Polynomial Clones on Squarefree Groups

Peter Mayr

University of Colorado at Boulder
Johannes Kepler Universität, Linz, Austria
peter.mayr@jku.at

Nashville, June 15, 2007

Clones

Definition. A set of finitary functions C on a set A is a *clone* if

- C contains all projections $p_i^{(k)} : A^k \to A, (x_1, \ldots, x_k) \mapsto x_i$,
- C is closed under composition, $\forall f \in C_k, g_1, \ldots, g_k \in C_n$:

$$f(g_1, \ldots, g_k) : A^n \to A,\ \bar{x} \mapsto f(g_1(\bar{x}), \ldots, g_k(\bar{x})) \text{ is in } C_n.$$

Clones

Definition. A set of finitary functions C on a set A is a *clone* if

- C contains all projections $p_i^{(k)} : A^k \to A, (x_1, \dots, x_k) \mapsto x_i$,
- C is closed under composition, $\forall f \in C_k, g_1, \dots, g_k \in C_n$:

$$f(g_1, \dots, g_k) : A^n \to A,\ \bar{x} \mapsto f(g_1(\bar{x}), \dots, g_k(\bar{x})) \text{ is in } C_n.$$

Some classical results.

clones on a finite set A:	$\aleph_0$ if $\lvert A \rvert = 2$, c else
clones containing all constants:	7 if $\lvert A \rvert = 2$, c else
constants and a Mal'cev operation:	finite iff $\lvert A \rvert \leq 3$ (Idziak, 1999)

Polynomial clones on groups

$\mathrm{Pol}(\mathbf{A})$ ... smallest clone that contains all constant functions and all operations F of an algebra $\mathbf{A} := \langle A, F \rangle$.

Examples.

- $\mathrm{Pol}(\mathbb{Z}_2, +)$ ... e.g. $(x_1, x_2) \mapsto x_1 + x_2 + 1$.
  $\mathrm{Pol}(\mathbb{Z}_2, +, \cdot)$ ... all (polynomial) functions.

Polynomial clones on groups

$\mathrm{Pol}(\mathbf{A})$ … smallest clone that contains all constant functions and all operations F of an algebra $\mathbf{A} := \langle A, F \rangle$.

Examples.

- $\mathrm{Pol}(\mathbb{Z}_2, +)$ … e.g. $(x_1, x_2) \mapsto x_1 + x_2 + 1$.
  $\mathrm{Pol}(\mathbb{Z}_2, +, \cdot)$ … all (polynomial) functions.
- Let $\mathbf{A}_k := \langle \mathbb{Z}_4, +, 2x_1 \dots x_k \rangle$.

$$\mathrm{Pol}(\mathbb{Z}_4, +) \subsetneq \mathrm{Pol}(\mathbf{A}_2) \subsetneq \mathrm{Pol}(\mathbf{A}_3) \subsetneq \dots$$

Polynomial clones on groups

$\mathrm{Pol}(\mathbf{A})$ ... smallest clone that contains all constant functions and all operations F of an algebra $\mathbf{A} := \langle A, F \rangle$.

Examples.

- $\mathrm{Pol}(\mathbb{Z}_2, +)$ ... e.g. $(x_1, x_2) \mapsto x_1 + x_2 + 1$.
  $\mathrm{Pol}(\mathbb{Z}_2, +, \cdot)$ ... all (polynomial) functions.
- Let $\mathbf{A}_k := \langle \mathbb{Z}_4, +, 2x_1 \dots x_k \rangle$.

$$\mathrm{Pol}(\mathbb{Z}_4, +) \subsetneq \mathrm{Pol}(\mathbf{A}_2) \subsetneq \mathrm{Pol}(\mathbf{A}_3) \subsetneq \dots$$

Conjectures. (Idziak, 1999) Let n be squarefree.

1. Only finitely many clones contain $\mathrm{Pol}(\mathbb{Z}_n, +)$.
2. For $\mathbf{A} := \langle \mathbb{Z}_n, \{+\} \cup F \rangle$, $\mathrm{Pol}(\mathbf{A})$ is uniquely determined by $\mathrm{Con}(\mathbf{A}, \wedge, \vee, [.,.])$.

Polynomial clones on groups

$\mathrm{Pol}(\mathbf{A})$ ... smallest clone that contains all constant functions and all operations F of an algebra $\mathbf{A} := \langle A, F \rangle$.

Examples.

- $\mathrm{Pol}(\mathbb{Z}_2, +)$ ... e.g. $(x_1, x_2) \mapsto x_1 + x_2 + 1$.
  $\mathrm{Pol}(\mathbb{Z}_2, +, \cdot)$ ... all (polynomial) functions.
- Let $\mathbf{A}_k := \langle \mathbb{Z}_4, +, 2x_1 \dots x_k \rangle$.

$$\mathrm{Pol}(\mathbb{Z}_4, +) \subsetneq \mathrm{Pol}(\mathbf{A}_2) \subsetneq \mathrm{Pol}(\mathbf{A}_3) \subsetneq \dots$$

Conjectures. (Idziak, 1999) Let n be squarefree.

1. Only finitely many clones contain $\mathrm{Pol}(\mathbb{Z}_n, +)$.
2. For $\mathbf{A} := \langle \mathbb{Z}_n, \{+\} \cup F \rangle$, $\mathrm{Pol}(\mathbf{A})$ is uniquely determined by $\mathrm{Con}(\mathbf{A}, \wedge, \vee, [.,.])$. False if 4 primes divide n.

Polynomial clones on groups

$\mathrm{Pol}(\mathbf{A})$ ... smallest clone that contains all constant functions and all operations F of an algebra $\mathbf{A} := \langle A, F\rangle$.

Examples.

- $\mathrm{Pol}(\mathbb{Z}_2, +)$ ... e.g. $(x_1, x_2) \mapsto x_1 + x_2 + 1$.
  $\mathrm{Pol}(\mathbb{Z}_2, +, \cdot)$ ... all (polynomial) functions.
- Let $\mathbf{A}_k := \langle \mathbb{Z}_4, +, 2x_1 \dots x_k\rangle$.

$$\mathrm{Pol}(\mathbb{Z}_4, +) \subsetneq \mathrm{Pol}(\mathbf{A}_2) \subsetneq \mathrm{Pol}(\mathbf{A}_3) \subsetneq \dots$$

Conjectures. (Idziak, 1999) Let n be squarefree.

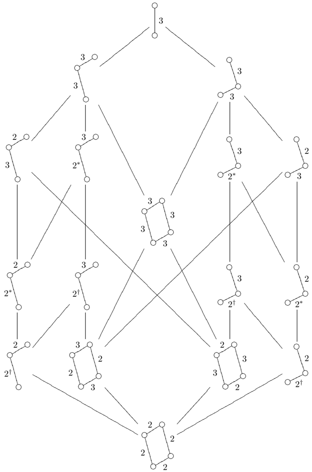
1. Only finitely many clones contain $\mathrm{Pol}(\mathbb{Z}_n, +)$. True.
2. For $\mathbf{A} := \langle \mathbb{Z}_n, \{+\} \cup F\rangle$, $\mathrm{Pol}(\mathbf{A})$ is uniquely determined by $\mathrm{Con}(\mathbf{A}, \wedge, \vee, [.,.])$. False if 4 primes divide n.

Results

Theorem. (PM, submitted 2007)
For an algebra $\mathbf{A}$ with squarefree group reduct, $\mathrm{Pol}(\mathbf{A})$ is determined by $\mathrm{Pol}_2(\mathbf{A})$.

Corollary. (PM, submitted 2007)
There are only finitely many clones on A that contain a group operation and all constants iff $|A|$ is squarefree.

Polynomial clones on $\langle \mathbb{Z}_{pq}, + \rangle$ (Aichinger, PM, 2007)



Outline of the proof of the Theorem.

Let **A** have a squarefree group reduct. Show

$$\mathrm{Pol}(\mathbf{A}) = \{f : A^k \to A \;\mid\; k \in \mathbb{N} \text{ and } f(g_1, \ldots, g_k) \in \mathrm{Pol}_2(\mathbf{A}) \; \forall g_1, \ldots, g_k \in \mathrm{Pol}_2(\mathbf{A})\}.$$

Outline of the proof of the Theorem.

Let **A** have a squarefree group reduct. Show

$$\mathrm{Pol}(\mathbf{A}) = \{f : A^k \to A \mid k \in \mathbb{N} \text{ and } f(g_1, \dots, g_k) \in \mathrm{Pol}_2(\mathbf{A}) \; \forall g_1, \dots, g_k \in \mathrm{Pol}_2(\mathbf{A})\}.$$

1. Reduce to **A** with cyclic group reduct.
   [**Lemma.** For a group $\langle A, \cdot \rangle$ with cyclic Sylow subgroups there is $+$ in $\mathrm{Pol}_2(A, \cdot)$ such that $\langle A, + \rangle$ is a cyclic group.]

Outline of the proof of the Theorem.

Let **A** have a squarefree group reduct. Show

$$\mathrm{Pol}(\mathbf{A}) = \{f : A^k \to A \mid k \in \mathbb{N} \text{ and } f(g_1, \ldots, g_k) \in \mathrm{Pol}_2(\mathbf{A}) \; \forall g_1, \ldots, g_k \in \mathrm{Pol}_2(\mathbf{A})\}.$$

1. Reduce to **A** with cyclic group reduct.
   [**Lemma.** For a group $\langle A, \cdot \rangle$ with cyclic Sylow subgroups there is $+$ in $\mathrm{Pol}_2(A, \cdot)$ such that $\langle A, + \rangle$ is a cyclic group.]
2. Reduce to subdirectly irreducible **A** with monolith μ.

Outline of the proof of the Theorem.

Let **A** have a squarefree group reduct. Show

$$\mathrm{Pol}(\mathbf{A}) = \{f : A^k \to A \mid k \in \mathbb{N} \text{ and } f(g_1, \ldots, g_k) \in \mathrm{Pol}_2(\mathbf{A}) \; \forall g_1, \ldots, g_k \in \mathrm{Pol}_2(\mathbf{A})\}.$$

1. Reduce to **A** with cyclic group reduct.
   [**Lemma.** For a group $\langle A, \cdot \rangle$ with cyclic Sylow subgroups there is $+$ in $\mathrm{Pol}_2(A, \cdot)$ such that $\langle A, + \rangle$ is a cyclic group.]
2. Reduce to subdirectly irreducible **A** with monolith μ.
3. Determine the polynomial functions $A^k \to 0/\mu$.

Outline of the proof of the Theorem.

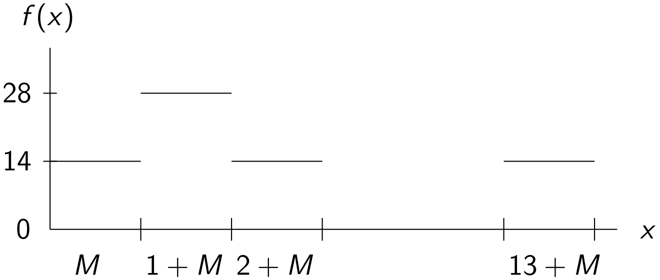
Let **A** have a squarefree group reduct. Show

$$\mathrm{Pol}(\mathbf{A}) = \{f : A^k \to A \mid k \in \mathbb{N} \text{ and } f(g_1,\dots,g_k) \in \mathrm{Pol}_2(\mathbf{A}) \; \forall g_1,\dots,g_k \in \mathrm{Pol}_2(\mathbf{A})\}.$$

1. Reduce to **A** with cyclic group reduct.
   [**Lemma.** For a group $\langle A,\cdot\rangle$ with cyclic Sylow subgroups there is $+$ in $\mathrm{Pol}_2(A,\cdot)$ such that $\langle A,+\rangle$ is a cyclic group.]
2. Reduce to subdirectly irreducible **A** with monolith μ.
3. Determine the polynomial functions $A^k \to 0/\mu$.
4. Reconstruct $\mathrm{Pol}_k(\mathbf{A})$ from $\mathrm{Pol}_k(\mathbf{A}/\mu)$ and $\mathrm{Pol}_k(\mathbf{A}) \cap (0/\mu)^{A^k}$.

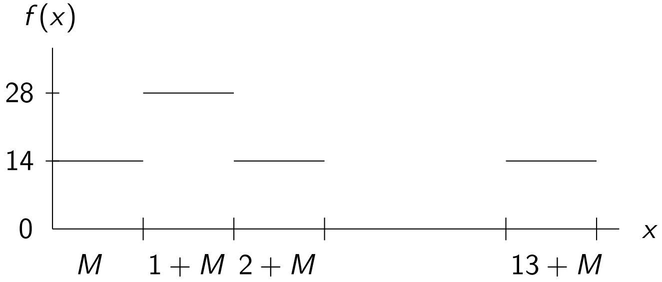
Piecewise constant functions into $0/\mu$

Assume $\mathbf{A} := \langle \mathbb{Z}_{42}, \{+\} \cup F \rangle$ has an abelian monolith μ with $M := 0/\mu$, $|M| = 3$.
$W := \{f : \mathbb{Z}_{42} \to M \mid f(x + M) = f(x)\ \forall x \in \mathbb{Z}_{42}\}$.



Piecewise constant functions into $0/\mu$

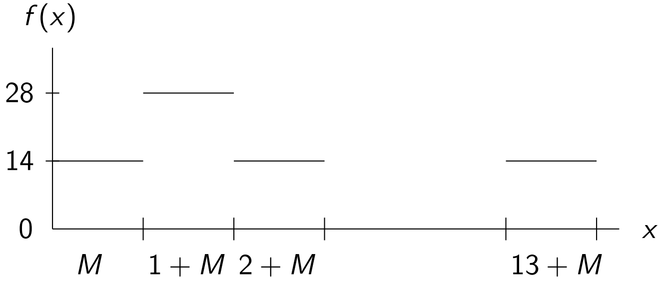
Assume $\mathbf{A} := \langle \mathbb{Z}_{42}, \{+\} \cup F \rangle$ has an abelian monolith μ with $M := 0/\mu$, $|M| = 3$.
$W := \{f : \mathbb{Z}_{42} \to M \mid f(x + M) = f(x)\ \forall x \in \mathbb{Z}_{42}\}$.



- Let $F := \mathrm{GF}(3)$. Then $W \cong F^{14}$.

Piecewise constant functions into $0/\mu$

Assume $\mathbf{A} := \langle \mathbb{Z}_{42}, \{+\} \cup F \rangle$ has an abelian monolith μ with $M := 0/\mu$, $|M| = 3$.
$W := \{f : \mathbb{Z}_{42} \to M \mid f(x + M) = f(x)\ \forall x \in \mathbb{Z}_{42}\}$.



- Let $F := \mathrm{GF}(3)$. Then $W \cong F^{14}$.
- Let $G := \{\mathbb{Z}_{14} \to \mathbb{Z}_{14}, x \mapsto ax + b \mid \gcd(a, 14) = 1, b \in \mathbb{Z}_{14}\}$. W is an $F[G]$-module that is the sum of simple $F[G]$-modules.

Interlude: Representation theory

Lemma.
Let F, K be finite fields with distinct characteristics, let $k \in \mathbb{N}$. Then $F[K^k]$ splits into 2 simple $F[\mathrm{AGL}(k, K)]$-modules whose endomorphism algebras are F.

- $\mathrm{Pol}_1(\mathbf{A}) \cap W$ is an $F[G]$-submodule of W.

- $\mathrm{Pol}_1(\mathbf{A}) \cap W$ is an $F[G]$-submodule of W.
- There exist $B_1, \ldots, B_l \leq \langle A, + \rangle$ such that

$$\begin{aligned} \mathrm{Pol}_1(\mathbf{A}) \quad &\cap \quad W \\ &= \quad \sum_{i=1}^{l} \{ f : A \to M \mid f(x + B_i) = f(x) \ \ \forall x \in A \}. \end{aligned}$$

- $\mathrm{Pol}_1(\mathbf{A}) \cap W$ is an $F[G]$-submodule of W.
- There exist $B_1, \ldots, B_l \leq \langle A, + \rangle$ such that

$$\begin{aligned}\mathrm{Pol}_1(\mathbf{A}) \quad &\cap \quad W \\ &= \quad \sum_{i=1}^{l} \{f : A \to M \mid f(x + B_i) = f(x) \ \ \forall x \in A\}.\end{aligned}$$

- Similarly there exist $C_1, \ldots, C_n \leq \langle A, + \rangle$ such that

$$\begin{aligned}\mathrm{Pol}_k(\mathbf{A}) \quad &\cap \quad \{f : A^k \to M \mid f(x + M^k) = f(x) \ \forall x \in A^k\} \\ &= \quad \sum_{j=1}^{n} \{f : A^k \to M \mid f(x + C_j^k) = f(x) \ \ \forall x \in A^k\}.\end{aligned}$$

- $\mathrm{Pol}_1(\mathbf{A}) \cap W$ is an $F[G]$-submodule of W.
- There exist $B_1, \dots, B_l \leq \langle A, + \rangle$ such that

$$\mathrm{Pol}_1(\mathbf{A}) \cap W = \sum_{i=1}^{l} \{ f : A \to M \mid f(x + B_i) = f(x) \ \ \forall x \in A \}.$$

- Similarly there exist $C_1, \dots, C_n \leq \langle A, + \rangle$ such that

$$\mathrm{Pol}_k(\mathbf{A}) \cap \{ f : A^k \to M \mid f(x + M^k) = f(x) \ \forall x \in A^k \} = \sum_{j=1}^{n} \{ f : A^k \to M \mid f(x + C_j^k) = f(x) \ \ \forall x \in A^k \}.$$

- $\{B_1, \dots, B_l\} = \{C_1, \dots, C_n\}$.

Congruences and commutators are not enough

Let $A := \mathbb{Z}_{210}$,

$$\mathbf{A}_1 := \langle A, +, g_6, g_{10}, g_{15} \rangle \text{ and } \mathbf{A}_2 := \langle A, +, g_{30} \rangle$$

with $g_r(rA) = 30$ and $g_r(A \setminus rA) = 0$.

Congruences and commutators are not enough

Let $A := \mathbb{Z}_{210}$,

$$\mathbf{A}_1 := \langle A, +, g_6, g_{10}, g_{15} \rangle \text{ and } \mathbf{A}_2 := \langle A, +, g_{30} \rangle$$

with $g_r(rA) = 30$ and $g_r(A \setminus rA) = 0$.

Then $\mathrm{Con}(\mathbf{A}_1, \wedge, \vee, [.,.]) = \mathrm{Con}(\mathbf{A}_2, \wedge, \vee, [.,.])$ but $\mathrm{Pol}(\mathbf{A}_1) \subsetneq \mathrm{Pol}(\mathbf{A}_2)$.

Congruences and commutators are not enough

Let $A := \mathbb{Z}_{210}$,

$$\mathbf{A}_1 := \langle A, +, g_6, g_{10}, g_{15} \rangle \text{ and } \mathbf{A}_2 := \langle A, +, g_{30} \rangle$$

with $g_r(rA) = 30$ and $g_r(A \setminus rA) = 0$.
Then $\mathrm{Con}(\mathbf{A}_1, \wedge, \vee, [.,.]) = \mathrm{Con}(\mathbf{A}_2, \wedge, \vee, [.,.])$ but $\mathrm{Pol}(\mathbf{A}_1) \subsetneq \mathrm{Pol}(\mathbf{A}_2)$.

$$\begin{aligned} R := \{(x_1, \ldots, x_8) \in A^8 \quad | \quad & \{x_2 - x_1, x_5 - x_3, x_7 - x_4, x_8 - x_6\} \subseteq 6A, \\ & \{x_3 - x_1, x_5 - x_2, x_6 - x_4, x_8 - x_7\} \subseteq 10A, \\ & \{x_4 - x_1, x_6 - x_3, x_7 - x_2, x_8 - x_5\} \subseteq 15A, \\ & x_1 - (x_2 + x_3 + x_4) + x_5 + x_6 + x_7 = x_8\} \end{aligned}$$

is preserved by $+, g_6, g_{10}, g_{15}$ but not by g_{30}.