Acta Universitatis Palackianae Olomucensis. Facultas Rerum Naturalium. Mathematica

Gábor Czédli; Eszter K. Horváth

Reflexive relations and Mal'tsev conditions for congruence lattice identities in modular varieties

Acta Universitatis Palackianae Olomucensis. Facultas Rerum Naturalium. Mathematica, Vol. 41 (2002), No. 1, 43--53

Persistent URL: http://dml.cz/dmlcz/120454

Acta Univ. Palacki. Olomuc., Fac. rer. nat.,
Mathematica **41** (2002) 43–53

Reflexive Relations and Mal'tsev Conditions for Congruence Lattice Identities in Modular Varieties *

Gábor Czédli [1], Eszter K. Horváth [2]

Bolyai Institute, University of Szeged, Szeged, Aradi vértanúk tere 1, Hungary–6720
[1] *e-mail: czedli@math.u-szeged.hu*
[2] *e-mail: horeszt@math.u-szeged.hu*

(Received March 25, 2002)

Abstract

Based on a property of tolerance relations, it was proved in [3] that for an arbitrary lattice identity implying modularity (or at least congruence modularity) there exists a Mal'tsev condition such that the identity holds in congruence lattices of algebras of a variety if and only if the variety satisfies the corresponding Mal'tsev condition. However, the Mal'tsev condition constructed in [3] is not the simplest known one in general. Now we extend the result of [3] from tolerances to reflexive compatible relations. This leads to a construction of simpler Mal'tsev conditions for lattice identities implying modularity. Notice that Day terms and Jónsson terms, as Mal'tsev conditions, are just particular cases of the general construction.

Key words: Congruence modularity, Mal'tsev condition, lattice identity, tolerance relation, Day terms, Jónsson terms.

2000 Mathematics Subject Classification: 18A05, sec. 20M99

*Partially supported by the NFSR of Hungary (OTKA), grant no. T034137 and T026243, and also by the Hungarian Ministry of Education, grant no. FKFP 0169/2001.

1 Introduction

It is an old problem if all congruence lattice identities are equivalent to Mal'tsev (=Mal'cev) conditions. In other words, we say that a lattice identity λ can be characterized by a Mal'tsev condition, or λ has a Mal'tsev condition, if there exists a Mal'tsev condition M such that, for any variety $\mathcal{V}$, λ holds in congruence lattices of all algebras in $\mathcal{V}$ if and only if M holds in $\mathcal{V}$; and the problem is if all lattice identities can be characterized this way. This problem was raised first in Grätzer [10], where the notion of a Mal'tsev condition was defined and its importance was pointed out. A *strong Mal'tsev condition* for varieties is a condition of the form "there exist terms $h_0, \dots, h_k$ satisfying a set Σ of identities" where k is fixed and the form of Σ is independent of the type of algebras considered. By a *Mal'tsev condition* we mean a condition of the form "there exists a natural number n such that P_n holds" where the P_n are strong Mal'tsev conditions and P_n implies P_{n+1} for every n. The condition "P_n implies P_{n+1}" is usually expressed by saying that a Mal'tsev condition must be weakening in its parameter. (For a more precise definition of Mal'tsev conditions cf. Taylor [26] or Neumann [22].) The problem was repeatedly asked by several authors, including Taylor [26], Jónsson [18], Freese and McKenzie [7], and Snow [25].

Certain lattice identities have known characterizations by Mal'tsev conditions. The first two results of this kind are Jónsson's characterization of (congruence) distributivity by the existence of Jónsson terms, cf. Jónsson [17], and Day's characterization of (congruence) modularity by the existence of Day terms, cf. Day [4]. Since Day's result will be needed in the sequel, we formulate it now. For $n \geq 2$ let $(\mathbf{D}_n)$ denote the strong Mal'tsev condition "there are quaternary terms $m_0, \dots, m_n$ satisfying the identities

$$\begin{aligned} m_0(x,y,z,u) = x, \quad m_n(x,y,z,u) = u,& \\ m_i(x,y,y,x) = x \quad \text{for } i = 0,1,\dots,n,& \\ m_i(x,x,y,y) = m_{i+1}(x,x,y,y) \quad \text{for } i = 0,1,\dots,n,\ i \text{ even},& \\ m_i(x,y,y,z) = m_{i+1}(x,y,y,z) \quad \text{for } i = 0,1,\dots,n,\ i \text{ odd}".& \end{aligned}$$

Now Day's celebrated result says that a variety $\mathcal{V}$ is congruence modular iff the Mal'tsev condition "$(\exists n)(\mathbf{D}_n)$" holds in $\mathcal{V}$.

Jónsson terms and Day terms were soon followed by some similar characterizations for other lattice identities, given for example by Gedeonová [9] and Mederly [20], but Nation [21] and Day [5] showed that these Mal'tsev conditions are equivalent to the existence of Day terms or Jónsson terms; the reader is referred to Jónsson [18] and Freese and McKenzie [7] (Chapter XIII) for more details.

The next milestone is Chapter XIII in Freese and McKenzie's book [7]. Let us call a lattice identity λ in n^2 variables a *frame identity* if λ implies modularity and λ holds in a modular lattice iff it holds for the elements of every (von Neumann) n-frame of the lattice. Freese and McKenzie showed that frame identities can be characterized by Mal'tsev conditions. Their approach is based on commutator theory. Although that time there was a hope that their method combined with [16] gives a Mal'tsev condition for each λ that implies modularity, cf. [7] (page 155), Pálfy and Szabó [23] destroyed this expectation.

The next step, motivated by Gumm's Shifting Principle [11], is based on elementary properties of tolerance relations. To formulate the result we recall a notion from Jónsson [18]. A lattice identity λ *is said to imply modularity in congruence varieties*, in notation $\lambda \models_c$ modularity, if for any variety $\mathcal{V}$ if all the congruence lattices $\mathrm{Con}(A)$, $A \in \mathcal{V}$, satisfy λ then all these lattices are modular. If λ implies modularity in the usual lattice theoretic sense then of course $\lambda \models_c$ modularity as well. However, it was a great surprise by Nation [21] that $\lambda \models_c$ modularity is possible even when λ does not imply modularity in the usual sense. Jónsson [18] gives an overview of similar results. We mention that there is an algorithm to test if $\lambda \models_c$ modularity, cf. [1], which is based on Day and Freese [6].

Now it was proved in [3] that if λ is a lattice identity such that $\lambda \models_c$ modularity then λ can be characterized by a *Mal'tsev* condition. The proof of this fact is relatively elementary and easy but the Mal'tsev conditions are far from being optimal in most of those cases where Mal'tsev conditions were previously known.

The purpose of this paper is to give an algorithm which associates essentially better Mal'tsev conditions with lattice identities implying modularity in congruence varieties. The price we pay for better Mal'tsev conditions is that the present approach is a bit more complicated than that in [3]. The starting point of our investigation is that not only tolerances but also reflexive compatible relations have a nice property in congruence modular varieties.

2 The Wille–Pixley algorithm

Let $\{\alpha_1, \ldots, \alpha_k\}$ be a fixed set of variables. (Later these variables will be substituted by reflexive compatible relations.) Let C_k denote the set of terms in operations $\cap$ (intersection) and $\circ$ (composition of relations) on the variables $\alpha_1, \ldots, \alpha_k$. Given p in C_k, we define a sequence $F_0(p)$, $F_1(p)$, $\ldots$ of sets of formulas. Each of these formulas will be of the form $(x_i, x_j) \in r$ for some $r \in C_k$ where x_i and x_j belong to a new set $\{x_i : i \geq 1\}$ of variables. If r is a variable, i.e., if $r \in \{\alpha_1, \ldots, \alpha_k\}$ then $(x_i, x_j) \in r$ will be called a *final formula.* Notice that the x_i will represent elements of algebras later.

Now $F_0(p)$ is the singleton consisting of $(x_1, x_2) \in p$. For $j > 0$, if all formulas in $F_{j-1}(p)$ are final then let $F_j(p) = F_{j-1}(p)$. Otherwise choose a formula $(x_i, x_\ell) \in r$ in $F_{j-1}(p)$ which is not final[1], and the definition of $F_j(p)$ depends on the form of r. If $r = r_1 \cap r_2$ then

$$F_j(p) := \Big(F_{j-1}(p) \setminus \{(x_i, x_\ell) \in r\}\Big) \cup \{(x_i, x_\ell) \in r_1,\, (x_i, x_\ell) \in r_2\}.$$

[1]There can be several formulas which are not final but, up to equivalence (namely, up to the order of terms and their variables), any choice leads to the same Mal'tsev condition.

If $r = r_1 \circ r_2$ then let m be the smallest positive integer such that x_m does not occur in any formula of $F_{j-1}(p)$ and define

$$F_j(p) := \Big(F_{j-1}(p) \setminus \{(x_i, x_\ell) \in r\}\Big) \cup \{(x_i, x_m) \in r_1,\ (x_m, x_\ell) \in r_2\}.$$

Clearly, there is a smallest t such that $F_t(p) = F_{t+1}(p)$ and we define $F(p) = F_t(p)$.

Example 1 If $k = 3$ and $p = \alpha_1 \cap (\alpha_2 \circ (\alpha_1 \cap \alpha_3) \circ \alpha_2)$, then $F(p) = \{(x_1, x_2) \in \alpha_1,\ (x_1, x_3) \in \alpha_2,\ (x_3, x_4) \in \alpha_1,\ (x_3, x_4) \in \alpha_3,\ (x_4, x_2) \in \alpha_2\}$.

Given an algebra A, the set $\mathrm{Rel_r}(A)$ of all reflexive and compatible relations on A (in other words, all subalgebras of A^2 including the diagonal subalgebra) has intersection, inverse and composition operations as usual: for Φ and Ψ in $\mathrm{Rel_r}(A)$, $(x, y) \in \Phi \circ \Psi$ iff there exists a $z \in A$ with $(x, z) \in \Phi$ and $(z, y) \in \Psi$, and $(x, y) \in \Phi^{-1}$ iff $(y, x) \in \Phi$. Now let $p, q \in C_k$. The inclusion formula (more precisely, the $\{\cap, \circ\}$*-inclusion*) $p \subseteq q$ is said to be satisfied for congruences of A if $p \subseteq q$ holds in $\mathrm{Rel_r}(A)$ whenever congruences $\beta_1, \ldots, \beta_k \in \mathrm{Con}(A)$ replace the variables $\alpha_1, \ldots, \alpha_k$, respectively. If this is the case for all algebras A in a given variety $\mathcal{V}$ then we say that $p \subseteq q$ holds for congruences of $\mathcal{V}$. The Mal'tsev condition $U(p \subseteq q)$ we are going to define will characterize this property of $\mathcal{V}$.

Compute $F(p)$ and $F(q)$, and modify $F(q)$ to obtain $\hat{F}(q)$ by replacing each variable x_i by the variable f_i in every formula belonging to $F(q)$. Suppose that $\{x_1, \ldots, x_m\}$ and $\{f_1, \ldots, f_s\}$ are the sets of variables appearing in the formulas of $F(p)$ and $\hat{F}(q)$, respectively, excluding the variables $\alpha_1, \ldots, \alpha_k$ of C_k. Clearly, m equals two plus the number of composition operators in p, and similarly for s.

Now construct partitions $\Theta_1, \ldots, \Theta_k$ of $\{x_1, \ldots, x_m\}$ corresponding to the variables $\alpha_1, \ldots, \alpha_k$ of p and q as follows: for each ℓ, $1 \le \ell \le k$, Θ_ℓ is the smallest partition of $\{x_1, \ldots, x_m\}$ such that x_i and x_j belong to the same block of Θ_ℓ for every formula $(x_i, x_j) \in \alpha_\ell$ belonging to $F(p)$. If α_ℓ does not occur in p then Θ_ℓ is the discrete partition $\{\{x_i\} : 1 \le i \le m\}$. For any partition Θ of $\{x_1, \ldots, x_m\}$ and $1 \le i \le m$, let $\hat{\Theta}(x_i)$ denote x_j where j is the smallest integer such that x_j and x_i belongs to the same block of Θ.

Example 1 (continued) If p is as before then $\Theta_1 = \{\{x_1, x_2\}, \{x_3, x_4\}\}$, $\Theta_2 = \{\{x_1, x_3\}, \{x_2, x_4\}\}$ and $\Theta_3 = \{\{x_3, x_4\}, \{x_1\}, \{x_2\}\}$.

Now let $U(p \subseteq q)$ stand for the following strong Mal'tsev condition: "there exist m-ary terms $f_1, f_2, \ldots, f_s$ satisfying the identities

$$f_1(x_1, x_2, \ldots, x_m) = x_1, \quad f_2(x_1, x_2, \ldots, x_m) = x_2,$$

and for each formula $(f_i, f_j) \in \alpha_\ell$ in $\hat{F}(q)$ the identity

$$f_i(\hat{\Theta}_\ell(x_1), \ldots, \hat{\Theta}_\ell(x_m)) = f_j(\hat{\Theta}_\ell(x_1), \ldots, \hat{\Theta}_\ell(x_m))."$$

Example 1 (continued) If p is as before and $q = (\alpha_1 \cap \alpha_2) \circ (\alpha_1 \cap \alpha_3)$ then $U(p \subseteq q)$ is the following condition: "There are quaternary terms f_1, f_2, f_3

satisfying the identities

$$
\begin{gathered}
f_1(x_1, x_2, x_3, x_4) = x_1, \quad f_2(x_1, x_2, x_3, x_4) = x_2, \\
f_1(x_1, x_1, x_3, x_3) = f_3(x_1, x_1, x_3, x_3), \\
f_1(x_1, x_2, x_1, x_2) = f_3(x_1, x_2, x_1, x_2) \\
f_3(x_1, x_1, x_3, x_3) = f_2(x_1, x_1, x_3, x_3), \\
f_3(x_1, x_2, x_3, x_3) = f_2(x_1, x_2, x_3, x_3)."
\end{gathered}
$$

Theorem 1 *(Wille [27] and Pixley [24]) Given an $\{\cap, \circ\}$-inclusion $p \subseteq q$ and a variety $\mathcal{V}$, $p \subseteq q$ holds for congruences of $\mathcal{V}$ if and only if $\mathcal{V}$ satisfies the strong Mal'tsev condition $U(p \subseteq q)$.*

Now let p be a lattice term on the variables $\alpha_1, \ldots, \alpha_k$, and let $k \geq 2$ be an integer. We define a term $p^{(k)}$ in C_k via induction as follows. If $p = \alpha_i$, a variable, then let $p^{(k)} = p$. If $p = r \wedge s$ then let $p^{(k)} = r^{(k)} \cap s^{(k)}$. Finally, if $p = r \vee s$ then let $p^{(k)} = r^{(k)} \circ s^{(k)} \circ r^{(k)} \circ s^{(k)} \circ \cdots$ (with k factors on the right).

Theorem 2 *(Wille [27] and Pixley [24]) Suppose p is an $\{\cap, \circ\}$-term and q is a lattice term on the variables $\alpha_1, \ldots, \alpha_k$. Then for any variety $\mathcal{V}$, the inclusion $p \subseteq q$ holds for congruences of $\mathcal{V}$ if and only if $\mathcal{V}$ satisfies the Mal'tsev condition "there exist an integer $k \geq 2$ such that $U(p \subseteq q^{(k)})$ holds".*

Notice that $(\exists k)\,(U(p \subseteq q^{(k)}))$ is indeed a Mal'tsev condition, for $U(p \subseteq q^{(k)})$ implies $U(p \subseteq q^{(k+1)})$ for any $k \geq 2$.

3 Reflexive relations in congruence modular varieties

Given an algebra A and $\Phi \in \mathrm{Rel_r}(A)$, the least congruence of A containing Φ will be denoted by $\mathrm{con}(\Phi)$. Similarly, Φ^* will stand for the least transitive relation containing Φ. It is easy to see that

$$\Phi^* = \bigcup_{k \in N} (\Phi \circ \Phi \circ \cdots) \quad (k \text{ factors) belongs to } \mathrm{Rel_r}(A) \tag{1}$$

and

$$\mathrm{con}(\Phi) = (\Phi \circ \Phi^{-1})^* = \bigcup_{k \in N} ((\Phi \circ \Phi^{-1}) \circ (\Phi \circ \Phi^{-1}) \circ \cdots). \tag{2}$$

If $\Gamma \in \mathrm{Rel_r}(A)$ happens to be symmetric, which means $\Gamma^{-1} = \Gamma$, in other words, if Γ belongs to $\mathrm{Tol}(A)$, the set of tolerance relations of the algebra A, then the formula simplifies:

$$\mathrm{con}(\Gamma) = \Gamma^* = \bigcup_{k \in N} (\Gamma \circ \Gamma \circ \cdots) \quad (k \text{ factors.}) \tag{3}$$

There are straightforward but useful connections among $\vee$, taken in the congruence lattice $\mathrm{Con}(A)$ of A, $\circ$ and $\mathrm{con}(\ )$, namely, for any $\Phi, \Psi \in \mathrm{Rel_r}(A)$ we have

$$\mathrm{con}(\Phi \circ \Psi) = \mathrm{con}(\Phi \circ \Psi \circ \Phi^{-1}) = \mathrm{con}(\Phi) \vee \mathrm{con}(\Psi). \tag{4}$$

Unfortunately, there is no similar result for intersection. For example, even when $\mathrm{Con}(A)$ is a three element chain, $\alpha \in \mathrm{Con}(A)$ and $\Gamma \in \mathrm{Tol}(A)$, $\mathrm{con}(\alpha \cap \Gamma)$ may be different from $\mathrm{con}(\alpha) \cap \mathrm{con}(\Gamma)$, cf. [2]. Hence the following theorem is a little bit surprising.

Theorem 3 *Let A be an algebra in a congruence modular variety, let $\Gamma \in \mathrm{Tol}(A)$ and $\Phi, \Psi \in \mathrm{Rel_r}(A)$. Then*

$$\mathrm{con}(\Gamma \cap \Phi) = \mathrm{con}(\Gamma) \cap \mathrm{con}(\Phi),$$

and

$$\mathrm{con}((\Phi \circ \Phi^{-1}) \cap \Psi) = \mathrm{con}(\Phi \cap (\Psi \circ \Psi^{-1})) = \mathrm{con}(\Phi) \cap \mathrm{con}(\Psi).$$

Proof Since A belongs to a congruence modular variety, we have Day terms, i.e., quaternary terms $m_0, \ldots, m_n$ satisfying the identities given in the introduction. We can assume that n is even. First we show that

$$\Gamma \cap (\Phi \circ \Phi^{-1}) \subseteq \mathrm{con}(\Gamma \cap \Phi). \tag{5}$$

Suppose $(a, b) \in \Gamma \cap (\Phi \circ \Phi^{-1})$, then there exists an element $c \in A$ with $(a, c), (b, c) \in \Phi$ and, of course, $(a, b), (b, a) \in \Gamma$. We define elements $d_i = m_i(a, c, c, b)$ and $e_i = m_i(a, a, b, b)$, $0 \le i \le n$. Then $(e_i, d_i) \in \Phi$ for all i. Using the trick

$$\begin{aligned} e_i = m_i(a,a,b,b) &= m_i(m_i(a,c,c,a), a, b, m_i(b,c,c,b))\ \Gamma \\ m_i(m_i(a,c,c,b), a, a, m_i(a,c,c,b)) &= m_i(a,c,c,b) = d_i, \end{aligned}$$

we obtain $(e_i, d_i) \in \Gamma$ for all i. Hence $(e_i, d_i) \in \Gamma \cap \Phi$ and $(e_i, d_i), (d_i, e_i) \in \mathrm{con}(\Gamma \cap \Phi)$. On the other hand, $e_i = e_{i+1}$ for i even and $d_j = d_{j+1}$ for j odd. Hence all the pairs

$$\begin{gathered} (a, e_0) = (d_0, e_0) = (a, e_1),\ (e_1, d_1) = (e_1, d_2),\ (d_2, e_2) = (d_2, e_3), \\ (e_3, d_3) = (e_3, d_4),\ (d_4, e_4) = (d_4, e_5),\ (e_5, d_5) = (e_5, d_6),\ \ldots\ , \\ (d_{n-2}, e_{n-2}) = (d_{n-2}, e_{n-1}),\ (e_{n-1}, d_{n-1}) = (e_{n-1}, d_n) = (e_{n-1}, b) \end{gathered}$$

belong to $\mathrm{con}(\Gamma \cap \Phi)$. So $(a, b) \in \mathrm{con}(\Gamma \cap \Phi)$ by transitivity. This proves (5).

Now we define $\Phi_1 = \Phi \circ \Phi^{-1}$ and $\Phi_{j+1} = \Phi_j \circ \Phi_j^{-1}$ for $j > 1$. We claim that, for all $j \ge 1$,

$$\Gamma \cap \Phi_j \subseteq \mathrm{con}(\Gamma \cap \Phi). \tag{6}$$

For $j = 1$ this is just (5). If (6) holds for some j then, by (5) for Φ_j instead of Φ and (6) for this j, we obtain

$$\Gamma \cap \Phi_{j+1} = \Gamma \cap (\Phi_j \circ \Phi_j^{-1}) \subseteq \mathrm{con}(\Gamma \cap \Phi_j) \subseteq \mathrm{con}(\mathrm{con}(\Gamma \cap \Phi)) = \mathrm{con}(\Gamma \cap \Phi),$$

proving (6) for $j + 1$. Thus (6) holds for all j. Clearly, $\Phi_j^{-1} = \Phi_j$ for $j \ge 1$. Hence $\Phi_j = \Phi_1 \circ \Phi_1 \circ \cdots \circ \Phi_1$, with 2^{j-1} factors on the right, for all $j \ge 1$, and we obtain from (2) that $\mathrm{con}(\Phi) = \bigcup_{j \ge 1} \Phi_j$. Hence we conclude from (6) that

$$\Gamma \cap \mathrm{con}(\Phi) = \Gamma \cap \bigcup_{j \ge 1} \Phi_j = \bigcup_{j \ge 1} (\Gamma \cap \Phi_j) \subseteq \mathrm{con}(\Gamma \cap \Phi),$$

i.e.,

$$\Gamma \cap \mathrm{con}(\Phi) \subseteq \mathrm{con}(\Gamma \cap \Phi). \tag{7}$$

Now, using (7) first for $\mathrm{con}(\Phi)$ and Γ and then for Γ and Φ, we obtain

$$\begin{aligned}\mathrm{con}(\Gamma) \cap \mathrm{con}(\Phi) &= \mathrm{con}(\Phi) \cap \mathrm{con}(\Gamma) \subseteq \mathrm{con}(\mathrm{con}(\Phi) \cap \Gamma)\\ &= \mathrm{con}(\Gamma \cap \mathrm{con}(\Phi)) \subseteq \mathrm{con}(\mathrm{con}(\Gamma \cap \Phi)) = \mathrm{con}(\Gamma \cap \Phi).\end{aligned}$$

The converse inclusion comes from the fact that con is a monotone operator. This proves the first formula of Theorem 3. Since $\Psi \circ \Psi^{-1} \in \mathrm{Tol}(A)$ and $\mathrm{con}(\Psi) = \mathrm{con}(\Psi \circ \Psi^{-1})$, and similarly for Φ instead of Ψ, the rest of Theorem 3 follows evidently. □

4 How to get rid of joins?

In order to make use of Theorem 2 for a lattice identity $p \leq q$, we have to get rid of joins in p. This can be done in various ways, and this freedom is built in the following definition.

Let C_k be the set of $\{\cap, \circ\}$-terms on the variables $\alpha_1, \ldots, \alpha_k$, as before. For $p \in C_k$ we define $p^{-1} \in C_k$ via induction as follows. (The idea is that $\alpha_1, \ldots, \alpha_k$ will be substituted by symmetric relations.) If p is a variable then $p^{-1} = p$. If $p = r \cap s$ then $p^{-1} = r^{-1} \cap s^{-1}$. If $p = r \circ s$ then $p^{-1} = s^{-1} \circ r^{-1}$. This way p^{-1} is defined and belongs to C_k for each $p \in C_k$.

Now, for any lattice term p on the variables $\alpha_1, \ldots, \alpha_k$ we define a subset $R(p)$ of C_k. The idea is that (4) and Theorem 3 should be applicable for members of $R(p)$. If p is a variable then $R(p) = \{p\}$. If $p = r \wedge s$ then

$$\begin{aligned}R(p) = R(r \wedge s) = \{\tilde{r} \cap \tilde{s} &: \tilde{r} \in R(r),\ \tilde{s} \in R(s) \text{ and } \tilde{r}^{-1} = \tilde{r}\}\\ \cup\{\tilde{r} \cap \tilde{s} &: \tilde{r} \in R(r),\ \tilde{s} \in R(s) \text{ and } \tilde{s}^{-1} = \tilde{s}\}\\ \cup\{\tilde{r} \cap (\tilde{s} \circ \tilde{s}^{-1}) &: \tilde{r} \in R(r),\ \tilde{s} \in R(s)\}\\ \cup\{(\tilde{r} \circ \tilde{r}^{-1}) \cap \tilde{s} &: \tilde{r} \in R(r),\ \tilde{s} \in R(s)\}.\end{aligned}$$

If $p = r \vee s$ then

$$\begin{aligned}R(p) = R(r \vee s) = \{\tilde{r} \circ \tilde{s} &: \tilde{r} \in R(r) \text{ and } \tilde{s} \in R(s)\}\\ \cup\{\tilde{r} \circ \tilde{s} \circ \tilde{r}^{-1} &: \tilde{r} \in R(r) \text{ and } \tilde{s} \in R(s)\}\\ \cup\{\tilde{s} \circ \tilde{r} \circ \tilde{s}^{-1} &: \tilde{r} \in R(r) \text{ and } \tilde{s} \in R(s)\}.\end{aligned}$$

Notice that if $R(r) \cup R(s)$ contains a symmetric term then so do $G(r \wedge s)$ and $G(r \vee s)$. Since variables are symmetric, we conclude that $R(p)$ contains a symmetric term for any lattice term p. We will prefer the shortest members of $R(p)$. Somehow the whole question is about symmetry, for symmetric subterms allow shorter formulas, but longer formulas are needed to produce symmetric subterms. Notice also that $p^{(3)} \in R(p)$ holds for any lattice term p.

5 Main Theorem

In this section we formulate and prove our main result, while the last section will be devoted for examples and comparison with previous results.

Theorem 4 *Let $\lambda : p \leq q$ be a lattice identity such that $\lambda \models_c$ modularity, and let $\tilde{p} \in R(p)$. Then for any variety $\mathcal{V}$ the following two conditions are equivalent.*

(a) For all $A \in \mathcal{V}$, λ holds in the congruence lattice of A.

(b) $\mathcal{V}$ satisfies the Mal'tsev condition "there is an $n \geq 2$ such that $U(\tilde{p} \subseteq q^{(n)})$ and $\mathbf{D}_n$ hold".

Proof Suppose (a). A straightforward induction on the length of p shows that for any $A \in \mathcal{V}$ and any $\alpha_1, \dots, \alpha_k \in \mathrm{Con}(A)$, $\tilde{p}(\alpha_1, \dots, \alpha_k) \subseteq p(\alpha_1, \dots, \alpha_k)$. Hence the inclusion $\tilde{p} \subseteq q$ holds for congruences of $\mathcal{V}$ and Theorem 2 gives an integer $n_1 \geq 2$ such that $U(\tilde{p} \subseteq q^{(n_1)})$ holds in $\mathcal{V}$. Since $\lambda \models_c$ modularity, $\mathcal{V}$ satisfies $\mathbf{D}_{n_2}$ for some $n_2 \geq 2$ by Day's result. Therefore (b) holds with $n = \max\{n_1, n_2\}$.

Suppose (b). By Day's result, $\mathcal{V}$ is congruence modular. It follows from Theorem 2 that the inclusion $\tilde{p} \subseteq q$ holds for congruences of $\mathcal{V}$. This means that for any $A \in \mathcal{V}$ and $\alpha_1, \dots, \alpha_k \in \mathrm{Con}(A)$, $\tilde{p}(\alpha_1 \dots, \alpha_k) \subseteq q(\alpha_1 \dots, \alpha_k)$, in short $\tilde{p}(\vec{\alpha}) \subseteq q(\vec{\alpha})$. Hence

$$\mathrm{con}(\tilde{p}(\vec{\alpha})) \subseteq \mathrm{con}(q(\vec{\alpha})).$$

Since $\mathrm{con}(q(\vec{\alpha})) = q(\vec{\alpha})$, it suffices to show that, for any lattice term p and any $\tilde{p} \in R(p)$,

$$\mathrm{con}(\tilde{p}(\vec{\alpha})) = p(\vec{\alpha}). \tag{8}$$

We verify (8) via induction on the length of p. If p is a variable then (8) is trivial.

If $p = r \wedge s$ then there are several cases. If, say, $\tilde{r} \in R(r)$ is symmetric and $\tilde{p} = \tilde{r} \cap \tilde{s}$ then using Theorem 3, the induction hypothesis for r and s, and the easy fact that symmetric terms in C_k give symmetric relations in $\mathrm{Rel_r}(A)$ when congruences are substituted for variables we conclude

$$\begin{aligned} \mathrm{con}(\tilde{p}(\vec{\alpha})) &= \mathrm{con}(\tilde{r}(\vec{\alpha}) \cap \tilde{s}(\vec{\alpha})) = \mathrm{con}(\tilde{r}(\vec{\alpha})) \cap \mathrm{con}(\tilde{s}(\vec{\alpha})) \\ &= r(\vec{\alpha}) \cap s(\vec{\alpha}) = p(\vec{\alpha}), \end{aligned}$$

indeed. When $\tilde{p} = (\tilde{r} \circ \tilde{r}^{-1}) \cap \tilde{s}$ and in other cases of $p = r \wedge s$ Theorem 3 applies similarly.

If $p = r \vee s$ then (4) and the induction hypothesis applies easily; for example, if $\tilde{p} = \tilde{r} \circ \tilde{s} \circ \tilde{r}^{-1}$ then

$$\begin{aligned} \mathrm{con}(\tilde{p}(\vec{\alpha})) &= \mathrm{con}(\tilde{r}(\vec{\alpha}) \circ \tilde{s}(\vec{\alpha}) \circ \tilde{r}(\vec{\alpha})^{-1}) = \mathrm{con}(\tilde{r}(\vec{\alpha})) \vee \mathrm{con}(\tilde{s}(\vec{\alpha})) \\ &= r(\vec{\alpha}) \vee s(\vec{\alpha}) = p(\vec{\alpha}). \end{aligned}$$

This proves (8) and the Theorem. □

6 Applications and comments

Corollary 1 *(Jónsson [17]) A variety $\mathcal{V}$ is congruence distributive if and only if there is an $n \geq 2$ and there are ternary $\mathcal{V}$-terms $t_0, \dots, t_n$ satisfying the identities $t_0(x,y,z) = x$, $t_n(x,y,z) = z$, $t_i(x,y,x) = x$ for $i = 0,1,\dots,n$, $t_i(x,x,z) = t_{i+1}(x,x,z)$ for $i = 0,1,\dots,n-1$, i even, and $t_i(x,z,z) = t_{i+1}(x,z,z)$ for $i = 0,1,\dots,n-1$, i odd.*

Proof The distributive law is $\alpha_1 \wedge (\alpha_2 \vee \alpha_3) \leq (\alpha_1 \wedge \alpha_2) \vee (\alpha_1 \wedge \alpha_3)$. Take $\tilde{p} = \alpha_1 \cap (\alpha_2 \circ \alpha_3) \in R(\alpha_1 \wedge (\alpha_2 \vee \alpha_3))$, apply Theorem 3 and interchange the last two variables in all terms. This way we obtain that the conjunction of the existence of Jónsson terms and the existence of Day terms characterizes distributivity. However, if we have Jónsson terms, then we automatically have Day terms; indeed, Jónsson terms trivially give Gumm terms, cf. Theorem 7.4 in Gumm [11], therefore $\mathcal{V}$ is congruence modular, so we have Day terms. □

Let us say that a Mal'tsev condition $U(\tilde{p} \subseteq q)$ is m-ary if the term symbols in it are m-ary. An easy induction shows that m equals two plus the number of composition operators $\circ$ in $\tilde{p}$. For example, $\mathbf{D}_n$ is a 4-ary Mal'tsev condition. It is reasonable to say that Mal'tsev conditions with smaller arities are simpler. Now we compare the output of our algorithm with some classical results. Consider the following lattice terms:

$$p_1 = \beta \wedge \bigvee_{i=0}^{n} \alpha_i, \quad q_1 = \bigvee_{j=0}^{n} \Big(\beta \wedge \bigvee_{\substack{i=0\\ i\neq j}}^{n} \alpha_i\Big)$$

$$p_2 = (\alpha \vee \beta_1) \wedge (\alpha \vee \beta_2), \quad q_2 = \alpha \vee \big((\alpha \vee \beta_1) \wedge (\alpha \vee \beta_2) \wedge (\beta_1 \vee \beta_2)\big),$$

$$p_3 = \alpha \wedge \big((\alpha \wedge \beta_1) \vee (\alpha \wedge \beta_2) \vee (\beta_1 \wedge \beta_2)\big), \quad q_3 = (\alpha \wedge \beta_1) \vee (\alpha \wedge \beta_2),$$

$$p_4 = \big(\alpha \vee (\beta \wedge \gamma)\big) \wedge \big(\gamma \vee (\alpha \wedge \beta)\big),$$

$$q_4 = \Big(\alpha \wedge \big(\gamma \vee (\alpha \wedge \beta)\big)\Big) \vee \Big(\gamma \wedge \big(\alpha \vee (\beta \wedge \gamma)\big)\Big),$$

and the lattice identities $\lambda_i : p_i \leq q_i$, $i = 1,2,3,4$. Mal'tsev conditions for λ_i, $i = 1,2,3$ resp. for $i = 4$ were given by Mederly [20] resp. Gedeonová [9]. Notice that Mederly and Gedeonová use equality rather than inequality in these identities, but this does not make any difference modulo lattice theory. Notice also that λ_1 is the n-distributive law introduced by Huhn [14], λ_2 is called ℓ-modularity introduced by McKenzie [19], λ_3 is the dual of λ_2, and λ_4, called p-modularity, is taken from Gedeonová [9]. The following statement is straightforward.

Example 2 *(a) Since $p_1^{(2)} \in R(p_1)$, there is an $(n+2)$-ary Mal'tsev condition characterizing n-distributivity; Mederly [20] also gave an $(n+2)$-ary one.*

(b) Since $(\alpha \circ \beta_1 \circ \alpha) \cap (\alpha \circ \beta_2) \in R(p_2)$, there is a 5-ary Mal'tsev condition characterizing ℓ-modularity; Mederly [20] gave a 6-ary one.

(c) Since $\alpha \cap \big((\alpha \cap \beta_1) \circ (\alpha \cap \beta_2) \circ (\beta_1 \cap \beta_2)\big) \in R(p_3)$, there is a 4-ary Mal'tsev condition characterizing dual ℓ-modularity; Mederly [20] gave a 7-ary one.

(d) Since $(\alpha \cap (\beta \circ \gamma)) \cap (\gamma \circ (\alpha \cap \beta) \circ \gamma) \in R(p_4)$, *there is a 5-ary Mal'tsev condition characterizing p-modularity; Gedeonová [9] gave a 6-ary one.*

Let us emphasize that the above example is only to illustrate Theorem 4 and a much stronger statement is known. Namely, Nation [21] proved that a variety $\mathcal{V}$ is congruence n-distributive if and only if it is congruence distributive, Day [5], and Freese and Nation [8] showed that any of λ_2, λ_3 and λ_4 is equivalent to modularity in $\models_c$ sense. Hence, thinking of Jónsson terms and Gumm terms, we can easily see that each of $\lambda_1, \ldots, \lambda_4$ can be characterized by a ternary Mal'tsev condition.

For frame identities Theorem 4 does not give the best known result either. Let

$$p_5 = \big((\alpha \wedge \beta) \vee (\gamma \wedge \delta)\big) \wedge \big((\alpha \wedge \gamma) \vee (\beta \wedge \delta)\big).$$

Example 3 *Let* q_5 *be any lattice term on the variables* $\alpha, \beta, \gamma, \delta$. *Then* $p_5 \leq q_5$ *can be characterized by a 4-ary Mal'tsev condition while the best Mal'tsev condition deduced from Theorem 4 is 5-ary.*

Proof It is proved in Herrmann and Huhn [12] that $p_5 \leq q_5$ is a so-called diamond identity. Combining Herrmann and Huhn [13], Lemma 1.7, and Huhn [15] we obtain that Huhn diamonds and von Neumann frames are equivalent in modular lattices. Hence, as one would expect, the method of Freese and McKenzie [7], Chapter XIII, works for $p_5 \leq q_5$ and we obtain that $p_5 \leq q_5$ holds for congruences of a variety if and only if $p_5^{(2)} \subseteq q_5$ holds, whence Theorem 2 gives a 4-ary Mal'tsev condition. □

One may ask if $\mathrm{con}(\Phi \cap \Psi) = \mathrm{con}(\Phi) \cap \mathrm{con}(\Psi)$ holds for arbitrary $\Phi, \Psi \in \mathrm{Rel}_{\mathrm{r}}(A)$ in a congruence modular variety since this improvement of Theorem 3 would lead to much better Mal'tsev conditions of the form $U(p^{(2)} \subseteq q)$. Unfortunately this is not the case. Indeed, if Φ denotes the usual order of a lattice L and $\Psi = \Phi^{-1}$ then $0_L = \mathrm{con}(\Phi \cap \Psi) \neq \mathrm{con}(\Phi) \cap \mathrm{con}(\Psi) = 1_L$ though lattices form a congruence modular (in fact, a congruence distributive) variety.

References

[1] Czédli, G., Freese, R.: *On congruence distributivity and modularity.* Algebra Universalis **17** (1983), 216–219.

[2] Czédli, G., Horváth, E. K.: *Congruence distributivity and modularity permit tolerances.* Acta Univ. Palacki. Olomuc., Fac. rer. nat., Math., to appear.

[3] Czédli, G., Horváth, E. K.: *All congruence lattice identities implying modularity have Mal'tsev conditions.* Algebra Universalis, to appear.

[4] Day, A.: *A characterization of modularity for congruence lattices of algebras.* Canad. Math. Bull. **12** (1969), 167–173.

[5] Day, A.: *p-modularity implies modularity in equational classes.* Algebra Universalis **3** (1973), 398–399.

[6] Day, A., Freese, R.: *A characterization of identities implying congruence modularity. I.* Canad. J. Math. **32** (1980), 1140–1167.

[7] Freese, R., McKenzie, R.: *Commutator theory for congruence modular varieties.* London Mathematical Society Lecture Note Series, 125, Cambridge University Press, Cambridge, 1987. iv+227.

[8] Freese, R., Nation, J. B.: *3,3 Lattice inclusions imply congruence modularity.* Algebra Universalis **7** (1977), 191–194.

[9] Gedeonová, E.: *A characterization of p-modularity for congruence lattices of algebras.* Acta Fac. Rerum Natur. Univ. Comenian. Math. Publ. **28** (1972), 99–106.

[10] Grätzer, G.: *Two Mal'cev-type theorems in universal algebra.* J. Combinatorial Theory **8** (1970), 334–342.

[11] Gumm, H. P.: *Geometrical methods in congruence modular algebras.* Mem. Amer. Math. Soc. **45**, 286 (1983), viii+79.

[12] Herrmann, C., Huhn, A. P.: *Zum Begriff der Charakteristik modularer Verbände.* Math. Z. **144** (1975), 185–194.

[13] Herrmann, C., Huhn, A. P.: *Lattices of normal subgroups which are generated by frames.* In: Lattice Theory, Proc. Conf. Szeged 1974, Coll. Math. Soc. J. Bolyai **12**, North-Holland, Amsterdam 1976, 97–136.

[14] Huhn, A. P.: *Schwach distributive Verbände. I.* Acta Sci. Math. (Szeged) **33** (1972), 297–305 (in German).

[15] Huhn, A. P.: *On Grätzer's problem concerning automorphisms of a finitely presented lattice.* Algebra Universalis **5** (1975), 65–71.

[16] Hutchinson, G., Czédli, G.: *A test for identities satisfied in lattices of submodules.* Algebra Universalis **8** (1978), 269–309.

[17] Jónsson, B.: *Algebras whose congruence lattices are distributive.* Math. Scandinavica **21** (1967), 110–121.

[18] Jónsson, B.: *Congruence varieties.* Algebra Universalis **10** (1980), 355–394.

[19] McKenzie, R.: *Equational bases and nonmodular lattice varieties.* Trans. Amer. Math. Soc. **174** (1972), 1–43.

[20] Mederly, P.: *Three Mal'cev type theorems and their application.* Mat. časopis SAV **25** (1975), 83–95.

[21] Nation, J. B.: *Varieties whose congruences satisfy certain lattice identities.* Algebra Universalis **4** (1974), 78–88.

[22] Neumann, W. D.: *On Malcev conditions.* J. Austral. Math. Soc. **17** (1974), 376–384.

[23] Pálfy, P. P., Szabó, Cs.: *An identity for subgroup lattices of abelian groups.* Algebra Universalis **33** (1995), 191–195.

[24] Pixley, A. F.: *Local Malcev conditions.* Canad. Math. Bull. **15** (1972), 559–568.

[25] Snow, J. W.: *Mal'tsev conditions and relations on algebras.* Algebra Universalis **42** (1999), 299–309.

[26] Taylor, W.: *Characterizing Mal'cev conditions.* Algebra Universalis **3** (1973), 351–397.

[27] Wille, R.: *Kongruenzklassengeometrien.* Lecture Notes in Mathematics **113**, Springer-Verlag, Berlin–New York, 1970, iii+99 (in German).