Ivan Chajda

On Grätzer's problem of binary 1-step congruence schemes

Czechoslovak Mathematical Journal, Vol. 39 (1989), No. 3, 470–476

Persistent URL: http://dml.cz/dmlcz/102318

Czechoslovak Mathematical Journal, 39 (114) 1989, Praha

ON GRÄTZER'S PROBLEM OF BINARY 1-STEP CONGRUENCE SCHEMES

IVAN CHAJDA, Přerov

(Received October 7, 1987)

For a type τ of algebras, a *congruence scheme* of type τ is a sequence $p_1, \ldots, p_n$ of polynomials of type τ together with a function $t: \{1, \ldots, n\} \to \{0, 1\}$. A class of algebras $\mathscr{K}$ of a type τ has a *Uniform Congruence Scheme* $\{p_1, \ldots, p_n; t\}$, briefly UCS, if for each $A \in \mathscr{K}$ and every a_0, a_1, b_0, b_1 of A, $\langle b_0, b_1 \rangle \in \theta(a_0, a_1)$ if and only if

$$b_0 = p_1(a_{t(1)}, c(1, 1), \ldots, c(1, n_1)) ,$$
$$p_i(a_{1-t(i)}, c(i, 1), \ldots, c(i, n_i)) =$$
$$= p_{i+1}(a_{t(i+1)}, c(i + 1, 1), \ldots, c(i + 1, n_{i+1})) \quad \text{for} \quad i = 1, \ldots, n - 1 ,$$
$$b_1 = p_n(a_{1-t(n)}, c(n, 1), \ldots, c(n, n_n))$$

for some elements $c(i, j) \in A$. A function t is called a *switching function*.

A class $\mathscr{K}$ has 1-*step principal congruences* (with a trivial switching function), see [1], if for any a, b, c, d of $A \in \mathscr{K}$, $\langle c, d \rangle \in \theta(a, b)$ if and only if $c = p(a, z_1, \ldots \ldots, z_n)$, $d = p(b, z_1, \ldots, z_n)$ for some $(n + 1)$-ary polynomial p and some elements $z_1, \ldots, z_n$ of A.

A class $\mathscr{K}$ has a 1-*step UCS* if it has a UCS and 1-step principal congruences with a trivial switching function. In this case, the congruence scheme is formed by a single polynomial p fixed for all $A \in \mathscr{K}$ and any $a, b \in A$. The function t can be omitted in this case.

It was proved in [2] (Theorem 13) that $\{p_1, \ldots, p_n; t\}$ is a UCS for some $\mathscr{K}$ of type τ containing no constant if and only if all p_i are at least binary. The paper [1] asked for a characterization of varieties with 1-step principal congruences. Moreover, G. Grätzer in [3] formulated the folloving

Problem. *Find a nontrivial class $\mathscr{K}$ of groupoids such that for every $A \in \mathscr{K}$ and every a, b, c, d of A,*

$$\langle c, d \rangle \in \theta(a, b) \quad \textit{if and only if} \quad c = a + y , \quad d = b + y$$

for some $y \in A$.

The aim of the paper is to give a description of such varieties of algebras.

Let A be an algebra. A binary relation R on A is *compatible* if it has the substitution property with respect to all operations of A. Denote $\omega = \{\langle x, x\rangle;\ x \in A\}$. R is *reflexive* if $\omega \subseteq R$. If $a, b \in A$, denote by $R(a, b)$ the least reflexive compatible binary relation on A containing the pair $\langle a, b\rangle$.

Lemma 1. *Let a, b, x, y be elements of an algebra A. Then $\langle x, y\rangle \in R(a, b)$ if and only if $x = p(a, z_1, \ldots, z_n)$, $y = p(b, z_1, \ldots, z_n)$ for some $(n + 1)$-ary polynomial p and some elements $z_i \in A$ $(i = 1, \ldots, n)$.*

The proof is straightforward.

Hence, an algebra A has 1-step principal congruences with a trivial switching function if and only if $\theta(a, b) = R(a, b)$ for each a, b of A.

Theorem 1. *Let $\mathscr{V}$ be a variety. The following conditions are equivalent:*

(1) *$\mathscr{V}$ has 1-step principal congruences with a trivial switching function;*

(2) *for every $A \in \mathscr{V}$ and every elements $a, b, c, d \in A$, $R(a, b) \,.\, R(c, d) \,.\, R(a, b) \subseteq$ $\subseteq R(c, d)\, R(b, a)\, R(c, d)$.*

Proof. (1) $\Rightarrow$ (2): Let $A \in \mathscr{V}$ and let a, b, c, d, x, y be elements of A. Suppose

$$\langle x, y\rangle \in R(a, b)\, R(c, d)\, R(a, b)\,.$$

By (1), we have

$$(*) \qquad \langle x, y\rangle \in \theta(a, b)\, \theta(c, d)\, \theta(a, b)\,.$$

Since A has 1-step principal congruences, we have

$$h(\theta(v, z)) = \theta(h(v), h(z))$$

for any homomorphism h of A and any elements v, z of A (see the remark after Theorem 3.5 in [1]). Let h: $A \to A/\theta(c, d)$ be the canonical homomorphism. Thus $(*)$ gives

$$\langle h(x), h(y)\rangle \in \theta(h(a), h(b))\, \theta(h(a), h(b)) = \theta(h(a), h(b))\,,$$

i.e.

$$\langle x, y\rangle \in \theta(c, d)\, \theta(a, b)\, \theta(c, d) = \theta(c, d)\, \theta(b, a)\, \theta(c, d)\,.$$

By (1), we have $\langle x, y\rangle \in R(c, d)\, R(b, a)\, R(c, d)$, which proves (2).

(2) $\Rightarrow$ (1): Applying the condition (2) four times, we obtain

$$R(a, b)\, R(c, d)\, R(a, b) \subseteq R(c, d)\, R(b, a)\, R(c, d) \subseteq$$
$$\subseteq R(b, a)\, R(d, c)\, R(b, a) \subseteq R(d, c)\, R(a, b)\, R(d, c) \subseteq$$
$$\subseteq R(a, b)\, R(c, d)\, R(a, b)\,;$$

thus (2) implies

$$(**) \qquad R(a, b)\, R(c, d)\, R(a, b) = R(c, d)\, R(b, a)\, R(c, d)$$

for any $A \in \mathscr{V}$ and any elements a, b, c, d of A. Since $R(a, b)$ is reflexive and compatible, we need only to show that $R(a, b)$ is also symmetrical and transitive. However,

$R(a, a) = \omega = \theta(a, a)$ and $(**)$ give

$$R(a, b) = \omega\, R(a, b)\, \omega = R(a, b)\, \omega\, R(a, b) = R(a, b)\, R(a, b)$$

proving the transitivity. Moreover, we have

$$R(a, b) = R(a, b)\, R(a, b) = R(a, b)\, \omega\, R(a, b) = \omega\, R(b, a)\, \omega = R(b, a)\,,$$

whence the symmetry is evident. Thus $\theta(a, b) = R(a, b)$ and A has 1-step principal congruences with a trivial switching function.

For the sake of brevity, denote by $\mathbf{z}$ the sequence $z_1, \ldots, z_n$. The foregoing Theorem 1 and Lemma 1 enable us to characterize 1-step principal congruence varieties in terms of polynomials:

Theorem 2. *Let $\mathscr{V}$ be a variety. The following conditions are equivalent:*

(1) *$\mathscr{V}$ has 1-step principal congruences with a trivial switching function;*

(2) *for each $(n + 1)$-ary polynomials f, g there exist $(n + 3)$-ary polynomials p, q, r such that*

$$\begin{aligned} f(x, \mathbf{z}) &= q(f(y, \mathbf{z}, x, y, \mathbf{z})\,, \\ p(y, x, y, \mathbf{z}) &= q(g(x, \mathbf{z}), x, y, \mathbf{z})\,, \\ p(x, x, y, \mathbf{z}) &= r(f(y, \mathbf{z}), x, y, \mathbf{z})\,, \\ g(y, \mathbf{z}) &= r(g(x, \mathbf{z}), x, y, \mathbf{z})\,. \end{aligned}$$

Proof. (1) $\Rightarrow$ (2): Let $A = F_{n+2}(x, y, z_1, \ldots, z_n)$ be a free algebra of $\mathscr{V}$ with free generators $x, y, z_1, \ldots, z_n$. Let f and g be $(n + 1)$-ary polynomials over $\mathscr{V}$. By Lemma 1,

$$\begin{aligned} \langle f(x, \mathbf{z}), f(y, \mathbf{z})\rangle &\in R(x, y)\,, \\ \langle g(x, \mathbf{z}), g(y, \mathbf{z})\rangle &\in R(x, y)\,, \end{aligned}$$

thus

$$\langle f(x, \mathbf{z}), g(y, \mathbf{z})\rangle \in R(x, y)\, R(f(y, \mathbf{z}), g(x, \mathbf{z}))\, R(x, y)\,.$$

By Theorem 1 this implies

$$\langle f(x, \mathbf{z}), g(y, \mathbf{z})\rangle \in R(f(y, \mathbf{z}), g(x, \mathbf{z}))\, R(y, x)\, R(f(y, \mathbf{z}), g(x, \mathbf{z}))\,,$$

i.e. there exist elements $c, d \in A$ such that

$$\begin{aligned} \langle f(x, \mathbf{z}), c\rangle &\in R(f(y, \mathbf{z}), g(x, \mathbf{z}))\,, \\ \langle c, d\rangle &\in R(y, x)\,, \\ \langle d, g(y, \mathbf{z})\rangle &\in R(f(y, \mathbf{z}), g(x, \mathbf{z}))\,. \end{aligned}$$

Since A is a free algebra, Lemma 1 implies the existence of $(n + 3)$-ary polynomials p, q, r such that

$$\begin{aligned} f(x, \mathbf{z}) &= q(f(y, \mathbf{z}), x, y, \mathbf{z})\,, \\ c &= q(g(x, \mathbf{z}), x, y, \mathbf{z})\,, \\ d &= r(f(y, \mathbf{z}), x, y, \mathbf{z})\,, \end{aligned}$$

$$g(y, z) = r(g(x, z), x, y, z),$$
$$c = p(y, x, y, z),$$
$$d = p(x, x, y, z).$$

(2) ⇒ (1): Let $A \in \mathscr{V}$, let a, b, c, d, x, y be elements of A and suppose

$$\langle x, y\rangle \in R(a, b)\, R(c, d)\, R(a, b).$$

Then $\langle x, z\rangle \in R(a, b)$, $\langle z, v\rangle \in R(c, d)$, $\langle v, y\rangle \in R(a, b)$ for some elements z, v of A. By Lemma 1, there exist polynomials f, g and elements $e_1, \ldots, e_n \in A$ with

$$x = f(a, \mathbf{e}), \quad z = f(b, \mathbf{e}),$$
$$v = g(a, \mathbf{e}), \quad y = g(b, \mathbf{e}).$$

By (2), there exist $(n + 3)$-ary polynomials p, q, r such that

$$x = f(a, \mathbf{e}) = q(f(b, \mathbf{e}), a, b, \mathbf{e}) = q(z, a, b, \mathbf{e}),$$
$$p(b, a, b, \mathbf{e}) = q(g(a, \mathbf{e}), a, b, \mathbf{e}) = q(v, a, b, \mathbf{e}),$$

thus

$$\langle x, p(b, a, b, \mathbf{e})\rangle \in R(z, v) \subseteq R(c, d).$$

Analogously, we can prove

$$\langle p(a, a, b, \mathbf{e}), y\rangle \in R(c, d).$$

Moreover, Lemma 1 implies

$$\langle p(b, a, b, \mathbf{e}), p(a, a, b, \mathbf{e})\rangle \in R(b, a),$$

thus

$$\langle x, y\rangle \in R(c, d)\, R(b, a)\, R(c, d).$$

By Theorem 1, (1) holds.

If $\mathscr{V}$ has a 1-step UCS, we need not investigate all polynomials f, g in (2) of Theorem 2 since $R(a, b)$ is determined by a single polynomial.

Let a, b be elements of an algebra A and let p be an $(n + 1)$-ary polynomial over A. Denote

$$D_p(a, b) = \{\langle x, y\rangle;\ x = p(a, \mathbf{z}),\ y = p(b, \mathbf{z}) \text{ for some } \mathbf{z} \in A^n\}.$$

Lemma 2. *Let p be an $(n + 1)$-ary polynomial of an algebra A. A has 1-step UCS $\{p\}$ if and if $\theta(a, b) = D_p(a, b)$ for every a, b of A.*

The proof is evident.

Definition. An $(n + 1)$-ary polynomial p of A is *generic* (in A) if $D_p(a, b) = R(a, b)$ fot every a, b of A. A polynomial p is *generic in a variety $\mathscr{V}$* if it is generic in each $A \in \mathscr{V}$.

Theorem 3. *Let p be an $(n + 1)$-ary polynomial of an algebra A. The following conditions are equivalent:*

(1) *p is generic;*

(2) (i) *for every* a, b *of* A *there exists* $z \in A^n$ *such that* $p(a, z) = a$, $p(b, z) = b$;

(ii) *for every* a, b, x *of* A *there exists* $z \in A^n$ *such that* $p(a, z) = x = p(b. z)$;

(iii) *for every* a, b *of* A, *for each m-ary operation* f *of* A *and each* $z_1, \ldots, z_m \in A^n$ *there exists* $z \in A^n$ *such that*

$$f(p(a, z_1), \ldots, p(a, z_m)) = p(a, z),$$
$$f(p(b, z_1), \ldots, p(b, z_m)) = p(b, z).$$

The proof is a direct consequence of the fact that $D_p(a, b) = R(a, b)$ if and only if $\langle a, b\rangle \in D_p(a, b)$, $\omega \subseteq D_p(a, b)$ and $D_p(a, b)$ is compatible.

Corollary 1. *Let* A *be a groupoid (i.e. an algebra with one binary operation* $+$*). The following conditions are equivalent:*

(1) $x + y$ *is a generic polynomial;*

(2) (i) *for every* $a, b \in A$ *there exists* $z \in A$ *with*

$$a + z = a, \quad b + z = b;$$

(ii) *for every* $a, b, x \in A$ *there exists* $v \in A$ *with*

$$a + v = x = b + v;$$

(iii) *for every* $a, b, x, y \in A$ *there exists* $w \in A$ *with*

$$(a + x) + (a + y) = a + w,$$
$$(b + x) + (b + y) = b + w.$$

Theorem 4. *Let* $\mathscr{V}$ *be a variety and* p *and* $(n + 1)$*-ary polynomial. The following conditions are equivalent:*

(1) $\{p\}$ *is the 1-step UCS in* $\mathscr{V}$, *i.e.* $\langle x, y\rangle \in \theta(a, b)$ *if and only if* $x = p(a, z)$, $y = p(b, z)$;

(2) p *is a generic polynomial in* $\mathscr{V}$ *and there exist* $(2n + 2)$*-ary polynomials* $w_1, \ldots, w_n, e_1, \ldots, e_n, f_1, \ldots, f_n$ *such that*

$$p(x, z) = p(p(y, z), e_1(x, y, z, v), \ldots, e_n(x, y, z, v)),$$
$$p(y, w_1(x, y, z, v), \ldots, w_n(x, y, z, v)) =$$
$$= p(p(x, v), e_1(x, y, z, v), \ldots, e_n(x, y, z, v)),$$
$$p(x, w_1(x, y, z, v), \ldots, w_n(x, y, z, v)) =$$
$$= p(p(y, z), f_1(x, y, z, v), \ldots, f_n(x, y, z, v)),$$
$$p(y, v) = p(p(x, v), f_1(x, y, z, v), \ldots, f_n(x, y, z, v)).$$

Proof. (1) $\Rightarrow$ (2): Since $\{p\}$ is a 1-step UCS, then clearly p is a generic polynomial in $\mathscr{V}$. Let $A = F_{2n+2}(x, y, z_1, \ldots, z_n, v_1, \ldots, v_n)$ be a free algebra in $\mathscr{V}$. Clearly

$$\langle p(x, z), p(y, z)\rangle \in R(x, y)$$

and

$$\langle p(x, \mathbf{v}), p(y, \mathbf{v})\rangle \in R(x, y),$$

thus

$$\langle p(x, \mathbf{z}), p(y, \mathbf{v})\rangle \in R(x, y)\, R(p(y, \mathbf{z}), p(x, \mathbf{v}))\, R(x, y).$$

By Theorem 1, this implies

$$\langle p(x, \mathbf{z}), p(y, \mathbf{v})\rangle \in R(p(y, \mathbf{z}), p(x, \mathbf{v}))\, R(y, x)\, R(p(y, \mathbf{z}), p(x, \mathbf{v})),$$

i.e., there exist elements c, d of A such that

$$\langle p(x, \mathbf{z}), c\rangle \in R(p(y, \mathbf{z}), p(x, \mathbf{v})),$$
$$\langle c, d\rangle \in (y, x),$$
$$\langle d, p(y, \mathbf{v})\rangle \in R(p(y, \mathbf{z}), p(x, \mathbf{v})).$$

By (1), there exist elements $e_1, \ldots, e_n, f_1, \ldots, f_n, w_1, \ldots, w_n$ of A such that

$$\begin{aligned} p(x, \mathbf{z}) &= p(p(y, \mathbf{z}), e_1, \ldots, e_n), \\ c &= p(p(x, \mathbf{v}), e_1, \ldots, e_n), \\ c &= p(y, w_1, \ldots, w_n), \\ d &= p(x, w_1, \ldots, w_n), \\ d &= p(p(y, \mathbf{z}), f_1, \ldots, f_n), \\ p(y, \mathbf{v}) &= p(p(x, \mathbf{v}), f_1, \ldots, f_n), \end{aligned}$$

whence (2) is evident.

(2) $\Rightarrow$ (1): Let $\mathscr{V}$ satisfy (2), $A \in \mathscr{V}$ and let a, b, c, d, x, y be elements of A. Suppose

$$\langle x, y\rangle \in R(a, b)\, R(c, d)\, R(a, b).$$

Then there exist elements $r, s \in A$ such that

$$\langle x, r\rangle \in R(a, b), \quad \langle r, s\rangle \in R(c, d), \quad \langle s, y\rangle \in R(a, b).$$

Since p is generic, we have $R(a, b) = D_p(a, b)$, $R(c, d) = D_p(c, d)$, thus

$$\begin{aligned} x &= p(a, \mathbf{z}), \quad r = p(b, \mathbf{z}) \quad \text{and} \\ s &= p(a, \mathbf{v}), \quad y = p(b, \mathbf{v}) \quad \text{for some } \mathbf{z}, \mathbf{v} \text{ of } A^n. \end{aligned}$$

By (2), there exist w_i, e_i, f_i $(i = 1, \ldots, n)$ such that

$$x = p(a, \mathbf{z}) = p(p(b, \mathbf{z}), e_1(a, b, \mathbf{z}, \mathbf{v}), \ldots, e_n(a, b, \mathbf{z}, \mathbf{v})),$$
$$p(y, w_1(x, y, \mathbf{z}, \mathbf{v}), \ldots, w_n(x, y, \mathbf{z}, \mathbf{v})) = p(p(a, \mathbf{v}), e_1(a, b, \mathbf{z}, \mathbf{v}), \ldots, e_n(a, b, \mathbf{z}, \mathbf{v})),$$

thus

$$\langle x, p(b, w_1, \ldots, w_n)\rangle \in R(p(b, \mathbf{z}), p(a, \mathbf{v})) = R(r, s) \subseteq R(c, d).$$

Analogously,

$$\langle p(a, w_1, \ldots, w_n), y\rangle \in R(c, d).$$

Moreover, $\langle p(b, w_1, \ldots, w_n), p(a, w_1, \ldots, w_n)\rangle \in R(b, a)$, thus $\langle x, y\rangle \in R(c, d) . R(b, a) R(c, d)$. By Theorem 1, $\theta(a, b) = R(a, b)$. Since p is generic, $\theta(a, b) = D_p(a, b)$ and Lemma 2 implies (1).

Corollary 2. *In a variety* $\mathscr{V}$ *of groupoids, the following conditions are equivalent:*

(1) $\langle x, y\rangle \in \theta(a, b)$ *if and only if* $x = a + z$, $y = b + z$;

(2) $x + y$ *is a generic polynomial in* $\mathscr{V}$ *and there exist 4-ary polynomials* e, f, w *such that*

$$x + z = (y + z) + e(x, y, z, v)\,,$$
$$y + w(x, y, z, v) = (x + v) + e(x, y, z, v)\,,$$
$$x + w(x, y, z, v) = (y + z) + f(x, y, z, v)\,,$$
$$y + v = (x + v) + f(x, y, z, v)\,.$$

Remark. Corollaries 1 and 2 give the answer to Grätzer's problem.The condition (ii) of Corollary 1 (or of Theorem 3) is rather restrictive. It can be deleted if we modify the congruence scheme as follows:

$\langle x, y\rangle \in \theta(a, b)$ *if and only if either* $x = y$ *or* $x = a + z$, $y = b + z$.

In such a case, (iii) of Corollary 2 must be replaced by

(iii′) *for any* a, b, x, y *of* A *there exist* w, u, z *of* A *with*

$$(a + x) + (a + y) = a + w\,, \quad (b + x) + (b + y) = b + w\,,$$
$$x + (a + y) = a + u\,, \quad x + (b + y) = b + u\,,$$
$$(a + x) + y = a + z\,, \quad (b + x) + y = b + z\,.$$

References

[1] *Baldwin J. T., Berman J.:* Definable principal congruence relations: kith and kin, Acta Sci. Math. (Szeged), *44* (1982), 255–270.

[2] *Berman J., Grätzer G.:* Uniform representations of congruence schemes, Pacific J. of Mathem. *76* (1978), 301–311.

[3] *Grätzer G.:* Universal algebra and lattice theory: A story and three research problems, Universal Algebra and its Links with Logic, Algebra Combinatorics and Computer Science, Proc. "25. Arbeitstandung über Allgemeine Algebra", Darmstadt 1983, Heldermann Verlag 1984, 1–13.

Author's address: třída Lidových milicí 22, 750 00 Přerov, Czechoslovakia.