Another characterization of congruence distributive varieties

PAOLO LIPPARINI

Abstract. We provide a Maltsev characterization of congruence distributive varieties by showing that a variety \( V \) is congruence distributive if and only if the congruence identity \( \alpha \cap (\beta \circ \gamma \circ \beta) \subseteq \alpha \beta \circ \gamma \circ \alpha \beta \circ \gamma \cdots \) (\( k \) factors) holds in \( V \), for some natural number \( k \).

July 2, 2019

We assume the reader is familiar with basic notions of lattice theory and of universal algebras. A small portion of [9] is sufficient as a prerequisite.

A lattice is distributive if and only if it satisfies the identity \( \alpha (\beta + \gamma) \leq \alpha \beta + \gamma \). It follows that an algebra \( A \) is congruence distributive if and only if, for all congruences \( \alpha, \beta \) and \( \gamma \) of \( A \) and for every \( h \), the inclusion \( \alpha (\beta \circ h \gamma) \subseteq \alpha \beta + \gamma \) holds. Here juxtaposition denotes intersection, + is join and \( \beta \circ h \gamma \) is \( \beta \circ \gamma \circ \beta \circ \gamma \cdots \) with \( h \) factors (\( h - 1 \) occurrences of \( \circ \)).

Considering now a variety \( V \), it follows from standard arguments in the theory of Maltsev conditions that \( V \) is congruence distributive if and only if, for every \( h \), there is some \( k \) such that the congruence identity

\[
\alpha (\beta \circ h \gamma) \subseteq \alpha \beta \circ k \gamma
\]

holds in \( V \). The naive expectation (of course, motivated by [4]) that the congruence identity

\[
\alpha (\beta \circ \gamma) \subseteq \alpha \beta \circ k \gamma
\]

is enough to imply congruence distributivity is false. Indeed, by [3, Theorem 9.11], a locally finite variety \( V \) satisfies (2) if and only if \( V \) omits types 1, 2, 5. More generally, with no finiteness assumption, Kearnes and Kiss [6, Theorem 8.14] proved that a variety \( V \) satisfies (2) if and only if \( V \) is join congruence semidistributive. Many other interesting equivalent conditions are presented in [3, 6].

In spite of the above results, we show that the next step is enough, namely, if we take \( h = 3 \) in identity (1), we get a condition implying congruence distributivity. After a short elementary proof relying on [1, 4], in Remark 3...
we sketch an alternative argument which relies only on \cite{7}. Then, by working directly with the terms associated to the Maltsev condition arising from \cite{11} for \( h = 3 \), we show that this instance of \cite{11} implies \( \alpha(\beta \circ \gamma) \subseteq \alpha \beta \circ \gamma \), for some \( r < k^2 \).

**Theorem 1.** A variety \( \mathcal{V} \) is congruence distributive if and only if the identity

\[
\alpha(\beta \circ \gamma) \subseteq \alpha \beta + \gamma
\]

holds in every congruence lattice of algebras in \( \mathcal{V} \).

**Proof.** If \( \mathcal{V} \) is congruence distributive, then \( \alpha(\beta \circ \gamma) \subseteq \alpha(\beta + \gamma) \leq \alpha \beta + \gamma \).

For the nontrivial direction, assume that \( (3) \) holds in \( \mathcal{V} \). By taking \( \alpha \gamma \) in place of \( \gamma \) in \( (3) \) we get \( \alpha(\beta \circ \alpha \gamma \circ \beta) \subseteq \alpha \beta + \gamma \). \cite{11} has showed that this identity implies congruence modularity within a variety. From \( (3) \) and congruence modularity we get \( \alpha(\beta \circ \gamma) \subseteq \alpha(\alpha \beta + \gamma) = \alpha \beta + \alpha \gamma \) and, since trivially \( \alpha(\beta \circ \gamma) \subseteq \alpha(\beta \circ \gamma) \), we obtain \( \alpha(\beta \circ \gamma) \subseteq \alpha \beta + \alpha \gamma \). Within a variety this identity implies congruence distributivity by \cite{4}. \( \square \)

It is standard to express Theorem 1 in terms of a Maltsev condition.

**Corollary 2.** A variety \( \mathcal{V} \) is congruence distributive if and only if there is some \( k \) such that any one of the following equivalent conditions hold.

(i) \( \mathcal{V} \) satisfies the congruence identity

\[
\alpha(\beta \circ \gamma) \subseteq \alpha \beta \circ_k \gamma.
\]

(ii) The identity \cite{11} holds in \( \mathcal{F}_V(4) \), the free algebra in \( \mathcal{V} \) generated by four elements \( x, y, z, w \); actually, it is equivalent to assume that \cite{11} holds in \( \mathcal{F}_V(4) \) in the special case when when \( \alpha = Cg(x, w) \), \( \beta = Cg((x, y), (z, w)) \) and \( \gamma = Cg(y, z) \).

(iii) \( \mathcal{V} \) has 4-ary terms \( d_0, \ldots, d_k \) such that the following equations are valid in \( \mathcal{V} \):

\[
\begin{align*}
(a) \quad x &= d_0(x, y, z, w); \\
(b) \quad d_i(x, x, w, w) &= d_{i+1}(x, x, w, w), \text{ for } i \text{ even}; \\
(c) \quad d_i(x, y, z, x) &= d_{i+1}(x, y, z, x), \text{ for } i \text{ even}; \\
(d) \quad d_i(x, y, y, w) &= d_{i+1}(x, y, y, w), \text{ for } i \text{ odd, and} \\
(e) \quad d_k(x, y, z, w) &= w.
\end{align*}
\]

**Proof.** (i) \( \Rightarrow \) (ii) is trivial; (ii) \( \Rightarrow \) (iii) and (iii) \( \Rightarrow \) (i) are standard; for example, there is no substantial difference with respect to \cite{11}. See, e. g., \cite{2, 5, 8} for further details, or \cite{10, 11} for a more general form of the arguments. Thus we have that (i) - (iii) are equivalent, for every \( k \).

Clearly congruence distributivity implies the second statement in (ii), for some \( k \); moreover identity \cite{11} in (i) implies identity \cite{4}, hence congruence distributivity follows from Theorem 1. \( \square \)

**Remark 3.** It is possible to give a direct proof that clause (i) in Corollary 2 implies congruence distributivity by using a theorem from \cite{7} and without
resorting to [1][4]. By [7] Theorem 3 (i) ⇒ (iii), a variety $\mathcal{V}$ satisfies identity (4) for congruences if and only if $\mathcal{V}$ satisfies the same identities when $\alpha$, $\beta$ and $\gamma$ are representable tolerances. A tolerance $\Theta$ is representable if it can be expressed as $\Theta = R \circ R^{-}$, for some admissible relation $R$, where $R^{-}$ denotes the converse of $R$. To show congruence distributivity, notice that the relation $\Delta_m = \beta \circ m \gamma$ is a representable tolerance, for every odd $m$. By induction on $m$, it is easy to see that the identity (4), when interpreted for representable tolerances, implies $\alpha(\Delta_m \circ \gamma \circ \Delta_m) \subseteq \alpha \beta \circ \gamma$, for every odd $m$ and some appropriate $p$ depending on $m$. In particular, we get that, for every $h$, there is some $p$ such that

$$\alpha(\beta \circ_h \gamma) \subseteq \alpha \beta \circ_p \gamma,$$

hence also $\alpha(\beta \circ_h \gamma) \subseteq \alpha(\alpha \beta \circ_p \gamma) = \alpha \beta \circ \alpha(\gamma \circ_{p-1} \alpha \beta)$. Taking now $\gamma$ in place of $\beta$, $\alpha \beta$ in place of $\gamma$ and $p-1$ in place of $h$ in (4), we get $\alpha(\gamma \circ_{p-1} \alpha \beta) \subseteq \alpha \gamma \circ_q \alpha \beta$, for some $q$, thus $\alpha(\beta \circ_h \gamma) \subseteq \alpha \beta \circ_{q+1} \alpha \gamma$. Compare [8] for corresponding arguments. If one works out the details, one obtains that if $k \leq 2^p$, $p \geq 1$ and $\ell \geq 2$, then identity (4) implies $\alpha(\beta \circ_{2\ell-1} \gamma) \subseteq \alpha \beta \circ_{2s+1} \alpha \gamma$, with $s = (p - 1)^2(\ell - 1) + 1$, a rather large number of factors on the right.

We are now going to show that we can obtain a lighter bound on the right using different methods.

Remark 4. Notice that if some sequence of terms satisfies Clause (iii) in Corollary 2 then the terms satisfy also

$$x = d_i(x, y, y, x),$$

for every $i \leq k$.

This follows immediately by induction from (a), (c) and (d). From the point of view of congruence identities, this corresponds to taking $\alpha \gamma$ in place of $\gamma$ in [4], as we did in the proof of Theorem 1. At the level of Maltsev conditions, this gives a proof that Clause (iii) in Corollary 2 implies congruence modularity, since the argument shows that the terms $d_0, \ldots, d_k$ obey Day’s conditions [1] for congruence modularity.

Theorem 5. If some variety $\mathcal{V}$ satisfies the congruence identity (4) $\alpha(\beta \circ \gamma \circ \beta) \subseteq \alpha \beta \circ_k \gamma$, for some $k \geq 3$, then $\mathcal{V}$ satisfies

$$\alpha(\beta \circ \gamma \circ \beta) \subseteq \alpha \beta \circ_r \alpha \gamma,$$

where $r = \frac{k^2 - 4k + 9}{2}$ for $k$ odd, and $r = \frac{k^2 - 4k + 4}{2}$ for $k$ even.

Proof. By Corollary 2 we have terms as given by (iii). Suppose that $(a, d) \in \alpha(\beta \circ \gamma \circ \beta)$ in some algebra in $\mathcal{V}$. Thus $a \alpha d$ and $a \beta \gamma c \beta d$, for certain elements $b$ and $c$. We claim that

$$(d_i(a, b, b, d), d_{i+2}(a, b, b, d)) \in \alpha(\gamma \circ \alpha \beta \circ \gamma),$$

for every odd index $i < k - 1$. Indeed,

$$d_i(a, b, b, d) \alpha d_i(a, b, b, a) = a = d_{i+2}(a, b, b, a) \alpha d_{i+2}(a, b, b, d),$$

by (f) in the above remark. Moreover, still assuming $i$ odd,
\[ d_{i+1}(a, b, c, d) \beta d_{i+1}(a, a, d, d) = d_{i+2}(a, a, d, d) \beta d_{i+2}(a, b, c, d), \] and
\[ d_{i+1}(a, b, c, d) \alpha d_{i+1}(a, b, c, a) = d_{i+2}(a, b, c, a) \alpha d_{i+2}(a, b, c, d), \] hence
\[ d_i(a, b, b, d) = d_{i+1}(a, b, b, d) \gamma d_{i+1}(a, b, c, d) \alpha \beta d_{i+2}(a, b, c, d) \gamma d_{i+2}(a, b, b, d), \] thus (1) follows. From (1) and (4) with \( \gamma \) in place of \( \beta \) and \( \alpha \beta \) in place of \( \gamma \), we get
\[ (d_i(a, b, b, d), d_{i+2}(a, b, b, d)) \in \alpha \gamma \circ_k \alpha \beta, \]
for every odd index \( i \).

Arguing as above, \( a \alpha \beta d_1(a, b, c, d) \alpha \gamma d_1(a, b, b, d) \). If \( k \) is odd, then
\[ d_{k-2}(a, b, b, d) = d_{k-1}(a, b, b, d) \alpha \beta d_{k-1}(a, a, d, d) = d_k(a, a, d, d) = d, \] thus the elements \( d_1(a, b, b, d), d_3(a, b, b, d), \ldots, d_{k-2}(a, b, b, d) \) witness \( (a, d) \in \alpha \beta \circ (\alpha \gamma \circ_k \alpha \beta) \). On the other hand, if \( k \) is even, then \( d_{k-1}(a, b, b, d) = d_k(a, b, b, d) = d. \) Moreover, since \( d_1(a, b, c, d) \alpha \gamma d_1(a, b, b, d) \), we have \( (d_1(a, b, c, d), d_3(a, b, b, d)) \in \alpha (\alpha \beta \circ \alpha \gamma) \), hence we can consider \( d_1(a, b, c, d) \) in place of \( d_1(a, b, b, d) \). We can consider the converse of (1) and, since \( k \) is even, we get \( (d_1(a, b, c, d), d_3(a, b, b, d)) \in \alpha \beta \circ_k \alpha \gamma \).

We can go on the same way, using alternatively (1) and its converse, getting
\[ (a, d) \in (\alpha \beta \circ_k \alpha \gamma) \circ_{k-2} (\alpha \gamma \circ_k \alpha \beta) = \alpha \beta \circ \alpha \gamma, \]
for \( r = \frac{k^2 - 3k + 4}{2} \).

We expect that the evaluation of \( r \) in Theorem 5 can be further improved, but we have no guess as to what extent.

References
[1] A. Day, A characterization of modularity for congruence lattices of algebras, Canad. Math. Bull. 12, 167–173 (1969).
[2] H.-P. Gumm, Geometrical methods in congruence modular algebras, Mem. Amer. Math. Soc. 45 (1983).
[3] D. Hobby, R. McKenzie, The structure of finite algebras, emp. Math. 76 (1988).
[4] B. Jónsson, Algebras whose congruence lattices are distributive, Math. Scand. 21, 110–121 (1967).
[5] B. Jónsson, Congruence varieties, Algebra Universalis 10, 355–394 (1980).
[6] K. A. Kearnes, E. W. Kiss, The shape of congruence lattices, Mem. Amer. Math. Soc. 222 (2013).
[7] P. Lipparini, From congruence identities to tolerance identities, Acta Sci. Math. (Szeged) 73, 31–51 (2007).
[8] P. Lipparini, On the number of terms witnessing congruence modularity, arXiv: 1709.06923v2, 1–23 (2017/2019).
[9] R. N. McKenzie, G. F. McNulty, W. F. Taylor, Algebras, Lattices, Varieties. Vol. I, Wadsworth & Brooks/Cole Advanced Books & Software (1987).
[10] A. Pixley, Local Mal’cev conditions, Canad. Math. Bull. 15, 559–568 (1972).
[11] R. Wille, Kongruenzzklassengeometrien, Lecture Notes in Mathematics 113 (1970).

Paolo Lipparini
Dipartimento Ulteriore di Matematica, Viale della Ricerca Scientifica, Università di Roma “Tor Vergata”, I-00133 ROME ITALY