

MINIMAL ALGEBRAS

ARTURO

ABSTRACT. In this note

1. PRELIMINARIES

Definition 1.1. Let F be a set of function symbols and \mathbf{A} be an algebra over F . We denote by $\text{Pol}(\mathbf{A})$ the smallest set containing

- (1) $\{f^{\mathbf{A}} : f \in F\}$;
- (2) $\{\pi_i^n : A^n \rightarrow A, 1 \leq i \leq n, n \in \omega\}$;
- (3) the constant 0-ary operations

and closed under composition. The elements of $\text{Pol}(\mathbf{A})$ are called **polynomial operations**. We say that two algebras \mathbf{A} and \mathbf{B} on the same carrier are **polynomial equivalent** if $\text{Pol}(\mathbf{A}) = \text{Pol}(\mathbf{B})$.

Example 1.2. If $\varphi \in \text{Clo}_{m+n}(\mathbf{A})$ and $(a_1, \dots, a_m) \in A^m$, then

$$\psi : A^n \rightarrow A \quad (b_1, \dots, b_n) \mapsto \varphi(a_1, \dots, a_m, b_1, \dots, b_n)$$

is a polynomial operation.

2. FINITE MINIMAL ALGEBRAS

Definition 2.1. A nontrivial finite algebra \mathbf{A} is **minimal** iff every nonconstant element of $\text{Pol}_1(\mathbf{A})$ is bijective.

The goal is to classify, up to polynomial equivalence, all the finite minimal algebras.

Example 2.2. The following are examples of minimal algebras.

- (1) any algebra with carrier 2;
- (2) a nontrivial finite vector space \mathbf{A} over a finite field \mathbf{k} : every $\pi \in \text{Pol}_1(\mathbf{A})$ is of the form $\pi(v) = av + b$ for some $a \in \mathbf{k}$, $b \in A$;
- (3) a group of permutations acting on a finite set¹.

We shall prove that, up to polynomial equivalence, there are no other finite minimal algebras.

¹Let \mathbf{G} be a group acting on a set A . Each $g \in G$ induces an operation $\varphi_g : A \rightarrow A$ given by $\varphi_g(a) = g \cdot a$. Let $\Phi_{\mathbf{G}} := \{\varphi_g : g \in G\}$. A \mathbf{G} -set can be seen as an algebra $(A, \Phi_{\mathbf{G}})$.

Lemma 2.3. *Let \mathbf{A} be a minimal algebra. If every element of $\text{Pol}(\mathbf{A})$ is essentially unary, then \mathbf{A} is polynomially equivalent to $(A, \Phi_{\mathbf{G}})$ where \mathbf{G} is a finite group acting on A .*

Proof. Since \mathbf{A} is minimal, $\text{Pol}_1(\mathbf{A}) \cap \text{Sym}(A)$ is a subgroup of $\text{Sym}(A)$. Let $\mathbf{G} := \text{Pol}_1(\mathbf{A}) \cap \text{Sym}(A)$. If $\psi \in \text{Pol}(\mathbf{A})$, either ψ is constant or ψ is essentially unary, hence $(A, \Phi_{\mathbf{G}})$ is polynomially equivalent to \mathbf{A} . \square

Theorem 2.4 ([3]). *Let \mathbf{A} be a minimal algebra with $|A| > 2$. If $\text{Pol}(\mathbf{A})$ contains an operation which is not essentially unary, then \mathbf{A} is polynomially equivalent to a \mathbf{k} -vector space for a finite field \mathbf{k} .*

Theorem 2.5. *Every algebra \mathbf{A} with carrier 2 is polynomially equivalent to one of the following:*

- (1) $\mathbf{E}_0 = (2, \emptyset)$;
- (2) $\mathbf{E}_1 = (2, \neg)$;
- (3) $\mathbf{E}_3 = (2, \wedge, \vee, \neg)$;
- (4) $\mathbf{E}_4 = (2, \wedge, \vee)$;
- (5) $\mathbf{E}_5 = (2, \vee)$;
- (6) $\mathbf{E}_6 = (2, \wedge)$.

Each of them is not polynomially equivalent to the other².

Remark 2.6. Up to isomorphism, $\mathbf{E}_5 (\simeq \mathbf{E}_6)$ is the only semilattice with two elements, while \mathbf{E}_3 and \mathbf{E}_4 are the only Boolean algebra and lattice, respectively, with two elements.

Definition 2.7. Let \mathbf{A} be a minimal algebra. We say that \mathbf{A} is of

- (1) **type 1** (or **unary**) if \mathbf{A} is polynomially equivalent to $(A, \Phi_{\mathbf{G}})$ for some $\mathbf{G} \leq \text{Sym}(A)$;
- (2) **type 2** (or **affine**) if \mathbf{A} is polynomially equivalent to a vector space over a finite field \mathbf{k} ;
- (3) **type 3** (or **Boolean**) if \mathbf{A} is polynomially equivalent to \mathbf{E}_3 ;
- (4) **type 4** (or **lattice**) if \mathbf{A} is polynomially equivalent to \mathbf{E}_4 ;
- (5) **type 5** (or **semilattice**) if \mathbf{A} is polynomially equivalent to \mathbf{E}_5 .

²A classical theorem by Post states that the set of clones of operations on 2 is countable infinite. By Theorem 2.5 among these there are exactly seven distinct clones containing the constant operations. However it has been proven that the set of clones on 3 containing the constant operations is uncountable.

3. RELATIVE MINIMAL ALGEBRAS

Definition 3.1. Let \mathbf{A} be a finite algebra and let $\delta < \theta \in \text{Con}(\mathbf{A})$. We say that \mathbf{A} is (δ, θ) -**minimal** if for all $\varepsilon \in \text{Pol}_1(\mathbf{A})$ either ε is bijective or $\varepsilon(\theta) \subseteq \delta$.

Remark 3.2. Observe that \mathbf{A} is minimal iff \mathbf{A} is (Δ, ∇) -minimal.

Definition 3.3. Let \mathbf{A} be a (α, β) -minimal algebra. An (α, β) -**trace** of \mathbf{A} is a β -equivalence class which contains at least two δ -equivalence classes.

Lemma 3.4. Let \mathbf{A} be a finite (δ, θ) -minimal algebra and let N be a (δ, θ) -trace. Then the algebra $(\mathbf{A}||N)/(\delta/N)$ is minimal.

Definition 3.5. Let \mathbf{A} be a finite algebra and $B, C \subseteq A$. We say that B, C are **polynomial isomorphic** ($B \sim C$) if there are $\varphi, \psi \in \text{Pol}_1(\mathbf{A})$ such that $\varphi[B] = C, \psi[C] = B$ and $\psi\varphi|B = 1_B, \varphi\psi|C = 1_C$.

4. TAME CONGRUENCES

Definition 4.1. Let \mathbf{A} be a finite algebra and $\alpha, \beta \in \text{Con}(\mathbf{A})$ with $\alpha < \beta$. We denote by

- (1) $E(\mathbf{A})$ the set of $\varepsilon \in \text{Pol}_1(\mathbf{A})$ such that $\varepsilon^2 = \varepsilon$;
- (2) $U_{\mathbf{A}}(\alpha, \beta)$ the set $\{\varphi[A] : \varphi \in \text{Pol}_1(\mathbf{A}), \varphi(\beta) \not\subseteq \alpha\}$;
- (3) $M_{\mathbf{A}}(\alpha, \beta)$ the set of minimal elements of $U_{\mathbf{A}}(\alpha, \beta)$.

Remark 4.2. Let \mathbf{A} be an algebra. An equivalence relation α is a congruence of \mathbf{A} iff $\varphi(\alpha) \subseteq \alpha$ for every $\varphi \in \text{Pol}_1(\mathbf{A})$.

Let \mathbf{A} be a finite algebra. In this section we adopt the following convention, concerning the restriction $(-|U)$ operation, for $U \subseteq A$:

- if $\theta \in \text{Con}(\mathbf{A})$, $\theta|U := \theta \cap U^2$;
- if $\varphi : A^n \rightarrow A$, $\varphi|U$ is the function $U^n \rightarrow A$, $(u_1, \dots, u_n) \mapsto \varphi(u_1, \dots, u_n)$;
- $\text{Pol}(\mathbf{A})|U := \{\psi|U : \psi \in \text{Pol}(\mathbf{A}) \text{ and } \psi[U^n] \subseteq U\}$;
- $\mathbf{A}||U := (U, \text{Pol}(\mathbf{A})|U)$.

Lemma 4.3. Let \mathbf{A} be a finite algebra. Let $\varepsilon \in E(\mathbf{A})$, $U = \varepsilon[A]$. Then $(-|U) : \text{Con}(\mathbf{A}) \rightarrow \text{Con}(\mathbf{A}||U)$ is a surjective (\wedge, \vee) -homomorphism.

Lemma 4.4. Let $\varepsilon \in E(\mathbf{A})$, $U := \varepsilon[A]$, and $\emptyset \neq N \subseteq U$. Then $\mathbf{A}||N = (\mathbf{A}||U)||N$.

Proof. That $(\text{Pol}(\mathbf{A})|U)||N \subseteq \text{Pol}(\mathbf{A})|N$ is obvious. Conversely, let $\psi = \varphi|N$ for some $\varphi \in \text{Pol}(\mathbf{A})$ with $\varphi[N^k] \subseteq N$. Clearly, $\varepsilon\varphi[U^k] \subseteq U$. If $(a_1, \dots, a_k) \in N$, $\varphi(a_1, \dots, a_k) \in N \subseteq U$, hence $\varphi(a_1, \dots, a_k) = \varepsilon(a)$ for some $a \in A$. Hence $\varepsilon\varphi(a_1, \dots, a_k) = \varepsilon^2(a) = \varepsilon(a) \in N$ so that $(\varepsilon\varphi|U)|N = \varphi|N$. We have shown that ψ is an operation of $(\mathbf{A}||U)||N$. \square

Definition 4.5. Let \mathbf{A} be a finite algebra and $\alpha, \beta \in \text{Con}(\mathbf{A})$ with $\alpha < \beta$. The pair (α, β) is a pair of **tame** congruences if there is $V \in M_{\mathbf{A}}(\alpha, \beta)$, $\varepsilon \in E(\mathbf{A})$ such that $\varepsilon[A] = V$ and $(-|V) : [\alpha, \beta] \rightarrow [\alpha|V, \beta|V]$ is 0, 1-separating³.

Lemma 4.6. Let (α, β) be a tame pair of congruences of a finite algebra \mathbf{A} . For every $U \in M_{\mathbf{A}}(\alpha, \beta)$, there is $\varepsilon \in E(\mathbf{A})$ such that $\varepsilon[A] = U$.

Proof. Since (α, β) is tame, there is $V_0 \in M_{\mathbf{A}}(\alpha, \beta)$ and $\varepsilon_0 \in E(\mathbf{A})$ such that $V_0 = \varepsilon_0[A]$ and $(-|V_0)$ is 0, 1-separating.

Claim 1. If $(x, y) \in \beta - \alpha$, there is $\varphi \in \text{Pol}_1(\mathbf{A})$ with $\varphi[A] = V_0$ and such that $(\varphi(x), \varphi(y)) \in \beta|V_0 - \alpha|V_0$.

Proof. Let $\theta := \{(x, y) \in \beta : (\varepsilon_0\varphi(x), \varepsilon_0\varphi(y)) \in \alpha \text{ for all } \varphi \in \text{Pol}_1(\mathbf{A})\}$. Now, $\theta \in [\alpha, \beta]$ and $\alpha|V_0 = \theta|V_0$; that $\alpha|V_0 \subseteq \theta|V_0$ is obvious, for the converse:

$$\begin{aligned} \theta|V_0 &= \{(a, b) \in \beta \cap V_0^2 : (\varepsilon_0\varphi(a), \varepsilon_0\varphi(b)) \in \alpha \quad \forall \varphi \in \text{Pol}_1(\mathbf{A})\} \\ &= \{(\varepsilon_0(x), \varepsilon_0(y)) \in \beta : (\varepsilon_0\varphi\varepsilon_0(x), \varepsilon_0\varphi\varepsilon_0(y)) \in \alpha \quad \forall \varphi \in \text{Pol}_1(\mathbf{A})\} \\ &\subseteq \{(\varepsilon_0(x), \varepsilon_0(y)) \in \beta : (\varepsilon_0(x), \varepsilon_0(y)) \in \alpha\} \\ &= \{(a, b) \in \beta : (a, b) \in \alpha \cap V_0^2\} \\ &= \alpha|V_0 \end{aligned}$$

This implies that $\theta = \alpha$, since $(-|V_0)$ is 0-separating. Thus $(x, y) \in \beta - \alpha$ implies $(x, y) \in \beta - \theta$. By definition of θ , there is $\psi \in \text{Pol}_1(\mathbf{A})$ such that $(\varepsilon_0\psi(x), \varepsilon_0\psi(y)) \notin \alpha$. Thus $\varphi := \varepsilon_0\psi$ satisfies the conditions $\varphi[A] \subseteq V_0$ and $(\varphi(x), \varphi(y)) \in \beta|V_0 - \alpha|V_0$. Hence $\varphi[A] = V_0$ by (α, β) -minimality. \square

Claim 2. The relation β is the transitive closure of

$$\alpha \cup \{(\psi(x), \psi(y)) : (x, y) \in \beta|V_0, \psi \in \text{Pol}_1(\mathbf{A})\}.$$

Proof. The transitive closure of $\alpha \cup \{(\psi(x), \psi(y)) : (x, y) \in \beta|V_0, \psi \in \text{Pol}_1(\mathbf{A})\}$ is $\alpha \vee \theta(\beta|V_0)$. But $\alpha \vee \theta(\beta|V_0) \in [\alpha, \beta]$, and therefore, since $(-|V_0)$ is 1-separating, $\beta = \alpha \vee \theta(\beta|V_0)$. \square

Assume that $U \in M_{\mathbf{A}}(\alpha, \beta)$. Then, by definition, there is $\mu \in \text{Pol}_1(\mathbf{A})$ such that $\mu[A] = U$ and $\mu(\beta) \not\subseteq \alpha$. This implies that the equivalence relation

$$\mu^{-1}(\alpha) = \{(a, b) : (\mu(a), \mu(b)) \in \alpha\}$$

is such that $\beta \not\subseteq \mu^{-1}(\alpha)$. Then by Claim 2 there are $a, b \in V_0$ and $\psi \in \text{Pol}_1(\mathbf{A})$ such that $(a, b) \in \beta$ and $(\mu\psi(a), \mu\psi(b)) \notin \alpha$. The function $\mu_1 := \mu\psi\varepsilon_0$ satisfies $\mu_1[A] \subseteq U$ and $\mu_1(\beta) \not\subseteq \alpha$: there are $x, y \in A$ such that $(a, b) = (\varepsilon_0(x), \varepsilon_0(y)) \in \beta$ but $(\mu_1(a), \mu_1(b)) = (\mu\psi\varepsilon_0(x), \mu\psi\varepsilon_0(y)) \notin \alpha$. Thus $\mu_1[A] = U$ by (α, β) -minimality. Observe that $\mu_1[V_0] = \mu_1\varepsilon_0[A] = \mu\psi\varepsilon_0^2[A] = \mu_1[A]$, so that $\mu_1[V_0] = U$. Apply Claim 1 to the pair $(\mu_1(a), \mu_1(b))$ to get $\nu \in \text{Pol}_1(\mathbf{A})$ such that $\nu[A] = V_0$ and $(\nu\mu_1(a), \nu\mu_1(b)) \notin \alpha$. Now, since $\mu_1\nu[A] = \mu_1[V_0] = U$, $\mu_1\nu|U$ is bijective; since U is finite, there is $k > 1$ such that $(\mu_1\nu|U)^k = (\mu_1\nu)^k|U = 1_U$. Let $\varepsilon := (\mu_1\nu)^k$.

³Let \mathbf{L}, \mathbf{N} be two lattices. A (\wedge, \vee) -homomorphism $\alpha : \mathbf{L} \rightarrow \mathbf{N}$ is 0, 1-separating if $\alpha^{-1}[\{\alpha(i)\}] = i$ for $i = 0, 1$.

We have: $\varepsilon[A] = (\mu_1\nu)^k[A] = (\mu_1\nu)^{k-1}[U] = U$ and, consequently, for all $a \in A$, $\varepsilon^2(a) = \varepsilon(a)$ since $\varepsilon(a) \in U$. Therefore $\varepsilon \in E(\mathbf{A})$. \square

Definition 4.7. Let \mathbf{A} be a finite algebra minimal with respect to (δ, θ) . We say that \mathbf{A} has **type i** relative to (δ, θ) if for every (δ, θ) -trace N , $(\mathbf{A}||N)/(\delta|N)$ is a minimal algebra of type **i**.

Definition 4.8. Let (α, β) be tame in a finite algebra \mathbf{A} . Let N be a (α, β) -trace. We define the **type** of (α, β) , written $\text{typ}(\alpha, \beta)$, to be the type of the minimal algebra $\mathbf{M} = (\mathbf{A}||N)/(\alpha|N)$.

Finally, for a finite algebra \mathbf{A} , we define $\text{typ}\{\mathbf{A}\} := \{\text{typ}(\alpha, \beta) : (\alpha, \beta) \text{ is tame}\}$ and for a class K of finite algebras, $\text{typ}\{K\} := \cup\{\text{typ}\{\mathbf{A}\} : \mathbf{A} \in K\}$.

5. OMITTING TYPES

Definition 5.1. Let \mathbf{V} be a variety. An algebra $\mathbf{A} \in \mathbf{V}$ is called

- (1) **free** if there is an isomorphism $\mathbf{A} \simeq \mathbf{F}_{\mathbf{V}}(\kappa)$ for some cardinal κ ;
- (2) **finitely generated** if there is a surjective homomorphism $\mathbf{F}_{\mathbf{V}}(n) \rightarrow \mathbf{A}$ for some $n \in \omega$.

Definition 5.2. A variety \mathbf{V} is called

- (1) **locally finite** if all its finitely generated algebras are finite;
- (2) **finitely presented** if \mathbf{V} has a finite set of function symbols and $\mathbf{V} = \text{Alg}(\Sigma)$ for a finite set of equations Σ ;
- (3) **finitely generated** if $\mathbf{V} = V(\mathbf{A}_1, \dots, \mathbf{A}_n)$ for $\mathbf{A}_1, \dots, \mathbf{A}_n$ finite similar algebras.

Remark 5.3. Observe that $V(\mathbf{A}_1, \dots, \mathbf{A}_n) = V(\mathbf{A}_1 \times \dots \times \mathbf{A}_n)$.

Lemma 5.4. *Let \mathbf{V} be a variety. If \mathbf{V} is finitely generated then it is locally finite.*

Proof. By the previous remark, we can assume that $\mathbf{V} = V(\mathbf{A})$ for some \mathbf{A} finite. Let $n < \omega$. We prove that $\mathbf{F}_{\mathbf{V}}(n)$ is finite. Consider the homomorphism

$$\mathbf{F}_{\mathbf{V}}(n) \rightarrow \mathbf{A}^{A^n}, \quad t(x_1, \dots, x_n) \mapsto t^{\mathbf{A}}$$

This homomorphism is injective: if $t^{\mathbf{A}} = s^{\mathbf{A}}$, then $\mathbf{A} \models t \equiv s$, i.e. $t = s$ in $\mathbf{F}_{\mathbf{V}}(n)$. Thus $\mathbf{F}_{\mathbf{V}}(n)$ is finite. \square

Definition 5.5. Let \mathbf{V} and \mathbf{W} be two varieties. We say that \mathbf{V} is **interpretable** into \mathbf{W} ($\mathbf{V} \leq \mathbf{W}$) if there is a clone homomorphism $\text{Clo}(\mathbf{V}) \rightarrow \text{Clo}(\mathbf{W})$.

Remark 5.6. Let \mathbf{W}, \mathbf{V} be two varieties. We unravel what $\mathbf{W} \leq \mathbf{V}$ means in a simple case. Let F be a finite set of function symbols. Let \mathbf{V} be a variety of algebras over F , defined by the equations

$$(1) \quad s_1 \equiv t_1, \dots, s_k \equiv t_k.$$

Assume that for each $f \in F_n$ there is $t \in \text{Clo}_n(W)$ such that the interpretation of the t 's satisfy the equations (1). Then the assignment $f \mapsto t$ extends to a clone homomorphism $\text{Clo}(V) \rightarrow \text{Clo}(W)$. Of course, the converse also holds; thus this is equivalent to $W \leq V$.

Lemma 5.7. *Let W, V be two varieties such that $W \leq V$. Assume that W is*

- *idempotent;*
- *finitely presented;*
- *the finite set of equations defining W contains at most one function symbol per side.*

Let $\mathbf{A} \in V$, $\varepsilon \in E(\mathbf{A})$, $U := \varepsilon[A]$, $\beta \in \text{Con}(\mathbf{A})$ and $S := a/\beta \cap U$ for $a \in U$. Then $W \leq V(\mathbf{A}||S)$.

Proof. By assumption W can be described by a finite set of equations of the form

$$(2) \quad f_i(x_{i_1}, \dots, x_{i_h}) \equiv f_j(x_{j_1}, \dots, x_{j_k})$$

where f_i and f_j are members of a finite set F of function symbols. Since $W \leq V$, there is an assignment $f \mapsto t$ extending to a clone homomorphism. We need to find a clone homomorphism $\text{Clo}(W) \rightarrow \text{Clo}(\mathbf{A}||S)$. Consider $f \mapsto \varphi := \varepsilon t_i^{\mathbf{A}}|S$. Firstly, it is well defined: if $(a_1, \dots, a_n) \in S$, $(\varphi(a_1, \dots, a_n), \varphi(a, \dots, a)) \in \beta$ but

$$\varphi(a, \dots, a) = \varepsilon t^{\mathbf{A}}(a, \dots, a) = \varepsilon(a) \in U$$

so that $\varphi(a_1, \dots, a_n) \in S$ and therefore $\varphi \in \text{Pol}(\mathbf{A})|S$. Finally, using that $W \leq V$

$$\begin{aligned} \varphi_i(a_{i_1}, \dots, a_{i_h}) &= \varepsilon t_i^{\mathbf{A}}(a_{i_1}, \dots, a_{i_h}) \\ &= \varepsilon t_j^{\mathbf{A}}(a_{j_1}, \dots, a_{j_k}) \\ &= \varphi_j(a_{j_1}, \dots, a_{j_k}). \end{aligned}$$

□

Theorem 5.8. *Let V be a locally finite variety. The following are equivalent:*

- (1) $1 \notin \text{typ}\{V\}$;
- (2) *there is an idempotent variety W such that $W \leq V$ and $W \not\leq \text{Set}$.*

Corollary 5.9. *Let \mathbf{A} be a finite idempotent algebra. There is $\mathbf{B} \in HS(\mathbf{A})$ such that $\text{Clo}(\mathbf{B}) = \mathbf{N}$ iff $1 \in \text{typ}\{HS(\mathbf{A})\}$.*

Proof. If $1 \in \text{typ}\{HS(\mathbf{A})\}$, then $1 \in \text{typ}\{HSP(\mathbf{A})\}$. Since \mathbf{A} is finite, then, by Lemma 5.4 $HSP(\mathbf{A})$ is locally finite, and therefore, by Theorem 5.8, for every idempotent variety W , either $W \not\leq HSP(\mathbf{A})$ or $W \leq \text{Set}$. In particular, since \mathbf{A} is idempotent, $HSP(\mathbf{A}) \leq \text{Set}$. This means that there is a clone homomorphism $\text{Clo}(\mathbf{A}) \rightarrow \mathbf{N}$. Equivalently, every term operation of \mathbf{A} is a projection. Hence, $\text{Clo}(\mathbf{A}) = \mathbf{N}$.

Conversely, let $\mathbf{B} \in HS(\mathbf{A})$ such that $\text{Clo}(\mathbf{B}) = \mathbf{N}$; this means that \mathbf{B} is term equivalent to a set. Hence \mathbf{B} is polynomial equivalent to a set on which the trivial group acts. Then $1 \in \text{typ}\{\mathbf{B}\}$, and therefore $1 \in \text{typ}\{HS(\mathbf{A})\}$. □

Theorem 5.10 ([2]). *Let \mathbf{A} be a finite idempotent algebra. Then $\text{Clo}(\mathbf{A})$ contains a weak near-unanimity operation iff $\mathbf{1} \notin \text{typ}\{HS(\mathbf{A})\}$.*

REFERENCES

- [1] Hobby, D., McKenzie, R. (1988). *The structure of Finite Algebras*. Contemporary Mathematics 76, American Mathematical Society.
- [2] Maróti, M., McKenzie, R. (2008). Existence theorems for weakly symmetric operations. *Algebra Universalis* 59, 463-489.
- [3] Pálffy, P. P. (1984). Unary polynomials in algebras I. *Algebra Universalis* 18, 262-273.