EVERY QUASIGROUP IS ISOMORPHIC TO A SUBDIRECTLY IRREDUCIBLE QUASIGROUP MODULO ITS MONOLITH

RALPH MCKENZIE AND DAVID STANOVSKÝ

Abstract. Every quasigroup (loop, Bol loop, group, respectively) is isomorphic to the factor of a subdirectly irreducible quasigroup (loop, Bol loop, group, respectively) over its monolithic congruence.

1. Introduction

An algebra is subdirectly irreducible, if and only if the intersection of its non-zero congruences, called the *monolith*, is non-zero. T. Kepka (in [5]) asked for a characterization of those algebras that are isomorphic to a quotient of a subdirectly irreducible algebra, or to the quotient of a subdirectly irreducible algebra over its monolithic congruence.

Kepka's questions were answered by T. Kepka and J. Ježek [3] and independently by D. Stanovský [7]. To explain their results, we need the following notation. For a class $\mathcal{K}$ of algebras, we use $\mathcal{K}_{SI}$ to denote the subclass of all subdirectly irreducible algebras from $\mathcal{K}$. Then $\mathrm{H}(\mathcal{K}_{SI})$ consists of those algebras that are isomorphic to a quotient of a subdirectly irreducible algebra from $\mathcal{K}$. We use $\mathrm{H}_\mu(\mathcal{K}_{SI})$ to denote the class of algebras that are isomorphic to an algebra that is the factor of a subdirectly irreducible algebra from $\mathcal{K}$ by its monolith.

The results of T. Kepka and J. Ježek, and of D. Stanovský are: If $\mathcal{K}$ is the variety of all algebras of a type τ containing at least one at least binary symbol, then $\mathrm{H}(\mathcal{K}_{SI}) = \mathrm{H}_\mu(\mathcal{K}_{SI})$ and this class consists of those algebras $\mathbf{A}$, for which the collection of all ideals of $\mathbf{A}$ has non-empty intersection. By an ideal of $\mathbf{A}$ we mean here a non-empty subset $I \subseteq A$ such that $f(a_1, \dots, a_n) \in I$ for every n-ary basic operation f $(n \geq 1)$ and for every $a_1, \dots, a_n \in A$ with $a_i \in I$ for at least one i. A similar characterization of $\mathrm{H}(\mathcal{K}_{SI})$ was found later for the class $\mathcal{K}$ of finite unary algebras by J. Ježek, P. Marković and D. Stanovský in [4]. However, $\mathrm{H}(\mathcal{K}_{SI}) \neq \mathrm{H}_\mu(\mathcal{K}_{SI})$ in this case.

Date: October 14, 2005.

1991 *Mathematics Subject Classification.* 20N05, 08B26.

Key words and phrases. subdirectly irreducible, quasigroup, loop, wreath product.

The work is a part of the research project MSM 0021620839 financed by MŠMT ČR. The first author was supported by US NSF Grant No. DMS–0245622. The second author was partly supported by the Grant Agency of the Czech Republic, grant #201/05/0002.

It can be interesting to ask Kepka's questions relative to a specific variety $\mathcal{V}$: characterize $\mathrm{H}(\mathcal{V}_{SI})$ and $\mathrm{H}_\mu(\mathcal{V}_{SI})$. In some cases, this leads to the same results as above. In varieties $\mathcal{V}$ where algebras possess no proper ideals, one finds a way to construct, given any algebra $\mathbf{G} \in \mathcal{V}$, a subdirectly irreducible algebra $\mathbf{H} \in \mathcal{V}$ with $\mathbf{G}$ isomorphic to $\mathbf{H}$ over its monolith. In this paper, for example, we do precisely that for these varieties: all groups, all quasigroups, all loops, all Bol loops. We can remark that R. Freese (unpublished) achieved the same result for lattices. S. Bulman-Fleming, E. Hotzel and J. Wang [1] found for every semigroup $\mathbf{S}$ with a non-empty intersection of semigroup ideals a subdirectly irreducible *semigroup* $\mathbf{T}$ with monolith μ such that $\mathbf{S} \simeq \mathbf{T}/\mu$. Finally, we remark that the construction from [7] yields for a binary algebra $\mathbf{G}$ with non-empty intersection of ideals, satisfying an equation of the form $t(x) \approx x$, a subdirectly irreducible algebra $\mathbf{H}$ satisfying the same equation, with $\mathbf{G}$ isomorphic to $\mathbf{H}$ over its monolith.

The situation is quite different for the variety $\mathcal{A}$ of Abelian groups. It is well known that every subdirectly irreducible abelian group is isomorphic to some Prüfer group $\mathbb{Z}_{p^k}$ for a prime p and some $k \in \{1, 2, \dots, \infty\}$. Hence $\mathrm{H}(\mathcal{A}_{SI}) = \mathrm{H}_\mu(\mathcal{A}_{SI}) = \mathcal{A}_{SI}$.

2. Results

We recall that a *quasigroup* is an algebra $\langle G, \cdot, /, \backslash \rangle$ satisfying the equations

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

A *loop* is a quasigroup with a constant e (the *unit element*) such that $e \cdot x \approx x \cdot e \approx x$. Groups can be regarded as loops, setting $x/y = x \cdot y^{-1}$ and $x\backslash y = x^{-1} \cdot y$. (An introduction to the theory of quasigroups and loops can be found in [2],[6]). A *Bol loop* is a loop satisfying the equation $x \cdot (y \cdot (x \cdot z)) \approx (x \cdot (y \cdot x)) \cdot z$. A *Moufang loop* is a loop satisfying the equation $x \cdot (y \cdot (x \cdot z)) \approx ((x \cdot y) \cdot x) \cdot z$. Note that every Moufang loop is a Bol loop.

Notice that quasigroups contain no proper ideals, hence every quasigroup is a homomorphic image of a subdirectly irreducible algebra, by the aforementioned results of [3], [7]. Our main result is the following theorem.

Theorem 1. *Every quasigroup* $\mathbf{G}$ *is isomorphic to the factor of a subdirectly irreducible quasigroup* $\mathbf{H}$ *over its monolithic congruence. If* $\mathbf{G}$ *is a loop (a Bol loop, a group, respectively), then* $\mathbf{H}$ *can be a loop (a Bol loop, a group, respectively). If* $\mathbf{G}$ *is finite, then* $\mathbf{H}$ *can be chosen finite.*

In other words,

$$\mathrm{H}_\mu(\mathcal{V}_{SI}) = \mathrm{H}(\mathcal{V}_{SI}) = \mathcal{V},$$

where $\mathcal{V}$ is the class of all (finite, respectively) quasigroups, loops, Bol loops or groups.

We prove Theorem 1 with the following construction. Let $\mathbf{G} = \langle G, \cdot, \backslash, / \rangle$ be a quasigroup. We choose any simple non-Abelian group $\mathbf{S}$, say the sixty-element alternating group on five letters. Consider $\mathbf{S}$ as a quasigroup $\langle S, \cdot, \backslash, / \rangle$ and form the extension $\mathbf{H} = \mathbf{S}^{(G)} \rtimes \mathbf{G}$ of $\mathbf{S}^{(G)}$ by $\mathbf{G}$. Here $\mathbf{S}^{(G)}$ is the subgroup of the direct power $\mathbf{S}^G$ consisting of the functions $f \in S^G$ of finite support (i.e., $f(x) = 1$ for all but finitely many $x \in G$) and the set H is identical with $S^{(G)} \times G$. The operations in $\mathbf{H}$ are defined by

$$\begin{aligned}
(f, c) \cdot (g, d) &= (f \cdot (g \circ L_c), c \cdot d)\,,\\
(f, c)/(g, d) &= (f \cdot (g^{-1} \circ L_{c/d}), c/d)\,,\\
(f, c)\backslash(g, d) &= ((f^{-1} g) \circ L_c^{-1}, c\backslash d)\,,
\end{aligned}$$

where $L_c : G \to G$ is $L_c(x) = c \cdot x$. In the formulas above, f^{-1}, g^{-1} denote the multiplicative inverses of the elements f, g in the group $\mathbf{S}^{(G)}$, while L_c^{-1} denotes the inverse of the function L_c in the group of permutations of G.

Lemma 2. $\mathbf{H}$ *is a quasigroup. If* $\mathbf{G}$ *is, respectively, a loop, a Bol loop, a group then* $\mathbf{H}$ *is, too.*

Proof. Note that $(f \cdot g) \circ L_c = (f \circ L_c) \cdot (g \circ L_c)$. The calculations below show that the equations defining quasigroups are valid in $\mathbf{H}$.

$$\begin{aligned}
((f, c) \cdot (g, d))/(g, d) &= (f \cdot (g \circ L_c) \cdot (g^{-1} \circ L_{(c\cdot d)/d}), (c \cdot d)/d) = (f, c)\,,\\
((f, c)/(g, d)) \cdot (g, d) &= (f \cdot (g^{-1} \circ L_{c/d}) \cdot (g \circ L_{c/d}), (c/d) \cdot d) = (f, c)\,,\\
(f, c)\backslash((f, c) \cdot (g, d)) &= ((f^{-1} \cdot f \cdot (g \circ L_c)) \circ L_c^{-1}, c\backslash(c \cdot d)) = (g, d)\,,\\
(f, c) \cdot ((f, c)\backslash(g, d)) &= (f \cdot ((f^{-1} g) \circ L_c^{-1} \circ L_c), c \cdot (c\backslash d)) = (g, d)\,.
\end{aligned}$$

If $\mathbf{G}$ is a group, then $\mathbf{H}$ is an ordinary wreath product, hence $\mathbf{H}$ is a group. If e is a unit in $\mathbf{G}$, then $(1, e)$ is a unit in $\mathbf{H}$, because L_e is the identity. Thus if $\mathbf{G}$ is a loop then $\mathbf{H}$ is a loop.

The calculation to show that if $\mathbf{G}$ satisfies the Bol equation, then $\mathbf{H}$ does likewise, is elementary and we leave it to the reader. □

Let η_2 be the kernel of the projection of $\mathbf{H}$ onto $\mathbf{G}$.

Lemma 3. $\mathbf{H}$ *is subdirectly irreducible,* η_2 *is its monolithic congruence, and* $\mathbf{G} \cong \mathbf{H}/\eta_2$.

We remark that $\mathbf{H}$ is never commutative, and it can be easily shown that $\mathbf{H}$ satisfies $x \cdot (y \cdot x) \approx (x \cdot y) \cdot x$ (the alternative law) if and only if $\mathbf{G}$ is a group. Thus we leave open the following questions. Is every commutative quasigroup isomorphic to a quotient of a subdirectly irreducible commutative quasigroup (over its monolith)? Is every Moufang loop isomorphic to a factor (over its monolith) of a subdirectly irreducible Moufang loop?

Proof. The projection of $\mathbf{H}$ onto $\mathbf{G}$ is evidently a homomorphism, thus $\mathbf{G} \cong \mathbf{H}/\eta_2$. It remains to show that η_2 is the smallest non-zero congruence of $\mathbf{H}$.

We will need the following observations. Let $\sim$ be any congruence of $\mathbf{H}$. For any $f,g,h,k \in S^{(G)}$ and $a,b,c,d \in G$ we have:

$$
\begin{array}{lll}
(1)\ (f,a) \sim (g,b) & \Leftrightarrow & (f \circ L_d, d \cdot a) \sim (g \circ L_d, d \cdot b) \\
 & & \text{[multiplication by } (1,d) \text{ on the left]} \\
(2)\ (f,a) \sim (g,b) & \Leftrightarrow & (kf,a) \sim (kg,b) \\
 & & \text{[multiplication by } (k \circ L_d, d) \text{ on the left, and (1)]} \\
(3)\ (f,a) \sim (g,b) & \Leftrightarrow & (f, a \cdot c) \sim (g, b \cdot c) \\
 & & \text{[multiplication by } (1,c) \text{ on the right]} \\
(4)\ (f,a) \sim (g,b) & \Leftrightarrow & (fh,a) \sim (g(h \circ L_a^{-1} \circ L_b), b) \\
 & & \text{[multiplication by } (h \circ L_a^{-1}, c) \text{ on the right, and (3)]} \\
(5)\ (f,a) \sim (g,a) & \Leftrightarrow & (fh,a) \sim (gh,a) \\
 & & [(4),\ a=b]\,.
\end{array}
$$

Now, let $\sim$ be any non-zero congruence of $\mathbf{H}$. We shall prove that $\sim$ contains η_2.

First we show that $\sim \cap \eta_2$ is a non-zero congruence. (This will allow us to assume that $\sim \subseteq \eta_2$.) To see this, let $(f,a) \sim (g,b)$ where $f \neq g$ or $a \neq b$. If $a = b$, we indeed have that $\sim \cap \eta_2$ is non-zero, as claimed. So assume that $a \neq b$. Observation (2) above implies that $(1,a) \sim (f^{-1}g, b)$. Next, an application of (4) for h and (2) for $k = h^{-1}$ yields that

$$(1,a) \sim (h^{-1}f^{-1}g(h \circ L_a^{-1} \circ L_b), b)$$

and hence

$$(f^{-1}g, b) \sim (h^{-1}f^{-1}g(h \circ L_a^{-1} \circ L_b), b)$$

for all $h \in S^{(G)}$. Let $x \in G$. Then

$$h^{-1}f^{-1}g(h \circ L_a^{-1} \circ L_b)(x) = h(x)^{-1}f(x)^{-1}g(x)h(a\backslash(b \cdot x))\,.$$

Since $a \neq b$ implies that $x \neq a\backslash(b\cdot x)$, there exists $h_0 \in S^{(G)}$ such that $h_0(x) = 1$ and $h_0(a\backslash(b\cdot x)) \neq 1$. Hence $f^{-1}g \neq h_0^{-1}f^{-1}g(h_0 \circ L_a^{-1} \circ L_b)$ and the second displayed formula above shows that $\sim \cap \eta_2$ is a non-zero congruence.

For the remainder of this proof, we assume that $\sim \subseteq \eta_2$ (or replace $\sim$ by $\sim \cap \eta_2$). First we note that, for any $f,g \in S^{(G)}$, $(f,a) \sim (g,a)$ for some $a \in G$, if and only if $(f,a) \sim (g,a)$ for all $a \in G$. (This follows by observation (3).) Hence, with the help of observations (2) and (5), we see that the group $\mathbf{S}^{(G)}$ has a non-zero congruence δ characterized by:

$$(f,g) \in \delta \text{ iff } (f,a) \sim (g,a) \text{ for some (all) } a \in G.$$

Moreover, this congruence is invariant under the group of automorphisms of $\mathbf{S}^{(G)}$ induced by the left-translations L_a, $a \in G$ — i.e., $(f,g) \in \delta$ iff $(f \circ L_a, g \circ L_a) \in \delta$ whenever $a \in G$. (This follows by observation (1).) A standard group-theoretic argument shows that, since $\mathbf{S}$ is simple and non-Abelian and the L_a act transitively on G, then δ must be the universal congruence of $\mathbf{S}^{(G)}$. This means that $\sim\ = \eta_2$, as required. Thus our proof of Lemma 3 is complete. $\square$

Acknowledgement. The authors thank the referee for reading the paper with a critical eye and contributing to a substantial improvement of it. Especially, we thank the referee for supplying the proof of Lemma 3 given here. Our original proof was long and awkward; and to make it work, we had made the assumption (unnecessarily, as our referee showed) that $|\mathbf{S}| > (|\,G|^2)\,!$.

References

[1] S. Bulman-Fleming, E. Hotzel and J. Wang, *Semigroups that are factors of subdirectly irreducible semigroups by their monolith.* Algebra Universalis **51** (2004), 1–7.
[2] O. Chein, H. O. Pflugfelder, J. D. H. Smith (eds.), *Quasigroups and loops: theory and applications.* Heldermann Verlag, 1990.
[3] J. Ježek and T. Kepka, *The factor of a subdirectly irreducible algebra through its monolith.* Algebra Universalis **47** (2002), 319–327.
[4] J. Ježek, P. Marković and D. Stanovský, *Homomorphic images of finite subdirectly irreducible unary algebras.* Submited.
[5] T. Kepka, *A note on subdirectly irreducible groupoids.* Acta Univ. Carolinae Math. Phys. **22/1** (1981), 25–28.
[6] H. O. Pflugfelder, *Quasigroups and loops: introduction.* Heldermann Verlag, 1990.
[7] D. Stanovský, *Homomorphic images of subdirectly irreducible groupoids.* Comment. Math. Univ. Carolinae **42/3** (2001), 443–450.

Ralph McKenzie, Department of Mathematics, Vanderbilt University, Nashville, TN, U.S.A.
E-mail address: mckenzie@math.vanderbilt.edu

David Stanovský, Charles University in Prague, Czech Republic
E-mail address: stanovsk@karlin.mff.cuni.cz