Algebraische Zugänge zur Beschreibung von Mal'cev-Klonen

Erhard Aichinger

Institut für Algebra
Johannes Kepler Universität Linz

TU Dresden, 24. Jänner 2013

Definition

Eine *Algebra* ist ein Paar $\langle A, (f_1, f_2, \ldots)\rangle$, wobei

- A eine nichtleere Menge,
- $(f_1, f_2, \ldots)$ eine Familie endlichstelliger (totaler) Operationen auf A ist.

Auftreten allgemeiner Algebren

Warum in dieser Allgemeinheit?

- Homomorphismen, Unteralgebren, direkte und subdirekte Produkte, . . . : gemeinsame Strukturtheorie, etwa für nilpotente oder abelsche Algebren, subdirekte Zerlegung (Birkhoff).
- Modelltheoretische Fragen, z.B.: Welche Klassen lassen sich durch Gleichungen definieren?
- Auftreten von allgemeinen Strukturen:
  - Koordinatenstruktur von projektiven Ebenen.
  - Entscheidbarkeitsfragen: Strukturen aus Turing-Maschinen.
  - Klassifikation von Bedingungserfüllungsproblemen (CSP).
  - Neue Methoden und neue Sätze für klassische Strukturen.

Termfunktionen

Definition von Termfunktionen ($\mathrm{Clo}_k(\mathbf{A})$)

Sei $\mathbf{A} = \langle A, F \rangle$ eine Algebra, $k \in \mathbb{N}$. $\mathrm{Clo}_k(\mathbf{A})$ is die Unteralgebra von

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

die von den Projektionen $\{\pi_1^{(k)}, \pi_2^{(k)}, \dots, \pi_k^{(k)}\}$ erzeugt wird.
Dabei gilt
$\pi_i^{(k)} : A^k \to A,\ \pi_i^{(k)}(x_1, \dots, x_k) := x_i$ für $x_1, \dots, x_k \in A$.

Beispiel

$\mathbf{S} = (S, \cdot)$ Halbgruppe, $k = 3$. Dann gilt

$$\alpha := \pi_1^{(3)} \cdot \pi_3^{(3)} \cdot \pi_2^{(3)} \cdot \pi_2^{(3)} \in \mathrm{Clo}_3(\mathbf{S}).$$

Es gilt

$$\alpha(x_1, x_2, x_3) = x_1 \cdot x_3 \cdot x_2 \cdot x_2 \text{ für alle } x_1, x_2, x_3 \in S.$$

Termfunktionen = von Termen induzierte Funktionen

Proposition

A Algebra, $k \in \mathbb{N}$. Dann gilt $p \in \mathrm{Clo}_k(\mathbf{A})$ genau dann, wenn es einen Term **t** in der “Sprache von **A**” gibt, sodass

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

für alle $x_1, x_2, \ldots, x_k \in A$.

Polynomfunktionen

Definition von Polynomfunktionen ($\mathrm{Pol}_k(\mathbf{A})$)

Sei $\mathbf{A} = \langle A, F \rangle$ eine Algebra, $k \in \mathbb{N}$. $\mathrm{Pol}_k(\mathbf{A})$ is die Unteralgebra von $\mathbf{A}^{A^k} = \langle \{f : A^k \to A\}, \text{“}F \text{ koordinatenweise”}\rangle$, die von den Projektionen und den konstanten Operationen

- $\pi_i^{(k)} : (x_1, \ldots, x_k) \mapsto x_i \ (i \in \{1, \ldots, k\})$,
- $c_a : (x_1, \ldots, x_k) \mapsto a \ (a \in A)$

erzeugt wird.

Beispiel

$\mathbf{S} = (\mathrm{Mat}_2(\mathbb{Z}_5), \cdot)$ Halbgruppe, $k = 3$. Dann gilt $\alpha := \pi_1^{(3)} \cdot c_{\left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right)} \cdot \pi_3^{(3)} \cdot c_{\left(\begin{smallmatrix} 1 & 4 \\ 1 & 1 \end{smallmatrix}\right)} \in \mathrm{Pol}_3(\mathbb{Z}_5)$, und es gilt

$$\alpha(x_1, x_2, x_3) = x_1 \cdot \left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right) \cdot x_3 \cdot \left(\begin{smallmatrix} 1 & 4 \\ 1 & 1 \end{smallmatrix}\right) \text{ für } x_1, x_2, x_3 \in \mathrm{Mat}_2(\mathbb{Z}_5).$$

Polynomfunktionen = von Termen und Konstanten induzierte Funktionen

Proposition

$\mathbf{A}$ Algebra, $k \in \mathbb{N}$. Dann gilt $\mathbf{p} \in \mathrm{Pol}_k(\mathbf{A})$ genau dann, wenn es einen Term t in der "Sprache von $\mathbf{A}$", $l \in \mathbb{N}_0$ und $a_1, \ldots, a_l \in A$ gibt, sodass

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

für alle $x_1, x_2, \ldots, x_k \in A$.

$$\mathrm{Clo}(\mathbf{A}) := \bigcup_{i \in \mathbb{N}} \mathrm{Clo}_i(\mathbf{A}), \quad \mathrm{Pol}(\mathbf{A}) := \bigcup_{i \in \mathbb{N}} \mathrm{Pol}_i(\mathbf{A})$$

Bestimmen von einstelligen Polynomfunktionen

```
elgar{erhard}: gap

gap> RequirePackage("sonata");
# SONATA by Aichinger, Binder, Ecker, Mayr, Noebauer
# loaded.

gap> G := SymmetricGroup (3);
Sym( [ 1 .. 3 ] )

gap> P := PolynomialNearRing (G);
PolynomialNearRing( Sym( [ 1 .. 3 ] ) )
gap> Size (P);
324

gap> G1 := GroupReduct (P);;

gap> Size (PolynomialNearRing (G1)); time;
4251528
176
```

Bestimmen von einstelligen Polynomfunktionen

```
gap> G := AlternatingGroup (5);
Alt( [ 1 .. 5 ] )

gap> Size (PolynomialNearRing (G));
48873677980689257489322752273774603865660
08501760000000000000000000000000000000000
000000000000000000000000000
gap> time;
3708

gap> 60^60;
48873677980689257489322752273774603865660
08501760000000000000000000000000000000000
000000000000000000000000000
```

Definition

$\mathbf{A} = \langle A, F\rangle$ und $\mathbf{B} = \langle B, G\rangle$ sind polynomäquivalent, wenn $A = B$ und $\mathrm{Pol}\,(\mathbf{A}) = \mathrm{Pol}\,(\mathbf{B})$.

Beispiele polynomäquivalenter Algebren

$$\langle \mathrm{Pot}(M), \Delta, \cap\rangle \sim \langle \mathrm{Pot}(M), \cup, {}'\rangle,$$

da

$$\begin{aligned} x\Delta y &= (x' \cup y)' \cup (x \cup y')' \\ x \cap y &= (x' \cup y')' \end{aligned}$$

$$\begin{aligned} x \cup y &= (x\Delta y)\Delta(x \cap y) \\ x' &= M\Delta x \end{aligned}$$

Polynomäquivalente Algebren

Satz (Grasegger, Horvàth, Kearnes, 2012)

Sei p Primzahl, $n \in \mathbb{N}$. Die Ringe $\mathbb{Z}_{p^n}$ und $\mathbb{Z}_p[t]/(t^n)$ sind isomorph zu polynomäquivalenten Ringen $\Leftrightarrow n \leq 2$ oder ($p = 2$ und $n = 3$).

Algebren modulo Polynomäquivalenz

Aufgabe

Klassifiziere endliche Algebren modulo Polynomäquivalenz.

Teilaufgabe

Sei $\mathbf{A} = \langle A, F \rangle$ eine Algebra. Klassifiziere alle Erweiterungen $\langle A, F \cup G \rangle$ von $\mathbf{A}$ modulo Polynomäquivalenz.

Resultate über Erweiterungen

Beispiele

- $\langle \mathbb{Z}_p, + \rangle$, p Primzahl, hat genau 2 polynominäquivalente Erweiterungen.
- [Aichinger and Mayr, 2007] $\langle \mathbb{Z}_{pq}, + \rangle$, p, q prim, $p \neq q$, hat genau 17 polynominäquivalente Erweiterungen.
- [Mayr, 2008] $\langle \mathbb{Z}_n, + \rangle$, n quadratfrei, hat nur endlich viele polynominäquivalente Erweiterungen.
- [Kaarli and Pixley, 2001] Jede endliche Algebra **A** mit Mal'cev-Term und $\mathrm{typ}(\mathbf{A}) = \{\mathbf{3}\}$ hat nur endlich viele polynominäquivalente Erweiterungen. (Halbeinfache Ringe mit Eins, Gruppen ohne abelsche Kompositionsfaktoren)

Funktionenalgebren (Klone)

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

Definition eines Klons

$\mathcal{C} \subseteq \mathcal{O}(A)$ ist ein Klon auf A :⇔

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

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

$\mathcal{C}^{[n]}$ … die n-stelligen Funktionen in $\mathcal{C}$.

Sei **A** Algebra. Pol(**A**) und Clo(**A**) sind Klone auf A.

Klone sind Mengen von Termfunktionen

Satz

Sei $A \neq \emptyset$, $\mathcal{C} \subseteq \mathcal{O}(A)$. Dann

$$\mathcal{C} \text{ ist Klon auf } A \;\Leftrightarrow\; \exists F \subseteq \mathcal{O}(A) : \mathcal{C} = \mathrm{Clo}(\langle A, F \rangle).$$

Definition

Ein Klon $\mathcal{C} \subseteq \mathcal{O}(A)$ ist *konstantiv* $:\Leftrightarrow \{x \mapsto a \,|\, a \in A\} \subseteq \mathcal{C}^{[1]}$.

Satz

Sei $\mathcal{C} \subseteq \mathcal{O}(A)$. Dann

$$\mathcal{C} \text{ ist konstantiver Klon auf } A \;\Leftrightarrow\; \exists F \subseteq \mathcal{O}(A) : \mathcal{C} = \mathrm{Pol}(\langle A, F \rangle).$$

Funktionale Beschreibung von Klonen

Satz

Seien $f_1, \dots, f_k \in \mathcal{O}(A)$. Dann ist

$$\mathrm{Clo}(\langle A, f_1, \dots, f_k \rangle)$$

der kleinste Klon auf A, der $f_1, \dots, f_k$ enthält.

Beispiel

Der Klon der Polynomfunktionen des Rings $\mathbb{R}$ der rellen Zahlen wird von

$$\{x \mapsto r \mid r \in \mathbb{R}\} \cup \{(x, y) \mapsto x + y\} \cup \{(x, y) \mapsto x\,y\}$$

erzeugt.

Definition

I eine endliche Menge, $\rho \subseteq A^I$, $f : A^n \to A$. f erhält ρ ($f \rhd \rho$) $:\Leftrightarrow$ $\forall v_1, \ldots, v_n \in \rho$:

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

Bemerkung

$f \rhd \rho \iff \rho$ ist Subuniversum von $\langle A, f \rangle^I$.

Definition (Polymorphismen)

Sei R eine Menge von endlichstelligen Relationen auf A, $\rho \in R$.

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

Ein Hauptsatz der Klontheorie ([Bodnarčuk et al., 1969], cf. [Pöschel and Kalužnin, 1979, p.53])

Sei A endlich, $\mathcal{C}$ ein Klon auf A. Dann gibt es eine Menge R von endlichstelligen Relationen auf A, sodass

$$\mathcal{C} = \text{Polym}(R).$$

Beweisskizze:

1. $\mathbf{A} := \langle A, \mathcal{C} \rangle$,
2. $R := \mathbb{S}\mathbb{P}_{<\omega}\mathbf{A}$.

Endliche Beschreibung von Klonen

Definition

Ein Klon $\mathcal{C}$ ist *endlich erzeugbar*, wenn es ein endliches $F \subseteq \mathcal{O}(A)$ gibt, sodass $\mathcal{C} = \text{Clo}(\langle A, F \rangle)$.

Definition

Ein Klon $\mathcal{C}$ ist *endlichrelational* oder *prädikativ beschreibbar*, wenn es eine endliche Menge R von endlichstelligen Relationen gibt, sodass $\mathcal{C} = \text{Polym}(R)$.

Anzahl von Klonen

Satz (Kardinalität des Klonverbands)

Sei A endlich.

1. $|A| \geq 3 \Rightarrow |\{\mathcal{C} \,|\, \mathcal{C}$ Klon auf $A\}| = 2^{\aleph_0}$.
   [Janov and Mučnik, 1959]
2. $|A| = 2 \Rightarrow |\{\mathcal{C} \,|\, \mathcal{C}$ Klon auf$A\}| = \aleph_0$. [Post, 1941]
3. $|A| \geq 3 \Rightarrow |\{\mathcal{C} \,|\, \mathcal{C}$ konstantiver Klon auf $A\}| = 2^{\aleph_0}$.
   [Ágoston et al., 1986]
4. $|A| = 2 \Rightarrow |\{\mathcal{C} \,|\, \mathcal{C}$ konstantiver Klon auf $A\}| = 7$.

Klassifizierung von Algebren mit 2 Elementen

Satz (Klassifikation 2-elementiger Algebren, Konsequenz aus Satz von E. Post, 1941)

Jede Algebra $\langle\{0,1\}, f_1, \ldots\rangle$ ist polynomäquivalent zu einer der folgenden 7 Algebren: $\langle\{0,1\}, \emptyset\rangle$, $\langle\{0,1\}, \vee\rangle$, $\langle\{0,1\}, \wedge\rangle$, $\langle\{0,1\}, \vee, \wedge\rangle$, $\langle\{0,1\}, \vee, \wedge, \neg\rangle$, $\langle\{0,1\}, \neg\rangle$, $\langle\{0,1\}, \oplus_2\rangle$.

Algebren mit n Elementen

Versuch der Klassifikation n-elementiger Algebren

Sei $n \geq 3$. Jede Algebra $\langle \{0, 1, 2, \ldots, n-1\}, f_1, \ldots \rangle$ ist polynomäquivalent zu einer der folgenden x Algebren.

Satz [Ágoston et al., 1986]

$x = 2^{\aleph_0}$.

Algebren mit n Elementen

Versuch der Klassifikation n-elementiger Algebren

Sei $n \geq 3$. Jede Algebra $\langle\{0, 1, 2, \dots, n-1\}, f_1, \dots\rangle$ ist polynomäquivalent zu einer der folgenden x Algebren.

Satz [Ágoston et al., 1986]

$x = 2^{\aleph_0}$.

Modifizierte Frage

Frage (R. McKenzie (2002), P. Idziak (1999))

Sei A eine endliche Menge. Wieviele polynominäquivalente Algebren $\langle A, f_1, f_2 \ldots \rangle$ gibt es, für die sich aus den Operationen $f_1, f_2 \ldots$ zumindest eine zweistellige Operation $*$ bauen lässt, sodass $\langle A, * \rangle$ eine Gruppe ist, also $\mathrm{Pol}_2(\langle A, f_1, f_2 \ldots \rangle)$ eine Gruppenmultiplikation enthält?

Teilantworten

- Endlich viele, wenn $|A|$ prim ist.
- Genau $\aleph_0$ viele, wenn $|A| = p^2$ mit p prim ist [Bulatov, 2002].
- Endlich viele, wenn $|A| = p\,q$ ist, und $p \neq q$. ([Aichinger and Mayr, 2007])
- Endlich viele, wenn $|A| = p_1 p_2 \cdots p_k$ mit lauter verschiedenen p_i ist ([Mayr, 2008])

Mal'cev-Operationen

Definition

A Menge. Eine Funktion $d : A^3 \to A$ ist eine Mal'cev-Operation $:\Leftrightarrow d(a, a, b) = d(b, a, a) = b$ für alle $a, b \in A$. Prototyp: $d(x, y, z) := x - y + z$.

Eine Algebra ist eine *Mal'cev-Algebra*, wenn es unter ihren ternären Termfunktionen eine Mal'cev-Operation gibt.[1]

Satz [Mal'cev, 1954]

$\mathbf{A}$ ist Mal'cev-Algebra $\Leftrightarrow$
$\forall \mathbf{B} \in \mathbb{HSP}(\mathbf{A})\ \forall \alpha, \beta \in \mathrm{Con}(\mathbf{A}) : \alpha \circ \beta = \beta \circ \alpha$.

Ein Klon ist ein *Mal'cev-Klon* wenn er eine Mal'cev-Operation enthält.

[1] *Algebra mit Mal'cev-Term*, falls *Mal'cev-Algebra* mit anderer Bedeutung verwendet wird.

Frage zur Anzahl von Mal'cev-Algebren

Frage [Bulatov and Idziak, 2003, Problem 8]

- A endliche Menge. Wie viele polynominäquivalente Mal'cev-Algebren gibt es auf A? (endlich für $|A| \leq 3$, $\aleph_0$ für $|A| = 4$, und $\geq \aleph_0$ für $|A| \geq 5$ [Idziak, 1999]).
- A endliche Menge. Wie viele konstantive Klone auf A enthalten eine Mal'cev-Operation?
- *Gibt es eine endliche Menge mit überabzählbar vielen konstantiven Mal'cev-Klonen?*

Konstantive Mal’cev-Klone sind prädikativ beschreibbar

Satz [Aichinger, 2010]

Sei A eine endliche Menge, und sei $\mathcal{M}$ die Menge aller konstantiven Mal’cev-Klone auf A. Dann gilt:

1. $(\mathcal{M}, \subseteq)$ hat keine unendlich absteigenden Ketten.
2. Für jedes $\mathcal{C} \in \mathcal{M}$ gibt es eine endlichstellige Relation ρ, sodass $\mathcal{C} = \mathrm{Polym}(\{\rho\})$.
3. $\mathcal{M}$ ist endlich oder abzählbar unendlich.

Klone mit Kantentermen sind prädikativ beschreibbar

Definition

Eine k-stellige Operation ist eine *Kantenoperation* $:\Leftrightarrow \ldots$

3-stellige Kantenoperationen $\triangleq$ Mal'cev-Operationen. Aus einer Majoritätsoperation enthält man eine 4-stellige Kantenoperation.

Satz (Aichinger, Mayr, McKenzie, 2010)

A endliche Menge, $k \geq 3$, $\mathcal{M}_k$ die Menge aller Klone auf A, die einen k-stelligen Kantenterm enthalten. Dann gilt:

1. $(\mathcal{M}_k, \subseteq)$ hat keine unendlich absteigenden Ketten.
2. Für jedes $\mathcal{C} \in \mathcal{M}_k$ gibt es eine endlichstellige Relation ρ, sodass $\mathcal{C} = \text{Polym}(\{\rho\})$.
3. $\mathcal{M}_k$ ist endlich oder abzählbar unendlich.

Eine Konsequenz für Gruppen

Korollar

Sei G endliche Gruppe. Dann gibt es $k \in \mathbb{N}$, $H \leq G^k$, sodass $\mathcal{S} := \bigcup_{n\in\mathbb{N}} \mathrm{Sub}(G^n)$ die kleinste Menge ist, für die folgendes gilt:

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

Konsequenzen

Mal'cev-Algebren

1. Bis auf Termäquivalenz und Isomorphismus gibt es nur abzählbar viele endliche Mal'cev-Algebren.
2. Jede Mal'cev-Algebra, auch wenn sie unendlich viele Operationen hat, kann durch eine einzige endlichstellige Relation dargestellt werden.

Konsequenzen für den Klonverband

Sei $\mathcal{C}$ ein Mal'cev-Klon auf der endlichen Menge A.

1. Das Intervall $\mathbb{I}[\mathcal{C}, \mathcal{O}(A)]$ hat nur endlich viele Atome [Pöschel and Kalužnin, 1979].
2. Jeder Klon $\mathcal{D}$ mit $\mathcal{C} \subset \mathcal{D}$ enthält eines dieser Atome.
3. Wenn $\mathbb{I}[\mathcal{C}, \mathcal{O}(A)]$ unendlich viele Klone enthält, so enthält es einen Klon, der nicht endlich erzeugbar ist. (cf. Königs Lemma).

Algebraische Methoden in der Beschreibung von Klonen

Ziel

Beschreibung eines Klons $\mathcal{C} = \langle F \rangle$ auf A durch Analyse der Algebren $\langle A, \mathcal{C} \rangle$ und $\langle A, F \rangle$.

Klassische Algebren als Teil eines Klons

Satz (Artin-Wedderburn, Wedderburn 1907)

R endlicher Ring mit Eins, M ein treuer einfacher unitärer R-Modul, $R \subseteq \mathrm{End}(M,+)$, $r * m := r(m)$. Dann gilt

$$R = \mathrm{Polym}_M^{[1]}(S),$$

wobei $S = \{\mathrm{Graph}(e) \mid e \in \mathrm{End}_R(M,+)\} \cup \{\mathrm{Graph}(+)\}$.

Satz (Wielandt-Betsch, [Betsch, 1973])

$\langle N,+,\circ\rangle$ endlicher Fastring mit Eins, $N \circ 0 = 0$, Γ treue endliche unitäre N-Gruppe ohne nichttriviale N-Untergruppen, $N \subseteq \Gamma^\Gamma$, $n * \gamma := n(\gamma)$. Dann gilt:

$$N = \mathrm{Polym}_M^{[1]}(S),$$

wobei $S = \{\mathrm{Graph}(e) \mid e \in \mathrm{End}_N(\Gamma,+)\}$. $S = G \cup \{0\}$, wobei $G \leq_{\mathrm{fpf}} \mathrm{Aut}(\Gamma,+)$.

Polynomvollständigkeit

Frage

Gegeben: $\mathbf{A}$ endliche Algebra.
Gesucht: R mit $\mathrm{Pol}(\mathbf{A}) = \mathrm{Polym}(R)$.

Polynomvollständigkeitseigenschaften

Beschreibe die Algebren $\mathbf{A}$, für die eine “offensichtliche” Wahl von R stimmt.

1. Gilt $\mathrm{Pol}(\mathbf{A}) = \mathcal{O}(\mathbf{A}) = \mathrm{Polym}(\emptyset)$? Ist $\mathbf{A}$ polynomvollständig?
2. $\mathrm{Pol}(\mathbf{A}) = \mathrm{Polym}(\mathrm{Con}(\mathbf{A}))$? Ist $\mathbf{A}$ affin vollständig?
3. Andere Eigenschaften: polynomreich, schwach polynomreich. Für Verbände: ordnungspolynomvollständig, ordnungsaffin vollständig.

Beispiel eines Satzes über affin vollständige Gruppen

Satz [Aichinger, 2002, Ecker, 2006]

$\mathbf{A}, \mathbf{B}$ nilpotente affin vollständige Gruppen. $\mathbf{G} = \mathbf{A} \rtimes \mathbf{B}$,
$\mathbf{B} \not\leq C_{\mathbf{G}}(\mathbf{A})$, $\{x \mapsto b^{-1} \cdot x \cdot b \mid b \in B\} \leq_{\text{fpf}} \langle \text{Aut}(\mathbf{A}) \cap \text{Pol}(\mathbf{A}), \circ \rangle$.
Dann ist $\mathbf{G}$ affin vollständig.

Beispiel

$\mathbf{A} := C_3 \times C_3$, $\mathbf{B} := C_2 \times C_2$, $\mathbf{G} = C_2 \times \text{Dih}(C_3 \times C_3)$. Dann ist $\mathbf{G}$ affin vollständig.

Bemerkung

[Aichinger and Mudrinski, 2009] untersucht Polynomvollständigkeitseigenschaften für bestimmte erweiterte Gruppen. Man erhält für manche $\mathbf{A}$ ein $m \in \mathbb{N}$ (oft $m \leq 4$) mit

$$\text{Polym}(\mathbb{S}((\mathbf{A}^*)^m)) = \text{Pol}(\mathbf{A}).$$

Aussagen mithilfe von Con($\mathbf{A}$)

Definition

$\mathcal{C}$ Klon auf A, $\mathbf{A} := \langle A, \mathcal{C} \rangle$, $\mathbb{L} := \mathrm{Con}(\mathbf{A}) = \mathbb{S}(\mathbf{A} \times \mathbf{A}) \cap \mathrm{\ddot{A}qv}(A)$.

Satz ([Aichinger, 2001] für erweiterte Gruppen, [Kaarli and Mayr, 2010] für Mal'cev-Algebren)

$\mathbf{A}$ endliche Mal'cev-Algebra, $\mu, \eta \in \mathrm{Con}(\mathbf{A})$ so, dass $\mu \vee \eta = 1_A$, $\mu \wedge \eta = 0_A$, $\forall \gamma \in \mathrm{Con}(\mathbf{A}) : (\gamma \wedge \mu) \vee (\gamma \wedge \eta) = \gamma$, $n \in \mathbb{N}$.

$$\Phi : \mathrm{Pol}_n(\mathbf{A}) \to \mathrm{Pol}_n(\mathbf{A}/\mu) \times \mathrm{Pol}_n(\mathbf{A}/\eta), \Phi(p) := (p/\mu, p/\eta).$$

Dann ist Φ bijektiv.

Aussagen mithilfe von Con(**A**)

Konsequenz

$\mathcal{C}$ konstantiver Mal'cev-Klon, $\mathbf{A} := \langle A, \mathcal{C} \rangle$, $\mu, \eta \in \mathrm{Con}(\mathbf{A})$ so, dass $\mu \vee \eta = 1_A$, $\mu \wedge \eta = 0_A$,

$$\forall \gamma \in \mathrm{Con}(\mathbf{A}) : (\gamma \wedge \mu) \vee (\gamma \wedge \eta) = \gamma,$$

und sei $n \in \mathbb{N}$.
Dann gibt es konstantive Mal'cev-Klone $\mathcal{D}$ und $\mathcal{E}$ auf A/μ und A/η,

$$\Phi : \mathcal{C}^{[n]} \to \mathcal{D}^{[n]} \times \mathcal{E}^{[n]}, \ \Phi(p) := (p/\mu, p/\eta).$$

bijektiv ist.

$$\mathcal{C} \cong \mathcal{D} \times \mathcal{E}$$

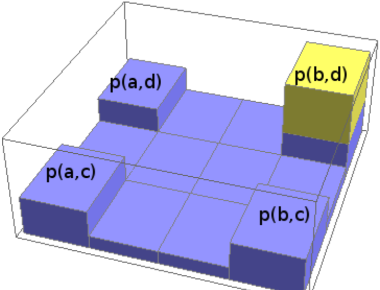
Binäre Kommutatoren

Lemma (Beschreibung binärer Kommutatoren [Aichinger and Mudrinski, 2010])

A Mal'cev-Algebra, $\alpha, \beta \in \mathrm{Con}(\mathbf{A})$. Dann ist $[\alpha, \beta]$ die Kongruenz, die von

$$\{(p(a,c), p(b,d)) \mid (a,b) \in \alpha, (c,d) \in \beta, p \in \mathrm{Pol}_2(\mathbf{A}),\\ p(a,c) = p(a,d) = p(b,c)\}.$$

erzeugt wird.



Binäre Kommutatoren für erweiterte Gruppen

Lemma (Beschreibung des binären Kommutators [Scott, 1997])

$\mathbf{V}$ erweiterte Gruppe, $A, B \trianglelefteq \mathbf{V}$. Dann wird $[A, B]$ von

$$\{p(a,b) \,|\, a \in A, b \in B, p \in \mathrm{Pol}_2(\mathbf{V}), \\ p(0,0) = p(a,0) = p(0,b) = 0\},$$

und ebenso von

$$\{p(a,b) \,|\, a \in A, b \in B, q \in \mathrm{Pol}_2(\mathbf{V}), \\ q(x,0) = q(0,x) \text{ for all } x \in V\}.$$

erzeugt.

Remark: $q(x,y) := p(x,y) - p(x,0) + p(0,0) - p(0,y)$.

Höhere Kommutatoren

Definition höherer Kommutatoren [Bulatov, 2001]

- Für $n \in \mathbb{N}$ hat [Bulatov, 2001] n-stellige Kommutatoren mithilfe von Polynomfunktionen definiert.
- Der n-stellige Kommutator von $\alpha_1, \ldots, \alpha_n \in \mathrm{Con}(\mathbf{A})$ ist eine Kongruenz $\gamma := [\alpha_1, \ldots, \alpha_n]$ von $\mathbf{A}$.
- [Mudrinski, 2009, Aichinger and Mudrinski, 2010] untersuchen diese Kommutatoren für Mal'cev-Algebren.

Nilpotenz

Definition der unteren Zentralreihe

$\gamma_1(\mathbf{A}) := 1_A$, $\gamma_n(\mathbf{A}) := [1_A, \gamma_{n-1}(\mathbf{A})]$ für $n \geq 2$.

Nilpotenz

$\mathbf{A}$ Mal'cev-Algebra. $\mathbf{A}$ ist *nilpotent von Klasse* k $:\Leftrightarrow \gamma_k(\mathbf{A}) \neq 0_A$, $\gamma_{k+1}(\mathbf{A}) = 0_A$.

Die "untere Superreihe"

$\sigma_n(\mathbf{A}) := [\underbrace{1_A, \ldots, 1_A}_{n}]$.

Supernilpotenz

$\mathbf{A}$ Mal'cev-Algebra. $\mathbf{A}$ ist *supernilpotent von Klasse* k $:\Leftrightarrow$ $\sigma_k(\mathbf{A}) \neq 0_A$, $\sigma_{k+1}(\mathbf{A}) = 0_A$.

Charakterisierung der Supernilpotenz durch das freie Spektrum

Satz (cf. [Berman and Blok, 1987])

$\mathbf{A}$ endliche Mal'cev-Algebra, $k \in \mathbb{N}$. Äquivalent sind:

1. $\exists p \in \mathbb{R}[t] : \deg(p) = k$ und $|\mathbf{F}_{\mathcal{V}(\mathbf{A})}(n)| \leq 2^{p(n)}$ für alle $n \in \mathbb{N}$.
2. $\mathbf{A}$ ist supernilpotent von Klasse $\leq k$.

Verbindungen zwischen Supernilpotenz und Nilpotenz

Satz (Supernilpotenz impliziert Nilpotenz [Mudrinski, 2009])

A Mal'cev-Algebra, supernilpotent von Klasse k. Dann ist **A** nilpotent von Klasse $\leq k$.

Bemerkung (Nilpotenz impliziert i.A. nicht Supernilpotenz)

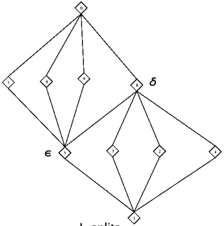
- $\mathbf{N}_6 := \langle \mathbb{Z}_6, +, f \rangle$ with $f(0) = f(3) = 3$, $f(1) = f(2) = f(4) = f(5) = 0$ ist nilpotent von Klasse 2 und nicht supernilpotent.
- $\langle \mathbb{Z}_4, +, 2x_1x_2, 2x_1x_2x_3, 2x_1x_2x_3x_4, \ldots \rangle$ ist nilpotent von Klasse 2 und nicht supernilpotent.

Aufspaltbare Verbände

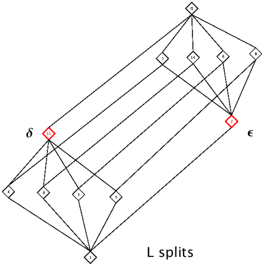
Definition

$\mathbb{L}$ Verband. $\mathbb{L}$ ist *aufspaltbar* $:\Leftrightarrow \exists \varepsilon, \delta \in \mathbb{L}$: $0 < \varepsilon$, $\delta < 1$ und

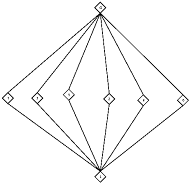
$$\forall \alpha \in \mathbb{L} : \alpha \geq \varepsilon \text{ or } \alpha \leq \delta.$$



L splits



L splits



L does not split

Algebren mit nicht aufspaltbarem Kongruenzverband

Satz [Aichinger and Mudrinski, 2012]

$\mathbf{A}$ endliche Mal'cev-Algebra. Wenn $\mathrm{Con}(\mathbf{A})$ nicht aufspaltbar ist, dann ist $\mathbf{A}$ supernilpotent.

Korollar

Der Kongruenzverband einer endlichen nicht nilpotenten Mal'cev-Algebra ist aufspaltbar.

Endliche Erzeugbarkeit aus Supernilpotenz

Satz [Aichinger and Mudrinski, 2010, Proposition 6.18]

Sei A endlich, $\mathcal{C}$ konstantiver Klon auf A. Wenn $\mathbf{A} = \langle A, \mathcal{C} \rangle$ supernilpotent ist, dann ist $\mathcal{C}$ endlich erzeugbar.

Korollar

Jeder konstantive Klon $\mathcal{C}$ auf endlichem A, für den $\mathrm{Con}(\langle A, \mathcal{C} \rangle)$ nicht aufspaltbar ist, ist endlich erzeugbar.

Klon der kongruenzerhaltenden Funktionen

Satz (EA, unveröffentlicht)

$\mathbf{A}$ endliche Mal'cev-Algebra, Con($\mathbf{A}$) einfacher Verband, $|\mathrm{Con}(\mathbf{A})| > 2$. Äquivalent sind:

1. $\mathcal{C} := \mathrm{Comp}(\mathbf{A}) = \mathrm{Polym}(\mathrm{Con}(\mathbf{A}))$ ist endlich erzeugbar.
2. Con($\mathbf{A}$) ist nicht aufspaltbar.

Offene Fragen in der Klontheorie

Welche der folgenden Fragen sind algorithmisch lösbar?

Gleichheit von Klonen

- Gegeben: A endlich, $f_1, \ldots, f_k \in \mathcal{O}(A)$, $\rho \subseteq A^l$.
- Gesucht: Gilt $\mathrm{Clo}(\langle A, f_1, \ldots, f_k \rangle) = \mathrm{Polym}(\rho)$?

Endliche Erzeugbarkeit

- Gegeben: A endlich, $\rho \subseteq A^l$.
- Gesucht: Ist $\mathrm{Polym}(\{\rho\})$ endlich erzeugbar?

Endlichrelationalität

- Gegeben: A endlich, $f_1, \ldots, f_k \in \mathcal{O}(\mathbf{A})$.
- Gesucht: Ist $\mathrm{Clo}(\langle A, f_1, \ldots, f_k \rangle)$ endlichrelational? Wenn ja, wie groß sind die Relationen?

Berechenbare Schranke für die Stelligkeit der benötigten Relationen

- Gegeben: $\mathbf{A} = \langle A, F \rangle$ endliche Mal'cev-Algebra (oder: Gruppe, Ring, Modul, ...).
- Gesucht: $m \in \mathbb{N}$, sodass $\mathrm{Clo}(\mathbf{A}) = \mathrm{Polym}(\mathbb{S}(\mathbf{A}^m))$ bzw. $\mathrm{Pol}(\mathbf{A}) = \mathrm{Polym}(\mathbb{S}((\mathbf{A}^*)^m))$.

Offene Fragen zu Mal’cev-Klonen

Satz

A endlich. $\mathcal{M} :=$ Menge aller Klone mit Mal’cev-Operation. Dann besitzt $\langle \mathcal{M}, \subseteq \rangle$ keine unendlichen absteigenden Ketten, und für $|A| \geq 4$ unendliche aufsteigende Ketten.

Frage

Unendliche Antiketten?

Offene Fragen zur Termäquivalenz

Termäquivalenz mit Länge der Terme

$\mathbf{A} = \langle A, F \rangle$ und $\mathbf{B} = \langle A, G \rangle$ sind *stark termäquivalent* $:\Leftrightarrow$ es gibt $p \in \mathbb{R}[x]$:

1. $\forall$s in der Sprache von **B** $\exists$t in der Sprache von **A** mit $||\mathrm{t}|| \leq p(||\mathrm{s}||)$ und $\mathrm{s}^{\mathbf{B}} = \mathrm{t}^{\mathbf{A}}$
2. und umgekehrt.

Länge von Termen

Syntaktische Komplexität

A Algebra.

$$\gamma_{\mathbf{A}}(n) := \min\{m \in \mathbb{N} \,|\, \forall f \in \mathrm{Clo}_n\mathbf{A}\ \exists \mathrm{t} : ||\mathrm{t}|| \leq m \text{ und } \mathrm{t}^{\mathbf{A}} = f\}.$$

Satz (Horvàth und Nehaniv, unveröffentlicht)

G Gruppe.

1. **G** nilpotent von der Klasse $k \Rightarrow \gamma_{\mathbf{G}^*}(n) \leq C(\mathbf{G}) \cdot n^k$.
2. **G** einfach und nicht abelsch $\Rightarrow \gamma_{\mathbf{G}^*}(n) \leq C(\mathbf{G}) \cdot n^8 \cdot |G|^n$.

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. (2001).
On near-ring idempotents and polynomials on direct products of Ω-groups.
Proc. Edinburgh Math. Soc. (2), 44:379–388.

Aichinger, E. (2002).
The polynomial functions on certain semidirect products of groups.
Acta Sci. Math. (Szeged), 68(1-2):63–81.

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).
Some applications of higher commutators in Mal'cev algebras.
Algebra Universalis, 63(4):367–403.

Aichinger, E. and Mudrinski, N. (2012).
Sequences of commutator operations.
submitted; available on arXiv:1205.3297v3 [math.RA] 24 May 2012.

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

Betsch, G. (1973).
Some structure theorems on 2-primitive near-rings.
Colloq. Math. Soc. János Bolyai, Vol. 6, pages 73–102.

Bodnarčuk, V. G., Kalužnin, L. A., Kotov, V. N., and Romov, B. A. (1969).
Galois theory for Post algebras. I, II.
Kibernetika (Kiev), (3):1–10; ibid. 1969, no. 5, 1–9.

Bulatov, A. (2001).
On the number of finite Mal'tsev algebras.
In *Contributions to general algebra, 13 (Velké Karlovice, 1999/Dresden, 2000)*, pages 41–54. Heyn, Klagenfurt.

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.

Ecker, J. (2006).
Affine completeness of generalised dihedral groups.
Canad. Math. Bull., 49(3):347–357.

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

Janov, J. I. and Mučnik, A. A. (1959).
Existence of k-valued closed classes without a finite basis.
Dokl. Akad. Nauk SSSR, 127:44–46.

Kaarli, K. and Mayr, P. (2010).
Polynomial functions on subdirect products.
Monatsh. Math., 159(4):341–359.

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

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.

Mudrinski, N. (2009).
On Polynomials in Mal'cev Algebras.
PhD thesis, University of Novi Sad.
http://people.dmi.uns.ac.rs/~nmudrinski/Disserta

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

Post, E. L. (1941).
The two-valued iterative systems of mathematical logic.
(Annals of Mathematics Studies. 5) Princeton, N.J.: Princeton University Press, VIII, 122 p.

Scott, S. D. (1997).
The structure of Ω-groups.
In *Nearrings, nearfields and K-loops (Hamburg, 1995)*, pages 47–137. Kluwer Acad. Publ., Dordrecht.