Algebra Univers. (2018) 79:88

1420-8911/18/040001-15
published online November 21, 2018
https://doi.org/10.1007/s00012-018-0568-y

Algebra Universalis

CrossMark

Congruence computations in principal arithmetical varieties

Kalle Kaarli and Alden Pixley

Abstract. This paper is a continuation of the earlier paper by the same authors in which a primary result was that every arithmetical affine complete variety of finite type is a principal arithmetical variety with respect to an appropriately chosen Pixley term. The paper begins by presenting an extension of this result to all finitely generated congruences and, as an example, constructs a closed form solution formula for any finitely presented system of pairwise compatible congruences (the Chinese remainder theorem). It is also shown that in all such varieties the meet of principal congruences is also principal, and finally, if a minimal generating algebra of the variety is regular, it is shown that the variety is also regular and the join of principal congruences is again principal.

Mathematics Subject Classification. 08A30, 08A40, 08B05, 08B10.

Keywords. Principal arithmetical varieties, Affine complete varieties, Congruence computations, Chinese remainder theorem, Discriminator.

1. Introduction

The present paper is a continuation of the paper [12] in which a primary result was:

Theorem 1.1. *If $\mathcal{V}$ is an arithmetical affine complete variety of finite type, a Pixley term $p(x, y, z)$ may be selected so that $\mathcal{V}$ is a principal arithmetical variety with respect to $p(x, y, z)$, i.e.: for all algebras $\mathbf{A}$ in $\mathcal{V}$,*

$$(z, w) \in \mathrm{Cg}^{\mathbf{A}}(x, y) \iff p(x, y, z) = p(x, y, w).$$

Presented by E. Aichinger.
The research of Kalle Kaarli was partially supported by institutional research funding IUT20-57 of the Estonian Ministry of Education and Research. Work by both authors was supported by the Austrian Science Fund (FWF) P29931; Alden Pixley was a recipient of an Anthony B. Mirante Travel Grant.

Theorem 1.1 applied to the free algebra of the variety in a countable number of generators establishes a significant connection between arithmetical affine complete varieties of finite type and algebraic logic as developed primarily by W. J. Blok and D. L. Pigozzi. (See [4] for a systematic treatment of recent work in this field.) In particular Theorem 1.1 is an algebraic version of the deduction theorem for the equational logic associated with such a variety. Algebraically, it relates congruence generation to the truth of an equation in the variety. In terms of the corresponding equational logic with the majority term $m(x, y, z) = p(x, p(x, y, z), z)$, it asserts that an equation $s \approx t$ is derivable from an equation $u \approx v$ and the defining equations of the variety iff the equation $p(u, v, s) \approx p(u, v, t)$ is derivable from the equations of the variety. In this light, Theorem 3.1 may be construed to assert that an equation is derivable from each of two equations $s \approx t$ and $u \approx v$ individually iff it is derivable from $m(s, t, u) \approx m(s, t, v)$. Likewise, if the variety is regular, Theorem 3.2 describes derivability of an equation from two equations jointly.

In Section 2 we shall show how in a principal arithmetical variety the description of principal congruences can be extended to arbitrary finitely generated, i.e.: compact, congruences. We will use this to obtain a closed form solution for any finitely presented system of congruences which are pairwise compatible, i.e.: an implementation of the Chinese remainder theorem.

In Section 3 we shall show that every arithmetical affine complete variety of finite type also has the property that the meet of principal congruences is principal. Under the additional assumption of regularity, a similar result is obtained for joins of principal congruences. The proofs of these results will follow the same method which was used in [12] to prove Theorem 1.1.

In the remainder of this Introduction the necessary background, in particular terminology, is provided. The reader can find most of the same information in [11].

For a set A, we denote by $\mathbf{Eq}(A)$ the lattice of all equivalence relations on A. All sublattices $\mathbf{L} \leq \mathbf{Eq}(A)$ are *equivalences lattices on* A and those which contain 0 and 1 (the smallest and the largest equivalence relations on A) are called $(0, 1)$-*equivalence lattices on* A. An equivalence lattice on A is called *complete* if it is a complete sublattice of $\mathbf{Eq}(A)$. Thus, every complete equivalence lattice on A is a $(0, 1)$-equivalence lattice on A and in the case of finite A, complete equivalence lattices are precisely $(0, 1)$-equivalence lattices. If $\mathbf{L}$ is a complete equivalence lattice on A and $a, b \in A$, the *principal equivalence* generated by (a, b), denoted $\mathrm{Eg}^{\mathbf{L}}(a, b)$, is the meet (intersection) of all equivalences $\theta \in L$ which contain the pair (a, b). We omit the superscript $\mathbf{L}$ when the context is clear. An equivalence lattice on A is called *arithmetical* if it is distributive and permutable, i.e.: the join operation is relation product.

Recall that a *Pixley function* on a set A is a ternary function f on A such that

$$f(x, y, y) = f(x, y, x) = f(y, y, x) = x, \tag{P}$$

for all $x, y \in A$. It is well known that an equivalence lattice $\mathbf{L}$ on A is arithmetical whenever there exists an $\mathbf{L}$-compatible Pixley function on A. Moreover, in case of finite A the converse is true: for every arithmetical equivalence lattice on A there exists an $\mathbf{L}$-compatible Pixley function on A ([11]).

Now let $\mathbf{L}$ be a complete equivalence lattice on A and f be an $\mathbf{L}$-compatible Pixley function on A. It is easy to see that, given any $a, b, c, d \in A$, we have

$$f(a,b,c) = f(a,b,d) \implies (c,d) \in \mathrm{Eg}(a,b).$$

We shall call the function f a *principal Pixley function* for $\mathbf{L}$ if the converse is also true, i.e:

$$f(a,b,c) = f(a,b,d) \iff (c,d) \in \mathrm{Eg}(a,b).$$

Thus, if f is a principal Pixley function for a complete equivalence lattice $\mathbf{L}$ on A, the principal equivalence relation $\mathrm{Eg}(a,b)$ consists of all pairs (c,d) such that $f_{(a,b)}(c) = f_{(a,b)}(d)$ where $f_{(a,b)}(x)$ is the derived unary function $f(a,b,x)$. In other words, $\mathrm{Eg}(a,b)$ is the kernel of the function $f_{(a,b)}$. It is easy to see that $(f_{(a,b)}(x), x) \in \mathrm{Eg}(a,b)$ for all $a, b, x \in A$, thus, the function $f_{(a,b)}$ selects an element in every class of $\mathrm{Eg}(a,b)$. We will call any such function a *selector* for $\mathrm{Eg}(a,b)$. More generally, if $\theta \in \mathbf{L}$, an $\mathbf{L}$-compatible function $f\colon A \to A$ is a *selector* for θ if for all $x, y \in A$,

$$(x,y) \in \theta \implies f(x) = f(y) \text{ and } (f(x), x) \in \theta.$$

(Selectors appeared under the name "choice function" in [9] and [11].)

For an algebra $\mathbf{A}$ a ternary term $p(x,y,z)$ in the language of $\mathbf{A}$ is a *Pixley term* for $\mathbf{A}$ if it induces a Pixley function on A, the universe of $\mathbf{A}$. A term that is a Pixley term for all algebras of the variety $\mathcal{V}$ is called a Pixley term for $\mathcal{V}$. An algebra $\mathbf{A}$ is called:

- *arithmetical* if its congruence lattice $\mathbf{Con}(\mathbf{A})$ is an arithmetical equivalence lattice on A;
- *affine complete* if its polynomial functions are precisely its congruence compatible functions.

A variety is called *arithmetical* (*affine complete*) if all of its members are arithmetical (affine complete). It is well known that a variety admits a Pixley term iff it is arithmetical. It is also known [10] that an arithmetical variety of finite type is affine complete iff it is generated by a finite minimal algebra. Here an algebra is called *minimal* if it has no proper subalgebras.

Definition 1.2. An algebra $\mathbf{A}$ is called a *principal arithmetical algebra* if it admits a *principal Pixley term*, i.e.: a term p that induces on A a principal Pixley function for $\mathbf{Con}(\mathbf{A})$. A variety $\mathcal{V}$ is called a *principal arithmetical variety* if there is a common principal Pixley term for all algebras $\mathbf{A} \in \mathcal{V}$.

The most common examples of principal arithmetical varieties are discriminator varieties. Recall that every set A admits a "standard" Pixley function $d(x,y,z)$ called the *discriminator*, which is defined by: $d(x,y,z) = z$ if $x = y$ and $d(x,y,z) = x$ otherwise. A *discriminator term* for an algebra $\mathbf{A}$ is a ternary term t in language of $\mathbf{A}$ such that $t^{\mathbf{A}}$ is the discriminator on A. An algebra $\mathbf{A}$ admitting a discriminator term is called a *discriminator algebra*. It is easy to see that all discriminator algebras are simple. If there is a common discriminator term for all subdirectly irreducibles of a variety, this variety is called a *dicriminator variety*. It was proved by McKenzie [13] that a discriminator term for a variety $\mathcal{V}$ is also a principal Pixley term for $\mathcal{V}$.

The most important example of a discriminator variety is the variety of Boolean algebras $\mathcal{B}$ in which a discriminator term is $(x \wedge y') \vee (x \wedge z) \vee (y' \wedge z)$. Since $\mathcal{B}$ is generated by the 2-element Boolean algebra which is minimal, the variety $\mathcal{B}$ is affine complete. Note that the latter was originally established by Grätzer [6]. Thus, discriminator varieties and arithmetical affine complete varieties of finite type are two different generalizations of the variety of Boolean algebras and principal arithmetical varieties generalize both of them.

2. Finitely generated congruences

2.1. Finite joins of principal congruences

Let $\mathcal{V}$ be a principal arithmetical variety with principal Pixley term $p(x, y, z)$, $\mathbf{A} \in \mathcal{V}$ and $a, b \in A$. Then the unary polynomial function $f_{(a,b)}(x) = p(a, b, x)$ is a selector function for $\mathrm{Cg}^{\mathbf{A}}(a, b)$, the principal congruence of $\mathbf{A}$ generated by (a, b). Clearly, $\mathrm{Cg}^{\mathbf{A}}(a, b) = \mathrm{Eg}^{\mathbf{L}}(a, b)$ where $\mathbf{L} = \mathbf{Con}(\mathbf{A})$. We often drop the superscript $\mathbf{A}$ when the context is clear.

Lemma 2.1. *If ρ, σ are congruences of an algebra $\mathbf{A}$ and f and g are selectors for ρ and σ, respectively, then the composition fg is a selector for $\rho \vee \sigma$.*

Proof. We must show that for $a, b \in A$, $(a, b) \in \rho \vee \sigma \ \Rightarrow \ fg(a) = fg(b)$ and $(fg(a), a) \in \rho \vee \sigma$.

For the first condition, first note that if $a \,\rho\, b$, then $g(a) \,\rho\, g(b)$ since g is congruence compatible, so $fg(a) = fg(b)$ since f is a selector for ρ; hence fg is constant on ρ-classes. Likewise if $a \,\sigma\, b$, then $g(a) = g(b)$ since g is a selector for σ, so $fg(a) = fg(b)$ and fg is also constant on σ-classes. Thus if a/ρ and b/σ overlap, $fg(a) = fg(b)$. Since $\rho \vee \sigma$ is the union of all finite products of ρ and σ, it follows that if $(a, b) \in \rho \vee \sigma$, then there is a finite sequence of alternating ρ- and σ-classes in which adjacent classes overlap and a is in the first class and b is in the last. Therefore $fg(a) = fg(b)$.

For the second condition, given any $a \in A$, we have $(fg(a), g(a)) \in \rho$ and $(g(a), a) \in \sigma$, hence $(fg(a), a) \in \rho \vee \sigma$. □

Finally, a simple induction proves the following result.

Theorem 2.2. *If $\mathbf{A}$ is an algebra in a principal arithmetical variety with principal Pixley term p and if $\theta \in \mathbf{Con}(\mathbf{A})$ is finitely generated, i.e.: is the join of finitely many principal congruences, say*

$$\theta = \mathrm{Cg}^{\mathbf{A}}(a_1, b_1) \vee \mathrm{Cg}^{\mathbf{A}}(a_2, b_2) \vee \cdots \vee \mathrm{Cg}^{\mathbf{A}}(a_m, b_m),$$

then the nested polynomial

$$f(x) = p(a_1, b_1, p(a_2, b_2, \ldots, p(a_m, b_m, x) \ldots)) \tag{2.1}$$

is a selector for θ.

Remarks. 1. It is important to note that selector polynomial for a given congruence is not usually unique. For example, though $\mathrm{Cg}(a,b) = \mathrm{Cg}(b,a)$, it is not generally true that $f_{(a,b)} = f_{(b,a)}$ since $f_{(a,b)}(a) = p(a,b,a) = a$ while $f_{(b,a)}(a) = p(b,a,a) = b$. More generally, the composition polynomial (2.1) of Theorem 2.2 is constant on each θ congruence class, but the particular constant depends upon the order of composition.

2. It is well-known that an algebra satisfies the ascending chain condition (ACC) for congruences iff each congruence is finitely generated. Thus an algebra in a principal arithmetical variety satisfies the ACC iff all of its congruences admit polynomial selectors.

3. It is obvious from the definition that every principal arithmetical variety $\mathcal{V}$ satisfies the congruence extension property for principal congruences, that is, if $\mathbf{B} \in \mathcal{V}$, $\mathbf{A} \leq \mathbf{B}$ and $a, b \in A$ then

$$\mathrm{Cg}^{\mathbf{A}}(a,b) = \mathrm{Cg}^{\mathbf{B}}(a,b) \cap (A \times A).$$

By a result of Day [5], this implies that $\mathcal{V}$ satisfies the general congruence extension property. Since Day's proof is complicated, we present a simpler proof directly from Theorem 2.2 which applies to the special case of a principal arithmetical variety.

Let $\mathbf{A}$ and $\mathbf{B}$ be as above and $\rho \in \mathrm{Con}(\mathbf{A})$. We want to show that $\rho = \sigma \cap (A \times A)$ where $\sigma = \bigvee\{\, \mathrm{Cg}^{\mathbf{B}}(a,b) \mid (a,b) \in \rho\,\}$. Obviously, $\rho \leq \sigma$. In order to prove the converse, take $(c,d) \in \sigma \cap (A \times A)$. Since the congruence $\mathrm{Cg}^{\mathbf{B}}(c,d)$ is compact, there are finitely many pairs $(a_1,b_1),\ldots,(a_m,b_m) \in \rho$ so that

$$\mathrm{Cg}^{\mathbf{B}}(c,d) \leq \mathrm{Cg}^{\mathbf{B}}(a_1,b_1) \vee \cdots \vee \mathrm{Cg}^{\mathbf{B}}(a_m,b_m) = \phi.$$

By Theorem 2.2 the nested polynomial f given by formula (2.1) is a selector for ϕ, hence $f(c) = f(d)$. But by the same theorem, the same polynomial function f restricted to A is also a selector for

$$\theta = \mathrm{Cg}^{\mathbf{A}}(a_1,b_1) \vee \cdots \vee \mathrm{Cg}^{\mathbf{A}}(a_m,b_m).$$

Therefore, $(c,d) \in \theta \leq \rho$.

2.2. The Chinese remainder theorem

The classical Chinese remainder theorem asserts that the system of simultaneous integer congruences

$$\begin{aligned} x &\equiv a_1 \ (m_1) \\ &\cdots\cdots\cdots\cdots \\ x &\equiv a_n \ (m_n) \end{aligned} \tag{A}$$

is solvable iff $a_i \equiv a_j \ ((m_i, m_j))$ for all $1 \leq i < j \leq n$. (Here the (m_i) are principal ideals (congruences) and (m_i, m_j) denotes the greatest common divisor of m_i and m_j.) If x_0 is any solution of (A) the general solution consists of all integers x congruent to x_0 modulo $[m_1,\ldots,m_n]$, the least common multiple of $m_1,\ldots,m_n$.

Using virtually the same proof as for the ring of integers, an algebra $\mathbf{A}$ is seen to be arithmetical iff the Chinese remainder theorem holds for $\mathbf{A}$, i.e.: for every $a_1, \dots, a_n \in A$ and $\theta_1, \dots, \theta_n \in \mathrm{Con}(\mathbf{A})$, the system of congruences

$$\begin{aligned} x &\equiv a_1 \ (\theta_1) \\ &\cdots\cdots\cdots\cdots \\ x &\equiv a_n \ (\theta_n) \end{aligned} \tag{B}$$

is solvable iff $a_i \equiv a_j \quad (\theta_i \vee \theta_j)$ for all $1 \leq i < j \leq n$, i.e.: are pairwise compatible.

It follows that a variety is arithmetical iff the Chinese remainder theorem holds for all of its members.

Now let us address the solvability of a system (B) in case $\mathcal{V}$ is a principal arithmetical variety with a principal Pixley term which for our purposes we imagine to be computable. We suppose the system is finitely presented, meaning that for some fixed integer m each θ_i is the join of at most m principal congruences:

$$\theta_i = \mathrm{Cg}(a_{i1}, b_{i1}) \vee \cdots \vee \mathrm{Cg}(a_{im}, b_{im}). \tag{2.2}$$

In this case we can construct selector polynomials $g_i(z)$ for each θ_i as prescribed by Theorem 2.2. Hence the system (B) is pairwise solvable iff

$$\text{for all } \ 1 \leq i < j \leq n, \ \ g_i(g_j(a_i)) = g_i(g_j(a_j)) \tag{C}$$

which can be effectively tested, assuming the computability of $p(x, y, z)$. If the conditions (C) all test positive, then actual pairwise solutions s_{ij} are computed by

$$p(g_i(a_i), g_i(g_j(a_j)), g_j(a_j)) = p(g_i(a_i), g_i(g_j(a_i)), g_j(a_j)). \tag{S}$$

This is because the two sides of (S) are equal by (C) and its left (right) side is congruent to a_i modulo θ_i (a_j modulo θ_j).

The computation of a solution of the system (B) from the pairwise solution which we shall describe is due to A.P. Huhn. The result was contained in his preprint "Weakly distributive lattices" which became available in 1972. It was published only in 1983 [8]. Specifically, as is well known, $m(x, y, z) = p(x, p(x, y, z), z)$ is a majority term for $\mathcal{V}$, i.e.: m satisfies the identities: $m(x, x, y) = m(x, y, x) = m(y, x, x) = x$. Thus, for example, if each of s_{12}, s_{13}, s_{23} solves the indicated two congruences of the first three of (B) then we can compute $s = m(s_{12}, s_{13}, s_{23})$ which clearly solves all three. More generally, we proceed by induction. For $n > 3$, denote by (B_i) the system of congruences obtained from (B) by removing the i-th congruence, $i = 1, 2, 3$. By induction, let s_1, s_2, s_3 be solutions which have been computed for $(\mathrm{B}_1), (\mathrm{B}_2), (\mathrm{B}_3)$, respectively. Then it is easy to see that $s = m(s_1, s_2, s_3)$ is a solution for (B).

Note that by Theorem 2.2 the polynomials g_i are obtained in a uniform way from the same $(2m + 1)$-ary terms composed only from p, regardless the choice of algebra $\mathbf{A}$ in $\mathcal{V}$. Moreover, by the discussion above, there is a $(2m+n)$-ary term t whose value after replacing its variables by a_{ij}, b_{ij} and a_i, $1 \leq i \leq n$, $1 \leq j \leq m$, is a solution of (B). Thus we have the following theorem.

Theorem 2.3. *Let $\mathcal{V}$ be a principal arithmetical variety with principal Pixley term p. Then there are $(2m+1)$-ary terms*

$$t_i(x_{i1}, y_{i1}, \ldots, x_{im}, y_{im}, z), \quad 1 \leq i \leq n$$

and a $(2m+n)$-ary term

$$t(x_{i1}, y_{i1}, \ldots, x_{im}, y_{im}, z_1, \ldots, z_n)$$

such that for any algebra $\mathbf{A} \in \mathcal{V}$, any system (B) over $\mathbf{A}$ with congruences θ_i as in (2.2) is solvable if and only if

$$g_i(g_j(a_i)) = g_i(g_j(a_j)), \quad 1 \leq i < j \leq n$$

where

$$g_i(z) = t_i(a_{i1}, b_{i1}, \ldots, a_{im}, b_{im}, z), \quad 1 \leq i \leq n.$$

If these conditions are satisfied then a solution of (B) is

$$c = t(a_{i1}, b_{i1}, \ldots, a_{im}, b_{im}, a_1, \ldots, a_n).$$

It is interesting to compare the solution above with the case of integer congruences (A): again we first solve the congruences two at a time and then use distributivity ($\mathbb{Z}$ is an arithmetical ring) to solve all. For two congruences, say the first and second, recall that by the Euclidean Algorithm, $m = (m_1, m_2)$ is expressible as $m = m_1 u + m_2 v$ for some integers u and v and since m divides $a_1 - a_2$, we have $a_1 - a_2 = m_1 uk + m_2 vk$ for some k; hence

$$a_1 - m_1 uk = a_2 + m_2 vk$$

and the left side of this equality is congruent to a_1 modulo m_1 and the right side is congruent to a_2 modulo m_2. This is analogous to the pairwise solutions presented in the proof of Theorem 2.3. Again we use induction and distributivity of the congruence lattice to complete the solution but we no longer have a majority term available to obtain a closed form solution.

3. The lattice of compact congruences

3.1. Summary and background

Throughout this section we will deal exclusively with an arithmetical affine complete variety $\mathcal{V}$ of finite type, that is, an arithmetical variety of finite type which is generated by a finite minimal algebra $\mathbf{A}$. We will prove the following two theorems.

Theorem 3.1. *Let $p(x, y, z)$ be any principal Pixley term for $\mathcal{V}$ and m be the majority term given by $m(x, y, z) = p(x, p(x, y, z), z)$. Then in all algebras of $\mathcal{V}$ the meet of principal congruences is given by the formula*

$$\mathrm{Cg}(a, b) \wedge \mathrm{Cg}(c, d) = \mathrm{Cg}(m(a, b, c), m(a, b, d)). \tag{M}$$

Theorem 3.2. *If the minimal algebra $\mathbf{A}$ generating $\mathcal{V}$ is regular, then there exists a principal Pixley term $p(x, y, z)$ for $\mathcal{V}$ such that for all algebras in $\mathcal{V}$ the join of principal congruences is given by the formula*

$$\mathrm{Cg}(a, b) \vee \mathrm{Cg}(c, d) = \mathrm{Cg}(p(a, b, c), p(b, a, d)). \tag{J}$$

Recall that an equivalence lattice $\mathbf{L}$ on a set A is called *regular* if for any $\theta, \phi \in L$ and an element $a \in A$, $a/\theta = a/\phi$ implies $\theta = \phi$. An algebra is *regular* if $\mathbf{Con}(\mathbf{A})$ if a regular equivalence lattice on A. A variety is called *regular*, if all of its members are regular.

Remarks. 1. We will soon see (Lemma 3.6) that if $\mathcal{V}$ is not regular, then the formula (J) no longer holds. This is not to say that in the absence of regularity some other formula might not be available.

2. Motivation for the formula (M) was provided by Baker [1]. In that paper elements $m(a, b, c)$, $m(a, b, d)$ satisfying (M) were called *principal intersection polynomials* and were illustrated for the variety of distributive lattices by the lattice median $m(x, y, z) = (x \vee y) \wedge (x \vee z) \wedge (y \vee z)$.

In general, the majority term $m(x, y, z) = p(x, p(x, y, z), z)$ in the statement of Theorem 3.1 cannot be replaced by some arbitrary majority term. For example let $\mathbf{A}$ be a simple algebra with the universe $A = \{a, b, c, d\}$, generating an arithmetical variety, for example a discriminator algebra, with an additional majority operation $m(x, y, z)$ such that $m(x, y, z) = d$ if x, y, z are all different. Then obviously

$$\mathrm{Cg}(a, b) \wedge \mathrm{Cg}(c, d) \neq \mathrm{Cg}(m(a, b, c), m(a, b, d)),$$

so (M) fails.

Early appearance of formula (J) is less clear but the paper [2] does obtain both (M) and (J) for finitely generated discriminator varieties (which are already known to be regular).

3. Note the reversal of a, b in (J). It is interesting [2] that for discriminator varieties, if $\mathrm{Cg}(a, b) \leq \mathrm{Cg}(c, d)$ then $\mathrm{Cg}(p(a, b, c), p(a, b, d))$ (p the discriminator term) is a relative complement of $\mathrm{Cg}(a, b)$ in the interval $[0, \mathrm{Cg}(c, d)]$. This, of course, is not generally applicable in the present context.

4. Theorems 3.1 and 3.2 together show that if $\mathcal{V}$ is regular, the principal (=compact) congruences of any algebra $\mathbf{A}$ in $\mathcal{V}$ form a sublattice of $\mathbf{Con}(\mathbf{A})$.

5. Assuming that p is computable, Theorem 2.2 and Theorem 3.2 provide two different ways for effectively determining membership in a finitely generated congruence, i.e.: determining if

$$(x, y) \in \mathrm{Cg}(a_1, b_1) \vee \cdots \vee \mathrm{Cg}(a_m, b_m),$$

both by repeatedly composing p with itself. Is one more efficient than the other? In fact it is easy to count the number of evaluations of p required and to see that in each case, perhaps surprisingly, exactly $2m$ evaluations are required.

6. Notice that in applying Theorem 3.2 to compute a single generating pair for the join of several principal congruences, different arrangements of the constituent principal congruences generally produce different generating pairs.

3.2. Proofs of Theorems 3.1 and 3.2

Proof of Theorem 3.1. Since our majority function $m(x, y, z)$ is compatible, the inequality

$$\mathrm{Cg}(m(x, y, u), m(x, y, v)) \leq \mathrm{Cg}(x, y) \wedge \mathrm{Cg}(u, v)$$

is trivial, so to prove (M), we only need to prove

$$\mathrm{Cg}(x,y) \wedge \mathrm{Cg}(u,v) \leq \mathrm{Cg}(m(x,y,u), m(x,y,v)). \tag{3.1}$$

Since $\mathcal{V}$ is principal with respect to the term $p(x,y,z)$, this is equivalent to

$$\begin{aligned} &\forall x,y,u,v,z,w,\\ &[p(x,y,z) = p(x,y,w) \& p(u,v,z) = p(u,v,w)]\\ &\Longrightarrow p(m(x,y,u), m(x,y,v), z) = p(m(x,y,u), m(x,y,v), w). \end{aligned} \tag{3.2}$$

It is easy to verify directly that if (3.2) is true on each of the factors of a subdirect product then it is true on the subdirect product. (More generally, (3.2) is a *special Horn sentence*; in fact it is a *quasi-identity*; such sentences are preserved under the formation of subdirect products.) Thus, it is sufficient to prove that the formula (M) holds in all subdirectly irreducible members of $\mathcal{V}$. However, by congruence distributivity of $\mathcal{V}$ and the minimality of $\mathbf{A}$, all subdirectly irreducible algebras of $\mathcal{V}$ are contained in $H(\mathbf{A})$. Hence, it is sufficient to prove that (M) (equivalently either of (3.1) or (3.2)) holds in all homomorphic images $\mathbf{B}$ of $\mathbf{A}$.

We proceed by induction on the height n of $\mathbf{Con}(\mathbf{B})$. If $n = 1$, then $\mathbf{B}$ is simple. So, since the term p is principal, it must be the discriminator and (3.2) follows by considering the cases $x = y,\ x \neq y$.

Suppose all homomorphic images of $\mathbf{A}$ with height less than n satisfy (3.2) and let $\mathbf{B}$ be isomorphic to $\mathbf{A}/\rho$ where $\rho \in \mathrm{Con}(\mathbf{A})$.

Case 1. ρ is not meet irreducible. In this case $\mathbf{B}$ is isomorphic to a subdirect product of algebras $\mathbf{C} \in H(\mathbf{A})$ with the height of $\mathbf{Con}(\mathbf{C})$ less than n. By the induction hypothesis, all these $\mathbf{C}$ satisfy (3.2) but then (3.2) is also true for $\mathbf{B}$.

Case 2. ρ is meet irreducible. In this case $\mathbf{B}$ is subdirectly irreducible; let μ be its monolith congruence. We verify (3.1) for $\mathbf{B}$. Let $x,y,u,v \in B$. Since μ covers 0, either

(a) $\mu \leq \mathrm{Cg}(x,y) \wedge \mathrm{Cg}(u,v)$ or (b) $0 = \mathrm{Cg}(x,y) \wedge \mathrm{Cg}(u,v)$.

In case (a), since μ is the monolith, both $\mu \leq \mathrm{Cg}(x,y)$ and $\mu \leq \mathrm{Cg}(u,v)$, so both $\mathrm{Cg}(x,y)/\mu = \mathrm{Cg}(x/\mu, y/\mu)$ and $\mathrm{Cg}(u,v)/\mu = \mathrm{Cg}(u/\mu, v/\mu)$ are defined. By the induction hypothesis, in $\mathbf{Con}(\mathbf{B}/\mu)$

$$0 \leq \mathrm{Cg}(x/\mu, y/\mu) \wedge \mathrm{Cg}(u/\mu, v/\mu) \leq \mathrm{Cg}(m(x/\mu, y/\mu, u/\mu), m(x/\mu, y/\mu, v/\mu))$$

from which follows

$$0 \leq (\mathrm{Cg}(x,y) \wedge \mathrm{Cg}(u,v))/\mu \leq \mathrm{Cg}(m(x,y,u), m(x,y,v))/\mu$$

in $\mathbf{Con}(\mathbf{B}/\mu)$, so in $\mathbf{Con}(\mathbf{B})$

$$\mu \leq \mathrm{Cg}(x,y) \wedge \mathrm{Cg}(u,v) \leq \mathrm{Cg}(m(x,y,u), m(x,y,v)),$$

which proves (3.1). In case (b), (3.1) is obvious. □

In order to prove Theorem 3.2, we need some background information and auxiliary results. If an algebra is regular then clearly only its zero congruence can have a singleton class. In what follows we will call this the NSC (no singleton classes) property. Surprisingly, we could not find in the literature an example showing that the NSC is strictly weaker than regularity. Therefore we present such an example here.

Example. A finite nonregular arithmetical algebra satisfying the NSC. Let $A = \{1, 2, 3, 4, 5, 6\}$ and let $\mathbf{L}$ be an equivalence lattice on A consisting of 0_A, σ, ρ and 1_A where σ has classes $\{1, 2\}$, $\{3, 4\}$, $\{5, 6\}$ and ρ has classes $\{1, 2\}$, $\{3, 4, 5, 6\}$. Since $\mathbf{L}$ is distributive, by a well known theorem of Quackenbush and Wolk [14], $\mathbf{L}$ is the congruence lattice of the algebra $\mathbf{A} = (A, F)$ where F is the clone of all $\mathbf{L}$-compatible functions on A. Obviously this algebra satisfies the NSC but is not regular.

At the level of varieties, however, the property NSC and regularity are known to be equivalent, i.e.: all members of a variety $\mathcal{V}$ are regular if and only if all members of $\mathcal{V}$ satisfy the NSC (Thurston [15]). The same proof of this fact can also be found in [3], and actually, in both cases, the proof only requires that all homomorphic images of a generating algebra satisfy the NSC. Hence we have the following stronger result.

Lemma 3.3. *An algebra is regular if and only if all of its homomorphic images satisfy the NSC.*

The next result was proved by Grätzer [7].

Lemma 3.4. *A variety is regular if and only if the free algebra in 3 generators of the variety is regular.*

Lemma 3.5. *Let* $\mathbf{A}$ *be a finite minimal regular algebra generating an arithmetical variety* $\mathcal{V}$*. Then* $\mathcal{V}$ *is regular.*

Remark. Lemma 3.5 is quite strong in that only the regularity of any finite minimal generator $\mathbf{A}$ is required to infer the regularity of $\mathcal{V}$; such an algebra may be considerably smaller than the free algebra in 3 generators generally required by Lemma 3.4. Moreover, it is clear from the proof of Lemma 3.5 below, that all that is actually needed is that $\mathbf{A}$ satisfy the following condition: for each meet irreducible congruence θ of $\mathbf{A}$, if μ is the unique cover of θ, then no μ-class consists of a single θ-class. This is just the NSC condition, and in this special form is easy to verify in particular cases.

Proof. We want to prove that all members of $\mathcal{V}$ are regular. Since $\mathbf{A}$ is finite, by Lemma 3.4 it suffices to show that every finite algebra $\mathbf{S} \in \mathcal{V}$ is regular and by Lemma 3.3 it is enough to prove that all finite algebras $\mathbf{S} \in \mathcal{V}$ satisfy the NSC. Let $\mathbf{S}$ be subdirect in $\mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ where $\mathbf{A}_i$ are subdirectly irreducible. We may assume that this representation is not redundant, i.e.: $\mathbf{S}$ is not a subdirect product of fewer than n of the $\mathbf{A}_i$. Since $\mathcal{V}$ is congruence distributive and $\mathbf{A}$ is minimal, $\mathcal{V} = P_S H(\mathbf{A})$, in particular, all $\mathbf{A}_i$ are just homomorphic images of $\mathbf{A}$; thus they all are regular by Lemma 3.3.

Let $a = (a_1, \ldots, a_n)$ be any element of S and θ be any non-zero congruence of $\mathbf{S}$. We have to show that $| a/\theta |> 1$. By congruence distributivity, $\theta = (\theta_1 \times \cdots \times \theta_n) |_S$, for congruences θ_i of $\mathbf{A}_i$. This means: for $x, y \in S$, $(x, y) \in \theta$ iff for each $1 \leq i \leq n$, $(x_i, y_i) \in \theta_i$. Since $\theta \neq 0$, at least one θ_i is not zero. Without loss of generality, let $\theta_1 \neq 0$.

For $i < j$, let $\mathbf{S}_{ij}$ be the projection of $\mathbf{S}$ in $\mathbf{A}_i \times \mathbf{A}_j$. Our particular interest is in projections $\mathbf{S}_{1i}$, $1 < i$. By congruence permutability there exist congruences α_i, β_i in $\mathrm{Con}(\mathbf{A}_1), \mathrm{Con}(\mathbf{A}_i)$, respectively, and an isomorphism $g_i \colon \mathbf{A}_1/\alpha_i \to \mathbf{A}_i/\beta_i$, such that $(s_1, s_i) \in S_{1i}$ if and only if $g_i(s_1/\alpha_i) = s_i/\beta_i$ (cf. Theorem 1.2.14 of [11]). Then $s_1/\alpha_i \times s_i/\beta_i = (s_1, s_i)/(\alpha_i \times \beta_i)$ is a component block of S_{1i} and S_{1i} is the disjoint union of all such blocks. Note that neither α_i nor β_i can be zero, for otherwise one of $\mathbf{A}_1$ and $\mathbf{A}_i$ would be a homomorphic image of the other, and hence would be a redundant factor.

By our assumption, the monolith congruence μ_1 of $\mathbf{A}_1$ has no singleton class. Thus, there exists $b_1 \in a_1/\mu_1$ such that $b_1 \neq a_1$. Since $\mu_1 \leq \alpha_2 \cap \cdots \cap \alpha_n$, we have $a_1/\alpha_i = b_1/\alpha_i$, hence,

$$(b_1, a_i) \in S_{1i}, \quad i = 2, \ldots, n.$$

Therefore, for each $i < j$, the projection of $b = (b_1, a_2, \ldots, a_n)$ into $A_i \times A_j$ is in S_{ij}. Since $\mathcal{V}$ has a majority term, S is uniquely determined by the S_{ij} ([11], page 133), so $b \in S$. Moreover, $(b_1, a_1) \in \mu_1 \leq \theta_1$ implies $b \in a/\theta$. □

The next lemma gives two characterizations of condition (J) that will be useful in the proof of Theorem 3.2.

Lemma 3.6. *Let* $\mathbf{L}$ *be a complete arithmetical equivalence lattice on a set* A *and let* $f(x, y, z)$ *be a principal Pixley function on* A *for* $\mathbf{L}$. *Let* $a, b, c, d \in A$. *Then the following are equivalent:*

(1) $\mathrm{Eg}(a, b) \vee \mathrm{Eg}(c, d) = \mathrm{Eg}(f(a, b, c), f(b, a, d))$;
(2) $f(f(a, b, c), f(b, a, d), a) = f(f(a, b, c), f(b, a, d), b)$;
(3) $\mathrm{Eg}(a, b) \leq \mathrm{Eg}(f(a, b, c), f(b, a, d))$.

Moreover, each of these equivalent conditions implies regularity of $\mathbf{L}$.

Proof. (1) ⇒ (2). Since $(a, b) \in \mathrm{Eg}(a, b) \vee \mathrm{Eg}(c, d)$, the equality (2) follows from (1) just by the definition of a principal Pixley function.

(2) ⇒ (3). Assume that (2) holds and $f(a, b, c) \equiv f(b, a, d)$ (ρ). Then $a \equiv b$ (ρ) follows from the definition of a Pixley function and the compatibility of f with ρ.

(3) ⇒ (1). Clearly, $\mathrm{Eg}(a, b) \vee \mathrm{Eg}(c, d) \geq \mathrm{Eg}(f(a, b, c), f(b, a, d))$ is trivially true. To prove the reverse inequality, put $\rho = \mathrm{Eg}(f(a, b, c), f(b, a, d))$. Then, by (3), $a \equiv b$ (ρ) and therefore

$$\begin{aligned} c/\rho &= f(a/\rho, a/\rho, c/\rho) = f(a/\rho, b/\rho, c/\rho) = f(a, b, c)/\rho = f(b, a, d)/\rho \\ &= f(b/\rho, a/\rho, d/\rho) = f(a/\rho, a/\rho, d/\rho) = d/\rho\,, \end{aligned}$$

thus $c \equiv d$ (ρ). We have proved that $(a, b), (c, d) \in \rho$; therefore $\mathrm{Eg}(a, b) \vee \mathrm{Eg}(c, d) \leq \rho$.

Now assume that any of the conditions (1)–(3) is satisfied. Let $c \in A$, $\rho, \sigma \in L$ and $c/\rho = c/\sigma$. Then, without loss of generality, $\rho \leq \sigma$. Assume that $\rho < \sigma$ and pick a pair $(a, b) \in \sigma \backslash \rho$. Then $f(a, b, c) \in c/\sigma = c/\rho$ and similarly $f(b, a, c) \in c/\sigma = c/\rho$. Hence, $f(a, b, c) \equiv f(b, a, c)$ (ρ) but $a \not\equiv b$ (ρ) which contradicts the third condition of the lemma. Therefore $\rho = \sigma$, so $\mathbf{L}$ is regular. □

Now we are ready to complete the proof of Theorem 3.2. As will be apparent below, the proof of Theorem 3.2 is much more complicated than that of Theorem 3.1. This is because in Theorem 3.1 we were able to show that for *any* given principal Pixley term, the corresponding majority term yields formula (M). The proof of Theorem 3.2, on the other hand, requires the construction of a new principal Pixley function, using the added hypothesis of regularity, to satisfy condition (J). This will require revisiting the proofs of Theorem 1.1 (Theorem 3.2 of [12]) and of Theorem 2.2.6 of [11]. We shall assume the reader's familiarity with both of these.

Proof of Theorem 3.2. By Lemma 3.5 we may assume that $\mathbf{A}$ is the largest minimal algebra of $\mathcal{V}$. Let $\mathbf{L} = \mathbf{Con}(\mathbf{A})$. In the sequel we say that $\sigma \in \mathbf{L}$ is of height m if $m = \mathrm{height}(\mathbf{Con}(\mathbf{A}/\sigma))$; thus the maximal congruences of $\mathbf{A}$ have height 1. Our aim is to prove by induction on m the following statement (S_m):

> *There exists a system of functions* $\{\, f_\sigma \mid \sigma \in L, \mathrm{height}(\sigma) \leq m \,\}$ *such that every* f_σ *is a principal Pixley function on* A/σ *satisfying (J) for the algebra* $\mathbf{A}/\sigma$ *and the system is compatible in the sense that each of the functions induces on every previous level the functions belonging to our function system.*

For proving (S_1), as in the proof of Theorem 2.2.6, we define f_σ to be the discriminator function on A/σ for all $\sigma \in L$ of height 1, that is, for maximal congruences σ of $\mathbf{A}$. We know that all these functions satisfy (J).

Proceeding with the induction step, we assume that (S_{m-1}), $m \geq 2$, holds and show how to define the functions f_ρ for the next level (i.e.: for $\rho \in L$ of height m) so that the system $\{\, f_\sigma \mid \sigma \in L, \mathrm{height}(\sigma) \leq m \,\}$ will satisfy (S_m).

Suppose first that ρ has more than one cover in $\mathbf{L}$. Then, as shown in the proof of Theorem 2.2.6, f_ρ is uniquely determined by the functions f_σ with $\rho < \sigma$. Moreover, since condition (J) is equivalent to the equation (2) in Lemma 3.6, f_ρ satisfies this condition because so do all f_σ with $\rho < \sigma$.

Next suppose that ρ has only one cover in $\mathbf{L}$, let it be μ. Without loss of generality let $\rho = 0$; thus $a/\rho = a$ for every $a \in A$ and $f_\rho = f$. Revisiting the proof of Theorem 2.2.6, we recall that any function f satisfying the following three conditions is a principal Pixley function for $\mathbf{L}$: for all $u, v, x \in A$, (i) $f(u,u,x) = x$; (ii) if $u \neq v$ and $x \equiv u$ $(\mathrm{Eg}^{\mathbf{L}}(u,v))$ then $f(u,v,x) = u$; (iii) if $u \neq v$ and $x \not\equiv u$ $(\mathrm{Eg}^{\mathbf{L}}(u,v))$ then $f(u,v,x)$ is any fixed element in $f_\mu(u/\mu, v/\mu, x/\mu)$ (not depending of the choice of x in its μ-class). Note that the third condition provides some freedom for constructing f. We shall use this freedom to construct an f which satisfies condition (J).

Since f is a principal Pixley function for $\mathbf{L}$, the derived unary functions $f(u,v,x)$ and $f(v,u,x)$ are selectors for $\mathrm{Eg}(u,v)$, for any fixed $u, v \in A$. We now prove that f can be defined so that, whenever $u \neq v$, these two functions agree at no element $a \in A$, i.e.:

$$u \neq v \implies f(u,v,a) \neq f(v,u,a). \tag{3.3}$$

Indeed, if condition (ii) applies this is obvious while if (iii) applies, $f(u,v,a)$ can be any fixed element $b \in f_\mu(u/\mu, v/\mu, a/\mu)$ and $f(v,u,a)$ can be any fixed element $c \in f_\mu(v/\mu, u/\mu, a/\mu)$. Regularity insures that these choices, with $b \neq c$ can always be made, even if $f_\mu(u/\mu, v/\mu, a/\mu) = f_\mu(v/\mu, u/\mu, a/\mu)$. Thus $f(u, v, a) \neq f(v, u, a)$ as required.

Now we show that the function f defined as above satisfies condition (3) of Lemma 3.6, hence it satisfies the condition (J), as well. Let $a, b, c, d \in A$, and $\sigma = \mathrm{Eg}(f(a, b, c), f(b, a, d))$. We must prove $a \equiv b\ (\sigma)$. Let first $\sigma = 0$. Then $f(a, b, c) = f(b, a, d)$ which implies $c \equiv d\ (\mathrm{Eg}(a, b))$ because f is a Pixley function. Since, $f(b, a, x)$ is a selector function for $\mathrm{Eg}(a, b)$, we now have $f(b, a, d) = f(b, a, c)$ but then also $f(a, b, c) = f(b, a, c)$, so $a = b$ by (3.3).

Now let $\sigma \neq 0$, hence $\mu \leq \sigma$ and $f(a, b, c) \equiv f(b, a, d)\ (\sigma)$ implies

$$f_\mu(a/\mu, b/\mu, c/\mu) \equiv f(b/\mu, a/\mu, d/\mu)\ (\sigma/\mu).$$

Then, by our induction hypothesis, $a/\mu \equiv b/\mu\ (\sigma/\mu)$ which clearly implies $a \equiv b\ (\sigma)$. Hence, f satisfies condition (3) and therefore also condition (J).

Thus, we have an **L**-compatible principal Pixley function f on A which satisfies (J). Since **A** is affine complete and minimal, there exists a 4-ary term t and an element $a \in A$ such that $f(x, y, z) = t(x, y, z, a)$ for all $x, y, z \in A$. By Lemma 2.1 of [12] there exists a unary term $s(x)$ such that $s(A)$ is contained in a single orbit of $\mathbf{Aut}(\mathbf{A})$ and then by the proof of Theorem 1.1, $p(x, y, z) = t(x, y, z, s(x))$ is a principal Pixley term for $\mathcal{V}$. It remains to prove that $p(x, y, z)$ satisfies condition (J).

Consider the terms

$$u(x_1, x_2, x_3, x_4, y) = t(t(x_1, x_2, x_3, y), t(x_2, x_1, x_4, y), x_1, y)$$

and

$$v(x_1, x_2, x_3, x_4, y) = t(t(x_1, x_2, x_3, y), t(x_2, x_1, x_4, y), x_2, y).$$

Since the function f satisfies equation (2) from Lemma 3.6, by the choice of the term t, we have:

$$u(x_1, x_2, x_3, x_4, a) = v(x_1, x_2, x_3, x_4, a),$$

for all $x_1, x_2, x_3, x_4 \in A$. Thus, by Lemma 2.2 of [12] the identity

$$u(x_1, x_2, x_3, x_4, s(x)) = v(x_1, x_2, x_3, x_4, s(x))$$

holds in **A**, hence also in $\mathcal{V}$. But this is exactly what we need: the term $p(x, y, z)$ satisfies condition (J). □

4. Conclusion

The proofs of both Theorems 1.1 and 3.2 make use of the same method. In each case we work with the largest minimal algebra **A** in the variety and construct a $\mathbf{Con}(\mathbf{A})$-compatible Pixley function f which, in addition to satisfying the identity (P), also satisfies other identities which characterize properties of particular interest. In the case of Theorem 1.1 the property is that of being a principal arithmetical variety, which is characterized by the identities (one for each basic operation g of **A**),

$$f(u, v, g(x_1, \ldots, x_m)) = f(u, v, g(f(u, v, x_1), \ldots, f(u, v, x_m))) \tag{4.1}$$

from Theorem 1.2.6 of [11]. Since **A** is minimal and affine complete, for any $a \in A$, f is a polynomial $t(u, v, x, a)$ for some term function $t(u, v, x, z)$. Since **A** is necessarily weakly diagonal, for an appropriate unary term $s(x)$, the term function $f(u, v, x, s(u))$ satisfies (4.1) as well as (P); hence the variety is a principal arithmetical variety.

The same strategy was used in proving Theorem 3.2, except that the function f, in addition to satisfying (P) and (4.1), was constructed to satisfy the identity (2) of Lemma 3.6 as well.

It seems likely that this strategy can be further developed and used to discover when other interesting properties of arithmetical affine complete varieties occur.

References

[1] Baker, K.A.: Primitive satisfaction and equational problems for lattices and other algebras. Trans. Am. Math. Soc. **190**, 125–150 (1974)

[2] Bulman-Fleming, S., Werner, H.: Equational compactness in quasi-primal varieties. Algebra Univers. **7**, 33–46 (1977)

[3] Chajda, I., Eigenthaler, G., Länger, H.: Congruence Classes in Universal Algebra, Research and Exposition in Mathematics, 26. Heldermann, Lemgo (2003)

[4] Czelakowski, J.: Protoalgebraic logics, Trends in Logic-Studia Logica Library, 10. Kluwer Academic Publishers, Dordrecht (2001)

[5] Day, A.: A note on the congruence extension property. Algebra Univers. **1**, 234–235 (1971)

[6] Grätzer, G.: On Boolean functions (notes on lattice theory II). Rev. Math. Pures Appl. (Bucarest) **7**, 693–697 (1962)

[7] Grätzer, G.: Two Mal'cev type theorems in universal algebra. J. Comb. Theory **8**, 334–342 (1970)

[8] Huhn, A.P.: Schwach distributive Verbände, II. Acta Sci. Math. (Szeged) **46**, 85–98 (1983)

[9] Kaarli, K.: A new characterization of arithmetical equivalence lattices. Algebra Univers. **45**, 345–347 (2001)

[10] Kaarli, K., Pixley, A.: Affine complete varieties. Algebra Univers. **24**, 74–90 (1987)

[11] Kaarli, K., Pixley, A.: Polynomial Completeness in Algebraic Systems. CRC Press, Boca Raton (2000)

[12] Kaarli, K., Pixley, A.: Weakly diagonal algebras and definable principal congruences. Algebra Univers. **55**, 203–212 (2006)

[13] McKenzie, R.M.: On spectra, and the negative solution of the decision problem for identities having a finite non-trivial model. J. Symb. Logic **40**, 186–196 (1975)

[14] Quackenbush, R., Wolk, B.: Strong representation of congruence lattices, Algebra Univers. **1**, 165–166 (1971/72)

[15] Thurston, H.A.: Derived operations and congruences. Proc. London Math. Soc. (3) **8**, 127–134 (1958)

Kalle Kaarli
University of Tartu
Tartu
Estonia
e-mail: kaarli@ut.ee
URL: https://www.ut.ee/en/kalle-kaarli

Alden Pixley
Harvey Mudd College
Claremont, California 91711
USA
e-mail: pixley@mcn.org

Received: 11 April 2018.
Accepted: 16 October 2018.