OPTIMAL MAL'TSEV CONDITIONS FOR CONGRUENCE MODULAR VARIETIES

GÁBOR CZÉDLI, ESZTER K. HORVÁTH, AND PAOLO LIPPARINI

Dedicated to the memory of Ivan Rival

Abstract. For varieties, congruence modularity is equivalent to the *tolerance intersection property*, TIP in short. Based on TIP, it was proved in [5] 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 [5] is not the simplest known one in general. Now we improve this result by constructing the best Mal'tsev condition and various related conditions. As an application, we give a particularly easy new proof of Freese and Jónsson [11] stating that modular congruence varieties are Arguesian, and we strengthen this result by replacing "Arguesian" by "higher Arguesian" in the sense of Haiman [18]. We show that lattice terms for congruences of an arbitrary congruence modular variety can be computed in two steps: the first step mimics the use of congruence distributivity while the second step corresponds to congruence permutability. Particular cases of this result were known; the present approach using TIP is even simpler than the proofs of the previous partial results.

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 [14], 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. The first strong Mal'tsev condition is due to A. I. Mal'tsev [25]; this classical condition characterizes the congruence permutability of varieties. 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

Date: Version of July 4, 2004.

1991 *Mathematics Subject Classification.* Primary 08B05, secondary 08B10.

Key words and phrases. Congruence modularity, Mal'tsev condition, lattice identity, tolerance relation, tolerance intersection property.

This research was partially supported by the NFSR of Hungary (OTKA), grant no. T034137 and T037877, and also by the Hungarian Ministry of Education, grant no. FKFP 0169/2001.

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 [32] or Neumann [28]. For an overview on Mal'tsev conditions cf., e.g., Appendix 3 by B. Jónsson in Grätzer [15] or Chajda, Eigenthaler and Länger [1].

The problem if each congruence lattice identity has a Mal'tsev condition was repeatedly asked by several authors, including Taylor [32], Jónsson [21], Freese and McKenzie [12], and Snow [31].

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 [20], and Day's characterization of (congruence) modularity by the existence of Day terms, cf. Day [7]. Jónsson terms and Day terms were soon followed by some similar characterizations for other lattice identities, given for example by Gedeonová [13] and Mederly [26], but Nation [27] and Day [8] showed that these Mal'tsev conditions are equivalent to the existence of Day terms or Jónsson terms; the reader is referred to Jónsson [21] and Freese and McKenzie [12] (Chapter XIII) for more details.

The next milestone is Chapter XIII in Freese and McKenzie's book [12]. 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 [19] gives a Mal'tsev condition for each λ that implies modularity, cf. [12] (page 155), Pálfy and Szabó [29] destroyed this expectation.

The next step, motivated by Gumm's Shifting Principle [17], is based on elementary properties of tolerance relations. To formulate the result we recall a notion from Jónsson [21]. For lattice identities λ and μ, λ *is said to imply* μ *in congruence varieties*, in notation $\lambda \models_c \mu$, if for any variety $\mathcal{V}$ if all the congruence lattices $\mathrm{Con}(A)$, $A \in \mathcal{V}$, satisfy λ then all these lattices satisfy μ as well. If λ implies μ in the usual lattice theoretic sense then of course $\lambda \models_c \mu$ as well. However, it was a great surprise by Nation [27] that $\lambda \models_c \mu$ is possible even when λ does not imply μ in the usual sense. Jónsson [21] gives an overview of similar results. We mention that R. Freese gave an algorithm to test if $\lambda \models_c$ modularity, cf. [3], which is based on Day and Freese [9].

Now it was proved in [5] 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 obtained are far from being optimal in most of those cases where Mal'tsev conditions were previously known.

One of our goals here is to improve [5] by giving the simplest (and in this sense hopefully the best) Mal'tsev condition and some related conditions associated with λ when $\lambda \models_c$ modularity. The usefulness of these conditions is demonstrated by proving new results of the form modularity $\models_c \lambda$. Using the tools of the present paper we prove that lattice terms for congruences of an arbitrary congruence modular variety can be computed in two steps: the first step mimics the use of congruence distributivity while the second step corresponds to congruence permutability.

Our approach is based on a condition on tolerance relations, which we call *tolerance intersection property*, TIP for short. An algebra A is said to satisfy the tolerance intersection property if for any two tolerances (i.e., reflexive symmetric compatible relations) α and β of A we have

$$\alpha^* \cap \beta^* = (\alpha \cap \beta)^*$$

where * stands for transitive closure. The importance of TIP comes from the following statement:

Theorem 1. *(*[6]*, cf. also* [5]*) Every algebra in a congruence modular variety satisfies TIP.*

This theorem was invented and proved in two steps. The first step was Proposition 1 (together with Theorem 1) of [4] while the second one is due to Radeleczki in [6]. For a more direct proof of Theorem 1 cf. [5]. Notice that Kearnes [22], motivated by [4], also invented Theorem 1 and applied it to obtain new results. He was the first to prove the converse of Theorem 1, namely that TIP implies congruence modularity; the present paper gives a new proof of this statement. Theorem 1 was heavily used in the papers [5], [6], and [2]. For example, Radeleczki proves in [6] that tolerance lattices of algebras in congruence modular varieties are 0-1 modular (i.e., no N_5 includes the greatest and the least elements simultaneously).

Since this paper and Theorem 1 came to existence under unusual circumstances, the authors decided to give an account on their contribution. Section "2. From TIP to Mal'tsev conditions" is a joint work of the three authors. The example after Proposition 2 is due to the second author. With this exception, the last two sections, "3. Identities in modular congruence varieties" and "4. Combining distributivity with permutability" belong to the third author. Finally, the first author is responsible for section "1. Introduction".

2. From TIP to Mal'tsev conditions

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 the operations intersection $\cap$, inverse $^{-1}$, composition $\circ$, transitive closure * and join $\vee$ as usual: for α and β in $\mathrm{Rel_r}(A)$, $(x,y) \in \alpha^{-1}$ iff $(y,x) \in \alpha$, $(x,y) \in \alpha \circ \beta$ iff there exists a $z \in A$ with $(x,z) \in \alpha$ and $(z,y) \in \beta$, and $\alpha \vee \beta$ is the transitive closure of $\alpha \cup \beta$. Notice that for *tolerances* $\alpha, \beta \in \mathrm{Rel_r}(A)$ we have

$$\alpha \vee \beta = (\alpha \vee \beta)^* = \alpha^* \vee \beta^* = (\alpha \circ \beta)^* = (\alpha^* \vee \beta^*)^*.$$

Sometimes we write $\wedge$ instead of $\cap$. When we speak of terms in these operations then the motivating idea is substituting the variables by reflexive compatible relations later.

For a term $p = p(x_1, \dots, x_k)$ in the binary operations $\cap, \vee, \circ$, in short for a $\{\cap, \vee, \circ\}$-term, and for $n \geq 2$ we define two kinds of derived $\{\cap, \circ\}$-terms, p_n and $p_{2,2}$ via induction as follows. If p is a variable then let $p_n = p_{2,2} = p$. If $p = r \cap s$ then let $p_n = r_n \cap s_n$ and $p_{2,2} = r_{2,2} \cap s_{2,2}$. Similarly, if $p = r \circ s$ then let $p_n = r_n \circ s_n$ and $p_{2,2} = (r_{2,2} \circ s_{2,2}) \cap (s_{2,2} \circ r_{2,2})$. Finally, if $p = r \vee s$ then let $p_n = r_n \circ s_n \circ \cdots$ with n factors on the right and $p_{2,2} = (r_{2,2} \circ s_{2,2}) \cap (s_{2,2} \circ r_{2,2})$. The tool to exploit TIP is provided by the following lemma; notice that part (D) was previously proved by Kearnes [22] in a different way.

Lemma 1. *Let A be an algebra satisfying TIP, let $p = p(x_1, \dots, x_k)$ be a $\{\cap, \vee, \circ\}$-term, let $q = q(x_1, \dots, x_k)$ be a lattice term (i.e., a $\{\cap, \vee\}$-term), and let $\alpha_1, \dots, \alpha_k \in \mathrm{Con}(A)$. Then*

(A) $p_{2,2}(\alpha_1, \dots, \alpha_k) \subseteq p_2(\alpha_1, \dots, \alpha_k) \subseteq p(\alpha_1, \dots, \alpha_k)$ (even without assuming TIP);

(B) $p_{2,2}(\alpha_1, \dots, \alpha_k)^* = p_2(\alpha_1, \dots, \alpha_k)^* = p(\alpha_1, \dots, \alpha_k)^*$;

(C) $q_2(\alpha_1, \dots, \alpha_k)^* = q_{2,2}(\alpha_1, \dots, \alpha_k)^* = q(\alpha_1, \dots, \alpha_k)$; and

(D) $\mathrm{Con}(A)$ is modular.

Proof. Since the operations $\cap, \vee$, and $\circ$ are monotone, an easy induction on the length of p shows part (A). Since * is isotone, $p_{2,2}(\alpha_1, \dots, \alpha_k)^* \subseteq p_2(\alpha_1, \dots, \alpha_k)^* \subseteq p(\alpha_1, \dots, \alpha_k)^*$ follows from (A). Hence, to prove (B), it suffices to show that

$$p_{2,2}(\alpha_1, \dots, \alpha_k)^* \supseteq p(\alpha_1, \dots, \alpha_k)^*. \tag{1}$$

This will be done via induction on the length of p.

First of all notice that $p_{2,2}(\alpha_1, \dots, \alpha_k)$ is always a tolerance of A; this follows via induction on the length of p. Now (1) is evident when p is a variable. Suppose that $p = r \cap s$ (and (1) holds for r and s). Then, with the notation $\vec{\alpha} = (\alpha_1, \dots, \alpha_k)$ and using TIP (indicated by $\overset{\text{TIP}}{=}$) and the induction hypothesis (indicated by $\overset{\text{ind}}{\supseteq}$) we have

$$\begin{gathered} p_{2,2}(\vec{\alpha})^* = \big(r_{2,2}(\vec{\alpha}) \cap s_{2,2}(\vec{\alpha})\big)^* = \big(r_{2,2}(\vec{\alpha}) \cap s_{2,2}(\vec{\alpha})\big)^{**} \overset{\text{TIP}}{=} \\ \big(r_{2,2}(\vec{\alpha})^* \cap s_{2,2}(\vec{\alpha})^*\big)^* \overset{\text{ind}}{\supseteq} \big(r(\vec{\alpha})^* \cap s(\vec{\alpha})^*\big)^* \supseteq \\ \big(r(\vec{\alpha}) \cap s(\vec{\alpha})\big)^* = p(\vec{\alpha})^*, \end{gathered}$$

indeed. Now suppose that $p = r \circ s$. Then

$$\begin{gathered} p_{2,2}(\vec{\alpha})^* = \Big(\big(r_{2,2}(\vec{\alpha}) \circ s_{2,2}(\vec{\alpha})\big) \cap \big(s_{2,2}(\vec{\alpha}) \circ r_{2,2}(\vec{\alpha})\big)\Big)^* \supseteq \\ \big(r_{2,2}(\vec{\alpha}) \cup s_{2,2}(\vec{\alpha})\big)^* = r_{2,2}(\vec{\alpha})^* \vee s_{2,2}(\vec{\alpha})^* \overset{\text{ind}}{\supseteq} \\ r(\vec{\alpha})^* \vee s(\vec{\alpha})^* = \big(r(\vec{\alpha}) \circ s(\vec{\alpha})\big)^* = p(\vec{\alpha})^*, \end{gathered}$$

indeed. Finally, if $p = r \vee s$ then

$$\begin{gathered} p_{2,2}(\vec{\alpha})^* = \Big(\big(r_{2,2}(\vec{\alpha}) \circ s_{2,2}(\vec{\alpha})\big) \cap \big(s_{2,2}(\vec{\alpha}) \circ r_{2,2}(\vec{\alpha})\big)\Big)^* \supseteq \\ \big(r_{2,2}(\vec{\alpha}) \cup s_{2,2}(\vec{\alpha})\big)^* = r_{2,2}(\vec{\alpha})^* \vee s_{2,2}(\vec{\alpha})^* \overset{\text{ind}}{\supseteq} \\ r(\vec{\alpha})^* \vee s(\vec{\alpha})^* = \big(r(\vec{\alpha}) \vee s(\vec{\alpha})\big)^* = p(\vec{\alpha})^*. \end{gathered}$$

This proves (1) and part (B) of the lemma.

Since $q(\alpha_1, \dots, \alpha_k)$ is a congruence, it equals its transitive closure and (C) becomes a particular case of (B).

Now, to prove (D), let $\alpha, \beta, \gamma \in \mathrm{Con}(A)$ with $\alpha \subseteq \gamma$ and consider the lattice terms $p(\alpha_1, \alpha_2, \alpha_3) = (\alpha_1 \vee \alpha_2) \wedge \alpha_3$ and $q(\alpha_1, \alpha_2, \alpha_3) = \alpha_1 \vee (\alpha_2 \wedge \alpha_3)$. We have to show that $p(\alpha, \beta, \gamma) \subseteq q(\alpha, \beta, \gamma)$. Let $(x, y) \in p_2(\alpha, \beta, \gamma) = (\alpha \circ \beta) \cap \gamma$. Then $(x, y) \in \gamma$ and there is a $z \in A$ such that $(x, z) \in \alpha$, $(z, y) \in \beta$. Since $\alpha \subseteq \gamma$, $(x, z) \in \gamma$ and $(z, y) \in \gamma$ by transitivity. So $(z, y) \in \beta \cap \gamma$ and we obtain $(x, y) \in \alpha \circ (\beta \cap \gamma) = q_2(\alpha, \beta, \gamma)$. This shows that $p_2(\alpha, \beta, \gamma) \subseteq q_2(\alpha, \beta, \gamma)$. Hence (C) applies and we conclude $p(\alpha,\beta,\gamma) = p_2(\alpha,\beta,\gamma)^* \subseteq q_2(\alpha,\beta,\gamma)^* = q(\alpha,\beta,\gamma)$, the modular law. $\square$

Part (D) of Lemma 1, first proved by Kearnes [22], says that TIP is a stronger property than congruence modularity. It is properly stronger, for [4], right before Proposition 1, gives an example of a three element (therefore congruence modular) monounary algebra which fails TIP. However, part (D) of Lemma 1 together with Theorem 1 imply the following statement, which is worth separate formulating even if it has been known for a while.

Theorem 2. *(*[6], [5], [22] *) Let $\mathcal{V}$ be a variety of algebras. Then $\mathcal{V}$ satisfies the tolerance intersection property if and only if $\mathcal{V}$ is congruence modular.*

The way we proved part (D) of Lemma 1 leads to the following more general statement, which we formulate for later reference.

Corollary 1. *Let A be an algebra satisfying TIP, let $p = p(x_1,\dots,x_k)$ be a $\{\cap,\vee,\circ\}$-term and let $q = q(x_1,\dots,x_k)$ be a lattice term. Then the following conditions are equivalent.*

*(*a*) $p \subseteq q$ holds for congruences of A,*

*(*b*) $p_2 \subseteq q$ holds for congruences of A,*

*(*c*) $p_{2,2} \subseteq q$ holds for congruences of A.*

Proof. According to Lemma 1 (A), (a) implies (b) and (b) implies (c). Now suppose (c). Then, in virtue of Lemma 1(B) we obtain

$$q(\vec{\alpha}) = q(\vec{\alpha})^* \supseteq p_{2,2}(\vec{\alpha})^* = p(\vec{\alpha})^* \supseteq p(\vec{\alpha}).$$

This shows that (c) implies (a). $\square$

Given two $\{\cap,\vee,\circ\}$-terms, $p = p(x_1,\dots,x_k)$ and $q = q(x_1,\dots,x_k)$, we say that the *congruence inclusion formula* $p \subseteq q$ holds in a variety $\mathcal{V}$ (or, in other words, *$p \subseteq q$ holds for congruences* of $\mathcal{V}$) if for any algebra $A \in \mathcal{V}$ and for any congruences $\alpha_1,\dots,\alpha_k$ of A we have $p(\alpha_1,\dots,\alpha_k) \subseteq q(\alpha_1,\dots,\alpha_k)$ in $\mathrm{Rel_r}(A)$. When both p and q are join-free, i.e. they are $\{\cap,\circ\}$-terms, then Wille [33] and Pixley [30] gives an algorithm to construct a strong Mal'tsev condition $M(p \subseteq q)$ such that, for any variety $\mathcal{V}$, the congruence inclusion formula $p \subseteq q$ holds in $\mathcal{V}$ if and only if $M(p \subseteq q)$ holds in $\mathcal{V}$. We do not give the details of the Wille–Pixley algorithm here, for it is also available from several secondary sources; for example from [19] or from Chapter XIII of Freese and McKenzie [12]. Notice that for an arbitrary lattice identity $p \le q$ Wille and Pixley show that this identity holds in all congruence lattices of $\mathcal{V}$ iff $\mathcal{V}$ satisfies the weak Mal'tsev condition $(\forall m \ge 2)\,(\exists n \ge n)\,\big(M(p_m \subseteq q_n)\big)$.

Given a lattice term q, let $q_{[d]}$ stand for its "disjunctive normal form", which is computed by distributing meets over joins everywhere as if we were in a distributive lattice, so $q_{[d]}$ is a join of meets of variables. The precise formal definition and the simultaneous proof that $q_{[d]}$ is a join of meets of variables go via induction on the length of q as follows. Let $q_{[d]} = q$ when q is a variable. If $q = r \vee s$ then let $q_{[d]} = r_{[d]} \vee s_{[d]}$. Finally, if $q = r \wedge s$ then $r_{[d]} = \bigvee_{i\in I} a_i$ and $s_{[d]} = \bigvee_{j \in J} b_j$ with the a_i and b_j being meets of variables, and we let $q_{[d]} = \bigvee_{i\in I,\ j\in J}(a_i \wedge b_j)$.

Now we formulate one of our main results.

Theorem 3. *Let $p \subseteq q$ be a congruence inclusion formula with q being $\circ$-free. (I.e., p is a $\{\cap,\vee,\circ\}$-term and q is a lattice term.) Then for any congruence modular variety $\mathcal{V}$ the following conditions are equivalent.*

(i) $p \subseteq q$ holds for congruences of $\mathcal{V}$,
(ii) $p_2 \subseteq q$ holds for congruences of $\mathcal{V}$,
(iii) $p_{2,2} \subseteq q$ holds for congruences of $\mathcal{V}$,
(iv) the Mal'tsev condition

$$(\exists n \geq 2)\,\big(M(p_2 \subseteq q_2 \circ q_2 \circ \cdots \circ q_2)\big)$$

(where $q_2 \circ q_2 \circ \cdots \circ q_2$ denotes a product of n factors) holds in $\mathcal{V}$.
(v) the Mal'tsev condition

$$(\exists n \geq 2)\,\big(M(p_2 \subseteq q_{[d]\,2} \circ \cdots \circ q_{[d]\,2} \circ q_2)\big)$$

(where $q_{[d]\,2} \circ \cdots \circ q_{[d]\,2}$ denotes a product of $n-1$ factors) holds in $\mathcal{V}$.

Proof. In virtue of Theorem 2 the algebras in $\mathcal{V}$ satisfy TIP. Hence the equivalence of (i), (ii) and (iii) follows from Corollary 1.

If (iv) holds then applying Wille and Pixley's result to the strong Mal'tsev condition $M(p_2 \subseteq q_2 \circ q_2 \circ \cdots \circ q_2)$ we obtain that $p_2 \subseteq q_2 \circ q_2 \circ \cdots \circ q_2$ (with n factors) holds for congruences of $\mathcal{V}$ for some n. But, using Lemma 1 (C), $q_2 \circ q_2 \circ \cdots \circ q_2 \subseteq q_2^* = q$, so the congruence inclusion formula $p_2 \subseteq q$ holds in $\mathcal{V}$. This shows that (iv) implies (ii).

Now let (ii) hold and suppose the reader has some basic idea how Wille and Pixley's proof works for lattice identities. What we have to know from their proof is the following. Associated with p_2 we construct a finitely generated free algebra F in $\mathcal{V}$ with distinguished free generators x_0 and x_1. Also, we construct finitely generated congruences $\alpha_1, \ldots, \alpha_k$ of F such that $(x_0, x_1) \in p_2(\alpha_1, \ldots, \alpha_k)$. Let $\vec{\alpha}$ stand for $(\alpha_1, \ldots, \alpha_k)$. Since $p_2(\vec{\alpha}) \subseteq q(\vec{\alpha})$, $(x_0, x_1) \in q(\vec{\alpha})$. Now $q(\vec{\alpha}) = q_2(\vec{\alpha})^*$ by Lemma 1 (C), so there is an integer $n \geq 2$ such that $(x_0, x_1) \in q_2(\vec{\alpha}) \circ \cdots \circ q_2(\vec{\alpha})$ (with n factors). And this is the formula from which Wille and Pixley conclude that $M(p_2 \subseteq q_2 \circ q_2 \circ \cdots \circ q_2)$ holds in $\mathcal{V}$. We have shown that (ii) implies (iv).

The treatment for (v) is very similar to that of (iv). The only difference is that instead of $q(\vec{\alpha}) = q_2(\vec{\alpha})^*$ now we use $q(\vec{\alpha}) = q_{[d]\,2}(\vec{\alpha})^* \circ q_2(\vec{\alpha})$, which follows from Lemma 1 (C) applied for $q_{[d]}$ and from the last theorem of the present paper.

□

Remarks. The spirit of Wille and Pixley's theorem says that part (iv) of Theorem 3 can be replaced with the Mal'tsev condition $(\exists n \geq 2)\,\big(M(p_2 \subseteq q_n\big)$.

However, (iv) and (v) are simpler conditions. In fact, no known Mal'tsev conditions for lattice identities are simpler than those supplied by (iv) and/or (v). Condition (ii) is not just an intermediate step between (i) and (iv), it will play a crucial role in the rest of the paper. Sometimes (iii) is the best to use: indeed, $p_{2,2} \subseteq p_2$ indicates that, for a given variety $\mathcal{V}$, it is easier to show (iii) than (ii).

According to the historical remarks from the introduction, the following corollary is worth formulating.

Corollary 2. *Let $p \leq q$ be a lattice identity which implies modularity in congruence varieties. Then, for an arbitrary variety $\mathcal{V}$, $p \leq q$ holds for congruences of $\mathcal{V}$ iff $M(p_2 \subseteq q_2 \circ q_2 \circ \cdots \circ q_2)$ holds in $\mathcal{V}$ for some $n \geq 2$ and $\mathcal{V}$ has Day terms.*

3. Identities in modular congruence varieties

As a generalization of the Arguesian law, Haiman [18] introduced the the following "higher" Arguesian identities D_n:

$$x_0 \wedge \Big(\Big(\bigwedge_{1\le i<n} (x_i \vee y_i) \Big) \vee y_0 \Big) \le x_1 \vee \Big((y_1 \vee y_0) \wedge \bigvee_{1\le i<n} \big((x_i \vee x_{i+1}) \wedge (y_i \vee y_{i+1}) \big) \Big),$$

where indices are understood modulo n (that is, $x_n = x_0$ and $y_n = y_0$). In [18] he mentions that D_3 is equivalent to the Arguesian law and he proves that D_n holds in every lattice of permuting equivalence relations. The proposition below shows somewhat more.

Proposition 1. *Let $n > 1$ and let $p(x_0, \dots, y_{n-1})$ resp. $q(x_0, \dots, y_{n-1})$ denote the left resp. right hand side of D_n. Then $p_2(\alpha_0, \dots, \beta_{n-1}) \subseteq q_2(\alpha_0, \dots, \beta_{n-1})$ holds for all symmetric relations $\alpha_0, \dots, \beta_{n-1}$ on any set X.*

Proof. In order to simplify notations, let

$$p_2 = p_2(\alpha_0, \dots, \beta_{n-1}) = \alpha_0 \wedge \Big(\Big(\bigwedge_{1\le i<n} (\alpha_i \circ \beta_i) \Big) \circ \beta_0 \Big),$$

$$\gamma_i = (\alpha_i \circ \alpha_{i+1}) \cap (\beta_i \circ \beta_{i+1}) \quad \text{for } 0 \le i \le n, \text{ and}$$

$$q_2 = q_2(\alpha_0, \dots, \beta_{n-1}) = \alpha_1 \circ \big((\beta_1 \circ \beta_0) \cap (\gamma_1 \circ \gamma_2 \cdots \circ \gamma_{n-1}) \big).$$

If ρ is a relation, we sometimes write $a\ \rho\ b$ instead of $(a, b) \in \rho$. The indices will be computed modulo n.

Suppose that $a, c \in X$, and $a\ p_2\ c$. Thus, $a\ \alpha_0\ c$, and there is a $b \in X$ such that $b\ \beta_0\ c$ and $(a, b) \in \bigcap_{1\le i<n} (\alpha_i \circ \beta_i)$, i.e., $(a, b) \in \alpha_i \circ \beta_i$, for $1 \le i < n$. Hence, for every $1 \le i < n$, there is a c_i such that $a\ \alpha_i\ c_i\ \beta_i\ b$ for $1 \le i < n$. (The reader is advised to draw a picture.) Letting $c_0 = c$ we have that $a\ \alpha_0\ c_0\ \beta_0\ b$; consequently, $a\ \alpha_i\ c_i\ \beta_i\ b$ for $0 \le i < n$.

Now, for every i, we have $c_i\ \alpha_i\ a\ \alpha_{i+1}\ c_{i+1}$ and $c_i\ \beta_i\ b\ \beta_{i+1}\ c_{i+1}$, so $c_i\ \gamma_i\ c_{i+1}$ for $0 \le i < n$. From $c_1\ \gamma_1\ c_2\ \gamma_2\ c_3 \dots\ \gamma_{n-2}\ c_{n-1}\ \gamma_{n-1}\ c_0 = c$ we conclude that $(c_1, c) \in \gamma_1 \circ \gamma_2 \dots \gamma_{n-2} \circ \gamma_{n-1}$. Since we also have $a\ \alpha_1\ c_1$ and $c_1\ \beta_1 \circ \beta_0\ c_0 = c$, it follows that $a\ q_2\ c$. □

Although the Arguesian law is stronger than modularity, Freese and Jónsson [11] proved that modularity implies the Arguesian law in congruence varieties. Since Haiman's D_3 is equivalent to the Arguesian law, the following theorem offers a surprisingly simple approach to Freese and Jónsson's result and generalizes it to the higher Arguesian identities. Recalling R. Freese's remark we mention that this theorem shortens the proof in [10] by immediately implying the fact that none of Haiman's lattices lies in any modular congruence variety.

Theorem 4. *Let A be an algebra with TIP. (This assumption necessarily holds when A belongs to a congruence modular variety.) Then $\mathrm{Con}(A)$ satisfies all the higher Arguesian identities D_n.*

Proof. Let p resp. q denote the left-hand resp. right-hand side of D_n. Since $\mathrm{Con}(A)$ is a sublattice of the equivalence lattice on A, Proposition 1 combined with (A) of Lemma 1 shows that $p_2 \subseteq q$ holds for congruences of A. Now the theorem follows from Corollary 1. □

The idea of the proof above is formulated in the following assertion, which follows immediately from Theorem 3.

Proposition 2. *Let $p \leq q$ be a lattice identity. If $p_2 \subseteq q$ or $p_{2,2} \subseteq q$ holds for arbitrary equivalence relations on any set then modularity implies $p \leq q$ in congruence varieties.*

Example. If

$$p = \big((a \wedge b) \vee (c \wedge d)\big) \wedge \big((e \wedge f) \vee (g \wedge h)\big) \wedge \big((c \wedge g) \vee (a \wedge e)\big),$$
$$\text{and } q = (a \wedge b) \vee (a \wedge c) \vee (e \wedge g) \vee (g \wedge h),$$

then $p_2 \subseteq q$ does not hold for equivalences on a five element set. However, $p_{2,2} \subseteq q$ holds for equivalences on any set, and therefore modularity implies $p \leq q$ in congruence varieties. Unfortunately we do not have a better example to demonstrate the superiority of part (iii) in Theorem 3 over (ii) and we have to admit that $p_2 \subseteq q$ would hold for arbitrary equivalences on any set if we changed $(c \wedge g) \vee (a \wedge e)$ to $(a \wedge e) \vee (c \wedge g)$ in the definition of p.

4. Combining distributivity with permutability

The notion of a "disjunctive normal form", defined right before Theorem 3, allows us to formulate the following theorem, which is the strongest known result for congruence modular varieties stating that distributivity can always be composed with permutability.

Theorem 5. *Let A be an algebra in a congruence modular variety and let $p = p(x_1, \ldots, x_k)$ be a lattice term. Then*

$$p(\alpha_1, \ldots, \alpha_k) = p_{[d]}(\alpha_1, \ldots, \alpha_k) \circ p_2(\alpha_1, \ldots, \alpha_k)$$

holds for all congruences $\alpha_1, \ldots, \alpha_k$ of A.

The particular case of Theorem 5, namely the case when p is a join of meets of variables, has already been published by the third author as Remark 5.8 in [24]. Now, armed with Lemma 1, we can give a simpler proof for a more general statement.

Notice that there is a general but precisely never formulated feeling that in congruence modular varieties one can combine distributivity with permutability. Perhaps this originates from the fact that the two extreme cases of the modular commutator operation mimics congruence distributivity resp. congruence permutability. But most likely the origin was Gumm's paper [16], where this phenomenon was formulated at Mal'tsev condition level. Later in [24], the third author gave a different meaning to this feeling at lattice term level; indeed, he proved an instance of Theorem 5 and exploited it for the left hand side of the Arguesian identity.

Recall that in a congruence modular variety one can define the *commutator* $[\alpha, \beta]$ of two congruences α and β. The commutator operation has many nice properties, cf. Freese and McKenzie [12] and Gumm [17]. From these well-known properties we recall the following ones: the commutator is a commutative and monotone operation on the congruence lattice, it distributes over joins, i.e., $[\alpha \vee \beta, \gamma] = [\alpha, \gamma] \vee [\beta, \gamma]$, and $[\alpha, \beta] \leq \alpha \wedge \beta$. Given a congruence α, its *solvable series* is defined by $\alpha^{(0)} = \alpha$, and $\alpha^{(n+1)} = [\alpha^{(n)}, \alpha^{(n)}]$. An easy induction shows that $(\alpha \vee \beta)^{(m+n)} \leq \alpha^{(m)} \vee \beta^{(n)}$. For meets we will need $(\alpha \wedge \beta)^{(m)} \leq \alpha^{(m)} \wedge \beta^{(m)}$, which follows from the monotonicity of the commutator.

The proof of Theorem 5 is based on the following lemma.

Lemma 2. *Under the hypotheses of Theorem 5 we have*

$$p(\alpha_1, \ldots, \alpha_k) = p(\alpha_1, \ldots, \alpha_n)^{(m)} \circ p_2(\alpha_1, \ldots, \alpha_k)$$

for every positive integer m.

Proof. The $\supseteq$ inclusion is trivial. To prove the reverse inclusion, let us observe by Lemma 1 (C) that the congruence generated by $p_2(\vec{\alpha})$ is $p(\vec{\alpha})$. Now we need Proposition 3.7 from [23]. This assertion says that, for any $m \geq 0$, the congruence δ generated by $\rho \in \mathrm{Rel_r}(A)$ is $\delta^{(m)} \circ \rho$, provided A has a difference term. Since congruence modular varieties have difference terms, cf. Freese and McKenzie [12] or Gumm [17], we infer that $p_2(\vec{\alpha})$ generates the congruence $p(\vec{\alpha})^{(m)} \circ p_2(\vec{\alpha})$. This proves Lemma 2. □

Now we are in the position to prove Theorem 5.

Proof. An easy induction on the length of p shows that

$$p_{[d]}(x_1, \ldots, x_k) \leq p(x_1, \ldots, x_k)$$

holds in all lattices. This implies the $\supseteq$ part of the theorem. In virtue of Lemma 2, the reverse inclusion will follow if we show that there is an m with $p(\vec{\alpha})^{(m)} \leq p_{[d]}(\vec{\alpha})$. This will be proved inductively. Since $\vec{\alpha}$ plays no specific role, it will not be indicated in the sequel.

If p is a variable, take $m = 0$.

Now let $p = r \vee s$, with $r^{(h)} \leq r_{[d]}$ and $s^{(k)} \leq s_{[d]}$ for some h and k. Then the afore-mentioned property of solvable series gives

$$p^{(h+k)} = (r \vee s)^{(h+k)} \leq r^{(h)} \vee s^{(k)} \leq r_{[d]} \vee s_{[d]} = p_{[d]}.$$

So $m = h + k$ works for p.

Now suppose that $p = r \wedge s$ with $r^{(h)} \leq r_{[d]}$ and $s^{(k)} \leq s_{[d]}$. Let $m = \max\{h, k\} + 1$. We have

$$p^{(m-1)} = (r \wedge s)^{(m-1)} \leq r^{(m-1)} \wedge s^{(m-1)} \leq r^{(h)} \wedge s^{(k)} \leq r_{[d]} \wedge s_{[d]}. \tag{2}$$

By definitions, $r_{[d]} = \bigvee_{i \in I} \gamma_i$ and $s_{[d]} = \bigvee_{j \in J} \delta_j$ where the γ_i and the δ_j are meets of some of the congruences $\alpha_1, \ldots, \alpha_k$. Using (2) we can compute:

$$p^{(m)} = [p^{(m-1)}, p^{(m-1)}] \leq [r_{[d]} \wedge s_{[d]}, r_{[d]} \wedge s_{[d]}] \leq [r_{[d]}, s_{[d]}] = \left[\bigvee_{i \in I} \gamma_i, \bigvee_{j \in J} \delta_j\right] = \bigvee_{i \in I,\ j \in J} [\gamma_i, \delta_j] \leq \bigvee_{i \in I,\ j \in J} (\gamma_i \wedge \delta_j) = p_{[d]},$$

completing the proof. □

Acknowledgment. The authors appreciate the referee's careful work and his hints to make the bibliography more complete.

References

[1] I. Chajda, G. Eigenthaler and H. Länger: *Congruence classes in universal algebra*, Heldermann Verlag, Lemgo, 2003.

[2] I. Chajda and S. Radeleczki: 0-conditions and tolerance schemes, *Acta Math. Univ. Comenian. (N.S.)* **72** (2003), 177–184

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

[4] G. Czédli and E. K. Horváth: Congruence distributivity and modularity permit tolerances, *Acta Univ. Palacki. Olomuc., Fac. Rer. Nat., Mathematica*, **41**(2002) 39–42.

[5] G. Czédli and E. K. Horváth: All congruence lattice identities implying modularity have Mal'tsev conditions, *Algebra Universalis* **50** (2003), 69–74.

[6] G. Czédli, E. K. Horváth, S. Radeleczki: On tolerance lattices of algebras in congruence modular varieties, *Acta Math. Hungar.* **100** (2003), 9–17.

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

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

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

[10] R. Freese: Finitely based modular congruence varieties are distributive, *Algebra Universalis* **32** (1994), 104–114,

[11] R. Freese and B. Jónsson: Congruence modularity implies the Arguesian identity. *Algebra Universalis* **6** (1976), 225–228.

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

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

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

[15] G. Grätzer: *Universal algebra* (Second edition), Springer-Verlag, New York-Heidelberg, 1979.

[16] H. P. Gumm: Congruence modularity is permutability composed with distributivity. *Arch. Math. (Basel)* **36** (1981), 569–576.

[17] H. P. Gumm: *Geometrical methods in congruence modular algebras*, *Mem. Amer. Math. Soc.* **45** (1983) no. 286, viii+79 pp.

[18] M. Haiman: Arguesian lattices which are not type-1. *Algebra Universalis* **28** (1991), 128–137.

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

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

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

[22] K. A. Kearnes, Communication via e-mails, 2001.

[23] P. Lipparini: Commutator theory without join-distributivity, *Trans. Amer. Math. Soc.* **346** (1994), 177–202.

[24] P. Lipparini: Congruence modularity implies the Arguesian law for single algebras with a difference term, *J. Algebra* **219** (1999), 658–681.

[25] A. I. Mal'tsev: On the general theory of algebraic systems (Russian), *Mat. Sb. (N. S.)* **35** (**77**) (1954), 3–20.

[26] P. Mederly: Three Mal'cev type theorems and their application, *Mat. Časopis Sloven. Akad. Vied* **25** (1975), 83–95.

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

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

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

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

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

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

[33] R. Wille: *Kongruenzklassengeometrien*, in German, Lecture Notes in Mathematics, Vol. **113** Springer-Verlag, Berlin-New York, 1970, iii+99 pp.

University of Szeged, Bolyai Institute, Szeged, Aradi vértanúk tere 1, HUNGARY 6720

E-mail address: `czedli@math.u-szeged.hu`

URL: `http://www.math.u-szeged.hu/ czedli/`

University of Szeged, Bolyai Institute, Szeged, Aradi vértanúk tere 1, HUNGARY 6720

E-mail address: `horeszt@math.u-szeged.hu`

URL: `http://www.math.u-szeged.hu/ horvath/`

Department of Mathematics, Tor Vergata University of Rome, I-00133 Rome, Italy

E-mail address: `lipparin@mat.uniroma2.it`