9-2015

Automorphism-primal algebras generate verbose varieties

Clifford Bergman
Iowa State University, cbergman@iastate.edu

Automorphism-primal algebras generate verbose varieties

Abstract

A finite algebra is called automorphism-primal if its clone of term operations coincides with all operations that preserve its automorphisms. We prove that the variety generated by an automorphism-primal algebra is verbose, that is, on every member algebra, every fully invariant congruence is verbal. The proof is a nice application of the theory of natural dualities as developed by Davey et al.

Keywords

verbal congruence, fully invariant congruence, verbose, automorphism-primal, natural duality

Disciplines

Algebra

Comments

This is a post-peer-review, pre-copyedit version of an article published in *Algebra universalis*. The final authenticated version is available online at DOI: 10.1007/s00012-015-0337-0. Posted with permission.

Automorphism-primal algebras generate verbose varieties

Clifford Bergman

Abstract. A finite algebra is called automorphism-primal if its clone of term operations coincides with all operations that preserve its automorphisms. We prove that the variety generated by an automorphism-primal algebra is verbose, that is, on every member algebra, every fully invariant congruence is verbal.

In [2] we discussed the notions of verbal and fully invariant congruences and examined the relationship between these two concepts. In particular, we called an algebra *verbose* if every fully invariant congruence is verbal. A variety is verbose if every member algebra has that property. In the earlier paper, we set ourselves the task of understanding verbose varieties.

Among the results in [2], we proved that every subalgebra-primal algebra generates a verbose variety. This suggests the conjecture that every quasiprimal algebra generates a verbose variety. While we are still unable to verify that conjecture in complete generality, we are able to prove another special case, namely that every automorphism-primal algebra generates a verbose variety. The purpose of this note is to provide that proof.

This result was announced at the conference on General Algebra and Its Applications in Melbourne, 2013. The proof utilizes NU-duality as developed by Brian Davey and his collaborators. We happily dedicate this paper to Brian on the occasion of his birthday and retirement.

We begin by formulating the two concepts that are our primary interest here. These notions are presented in isolation in this paper. For a more thorough explanation, consult [2]. See [1] for any concepts or results not fully described in this paper.

Definition 1. Let $\mathbf{A}$ be an algebra and $\mathcal{V}$ a variety of the same similarity type as $\mathbf{A}$.

- $\Lambda^{\mathbf{A}}_{\mathcal{V}} = \{\, \theta \in \operatorname{Con}(\mathbf{A}) : \mathbf{A}/\theta \in \mathcal{V} \,\}$.
- $\lambda^{\mathbf{A}}_{\mathcal{V}} = \bigcap \Lambda^{\mathbf{A}}_{\mathcal{V}}$.
- A congruence relation of the form $\lambda^{\mathbf{A}}_{\mathcal{V}}$ for some variety, $\mathcal{V}$, is called a *verbal congruence.*

Definition 2. Let $\mathbf{A}$ be an algebra. Write $\operatorname{End}(\mathbf{A})$ for the set of endomorphisms of $\mathbf{A}$. A congruence relation, θ, on $\mathbf{A}$ is called *fully invariant* if and only if

$$\forall s \in \operatorname{End}(\mathbf{A}) \;\; (x,y) \in \theta \implies \big(s(x), s(y)\big) \in \theta.$$

It is well-known that every verbal congruence is fully invariant. The converse is false in general. That phenomenon forms the root of our inquiry. We call an algebra *verbose* if every fully invariant congruence is verbal. A variety is verbose if every member algebra is verbose.

A finite algebra $\mathbf{M}$ is called *automorphism-primal* if its clone of term operations coincides with the clone of all operations that preserve $\mathrm{Aut}(\mathbf{M})$. A classical theorem due to Werner [4, 1.14(5)], asserts that a finite algebra $\mathbf{M}$ is automorphism-primal if and only if it is quasiprimal, every subuniverse is the set of fixed points of a group of automorphisms, and every isomorphism between nontrivial subalgebras extends to an automorphism of $\mathbf{M}$.

An isomorphism between two subalgebras of an algebra $\mathbf{M}$ is called an *internal isomorphism.* We denote by $\mathrm{Iso}(\mathbf{M})$ the set of internal isomorphisms of $\mathbf{M}$, viewed as unary partial operations on M, and by $\mathrm{Aut}(\mathbf{M})$ the set of automorphisms of $\mathbf{M}$, viewed as unary total operations.

As an example, any finite field is automorphism-primal. In this case, the discriminator term is $q(x, y, z) = (x - y)^{n-1} \cdot (x - z) + z$, where n is the cardinality of the field. The only subuniverses are the subfields and the only internal isomorphisms are the Frobenius automorphisms, which extend to an automorphism on any field extension.

As we remarked above, every automorphism-primal algebra is quasiprimal. We remind the reader that quasiprimal algebras have very special properties. They generate varieties that are semisimple and congruence-distributive, in fact, they have a majority term. Consequently, there are only finitely many subdirectly irreducible algebras, and they are all finite, simple subalgebras of $\mathbf{M}$. Finally, the variety generated by a quasiprimal algebra, $\mathbf{M}$, coincides with $\mathsf{SP}(\mathbf{M})$, see [1, Sec. 6.1].

Quasiprimal algebras are strongly dualizable [3, Theorem 3.3.13], however, we need only a "plain vanilla" duality, which is easier to state and will presumably generalize more readily. For the remainder, let $\mathbf{M}$ denote an automorphism-primal algebra and $\mathcal{V}$ the variety generated by $\mathbf{M}$.

Lemma 3. *Let* $\mathbf{M}$ *be automorphism-primal and* $\mathbb{M} = \langle M, \mathrm{Aut}(\mathbf{M}), T\rangle$ *in which* T *is the discrete topology. Then* $\mathbb{M}$ *yields a duality on* $\mathcal{V}$.

Proof. By [3, Theorem 3.3.12], every subalgebra of $\mathbf{M}^2$ is either an internal isomorphism or of the form $\mathbf{Q}_1 \times \mathbf{Q}_2$, for subalgebras $\mathbf{Q}_1, \mathbf{Q}_2$ of $\mathbf{M}$. The NU-duality theorem [3, Theorem 2.3.4] tells us that $\mathcal{V}$ is dualized by $\langle M, \mathrm{Sub}(\mathbf{M}^2), T\rangle$. Thus we need only use automorphism-primality to show that $\mathrm{Aut}(\mathbf{M})$ entails $\mathrm{Iso}(\mathbf{M})$ and $Q_1 \times Q_2$, for every $Q_1, Q_2 \leq \mathbf{M}$.

All of the entailments are easily obtained from [3, Theorem 2.4.5]. For every automorphism g, $\mathrm{fix}(g)$ is entailed by g. By Werner's theorem, every subalgebra of $\mathbf{M}$ is of the form $\bigcap_i \mathrm{fix}(g_i)$, so they are all entailed. Therefore, every product $Q_1 \times Q_2$ is entailed. Finally, suppose $h\colon Q_1 \to Q_2$ is an internal isomorphism. If Q_1 is nontrivial, then by Werner result cited above, $h = g{\restriction}_{Q_1}$

for some $g \in \mathrm{Aut}(\mathbf{M})$, so h is entailed. On the other hand, if Q_1 is trivial, then $h = Q_1 \times Q_2$, so, as we have already shown, h is entailed. □

We need to review a few details of the duality guaranteed by Lemma 3. Let $\mathcal{X}$ denote the category of closed subspaces of powers of $\mathbb{M}$. There is a pair of functors

$$\mathcal{V} \underset{E}{\overset{D}{\rightleftarrows}} \mathcal{X}$$

which we shall describe. First, let $\mathbf{A} \in \mathcal{V}$. Then $D(\mathbf{A}) = \langle X, G^X, T^X \rangle$ in which

$$\begin{aligned} X &= \mathrm{Hom}_{\mathcal{V}}(\mathbf{A}, \mathbf{M}); \\ G^X &= \{\, \hat{g} : g \in \mathrm{Aut}(\mathbf{M}) \,\},\ \text{where for } \tau \in X,\ \hat{g}(\tau) = g \circ \tau; \\ T &\quad \text{is the topology on } X \text{ with subbasis } \{\, T(a,q) : a \in A, q \in F \,\}. \end{aligned}$$

Here, $T(a,q) = \{\, \phi \in X : \phi(a) = q \,\}$. Finally, for $\mathbf{A}, \mathbf{B} \in \mathcal{V}$ and a homomorphism $h \colon \mathbf{A} \to \mathbf{B}$, we have $D(h) \colon D(\mathbf{B}) \to D(\mathbf{A})$ mapping ϕ to $\phi \circ h$. Then D is a contravariant functor from $\mathcal{V}$ to $\mathcal{X}$.

To describe the functor E operating in the opposite direction, let $\mathbf{X} \in \mathcal{X}$. Then $E(\mathbf{X}) = \mathrm{Hom}_{\mathcal{X}}(\mathbf{X}, \mathbb{M}) \subseteq M^X$. It is not hard to show that $\mathrm{Hom}_{\mathcal{X}}(\mathbf{X}, \mathbb{M})$ is, in fact, a subuniverse of $\mathbf{M}^X$. Consequently, $E(\mathbf{X}) \in \mathcal{V}$. If $f \colon \mathbf{X} \to \mathbf{Y}$ is an $\mathcal{X}$-morphism, then $E(f) \colon E(\mathbf{Y}) \to E(\mathbf{X})$ maps y to $y \circ f$.

Finally, for every $\mathbf{A} \in \mathcal{V}$, there is an embedding $e_{\mathbf{A}} \colon \mathbf{A} \to ED(\mathbf{A})$ mapping $a \in A$ to $\hat{a}$, in which $\hat{a}(\tau) = \tau(a)$. From this we obtain

$$\begin{aligned} &(\forall a, b \in A)\big(\forall \tau \in \mathrm{Hom}_{\mathcal{V}}(\mathbf{A}, \mathbf{M})\big) \\ &\qquad (a,b) \in \ker \tau \iff \tau(a) = \tau(b) \iff \hat{a}(\tau) = \hat{b}(\tau). \end{aligned} \tag{1}$$

In the language of the Clark-Davey monograph, the pair (D, E) forms a preduality between $\mathcal{V}$ and $\mathcal{X}$. The duality provided by Lemma 3 tells us more: for every $\mathbf{A} \in \mathcal{V}$, the map e_A is surjective as well as injective. Thus we have a representation of each member of $\mathcal{V}$ as an algebra of continuous functions.

Now, let $\mathbf{X} = D(\mathbf{A})$, and $f \colon \mathbf{X} \to \mathbf{X}$ an $\mathcal{X}$-endomorphism. Write $\check{f}$ in place of $E(f)$. Thus $\check{f}(\hat{a}) = \hat{a} \circ f$. If we now define s to be $e_{\mathbf{A}}^{-1} \circ \check{f} \circ e_{\mathbf{A}}$, then s is an endomorphism of $\mathbf{A}$ in which, for $a \in A$ we have $s(a) = e^{-1}\check{f}e(a)$. Thus

$$\widehat{s(a)} = \check{f}e(a) = \check{f}(\hat{a}) = \hat{a} \circ f \tag{2}$$

see Figure 1.

Theorem 4. *$\mathcal{V}$ is verbose.*

Proof. Let $\mathbf{A} \in \mathcal{V}$ and suppose that θ is a congruence on $\mathbf{A}$ that is not verbal. We shall show that θ is not fully invariant. We first prove the following claim.

Claim. *There are maximal congruences α and β on $\mathbf{A}$, such that $\theta \leq \alpha$, $\theta \nleq \beta$, and $\mathbf{A}/\beta \in \mathsf{S}(\mathbf{A}/\alpha)$.*

$$\begin{tikzcd} X \arrow[rr, "f"] \arrow[dr, dotted, "\check{f}(\hat{a})"'] & & X \arrow[dl, "\hat{a}"] \\ & M & \end{tikzcd} \qquad \begin{tikzcd} \mathbf{A} \arrow[r, "e"] \arrow[d, dotted, "s"'] & ED(\mathbf{A}) \arrow[d, "\check{f}"] \\ \mathbf{A} \arrow[r, "e"'] & ED(\mathbf{A}) \end{tikzcd}$$

Figure 1

Proof. Since θ is not verbal, there is a congruence ψ such that $\mathbf{A}/\psi \in \mathsf{V}(\mathbf{A}/\theta)$ but $\theta \nleq \psi$. Since $\mathcal{V}$ is semisimple, ψ is a meet of maximal congruence relations. Thus there is a maximal congruence β such that $\mathbf{A}/\beta \in \mathsf{V}(\mathbf{A}/\theta)$ but $\theta \nleq \beta$.

By semisimplicity, $\theta = \bigwedge_{i\in I} \alpha_i$ in which each α_i is a maximal congruence. Then $\mathsf{V}(\mathbf{A}/\theta) = \mathsf{V}\{\, \mathbf{A}/\alpha_i : i \in I \,\}$. Recall that $\mathcal{V}$ is congruence-distributive and has only finitely many subdirectly irreducible algebras, up to isomorphism. Thus, up to isomorphism, $\{\mathbf{A}/\alpha_i : i \in I\}$ is a finite set of finite algebras. Finally, since $\mathbf{A}/\beta$ is subdirectly irreducible, Jónsson's lemma imples that $\mathbf{A}/\beta \in \mathsf{HS}\{\, \mathbf{A}/\alpha_i : i \in I \,\} = \mathsf{S}\{\, \mathbf{A}/\alpha_i : i \in I \,\}$. Therefore, for some $i \in I$, $\mathbf{A}/\beta \in \mathsf{S}(\mathbf{A}/\alpha_i)$. $\square$

Now we proceed to prove the theorem. Set $\mathbf{X} = D(\mathbf{A}) = \mathrm{Hom}_{\mathcal{V}}(\mathbf{A}, \mathbf{M})$. Let $G = \mathrm{Aut}(\mathbf{M})$. There is an action of G on $\mathbf{X}$ given by $g\phi = \hat{g}(\phi)$. Also, for a subset Q, of M, let $G_Q = \{\, g \in G : (\forall q \in Q)\ g(q) = q \,\}$.

Let α and β be the congruences provided by the claim. Since α is a maximal proper congruence, there is $\psi \in X$ with kernel α. Let $Q = \vec{\psi}(A) \subseteq M$. Since $\mathbf{A}/\beta \in \mathsf{S}(\mathbf{A}/\alpha)$, $\mathbf{Q}$ has a subalgebra $\mathbf{R} \cong \mathbf{A}/\beta$. Choose $\phi\ \mathbf{A} \to \mathbf{R}$ with kernel β. Then $\mathbf{R} \leq \mathbf{Q} \leq \mathbf{M}$. Consequently, $G_Q \subseteq G_R \subseteq G$.

Let $Q = \{u_1, \dots, u_t\}$. Choose $c_1, \dots, c_t \in A$ such that $\psi(c_i) = u_i$, for $i \leq t$. Since each $\hat{c}_i \colon \mathbf{X} \to \mathbb{M}$ is continuous, the set

$$N = \bigcap_{i=1}^{t} \overleftarrow{\hat{c}_i}(u_i) = \{\, \tau \in X : (\forall i \leq t)\ \tau(c_i) = u_i \,\}$$

is a clopen subset of X. Note that $\psi \in N$. Moreover

$$\tau \in N \implies \vec{\tau}(A) \supset Q \implies G_{\vec{\tau}(A)} \subseteq G_Q \subseteq G_R. \tag{3}$$

Observe that N is not closed under arbitrary actions by members of G. By definition, the elements of G_Q act trivially on Q. Consequently, N is closed under the action of G_Q.

For $g \in G$ let $N_g = g \cdot N = \{\, g\tau : \tau \in N \,\}$. Since $\hat{g}$ is a homeomorphism, each N_g is a clopen subset of X. Thus, $P = \bigcup_{g\in G} N_g$ is also clopen. P is obviously closed under the action of G. Thus P is partitioned into orbits under this action. Every orbit passes through N. Choose one representative, $\tau_i \in N$, $i \in I$, for each orbit. Therefore every element of P can be written in the form $g\tau_i$, for $i \in I$, $g \in G$, with i unique.

Now define $f\colon X \to X$ by

$$f(\tau) = \begin{cases} \tau & \text{if } \tau \notin P \\ g\phi & \text{if } \tau = g\tau_i \in P. \end{cases}$$

A consequence of this definition is that $\vec{f}(N_g) = \{g\phi\}$.

The map f is well-defined since, if $g_1\tau = g_2\tau$ then (with $g = g_1^{-1}g_2$), $g\tau = \tau \in N$. But this means that $g \in G_{\vec{\tau}(A)}$, so by (3), $g \in G_R$, thus $g\phi = \phi$, equivalently $g_1\phi = g_2\phi$.

We wish to show that f is a $\mathcal{X}$-morphism. First, to see that f is continuous, let U be an open subset of X. If the G-orbit of ϕ intersects U in $\{g_1\phi, g_2\phi, \dots, g_r\phi\}$, then $\overleftarrow{f}(U) = N_{g_1} \cup \cdots \cup N_{g_r} \cup (P' \cap U)$, which is open. Here, P' denotes the compliment of P in X.

Finally, we must check that for every $g \in G$, $\hat{g} \circ f = f \circ \hat{g}$. First suppose that $\tau \notin P$. Then $g\tau \notin P$, since P is a sub-G-set of X. Therefore both τ and $g\tau$ are fixed by f. Thus $f(g\tau) = g\tau = gf(\tau)$.

On the other hand, if $\tau \in P$, then for some $h \in G$, $\tau \in N_h$. In that case, for every $g \in G$

$$gf(\tau) = g(h\phi) = (gh)\phi$$

while

$$g\tau \in N_{gh} \text{ so } f(g\tau) = (gh)\phi.$$

We have shown that f is an endomorphism of $\mathbf{X}$. So $s = e^{-1} \circ \check{f} \circ e$ is an endomoprhism of $\mathbf{A}$. Since $\theta \nleq \beta$, we can choose $(a, b) \in \theta - \beta$. The fact that $\theta \leq \alpha$ implies that $\psi(a) = \psi(b)$, hence from (1), $\hat{a}(\psi) = \hat{b}(\psi)$. By construction, $\psi \in N$, so $f(\psi) = \phi$. Therefore from (2),

$$\widehat{s(a)}(\psi) = \hat{a}\big(f(\psi)\big) = \hat{a}(\phi) = \phi(a)$$

and similarly, $\widehat{s(b)}(\psi) = \phi(b)$. But $(a, b) \notin \beta = \ker\phi$, so from (1) (with ψ replacing τ and $\big(s(a), s(b)\big)$ replacing (a, b)) that $\big(s(a), s(b)\big) \notin \ker\psi \geq \theta$. Hence θ is not fully invariant. $\square$

As an example, the variety of rings generated by a finite field is verbose.

References

[1] Bergman, C.: Universal algebra. Fundamentals and selected topics, *Pure and Applied Mathematics (Boca Raton)*, vol. 301. CRC Press, Boca Raton, FL (2012)

[2] Bergman, C., Berman, J.: Fully invariant and verbal congruence relations. Algebra Universalis **70**(1), 71–94 (2013). DOI 10.1007/s00012-013-0238-z

[3] Clark, D.M., Davey, B.A.: Natural dualities for the working algebraist, *Cambridge Studies in Advanced Mathematics*, vol. 57. Cambridge University Press, Cambridge (1998)

[4] Werner, H.: Discriminator Algebras. Studium zur Algebra und ihre Andwendungen 6. Akademie Verlag, Berlin (1978)

Clifford Bergman
Department of Mathematics, Iowa State University, Ames, Iowa, 50011, USA