{A})$ denote the clone of **polynomial functions** on $\mathbf{A}$.

Theorem (M, 2021)

Let $\mathbf{A}$ be a finite Mal'cev algebra.
For each SI $\mathbf{B} \in \mathbb{H}(\mathbf{A})$ with monolith μ:

- Let $\mathbf{B}^{\mathfrak{C}}$ be the algebra from the centralizer$(0 : \mu)$.
  (SI Mal'cev with central monolith)
- Assume $P(\mathbf{B}^{\mathfrak{C}}) = \mathrm{Pol}(R_{\mathbf{B}}^{\mathfrak{C}})$ for some subpower $R_{\mathbf{B}}$ of $\mathbf{B}$.

Then

$$P(\mathbf{A}) = \mathrm{Pol}\big(\,\mathrm{Con}(\mathbf{A}) \cup \{R_{\mathbf{B}} \mid \mathbf{B} \in \mathbb{H}(\mathbf{A}) \text{ is SI}\}\,\big).$$

Reference

P. Mayr and Á. Szendrei. *Algebras from congruences.* Submitted 2019. https://arxiv.org/abs/1910.00689