A POLYNOMIAL CHARACTERIZATION OF CONGRUENCE CLASSES

Radim Bělohlávek

Department of Computer Science
Technical University of Ostrava
tř. 17. listopadu
708 33 Ostrava-Poruba
Czech Republic
e-mail: radim.belohlavek@vsb.cz

Ivan Chajda

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

Abstract

Let $\mathcal{V}$ be a regular and permutable variety and $\mathcal{A} = (A, F) \in \mathcal{V}$. Let $\emptyset \neq C \subseteq A$. We get an explicite list L of polynomials such that C is a congruence class of some $\theta \in Con\,A$ iff C is closed under all terms of L. Morevover, if $\mathcal{V}$ is of a finite similarity type, L is finite. If also $\mathcal{A} \in \mathcal{V}$ is finite, all polynomials of L can be considered to be unary. We get a formula for the estimation of $card\,L$. The problem of deciding whether C is a congruence class is a finite algebra is in NP but for $\mathcal{A} \in \mathcal{V}$ it is in P.

1991 Mathematics Subject Classification: 08A30, 08A40, 08B05, 68Q25

Let $\mathcal{A} = (A, F)$ be an algebra, let $\emptyset \neq C \subseteq A$. It was proved by A. I. Mal'cev [5] that C is a class of some $\theta \in Con\,\mathcal{A}$ if and only if

$$\text{either} \quad \tau(C) \cap C = \emptyset \quad \text{or} \quad \tau(C) \subseteq C$$

for any *translation* of $\mathcal{A}$. Let us recall that by a translation is in [5] meant a unary polynomial. Although this characterization is simple and very useful thourough general algebra, its disadvantage is that an algebra $\mathcal{A} = (A, F)$ can have an infinite number of unary polynomials even if A or F are finite. We are going to give another polynomial characterization of congruence classes for algebras of regular and permutable varieties where for F finite we need only a finite set of testing polynomials.

Recall that an algebra $\mathcal{A} = (A, F)$ is *regular* if $\theta = \Phi$ for $\theta, \Phi \in Con\,\mathcal{A}$ whenever they have a congruence class in common. $\mathcal{A}$ is permutable if $\theta \circ \Phi = \Phi \circ \theta$ for every $\theta, \Phi \in Con\,\mathcal{A}$. A variety $\mathcal{V}$ is regular or permutable if each $\mathcal{A} \in \mathcal{V}$ has this property.

The following Mal'cev type characterization was derived independently in [2], [3].

Proposition. *A variety $\mathcal{V}$ is regular and permutable if and only if there exist $n \geq 1$ ternary terms $t_1, \ldots, t_n$ and a $(3+n)-$ary term q such that*

$$(*) \qquad \begin{array}{rcl} t_i(x,x,z) & = & z \qquad \text{for} \quad i = 1, \ldots, n \\ x & = & q(x,y,z,t_1(x,y,z), \ldots, t_n(x,y,z)) \\ y & = & q(x,y,z,z,\ldots,z) \ . \end{array}$$

Throughout the paper all refered terms $t_1, \ldots, t_n, q$ are those of $(*)$.

Theorem 1. *Let $\mathcal{V}$ be a regular and permutable variety, let $\mathcal{A} = (A,F) \in \mathcal{V}$ and $\emptyset \neq C \subseteq A$. Then C is a class of some $\theta \in Con\,\mathcal{A}$ if and only if the following conditions hold:*

(A) if $t_i(a_j,b_j,c) \in C$ for $c \in C$, $i = 1, \ldots, n$, $j = 1, \ldots, m$ and $f \in F$ is $m-$ary then $t_i(f(a_1,\ldots,a_m), f(b_1,\ldots,b_m), c) \in C$;

(B) if $c, d \in C$, $a \in A$ and $t_i(a,d,c) \in C$ for $i = 1, \ldots, n$ then $a \in C$;

(C) if $c, d \in C$ then $t_i(d,c,c) \in C$ for $i = 1, \ldots, n$.

Proof: Consider $\mathcal{A} \in \mathcal{V}$, $\emptyset \neq C \subseteq A$, $c \in C$ and suppose (A), (B), (C). We prove that C is a class of some $\theta \in Con\,\mathcal{A}$.
Introduce a binary relation θ on A as follows:

$$(**) \qquad \langle a,b \rangle \in \theta \quad \text{iff} \quad t_1(a,b,c) \in C, \ldots, t_n(a,b,c) \in C$$

for the terms $t_1, \ldots, t_n$ of $(*)$. Since $t_i(a,a,c) = c \in C$, θ is reflexive. By (A) we easily infer that θ is also compatible with any $m-$ary operation $f \in F$. Hence, by [6], $\theta \in Con\,\mathcal{A}$.
Let $x \in [c]_\theta$. Then $\langle x,c \rangle \in \theta$ and, by $(**)$, $t_i(x,c,c) \in C$ for $i = 1, \ldots, n$. By (B) we infer $x \in C$, i.e. $[c]_\theta \subseteq C$. Suppose $x \in C$. Using (C) we get $t_i(x,c,c) \in C$ $(i = 1, \ldots, n)$. By $(**)$ we have $\langle x,c \rangle \in \theta$ thus $x \in [c]_\theta$. Hence $C \subseteq [c]_\theta$. We have proved that C is a congruence class of θ.
Conversely, let C be a class of some $\theta \in Con\,\mathcal{A}$ and $c \in C$. Suppose $t_i(a_j,b_j,c) \in C$ for $j = 1, \ldots, m$, $i = 1, \ldots, n$ and let $f \in F$ be $m-$ary. Then $\langle t_i(a_j,b_j,c), c \rangle \in \theta$ and, by $(*)$, we obtain

$$\begin{array}{rcl} a_j & = & q(a_j,b_j,c,t_1(a_j,b_j,c), \ldots, t_n(a_j,b_j,c)) \\ b_j & = & q(a_j,b_j,c,c,\ldots,c) \end{array}$$

whence $\langle a_j,b_j \rangle \in \theta$. Applying compatibility of θ we conclude $\langle f(a_1,\ldots,a_m), f(b_1,\ldots,b_m) \rangle \in \theta$. Thus

$$\langle t_i(f(a_1,\ldots,a_m), f(b_1,\ldots,b_m), c), c \rangle =$$

$$= \langle t_i(f(a_1,\ldots,a_m), f(b_1,\ldots,b_m), c), t_i(f(b_1,\ldots,b_m), f(b_1,\ldots,b_m), c), c \rangle \in \theta$$

by $(*)$ of Proposition. Hence, (A) holds.
Now, let $t_i(a,d,c) \in C = [c]_\theta$ for some $d \in C$ and $i = 1, \ldots, n$. Then $\langle t_i(a,d,c), c \rangle \in \theta$ and, by $(*)$,

$$\begin{array}{rcl} a & = & q(a,d,c,t_1(a,d,c), \ldots, t_n(a,d,c)) \\ d & = & q(a,d,c,c,\ldots,c) \ . \end{array}$$

Hence $\langle a,d \rangle \in \theta$. However, $d \in C = [c]_\theta$ thus also $a \in C$ proving (B).
If $c, d \in C = [c]_\theta$ then

$$\langle t_i(d,c,c), c \rangle = \langle t_j(d,c,c), t_i(c,c,c) \rangle \in \theta$$

thus $t_i(d,c,c) \in C$ as required in (C). □

Let us introduce the following concept. If $p(x_1,\ldots,x_n,y_1,\ldots,y_m)$ is an $(m+n)-$ary term of an algebra $\mathcal{A} = (A,F)$ and $C \subseteq A$, we say that C is *$y-$closed under p* if $p(a_1,\ldots,a_n,c_1,\ldots,c_m) \in C$ for any $a_1,\ldots,a_n \in A$ and any $c_1,\ldots,c_m \in C$.

Theorem 2. *Let $\mathcal{V}$ be a regular and permutable variety, let $\mathcal{A} = (A,F) \in \mathcal{V}$ and $\emptyset \neq C \subseteq A$. Then C is a congruence class of some $\theta \in Con\,\mathcal{A}$ if and only if C is $y-$closed under the following terms:*

(a) $\quad t_i(f(q(x_1,x_1',y,y_{11},\dots,y_{1n}),\dots,q(x_m,x_m',y,y_{m1},\dots,y_{mn})),$
$\quad f(x_1',,\dots,x_m'),y)$
for each $m-$*ary* $f\in F$ *and every* $i=1,\dots,n$*;*

(b) $q(x,y,y',y_1,\dots,y_n)$

(c) $r_i(y_1,y_2)=t_i(y_1,y_2,y_2)$ *for* $i=1,\dots,n$.

Proof: Let $\emptyset\neq C\subseteq A$ be $y-$closed under the terms of (a), (b) and (c). By Theorem 1 we have to show the validity of (A), (B) and (C).
Let $t_i(a_j,b_j,c)\in C$ for $i=1,\dots,n,\ j=1,\dots,m$ and $f\in F$ be $m-$ary. By (a) and $(*)$ of Proposition we have

$$\begin{aligned}&t_i(f(a_1,\dots,a_m),f(b_1,\dots,b_m),c)=\\&=t_i(f(q(a_1,b_1,c,t_1(a_1,b_1,c),\dots,t_n(a_1,b_1,c)),\dots,\\&\qquad q(a_m,b_m,c,t_1(a_m,b_m,c),\dots,t_n(a_m,b_m,c))),f(b_1,\dots,b_m),c)\in C\end{aligned}$$

proving (A).
Suppose $t_i(a,d,c)\in C$ for some $c,d\in C$, $a\in A$ and $i=1,\dots,n$. By (b) and $(*)$ we obtain

$$a=q(a,d,c,t_1(a,d,c),\dots,t_n(a,d,c))\in C\ ,$$

whence (B) is evident.
Clearly, from (c) we infer (C).
By Theorem 1, C is a class of some $\theta\in Con\,\mathcal{A}$.

Conversely, if C is a congruence class of some $\theta\in Con\,\mathcal{A}$ then the closeness under terms listed in (a), (b) and (c) follows immediately from $(*)$ and the substitution property of θ. □

Corollary 1. *Let* $\mathcal{V}$ *be regular and permutable variety of a finite similarity type, let* $\mathcal{A}=(A,F)\in\mathcal{V}$, $\emptyset\neq C\subseteq A$*. Then* C *is a congruence class of some* $\theta\in Con\,\mathcal{A}$ *if and only if* C *is* $y-$*closed under a* finite *number* h *of terms of* (a)*,* (b)*,*(c)*; especially, if* $k=card\,F$ *then* $h\leq n(k+1)+1$ *where* n *is taken from Proposition.*

Examples. Let $\mathcal{V}$ be a variety of quasigroups, i.e. a variety of type $(2,2,2)$ satisfying the identities

$$\begin{aligned}x\cdot(x\backslash y)&=y &\qquad (y/x)\cdot x&=y\\ x\backslash(x\cdot y)&=y &\qquad (y\cdot x)/x&=y\ .\end{aligned}$$

Then $\mathcal{V}$ is regular and permutable since

$$\begin{aligned}t_1(x,y,z)&=y/(z\backslash x)\\ q(x,y,z,u)&=z(u\backslash y)\end{aligned}$$

are the terms of $(*)$ of the Proposition. Let $\mathcal{Q}=(Q,\cdot,\backslash,/)\in\mathcal{V}$ and $\emptyset\neq C\subseteq Q$. By Theorem 2, C is a congruence class of some $\theta\in Con\,\mathcal{Q}$ if and only if C is closed under the following terms (see also [1]):

$$\begin{aligned}p_1(x_1,x_2,y_1,y_2,y_3)&=(x_1x_2)/(y_3\backslash[(y_3(y_1\backslash x_1))(y_3(y_2\backslash x_2))])\\ p_2(x_1,x_2,y_1,y_2,y_3)&=(x_1/x_2)/(y_3\backslash[(y_3(y_1\backslash x_1))/(y_3(y_2\backslash x_2))])\\ p_3(x_1,x_2,y_1,y_2,y_3)&=(x_1\backslash x_2)/(y_3\backslash[(y_3(y_1\backslash x_1))\backslash(y_3(y_2\backslash x_2))])\\ p_4(y_1,y_2,y_3)&=y_1(y_2\backslash y_3)\\ p_5(y_1,y_2,y_2)&=y_2/(y_2\backslash y_1)\ .\end{aligned}$$

Remark. Let us note that in the just presented example, $n = 1$, $k = 3$, the upper estimation of number of terms is $1 \cdot (3 + 1) + 1 = 5$ so the upper bound is reached. Consider a variety $\mathcal{V}$ of groups. $\mathcal{V}$ is regular and permutable, one can take

$$\begin{aligned} t_1(x, y, z) &= xy^{-1}z \\ q(x, y, z, u) &= uz^{-1}y \ . \end{aligned}$$

Following Theorem 2 we get the terms

$$\begin{array}{lcl} p_1(x_1, y_1, y_2, y_3) & = & y_1y_3^{-1}x_1y_2y_3^{-1}x_1^{-1}y^3 \\ p_2(x_1, y_1, y_2) & = & x_1^{-1}y_2y_1^{-1}x_1y_2 \\ p_3(y_1) & = & y_1 \\ p_4(y_1, y_2, y_3) & = & y_3y_2^{-1}y_1 \\ p_5(y_1) & = & y_1 \ . \end{array}$$

If a subset of a carrier set of a group is $y-$closed under p_1 then it is evidently $y-$closed under p_3, p_4 and p_5. For example, substituing the unit element e for x_1 in p_1 we get p_4 (variable indicies are unimportant). Furthermore, the $y-$closeness under p_1 and p_4 implies the $y-$closeness under $p_4(y_3, p_1(x_1^{-1}, y_1, y_2, y_3), y_1)$. Since the last term is the same as p_2, we have shown that in the case of groups we have only one characterisctic term (p_1), although the upper bound is 5.

Remark. Returning to Mal'cev result from the computational point of view, we must verify possible infinite number of unary polynomials even in the case of finite algebra having finite similarity type. Our method deals with a finite number of unary polynomials in the regular and permutable case:

Corollary 2. *Let $\mathcal{V}$ be regular and permutable variety of a finite similarity type F, $\mathcal{A} \in \mathcal{V}$, $\emptyset \neq C \subseteq A$. Then C is a class of some $\theta \in Con\,\mathcal{A}$ iff it is closed under finite number h of unary polynomials. Especially, if $F = \{f_i;\ i = 1, \ldots, k\}$ and each f_i is $\sigma(f_i)-$ary, $l = card\,C$, $m = card\,A$ then*

$$h \leq n \sum_{i=1}^{k} m^{2\sigma(f_i)} l^{n\sigma(f_i)} + ml^{n+1} + nl \ .$$

Proof: Consider any term of the form

$$\begin{aligned} &t_i(f(q(x_1, x_1', y, y_{11}, \ldots, y_{1n}), \ldots, q(x_m, x_m', y, y_{m1}, \ldots, y_{mn})), \\ &\quad f(x_1', , \ldots, x_m'), y) \end{aligned}$$

of Theorem 2(a). It is clear that C is $y - closed$ under this term if and only if it is closed under all the unary polynomials (the variable is y)

$$\begin{aligned} &t_i(f(q(a_1, a_1', y, c_{11}, \ldots, c_{1n}), \ldots, q(a_m, a_m', y, c_{m1}, \ldots, c_{mn})), \\ &\quad f(a_1', , \ldots, a_m'), y) \end{aligned}$$

where $a_1, a_1', \ldots, a_m, a_m' \in A$, $c_{11}, \ldots, c_{mn} \in C$. It is easy to see that the number of these terms is $m^{2\sigma(f)} l^{n\sigma(f)}$ for each $i = 1, \ldots, n$. Summing over F we get the number $n \sum_{i=1}^{k} m^{2\sigma(f_i)} l^{n\sigma(f_i)}$ of unary polynomials, the first term. Similarly, for conditions (b) and (c) of Theorem 2 we get the resting terms ml^{n+1} and nl. □

Let us think about the computational complexity of this problem. We are given an algebra $\mathcal{A} = (A, F)$ with both A and F finite of a regular and permutable variety and a nonempty set $C \subseteq A$. Decide whether C is a congruence class of some $\theta \in Con\,\mathcal{A}$. Denote this problem by p. Furthermore, denote by $p_{\mathcal{V}}$ the same problem for algebras of a given regular and permutable variety $\mathcal{V}$ only for which the terms $q, t_1, \ldots, t_n$ are known. In the resting part let k, l, mf_i, σ have the same meaning as in Corollary 2.

Following the conventional approach (which is applicable for arbitrary algebras) one would generate all the partitions of A with C as a class. Note that in the case of regular algebras, if $card\,C > 1$ then the partitions containing at least one singleton class can be omitted (there is only one congruence relation with singleton classes, namely ω), while the case $card\, C = 1$ is trivial. For each such a partition we have to testify the substitution property with respect to every operation $f \in F$. Let us enumerate the number of partitions to testify.

Using the Principle of Inclusion and Exclusion (see e.g. [4]) there are

$$\sum_{i=0}^{r} (-1)^i \binom{r}{i} (r-i)^p$$

onto mappings from a $p-$element A set onto an $r-$element set. Each such a mapping induces a partition on A (its kernel). For each partition there are exactly $r!$ mappings inducing it. Therefore, there are

$$\frac{1}{r!} \sum_{i=0}^{r} (-1)^i \binom{r}{i} (r-i)^p$$

partitions of a $p-$element set into r classes. The number of all partitions of a $p-$element set is thus

$$\pi(p) = \sum_{r=1}^{p} \frac{1}{r!} \sum_{i=0}^{r} (-1)^i \binom{r}{i} (r-i)^p$$

Little bit more complicated arguments using the Generalized principle of inclusion and exclusion ([4]) lead to the observation that there are

$$\pi'(p) = \sum_{r=1}^{p} p! \sum_{j=1}^{p} \frac{(-1)^j}{j!} \sum_{i=j}^{r} \frac{(-1)^i (r-p)^{(p-i)}}{(i-j)!(p-i)!(r-i)!}$$

partitions of a $p-$element set containing at least one singleton class.

The problem $p_{\mathcal{V}}$ is much more simple. By Theorem 2 it is enough to verify the $y-$closeness under the listed terms. Arguments similar to those of Corollary 2 lead to the observation stating that there are

$$\sum_{i=1}^{k} n m^{2\sigma(f_i)} l^{n\sigma(f_i)+1} + m l^{n+2} + n l^2 \ .$$

substitutions of variables necessary to check the $y-$closeness.

Recall that by a time complexity of a given algorithm is meant a function $f : N \rightarrow N$ such that every problem of size n will by succesfully solved by this algorithm after at most $f(n)$ computational steps. A given problem is of time complexity $f(n)$ if there is an algorithm solving it which is of time complexity $f(n)$. Problems which can be solved by nondeterministic algorithms (deterministic algorithms) of polynomial (i.e. f is a polynomial) time complexity form the well-known class NP (P). Problems of NP are exactly those ones for which there is a deterministic algorithm of polynomial time complexity verifying the correctness of their solutions. The class P is considered as the class of tractable problems. Algorithms of complexities greater than polynomial are considered as unusable.

Suppose one evaluation of any fundamental operation $f \in F$ represents one computational step. From the above considerations it follows that by the conventional approach to solving our problem we have to verify the substitution property for $\pi(m-l)$ equivalence relations. In the case of regular algebras a little work can be saved, we have only $\pi(m-l) - \pi'(m-l)$ equivalences to test. It is clear that in none of these cases the computational time complexity is polynomial (it is much greater). On the contrary, for algebras from regular and permutable varieties a polynomial number of computational steps is enough. We have

Theorem 3. *$p \in NP$, $p_{\mathcal{V}} \in P$.*

References

[1] R. Bělohlávek: A characterization of congruence classes of quasigroups, *submitted.*

[2] I. Chajda: Regularity and permutability of congruences, *Algebra Univ.* **17**(1983), 170-173.

[3] J. Duda: Mal'cev conditions for regular and weakly regular subalgebras of the square, *Acta Sci. Math.* (Szeged) **46**(1983), 29-34.

[4] R. P. Grimaldi: *Discrete and combinatorial mathematics*, 3rd ed. Addison-Wesley, 1994.

[5] A. I. Mal'cev: On the general theory of algebraic systems (Russian), *Matem. Sbornik* **35**(1954), 3-20.

[6] H. Werner: A Mal'cev condition on admissible relations, *Algebra Univ.*, **3**(1973), 263.