MORITA EQUIVALENCE OF ALMOST-PRIMAL CLONES

Clifford Bergman and Joel Berman

December, 1994

Abstract. Two algebraic structures $\mathbf{A}$ and $\mathbf{B}$ are called categorically equivalent if there is a functor from the variety generated by $\mathbf{A}$ to the variety generated by $\mathbf{B}$, carrying $\mathbf{A}$ to $\mathbf{B}$, that is an equivalence of the varieties when viewed as categories. We characterize those algebras categorically equivalent to $\mathbf{A}$ when $\mathbf{A}$ is an algebra whose set of term operations is as large as possible subject to constraints placed on it by the subalgebra or congruence lattice of $\mathbf{A}$, or the automorphism group of $\mathbf{A}$.

Two categories C and D are said to be *equivalent* if there are functors $F\colon C \to D$ and $G\colon D \to C$ such that the composite functors $F \circ G$ and $G \circ F$ are naturally isomorphic to the identities on D and C respectively. It is natural to ask whether some property of an object, morphism or an entire category is preserved under every equivalence of categories. Moreover, given an object (or morphism, or category), one might wish to characterize the class of objects obtained by applying all equivalences to that starting object.

Any variety of algebras (that is, a class of algebras closed under the formation of subalgebra, product, and homomorphic image) forms a category, in which the morphisms are taken to be all homomorphisms between algebras. A surprising number of "algebraic" properties have been shown to be preserved under equivalence, when the domain of categories is restricted to varieties of algebras. Some of these are familiar to anyone who has worked with categories of algebras, such as Cartesian products and homomorphism kernels; others are somewhat unexpected. Examples of the latter are 'surjective homomorphism' and 'finite algebra'. A large collection of examples of this phenomenon can be found in [5].

A classical example of categorical equivalences of varieties of algebras is Morita's Theorem, which provides necessary and sufficient algebraic conditions on two rings with unit in order for their varieties of unitary modules to be equivalent as categories. Other instances of categorical equivalence of varieties have been discovered using the tools of duality theory as in [5] and [17].

There are also examples of objects characterized up to categorical equivalence in the literature. One of the most striking is a result of Hu's [14]. A finite, nontrivial algebra $\mathbf{A}$ is called *primal* if every operation on the universe of $\mathbf{A}$ is a term operation of $\mathbf{A}$. For example, the two-element Boolean algebra is primal. Hu's theorem for primal algebras asserts that if $\mathbf{P}$ is a primal algebra, then the class of all algebras of the form $F(\mathbf{P})$ as F ranges through all equivalences between varieties, is

This paper was written while the first author was visiting the University of Illinois at Chicago.

exactly the class of all primal algebras. The main theorems of this paper can all be seen as generalizations of this result, obtained by considering several well-known generalizations of 'primality'.

A *clone* C on a set A is a collection of operations on A that is closed under composition and contains all of the projection operations. For any algebra $\mathbf{A}$ with universe A, the set of all term operations of $\mathbf{A}$, denoted $\operatorname{Clo}\mathbf{A}$, forms a clone on A. Thus $\mathbf{A}$ is primal if and only if $1 < |A| < \aleph_0$ and $\operatorname{Clo}\mathbf{A}$ consists of all operations on A. By our informal term "almost-primal", we mean an algebra $\mathbf{A}$ in which $\operatorname{Clo}\mathbf{A}$ is as large a set as possible, subject to constraints placed on it by the various derived structures of $\mathbf{A}$. In this paper the derived structures that we consider are the subalgebra and congruence lattices, and the automorphism group.

Definition 0.1. Let $\mathbf{A}$ and $\mathbf{B}$ be algebras, not necessarily of the same type. We call $\mathbf{A}$ and $\mathbf{B}$ *categorically equivalent* if there is a functor F which is an equivalence from the category $\operatorname{Var}(\mathbf{A})$ to $\operatorname{Var}(\mathbf{B})$ such that $F(\mathbf{A}) = \mathbf{B}$. We write $\mathbf{A} \equiv_{\mathrm{c}} \mathbf{B}$ to indicate this relationship.

It is not hard to show that if F is an equivalence between two varieties, then for any algebra $\mathbf{A}$, F restricts to an equivalence between the varieties $\operatorname{Var}(\mathbf{A})$ and $\operatorname{Var}(F(\mathbf{A}))$. Thus our Definition exactly captures the notion discussed above. It is also obvious that '$\equiv_{\mathrm{c}}$' is an equivalence relation on algebras. Hu's result can be stated as follows: an algebra $\mathbf{P}$ is primal if and only if $\mathbf{P}/\equiv_{\mathrm{c}}$ is the class of primal algebras.

Let $\mathbf{A}$ be a finite algebra that is subalgebra-primal, or automorphism-primal, or arithmetical and congruence-primal (see below for the definitions). In this paper, we give a characterization of the class $\mathbf{A}/\equiv_{\mathrm{c}}$ (see Theorem 3.2, Theorem 5.8, and Corollary 4.5). Furthermore, in the first and second cases, we describe the member of $\mathbf{A}/\equiv_{\mathrm{c}}$ of smallest cardinality, and in the third, provide a canonical member of the class. Along the way, we discover several new properties invariant under categorical equivalence.

1. Preliminaries

As much as possible, we follow the terminology and notation of [20]. Our usage of common concepts such as 'operation', 'term' and 'polynomial' is the same as that text. However, we do tend to blur the distinction between a term and its associated term operation, when no confusion will result.

Let $\mathbf{A}$ be an algebra with universe A. We write $\operatorname{Sg}^{\mathbf{A}}(X)$ to denote the subuniverse of $\mathbf{A}$ generated by a set X. We sometimes abbreviate $\operatorname{Sg}(x)$ by $\langle x \rangle$. The symbol Δ_A denotes the diagonal subset $\{\, (a, a) : a \in A \,\}$. If $R \subseteq A^k$ and $B \subseteq A$, then $R{\restriction_B}$ is shorthand for $R \cap B^k$. Let $\mathbf{L}$ be a complete lattice. By $J(\mathbf{L})$ we mean the set of completely join-irreducible elements in $\mathbf{L}$.

Our arguments are made a bit cleaner by avoiding nullary operations. There is no loss of generality here, since "constant" symbols can be replaced by unary operations with singleton range. One consequence of this convention is that the empty set is always a subuniverse of every algebra. Thus the minimal nonempty subuniverses of $\mathbf{A}$ are precisely the atoms of $\operatorname{Sub}\mathbf{A}$. With this in mind, we make the following definition.

Definition 1.1. Let $\mathbf{A}$ be an algebra. $\mathrm{N}(\mathbf{A})$ denotes the set of non-singleton atoms of $\operatorname{Sub}\mathbf{A}$.

Let A be a nonempty set, F a family of operations of A, and R a family of relations on A. By $\mathcal{P}R$ we mean the set of all operations on A preserving every member of R. These operations are sometimes called the polymorphisms of R. It is easy to see that $\mathcal{P}R$ is always a clone on A. For any natural number n, the set of n-ary members of this clone is denoted $\mathcal{P}_n(R)$. Dually, the set of all relations preserved by every member of F is denoted $\mathcal{I}F$. The set of n-ary members of $\mathcal{I}F$ is equal to $\operatorname{Sub}(\langle A, F\rangle^n)$. Finally, for an algebra $\mathbf{A} = \langle A, F\rangle$, $\operatorname{Clo}\mathbf{A}$ denotes the clone of all term operations on $\mathbf{A}$, and $\operatorname{Clo}_n\mathbf{A}$ the n-ary members of $\operatorname{Clo}\mathbf{A}$. If A is finite, we have $\operatorname{Clo}\mathbf{A} = \mathcal{P}(\mathcal{I}F)$.

Two algebras $\mathbf{A}$ and $\mathbf{B}$ are called *term equivalent,* written $\mathbf{A} \equiv \mathbf{B}$, if they have the same underlying set and the same clone of term operations. The algebras $\mathbf{A}$ and $\mathbf{B}$ are *weakly isomorphic,* denoted $\mathbf{A} \simeq \mathbf{B}$, if $\mathbf{A}$ is isomorphic to an algebra that is term equivalent to $\mathbf{B}$.

The notion of categorical equivalence has been applied to algebraic structures numerous times in the literature. We mention papers of Davey and Werner [5], Freyd [11], Isbell [15] and Wraith [30] in this regard. Recently in [18], R. McKenzie provided a powerful tool that is particularly well-suited to studying the behavior of "algebraic" properties under equivalence and to giving a complete algebraic description of $\mathbf{A}/\equiv_{\mathrm{c}}$ for an arbitrary algebra $\mathbf{A}$. We summarize his result here.

Definition 1.2. Let $\mathbf{A}$ be an algebra, n a positive integer, and σ a unary term operation of $\mathbf{A}$.

- For every positive integer k and every sequence $t_1, t_2, \ldots, t_n$ of kn-ary operations on A, $(t_1, \ldots, t_n)$ denotes the k-ary operation on A^n that maps $(\mathbf{a}_1, \ldots, \mathbf{a}_k)$ to $(\, t_1(\vec{\mathbf{a}}), t_2(\vec{\mathbf{a}}), \ldots, t_n(\vec{\mathbf{a}})\,)$, where $\mathbf{a}_i = (a_{i,1}, \ldots, a_{i,n}) \in A^n$, and
$$\vec{\mathbf{a}} = (a_{1,1}, a_{1,2}, \ldots, a_{1,n}, a_{2,1}, \ldots, a_{k,n}) \in A^{kn}.$$
- The *n-th matrix power* of $\mathbf{A}$ is the algebra $\mathbf{A}^{[n]}$ with universe A^n and whose basic k-ary operations are, for every k, the operations $(t_1, \ldots, t_n)$, as $t_1, \ldots, t_n$ range through $\operatorname{Clo}_{kn}(\mathbf{A})$.
- The operation σ is *idempotent* if for every $x \in A$, $\sigma\big(\sigma(x)\big) = \sigma(x)$. The operation σ is *invertible* if for some k there are $f \in \operatorname{Clo}_k(\mathbf{A})$ and $t_1, \ldots, t_k \in \operatorname{Clo}_1(\mathbf{A})$ such that, for every $a \in A$, $f\big(\sigma t_1(a), \sigma t_2(a), \ldots, \sigma t_k(a)\big) = a$.
- Let σ be an idempotent term of $\mathbf{A}$. By $\mathbf{A}(\sigma)$ we denote the algebra with universe $\sigma(A)$ and basic operations $\sigma \circ g{\restriction}_{\sigma(A)}$, as g ranges through $\operatorname{Clo}\mathbf{A}$.

Theorem 1.3 (McKenzie). *Let $\mathbf{A}$ and $\mathbf{B}$ be algebras. Then $\mathbf{A} \equiv_{\mathrm{c}} \mathbf{B}$ if and only if there is a positive integer n and an idempotent, invertible, unary term σ for $\mathbf{A}^{[n]}$ such that $\mathbf{B} \simeq \mathbf{A}^{[n]}(\sigma)$.*

Note that the similarity types of $\mathbf{A}^{[n]}$ and $\mathbf{A}(\sigma)$ are radically different from that of $\mathbf{A}$. In fact, these new algebras are best viewed as "untyped". It is possible to create an algebra term equivalent to $\mathbf{A}^{[n]}$ by adding only two basic operations to the type of $\mathbf{A}$. We know of no similar construction for $\mathbf{A}(\sigma)$.

One immediate consequence of this theorem is that if $\mathbf{A} \equiv_c \mathbf{B}$ then A is finite if and only if B is finite. This observation is used several times in the sequel.

As McKenzie points out, for any algebra $\mathbf{A}$ and positive integer n, there is an invertible, idempotent term σ on $\mathbf{A}^{[n]}$ such that $\mathbf{A}^{[n]}(\sigma) \simeq \mathbf{A}$. For example, we can take $\sigma(a_1, a_2, \ldots, a_n) = (a_1, a_1, \ldots, a_1)$. This is a useful device for simplifying proofs.

Definition 1.4. Let $\mathbf{A}$ be a nontrivial algebra. $\mathbf{A}$ is called

- *subalgebra-primal* if $\operatorname{Clo}\mathbf{A} = \mathcal{P}(\operatorname{Sub}\mathbf{A})$;
- *congruence-primal* if $\operatorname{Clo}\mathbf{A} = \mathcal{P}(\operatorname{Con}\mathbf{A})$; and
- *automorphism-primal* if $\operatorname{Clo}\mathbf{A} = \mathcal{P}(\operatorname{Aut}\mathbf{A})$.

In order for the notion of automorphism-primal to make sense, we must view an automorphism of an algebra as a binary relation on its underlying set. This ambiguity should not cause any confusion. In the literature, the finite subalgebra-primal algebras have been called semi-primal. Similarly, the finite members of the other two classes have been called hemi-primal and demi-primal, respectively. See [22], [24] and [29].

The primary goal of this paper is to describe, up to categorical equivalence, all finite algebras that are subalgebra-primal, congruence-primal and arithmetical, or automorphism-primal. Obviously, this would not be feasible if these three properties were not themselves preserved by categorical equivalence. We begin there.

Lemma 1.5. *Let $\mathbf{A}$ be an algebra, σ an invertible, idempotent, unary term of $\mathbf{A}$, and n a positive integer.*

(1) *For every subuniverse S of $\mathbf{A}$, $S\restriction_{\sigma(A)} = \sigma(S)$. The lattice $\operatorname{Sub}(\mathbf{A})$ is isomorphic to each of $\operatorname{Sub}\big(\mathbf{A}(\sigma)\big)$ and $\operatorname{Sub}\big(\mathbf{A}^{[n]}\big)$ via the mappings $S \mapsto S\restriction_{\sigma(A)}$ and $S \mapsto S^n$.*

(2) *For all $B \in J(\operatorname{Sub}\mathbf{A})$ there exists $b \in B \cap \sigma(A)$ with $\langle b \rangle = B$.*

(3) *$S \in \mathrm{N}(\mathbf{A})$ if and only if $S \cap \sigma(A) \in \mathrm{N}(\mathbf{A}(\sigma))$.*

(4) *For every $X \subseteq \sigma(A)$, $\operatorname{Sg}^{\mathbf{A}}(X)\restriction_{\sigma(A)} = \operatorname{Sg}^{\mathbf{A}(\sigma)}(X)$.*

(5) *$\operatorname{Con}\mathbf{A} \cong \operatorname{Con}\big(\mathbf{A}(\sigma)\big) \cong \operatorname{Con}\big(\mathbf{A}^{[n]}\big)$ by $\theta \mapsto \theta\restriction_{\sigma(A)}$ and $\theta \mapsto \theta^{[n]}$. These mappings preserve the permutability of congruences.*

(6) *$\operatorname{Aut}(\mathbf{A}) \cong \operatorname{Aut}\big(\mathbf{A}(\sigma)\big) \cong \operatorname{Aut}\big(\mathbf{A}^{[n]}\big)$ by $\gamma \mapsto \gamma\restriction_{\sigma(A)}$ and $\gamma \mapsto \gamma^{[n]}$.*

Proof. First consider (4). Let $X \subseteq \sigma(A)$ and let $B = \operatorname{Sg}^{\mathbf{A}(\sigma)}(X)$. Every element of B is of the form $\sigma t(x_1, \ldots, x_m)$, with $x_1, \ldots, x_m \in X$ and $t \in \operatorname{Clo}_m(\mathbf{A})$, since that is the form of every term of $\mathbf{A}(\sigma)$. But each such term is also a term of $\mathbf{A}$, so it follows that $B \subseteq \operatorname{Sg}^{\mathbf{A}}(X)$. Conversely, every element y of $\operatorname{Sg}^{\mathbf{A}}(X)$ is of the form $t(x_1, \ldots, x_m)$. If $y \in \sigma(A)$, then $y = \sigma(y) = \sigma t(x_1, \ldots, x_m) \in B$.

Part (1) follows easily from (4) by taking X to be an arbitrary subuniverse of $\mathbf{A}(\sigma)$. For the claim involving matrix powers, use the fact that there is an invertible, idempotent, unary term τ such that $\mathbf{A} \simeq \mathbf{A}^{[n]}(\tau)$.

Let $B \in J(\operatorname{Sub}\mathbf{A})$. By part (1), $B\restriction_{\sigma(A)} \in J(\operatorname{Sub}(\mathbf{A}(\sigma)))$. Since every completely join-irreducible subuniverse is 1-generated, there is an element b generating $B\restriction_{\sigma(A)}$ as a subuniverse of $\mathbf{A}(\sigma)$. Then b also generates B by part (4).

Part (3) follows from (1), together with the fact that any categorical equivalence must preserve 1-element algebras (i.e., terminal objects). The permutability claim of part (5) is easily verified, and the rest of parts (5) and (6) are proved in [18, Theorems 2.2 and 2.3]. □

Theorem 1.6. *Let* $\mathbf{A}$ *and* $\mathbf{B}$ *be algebras, with* $\mathbf{A} \equiv_{\mathrm{c}} \mathbf{B}$. *If* $\mathbf{A}$ *is subalgebra-, congruence- or automorphism-primal, then so is* $\mathbf{B}$.

Proof. It is easy to see that each of these properties is preserved by weak isomorphism. Therefore, in each case, it suffices to assume, by McKenzie's Theorem, that $\mathbf{B} = \mathbf{A}^{[n]}$ or $\mathbf{B} = \mathbf{A}(\sigma)$, for some invertible, idempotent, unary term σ and some positive integer n. We do the subalgebra-primal case in detail, and leave the other two cases to the reader.

We shall use the following characterization of subalgebra-primal algebras: $\mathbf{B}$ is subalgebra-primal if for every $f\colon B^m \to B$

$$\big[(\forall b_1, \dots, b_m \in B)\ f(b_1, \dots, b_m) \in \mathrm{Sg}^{\mathbf{B}}(\{b_1, \dots, b_m\})\big] \implies f \in \mathrm{Clo}_m(\mathbf{B}).$$

First consider the case that $\mathbf{B} = \mathbf{A}^{[n]}$. Let $f\colon B^m \to B$ be such that for every $\overline{a}_1, \dots, \overline{a}_m \in B$ we have $f(\overline{a}_1, \dots, \overline{a}_m) \in \mathrm{Sg}^{\mathbf{B}}\big(\{\overline{a}_1, \dots, \overline{a}_m\}\big)$. Let $\overline{a}_1, \dots, \overline{a}_m \in B$. By Lemma 1.5(1), there is a $C \in \mathrm{Sub}(\mathbf{A})$ such that $\mathrm{Sg}^{\mathbf{B}}\big(\{\overline{a}_1, \dots, \overline{a}_m\}\big) = C^n$. We let $(c_1, \dots c_n)$ denote $f(\overline{a}_1, \dots, \overline{a}_m)$. Thus $c_i \in C$ for every i. Define $f_i : A^{mn} \to A$ by $f_i(\overline{a}_1, \dots, \overline{a}_m) = c_i$. Since $\mathbf{A}$ is subalgebra-primal, $f_i \in \mathrm{Clo}_{mn}(\mathbf{A})$. Hence $f = (f_1, \dots, f_n)$ is in $\mathrm{Clo}_m(\mathbf{B})$.

To show that $\mathbf{A}(\sigma)$ is subalgebra-primal whenever $\mathbf{A}$ is, let $\mathbf{B} = \mathbf{A}(\sigma)$. Let $f\colon B^m \to B$ be an operation such that for all $c_1, \dots, c_m \in B$, $f(c_1, \dots, c_m) \in \mathrm{Sg}^{\mathbf{B}}(\{c_1, \dots, c_m\})$. Define an operation g on A by: $g{\restriction_B} = f$ and $g(x_1, \dots, x_m) = x_1$ otherwise. Then by Lemma 1.5(4), $g(a_1, \dots, a_m) \in \mathrm{Sg}^{\mathbf{A}}\{a_1, \dots, a_m\}$. So by assumption, $g \in \mathrm{Clo}_m \mathbf{A}$. Then $f = \sigma \circ (g{\restriction_B}) \in \mathrm{Clo}(\mathbf{B})$ as desired. □

2. Invertible Terms

In creating algebras categorically equivalent to a given algebra $\mathbf{A}$, the matrix power construction poses no difficulties: for any n, the matrix power $\mathbf{A}^{[n]}$ always exists. This, of course, yields an algebra (in the finite case) of larger cardinality. Creating a smaller algebra is not so straightforward. To create an algebra categorically equivalent to $\mathbf{A}$ with universe $S \subseteq A$, one needs to find a *term* σ with $\sigma(A) = S$ that is idempotent and invertible. The biggest obstacle is usually invertibility. Most of the results in this section are geared to providing sufficient conditions for invertibility. They are all based on the following.

Theorem 2.1. *Let* $\mathbf{A}$ *be a finite algebra,* $k \geq 2$ *an integer, and* $\sigma \in \mathrm{Clo}_1 \mathbf{A}$ *idempotent. Suppose*

1. *every partial operation on* A *that preserves every* $R \in \mathrm{Sub}(\mathbf{A}^k)$ *can be extended to a term operation of* $\mathbf{A}$*; and*
2. *if* $R \neq S$ *in* $\mathrm{Sub}(\mathbf{A}^k)$, *then* $R{\restriction_{\sigma(A)}} \neq S{\restriction_{\sigma(A)}}$.

Then σ *is invertible.*

Proof. For any $\mathbf{a} = (a_1, \dots, a_k) \in A^k$ define $\mu(\mathbf{a})$ to be the subuniverse of $\mathbf{A}^k$ generated by $\{\mathbf{a}\}$, that is, $\mu(\mathbf{a}) = \bigcap\big\{R \in \mathrm{Sub}(\mathbf{A}^k) : \mathbf{a} \in R\big\}$. Each $\mu(\mathbf{a})$ is

a uniquely determined subuniverse of $\mathbf{A}^k$ with $\mathbf{a} \in \mu(\mathbf{a})$, since $\mathrm{Sub}(\mathbf{A}^k)$ forms a complete lattice when ordered by inclusion. For the remainder of the proof let Σ denote $\sigma(A^k)$. Let $\mathbf{a} \in A^k$. Since A is finite, we can write $\mu(\mathbf{a}) \cap \Sigma = \{\mathbf{b}_1, \dots, \mathbf{b}_m\}$, where $\mathbf{b}_i = (b_{i,1}, \dots, b_{i,k})$, for $i \leq m$.

We first observe that in the lattice $\mathrm{Sub}(\mathbf{A}^k)$,

$$\mu(\mathbf{a}) \cap \Sigma = \{\mathbf{b}_1, \dots, \mathbf{b}_m\} \subseteq \Big[\bigvee_{i=1}^{m} \mu(\mathbf{b}_i)\Big] \cap \Sigma \subseteq \mu(\mathbf{a}) \cap \Sigma.$$

Applying assumption (2) we obtain $\bigvee_{i=1}^{m} \mu(\mathbf{b}_i) = \mu(\mathbf{a})$.

For every $\mathbf{a} \in A^k$ and $i \leq m$ we certainly have $\mathbf{b}_i \in \mu(\mathbf{a})$. It follows that there is a unary term $p_{\mathbf{a},i}$ such that $p_{\mathbf{a},i}^{\mathbf{A}^k}(\mathbf{a}) = \mathbf{b}_i$, and therefore, for every $j \leq k$, $p_{\mathbf{a},i}^{\mathbf{A}}(a_j) = b_{i,j}$. Since A is finite, we can enumerate the set of all $p_{\mathbf{a},i}$ as a list $t_1, \dots, t_n \in \mathrm{Clo}_1(\mathbf{A})$. In particular, from the previous paragraph we have

$$(\forall \mathbf{a} \in A^k) \quad \mu(\mathbf{a}) = \bigvee_{l=1}^{n} \mu\big(\sigma t_l(a_1), \dots, \sigma t_l(a_k)\big). \tag{2–1}$$

For every $a \in A$, let $\overline{a}$ denote the n-tuple $\big(\sigma t_1(a), \dots, \sigma t_n(a)\big)$.

Claim. *For every $a, a' \in A$, $a \neq a' \implies \overline{a} \neq \overline{a'}$.*

Proof. Let $\mathbf{a} = (a, a', a', \dots, a') \in A^k$ and let E denote $\{\mathbf{x} \in A^k : x_1 = x_2\}$, a subuniverse of $\mathbf{A}^k$. Suppose that $\mu(\mathbf{a}) \cap \Sigma \subseteq E$. Then $\big(\mu(\mathbf{a}) \cap E\big) \cap \Sigma = \mu(\mathbf{a}) \cap \Sigma$. So from assumption (2) we have $\mathbf{a} \in \mu(\mathbf{a}) \subseteq E$ contradicting the fact that $a \neq a'$.

Therefore there is a k-tuple $\mathbf{b} \in \big(\mu(\mathbf{a}) \cap \Sigma\big) - E$. Hence, for some $l \leq n$, $t_l(a) = b_1 \neq b_2 = t_l(a')$. The Claim follows.

Let p be the n-ary partial operation on A for which $p(\overline{a}) = a$ for all $a \in A$. From the previous Claim p is well-defined on its domain. We wish to verify that p preserves every member of $\mathrm{Sub}\,\mathbf{A}^k$. Let $R \in \mathrm{Sub}\,\mathbf{A}^k$ and let $a_1, \dots, a_k$ be elements of A such that $\big(\sigma t_l(a_1), \dots, \sigma t_l(a_k)\big) \in R$ for $l = 1, \dots, n$. From (2–1) we derive

$$(a_1, \dots, a_k) \in \mu(a_1, \dots, a_k) = \bigvee_{l=1}^{n} \mu\big(\sigma t_l(a_1), \dots, \sigma t_l(a_k)\big) \subseteq R.$$

As every $a_j = p\big(\sigma t_1(a_j), \dots, \sigma t_n(a_j)\big)$, p preserves R.

Finally, we apply assumption (1) to obtain a term $t \in \mathrm{Clo}_n(\mathbf{A})$ extending p. Then $t(\sigma t_1(x), \dots, \sigma t_n(x)) = x$ for all $x \in A$ showing σ is invertible. $\square$

In [1] Baker and Pixley show that a finite algebra satisfies condition (1) of Theorem 2.1 if and only if it possesses a $(k+1)$-ary near-unanimity term. (The reader may consult that paper for the definition.) In the remainder of this paper we restrict ourselves to the case $k = 2$. We do this because most of the examples of "almost-primal" algebras that have been considered in the literature can be described in terms of subalgebras of the square. A ternary near-unanimity term is generally called a *majority term,* that is, a ternary term m satisfying the identities

$$m(x, x, y) = m(x, y, x) = m(y, x, x) = x.$$

Applying the Baker-Pixley result to Theorem 2.1 yields the following.

Corollary 2.2. *Let* $\mathbf{A}$ *be a finite algebra with* $\sigma \in \mathrm{Clo}_1 \mathbf{A}$ *idempotent and suppose* $\mathbf{A}$ *has a majority term operation. If* $R\restriction_{\sigma(A)} \neq S\restriction_{\sigma(A)}$ *for every* $R \neq S$ *in* $\mathrm{Sub}(\mathbf{A}^2)$*, then* σ *is invertible.*

In order to apply Corollary 2.2, we need to have a good understanding of the subalgebras of the square. If an algebra has permuting congruences, a useful tool is Fleischer's Lemma (see [20, pg. 203]). For $i = 1, 2$, we use $\pi_i \colon \mathbf{A}_1 \times \mathbf{A}_2 \to \mathbf{A}_i$ to denote the coordinate projection mapping a pair (x_1, x_2) to x_i.

Lemma 2.3 (Fleischer). *Let* $\mathbf{A}$ *be an algebra in a congruence-permutable variety, and let* $R \in \mathrm{Sub}(\mathbf{A}^2)$*. Let* $R_i = \pi_i(R)$*, for* $i = 1, 2$*. There is an algebra* $\mathbf{E}$ *together with surjective homomorphisms* $\alpha_i \colon \mathbf{R}_i \to \mathbf{E}$*, such that*

$$R = \big\{\, (r_1, r_2) \in R_1 \times R_2 : \alpha_1(r_1) = \alpha_2(r_2) \,\big\}.$$

Lemma 2.4. *Let* $\mathbf{A}$ *be an algebra in a congruence-permutable variety.*

(1) *If* $\mathbf{A}$ *is hereditarily simple, then every subuniverse of* $\mathbf{A}^2$ *is either of the form* $R_1 \times R_2$*, or of the form* $\{\, (a, \alpha(a)) : a \in R_1 \,\}$*, where* $R_i \in \mathrm{Sub}\,\mathbf{A}$*,* $i = 1, 2$*, and* $\alpha \colon \mathbf{R}_1 \to \mathbf{R}_2$ *is an isomorphism.*
(2) (Werner) *If* $\Delta_A \subseteq R \in \mathrm{Sub}(\mathbf{A}^2)$*, then* R *is a congruence of* $\mathbf{A}$*.*

Proof. Let R be a subalgebra of $\mathbf{A}^2$, and let R_i, α_i and $\mathbf{E}$ be as in Fleischer's Lemma. Suppose first that $\mathbf{A}$ is hereditarily simple. Since both α_1 and α_2 are surjective and R_1, R_2 are simple, if $|E| > 1$ then $\alpha_2^{-1} \circ \alpha_1$ is an isomorphism from $\mathbf{R}_1$ to $\mathbf{R}_2$, and R will be its graph. Otherwise, E is a singleton, and $R = R_1 \times R_2$.

Now suppose that $\Delta \subseteq R$. From Fleischer's Lemma,

$$R = \{\, (r_1, r_2) : \alpha_1(r_1) = \alpha_2(r_2) \,\} \supseteq \Delta$$

implies that $\alpha_1 = \alpha_2$. From this it follows that $R = \ker \alpha_1$. □

With these observations in hand, we can develop a condition equivalent to the second requirement of Theorem 2.1.

Definition 2.5. Let $\mathbf{A}$ be an algebra.

(1) A subset $S \subseteq A$ is called *separating* if for every $B \in J(\mathrm{Sub}\,\mathbf{A})$ there exists $b \in B \cap S$ such that $\langle b \rangle = B$, and for all $B \in \mathrm{Sub}\,\mathbf{A}$, if $|B| > 1$, then $|B \cap S| > 1$.
(2) An idempotent term $\sigma \in \mathrm{Clo}_1 \mathbf{A}$ is called *separating* if $\sigma(A)$ is separating.

For finite algebras, Lemma 2.6 provides an equivalent formulation of the latter condition in the definition of separating that is useful in practice.

Lemma 2.6. *Let* $\mathbf{A}$ *be a finite algebra, and* $S \subseteq A$*. Then* S *is separating iff every* $B \in J(\mathrm{Sub}\,\mathbf{A})$ *is generated by a member of* S*, and for every* $B \in \mathrm{N}(\mathbf{A})$ *we have* $|B \cap S| > 1$*.*

Proof. One direction holds *a fortiori*. Suppose that S has the condition given in the Lemma. Let B be any subuniverse of cardinality greater than 1. If B is an atom of $\mathrm{Sub}\,\mathbf{A}$, then we have $B \in \mathrm{N}(\mathbf{A})$, so $|B \cap S| > 1$, by assumption. On the other hand,

if B is not an atom, then since $\operatorname{Sub}\mathbf{A}$ is finite, there are distinct elements C_1, C_2 of $J(\operatorname{Sub}\mathbf{A})$ with $B \supseteq C_1, C_2$. By assumption, each of C_1 and C_2 are generated by a member of S. Thus B contains these two (necessarily distinct) generators. $\square$

Combining this Lemma with Lemma 1.5, we see that every invertible, idempotent, unary term term is separating. Let us investigate the converse.

Lemma 2.7. *Let $\mathbf{A}$ be a finite algebra with an idempotent, separating, unary term σ. Suppose $\mathbf{A}$ has a Mal'cev term and is hereditarily simple. Then for every $R \neq S$ in $\operatorname{Sub}(\mathbf{A}^2)$, $R\restriction_{\sigma(A)} \neq S\restriction_{\sigma(A)}$.*

Proof. Let $R \nsubseteq S$ in $\operatorname{Sub}(\mathbf{A}^2)$ and let Σ denote $(\sigma(A))^2$. If $R \cap \Sigma = S \cap \Sigma$, then $R \cap S \cap \Sigma = R \cap \Sigma$, so we may assume at the outset that $S \subsetneq R$. For $i = 1, 2$, let $\pi_i(x_1, x_2) = x_i$. Define $R_i = \pi_i(R)$ and $S_i = \pi_i(S)$. We have $S_i \subseteq R_i$ for $i = 1, 2$. First suppose $S_1 \neq R_1$. Let $B \in J(\operatorname{Sub}\mathbf{A})$ with $B \subseteq R_1$ and $B \nsubseteq S_1$. By hypothesis there is an element $b \in B \cap \sigma(A)$ with $B = \langle b \rangle$. So $b \in R_1 - S_1$. Let $c \in R_2$ be such that $(b, c) \in R$. Then $(\sigma(b), \sigma(c)) = (b, \sigma(c)) \in R$ as well. But $(b, \sigma(c)) \in \Sigma$ and $(b, \sigma(c)) \notin S$, so $R \cap \Sigma \neq S \cap \Sigma$. A similar argument applies if $S_2 \neq R_2$.

So suppose $R_1 = S_1$ and $R_2 = S_2$. Since $\mathbf{A}$ has a Mal'cev term, it generates a congruence-permutable variety. From the hereditary simplicity of $\mathbf{A}$ and from Lemma 2.4 we see that every $R \in \operatorname{Sub}(\mathbf{A}^2)$ is either of the form $R_1 \times R_2$ for $R_i \in \operatorname{Sub}\mathbf{A}$ or of the form $\{\, (a, \alpha(a)) : a \in R_1 \,\}$ where α is an isomorphism from $\mathbf{R_1}$ onto $\mathbf{R_2}$. If $S \subsetneq R$ and $R_1 = S_1$, then we must have $R = R_1 \times R_2$ and $S = \{\, (a, \alpha(a)) : a \in R_1 \,\}$. From $R_2 = S_2$ we see that $|R_1| = |R_2|$ and thus $|R_1| > 1$. Since σ is separating, there exist $a, a' \in R_1 \cap \sigma(A)$, with $a \neq a'$. Let $b \in R_2 \cap \sigma(A)$. Then (a, b), $(a', b) \in R$ but at least one of $(a, b), (a', b)$ is not in S since α is a bijection. $\square$

A finite, hereditarily simple algebra with a Mal'cev term has been called *paraprimal* in the literature. A paraprimal algebra possessing a majority term is usually called *quasiprimal*. Combining Corollary 2.2 and Lemmas 1.5, 2.6 and 2.7 yields the following.

Corollary 2.8. *Let $\mathbf{A}$ be a quasiprimal algebra and suppose σ is an idempotent unary term for $\mathbf{A}$. The following are equivalent:*

(1) *σ is invertible.*
(2) *For all $R \neq S$ in $\operatorname{Sub}(\mathbf{A}^2)$, $R\restriction_{\sigma(A)} \neq S\restriction_{\sigma(A)}$.*
(3) *σ is separating.*

We close this section with one final consequence of invertibility.

Corollary 2.9. *Let $\mathbf{A}$ be an algebra with σ an idempotent, invertible, unary term for $\mathbf{A}$. Then $\big|\sigma(A)\big| \geq \big|J(\operatorname{Sub}\mathbf{A})\big| + \big|\mathrm{N}(\mathbf{A})\big|$.*

Proof. Use Lemma 1.5, parts (2) and (3). $\square$

3. Subalgebra-primal Algebras

Let $\mathbf{A}$ be a finite subalgebra-primal algebra. We give necessary and sufficient conditions for membership in the equivalence class $\mathbf{A}/\equiv_{\mathrm{c}}$. We also describe the minimal-sized members of $\mathbf{A}/\equiv_{\mathrm{c}}$.

Let $\mathbf{A}$ be any finite algebra. Suppose the join-irreducible members of $\operatorname{Sub}\mathbf{A}$ are $B_1, \ldots, B_j$ with the numbering such that the non-singleton atoms are $B_1, \ldots, B_l$. Choose $b_1, \ldots, b_j \in A$ such that $\langle b_i \rangle = B_i$. Since each B_i is join-irreducible, such a choice of b_i is possible. Let $c_1, \ldots, c_l \in A$ be such that $\langle c_i \rangle = B_i$ and $\{c_1, \ldots, c_l\} \cap \{b_1, \ldots, b_j\} = \emptyset$. Define $\sigma : A \to A$ by $\sigma(b_i) = b_i$, $\sigma(c_i) = c_i$, and for $a \in A - \{b_1, \ldots, b_j, c_1, \ldots, c_l\}$, let $\sigma(a) = b_i$ for a choice of b_i with $b_i \in \langle a \rangle$. Since every $\langle a \rangle$ is a join of join-irreducible members of $\operatorname{Sub}\mathbf{A}$, such a function σ exists. From this construction and Lemma 2.6, it is immediate that (*i*) $\sigma(\sigma(x)) = \sigma(x)$ for all $x \in A$, (*ii*) $\sigma(A) = \{b_1, \ldots, b_j, c_1, \ldots, c_l\}$, and (*iii*) σ is separating.

If the algebra $\mathbf{A}$ in the previous paragraph is subalgebra-primal, then the function σ is also a term operation of $\mathbf{A}$ since $\sigma(a) \in \langle a \rangle$ for every $a \in A$. Since a finite subalgebra-primal algebra is quasiprimal, we deduce that σ is invertible by Corollary 2.8. From Corollary 2.9 it follows that the algebra $\mathbf{A}(\sigma)$ is minimal-sized in $\mathbf{A}/\equiv_{\mathrm{c}}$. We summarize this as follows.

Theorem 3.1. *Let $\mathbf{A}$ be a finite subalgebra-primal algebra and suppose $\mathbf{B} \equiv_{\mathrm{c}} \mathbf{A}$ with $|B|$ minimal. Then $|B| = j + l$ for j the number of join-irreducible elements of $\mathbf{Sub}(\mathbf{A})$ and l the number of non-singleton atoms of $\mathbf{Sub}(\mathbf{A})$.*

Theorem 3.2. *Let $\mathbf{A}$ be a finite subalgebra-primal algebra and let $\mathbf{B}$ be any algebra. Then $\mathbf{A} \equiv_{\mathrm{c}} \mathbf{B}$ if and only if*

(1) *$\mathbf{B}$ is finite and subalgebra-primal, and*
(2) *there is a lattice isomorphism $h\colon \mathbf{Sub}(\mathbf{A}) \to \mathbf{Sub}(\mathbf{B})$ that is a bijection between the set of singleton subalgebras of $\mathbf{A}$ and of $\mathbf{B}$.*

Proof. First suppose $\mathbf{A} \equiv_{\mathrm{c}} \mathbf{B}$. The conclusions follow from Theorem 1.6 and Lemma 1.5.

Conversely let (1) and (2) hold. Let $b_1, \ldots, b_j, c_1, \ldots, c_l \in A$ and σ be as in the two paragraphs before Theorem 3.1. We have $\sigma(A) = \{b_1, \ldots, b_j, c_1, \ldots, c_l\}$ and $\sigma \in \operatorname{Clo}_1(\mathbf{A})$ with $\mathbf{A} \equiv_{\mathrm{c}} \mathbf{A}(\sigma)$ and $\mathbf{A}(\sigma)$ is a subalgebra-primal algebra. For the algebra $\mathbf{B}$ we also apply the two paragraphs before Theorem 3.1 to obtain $\sigma' \in \operatorname{Clo}_1\mathbf{B}$ and elements $\{b'_1, \ldots, b'_{j'}, c'_1, \ldots, c'_{l'}\} = \sigma'(B) \subseteq B$. Hypothesis (2) insures that $j = j', l = l'$, and that there is a bijection from $\sigma(A)$ to $\sigma'(B)$ given by, say, $b_i \mapsto b'_i$ and $c_i \mapsto c'_i$ that induces a bijection from $\operatorname{Sub}(\mathbf{A}(\sigma))$ to $\operatorname{Sub}(\mathbf{B}(\sigma'))$. Finally, we note that if two subalgebra-primal algebras share the same universe and have the same set of subuniverses, then the algebras are term equivalent. It follows that that $\mathbf{A}(\sigma)$ and $\mathbf{B}(\sigma')$ are weakly isomorphic and thus $\mathbf{A} \equiv_{\mathrm{c}} \mathbf{A}(\sigma) \equiv_{\mathrm{c}} \mathbf{B}(\sigma') \equiv_{\mathrm{c}} \mathbf{B}$. □

Example 3.3. Let $\mathbf{A}$ be a k-element subalgebra-primal algebra having exactly one proper subalgebra, and suppose this subalgebra has cardinality m. It is known (see [27]) that $\operatorname{Clo}(\mathbf{A})$ is a co-atom in the lattice of clones on $\mathbf{A}$. If $k = 3$ and $m = 2$, then $\mathbf{A}$ is term equivalent to the 3-element Łukasiewicz algebra $\mathbf{Ł}$ and if $k = 2$ and $m = 1$, then $\mathbf{A}$ is term equivalent to the 2-element Boolean ring without unit, $\mathbf{R}$. From Theorems 3.1 and 3.2 we see that for every such $\mathbf{A}$ with $m = 1, \mathbf{A} \equiv_{\mathrm{c}} \mathbf{R}$ and if $m > 1$ then $\mathbf{A} \equiv_{\mathrm{c}} \mathbf{Ł}$. Denecke and Lüders [7] have carried out a classification with respect to $\equiv_{\mathrm{c}}$ of the algebras corresponding to all the clones that are co-atoms in the lattice of clones on a finite set.

Example 3.4. For $n \geq 1$ an n-element Wajsberg chain is an algebra isomorphic to

$$\mathbf{C}_n = \langle\, \{0, 1, \ldots, n\}, \neg, \rightarrow, 0, n \,\rangle$$

in which $\neg x = n - x$ and $x \rightarrow y = \max\{y - x, 0\}$. These algebras are the natural generalization of the 3-element Łukasiewicz algebras in Example 3.3. See [9] and [12]. Each $\mathbf{C}_n$ is term equivalent to a bounded, commutative BCK chain as studied by Traczyk [28]. From Denecke [6, pg. 134] we see that each $\mathbf{C}_n$ is subalgebra-primal. The lattice $\mathbf{Sub}(\mathbf{C}_n)$ is isomorphic to the lattice of divisors of n in which a new bottom element (corresponding to $\emptyset$) has been added. The unique atom in $\mathbf{Sub}(\mathbf{C}_n)$ has precisely two elements, $\{0, n\}$. Thus, by Theorem 3.2, we have $\mathbf{C}_n \equiv_{\mathrm{c}} \mathbf{C}_m$ if and only if n and m have isomorphic lattices of divisors.

In [21], Murskiĭ proved that almost all algebras of a sufficiently rich similarity type are subalgebra-primal. We conclude this section by considering his theorem in conjunction with Theorem 3.2.

Let τ be a finite similarity type and let τ_k denote all algebras of type τ having universe $\{0, 1, \ldots, k-1\}$. For a property P of algebras, let

$$\Pr(P; \tau_k) = \frac{|\{\mathbf{A} \in \tau_k : \mathbf{A} \vDash P\}|}{|\tau_k|}$$

and

$$\Pr(P; \tau) = \lim_{k \to \infty} \Pr(P; \tau_k)$$

if this limit exists. Thus, $\Pr(P; \tau)$ is the probability that an arbitrary finite algebra of type τ has property P. For a discussion of this concept see Freese [10]. We say "almost all" algebras of type τ have property P if $\Pr(P; \tau) = 1$.

For an operation f on a set A, let $\mathrm{Fix}(f) = \{i \in A : f(i, \ldots, i) = i\}$. For $S \subseteq A$ we denote by $C(A, S)$ the clone of all operations f on A having $S \subseteq \mathrm{Fix}(f)$. Thus $C(A, \emptyset)$ is the clone of all operations on A. Note that the algebra $\langle A, C(A, S)\rangle$ is subalgebra-primal for every $S \subseteq A$, and the only proper, nonempty subuniverses of this algebra are the singleton subsets of S. The clones on the set A that contain the clone $C(A, S)$ are precisely the clones $C(A, T)$ for $T \subseteq S$. Thus, in the lattice of clones on the set A, the family of clones that contain $C(A, A)$ is a Boolean lattice having $|A|$ atoms.

We will be interested in the following family of algebras:

$$\mathbf{S}_0 = \langle \{0, 1\},\, C(\{0, 1\}, \emptyset)\rangle,$$

$$\mathbf{S}_1 = \langle \{0, 1\},\, C(\{0, 1\}, \{0\})\rangle,$$

and for $k \geq 2$, $\mathbf{S}_k = \langle A, C(A, A)\rangle$ with $A = \{0, 1, \ldots, k-1\}$. So $\mathbf{S}_0$ is term equivalent to a 2-element Boolean algebra and $\mathbf{S}_1$ is term equivalent to the Boolean ring $\mathbf{R}$ in Example 3.3.

Murskiĭ [21], in conjunction with his work on the existence of finite equational bases for finite algebras, shows that if a finite similarity type τ has at least one at least binary operation, then almost all finite algebras $\mathbf{A}$ of similarity type τ

contain $C(A, A)$ in $\operatorname{Clo}\mathbf{A}$. Thus, almost all algebras of type τ are subalgebra-primal. McKenzie [19], in an exposition of Murskiĭ's result, shows that if τ contains at least two operation symbols, at least one of which has arity ≥ 2, then almost all finite algebras of type τ are primal. Combining this with Hu's result that every primal algebra is categorically equivalent to the two-element Boolean algebra gives the following.

Theorem 3.5. *If τ is a finite similarity type that contains an operation symbol of arity ≥ 2 and at least one other operation symbol, then almost all finite algebras having similarity type τ are categorically equivalent to $\mathbf{S}_0$.*

We now focus on the case of a similarity type τ consisting of precisely one operation symbol f, with f having arity $n \geq 2$. Note that $|\tau_k| = k^{k^n}$. The number of algebras of type τ with universe $\{0, 1, \ldots, k-1\}$ having $|\operatorname{Fix}(f)| = r$ is

$$\binom{k}{r}(k-1)^{k-r}k^{k^n-k}$$

and so if P is the property that $|\operatorname{Fix}(f)| = r$, then

$$\Pr(P; \tau_k) = \frac{k!}{r!(k-r)!}\frac{1}{k^k}(k-1)^{k-r} = \frac{1}{r!}\frac{k!}{(k-r)!k^r}\left(\frac{k-1}{k}\right)^{k-r}.$$

If we fix r and let $k \to \infty$ we see that $\Pr(P; \tau) = 1/(r!e)$. From Murskiĭ's result almost all finite algebras $\mathbf{A}$ of type τ contain $C(A, A)$ in their clone of term operations and thus almost all algebras $\mathbf{A}$ of type τ have $\operatorname{Clo}\mathbf{A} = C(A, \operatorname{Fix}(f))$. Note that by Theorem 3.2 if $|S| = r$ for $r \geq 0$, then the subalgebra-primal algebra $\langle A, C(A, S)\rangle$ is categorically equivalent to $\mathbf{S}_r$. These observations may be summarized as follows.

Theorem 3.6. *Let τ be a similarity type consisting of precisely one operation symbol and let the arity of this symbol be at least 2. Then the probability that an algebra $\mathbf{A}$ of type τ is categorically equivalent to the algebra $\mathbf{S}_r$ is $1/(r!e)$. Thus, almost all algebras of type τ are categorically equivalent to an $\mathbf{S}_r$ for $r = 0, 1, \ldots$.*

4. Congruence-primal, Arithmetical Algebras

Recall from the introduction, that an algebra $\mathbf{A}$ is called *congruence-primal* if every operation on $\mathbf{A}$ that preserves every congruence of $\mathbf{A}$ is a term operation of $\mathbf{A}$. Unlike the case for subalgebra-primal algebras for which we have the concrete version of the Birkhoff-Frink Theorem, (see [3] or [20, pg. 183]), there exist 0,1-sublattices $\mathbf{L}$ of $\operatorname{Eqv} A$ with A finite for which there is no algebra $\mathbf{A}$ with universe A and $\mathbf{Con}\,\mathbf{A} = \mathbf{L}$. In fact, a long-standing open question asks whether every finite lattice is isomorphic to the congruence lattice of a finite algebra.

On the other hand, if $\mathbf{L}$ is a finite, distributive 0,1-sublattice of $\operatorname{Eqv} A$ then Quackenbush and Wolk proved in [26] (see also [2], [16]) that $\mathbf{L} = \mathbf{Con}\,\mathbf{A}$ for an algebra $\mathbf{A}$ with universe A. In fact, if we form the algebra $\mathbf{B} = \langle A, \mathcal{P}(L)\rangle$ then $\mathbf{B}$ will be congruence primal and $\mathbf{Con}\,\mathbf{B} = \mathbf{L}$.

We focus on distributive 0,1-sublattices $\mathbf{L}$ of $\operatorname{Eqv} A$, for A finite, having the additional virtue that the members of L are pairwise permutable. For each such $\mathbf{L}$ there is a finite, congruence-primal algebra $\mathbf{A}$ with $\mathbf{Con}\,\mathbf{A} = \mathbf{L}$. We will describe the class $\mathbf{A}/\equiv_{\mathrm{c}}$ for such congruence-primal, arithmetical algebras.

Definition 4.1. An algebra $\mathbf{A}$ is called *arithmetical* if $\mathbf{Con}\,\mathbf{A}$ is a distributive lattice of permuting equivalence relations. A variety V is called arithmetical if every $\mathbf{A} \in V$ is arithmetical.

In general, the variety generated by an arithmetical algebra $\mathbf{A}$ need not be arithmetical. However, we have the following result of A. Pixley [22, Theorem 3.5].

Theorem 4.2. *Let $\mathbf{A}$ be a finite arithmetical algebra. Then $\mathbf{A}$ is congruence-primal if and only if the following three conditions hold:*

(1) *$\mathbf{A}$ has no proper subalgebras.*
(2) *If $\alpha, \beta \in \operatorname{Con}\mathbf{A}$, then any isomorphism $h\colon \mathbf{A}/\alpha \to \mathbf{A}/\beta$ is the identity.*
(3) *The variety generated by $\mathbf{A}$ is arithmetical.*

Let x, y be elements of an algebra $\mathbf{A}$. We denote by $\Theta_{\mathbf{A}}(x, y)$ the congruence of $\mathbf{A}$ generated by (x, y) . If $\mathbf{L}$ is a distributive lattice with 0, then it is known that $\Theta_{\mathbf{L}}(0, a) = \{\, (x, y) : x \vee a = y \vee a \,\}$, and the congruence class of 0 modulo $\Theta_{\mathbf{L}}(0, a)$ is the principal ideal generated by a.

Let $\mathbf{L}$ be a finite distributive lattice. The map $x \mapsto \Theta(0, x)$ is an embedding of $\mathbf{L}$ into $\mathbf{Con}\,\mathbf{L}$. Let L_0 be the range of this map. Then L_0 is a $0,1$-sublattice of $\mathbf{Con}\,\mathbf{L}$ which in turn is a $0,1$-sublattice of $\operatorname{Eqv} L$. Furthermore, the elements of L_0 permute. For, if $x \equiv y \pmod{\Theta(0, a \vee b)}$ then $x \vee (a \vee b) = y \vee (a \vee b)$, so $x\ \Theta(0, a)\ z\ \Theta(0, b)\ y$, where $z = (a \vee x) \wedge (b \vee y)$.

Define $\mathbf{L}^*$ to be the algebra $\langle L,\, \mathcal{P}L_0 \rangle$. Observe that $\mathbf{L}^*$ is an expansion of $\mathbf{L}$, since the lattice operations preserve all of $\operatorname{Con}\mathbf{L}$, so they certainly preserve L_0. From the Quackenbush-Wolk result mentioned above, we deduce that $\operatorname{Con}\mathbf{L}^* = L_0$. Therefore, $\mathbf{L}^*$ is a congruence-primal, arithmetical algebra. By Theorem 4.2, $\mathbf{L}^*$ generates an arithmetical variety.

Theorem 4.3. *Let $\mathbf{A}$ be a congruence-primal, arithmetical algebra, and let $\mathbf{L} = \mathbf{Con}\,\mathbf{A}$. Then $\mathbf{A} \equiv_{\mathrm{c}} \mathbf{L}^*$.*

Proof. From Theorem 1.3, we need to find a positive integer m and an invertible, idempotent, unary term σ such that $\mathbf{L}^* \simeq \mathbf{A}^{[m]}(\sigma)$. Let $\{\alpha_1, \ldots, \alpha_m\}$ be the join-irreducible elements of L. For every $i \leq m$, there are elements $a_i, b_i \in A$ such that $\alpha_i = \Theta_{\mathbf{A}}(a_i, b_i)$. For every $\beta \in L$ let $J_\beta = \{\, i \leq m : \alpha_i \leq \beta \,\}$. Of course, $\beta = \bigvee \{\, \alpha_i : i \in J_\beta \,\}$.

Let $\mathbf{B} = \mathbf{A}^{[m]}$. For every $\beta \in L$, define $c_\beta = (x_1, \ldots, x_m) \in B$, where $x_i = b_i$ if $i \in J_\beta$, and a_i otherwise. In particular, $c_0 = (a_1, \ldots, a_m)$. It is easy to check that $\beta^{[m]} = \Theta_{\mathbf{B}}(c_0, c_\beta)$. For every $\alpha, \beta \in L$ we have $J_{\alpha\vee\beta} = J_\alpha \cup J_\beta$. Therefore, $c_0\ \alpha^{[m]}\ c_\alpha\ \beta^{[m]}\ c_{\alpha\vee\beta}$.

Recall that $\mathbf{B} = \mathbf{A}^{[m]}$ will also be congruence-primal and arithmetical, and that the map $\alpha \mapsto \alpha^{[m]}$ is an isomorphism of $\mathbf{L} = \mathbf{Con}\,\mathbf{A}$ with $\mathbf{Con}\,\mathbf{B}$. Without loss of generality, we will assume, for the remainder of the proof, that $\mathbf{L} = \operatorname{Con}\mathbf{B}$. We have established the following

Claim. *In the algebra $\mathbf{B} = \mathbf{A}^{[m]}$ there is a subset $C = \{\, c_\beta : \beta \in L \,\}$ satisfying*

$$(\forall \beta \in L)\ \ \beta = \Theta_{\mathbf{B}}(c_0, c_\beta) \quad \text{and} \tag{4–1}$$

$$(\forall \alpha, \beta \in L)\ \ c_0\ \alpha\ c_\alpha\ \beta\ c_{(\alpha\vee\beta)}. \tag{4–2}$$

The next task is to find an appropriate term σ. Define a unary operation on B by

$$\sigma(x) = c_{\Theta(c_0,x)}.$$

From (4–1) we see that $\sigma(B) = C$ and, for every $\beta \in L$, $\sigma(c_\beta) = c_{\Theta(c_0,c_\beta)} = c_\beta$. Thus $\sigma(\sigma(x)) = \sigma(x)$, that is, σ is an idempotent operation. Suppose for the moment that σ is actually a term operation on $\mathbf{B}$. We wish to apply Corollary 2.2 to show that σ is invertible. From Lemma 1.5 and Theorem 1.6, $\mathbf{B}$ is congruence-primal and arithmetical. By Theorem 4.2, the variety generated by $\mathbf{B}$ is arithmetical. Consequently, it has both a Mal'cev term and a majority term. Congruence-primality implies that every element of B is the value of a constant term, and therefore by Lemma 2.4 part (2), every subalgebra of $\mathbf{B}^2$ is a congruence relation. Thus to apply Corollary 2.2 we need only verify that $\alpha\restriction_{\sigma(B)} \neq \beta\restriction_{\sigma(B)}$ for all $\alpha \neq \beta$ in L. But from (4–1) we see that $\alpha \neq \beta \implies c_\alpha \neq c_\beta \implies \alpha\restriction_{\sigma(B)} \neq \beta\restriction_{\sigma(B)}$ as desired.

It remains to verify that σ is in fact a term operation on $\mathbf{B}$. By the congruence-primality of $\mathbf{B}$, this is equivalent to showing that σ preserves every member of L. We require an observation on the preservation of congruences.

Lemma 4.4. *Let U be a set, f an operation on U, and let $\alpha, \beta \in \mathrm{Eqv}(U)$. If α and β are preserved by f, then so are $\alpha \wedge \beta$ and $\alpha \vee \beta$ (in the lattice $\mathrm{Eqv}(U)$).*

Proof of Lemma. It is trivial to verify that f preserves both $\alpha \cap \beta$ and $\alpha \circ \beta$. Since $\alpha \wedge \beta$ is equal to the former, it is preserved by f. The congruence $\alpha \vee \beta = \bigcup \{ (\alpha \circ \beta)^n : n > 0 \}$, where $(\alpha \circ \beta)^{k+1} = (\alpha \circ \beta)^k \circ \alpha \circ \beta$. This is the union of an ascending chain of relations that are all preserved by f, so it too is preserved. □

We return to the verification that σ preserves every element of $L = \mathrm{Con}\,\mathbf{B}$. Let $\alpha \in L$. We prove that σ preserves α by induction on the height of α in $\mathbf{L}$. If $\alpha = 0$, then α is certainly preserved by σ. Suppose that every congruence dominated by α is preserved. If α is not join-irreducible, then by Lemma 4.4 (and the finiteness of L) α will be preserved.

So assume α is join-irreducible. Let $(b, d) \in \alpha$. If $\Theta_{\mathbf{B}}(b, d) < \alpha$, then by the induction assumption $(\sigma(b), \sigma(d)) \in \Theta(b, d) < \alpha$. So suppose that $\alpha = \Theta(b, d)$. Let $\beta = \Theta(c_0, b)$ and $\gamma = \Theta(c_0, d)$. Then $b \;\beta\; c_0 \;\gamma\; d$ implies that $\alpha \leq \beta \vee \gamma$. Since α is join-irreducible and L is distributive, it follows that $\alpha \leq \beta$ or $\alpha \leq \gamma$. Without loss of generality, assume the former. Now, $\gamma \leq \alpha \vee \beta = \beta$, so $\beta \leq \alpha \vee \gamma \leq \beta$; in other words, $\beta = \alpha \vee \gamma$. But now by (4–2) we have $c_\beta \;\alpha\; c_\gamma$. By definition, and by (4–1), $\sigma(b) = c_\beta$ and $\sigma(d) = c_\gamma$. Therefore $(\sigma(b), \sigma(d)) \in \alpha$, so α is preserved.

We have established that σ is an idempotent, invertible, unary term on $\mathbf{B}$, and $\sigma(B) = C$. Therefore, $\mathbf{A} \equiv_{\mathrm{c}} \mathbf{B} \equiv_{\mathrm{c}} \mathbf{B}(\sigma)$. Finally, we show that $\mathbf{L}^* \simeq \mathbf{B}(\sigma)$. There is a bijection $\beta \mapsto c_\beta$ from L to C. Furthermore, $\mathbf{Con}\,\mathbf{L}^* = \{ \Theta_{\mathbf{L}}(0, \alpha) : \alpha \in L \} \cong \mathbf{L} = \mathbf{Con}\,\mathbf{B}$ by $\Theta_{\mathbf{L}}(0, \alpha) \mapsto \alpha$.

We claim that

$$(\forall \alpha, \beta, \gamma \in L) \quad (\beta, \gamma) \in \Theta_{\mathbf{L}}(0, \alpha) \iff c_\beta \;\alpha\; c_\gamma.$$

Recall that $(\beta, \gamma) \in \Theta_{\mathbf{L}}(0, \alpha) \iff \beta \vee \alpha = \gamma \vee \alpha$. If this latter equality holds, then $c_\beta \;\alpha\; c_{(\beta \vee \alpha)} = c_{(\gamma \vee \alpha)} \;\alpha\; c_\gamma$, by (4–2). Conversely, if $c_\beta \;\alpha\; c_\gamma$, then, again

by (4–2), $c_0\ \beta\ c_\beta\ \alpha\ c_\gamma\ \alpha\ c_{(\gamma\vee\alpha)}$. Thus $\Theta_{\mathbf{B}}\big(c_0, c_{(\gamma\vee\alpha)}\big) \subseteq \beta \vee \alpha$. But from (4–1), $\gamma \vee \alpha = \Theta_{\mathbf{B}}\big(c_0, c_{(\gamma\vee\alpha)}\big)$. Combining these last two relationships, and applying symmetry, we conclude that $\beta \vee \alpha = \gamma \vee \alpha$.

Finally, since the bijection $\beta \mapsto c_\beta$ induces a correspondence of the congruences of $\mathbf{L}^*$ with those of $\mathbf{B}(\sigma)$, and since both algebras are congruence-primal, it follows that they are weakly isomorphic. □

Corollary 4.5. *Let* $\mathbf{A}$ *be a finite, congruence-primal, arithmetical algebra, and let* $\mathbf{B}$ *be any algebra. Then* $\mathbf{A} \equiv_{\mathrm{c}} \mathbf{B}$ *if and only if* $\mathbf{B}$ *is finite, congruence-primal, arithmetical and* $\operatorname{Con}\mathbf{A} \cong \operatorname{Con}\mathbf{B}$.

Proof. Suppose $\mathbf{A} \equiv_{\mathrm{c}} \mathbf{B}$. That $\mathbf{B}$ has each of the four conditions follows from Lemma 1.5 and Theorem 1.6 and the fact that finiteness is preserved by categorical equivalence. Suppose conversely, that $\mathbf{B}$ is finite, congruence-primal, arithmetical, and that $\mathbf{L} = \operatorname{Con}\mathbf{A} \cong \operatorname{Con}\mathbf{B}$. By Theorem 4.3, $\mathbf{A} \equiv_{\mathrm{c}} \mathbf{L}^* \equiv_{\mathrm{c}} \mathbf{B}$. □

From Corollary 4.5 we see that the classes $\mathbf{A}/\equiv_{\mathrm{c}}$ as $\mathbf{A}$ ranges over all finite, congruence-primal and arithmetical algebras can be indexed by the collection of non-isomorphic, finite, distributive lattices. We provide a natural family of distinct representatives for these classes. A *dual Heyting algebra* $\mathbf{H} = \langle H, \vee, \wedge, *, 0, 1\rangle$ is an algebra in which $\langle H, \vee, \wedge, 0, 1\rangle$ is a bounded distributive lattice and $*$ is a binary operation satisfying

$$x \vee z \geq y \iff z \geq x * y.$$

For a dual Heyting algebra $\mathbf{H}$ let $\mathbf{H}^+$ denote $\mathbf{H}$ in which all elements of H have been included as constant terms. Note that $\operatorname{Con}(\mathbf{H}^+) = \operatorname{Con}(\mathbf{H})$. The following facts are well known.

(1) The variety of all dual Heyting algebras is arithmetical.
(2) The behavior of the operation $*$ in a dual Heyting algebra $\mathbf{H}$ is uniquely determined by the lattice structure on $\langle H, \vee, \wedge\rangle$.
(3) If $\mathbf{H}$ is a finite dual Heyting algebra, then every $\theta \in \operatorname{Con}(\mathbf{H})$ is of the form $\Theta(0, a)$ for $a \in H$, and thus $\mathbf{Con}(\mathbf{H}) \cong \langle H, \vee, \wedge\rangle$.

Finally, it follows from [23] that for every finite dual Heyting algebra $\mathbf{H}$, the algebra $\mathbf{H}^+$ is congruence-primal. The collection of all $\mathbf{H}^+$ as $\mathbf{H}$ ranges over finite distributive lattices form a system of representatives for the $\equiv_{\mathrm{c}}$ classes of congruence-primal, arithmetical algebras. In fact, it is not hard to show that if $\mathbf{L}$ is a finite distributive lattice, then $\mathbf{L}$ has a unique expansion to a dual Heyting algebra $\mathbf{H}$ and the algebras $\mathbf{L}^*$ and $\mathbf{H}^+$ are term-equivalent.

It is natural to ask for the size of the smallest member of $\mathbf{A}/\equiv_{\mathrm{c}}$, when $\mathbf{A}$ is finite, congruence-primal and arithmetical. We can phrase the problem in the following way. Let $\mathbf{L}$ be a finite distributive lattice. Find the smallest integer $n(\mathbf{L})$ such that $\mathbf{L}$ can be embedded as a permuting, 0,1-sublattice of $\operatorname{Eqv} A$ for a set A of size $n(\mathbf{L})$.

The embedding $\mathbf{L} \rightarrowtail \operatorname{Con}\mathbf{L}$ given before Theorem 4.3 shows that $n(\mathbf{L})$ always exists, and in fact $n(\mathbf{L}) \leq |L|$. If $\mathbf{L}$ is a chain, it is easy to see that $n(\mathbf{L}) = |L|$. Likewise if $\mathbf{L}$ is a Boolean lattice with n atoms, then the embedding $\mathbf{L} \rightarrowtail \operatorname{Eqv} A$ by permuting equivalences ensures that the set A decomposes into a Cartesian product of at least n sets of cardinality greater than 1. So in this case too, $n(\mathbf{L}) \geq 2^n = |L|$. On the other hand, the next example shows that $|L|$ is far from a lower bound for $n(\mathbf{L})$.

Example 4.6. An example of a congruence-primal and arithmetical algebra $\mathbf{A}$ with $|\operatorname{Con}\mathbf{A}| > 2^{|A|/2}$ for arbitrarily large finite $\mathbf{A}$.

For $m \geq 2$ let $A = \{0, 1, \ldots, 2^m - 1\}$. For each i with $1 \leq i \leq 2^{m-1} - 1$, define $b_i = \{2i, 2i + 1\}$, and let β_i be the equivalence relation on A having b_i as its only nontrivial block. Let B be the sublattice of $\operatorname{Eqv} A$ generated by the β_i. Then $\mathbf{B}$ is isomorphic to the power set of $\{b_0, \ldots, b_{2^{m-1}-1}\}$ and has $2^{2^{m-1}}$ elements. Let β denote the top element of B. So β has 2^{m-1} blocks. For $0 \leq j \leq 2^{m-2} - 1$, let $c_j = b_{2j} \cup b_{2j+1}$ and define γ_j to be the unique equivalence relation covering β in $\operatorname{Eqv} A$ having c_j as a block. Let C be the sublattice of $\operatorname{Eqv} A$ generated by the γ_i, and let γ denote the largest element of C. Then the interval from β to γ is isomorphic to the power set of $\{c_0, \ldots, c_{2^{m-2}-1}\}$ and has $2^{2^{m-2}}$ elements. We continue in this fashion until we reach a co-atom of $\operatorname{Eqv} A$ consisting of the equivalence relation with the two blocks $\{0, 1, \ldots, 2^{m-1} - 1\}$ and $\{2^{m-1}, \ldots, 2^m - 1\}$. Let $\mathbf{L}$ be the resulting $0, 1$-sublattice of $\operatorname{Eqv} A$. The lattice $\mathbf{L}$ has $2^{2^{m-1}} + 2^{2^{m-2}} + \cdots + 2^{2^1} + 2^{2^0} - (m-1)$ elements. (Here we subtract $m - 1$ because of the overlap of successive layers.) Thus, $\mathbf{L}$ is distributive since it is the linear sum of Boolean lattices. Hence by [26], $\mathbf{L}$ is the congruence lattice of a congruence-primal algebra $\mathbf{A}$ with universe A. It is easy to see that all the equivalence relations of L permute, since if $\alpha, \beta \in L$ and if $i \in A$, then either $i/\alpha \subseteq i/\beta$ or $i/\beta \subseteq i/\alpha$. So $\mathbf{A}$ is congruence-primal and arithmetical. $\square$

5. Automorphism-primal Algebras

Let $\mathbf{A}$ be a finite automorphism-primal algebra. In this section we give a characterization of the members of $\mathbf{A}/\equiv_{\mathrm{c}}$ and describe explicitly (up to weak isomorphism) the member of minimal size. The results here seem to be inherently more difficult than those of the preceding sections. A possible explanation is this: although the definition of automorphism-primal seems to precisely parallel that of subalgebra-primal and congruence-primal, the algebraic characterizations are not quite analogous. A finite subalgebra-primal algebra has neither automorphisms nor congruences. A finite congruence-primal algebra has neither automorphisms nor subalgebras. But a finite automorphism-primal algebra *can* have subalgebras (although no congruences). Specifically, the set of fixed points of an automorphism is a subalgebra of any algebra. (On the other hand, in Section 4 we restrict ourselves to congruence-primal algebras that are *arithmetical*. Questions about arbitrary congruence-primal algebras seem to be very difficult. In particular, no analogue of Theorem 4.2 is known.)

If we require our automorphism-primal algebras to have no subalgebras we arrive at the notion of demi-primal algebra originally proposed by Quackenbush in [25]: we shall call a finite algebra $\mathbf{A}$ *Q-demi-primal* if $\mathbf{A}$ is automorphism-primal and no non-identity automorphism has a fixed point. When we restrict our attention to that class, we get an easily stated result: If $\mathbf{A}$ is Q-demi-primal, then $\mathbf{A} \equiv_{\mathrm{c}} \mathbf{B}$ if and only if $\mathbf{B}$ is Q-demi-primal and $\operatorname{Aut}\mathbf{A} \cong \operatorname{Aut}\mathbf{B}$. A proof of this would be much simpler than that of Theorem 5.8.

Let $\mathbf{A}$ be any finite algebra. Consider again the necessary conditions imposed by Corollary 2.9 on $\sigma(A)$ for an invertible, idempotent term σ. The set $\sigma(A)$ was shown to contain a generator of each join-irreducible member of $\operatorname{Sub}\mathbf{A}$ and a

second element of each member of $\mathrm{N}(\mathbf{A})$. In Theorem 3.1 it is shown that every finite subalgebra-primal algebra has a term σ such that $\sigma(A)$ contains exactly these elements.

Let Γ denote the automorphism group of $\mathbf{A}$. It is easy to see that for any unary term operation f of $\mathbf{A}$, the set $f(A)$ must be a union of orbits under the action of Γ. That is, if $a \in f(A)$ and $\gamma \in \Gamma$, then $\gamma(a) \in f(A)$. Note that a subalgebra-primal algebra has trivial automorphism group, so this observation does not contradict Theorem 3.1. However, for an invertible, idempotent term operation σ on an arbitrary algebra $\mathbf{A}$, we see that $\sigma(A)$ must contain the entire orbit of a generator of each join-irreducible subalgebra, and also the orbit of a second generator of each member of $\mathrm{N}(\mathbf{A})$.

It turns out that when $\mathbf{A}$ is automorphism-primal, there is always a term operation σ such that $\sigma(A)$ consists of precisely those orbits. Unfortunately, the organization of these orbits can be quite complex. A precise statement of the result is somewhat awkward, and is best given in the language of group actions. So we begin with a review of the relevant notions.

Let Γ be a group. A Γ-*set* is an algebra $\mathcal{A} = \langle A, f_\gamma \rangle_{\gamma \in \Gamma}$ such that the map $\gamma \mapsto f_\gamma$ is a group homomorphism from Γ to the group of permutations of the set A. The structure $\mathcal{A}$ is called *faithful* if this group homomorphism is injective. Since the letter f serves no useful purpose here, we follow the usual custom and write $\gamma{\cdot}a$ instead of $f_\gamma(a)$. For each $a \in A$, $\Gamma{\cdot}a = \{\, \gamma{\cdot}a : \gamma \in \Gamma \,\}$ denotes the *orbit of* a. It is easy to see that the orbits partition A and that a subset of A is a subuniverse (i.e., a sub-Γ-set) of $\mathcal{A}$ if and only if it is a union of orbits. A Γ-set is called *transitive* if it consists of a single orbit.

The binary relation $\{\, (\gamma, a) \in \Gamma \times A : \gamma{\cdot}a = a \,\}$ induces a Galois connection between the subsets of Γ and of A. The closed subsets of Γ are of the form $\Gamma_X = \{\, \gamma \in \Gamma : (\forall x \in X)\ \ \gamma{\cdot}x = x \,\}$ for some $X \subseteq A$. The set Γ_X is always a subgroup of Γ, called the *stabilizer of* X. For $a \in A$, we write Γ_a instead of $\Gamma_{\{a\}}$. On the other side, for any subset Λ of Γ, the set $\operatorname{Fix}\Lambda = \{\, a \in A : (\forall \lambda \in \Lambda)\ \ \lambda{\cdot}a = a \,\}$ is a typical closed subset of A under the Galois connection. Note that these fixed point sets are *not* sub-Γ-sets of $\mathcal{A}$. From the theory of Galois connections, we have an anti-isomorphism between the lattice of stabilizers and the lattice of fixed point sets. Thus, for example, the smallest fixed point set containing an element $a \in A$ is $\operatorname{Fix}(\Gamma_a)$, and this set is join-irreducible (in the lattice of fixed point sets) if and only if Γ_a is meet-irreducible (in the lattice of stabilizers).

Let Λ be any subgroup of Γ. We can form a (transitive) Γ-set with universe Γ/Λ (the set of left cosets of Λ) by defining $\gamma{\cdot}\alpha\Lambda$ to be $(\gamma\alpha)\Lambda$. For any Γ-set $\mathcal{A}$, and $a \in A$ we have the fundamental relationship

$$\Gamma/\Gamma_a \cong \Gamma{\cdot}a$$

(isomorphism as Γ-sets). Thus every transitive Γ-set is isomorphic to one of the form Γ/Λ for some subgroup Λ.

We need a bit more notation. Let Δ and Λ be subgroups of a group Γ, $\gamma \in \Gamma$ and let $\mathcal{A}$ and $\mathcal{B}$ be Γ-sets. Then we define

- $\Lambda^\gamma = \gamma\Lambda\gamma^{-1}$. (The *conjugate* of Λ by γ.)
- $\mathrm{Nm}(\Lambda) = \{\, \gamma \in \Gamma : \Lambda^\gamma = \Lambda \,\}$. (The *normalizer* of Λ.)

- $\Lambda \sim \Delta$ if and only if there is γ such that $\Lambda = \Delta^\gamma$.
- $\mathcal{A} \uplus \mathcal{B}$ denotes the Γ-set whose universe is the disjoint union of A and B.

We have the following relationships which the reader will find easy to verify.

Proposition 5.1. *Let Γ be a group and let $\mathcal{A}$ be a Γ-set.*

(1) *For every $\gamma \in \Gamma$ and $a \in A$, $\Gamma_{\gamma \cdot a} = (\Gamma_a)^\gamma$. In particular, $\Gamma_{\gamma \cdot a} = \Gamma_a$ if and only if $\gamma \in \mathrm{Nm}(\Gamma_a)$.*
(2) *There is a unique Γ-set map from the orbit $\Gamma \cdot a$ onto the orbit $\Gamma \cdot b$ carrying a to b if and only if $\Gamma_a \subseteq \Gamma_b$. This mapping is an isomorphism iff $\Gamma_a = \Gamma_b$.*
(3) *The orbits $\Gamma \cdot a$ and $\Gamma \cdot b$ are isomorphic if and only if $\Gamma_a \sim \Gamma_b$. (However this isomorphism does not necessarily map a to b.)*

Definition 5.2. Let Γ be a group, $\mathcal{O}$ a family of subgroups of Γ, and Λ a subgroup of Γ.

(1) Λ is called *self-normalizing* if $\mathrm{Nm}(\Lambda) = \Lambda$.
(2) Λ is *$\mathcal{O}$-irreducible* if it can not be written as a non-trivial intersection of members of $\mathcal{O}$. We write $\mathcal{O}_{\mathrm{irr}}$ for the set of $\mathcal{O}$-irreducible members of $\mathcal{O}$.
(3) Λ is *$\mathcal{O}$-maximal* if Λ is a maximal member of $\mathcal{O}$ under the usual ordering.
(4) $\Gamma/\mathcal{O}$ is the Γ-set $\bigcup\!\!\!\cdot_{i \in I} \Gamma/\Lambda_i$, where $\{ \Lambda_i : i \in I \}$ forms a set of representatives for the conjugacy classes of the subgroups in $\mathcal{O}$.
(5) Let $\mathcal{A}$ be a Γ-set. An orbit T of $\mathcal{A}$ is *solitary* if no other orbit of $\mathcal{A}$ is isomorphic to T. If T is not solitary, we call T *gregarious.*

Finally, For a Γ-set $\mathcal{A}$ we define

$$\mathcal{O}(\mathcal{A}) = \{ \Gamma_a : a \in A \};$$
$$\mathcal{O}^*(\mathcal{A}) = \{ \Gamma_a : \Gamma_a \text{ is } \mathcal{O}(A)\text{-maximal and self-normalizing, and } \Gamma \cdot a \text{ is gregarious} \}.$$

A few remarks on these definitions are in order. First, $\mathcal{O}^*(\mathcal{A})$ is well-defined. For if $\Gamma_a = \Gamma_b$ and $\Gamma \cdot a$ is gregarious, then there is some $c \in A$ with $\Gamma_c = \Gamma_a$ and $\Gamma \cdot c \neq \Gamma \cdot a$. Then either $b \neq a$ or $b \neq c$. Each of these implies that $\Gamma \cdot b$ is gregarious. Let $\mathcal{A}$ be a Γ-set, $a \in A$. The orbit $\Gamma \cdot a$ will be rigid (i.e., have no non-trivial Γ-set automorphisms) iff Γ_a is self normalizing. The stabilizer Γ_a is $\mathcal{O}(\mathcal{A})$-irreducible if and only if the corresponding orbit $\Gamma \cdot a$ can not be written as a subdirect product of other orbits of $\mathcal{A}$. Because of this, and the close connection between orbits and stabilizers, we call an orbit T irreducible if for any (equivalently, for all) $a \in T$, $\Gamma_a \in \mathcal{O}(\mathcal{A})_{\mathrm{irr}}$.

From Proposition 5.1(2) we see that an orbit $\Gamma \cdot a$ is gregarious if and only if there is a $b \in A$ such that $\Gamma_a = \Gamma_b$ but $\Gamma \cdot a \neq \Gamma \cdot b$. With regard to part (4) of the definition, observe that $\Gamma/\mathcal{O}$ will be a Γ-set consisting of pairwise non-isomorphic orbits. For each $\Lambda \in \mathcal{O}$, Γ/Λ will be isomorphic to a unique orbit in $\Gamma/\mathcal{O}$.

Now we return to the realm of arbitrary algebraic structures. Starting from any algebra $\mathbf{A}$, we can build a faithful Γ-set $\mathcal{A} = \langle A, \gamma \rangle_{\gamma \in \Gamma}$, with $\Gamma = \mathrm{Aut}(\mathbf{A})$. It is important to observe that every n-ary term operation of $\mathbf{A}$ is a Γ-set homomorphism $\mathcal{A}^n \to \mathcal{A}$. Conversely, let Γ be a group of permutations of a finite set A and $\mathcal{A} = \langle A, \gamma \rangle_{\gamma \in \Gamma}$ a finite Γ-set. Let C denote the clone of all operations on A that

preserve all members of Γ. Jónsson proved (see [16, Theorem 2.4.3]) that the algebra $\langle A, C\rangle$ will be automorphism-primal with automorphism group Γ. We shall denote this algebra $\mathcal{A}^+$, or $\mathbf{A}^+$ if $\mathcal{A}$ is built from an algebra $\mathbf{A}$. Actually, Jónsson proved more: if $\mathbf{A}$ is any algebra (finite or not), then $\mathbf{A}^+$ will be automorphism-primal.

Now let $\mathbf{A}$ be automorphism-primal. It is known that every non-empty subuniverse of an automorphism-primal algebra $\mathbf{A}$ is of the form $\mathrm{Fix}(\Lambda)$ for some $\Lambda \subseteq \Gamma = \mathrm{Aut}\,\mathbf{A}$. Recall the Galois connection between the sets Γ and A discussed earlier. We have an anti-isomorphism between the lattice of closed subsets of A—that is, all non-empty subuniverses, and possibly the empty subuniverse as well—and the lattice of closed subsets of Γ, which are the stabilizer subgroups. Note that in both lattices, the meet operation is simply intersection.

This connection yields several important relationships among the concepts discussed so far. First, for any non-empty subset X of A, $\langle X\rangle = \mathrm{Fix}(\Gamma_X)$. Thus for every $a, b \in A$,

$$\Gamma_a = \Gamma_b \iff \langle a\rangle = \langle b\rangle. \tag{5–1}$$

As we observed earlier, every member of $J(\mathrm{Sub}\,\mathbf{A})$ is 1-generated. From this it follows that for every $a \in A$

$$\Gamma_a \in \mathcal{O}(\mathcal{A})_{\mathrm{irr}} \iff \langle a\rangle \in J(\mathrm{Sub}\,\mathbf{A}) \tag{5–2}$$

since the members of $\mathcal{O}(\mathcal{A})_{\mathrm{irr}}$ are precisely the completely meet-irreducible closed subsets of Γ. The atoms of $\mathrm{Sub}\,\mathbf{A}$ correspond to the maximal members of $\mathcal{O}(\mathcal{A})$. Furthermore for every $a \in A$

(5–3) Γ_a is maximal & self-normalizing $\iff$ $\langle a\rangle$ is an atom & $\langle a\rangle \cap \Gamma\cdot a = \{a\}$.

Perhaps this last remark warrants a proof. Suppose Γ_a is maximal and self-normalizing. Maximality implies that $\langle a\rangle$ is an atom. Suppose that for some $\gamma \in \Gamma$, $\gamma\cdot a \in \langle a\rangle$. Then $\langle \gamma\cdot a\rangle = \langle a\rangle$ (since $\langle a\rangle$ is an atom). Therefore by (5–1), $\Gamma_a = \Gamma_{\gamma\cdot a} = \Gamma_a^\gamma$. Since Γ_a is self-normalizing, we must have $\gamma\cdot a = a$. Since $\gamma\cdot a$ is a typical element of $\Gamma\cdot a$, one direction of (5–3) follows. The other direction is similar.

Let us pursue this line of reasoning a bit further. Again assume that Γ_a is both maximal and self-normalizing. Suppose $\Gamma\cdot a$ is gregarious. Then there is a $b \in A$ such that $\Gamma_b = \Gamma_a$ and $b \notin \Gamma\cdot a$. Then from (5–1), $\langle a\rangle = \langle b\rangle$, so $\langle a\rangle \in \mathrm{N}(\mathbf{A})$. This proves one direction of

$$\Gamma_a \in \mathcal{O}^*(\mathcal{A}) \iff \langle a\rangle \in \mathrm{N}(\mathbf{A}) \ \&\ \langle a\rangle \cap \Gamma\cdot a = \{a\}. \tag{5–4}$$

Running the argument backwards yields the converse.

We can use these observations to understand the relationship that categorical equivalence imposes on the associated permutational algebras. From Lemma 1.5, $\mathbf{A} \equiv_{\mathrm{c}} \mathbf{B}$ implies $\mathrm{Aut}(\mathbf{A}) \cong \mathrm{Aut}(\mathbf{B})$. In this case, we may view both $\mathcal{A}$ and $\mathcal{B}$ as $\mathrm{Aut}(\mathbf{A})$-sets.

Lemma 5.3. *Let σ be a unary, invertible, idempotent term on an automorphism-primal algebra $\mathbf{A}$, and let $\mathbf{B} = \mathbf{A}(\sigma)$. Then $\mathcal{O}(\mathcal{A})_{\text{irr}} = \mathcal{O}(\mathcal{B})_{\text{irr}}$ and $\mathcal{O}^*(\mathcal{A}) = \mathcal{O}^*(\mathcal{B})$.*

Proof. Let $b \in B$. Observe that $\Gamma{\cdot}b \subseteq B$. Therefore by Lemma 1.5(4),

$$\langle b \rangle_{\mathbf{A}} \cap \Gamma{\cdot}b = \{b\} \iff \langle b \rangle_{\mathbf{B}} \cap \Gamma{\cdot}b = \{b\}.$$

(Here $\langle b \rangle_{\mathbf{A}}$ denotes the subalgebra of $\mathbf{A}$ generated by $\{b\}$.) Let Γ_a be a member of either $\mathcal{O}(\mathcal{A})_{\text{irr}}$ or $\mathcal{O}^*(\mathcal{A})$. In either case, $\langle a \rangle$ is completely join-irreducible, so there is $b \in B$ such that $\Gamma_a = \Gamma_b$. Both claims of the Lemma now follow from equivalences (5–2) and (5–4) and Lemma 1.5 parts 1–3. □

From this we discover a somewhat unexpected pair of invariants under categorical equivalence.

Theorem 5.4. *Let $\mathbf{A}$ and $\mathbf{B}$ be categorically equivalent algebras. Then $\mathcal{O}(\mathcal{A})_{\text{irr}} = \mathcal{O}(\mathcal{B})_{\text{irr}}$ and $\mathcal{O}^*(\mathcal{A}) = \mathcal{O}^*(\mathcal{B})$.*

Proof. Suppose first that $\mathbf{B} = \mathbf{A}(\sigma)$ for some invertible, idempotent term operation σ of $\mathbf{A}$. Then σ is also an invertible, idempotent term operation of $\mathbf{A}^+$, and $\mathbf{B}^+ = \mathbf{A}^+(\sigma)$. Since the underlying Γ-set structures of $\mathbf{A}^+$ and $\mathbf{B}^+$ are still $\mathcal{A}$ and $\mathcal{B}$ respectively, from Lemma 5.3 we obtain $\mathcal{O}(\mathcal{A})_{\text{irr}} = \mathcal{O}(\mathcal{B})_{\text{irr}}$ and $\mathcal{O}^*(\mathcal{A}) = \mathcal{O}^*(\mathcal{B})$.

Now suppose that for some integer k, $\mathbf{B} = \mathbf{A}^{[k]}$. Then there is an invertible, idempotent term operation σ on $\mathbf{B}$ so that $\mathbf{A} \simeq \mathbf{B}(\sigma)$. So from the previous paragraph, we derive the desired conclusion. The Theorem itself now follows from Theorem 1.3. □

We pause to present a pair of examples. These two examples are completely contrived, but do serve to illustrate the concepts introduced above.

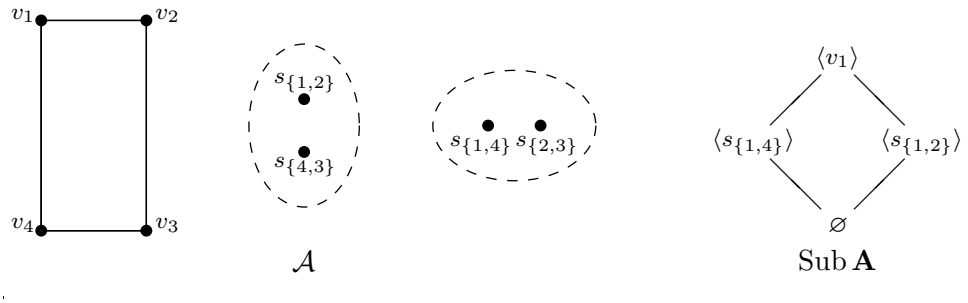

FIGURE 1

Example 5.5. Let Γ be the group of symmetries of the rectangle pictured in Figure 1. We can represent Γ as a group of permutations on $\{1, 2, 3, 4\}$ in cycle notation:

$$\Gamma = \{\, (1),\ (12)(34),\ (13)(24),\ (14)(23) \,\}.$$

Let $A = \{v_1, v_2, v_3, v_4, s_{\{1,2\}}, s_{\{4,3\}}, s_{\{1,4\}}, s_{\{2,3\}}\}$. We define an action of Γ on A by permuting the subscripts on the elements of A according to the above representation. Thus if $\gamma = (12)(34)$, then $\gamma{\cdot}v_1 = v_2$, $\gamma{\cdot}s_{\{1,2\}} = s_{\{1,2\}}$ and $\gamma{\cdot}s_{\{1,4\}} = s_{\{2,3\}}$.

(Geometrically, $s_{\{i,j\}}$ represents the side of the rectangle connecting v_i with v_j.) Let $\mathcal{A}$ denote the resulting Γ-set, and let $\mathbf{A} = \mathcal{A}^+$. Keep in mind that $\mathrm{Clo}_n(\mathbf{A}) = \mathrm{Hom}(\mathcal{A}^n, \mathcal{A})$. Figure 1 illustrates the orbits of $\mathcal{A}$.

It is easy to see that $\Gamma_{v_1} = \{(1)\} = \Gamma_{v_2}$. Consequently, equivalence (5–1) tells us that $\langle v_1 \rangle = \langle v_2 \rangle = \mathrm{Fix}(\Gamma_{v_1}) = A$. This can be verified directly: for any $x \in A$, it is not hard to find a term τ of $\mathbf{A}$ mapping v_1 to x. For example, with $x = s_{\{2,3\}}$, $\tau(v_1) = \tau(v_4) = s_{\{2,3\}}$, $\tau(v_2) = \tau(v_3) = s_{\{1,4\}}$, and $\tau(y) = y$ otherwise.

We also see that $\Gamma_{s_{\{1,4\}}} = \{(1), (14)(23)\}$ and $\Gamma_{s_{\{1,2\}}} = \{(1), (12)(34)\}$. Therefore $\Gamma_{v_1} = \Gamma_{s_{\{1,4\}}} \cap \Gamma_{s_{\{1,2\}}}$ is not $\mathcal{O}(\mathcal{A})$-irreducible. On the other hand, $\Gamma_{s_{\{1,4\}}}$ and $\Gamma_{s_{\{1,2\}}}$ are in $\mathcal{O}(\mathcal{A})_{\mathrm{irr}}$. It follows that $\langle v_1 \rangle = \langle s_{\{1,4\}} \rangle \vee \langle s_{\{1,2\}} \rangle$ in $\mathrm{Sub}\,\mathbf{A}$. The reader may find it instructive to compute these subalgebras and verify this last relationship explicitly.

Finally, since Γ is Abelian, there are no proper, self-normalizing subgroups. Since $\langle s_{\{1,2\}} \rangle$ is an atom, equivalence (5–3) tells us that $\langle s_{\{1,2\}} \rangle \cap \Gamma \cdot s_{\{1,2\}} \neq \{s_{\{1,2\}}\}$. In fact, $s_{\{3,4\}}$ lies in this intersection.

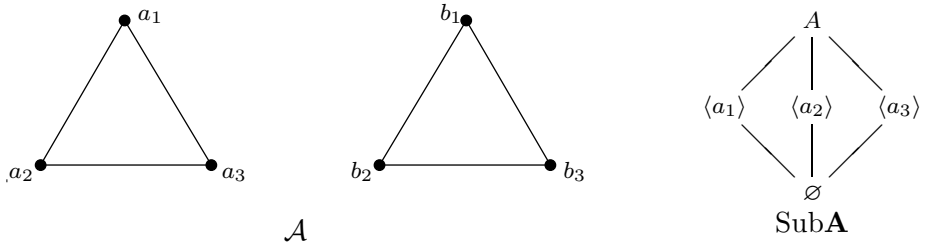

FIGURE 2

Example 5.6. Let Γ be the symmetry group of an equilateral triangle, which is the full symmetric group on $\{1, 2, 3\}$. Let A be the set $\{a_1, a_2, a_3, b_1, b_2, b_3\}$, and let Γ act by permuting the indices. Define $\mathcal{A}$ and $\mathbf{A}$ as in the previous example. (See Figure 2.)

We have $\Gamma_{a_i} = \Gamma_{b_i}$ for $i = 1, 2, 3$, and $\Gamma_{a_1} \sim \Gamma_{a_2} \sim \Gamma_{a_3}$. For example $\Gamma_{a_1} = \{(1), (23)\} = \Gamma_{b_1}$. Since this accounts for every member of $\mathcal{O}(\mathcal{A})$, we conclude that all three of these stabilizers are maximal and self-normalizing. We can verify equivalence (5–3) directly by observing that $\langle a_1 \rangle = \{a_1, b_1\}$, since there is a term that "exchanges" the two triangles, while no term can carry, say, a_1 to a_2 since they have different stabilizers. Note that in contrast to the previous example, the subalgebras cut across the orbits. Thus $\langle a_1 \rangle \cap \Gamma \cdot a_1 = \{a_1\}$. Therefore, by equivalence (5–4), $\Gamma_{a_1} \in \mathcal{O}^*(\mathcal{A})$, in other words, Γ_{a_1} is maximal and self-normalizing, as we have already observed, and $\Gamma \cdot a_1$ is gregarious—that is to say, there are two isomorphic triangles.

On the class of finite, automorphism-primal algebras, Theorem 5.4 has a converse. We prove this by first showing that the minimal sized member of the class $\mathbf{A}/\equiv_{\mathrm{c}}$ (for $\mathbf{A}$ finite and automorphism-primal) is completely determined by $\mathcal{O}(\mathcal{A})_{\mathrm{irr}}$ and $\mathcal{O}^*(\mathcal{A})$. Technically speaking, the sets $\mathcal{O}(\mathcal{A})_{\mathrm{irr}}$ and $\mathcal{O}^*(\mathcal{A})$ contain stabilizers, not orbits. This is the reason for introducing part 4 of Definition 5.2.

Theorem 5.7. *Let* $\mathbf{A}$ *be a finite automorphism-primal algebra with automorphism group* Γ*. There is an invertible, idempotent term* σ *on* $\mathbf{A}$ *such that* $\sigma(A)$ *is isomorphic as a* Γ*-set to* $\Gamma/\mathcal{O}(\mathcal{A})_{\mathrm{irr}} \uplus \Gamma/\mathcal{O}^*(\mathcal{A})$*.*

Proof. Let us define an equivalence relation on A by

$$a \approx b \iff \Gamma_a \sim \Gamma_b.$$

Observe that for any $\gamma \in \Gamma$, $\Gamma_a^\gamma = \Gamma_{\gamma\cdot a} = \Gamma_b$ iff $\gamma\cdot\langle a\rangle = \langle\gamma\cdot a\rangle = \langle b\rangle$. Thus

$$a \approx b \iff (\exists\gamma \in \Gamma)\ \ \gamma\cdot\langle a\rangle = \langle b\rangle.$$

In particular, if a and b generate either the same orbit of $\mathcal{A}$ or the same subalgebra of $\mathbf{A}$, then $a \approx b$.

Start with the set $\{\, a \in A : \langle a\rangle \in J(\mathrm{Sub}\,\mathbf{A})\,\}$. Let A_0 be a subset of this set containing one representative from each equivalence class modulo '$\approx$'. By equivalence (5–2), the mapping $a \mapsto \Gamma_a/\sim$ is a one-to-one correspondence between A_0 and $\mathcal{O}(\mathcal{A})_{\mathrm{irr}}/\sim$.

Now define

$$A_1 = \big\{\, a \in A_0 : \langle a\rangle \in \mathrm{N}(\mathbf{A})\ \ \&\ \ \langle a\rangle \cap \Gamma\cdot a = \{a\}\big\}.$$

For each $a \in A_1$, we can choose an element $a' \in A$ such that $\langle a'\rangle = \langle a\rangle$ (so $a' \approx a$) and $a' \neq a$ (consequently, $a' \notin \Gamma\cdot a$). Finally, define

$$A_1' = \{\, a' : a \in A_1\,\}.$$

By equivalence (5–4), the sets A_1' and $\mathcal{O}^*(\mathcal{A})/\sim$ are in one-one correspondence.

Claim. *No two elements of* $A_0 \cup A_1'$ *generate the same orbit.*

Proof. Let x and y be distinct elements of $A_0 \cup A_1'$. If both elements lie in A_0 then, since the elements of A_0 are pairwise inequivalent, it follows that $\Gamma\cdot x \neq \Gamma\cdot y$. Suppose $x \in A_0$ and $y \in A_1'$. Then $y = a'$ for some $a \in A_1$. If $\gamma\cdot x = y$ then $\langle a\rangle = \langle y\rangle = \gamma\cdot\langle x\rangle$ which implies that $a \approx x$, and therefore $a = x$, since $a, x \in A_0$. However, this implies that $a' = \gamma\cdot a$, a contradiction.

Lastly, suppose that $x, y \in A_1'$. Then $x = b'$, $y = a'$ and $a, b \in A_1$. If $\gamma\cdot x = y$ then $\langle a\rangle = \langle y\rangle = \gamma\cdot\langle x\rangle = \gamma\cdot\langle b\rangle$ from which it follows that $a \approx b$, so $a = b$ and therefore $y = a' = b' = x$, again, a contradiction. □

Define $B = \bigcup\{\, \Gamma\cdot a : a \in A_0 \cup A_1'\,\}$. By the Claim,

$$B = \bigdot\bigcup_{a\in A_0} \Gamma\cdot a \ \uplus\ \bigdot\bigcup_{a\in A_1'} \Gamma\cdot a,$$

(thus $\mathcal{B}$ is a sub-Γ-set of $\mathcal{A}$). By the correspondences established above, $\mathcal{B} \cong \Gamma/\mathcal{O}(\mathcal{A})_{\mathrm{irr}} \uplus \Gamma/\mathcal{O}^*(\mathcal{A})$.

Claim. *B is a separating subset of $\mathbf{A}$.*

Proof. We wish to apply Lemma 2.6. Let $T \in J(\operatorname{Sub}\mathbf{A})$. As we have observed earlier, there is $t \in A$ such that $T = \langle t\rangle$. Therefore there is (a unique) $a \in A_0$ with $t \approx a$. Consequently, for some $\gamma \in \Gamma$ we have $\langle \gamma\cdot a\rangle = \gamma\cdot\langle a\rangle = \langle t\rangle$. Thus, B contains the generator $\gamma\cdot a$ of T.

Suppose now that $T \in \mathrm{N}(\mathbf{A})$. Continuing with the notation of the previous paragraph, $\langle a\rangle = \gamma^{-1}\cdot\langle t\rangle$. Since γ is an automorphism of $\mathbf{A}$, $\langle a\rangle \in \mathrm{N}(\mathbf{A})$. There are two possibilities. If $\langle a\rangle \cap \Gamma\cdot a = \{a\}$, then $a \in A_1$ so $a' \in B$ and it follows that $\gamma\cdot a' \in T \cap B$, and $\gamma\cdot a \neq \gamma\cdot a'$. On the other hand, if there is $\delta\cdot a \in \langle a\rangle - \{a\}$, then $\gamma\delta\cdot a$ is a member of $T \cap B$ and is distinct from $\gamma\cdot a$. □

We now wish to prove the existence of a term operation σ on $\mathbf{A}$ with $\sigma(A) = B$. By the first of the two Claims, we can extend the set $A_0 \cup A_1'$ to a set C containing exactly one element from each orbit of $\mathcal{A}$. In light of the automorphism-primality of $\mathbf{A}$ and Proposition 5.1, it suffices to construct a function $f\colon C \to B$ such that $\Gamma_c \subseteq \Gamma_{f(c)}$ for every $c \in C$. Note that $C \cap B = A_0 \cup A_1'$.

For $c \in A_0 \cup A_1'$, define $f(c) = c$. Obviously, $\Gamma_c \subseteq \Gamma_{f(c)}$. Now assume that $c \notin A_0 \cup A_1'$. Since every subalgebra is a join of join-irreducibles and B is a separating set, there is a $b \in B$ such that $\langle c\rangle \supseteq \langle b\rangle$. From the order-reversing properties of the Galois connection, $\Gamma_c \subseteq \Gamma_b$. We define $f(c)$ to be this element b.

The resulting term operation σ is clearly the identity map on B, consequently it is idempotent. By the second Claim, $\sigma(A)$ is separating. Since every finite, automorphism-primal algebra is quasiprimal, we can apply Corollary 2.8 to deduce that σ is invertible. □

Since the algebra $\mathbf{A}(\sigma)$ constructed in Theorem 5.7 consists precisely of the orbits induced by $\mathcal{O}(\mathcal{A})_{\mathrm{irr}}$ and $\mathcal{O}^*(\mathcal{A})$, it is the algebra of smallest cardinality in $\mathbf{A}/\equiv_{\mathrm{c}}$. The following Theorem supplies a complete set of invariants for $\mathbf{A}/\equiv_{\mathrm{c}}$.

Theorem 5.8. *Let $\mathbf{A}$ be a finite automorphism-primal algebra and let $\mathbf{B}$ be any algebra. Then $\mathbf{A} \equiv_{\mathrm{c}} \mathbf{B}$ if and only if*

(1) *$\mathbf{B}$ is finite and automorphism-primal,*
(2) $\mathrm{Aut}(\mathbf{A}) \cong \mathrm{Aut}(\mathbf{B})$*,*
(3) $\mathcal{O}(\mathcal{A})_{\mathrm{irr}} = \mathcal{O}(\mathcal{B})_{\mathrm{irr}}$*, and*
(4) $\mathcal{O}^*(\mathcal{A}) = \mathcal{O}^*(\mathcal{B})$*.*

Proof. Conditions (3) and (4) only make sense if we view $\mathcal{A}$ and $\mathcal{B}$ as being acted upon by the same group. This is reasonable, in light of condition (2). First assume that $\mathbf{B} \equiv_{\mathrm{c}} \mathbf{A}$. Conditions 2–4 follow from Theorem 5.4 and Lemma 1.5, part 6. Condition 1 follows from Theorem 1.6.

For the converse, assume that conditions 1–4 hold. By Theorem 5.7, there are unary, invertible, idempotent term functions σ and τ on $\mathbf{A}$ and $\mathbf{B}$ respectively, such that $\sigma(A) = \Gamma/\mathcal{O}(\mathcal{A})_{\mathrm{irr}} \cup \Gamma/\mathcal{O}^*(\mathcal{A})$ and $\tau(B) = \Gamma/\mathcal{O}(\mathcal{B})_{\mathrm{irr}} \cup \Gamma/\mathcal{O}^*(\mathcal{B})$. It follows from the hypotheses that $\sigma(A)$ and $\tau(B)$ are isomorphic as Γ-sets (where $\Gamma = \mathrm{Aut}(\mathbf{A})$). Let ϕ be that isomorphism. Since $\mathbf{A}$ and $\mathbf{B}$ are automorphism-primal, so are $\mathbf{A}(\sigma)$ and $\mathbf{B}(\tau)$. Then the mapping $g \mapsto g^\phi$ is a bijection from the set $\mathcal{P}\big[\mathrm{Aut}(\mathbf{B}(\tau))\big]$ to $\mathcal{P}\big[\mathrm{Aut}(\mathbf{A}(\sigma))\big]$, where $g^\phi(x_1, \ldots, x_n) = \phi^{-1}\big(g(\phi(x_1), \ldots, \phi(x_n))\big)$. Therefore, $\mathbf{A}(\sigma)$ and $\mathbf{B}(\tau)$ are weakly isomorphic, so $\mathbf{A}$ and $\mathbf{B}$ are categorically equivalent. □

Let us reconsider the two examples discussed above, and see how the construction in Theorem 5.7 applies. In Example 5.5, there are three $\approx$-classes: the four vertices of the rectangle, the two horizontal sides, and the two vertical sides. However, the vertices do not generate join-irreducible subalgebras. Thus, we set $A_0 = \{s_{\{1,4\}}, s_{\{1,2\}}\}$. From our earlier discussion, it follows that $A_1 = A_1' = \varnothing$. The set B then turns out to be the four $s_{\{i,j\}}$ elements. There are several different terms σ that will now do the job. The term σ must be the identity on B. If we choose $\sigma(v_1) = s_{\{1,4\}}$, then we obtain $\sigma(v_2) = \sigma(v_3) = s_{\{2,3\}}$ and $\sigma(v_4) = s_{\{1,4\}}$. Thus the algebra $\mathbf{A}(\sigma)$ has cardinality 4, and will be minimal in $\mathbf{A}/\equiv_{\mathrm{c}}$.

Now recall Example 5.6 (the triangle example). All six elements are equivalent modulo '$\approx$', and all of the subalgebras are join-irreducible. So we might as well take A_0 to be $\{a_1\}$. In this case, we obtain $A_1 = A_0$ and $A_1' = \{b_1\}$. Therefore $B = A$, in other words, this algebra is already minimal. In fact it is easy to see directly that there are only 4 unary terms on $\mathbf{A}$: the identity, the map that exchanges the two triangles, and the two maps whose range is one of the two triangles. Of these, the only one that is idempotent and invertible is the identity.

We can derive one more interesting observation from Example 5.6. If we let $\mathcal{C}$ denote the sub-Γ-set of $\mathcal{A}$ consisting of just the left-hand triangle, and set $\mathbf{C} = \mathcal{C}^+$, then $\mathbf{A} \not\equiv_{\mathrm{c}} \mathbf{C}$, although they have isomorphic automorphism groups and subalgebra lattices. In fact, the only difference is $\mathcal{O}^*(\mathcal{A}) \neq \mathcal{O}^*(\mathcal{C})$. The reader might like to reproduce Example 5.6 using squares instead of triangles, to see how the analysis changes.

At the beginning of this section, we promised an easy characterization of Q-demi-primal algebras, up to categorical equivalence. In analogy with the congruence-primal, arithmetical case, we have the following.

Corollary 5.9. *Let* $\mathbf{A}$ *be a Q-demi-primal algebra, with automorphism group* Γ. *Then there is an invertible, idempotent term* σ *such that* $\sigma(A) \cong \Gamma$ *as a* Γ*-set. For any algebra* $\mathbf{B}$, $\mathbf{B} \equiv_{\mathrm{c}} \mathbf{A}$ *if and only if* $\mathbf{B}$ *is Q-demi-primal and* $\operatorname{Aut}\mathbf{B} \cong \operatorname{Aut}\mathbf{A}$.

Proof. The Q-demi-primality of $\mathbf{A}$ implies that the stabilizer of every a in A is trivial. Writing I for the trivial subgroup of $\operatorname{Aut}\mathbf{A}$, this is equivalent to $\mathcal{O}(\mathcal{A}) = \{I\}$. Therefore $\mathcal{O}(\mathcal{A})_{\mathrm{irr}} = \{I\}$ and $\mathcal{O}^*(\mathcal{A}) = \varnothing$. The two claims now follow from Theorems 5.7 and 5.8. $\square$

Example 5.10. Let us consider finite fields as algebras $\langle A, +, -, \cdot, 0, 1 \rangle$, in which, according to our convention, 0 and 1 are unary constant operations. According to Werner [29, 1.14(5)], a finite algebra $\mathbf{A}$ is automorphism-primal if and only if it is quasi-primal, every non-empty subalgebra is the set of fixed points of a group of automorphisms, and every isomorphism between non-trivial subalgebras extends to an automorphism of $\mathbf{A}$.

Let $\mathbf{A}$ be a finite field of order n. The term $d(x, y, z) = (x - y)^{n-1}(x - z) + z$ induces a discriminator operation on A, so $\mathbf{A}$ is quasi-primal. Let $\mathbf{B}$ be a non-empty subalgebra of $\mathbf{A}$. B contains both of the elements 0 and 1, so is non-trivial. If $x \in B$, $x \neq 0$, then $x^{-1} = x^{n-2} \in B$ so $\mathbf{B}$ is a subfield of $\mathbf{A}$. Now, standard results from field theory (see, for example, [13, Section V.5]), tell us that the extension $\mathbf{A}/\mathbf{B}$ is Galois. That means precisely that $B = \operatorname{Fix}(\Gamma_B)$, where $\Gamma = \operatorname{Aut}\mathbf{A}$. Also, B is the unique subfield of cardinality $|B|$. Therefore, every isomorphism from $\mathbf{B}$

to another subfield of $\mathbf{A}$ is in fact an automorphism of $\mathbf{B}$. Since $\mathrm{Aut}(\mathbf{B})$ is a cyclic group generated by the Frobenius automorphism $x \mapsto x^p$, (p the characteristic of $\mathbf{A}$), and that map extends to an automorphism of $\mathbf{A}$, we conclude that $\mathbf{A}$ is automorphism-primal.

Suppose now that $\mathbf{A}$ and $\mathbf{B}$ are fields of orders p^n and q^m respectively, where p and q are prime. Then the automorphism groups are cyclic, of orders n and m respectively. If $\mathbf{A} \equiv_{\mathrm{c}} \mathbf{B}$ then we must have $n = m$.

On the other hand, let $\Gamma = \operatorname{Aut} \mathbf{A}$. By automorphism-primality, there is a one-to-one correspondence between the subfields of $\mathbf{A}$ and the subgroups of Γ. In particular, Γ itself corresponds to the prime subfield, generated by 1. Furthermore every subfield is a simple extension of the prime subfield, in other words, every subalgebra of $\mathbf{A}$ is generated by a singleton. It follows that $\mathcal{O}(\mathcal{A}) = \operatorname{Sub} \Gamma$. Since Γ is Abelian, there are no proper self-normalizing subgroups, so $\mathcal{O}^*(\mathcal{A}) = \{\Gamma\}$. Since the same arguments obviously apply to $\mathbf{B}$, we conclude from Theorem 5.8 that if $n = m$, then $\mathbf{A} \equiv_{\mathrm{c}} \mathbf{B}$.

Notice that the fields of order 2^6 and 2^{10} have isomorphic lattices of subuniverses, but are not categorically equivalent, since their automorphism groups are different.

References

1. K.A. Baker and A.F. Pixley, *Polynomial interpolation and the Chinese remainder theorem for algebraic systems*, Math. Z. **143** (1975), 165–174.
2. J. Berman, *Congruence Lattices of Finite Universal Algebras*, Ph.D. Thesis, University of Washington, Seattle, WA, 1970.
3. G. Birkhoff and O. Frink, *Representations of lattices by sets*, Trans. Amer. Math. Soc. **64** (1948), 299–316.
4. W.J. Blok and I.M.A. Ferreirim, *Hoops and their implicational reducts*, Algebraic Methods in Logic and Computer Science, Banach Center Publications, vol. 28, Polish Academy of Sciences, Warszawa, 1993, pp. 219–230.
5. B.A. Davey and H. Werner, *Dualities and equivalences for varieties of algebras*, Contributions to Lattice Theory, Colloq. Math. Soc. János Bolyai vol. 33, North-Holland, 1983, pp. 101–275.
6. K. Denecke, *Preprimal Algebras*, Akademie-Verlag, Berlin, 1982.
7. K. Denecke and O. Lüders, *Category equivalences of clones*, preprint, October, 1992.
8. I.M.A. Ferreirim, *On varieties and quasivarieties of hoops and their reducts*, Ph.D. thesis, Univ. of Illinois at Chicago, Chicago, IL, 1992.
9. J.M. Font, A.J. Rodrigues and A. Torrens, *Wajsberg algebras*, Stochastica **8** (1984), 5–31.
10. R. Freese, *On the two kinds of probability in algebra*, Algebra Universalis **27** (1990), 70–79.
11. P. Freyd, *Algebra valued functors in general and tensor products in particular*, Coll. Math. **14** (1966), 89–106.
12. H. Gaitan, *Quasivarieties of p-algebras and Wajsberg algebras*, Ph.D. thesis, Iowa State Univ., Ames, IA.
13. T. W. Hungerford, *Algebra*, Holt, Reinhart and Winston, Inc., New York, 1974.
14. T. K. Hu, *Stone duality for primal algebra theory*, Math. Z. **110** (1969), 180–198.
15. J.R. Isbell, *Subobjects, adequacy, completeness and categories of algebras*, Rozprawy Matematyczne **36** (1964), 3–33.
16. B. Jónsson, *Topics in Universal Algebra*, Lecture Notes in Math., Vol 250, Springer-Verlag, Berlin, Heidelberg, New York, 1972.
17. K. Keimel and H. Werner, *Stone duality for varieties generated by quasiprimal algebras*, Memoirs Amer. Math. Soc. **148** (1974), 59–85.
18. R.N. McKenzie, *Algebraic version of the general Morita theorem for algebraic theories*, preprint, August, 1992.
19. R.N. McKenzie, *Finite algebras and their clones*, manuscript.

20. R.N. McKenzie, G.F. McNulty and W.F. Taylor, *Algebras, Lattices, Varieties*, vol. I, Wadsworth and Brooks/Cole, Monterey, CA, 1987.
21. V.L. Murskiĭ, *The existence of a finite basis of identities and other properties of "almost all" finite algebras*, Problemy Kibernet. **30** (1975), 43–56. (Russian)
22. A.F. Pixley, *Completeness in arithmetical varieties*, Algebra Universalis **2** (1972), 179–196.
23. A.F. Pixley, *Characterizations of arithmetical varieties*, Algebra Universalis **9** (1979), 87–98.
24. R.W. Quackenbush, *Primality: The influence of Boolean algebras in universal algebra*, Universal Algebra, Second Edition, G. Grätzer, Springer-Verlag, New York, 1979, pp. 401–416.
25. R.W. Quackenbush, *Demi-semi-primal algebras and Mal'cev type conditions*, Math. Z. **122** (1971), 166–176.
26. R.W. Quackenbush and B. Wolk, *Strong representations of congruence lattices*, Algebra Universalis **1** (1971), 165–166.
27. I.G. Rosenberg, *Über die funktionale Vollständigkeit in den mehrwertigen Logiken*, Roz. Československé Akad. Véd **80** (1970), 3–90.
28. T. Traczyk, *On the variety of bounded commutative BCK-algebras*, Math. Japonica **24** (1979), 283–292.
29. H. Werner, *Discriminator-Algebras*, Akademie-Verlag, Berlin, 1978.
30. G.C. Wraith, *Algebraic Theories*, Aarhus University Lecture Notes Series, No. 22, Aarhus University, 1970.

CB: Department of Mathematics, Iowa State University, Ames, Iowa 50011
E-mail address: cbergman@iastate.edu

JB: Department of Mathematics, Statistics, and Computer Science, University of Illinois at Chicago, 851 S. Morgan (m/c 249), Chicago, Illinois 60607–7045
E-mail address: jberman@uic.edu