Another characterization of congruence distributive varieties

Paolo Lipparini

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

September 29, 2019

We assume the reader is familiar with basic notions of lattice theory and of universal algebra. 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 $\mathbf{A}$ is congruence distributive if and only if, for all congruences α, β and γ of $\mathbf{A}$ and for every h, the inclusion $\alpha(\beta \circ_h \gamma) \subseteq \alpha\beta+\gamma$. holds. Here juxtaposition denotes intersection, $+$ is join in the congruence lattice and $\beta \circ_h \gamma$ is $\beta \circ \gamma \circ \beta \circ \gamma \dots$ with h factors ($h-1$ occurrences of $\circ$).

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

$$\alpha(\beta \circ_h \gamma) \subseteq \alpha\beta \circ_k \gamma \tag{1}$$

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

$$\alpha(\beta \circ \gamma) \subseteq \alpha\beta \circ_k \gamma, \quad \text{for some } k, \tag{2}$$

is enough to imply congruence distributivity is false. Indeed, by [3, Theorem 9.11], a locally finite variety $\mathcal{V}$ satisfies (2) if and only if $\mathcal{V}$ omits types **1, 2, 5**. More generally, with no finiteness assumption, Kearnes and Kiss [6, Theorem 8.14] proved that a variety $\mathcal{V}$ satisfies (2) if and only if $\mathcal{V}$ 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

2010 *Mathematics Subject Classification*: Primary 08B10; Secondary 08B05.

Key words and phrases: congruence distributive variety; Maltsev condition; congruence identity.

Work performed under the auspices of G.N.S.A.G.A. Work partially supported by PRIN 2012 "Logica, Modelli e Insiemi". The author acknowledges the MIUR Department Project awarded to the Department of Mathematics, University of Rome Tor Vergata, CUP E83C18000100006.

we sketch an alternative argument which relies only on [7]. Then, by working directly with the terms associated to the Maltsev condition arising from (1) for $h = 3$, we show that this instance of (1) implies $\alpha(\beta \circ \gamma \circ \beta) \subseteq \alpha\beta \circ_r \alpha\gamma$, for some $r < \frac{k^2}{2}$.

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

$$\alpha(\beta \circ \gamma \circ \beta) \subseteq \alpha\beta + \gamma \tag{3}$$

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

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

For the nontrivial direction, assume that (3) holds in $\mathcal{V}$. By taking $\alpha\gamma$ in place of γ in (3) we get $\alpha(\beta \circ \alpha\gamma \circ \beta) \subseteq \alpha\beta + \alpha\gamma$. Day [1] has showed that this identity implies congruence modularity within a variety. From (3) and congruence modularity we get $\alpha(\beta \circ \gamma \circ \beta) \subseteq \alpha(\alpha\beta + \gamma) = \alpha\beta + \alpha\gamma$ and, since trivially $\alpha(\beta \circ \gamma) \subseteq \alpha(\beta \circ \gamma \circ \beta)$, we obtain $\alpha(\beta \circ \gamma) \subseteq \alpha\beta + \alpha\gamma$. Within a variety this identity implies congruence distributivity by [4]. □

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*

$$\alpha(\beta \circ \gamma \circ \beta) \subseteq \alpha\beta \circ_k \gamma. \tag{4}$$

(ii) *The identity (4) holds in $\mathbf{F}_{\mathcal{V}}(4)$, the free algebra in $\mathcal{V}$ generated by four elements x, y, z, w; actually, it is equivalent to assume that (4) holds in $\mathbf{F}_{\mathcal{V}}(4)$ 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 $d_0, \dots, d_k$ such that the following equations are valid in $\mathcal{V}$:*

- *(a)* $x = d_0(x, y, z, w)$;
- *(b)* $d_i(x, x, w, w) = d_{i+1}(x, x, w, w)$, *for i even;*
- *(c)* $d_i(x, y, z, x) = d_{i+1}(x, y, z, x)$, *for i even;*
- *(d)* $d_i(x, y, y, w) = d_{i+1}(x, y, y, w)$, *for i odd, and*
- *(e)* $d_k(x, y, z, w) = w$.

Proof. (i) ⇒ (ii) is trivial; (ii) ⇒ (iii) and (iii) ⇒ (i) are standard; for example, there is no substantial difference with respect to [1]. See, e. g., [2, 5, 8] for further details, or [10, 11] for a more general form of the arguments. Thus we have that (i) - (iii) are equivalent, for any given k.

Clearly congruence distributivity implies the second statement in (ii), for some k; moreover identity (4) in (i) implies identity (3), hence congruence distributivity follows from Theorem 1. □

Remark 3. It is possible to give a direct proof that clause (i) in Corollary 2 implies congruence distributivity by using a theorem from [7] and without

resorting to [1, 4]. By [7, Theorem 3 (i) $\Rightarrow$ (iii)], a variety $\mathcal{V}$ satisfies identity (4) for congruences if and only if $\mathcal{V}$ satisfies the same identities when α, β and γ are *representable tolerances*. A tolerance Θ is *representable* if it can be expressed as $\Theta = R \circ R^{\smile}$, for some admissible relation R, where $R^{\smile}$ 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 $\alpha(\Delta_m \circ \gamma \circ \Delta_m) \subseteq \alpha\beta \circ_p \gamma$, 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

$$\alpha(\beta \circ_h \gamma) \subseteq \alpha\beta \circ_p \gamma, \tag{5}$$

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 γ in place of β, $\alpha\beta$ in place of γ and $p-1$ in place of h in (5), we get $\alpha(\gamma \circ_{p-1} \alpha\beta) \subseteq \alpha\gamma \circ_q \alpha\beta$, for some q, thus $\alpha(\beta \circ_h \gamma) \subseteq \alpha\beta \circ_{q+1} \alpha\gamma$. In particular, $\alpha(\beta \circ_h \gamma) \subseteq \alpha\beta + \alpha\gamma$, for every h, hence we get congruence distributivity, by a remark at the beginning. Compare [8] for corresponding arguments. If one works out the details, one obtains that if $k \leq 2^t$, $t \geq 1$ and $\ell \geq 2$, then identity (4) implies $\alpha(\beta \circ_{2^\ell - 1} \gamma) \subseteq \alpha\beta \circ_{2^s+1} \alpha\gamma$, with $s = (t-1)^2(\ell - 1) + 1$, a rather large number of factors on the right. We shall present explicit details in the Appendix.

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

(f) $x = d_i(x, y, y, x)$, 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 γ in (3), 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 $r = \frac{k^2-3k+4}{2}$ 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 $a\ \beta\ b\ \gamma\ c\ \beta\ d$, for certain elements b and c. We claim that

$$(d_i(a, b, b, d), d_{i+2}(a, b, b, d)) \in \alpha(\gamma \circ \alpha\beta \circ \gamma), \tag{6}$$

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,

$$d_{i+1}(a,b,c,d)\ \beta\ d_{i+1}(a,a,d,d) = d_{i+2}(a,a,d,d)\ \beta\ d_{i+2}(a,b,c,d), \text{ and}$$
$$d_{i+1}(a,b,c,d)\ \alpha\ d_{i+1}(a,b,c,a) = d_{i+2}(a,b,c,a)\ \alpha\ d_{i+2}(a,b,c,d), \text{ hence}$$
$$d_i(a,b,b,d) = d_{i+1}(a,b,b,d)\ \gamma\ d_{i+1}(a,b,c,d)\ \alpha\beta\ d_{i+2}(a,b,c,d)\ \gamma\ d_{i+2}(a,b,b,d),$$

thus (6) follows. From (6) and (4) with γ in place of β and $\alpha\beta$ in place of γ, 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 $d_1(a,b,b,d), d_3(a,b,b,d), \dots, d_{k-2}(a,b,b,d)$ witness

$$(a,d) \in \alpha\beta \circ \alpha\gamma \circ (\alpha\gamma \circ_k \alpha\beta)^{\frac{k-3}{2}} \circ \alpha\beta = \alpha\beta \circ_r \alpha\gamma, \tag{7}$$

for $r = \frac{k^2-4k+9}{2}$. In the computation of r we have used that, say, $(\alpha\gamma \circ_k \alpha\beta) \circ (\alpha\gamma \circ_k \alpha\beta) = \alpha\gamma \circ_{2k-1} \alpha\beta$, $(\alpha\gamma \circ_k \alpha\beta)^3 = \alpha\gamma \circ_{3k-2} \alpha\beta$, etc., since k is odd, hence there are adjacent occurrences of $\alpha\gamma$ which join into one. In the general case, $(\alpha\gamma \circ_k \alpha\beta)^t = \alpha\gamma \circ_{t(k-1)+1} \alpha\beta$, for k odd. Finally, we have two adjacent occurrences of $\alpha\gamma$ at the second and third place in (7), too. From the above observations we get the value $\frac{k^2-4k+9}{2}$ of r.

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 by (6)

$$(d_1(a,b,c,d), d_3(a,b,b,d)) \in \alpha\gamma \circ \alpha(\gamma \circ \alpha\beta \circ \gamma) = \alpha(\gamma \circ \alpha\beta \circ \gamma), \tag{8}$$

hence we can consider $d_1(a,b,c,d)$ in place of $d_1(a,b,b,d)$. By considering the converse of (4), we get

$$\alpha(\beta \circ \gamma \circ \beta) \subseteq \gamma \circ_k \alpha\beta, \text{ if } k \text{ is even.} \tag{9}$$

Taking γ in place of β and $\alpha\beta$ in place of γ in (9), then from (8) 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 (9) and (4) and considering the elements $d_1(a,b,c,d), d_3(a,b,b,d), d_5(a,b,b,d), \dots, d_{k-3}(a,b,b,d)$, getting $(a,d) \in (\alpha\beta \circ_k \alpha\gamma) \circ_{\frac{k-2}{2}} (\alpha\gamma \circ_k \alpha\beta) = \alpha\beta \circ_r \alpha\gamma$, 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.

One can consider an identity intermediate between (2) and (1) by shifting the occurrence of α the other way, with respect to (4).

Problem 6. Within a variety, is the following identity equivalent to congruence distributivity?

$$\alpha(\beta \circ \gamma \circ \beta) \subseteq \beta + \alpha\gamma \tag{10}$$

We are not claiming that the above problem is difficult; in any case, it is not solved by the present note. As usual, a variety satisfies (10) if and only if there is some k such that $\alpha(\beta \circ \gamma \circ \beta) \subseteq \beta \circ_k \alpha\gamma$ holds in $\mathcal{V}$. Let us also notice that the identity (10) implies congruence distributivity if and only if it implies congruence modularity. Indeed, if (10) implies congruence modularity, then we get distributivity arguing as in the last two sentences of the proof of Theorem 1.

The author considers that it is highly inappropriate, and strongly discourages, the use of indicators extracted from the list below (even in aggregate forms in combination with similar lists) in decisions about individuals (job opportunities, career progressions etc.), attributions of funds and selections or evaluations of research projects.

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*, Contemp. 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:1709.06023v2, 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), corrected reprint with additional bibliography, AMS Chelsea Publishing/American Mathematical Society (2018).
[10] A. Pixley, *Local Mal'cev conditions*, Canad. Math. Bull. **15**, 559–568 (1972).
[11] R. Wille, *Kongruenzklassengeometrien*, Lecture Notes in Mathematics **113** (1970).

Appendix

In this appendix we justify the values reported in Remark 3.

Lemma 7. *The conditions in Corollary 2 are also equivalent to:*
(iv) For every algebra $\mathbf{A} \in \mathcal{V}$, the following identity

$$\alpha(\Delta \circ \gamma \circ \Delta) \subseteq \alpha\Delta \circ_\kappa \gamma, \tag{11}$$

holds, for all congruences α and γ on $\mathbf{A}$ and every tolerance Δ on $\mathbf{A}$ such that there exists an admissible relation R on $\mathbf{A}$ for which $\Delta = R \circ R^\smile$.

Proof. The equivalence of (i) and (iv) is a special case of [7, Theorem 3 (i) $\Rightarrow$ (iii)]. For the reader's convenience, we sketch a direct proof of (iii) $\Rightarrow$ (iv), while, of course, (iv) $\Rightarrow$ (i) is obvious.

So let us assume that we have terms as given by (iii) and that α, Δ and γ satisfy the assumptions in (iv). Suppose that $(a, d) \in \alpha(\Delta \circ \gamma \circ \Delta)$, thus

$a\ \alpha\ d$ and $a\ \Delta\ b\ \gamma\ c\ \Delta\ d$, for certain $b, c \in A$. Moreover, by the assumption on Δ, $a\ R\ b'\ R^\smile\ b$ and $c\ R\ c'\ R^\smile\ d$, for certain $b', c' \in A$. We claim that the elements $d_i(a,b,c,d)$, for $i = 0, \dots, k$, witness that $(a,d) \in \alpha\Delta \circ_\kappa \gamma$. For example, let us check that $d_i(a,b,c,d)\ \Delta\ d_{i+1}(a,b,c,d)$, for i even. Indeed, $d_i(a,b,c,d)\ R\ d_i(b',b',c',c') = d_{i+1}(b',b',c',c')\ R^\smile\ d_{i+1}(a,b,c,d)$, since, say, $b\ R\ b'$ and since, by assumption, $\Delta = R \circ R^\smile$. All the rest is standard and simpler. We have proved that (i) - (iv) are equivalent, for every k. □

We now prove that (iv) implies $\alpha(\beta + \gamma) \leq \alpha\beta + \gamma$, an identity equivalent to distributivity. We shall actually show that if k is even, say, $k = 2r$, then (iv) implies

$$\alpha(\beta \circ_{2^\ell - 1} \gamma) \subseteq \alpha\beta \circ_{2r^{\ell-1}} \gamma, \qquad \text{for every } \ell \geq 2. \tag{12}$$

Clearly, it is no loss of generality to assume that k is even, since if the identity (11) holds for some odd k, then (11) holds for $k+1$, as well. Moreover, if $(a,b) \in \alpha(\beta + \gamma)$ in some algebra, then $(a,b) \in \alpha(\beta \circ_{2^\ell - 1} \gamma)$, for some sufficiently large ℓ depending on a and b. Hence, in order to show congruence distributivity, it is enough to prove the identity (12).

The proof of (12) is by induction on $\ell \geq 2$. The base case $\ell = 2$ is the special case $\Delta = \beta$ of identity (11). Suppose that the identity (12) holds for some $\ell \geq 2$ and set $\Delta = \beta \circ_{2^\ell - 1} \gamma$. By the inductive hypothesis, we have $\alpha\Delta \subseteq \alpha\beta \circ_{2r^{\ell-1}} \gamma$.

If $R = \beta \circ_{2^{\ell-1}} \gamma$, then $\Delta = R \circ R^\smile$. Indeed, $\ell \geq 2$, thus $2^{\ell-1}$ is even, hence the last factor in the definition of R is γ and γ is also the first factor of $R^\smile$. Since γ is a congruence, we have $\gamma \circ \gamma = \gamma$, namely, one factor absorbs in $R \circ R^\smile$, thus $R \circ R^\smile$ has $2^\ell - 1$ factors, hence $\Delta = R \circ R^\smile$. Thus we can apply (iv) and we have

$$\alpha(\beta \circ_{2^{\ell+1}-1} \gamma) = \alpha(\Delta \circ \gamma \circ \Delta) \subseteq^{(11)} \alpha\Delta \circ_{2r} \gamma \subseteq^{\text{ih}} (\alpha\beta \circ_{2r^{\ell-1}} \gamma) \circ_{2r} \gamma = \alpha\beta \circ_{2r^\ell} \gamma,$$

where the superscripts (11) and "ih" mean that we have applied, respectively, identity (11) and the inductive hypothesis and where in the last identity we have used again $\gamma \circ \gamma = \gamma$, noticing that $2r^{\ell-1}$ is even, hence the last factor in the expression $\alpha\beta \circ_{2r^{\ell-1}} \gamma$ is γ.

The induction step is thus complete, hence we have proved (12).

In the next corollary we state explicitly some informations which can be obtained from the above arguments.

Corollary 8. *If some variety $\mathcal{V}$ satisfies one of the equivalent conditions in Theorem 2 with $k \leq 2r$, then $\mathcal{V}$ satisfies the identity* (12)*, for every $\ell \geq 2$.*

If in addition $k \leq 2^p$, for some $p \geq 1$, then, for every $\ell \geq 2$, $\mathcal{V}$ satisfies

$$\alpha(\beta \circ_{2^\ell - 1} \gamma) \subseteq \alpha\beta \circ_{2^s + 1} \alpha\gamma,$$

where $s = (p-1)^2(\ell-1)+1$. In particular, taking $\ell = 2$, we get that $\mathcal{V}$ satisfies

$$\alpha(\beta \circ \gamma \circ \beta) \subseteq \alpha\beta \circ_{2^t + 1} \alpha\gamma,$$

for $t = (p-1)^2 + 1$.

Proof. The first statement is given by the above proof of (12).

To prove the second statement, it is no loss of generality to assume that $k = 2r$ and $k = 2^p$. Notice that from (12) we get

$$\alpha(\beta \circ_{2^\ell - 1} \gamma) \subseteq \alpha(\alpha\beta \circ_{2r^{\ell-1}} \gamma) = \alpha\beta \circ \alpha(\gamma \circ_{2r^{\ell-1}-1} \alpha\beta), \tag{13}$$

since α is supposed to be a congruence, in particular, transitive. From $k = 2r$ and $k = 2^p$, we get $r = 2^{p-1}$, hence $2r^{\ell-1} - 1 = 2^q - 1$, for $q = (p-1)(\ell-1)+1$. Applying (12) with γ in place of β, with $\alpha\beta$ in place of γ and q in place of ℓ, we get

$$\alpha(\gamma \circ_{2r^{\ell-1}-1} \alpha\beta) = \alpha(\gamma \circ_{2^q-1} \alpha\beta) \subseteq \alpha\gamma \circ_{2r^{q-1}} \alpha\beta$$

and the conclusion follows from (13), since $2r^{q-1} = 2(2^{p-1})^{(p-1)(\ell-1)} = 2^s$. □

Paolo Lipparini

Dipartimento Ulteriore di Matematica, Viale della Ricerca Scientifica, Università di Roma "Tor Vergata", I-00133 ROME ITALY