Congruence computations in principal arithmetical varieties

Kalle Kaarli, Alden Pixley

56th SSAOS
Špindlerův Mlýn, September 2-7, 2018

Alden Pixley, K.K. and Béla Csákány during Szeged confernece in 1998.

Prelimimaries

Algebra is called **arithmetical** if its congruences permute and the congruence lattice is distributive.

Algebra is called **affine complete** if its polynomial functions are precisely the congruence preserving functions.

Variety is called **arithmetical (affine complete)** if so are all its members.

Pixley function on a set A – a ternary function f on A satisfying the identity $f(x, y, y) = f(x, y, x) = f(y, y, x) = x$.

Pixley term for an algebra A – a ternary term that induces a Pixley function on A.

Pixley term for a variety V – a ternary term that is a Pixley term for all members of V.

Theorem (A. Pixley)

A variety is arithmetical iff it admits a Pixley term.

minimal algebra – an algebra that has no proper subalgebras.

Theorem (K.K., Pixley)

An arithmetical variety of finite type is affine complete iff it is generated by a finite minimal algebra.

Principal arithmetical varieties

$\mathrm{Cg}^{\mathbf{A}}(a, b)$ – the principal congruence generated by the pair of elements a, b of an algebra $\mathbf{A}$.

Let p be a Pixley term for a variety V, $\mathbf{A} \in V$ and $a, b, c, d \in A$. It is easy to check that then the following holds:

$$p(a, b, c) = p(a, b, d) \implies (c, d) \in \mathrm{Cg}^{\mathbf{A}}(a, b)\,. \qquad (*)$$

We call V a **principal arithmetical variety** if there is a Pixley term p (called a **principal Pixley term**) for V such that in (*) the opposite implication holds, too.

Thus, if p is a principal Pixley term for a variety V, $\mathbf{A} \in V$ and $a, b \in A$ then the principal congruence $\mathrm{Cg}^{\mathbf{A}}(a, b)$ 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 $p(a, b, x)$. In other words, $\mathrm{Cg}^{\mathbf{A}}(a, b)$ 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 $\mathrm{Cg}^{\mathbf{A}}(a, b)$. We will call any such function a **selector** for $\mathrm{Cg}^{\mathbf{A}}(a, b)$.

We also mention that, as it directly follows from the definition, every principal arithmetical variety has **equationally defined principal congruences**. Such varieties were first studied in 1984 by Blok, Köhler and Pigozzi.

The present work is a continuation of the paper

K.K., A. Pixley, Weakly diagonal algebras and definable principal congruences, AU 55 (2006)

where the main result was

Theorem (Principality)

Every arithmetical affine complete variety of finite type is a principal arithmetical variety with respect to an appropriately chosen Pixley term.

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 **discriminator** and defined as follows: $d(x, y, z) = z$ if $x = y$ and $d(x, y, z) = x$ otherwise.

discriminator term for an algebra **A** – a ternary term d that induces the discriminator on A.

discriminator algebra – an algebra **A** admitting a discriminator term.

It is easy to see that all discriminator algebras are simple.

dicriminator variety – a variety that admits a common discriminator term for all its subdirectly irreducibles.

Theorem (Werner, 1978)

A discriminator term for a variety V is also a principal Pixley term for V.

Hence, every discriminator variety is a principal arithmetical variety.

The most important example of a discriminator variety is the variety of Boolean algebras $\mathcal{B}$. Its 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, this variety is affine complete. 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.

Finitely generated congruences

Theorem

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

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

then the nested polynomial

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

is a selector for θ*.*

The latter allows to construct a closed form solution formula for any finitely presented system of pairwise compatible congruences (the Chinese Remainder Theorem).

The classical Chinese Remainder Theorem asserts that the system of simultaneous integer congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ &\cdots\cdots\cdots\cdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

is solvable iff $a_i \equiv a_j \pmod{g.c.d.(m_i, m_j)}$ for all $1 \leq i < j \leq n$.

This fact generalizes to arbitrary arithmetical algebras as follows.

Theorem

Let $\mathbf{A}$ *be an arithmetical algebra,* $a_1, \ldots, a_n \in A$ *and* $\theta_1, \ldots, \theta_n \in \mathrm{Con}(\mathbf{A})$*. Then the system of congruences*

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

is solvable iff $a_i \equiv a_j \mod (\theta_i \vee \theta_j)$ *holds for all* $1 \leq i < j \leq n$*.*

The following theorem shows that for every principal arithmetical variety V and natural numbers m and n, there is a formula that solves any system of congruences **(B)** over any algebra $\mathbf{A} \in V$ where every θ_i is the join of at most m principal congruences:

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

Theorem

Let V be a principal arithmetical variety with principal Pixley term p. Then there are $(2m+1)$-ary terms $t_i(x_{i1}, y_{i1}, \ldots, x_{im}, y_{im}, z)$, $1 \leq i \leq n$, 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 $\mathbf{A} \in V$, any system **(B)** *over* **A** *with congruences $\theta_1, \ldots, \theta_n$ as in (**) is solvable iff*

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

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*

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

Note that the terms $t_1, \ldots, t_n$ and t that appear in the theorem above are composed only from p.

It is interesting to compare the solution above with the case of integer congruences **(A)**. In both cases one has to solve the congruences two at a time and then to use distributivity of the congruence lattice. The difference comes from the fact that the ring of integers $\mathbb{Z}$ is an arithmetical algebra but it does not generate an arithmetical variety.

Regular algebras

An algebra **A** is called **(congruence) regular** if every congruence of **A** is determined by each of its classes, i.e.: if $a \in A$ and $\rho, \sigma \in \mathrm{Con}\mathbf{A}$ then $a/\rho = a/\sigma$ implies $\rho = \sigma$.

A variety is called **(congruence) regular** if so are all its members.

Clearly, regularity implies the condition **NSC** (**no singleton classes**) meaning that only the zero congruence may have a singleton class.

The converse is not true. There exists a six-element non-regular arithmetical algebra that satisfies NSC.

It is known (Thurston, 1958) that if all members of a variety V have the property NSC then the variety is regular. In fact, a stronger results holds: an algebra is regular iff all of its homomorphic images have the property NSC.

It is known (Grätzer, 1970) that a variety is regular, if so is its free algebra in three generators.

Theorem

A finite minimal regular algebra contained in an arithmetical variety generates a regular variety.

Lattice of compact congruences

Throughout this section we will deal exclusively with an arithmetical affine complete variety 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 (Meets)

Let $p(x, y, z)$ be any principal Pixley term for 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 V the meet of principal congruences is given by the formula

$$\operatorname{Cg}(a, b) \wedge \operatorname{Cg}(c, d) = \operatorname{Cg}(m(a, b, c), m(a, b, d)). \qquad \text{(M)}$$

Theorem (Joins)

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

$$\operatorname{Cg}(a, b) \vee \operatorname{Cg}(c, d) = \operatorname{Cg}(p(a, b, c), p(b, a, d)) . \qquad \text{(J)}$$

The formulas **(M)** and **(J)** first appeared in

S. Bulman-Fleming, H. Werner, *Equational compactness in quasi-primal varieties*, Algebra Universalis **7** (1977), 33–46.

The basic difference between these two Theorems (Meets and Joins) is that in the first of them any principal Pixley term for V works while in the second a new principal Pixley term has to be constructed and this is possible only if V is regular.

Sketch of proof of Joins Theorem

The proof follows the general scheme of the proof of Principality Theorem and relies on the fact that a variety generated by a finite minimal algebra contains a largest minimal algebra.

Lemma

Suppose $p(x, y, z)$ is a principal Pixley term for an algebra $\mathbf{A}$ and $a, b, c, d \in A$. Then the following are equivalent:

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

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

Let V be a principal arithmetical variety with principal Pixley term $p(x, y, z)$. Assume that V is regular and take a largest minimal member $\mathbf{A}$ of V. It is known that such algebra is weakly diagonal, that is every subalgebra of its square contains the graph of some automorphism of $\mathbf{A}$.

As the first step, we construct a principal Pixley function $f(x, y, z)$ on A that satisfies the conditions of Lemma. We do this step by step, starting from the top. This means that for every $\rho \in \mathrm{Con}\mathbf{A}$ we define a ternary function f_ρ on $\mathbf{A}/\rho$ that satisfies the necessary conditions. We start by defining for all maximal congruences ρ the function f_ρ to be the discriminator. Next we take congruencwes covered by maximal congruences and so on.

Since $\mathbf{A}$ is affine complete, the function f is polynomial and because $\mathbf{A}$ is weakly diagonal, we can define a term function satisfying the same conditions.

THANK YOU!