Radim Bělohlávek

A characterization of congruence classes of quasigroups

Mathematica Slovaca, Vol. 50 (2000), No. 4, 377--380

Persistent URL: http://dml.cz/dmlcz/130560

Math. Slovaca, **50** (2000), No. 4, 377–380

Mathematica Slovaca

A CHARACTERIZATION OF CONGRUENCE CLASSES OF QUASIGROUPS

RADIM BĚLOHLÁVEK

(*Communicated by Tibor Katriňák*)

ABSTRACT. The property of being a congruence class for a subset of a quasigroup is characterized by the notion of closedness under terms. The presented characterization is of polynomial time complexity.

There are various ways to introduce the concept of a normal subgroup. One of them uses the notion of closedness under certain group terms. A nonempty subset N of a group G is a normal subgroup (and hence a congruence class containing the unit e) if and only if it is closed under the terms $p_1(y_1, y_2) = y_1 \cdot y_2^{-1}$, $p_2(x_1, y_1) = x_1 \cdot y_1 \cdot x_1^{-1}$ in the following sense. Whenever we substitute arbitrary element $a \in G$ for x_1 and arbitrary elements $b_1, b_2 \in N$ for y_1 and y_2 the result will be in N.

In what follows we give a similar characterization of congruence classes of quasigroups. By a quasigroup (cf. [1]) we mean an algebra Q endowed with three binary operations $\cdot$, $\backslash$ and $/$ which satisfy the following identities:

$$x \cdot (x\backslash y) = y \qquad (y/x) \cdot x = y\,,$$
$$x\backslash(x \cdot y) = y \qquad (y \cdot x)/x = y\,.$$

As the operations $/$ and $\backslash$ can be interpreted as right and left division, the quasigroup can be viewed as a uniquely two-sidedly divisible and cancelable groupoid.

Given a quasigroup term p in variables x_i and y_j, $p = p(x_1, \dots, x_n, y_1, \dots \dots, y_m)$, we say that a subset C of a quasigroup Q is *y-closed under p* if for all $a_1, \dots, a_n \in Q$, $c_1, \dots, c_m \in C$ we have $p(a_1, \dots, a_n, c_1, \dots, c_m) \in C$.

2000 Mathematics Subject Classification: Primary 08A30, 20N05.
Key words: quasigroup, congruence class, time complexity.

THEOREM. *A nonempty subset C of a quasigroup Q is a class of some congruence relation on Q if and only if it is y-closed under the following terms:*

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

Proof. Let C be a class of some congruence relation, say θ, i.e. $C=[c]_\theta$ for $c\in C$. Let a_1,a_2 be in Q, c_1,c_2,c_3 in C. By the substitution property of θ we have

$$\langle p_1(a_1,a_2,c_1,c_2,c_3),p_1(a_1,a_2,c,c,c)\rangle\in\theta\,.$$

Since $p_1(a_1,a_2,c,c,c)=c$ we have $p_1(a_1,a_2,c_1,c_2,c_3)\in[c]_\theta=C$, i.e. C is y-closed under p_1. One can similarly prove the y-closedness under the other terms.

Conversely, let C be y-closed under the terms mentioned above, and let $c\in C$. We shall show that the relation θ defined by

$$\langle x,y\rangle\in\theta \iff y/(c\backslash x)\in C$$

is a congruence relation on Q with a class C. It is well-known that the variety of all quasigroups is congruence-permutable. Following [4], it is enough to prove the reflexivity and the substitution property of θ. For any $a\in Q$ we have $a/(c\backslash a)=c\in C$, proving reflexivity of θ. Suppose $\langle a_1,a_2\rangle\in\theta$, $\langle b_1,b_2\rangle\in\theta$. By definition of θ, $a_2/(c\backslash a_1)\in C$ and $b_2/(c\backslash b_1)\in C$. Since C is y-closed under p_1, we have

$$p\big(a_2,b_2,a_2/(c\backslash a_1),b_2/(c\backslash b_1),c\big)\in C\,.$$

On the other hand,

$$p\big(a_2,b_2,a_2/(c\backslash a_1),b_2/(c\backslash b_1),c\big)=(a_2b_2)/\big(c\backslash(a_1b_1)\big)\,.$$

which gives $\langle a_1b_1,a_2b_2\rangle\in\theta$, proving the substitution property of the operation $\cdot$. Analogously, the terms p_2 and p_3 ensure that $\langle a_1/b_1,a_2/b_2\rangle\in\theta$ and $\langle a_1\backslash b_1,a_2\backslash b_2\rangle\in\theta$, i.e. θ is a congruence relation.

It remains to prove $C=[c]_\theta$. From $c'\in C$ it follows that

$$c/(c\backslash c')=p_4(c,c,c')\in C\,,$$

i.e. $\langle c', c\rangle \in \theta$ which means $C \subseteq [c]_\theta$. If, conversely, $c' \in [c]_\theta$, we have $\langle c, c'\rangle \in \theta$, thus $c'' = c'/(c\backslash c) \in C$. But then $c' = c''(c\backslash c) = p_5(c'', c, c) \in C$, hence $[c]_\theta \subseteq C$. We have proved C is a class of the congruence relation θ. □

Remark 1. A useful characterization of congruence classes of algebras was given by Mal'cev, see [3]: For an algebra (A, F) and a subset $C \subseteq A$, C is a class of some congruence relation if and only if $\tau(C) \cap C = \emptyset$ or $\tau(C) \subseteq C$ holds for any translation (i.e. unary algebraic function) τ of A. This characterization yields an infinite number of polynomials even in the case of a finite algebra with finite similarity type. In the case of a quasigroup, our Theorem gives only a finite number of translations to testify in the Mal'cev characterization.

Remark 2. Call the group $\mathcal{M}(Q)$ of permutations of a quasigroup Q generated by all $R_a, L_a \colon Q \to Q$, $R_a(x) = x \cdot a$, $L_a(x) = a \cdot x$, $a \in Q$, the group associated to Q ([1], [2]). For $e \in Q$, the permutation $p \in \mathcal{M}(Q)$ is called an e-inner permutation if $p(e) = e$. Congruence classes of quasigroups (called normal subsets of quasigroups) are characterized in [2] as follows: If $C \subseteq Q$, $e \in C$, then C is a class of some congruence on Q if and only if

(i) any e-inner permutation $p \in \mathcal{M}(Q)$ maps C into C (i.e. $p(C) \subseteq C$),
(ii) if $(a/e) \cdot b = c$ and any two of the elements a, b, c belong to C, then the third one belongs to C.

Note that this result, like that of Mal'cev, yields possibly infinite number of functions (e-inner permutations) to testify, i.e. it does not give a finite list.

Remark 3. From the computational complexity point of view we deal with the following problem: Decide whether for a given finite quasigroup and its subset C, C is a congruence class of Q. The conventional approach, i.e. testing all relevant partitions of Q, leads to an algorithm of exponential time complexity with respect to card Q. It is easy to see that by Theorem, a polynomial number of steps is sufficient. Hence the problem is in P, the class of problems solvable in polynomial time.

Acknowledgement

The author would like to thank to the anonymous referee for calling his attention to [2].

REFERENCES

[1] BRUCK, R. H.: *A Survey of Binary Systems*, Springer Verlag, Berlin-Göttingen-Heidelberg, 1971.
[2] JEŽEK, J.: *Normal subsets of quasigroups*, Comment. Math. Univ. Carolin. **16** (1975), 77–85.
[3] MAL'CEV, A. I.: *On the general theory of algebraic systems*, Mat. Sb. **35** (1954), 3–20.
[4] WERNER, H.: *A Mal'cev condition on admissible relations*, Algebra Universalis **3** (1973), 263.

Received March 14, 1997
Revised December 16, 1998

Dept. Comput. Sci.
Technical University of Ostrava
Tř. 17. listopadu
CZ–708 33 Ostrava
CZECH REPUBLIC
E-mail: radim.belohlavek@vsb.cz