Radim Bělohlávek; Ivan Chajda Polynomially determined congruences in algebras without constants

Acta Universitatis Palackianae Olomucensis. Facultas Rerum Naturalium. Mathematica, Vol. 36 (1997), No. 1, 7--14

Persistent URL: http://dml.cz/dmlcz/120356

Terms of use:

© Palacký University Olomouc, Faculty of Science, 1997

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.



This paper has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* http://project.dml.cz

Polynomially Determined Congruences in Algebras without Constants

RADIM BĚLOHLÁVEK¹, IVAN CHAJDA²

¹Department of Computer Science, Faculty of Electrical Engeneering, Technical University of Ostrava, tř. 17. listopadu, 708 33 Ostrava–Poruba, Czech Republic

²Department of Algebra and Geometry, Faculty of Science, Palacký University, Tomkova 40, 779 00 Olomouc, Czech Republic e-mail: chajda@risc.upol.cz

(Received September 3, 1996)

Abstract

An algebra \mathcal{A} has q-determined congruences if there is a binary algebraic function (i.e. a polynomial) q such that for each $\theta \in \text{Con } \mathcal{A}$ we have $\langle a, b \rangle \in \theta$ iff $\langle q(a, b), q(a, a) \rangle \in \theta$. We characterize q-determined algebras and their varieties.

Key words: Polynomially determined congruences, algebra without constants.

1991 Mathematics Subject Classification: 08A30

Let $\mathcal{A} = (A, F)$ be an algebra of type τ .

For two *n*-ary terms $p(x_1, \ldots, x_n)$, $q(x_1, \ldots, x_n)$ of type τ we say that \mathcal{A} satisfies the identity $p(x_1, \ldots, x_n) = q(x_1, \ldots, x_n)$ if for any choice of elements $a_1, \ldots, a_n \in \mathcal{A}$ the element $p(a_1, \ldots, a_n)$ coincides with the element $q(a_1, \ldots, a_n)$.

Following [4] we say that an algebra \mathcal{A} has an equationally defined constant if there exists an *n*-ary term $t(x_1, \ldots, x_n)$ such that $t(x_1, \ldots, x_n) = t(y_1, \ldots, y_n)$ is satisfied in \mathcal{A} . Hence, if n = 0 then this equationally defined constant is evidently a nullary operation of type τ . However, for n > 0 it says that the value of $t(a_1, \ldots, a_n)$ does not depend on the choice of elements $a_1, \ldots, a_n \in \mathcal{A}$, i.e. it is a constant.

J. Słominski [4] introduced the following concept.

Definition 1 Let $\mathcal{A} = (A, F)$ be an algebra of type τ and $p(x_1, x_2)$ be a binary term of type τ . We say that the congruence $\theta \in \text{Con } \mathcal{A}$ is p-determined if there exists an element $e \in A$ such that

 $\langle a, b \rangle \in \theta$ if and only if $\langle p(a, b), p(e, e) \rangle \in \theta$.

We say that an algebra \mathcal{A} has *p*-determined congruences if every $\theta \in \text{Con } \mathcal{A}$ is *p*-determined. A class \mathcal{C} of algebras of the same type τ has *p*-determined congruences if each $\mathcal{A} \in \mathcal{C}$ has this property.

For such algebras, we can state the following:

Proposition 1 (see [4] or [5]) Let $\mathcal{A} = (A, F)$ be an algebra of type τ and $p(x_1, x_2)$ be a binary term of type τ . For $\theta \in \text{Con } \mathcal{A}$, the following are equivalent:

- (i) θ is p-determined;
- (ii) $\langle a, b \rangle \in \theta$ if and only if $\langle p(a, b), p(c, c) \rangle \in \theta$ for each $c \in A$;
- (iii) there exists a congruence class N of θ such that $\langle a, b \rangle \in \theta$ if and only if $p(a, b) \in N$.

Remark 1 (i). By (ii) of Proposition 1, one can see that the definition of *p*-determined congruence (or algebra or class of algebras) does not depend on the choosen element $e \in A$.

(ii). Every p-determined congruence $\theta \in \text{Con } \mathcal{A}$ is in fact determined by the unique congruence class N; call this class p-normal.

Let us note that [5] contains a characterization of *p*-normal classes of \mathcal{A} and an assertion showing that if \mathcal{A} has *p*-determined congruences then p(a, a) = p(b, b) for any a, b of \mathcal{A} , i.e. \mathcal{A} has an equationally defined constant p(a, a). If e.g. \mathcal{A} is a group, one can take $p(x, y) = x \cdot y^{-1}$ and, evidently, a class N of $\theta \in \text{Con } \mathcal{A}$ is *p*-normal if and only if N is a normal subgroup of \mathcal{A} ; moreover, p(a, a) = e, the identity element of \mathcal{A} .

G. Matthiessen [3] gave a Mal'cev characterization of varieties with p-determined congruences. We give more convenient form of such a condition.

Theorem 1 Let \mathcal{V} be a variety of type τ and $p(x_1, x_2)$ be a binary term of type τ . \mathcal{V} is p-determined if and only if there exist 4-ary terms t_1, \ldots, t_n of type τ such that

$$p(x,x) = p(y,y)$$

$$x = t_1(p(x,y), p(x,x), x, y)$$

$$t_i(p(x,x), p(x,y), x, y) = t_{i+1}(p(x,y), p(x,x), x, y) \text{ for } i = 1, ..., n-1$$

$$y = t_n(p(x,x), p(x,y), x, y).$$

are identities in \mathcal{V} .

Proof Let \mathcal{V} has *p*-determined congruences. Let $\mathcal{A} = F_{\mathcal{V}}(x, y)$ be the free algebra of \mathcal{V} with two free generators x, y. By Theorem 12.3 in [5] for any $a, b \in \mathcal{A}$ we have p(a, a) = p(b, b) and $\langle a, b \rangle \in \theta(p(a, b), p(a, a))$. Hence, p(x, x) = p(y, y) is the identity in $F_{\mathcal{V}}(x, y)$ and

$$\langle x, y \rangle \in \theta(p(x, y), p(x, x)).$$

Therefore, there exist binary algebraic functions $\varphi_1, \ldots, \varphi_n$ such that

$$x = \varphi_1(p(x, y), p(x, x))$$

$$\varphi_i(p(x, x), p(x, y)) = \varphi_{i+1}(p(x, y), p(x, x)) \quad i = 1, \dots, n-1$$

$$y = \varphi_n(p(x, x), p(x, y))$$

Since \mathcal{A} has exactly two generators x, y, there exist 4-ary terms t_1, \ldots, t_n with

$$\varphi_i(z,v) = t_i(z,v,x,y) \quad (i=1,\ldots,n)$$

whence we obtain the identities of the statement.

Conversely, suppose $A \in \mathcal{V}$, A = (A, F) and $a, b \in A$. Then p(a, a) = p(b, b) and, by using of the identities, $\langle a, b \rangle \in \theta(p(a, b), p(a, a))$. By Theorem 12.3. in [5], it is equivalent to the fact that A has *p*-determined congruences. \Box

For congruence permutable varieties the foregoing condition can have a very readable form.

Theorem 2 Let \mathcal{V} be a variety of type τ and p be a binary term of type τ . The following are equivalent:

- (i) V is congruence-permutable and has p-determined congruences
- (ii) there exists a 3-ary term t of type τ such that

$$p(x,x) = p(y,y)$$

 $x = t(p(x,y),x,y)$
 $y = t(p(x,x),x,y).$

are identities in \mathcal{V} .

Proof By Theorem 1, (ii) clearly implies that \mathcal{V} has p-determined congruences. Moreover, we can put m(x, y, z) = t(p(x, y), x, z). Then

$$egin{array}{lll} m(x,x,y) &=& t(p(x,x),x,y) = y, \ m(x,y,y) &=& t(p(x,y),x,y) = x, \end{array}$$

i.e. m is a Mal'cev term and, therefore, \mathcal{V} is congruence-permutable.

Conversely, suppose \mathcal{V} is congruence permutable and has p-determined congruences. By using of Theorem 12.3 in [5], we conclude p(x,x) = p(y,y) and $\langle x,y \rangle \in \theta(p(x,y), p(x,x))$ analogously as in the proof of Theorem 1 for $\mathcal{A} =$

 $F_{\mathcal{V}}(x, y)$. Since \mathcal{V} is congruence-permutable, every reflexive compatible relation on $\mathcal{A} \in \mathcal{V}$ is a congruence on \mathcal{A} , see e.g. [6]. Hence $\langle x, y \rangle \in R(p(x, y), p(x, x))$ where R(a, b) denotes the least reflexive and compatible relation on \mathcal{A} containing the pair $\langle a, b \rangle \in \mathcal{A}^2$. Hence, there exists a unary algebraic function μ with

$$x=\mu(p(x,y)) \quad ext{and} \quad y=\mu(p(x,x)).$$

Since \mathcal{A} has exactly two generators x, y, there exists a 3-ary term t with $\mu(z) = t(z, x, y)$ whence *(ii)* is evident.

Example 1 Let \mathcal{V} be a variety of groups. We can take $t(z, x, y) = z \cdot y$ and $p(x, y) = x \cdot y^{-1}$. Then p(x, x) = e = p(y, y) and

$$t(p(x,y),x,y) = x \cdot y^{-1} \cdot y = x$$

$$t(p(x,x),x,y) = x \cdot x^{-1} \cdot y = y.$$

Unfortunately, the foregoing theory is sound only in the case if \mathcal{A} (and hence \mathcal{V}) has an equationally defined constant. Hence, it is not applicable in the case of quasigroups although they obey similar properties as loops for which the theory works. The aim of the remaining part is to generalize the foregoing concepts for algebras without constants.

Let $\mathcal{A} = (A, F)$ be an algebra of type τ and let $p(x_1, \ldots, x_n, x_{n+1}, \ldots, x_{n+m})$ be an (n + m)-ary term of type τ (n, m nonnegative integers). Let a_1, \ldots, a_m be elements of A. As it was mentioned in the proofs of foregoing theorems, an *n*-ary function

$$q(x_1,\ldots,x_n)=p(x_1,\ldots,x_n,a_1,\ldots,a_m)$$

is called an *algebraic function over* \mathcal{A} .

Definition 2 Let $\mathcal{A} = (A, F)$ be an algebra and q be a binary algebraic function over \mathcal{A} . A congruence $\theta \in \text{Con } \mathcal{A}$ is called *q*-determined if there exists an element $d \in A$ such that

$$\langle a, b \rangle \in \theta$$
 if and only if $\langle q(a, b), q(d, d) \rangle \in \theta$. (*)

An algebra \mathcal{A} has *q*-determined congruences if each $\theta \in \text{Con } \mathcal{A}$ is *q*-determined.

Theorem 3 Let $\mathcal{A} = (\mathcal{A}, F)$ be an algebra, q be a binary algebraic function over \mathcal{A} and $\theta \in \text{Con } \mathcal{A}$. The following conditions are equivalent:

- (i) θ is q-determined;
- (ii) $\langle a, b \rangle \in \theta$ if and only if $\langle q(a, b), q(c, c) \rangle \in \theta$ for each $c \in A$;
- (iii) there exists a class N of the congruence θ such that $\langle a, b \rangle \in \theta$ if and only if $q(a, b) \in N$.

Proof $(i) \Rightarrow (ii)$: Suppose $c \in A$. Then $\langle c, c \rangle \in \theta$ and, by (i), $\langle q(c, c), q(d, d) \rangle \in \theta$. However, $\langle a, b \rangle \in \theta$ if and only if $\langle q(a, b), q(d, d) \rangle \in \theta$, thus using symetry and transitivity of θ , we conclude $\langle q(a, b), q(c, c) \rangle \in \theta$.

 $(ii) \Rightarrow (iii)$: Suppose N is a class of θ with $q(d, d) \in N$. By $(ii), q(c, c) \in N$ for each $c \in A$, i.e. $(a, b) \in \theta$ if and only if $q(a, b) \in N$.

 $(iii) \Rightarrow (i)$: Evidently, any element of A plays the role of d from (*).

Lemma 1 Let q be a binary algebraic function over an algebra \mathcal{A} . Denote by ω_A the least congruence on \mathcal{A} . If ω_A is q-determined then q(a, a) = q(b, b) for every a, b of A.

Proof For any $a \in A$ we have $\langle a, a \rangle \in \omega_A$. Since ω_A is q-determined, it implies $\langle q(a, a), q(d, d) \rangle \in \omega_A$, i.e. q(a, a) = q(d, d) (for some $d \in A$). The assertion is evident.

Definition 3 Let $\theta \in \text{Con } \mathcal{A}$ is q-determined (for some binary algebraic function q over \mathcal{A}). The class N of θ satisfying

$$\langle a,b\rangle \in \theta$$
 iff $q(a,b) \in N$

(by (iii) of Theorem 3) will be called q-normal.

Theorem 4 A subset N of an algebra $\mathcal{A} = (A, F)$ is a q-normal class of some congruence of \mathcal{A} if and only if N satisfies the following conditions:

- (i) for each $a \in A$, $q(a, a) \in N$;
- (ii) if $q(a, b) \in N$ then $q(b, a) \in N$;
- (iii) if $q(a,b) \in N$ and $q(b,c) \in N$ then $q(a,c) \in N$;
- (iv) if $f \in F$ is n-ary and $q(a_i, b_i) \in N$ for i = 1, ..., n then $q(f(a_1, ..., a_n), f(b_1, ..., b_n)) \in N$;
- (v) for each $a, b \in N$ also $q(a, b) \in N$;
- (vi) if $a \in A$ and $b \in N$ then $q(a, q(b, b)) \in N$ implies $a \in N$.

Proof It is an easy exercise to check that any q-normal class satisfies the conditions (i)-(vi).

Conversely, let $N \subseteq A$ satisfies (i)-(vi). Introduce a binary relation θ on A as follows :

$$\langle a,b\rangle \in \theta$$
 if and only if $q(a,b) \in N$. (**)

By (i), (ii) and (iii), θ is an equvivalence on A. Applying (iv) we check the substitution property, i.e. $\theta \in \text{Con } A$. Suppose $x, y \in N$. By (v), $q(x, y) \in N$ and, by (**), $\langle x, y \rangle \in \theta$. Hence, N is contained in some congruence class of θ . Now suppose $a \in A$ and $b \in N$. Let $\langle a, b \rangle \in \theta$. Since $\langle b, b \rangle \in \theta$, also $q(b, b) \in N$. However, N is contained in some class of θ , thus $b \in N$ and $q(b, b) \in N$ give $\langle b, q(b, b) \rangle \in \theta$. Applying transitivity we conclude $\langle a, q(b, b) \rangle \in \theta$. By (vi), it gives also $a \in N$. Thus the congruence class of θ containing a is included in N, i.e. N is a congruence class of θ . By (iii) of Theorem 3, θ is q-determined. \Box

Corollary 1 Let \mathcal{A} be an algebra with q-determined congruences. The set $\mathcal{N}_q(\mathcal{A})$ of all normal congruence classes forms a complete lattice with respect to set inclusion. The greatest element of $\mathcal{N}_q(\mathcal{A})$ is the whole set \mathcal{A} , the least element is the singleton $\{q(a,a)\}$ for some $a \in \mathcal{A}$.

Proof By (i)-(vi) of Theorem 4 it is evident that $\mathcal{N}_q(\mathcal{A})$ is closed under set intersection. Clearly $\mathcal{A} \in \mathcal{N}_q(\mathcal{A})$, i.e. $\mathcal{N}_q(\mathcal{A})$ is a complete lattice. Since also $\omega_{\mathcal{A}} \in \text{Con } \mathcal{A}$, Lemma 1 completes the proof.

Denote by $\operatorname{Con}_q \mathcal{A}$ the set of all *q*-determined congruences on an algebra \mathcal{A} . Evidently, $\operatorname{Con}_q \mathcal{A}$ is an algebraic lattice and, moreover, $\operatorname{Con}_q \mathcal{A} \cong \mathcal{N}_q(\mathcal{A})$.

Theorem 5 Let q be a binary algebraic function over an algebra \mathcal{A} . \mathcal{A} has q-determined congruences if and only if for each $a, b \in \mathcal{A}$ of \mathcal{A} it holds:

- (*i*) q(a,a) = q(b,b);
- (ii) $\langle a,b\rangle \in \theta(q(a,b),q(a,a)).$

Proof Let \mathcal{A} has q-determined congruences. By Lemma 1 we obtain (i). By Definition 2 and Theorem 3, $\langle q(a,b), q(a,a) \rangle \in \theta$ implies $\langle a, b \rangle \in \theta$. Taking $\theta = \theta(q(a,b), q(a,a))$ we obtain (ii).

Conversely, suppose (i) and (ii). Let $\theta \in \text{Con } \mathcal{A}$. If $\langle a, b \rangle \in \theta$ then clearly also $\langle q(a,b), q(a,a) \rangle \in \theta$. If $\langle q(a,b), q(a,a) \rangle \in \theta$ then, by (ii), also $\langle a, b \rangle \in \theta$, i.e. $\langle a, b \rangle \in \theta$ iff $\langle q(a,b), q(a,a) \rangle \in \theta$. Applying (i) we conclude that θ is q-determined.

Example 2 By Example 1, every group G has p-determined congruences for $p(x,y) = x \cdot y^{-1}$ and the p-normal class of $\theta \in \text{Con } G$ is the normal subgroup $N = \{x \in G; \langle x, e \rangle \in \theta\}$. However, every class of θ is a q-normal class of θ . Let us pick up $a \in K$ for any congruence class K of θ and put $q(x,y) = x \cdot y^{-1} \cdot a$. Then θ is also q-determined and $\langle v, w \rangle \in \theta$ iff $q(v, w) \in K$.

Every convex sublattice of a Boolean algebra B containing a given element c is a q-normal class for $q(x, y) = x \oplus y \oplus c$ where $x \oplus y = (x' \land y) \lor (x \land y')$, the symmetrical difference.

Let $\mathcal{R} = (R, t, u, 0, 1)$ be a bi-ternary ring (see [2]), $\theta \in \text{Con } \mathcal{R}$. Every class of θ is q-normal. To show this, let $[a]_{\theta}$ be any class of θ and put q(x, y) =t(1, a, u(1, x, y)). If $\langle x, y \rangle \in \theta$ then $\langle u(1, x, y), 0 \rangle = \langle u(1, x, y), u(1, x, x) \rangle \in \theta$ which implies $\langle t(1, a, u(1, x, y)), a \rangle = \langle t(1, a, u(1, x, y)), t(1, a, 0) \rangle \in \theta$. Conversely, if $\langle t(1, a, u(1, x, y)), a \rangle \in \theta$ then

$$\langle u(1,x,y),0\rangle = \langle u(1,a,t(1,a,u(1,x,y))),u(1,a,a)\rangle \in \theta$$

which gives $\langle y, x \rangle = \langle t(1, x, u(1, x, y)), t(1, x, 0) \rangle \in \theta$.

Remark 2 Evidently, every algebra with p-determined congruences has also q-determined congruences since every term is an algebraic function. We are going to show that algebras with q-determined congruences from a larger class.

Polynomially determined congruences in algebras without constants

Definition 4 For an algebra \mathcal{A} , denote by $AF(\mathcal{A})$ the set of all algebraic functions over \mathcal{A} . Let $A \neq \emptyset$ be a set and $\mathcal{A}_1 = (A, F_1)$, $\mathcal{A}_2 = (A, F_2)$ be two algebras. We say that \mathcal{A}_2 is a *function reduct* of \mathcal{A}_1 if $F_2 \subseteq AF(\mathcal{A}_1)$.

Hence, \mathcal{A}_2 is a function reduct of \mathcal{A}_1 if for each *n*-ary $f \in F_2$ there exists an *n*-ary algebraic function g over \mathcal{A}_1 such that

$$f(a_1,\ldots,a_n)=g(a_1,\ldots,a_n)$$

for any $a_1, \ldots, a_n \in A$.

Lemma 2 Let A_2 be a function reduct of A_1 .

- (i) if $\theta \in \text{Con } \mathcal{A}_1$ then $\theta \in \text{Con } \mathcal{A}_2$;
- (ii) if A_2 has p-determined congruences (for some binary term p) then A_1 has q-determined congruences (for some binary algebraic function over A_1).

Proof The proof follows directly by Definition 4 an by Proposition 1(iii) and Theorem 3(iii).

Remark 3 The converse of (i) of Lemma 2 does not hold in general, see the following:

Example 3 Let $A = \{a, b, c, d\}$ and consider the quasiqroup $Q_1 = (A; \cdot, /, \cdot)$, where the table for \cdot is

•	a	b	c	d
a	a	b	с	d
b	c	d	b	a
с	b	a	d	c
d	d	c	a	b

Let $Q_2 = (A; \circ, //, \backslash)$ be a quasigroup with operations introduced as follows:

$$\begin{aligned} x \circ y &= (x/b) \cdot (a \setminus y) \\ x//y &= (x/(a \setminus y)) \cdot b \\ x \setminus y &= a \cdot ((x/b) \setminus y). \end{aligned}$$

Then Q_2 is a function reduct of Q_1 . However the equivalence θ with the partition $\{\{a, b\}, \{c, d\}\}$ is a congruence on Q_2 but not on Q_1 .

Definition 5 (see [1]) Let $Q_1 = (A_1; \cdot, /, \backslash)$, $Q_2 = (A_2; \circ, //, \backslash \backslash)$ be quasigroups. By an *isotopy* between Q_1 and Q_2 we mean the triple $\langle \alpha, \beta, \gamma \rangle$ of bijections of A_1 onto A_2 satisfying

$$\alpha(a) \circ \beta(b) = \gamma(a \cdot b) \text{ for each } a, b \in A_1.$$

By a loop L we mean a quasigroup with an identity element, i.e. with an element e satisfying $x \cdot e = e \cdot x = x$ for each $x \in L$.

The following statements are well-known, see e.g. [1] for the proofs.

Lemma 3 Every quasigroup $Q = (A; \cdot, /, \setminus)$ is isotopic to a loop

 $L = (A; \circ, //, \backslash \backslash, e)$

where $\langle R_b^{-1}, L_a^{-1}, id_A \rangle$ is this isotopy $(R_b(x) = x \cdot b, L_a(x) = a \cdot x)$. In this case we have $e = a \cdot b$ and

Theorem 6 Every quasigroup has q-determined congruences (for some binary algebraic function q).

Proof Let $Q = (A; \cdot, /, \backslash)$ be a quasigroup. By Lemma 3, Q is isotopic with a loop $L = (A; \circ, //, \backslash \backslash)$ and, by Lemmas 2 and 3, every congruence on Q is also a congruence on L. By Lemma 2 (*ii*), Q has q-determined congruences provided L has p-determined congruences for some binary term p of type $\{\circ, //, \backslash \backslash, e\}$. However, it is well-known (see [1]) that for $\theta \in \text{Con } L$,

 $\langle x, y \rangle \in \theta$ if and only if $x//y \in N$

where N is the class of θ containing e. By *(iii)* of Proposition 1, L has p-determined congruences for p(x, y) = x//y finishing the proof.

Corollary 2 Let $Q = (A; \cdot, /, \setminus)$ be a quasigroup and $a, b \in A$. Then

- (a) Q has q-determined congruences for $q(x,y) = (x/(a \setminus y)) \cdot b$;
- (b) for each $\theta \in \text{Con } Q$, the class of θ containing the element $a \cdot b$ is q-normal.

References

- [1] Bruck, R. H.: A Survey of Binary Systems. Springer-Verlag, Berlin, 1971.
- [2] Chajda, I., Halaš, R.: Ideals of bi-ternary rings. Discussione Math., Algebra and Stoch. Meth. 15 (1995), 11-21.
- Matthiessen, G.: Ideals, normal sets and congruences. Colloq. Math. J. Bolyai, 17th Contribution to Universal Algebra, Szeged (Hungary) 1975, 295-310.
- [4] Slominski, J.: On the determining of the form of congruences in abstract algebras with equationally defined constant elements. Fundamenta Math. 48 (1960), 325-341
- [5] Schmidt, E. T.: Kongruenzrelationen algebraischer Strukturen. Mathem. Forschungsberichte, Deutscher Verlag der Wissenschaften, Berlin, 1969
- [6] Werner, H.: A Mal'cev conditions for admissible relations. Algebra Univ. 3 (1973), 263.