Varieties with a Difference Term

Keith A. Kearnes *
Fachbereich Mathematik, AG1
Technische Hochschule Darmstadt
D 64289 Darmstadt
Germany

Abstract

We give characterizations of varieties with a difference term and outline the commutator theory for such varieties.

1 Introduction

In 1954, A. I. Mal'cev published [11] which contains the result that all members of a variety of algebras have permuting congruences if and only if the variety satisfies the equations:

$$m(x, x, y) = y \text{ and } m(x, y, y) = x$$

with respect to some ternary term $m(x, y, z)$. Such a term is now called a **Mal'cev term**. Any variety whose members have an underlying group structure has a Mal'cev term: $m(x, y, z) = xy^{-1}z$. (E.g., any variety of groups, rings, modules, Boolean algebras or Lie algebras has a Mal'cev term.) It is shown by J. D. H. Smith in [14] that it is possible to extend the theory of the group commutator to any variety of algebras which has a Mal'cev term. The theory developed for such varieties is essentially as powerful a theory in general as it is in the particular variety of groups. Later, in [4], J. Hagemann and C. Herrmann extended Smith's results to congruence modular varieties without any loss in the generality of the theory. Other approaches to the commutator theory of congruence modular varieties are contained in [1] and [3]. In the latter accounts the role of a difference term plays an essential role. A **difference term** is a term $d(x, y, z)$ which satisfies

$$d(x, x, y) = y \text{ and } d(x, y, y) \ [\theta, \theta] \ x$$

where $[-, -]$ is the commutator and θ is any congruence containing (x, y). Herrmann was the first to show how to construct a difference term for a congruence modular variety (in [5]) and Gumm was the first to publish an account of the properties of the difference term and indicate that much of modular commutator theory can be derived from the properties of a difference term (see [3]).

In [6], D. Hobby and R. McKenzie have a chapter devoted to commutator theory for non-modular varieties. The commutator theory developed in [6] is necessarily weaker than the commutator theory for congruence modular varieties; but it remains a useful theory, especially for locally finite varieties. Hobby and McKenzie show that there is a largest special Mal'cev condition for locally finite varieties and this Mal'cev condition is equivalent to the existence of a **weak difference term:** a term $w(x, y, z)$ satisfying

$$w(x, x, y) \ [\theta, \theta] \ y \text{ and } w(x, y, y) \ [\theta, \theta] \ x.$$

*Supported by a fellowship from the Alexander von Humboldt Stiftung.

The commutator theory for non-modular varieties is somewhat better behaved for varieties with a weak difference term; certain fragments of modular commutator theory can be extended to this generality. The biggest gap in non-modular commutator theory is that the structure of abelian algebras is not understood. Weak difference terms come to the rescue here. In a variety with a weak difference term, the abelian algebras are affine.

In [10], P. Lipparini begins a program to determine which fragments of modular commutator theory extend to varieties with a difference term or a weak difference term. In his paper he asks for a local characterization of those locally finite varieties which have a difference term. The book [6] by Hobby and McKenzie contains two chapters on the relationship between global properties of a variety (e.g., Mal'cev conditions) and local properties (e.g., the structure of induced algebras). This book contains local characterizations of congruence distributivity, congruence modularity, congruence n-permutability for some n, congruence neutrality and other conditions. Most importantly for us, [6] gives a local characterization of those varieties with a weak difference term. Hobby and McKenzie do not characterize the varieties with a difference term, nor those with a Mal'cev term. However, they suggested a plausible local characterization for varieties with a Mal'cev term (i.e., for congruence permutable varieties). Their guess was proved to be correct by M. Valeriote and R. Willard in [15]. A second proof of this fact was given in [8] and the result was extended to a characterization of congruence 3-permutable varieties.

Since a local characterization of locally finite varieties with a weak difference term appears in [6] and a local characterization of locally finite varieties with a Mal'cev term appears in [15], the remaining problem in this collection which is open is the problem posed by Lipparini: give a local description of those locally finite varieties which have a difference term. In this paper we solve this problem. Our main result is slightly more than Lipparini asks for, since we do not completely restrict ourselves to locally finite varieties.

THEOREM 1.1 *Let $\mathcal{V}$ be a variety such that $\mathbf{F}_{\mathcal{V}}(2)$ is finite. Then $\mathcal{V}$ has a difference term iff for all finite $\mathbf{A} \in \mathcal{V}$ it is the case that*

(i) $\mathbf{1} \notin \mathrm{typ}\{\mathbf{A}\}$ *and*

(ii) *all type* $\mathbf{2}$ *minimal sets of* $\mathbf{A}$ *have empty tail.*

Although this theorem is not restricted to locally finite varieties, our arguments shall concern locally finite varieties only. What allows us to state the final result in the generality we do is the following observation. If $\mathcal{V}$ is a variety and $\mathbf{F} = \mathbf{F}_{\mathcal{V}}(2)$, then $d(x, y, z)$ is a difference term for $\mathcal{V}$ iff it is a difference term for $\mathsf{HSP}(\mathbf{F})$. The forward implication of this claim is trivial. For the reverse implication, assume that $d(x, y, z)$ is a difference term for $\mathsf{HSP}(\mathbf{F})$. Choose $\mathbf{A} \in \mathcal{V}$ and $a, b \in A$. Let $\mathbf{B} = \mathrm{Sg}^{\mathbf{A}}(\{a, b\})$. Since $\mathbf{B}$ is 2-generated, $\mathbf{B} \in \mathsf{HSP}(\mathbf{F})$. Hence $d(x, y, z)$ interprets as a difference term in $\mathbf{B}$. This means that

$$d^{\mathbf{A}}(a, a, b) = d^{\mathbf{B}}(a, a, b) = b.$$

Furthermore,

$$d^{\mathbf{A}}(a, b, b) = d^{\mathbf{B}}(a, b, b) \;\; [\mathrm{Cg}^{\mathbf{B}}(a, b), \mathrm{Cg}^{\mathbf{B}}(a, b)] \;\; a.$$

But $[\mathrm{Cg}^{\mathbf{B}}(a, b), \mathrm{Cg}^{\mathbf{B}}(a, b)] \subseteq [\theta, \theta]$ for any congruence $\theta \in \mathrm{Con}\,\mathbf{A}$ for which $(a, b) \in \theta$. Consequently $d^{\mathbf{A}}(a, b, b)$ $[\theta, \theta]$ a as desired. Thus, it suffices for us to prove Theorem 1.1 with the hypothesis "$\mathbf{F}_{\mathcal{V}}(2)$ is finite" changed to "$\mathcal{V}$ is locally finite."

Theorem 1.1 might be considered to be a natural amalgam of some theorems in [6]. As we have mentioned, any congruence modular variety has a difference term. Furthermore, for any variety satisfying $[\theta, \theta] = \theta$ as a congruence identity the projection $d(x, y, z) = z$ is a difference term. The congruence identity $[\alpha, \beta] = \alpha \wedge \beta$, called **congruence neutrality**, is equivalent to the congruence identity $[\theta, \theta] = \theta$, so the third projection is a difference term for any congruence neutral variety. The local characterizations of congruence modular and congruence neutral varieties are:

THEOREM 1.2 *A locally finite variety $\mathcal{V}$ is congruence neutral iff* $\operatorname{typ}\{\mathbf{A}\} \subseteq \{\mathbf{3}, \mathbf{4}, \mathbf{5}\}$ *for all finite* $\mathbf{A} \in \mathcal{V}$. *A locally finite variety is congruence modular iff*

(*i*) $\operatorname{typ}\{\mathbf{A}\} \subseteq \{\mathbf{2}, \mathbf{3}, \mathbf{4}\}$ *for all finite* $\mathbf{A} \in \mathcal{V}$ *and*

(*ii*) *all minimal sets have empty tail.*

The local restrictions in Theorem 1.1 are the natural join of those for congruence neutrality and congruence modularity so we may think of the existence of a difference term as the amalgam of congruence neutrality and congruence modularity (in a sense similar to Gumm's assertion in [2] that congruence modularity is the amalgam of congruence distributivity and congruence permutability). In fact, we will show that even in the absence of any finiteness hypotheses, one may consider the existence of a difference term to be the amalgam of congruence neutrality and congruence modularity. We will prove that when $\mathcal{V}$ has a difference term and $\mathbf{A} \in \mathcal{V}$, then any interval in $\mathbf{Con A}$ defined by a failure of the modular law must be neutral. That is, we show that:

THEOREM 1.3 *If $\mathcal{V}$ has a difference term and $\mathbf{A} \in \mathcal{V}$ and $\alpha, \beta, \gamma \in \operatorname{Con} \mathbf{A}$ and $\alpha \geq \gamma$, then the interval $I[(\alpha \wedge \beta) \vee \gamma, \alpha \wedge (\beta \vee \gamma)]$ is neutral.*

(An *interval* $I[\delta, \theta]$ is neutral if whenever $\delta \leq \mu \leq \nu \leq \theta$ and $C(\nu, \nu; \mu)$ holds we have $\mu = \nu$.)

Our reference for tame congruence theory is, of course, [6], while our reference for universal algebra is [13]. For commutator theory we refer the reader to Chapter 3 of [6] and also to [9].

2 Commutator Theory With a Difference Term

In this section we indicate which features of modular commutator theory depend only on the existence of a difference term. We want to show that essentially all of modular commutator theory holds for varieties with a difference term, except that the complete additivity of the commutator is weakened. The results in this section are summarized in Theorem 2.10. [10] contains some of these results as well as a further exploration of the commutator properties of varieties which have a difference term or a weak difference term.

One must have some familiarity with non-modular commutator theory in order to read some of the proofs in this section. In particular, the following definition should be familiar.

Definition 2.1 If R and S are binary relations on $\mathbf{A}$ and $\delta \in \operatorname{Con} \mathbf{A}$, then $C(R, S; \delta)$ holds if for all n whenever $(a, b) \in R$, $(u_i, v_i) \in S, i < n$, and $p(x, \bar{y}) \in \operatorname{Pol}_{n+1} \mathbf{A}$ one has

$$p(a, \bar{u}) \equiv_\delta p(a, \bar{v}) \Longleftrightarrow p(b, \bar{u}) \equiv_\delta p(b, \bar{v}).$$

We write $[R, S]$ to denote the least $\delta \in \operatorname{Con} \mathbf{A}$ such that $C(R, S; \delta)$ holds.

The relation $C(x, y; z)$ is called the **centralizer relation**. Observe that $C(R, S; \delta)$ holds if and only if $C(\alpha, \beta; \delta)$ holds, where α is the congruence generated by $R \cup \delta$ and β is the reflexive, compatible relation generated by $S \cup \delta$. We shall usually only consider $C(\alpha, \beta; \delta)$ when α and β are congruences. When α and β are reflexive, compatible relations there is a useful alternate description of $[\alpha, \beta]$. First, when β is a reflexive, compatible binary relation on $\mathbf{A}$ we use the notation $\mathbf{A} \times_\beta \mathbf{A}$ to denote the subalgebra of $\mathbf{A}^2$ with universe β. That is, $\mathbf{A} \times_\beta \mathbf{A} = \operatorname{Sg}^{\mathbf{A}^2}(\beta)$. Now let $\Delta_{\beta,\alpha}$ be the congruence on $\mathbf{A} \times_\beta \mathbf{A}$ generated by

$$\{\langle (x, x), (y, y) \rangle \mid (x, y) \in \alpha\}.$$

Call a subset $G \subseteq A^2$ **Δ-closed** if

$$\Delta_{\beta,\alpha} \circ G \circ \Delta_{\beta,\alpha} \subseteq G.$$

When α and β are reflexive, compatible relations, then $[\alpha, \beta]$ is the smallest subset $\gamma \subseteq A^2$ such that (i) γ is a congruence of $\mathbf{A}$ and (ii) γ is Δ-closed.

The following definition from [9] is useful: Given congruences α, β and γ on $\mathbf{A}$, let $[\alpha, \beta]_\gamma$ denote the least congruence $\delta \geq \gamma$ such that $C(\alpha, \beta; \delta)$ holds. Of course, $[\alpha, \beta]_0 = [\alpha, \beta]$.

LEMMA 2.2 *If $\mathcal{V}$ has a difference term, $\mathbf{A} \in \mathcal{V}$ and $\alpha, \beta \in \mathrm{Con}\,\mathbf{A}$, then $[\alpha, \beta] = [\beta, \alpha]$.*

Proof: Assume not. Then for some α and β we have that $[\alpha, \beta] \not\leq [\beta, \alpha]$. From this we obtain that $[\beta, \alpha] < [\alpha, \beta]_{[\beta,\alpha]}$ holds. If we let $\mathbf{A}' = \mathbf{A}/[\beta, \alpha]$ and $\alpha' = \alpha/[\beta, \alpha]$, $\beta' = \beta/[\beta, \alpha]$, then we get $[\beta', \alpha'] = 0 < [\alpha', \beta']$ in $\mathbf{A}'$. By changing notation we may assume that $[\beta, \alpha] = 0 < [\alpha, \beta]$ in $\mathbf{A}$.

Since $[\alpha, \beta] \neq 0$, there is a polynomial $p(x, \bar{y})$, $(a, b) \in \alpha$ and $(\bar{u}, \bar{v}) \in \beta^k$ such that

$$p(a, \bar{u}) = p(a, \bar{v})$$

while

$$c = p(b, \bar{u}) \; [\alpha, \beta] - 0_{\mathbf{A}} \; p(b, \bar{v}) = e.$$

Let $\theta = \mathrm{Cg}(c, e)$. Clearly $\theta \leq [\alpha, \beta] \leq \alpha \wedge \beta$. Hence

$$[\theta, \theta] \leq [\alpha \wedge \beta, \alpha \wedge \beta] \leq [\beta, \alpha] = 0.$$

Let $p'(x, \bar{y}) = d(p(x, \bar{y}), p(x, \bar{u}), p(b, \bar{u}))$. Then

$$p'(a, \bar{u}) = p(b, \bar{u}) = p'(b, \bar{u})$$

while

$$c = p'(a, \bar{v}) \; [\beta, \alpha] \; p'(b, \bar{v}) = d(e, c, c) = e.$$

This implies that $c = e$ (since $[\beta, \alpha] = 0$, $(c, e) \in \theta$ and $[\theta, \theta] = 0$), which clearly contradicts the second displayed line of this paragraph. □

In a congruence modular variety, centralizer relation is symmetric in its first two variables: $C(\alpha, \beta; \delta)$ iff $C(\beta, \alpha; \delta)$. This is a consequence of Lemma 2.2 and the fact that

$$C(\alpha, \beta; \delta) \Leftrightarrow [\alpha, \beta] \leq \delta$$

in a congruence modular variety. However, the centralizer is not symmetric in its first two variables in non-modular varieties with a difference term. I.e., if $\mathcal{V}$ has a difference term, then the centralizer is symmetric in its first two variables throughout $\mathcal{V}$ iff $\mathcal{V}$ is congruence modular. What this implies is that when $\mathcal{V}$ has a difference term but is not congruence modular, then $C(\alpha, \beta; \delta)$ is not equivalent to $[\alpha, \beta] \leq \delta$. The correct relationship between these properties is given in the next lemma.

LEMMA 2.3 *Suppose that $\mathbf{A} \in \mathcal{V}$ where $\mathcal{V}$ is a variety with a difference term. The following conditions are equivalent.*

(i) $C(\alpha, \beta; \delta)$.

(ii) $[\alpha, \beta]_\delta = \delta$.

(*iii*) $[\alpha,\beta] \le \delta$ *and* $[\gamma,\gamma] \le \delta$ *where* $\gamma := \beta \wedge [\alpha,\beta]_\delta$.

(In particular, $[\alpha,\beta] \le \delta \;\&\; [\beta,\beta] \le \delta \Rightarrow C(\alpha,\beta;\delta)$.*)*

Proof: That $(i) \Rightarrow (ii) \Rightarrow (iii)$ is clear. The final statement of the lemma follows from the implication $(iii) \Rightarrow (i)$, so we concentrate only on this implication.

Assume that (iii) holds, but that (i) fails. Since $C(\alpha,\beta;\delta)$ fails, there exist $p(x,\bar{y}) \in \mathrm{Pol}_{n+1}\,\mathbf{A}$ $(a,b) \in \alpha$ and $(u_i,v_i) \in \beta$, $i < n$, such that

$$p(a,\bar{u})\ \delta\ p(a,\bar{v})$$

while

$$c = p(b,\bar{u})\ [\alpha,\beta]_\delta - \delta\ p(b,\bar{v}) = e.$$

Clearly $(c,e) \in \beta$, since each $(u_i,v_i) \in \beta$, so in fact $(c,e) \in \gamma$. If $d(x,y,z)$ is the difference term for $\mathcal{V}$, let $p'(x,\bar{y}) = d(p(x,\bar{y}), p(x,\bar{u}), p(b,\bar{u}))$. Then we have

$$p'(a,\bar{u}) = p(b,\bar{u}) = p'(b,\bar{u})$$

and therefore

$$p'(a,\bar{v})\ [\beta,\alpha]\ p'(b,\bar{v}).$$

But $p'(a,\bar{v})\ \delta\ p(b,\bar{u})$ and $p'(b,\bar{v}) = d(e,c,c)\ [\gamma,\gamma]\ e = p(b,\bar{v})$. Altogether, this means that

$$c = p(b,\bar{u})\ \delta\ p'(a,\bar{v})\ [\beta,\alpha]\ p'(b,\bar{v})\ [\gamma,\gamma]\ e.$$

Assuming (iii) we have $[\gamma,\gamma] \le \delta$ and $[\beta,\alpha] = [\alpha,\beta] \le \delta$, so we conclude that $(c,e) \in \delta$. But we deliberately arranged things so that $(c,e) \notin \delta$. This contradiction concludes the proof. □

In order to describe the way the commutator behaves with respect to homomorphisms we introduce additional notation. If $\phi : \mathbf{A} \to \mathbf{B}$ is a homomorphism and R is a binary relation on B (usually a congruence), then $\phi^{<}(R)$ is the relation $\{(x,y) \in A^2 \mid (\phi(x),\phi(y)) \in R\}$. We may also write this as simply $R^{<}$ if ϕ is understood. Thus, for example, $\phi^{<}(0_{\mathbf{B}})$ and $0^{<}_{\mathbf{B}}$ both denote $\ker\phi$. If S is a binary relation on A, then $\phi(S)$ will denote the relation $\{(\phi(x),\phi(y)) \in B^2 \mid (x,y) \in S\}$ on B. Both $\phi^{>}(S)$ and $S^{>}$ will denote the congruence on $\mathbf{A}$ generated by $\phi(S)$. In the rare cases where we may need words to go with these symbols we call $\phi(S)$ the **image** of S, $\phi^{>}(S)$ the **push-forward** of S and $\phi^{<}(R)$ the **pull-back** of R. When we "push S forward" we obtain $S^{>}$. When we "pull R back" we obtain $R^{<}$.

LEMMA 2.4 *If $\mathcal{V}$ has a difference term, $\mathbf{A} \in \mathcal{V}$ and α,β and γ are congruences on $\mathbf{A}$ with $\gamma \le \alpha \wedge \beta$, then*

$$[\alpha,\beta]_\gamma = [\alpha,\beta] \vee \gamma.$$

In particular, if $\phi : \mathbf{A} \to \mathbf{B}$ is surjective and $\rho,\sigma \in \mathrm{Con}\,\mathbf{B}$, then

$$[\rho,\sigma]^{<} = [\rho^{<},\sigma^{<}] \vee 0^{<}.$$

Proof: For the first claim, let $\delta = [\alpha,\beta] \vee \gamma$. Then we have

$$[\alpha,\beta] \vee \delta = [\alpha,\beta] \vee \gamma \le [\alpha,\beta]_\gamma \le [\alpha,\beta]_\delta.$$

Hence it suffices to prove the first statement of the lemma only in the case $\gamma = \delta \ge [\alpha,\beta]$. In this case, we need to show that

$$[\alpha,\beta] \le \delta \le \alpha \wedge \beta \Rightarrow [\alpha,\beta]_\delta = \delta.$$

Assume instead that $[\alpha,\beta] \leq \delta \leq \alpha \wedge \beta$ while $\delta < [\alpha,\beta]_\delta$. Then there is a polynomial $p(x,\bar{y})$, $(a,b) \in \alpha$ and $(\bar{u},\bar{v}) \in \beta^k$ such that

$$p(a,\bar{u}) \ \delta \ p(a,\bar{v})$$

while

$$c = p(b,\bar{u}) \ [\alpha,\beta]_\delta - \delta \ p(b,\bar{v}) = e.$$

Let $\theta = \mathrm{Cg}(c,e)$. Clearly $\theta \leq [\alpha,\beta]_\delta \leq \alpha \wedge \beta$. Hence

$$[\theta,\theta] \leq [\alpha\wedge\beta, \alpha\wedge\beta] \leq [\alpha,\beta] \leq \delta.$$

Let $p'(x,\bar{y}) = d(p(x,\bar{y}), p(x,\bar{u}), p(b,\bar{u}))$. Then

$$p'(a,\bar{u}) = p(b,\bar{u}) = p'(b,\bar{u})$$

while

$$c \ \delta \ p'(a,\bar{v}) \ [\beta,\alpha] \ p'(b,\bar{v}) = d(e,c,c).$$

Now $d(e,c,c) \ [\theta,\theta] \ e$, so since $[\theta,\theta] \leq \delta$ we get $d(e,c,c) \ \delta \ e$. Furthermore, by Lemma 2.2 and our hypotheses that $[\alpha,\beta] \leq \delta$ we get that $[\beta,\alpha] \leq \delta$. Hence, in the last displayed line we have

$$c \ \delta \ p'(a,\bar{v}) \ \delta \ p'(b,\bar{v}) = d(e,c,c) \ \delta \ e.$$

But this contradicts the second displayed line of this paragraph. I.e., $(c,e) \in \delta$ is false. This finishes the proof of the first statement of this lemma.

The second statement follows from the first by taking $\gamma = 0^<$, $\alpha = \rho^<$ and $\beta = \sigma^<$. Then it turns out that $[\rho,\sigma]^< = [\alpha,\beta]_\gamma$. $\Box$

Generalizing notation from [1] we define $[\theta]^0_\delta = \theta$ and $[\theta]^{n+1}_\delta = [[\theta]^n_\delta, [\theta]^n_\delta]_\delta$. $[\theta]^n$ is defined to be $[\theta]^n_0$.

LEMMA 2.5 *If $\mathcal{V}$ has a difference term, $\mathbf{A} \in \mathcal{V}$ and $\alpha,\gamma,\delta \in \mathrm{Con}\,\mathbf{A}$, then for each n we have*

$$[\alpha \vee \gamma]^n_\delta \leq [\alpha]^n_\delta \vee \gamma.$$

In particular, $[\alpha\vee\gamma]^n_\gamma = [\alpha]^n_\gamma$.

Proof: The second claim of the lemma follows from the first (taking $\delta = \gamma$), since $[\alpha]^n_\gamma \geq \gamma$ always holds and $[\alpha\vee\gamma]^n_\gamma \geq [\alpha]^n_\gamma$ is a consequence of the monotonicity of the commutator.

The first claim of the lemma is trivial if $n = 0$. Assume that this claim is false for $n = 1$. Then we can find α, γ and δ so that $[\alpha\vee\gamma, \alpha\vee\gamma]_\delta \not\leq [\alpha,\alpha]_\delta \vee \gamma$. Set $\gamma' = [\alpha,\alpha]_\delta \vee \gamma$. Then again we have $[\alpha\vee\gamma', \alpha\vee\gamma']_\delta \not\leq [\alpha,\alpha]_\delta \vee \gamma'$, but we also have $[\alpha,\alpha]_\delta \leq \gamma'$. Changing notation back, we assume that our original choice of γ satisfies $[\alpha,\alpha]_\delta \leq \gamma$. (In particular, $\delta \leq \gamma$.)

Choose $(x,z) \in \alpha\circ\gamma$. There is a $y \in A$ such that $x \equiv_\alpha y \equiv_\gamma z$. We have

$$x \equiv_{[\alpha,\alpha]} d(x,y,y) \equiv_\gamma d(x,y,z) \equiv_\alpha d(y,y,z) = z.$$

Since $[\alpha,\alpha] \leq [\alpha,\alpha]_\delta \leq \gamma$, this forces $(x,z) \in \gamma\circ\alpha$. Hence $\alpha\circ\gamma \subseteq \gamma\circ\alpha$. It follows that $\alpha\vee\gamma = \alpha\circ\gamma$.

We have assumed that $[\alpha\vee\gamma, \alpha\vee\gamma]_\delta \not\leq [\alpha,\alpha]_\delta \vee \gamma = \gamma$. Thus, $\gamma < [\alpha\vee\gamma, \alpha\vee\gamma]_\gamma$. For any pair of congruences on any algebra the statement $\gamma < [\alpha\vee\gamma,\alpha\vee\gamma]_\gamma$ is equivalent to $\gamma < [\alpha,\alpha\vee\gamma]_\gamma$. (The latter surely implies the former by monotonicity. Conversely, $\gamma = [\gamma,\alpha\vee\gamma]_\gamma$ always holds; so if $\gamma = [\alpha,\alpha\vee\gamma]_\gamma$, then $\gamma = [\alpha\vee\gamma,\alpha\vee\gamma]_\gamma$ holds too because the commutator is semidistributive over join in its first variable.) Thus we need to obtain a contradiction to

(i) $\mathcal{V}$ has a difference term,

(ii) $[\alpha,\alpha]_\delta \le \gamma$,

(iii) $\alpha \vee \gamma = \alpha \circ \gamma$ and

(iv) $\gamma < [\alpha, \alpha \vee \gamma]_\gamma$.

Because of (iv) we can find a polynomial $p(x,\bar{y})$, $(a,b) \in \alpha$ and $(\bar{u},\bar{v}) \in (\alpha \vee \gamma)^k$ such that

$$p(a,\bar{u})\ \gamma\ p(a,\bar{v})$$

while

$$p(b,\bar{u})\ [\alpha,\alpha \vee \gamma]_\gamma - \gamma\ p(b,\bar{v}).$$

Since $\alpha \vee \gamma = \alpha \circ \gamma$, we can find a w_i for each $i < k$ such that $u_i \equiv_\alpha w_i \equiv_\gamma v_i$. Then for $z \in \{a,b\}$ we have

$$p(z,\bar{u}) \equiv_\alpha p(z,\bar{w}) \equiv_\gamma p(z,\bar{v}).$$

Using this for $z = a$ and using also $p(a,\bar{u}) \equiv_\gamma p(a,\bar{v})$ we obtain that

$$p(a,\bar{u})\ \gamma\ p(a,\bar{w}).$$

By the same argument with $z = b$ instead we obtain

$$c = p(b,\bar{u})\ [\alpha,\alpha]_\gamma - \gamma\ p(b,\bar{w}) = e.$$

Let $p'(x,\bar{y}) = d(p(x,\bar{y}), p(x,\bar{u}), p(b,\bar{u}))$. Then

$$p'(a,\bar{u}) = p(b,\bar{u}) = p'(b,\bar{u})$$

while

$$c\ \gamma\ p'(a,\bar{w})\ [\alpha,\alpha]\ p'(b,\bar{w}) = d(e,c,c).$$

Now $(c,e) \in \alpha$ and $[\alpha,\alpha] \le [\alpha,\alpha]_\delta \le \gamma$. Hence $d(e,c,c) \equiv_\gamma e$. The last displayed line gives us that $(c,e) \in \gamma$. This contradicts our previous conclusion that

$$c = p(b,\bar{u})\ [\alpha,\alpha]_\gamma - \gamma\ p(b,\bar{w}) = e.$$

Now assume that the first claim of the lemma holds for a fixed $k \ge 1$. Then

$$\begin{aligned}[\alpha \vee \gamma]_\delta^{k+1} &= [[\alpha \vee \gamma]_\delta^k, [\alpha \vee \gamma]_\delta^k]_\delta \\ &\le [[\alpha]_\delta^k \vee \gamma, [\alpha]_\delta^k \vee \gamma]_\delta \\ &\le [[\alpha]_\delta^k, [\alpha]_\delta^k]_\delta \vee \gamma \\ &= [\alpha]_\delta^{k+1} \vee \gamma.\end{aligned}$$

By induction, the claim holds for all n $\Box$

The next lemma perhaps doesn't really belong in a sequence of results concerning varieties with a difference term, because it is true in any variety.

LEMMA 2.6 *Assume that $\phi : \mathbf{A} \to \mathbf{B}$ is surjective. If $\alpha, \beta \in \mathrm{Con}\,\mathbf{A}$, then $\phi([\alpha,\beta]) \subseteq [\phi(\alpha),\phi(\beta)]$. If there exists $\psi : \mathbf{B} \to \mathbf{A}$ such that $\phi \circ \psi = id_{\mathbf{B}}$ and $\rho, \sigma \in \mathrm{Con}\,\mathbf{B}$, then*

$$\psi^<([\psi^>(\rho), \psi^>(\sigma)]) = \phi([\psi^>(\rho), \psi^>(\sigma)]) = [\rho,\sigma].$$

Proof: In order to prove this lemma, we need to understand how $[\alpha,\beta]$ is generated from α and β. Recall that $\gamma = [\alpha,\beta]$ iff $\gamma \in \operatorname{Con}\mathbf{A}$ is the least Δ-closed congruence on $\mathbf{A}$. Here $\Delta_{\beta,\alpha}$ is the congruence on $\mathbf{A}\times_\beta \mathbf{A}$ generated by

$$\{\langle (x,x),(y,y)\rangle \mid (x,y)\in\beta\}.$$

More simply put, if $\delta : \mathbf{A}\to\mathbf{A}\times_\beta\mathbf{A}$ is the canonical embedding of $\mathbf{A}$ onto the diagonal, then $\Delta_{\beta,\alpha} = \delta^{>}(\alpha)$.

We can build $\gamma = [\alpha,\beta]$ in a "bottom-up" fashion: Begin with $\gamma_0 = 0_{\mathbf{A}}$, the trivial congruence on $\mathbf{A}$. Certainly $\gamma_0 \subseteq \gamma$ since γ is a congruence. Now γ_0 may not be Δ-closed, but

$$\gamma_1 := \Delta_{\beta,\alpha}\circ\gamma_0\circ\Delta_{\beta,\alpha}$$

is. Clearly $\gamma_0\subseteq\gamma_1\subseteq\gamma$, since $\Delta_{\beta,\alpha}$ is reflexive and γ is Δ-closed. γ_1 is a Δ-closed tolerance of $\mathbf{A}$, but it may not be transitive. We let $\dagger(R)$ denote the transitive closure of a subset $R\subseteq A^2$. Since γ_1 is a tolerance, $\gamma_2 := \dagger(\gamma_1)$ is a congruence. We have $\gamma_0\subseteq\gamma_1\subseteq\gamma_2\subseteq\gamma$, since γ is transitive. γ_2 need not be Δ-closed, but $\gamma_3 := \Delta_{\beta,\alpha}\circ\gamma_2\circ\Delta_{\beta,\alpha}$ is. Continuing in this way we get a sequence

$$\gamma_0\subseteq\gamma_1\subseteq\gamma_2\subseteq\gamma_3\subseteq\cdots\subseteq\gamma$$

where the relations with even subscripts are congruences and the relations with odd subscripts are Δ-closed tolerances. We must have $\gamma = \bigcup_{n<\omega}\gamma_n$ since the latter is a Δ-closed congruence contained in γ.

Now we begin our argument that $\phi([\alpha,\beta])\subseteq[\phi(\alpha),\phi(\beta)]$. As we have just explained, $[\alpha,\beta]=\bigcup_{n<\omega}\gamma_n$. Hence

$$\phi([\alpha,\beta]) = \phi(\bigcup_{n<\omega}\gamma_n) = \bigcup_{n<\omega}\phi(\gamma_n).$$

Note that $\phi(\alpha)$ and $\phi(\beta)$ are tolerances on $\phi(\mathbf{A})=\mathbf{B}$. Let $\Gamma_0 = 0_{\mathbf{B}}$ and define

(1) $\Gamma_{i+1} = \Delta_{\phi(\beta),\phi(\alpha)}\circ\Gamma_i\circ\Delta_{\phi(\beta),\phi(\alpha)}$ if i is even and

(2) $\Gamma_{i+1} = \dagger(\Gamma_i)$ if i is odd.

Then $[\phi(\alpha),\phi(\beta)] = \bigcup_{n<\omega}\Gamma_i$. We can finish the first part of the proof by showing that $\phi(\gamma_i)\subseteq\Gamma_i$ for each i. For this we need to prove the following claim.

Claim. $\phi(\Delta_{\beta,\alpha})\subseteq\Delta_{\phi(\beta),\phi(\alpha)}$.

Proof of Claim: $\Delta_{\beta,\alpha}$ is a congruence on $\mathbf{A}\times_\beta\mathbf{A}$ and $\Delta_{\phi(\beta),\phi(\alpha)}$ is a congruence on $\mathbf{B}\times_{\phi(\beta)}\mathbf{B} = \phi(\mathbf{A}\times_\beta\mathbf{A})$. Hence it suffices to show that ϕ maps the generators of $\Delta_{\beta,\alpha}$ into $\Delta_{\phi(\beta),\phi(\alpha)}$. A typical generator of $\Delta_{\beta,\alpha}$ is of the form $\langle(a,a),(b,b)\rangle$ where $(a,b)\in\alpha$. Applying ϕ we obtain $\langle(\phi(a),\phi(a)),(\phi(b),\phi(b))\rangle$ which certainly belongs to $\Delta_{\phi(\beta),\phi(\alpha)}$.

Now we get back to the proof of the lemma. Clearly $\phi(\gamma_0)=\Gamma_0$. Assume that $\phi(\gamma_i)\subseteq\Gamma_i$ for all $i<k$. If k is odd, then $\gamma_k = \Delta_{\beta,\alpha}\circ\gamma_{k-1}\circ\Delta_{\beta,\alpha}$. Hence

$$\begin{aligned}\phi(\gamma_k) &= \phi(\Delta_{\beta,\alpha}\circ\gamma_{k-1}\circ\Delta_{\beta,\alpha})\\ &\subseteq \phi(\Delta_{\beta,\alpha})\circ\phi(\gamma_{k-1})\circ\phi(\Delta_{\beta,\alpha})\\ &\subseteq \Delta_{\phi(\beta),\phi(\alpha)}\circ\Gamma_{k-1}\circ\Delta_{\phi(\beta),\phi(\alpha)}\\ &= \Gamma_k.\end{aligned}$$

If $k>0$ is even, then $\gamma_k = \dagger(\gamma_{k-1})$. Hence

$$\begin{aligned}\phi(\gamma_k) &= \phi(\dagger(\gamma_{k-1}))\\ &\subseteq \dagger(\phi(\gamma_{k-1}))\\ &\subseteq \dagger(\Gamma_{k-1})\\ &= \Gamma_k.\end{aligned}$$

Thus in either case we have $\phi(\gamma_k) \subseteq \Gamma_k$. By induction we have $\phi([\alpha,\beta]) \subseteq [\phi(\alpha),\phi(\beta)]$.

Now we consider the case where there is a homomorphism $\psi : \mathbf{B} \to \mathbf{A}$ such that $\phi \circ \psi = id_{\mathbf{B}}$. Of course, this hypothesis implies that ψ is 1-1. From this it follows that for $\alpha, \beta \in \mathrm{Con}\,\mathbf{A}$ we have

$$[\psi^{<}(\alpha), \psi^{<}(\beta)] \subseteq \psi^{<}([\alpha,\beta]).$$

(Thinking of ψ as an inclusion, this displayed line is just the familiar commutator inclusion $[\alpha|_{\mathbf{B}}, \beta|_{\mathbf{B}}] \subseteq [\alpha,\beta]|_{\mathbf{B}}$.) We choose to rewrite this for the case $\alpha = \psi^{>}(\rho)$, $\beta = \psi^{>}(\sigma)$ where $\rho, \sigma \in \mathrm{Con}\,\mathbf{B}$. In this case we have

$$[\psi^{<}\psi^{>}(\rho), \psi^{<}\psi^{>}(\sigma)] \subseteq \psi^{<}[\psi^{>}(\rho), \psi^{>}(\sigma)].$$

Observe that for any $S \subseteq A$ we have $\psi^{<}(S) \subseteq \phi(S)$. If $\rho \in \mathrm{Con}\,\mathbf{B}$ this forces

$$\rho \subseteq \psi^{<}\psi^{>}(\rho) \subseteq \phi\psi^{>}(\rho) \subseteq \rho.$$

Hence $\psi^{<}\psi^{>}(\rho) = \phi\psi^{>}(\rho) = \rho$. Putting these observations together with the first part of this lemma, when $\rho, \sigma \in \mathrm{Con}\,\mathbf{B}$ we have

$$\begin{aligned} \psi^{<}[\psi^{>}(\rho), \psi^{>}(\sigma)] &\subseteq \phi[\psi^{>}(\rho), \psi^{>}(\sigma)] \\ &\subseteq [\phi\psi^{>}(\rho), \phi\psi^{>}(\sigma)] \\ &= [\psi^{<}\psi^{>}(\rho), \psi^{<}\psi^{>}(\sigma)] \\ &= [\rho,\sigma] \\ &\subseteq \psi^{<}[\psi^{>}(\rho), \psi^{>}(\sigma)]. \end{aligned}$$

We conclude that $\psi^{<}[\psi^{>}(\rho), \psi^{>}(\sigma)] = \phi[\psi^{>}(\rho), \psi^{>}(\sigma)] = [\rho,\sigma]$ as we claimed. This finishes the proof of the lemma. □

In the first statement of the previous lemma we assumed that ϕ was surjective only to avoid discussing the commutator of non-reflexive relations.

Gumm proved that the four properties listed in the next lemma hold for any congruence modular variety. We show that any variety satisfying one of them satisfies all of them. The point of this lemma is to show that, not only is a difference term formally a weak version of a Mal'cev term, a difference term is associated with a weak version of congruence permutability.

LEMMA 2.7 *If $\mathcal{V}$ is a variety, then the following conditions are equivalent.*

(i) *$\mathcal{V}$ has a difference term.*

(ii) $\mathcal{V} \models_{con} \alpha \circ \beta \subseteq [\alpha,\alpha] \circ \beta \circ \alpha$.

(iii) $\mathcal{V} \models_{con} \alpha \circ \beta \subseteq [\alpha]^n \circ \beta \circ \alpha$ *for each n.*

(iv) *For each n there is a term d_n such that $\mathcal{V}$ satisfies the equations $d_n(x,x,y) = y$ and $d_n(x,y,y) \equiv_{[\theta]^n} x$ for any θ containing (x,y).*

Proof: Clearly (iv) implies (i) since each d_n, $n > 0$, is a difference term.

Assume (i) and choose $(x,z) \in \alpha \circ \beta$ (where $\alpha, \beta \in \mathrm{Con}\,\mathbf{A}$, $\mathbf{A} \in \mathcal{V}$). There exists $y \in A$ such that $x \equiv_\alpha y \equiv_\beta z$. Hence

$$x \equiv_{[\alpha,\alpha]} d(x,y,y) \equiv_\beta d(x,y,z) \equiv_\alpha d(y,y,z) = z.$$

This shows that $(x,z) \in [\alpha,\alpha] \circ \beta \circ \alpha$ and (ii) holds.

Given (ii) we have $\alpha \circ \beta \subseteq [\alpha, \alpha] \circ \beta \circ \alpha$. Similarly, we have $[\alpha]^k \circ \beta \subseteq [\alpha]^{k+1} \circ \beta \circ [\alpha]^k$. Thus,

$$\begin{aligned} \alpha \circ \beta &\subseteq [\alpha, \alpha] \circ \beta \circ \alpha \\ &= ([\alpha]^1 \circ \beta) \circ \alpha \\ &\subseteq ([\alpha]^2 \circ \beta \circ [\alpha]^1) \circ \alpha \\ &= [\alpha]^2 \circ \beta \circ ([\alpha]^1 \circ \alpha) \\ &= [\alpha]^2 \circ \beta \circ \alpha \\ &= ([\alpha]^2 \circ \beta) \circ \alpha \\ &\subseteq [\alpha]^4 \circ \beta \circ \alpha \\ &\subseteq ([\alpha]^8 \circ \beta) \circ \alpha \\ &\vdots \end{aligned}$$

This shows why $\alpha \circ \beta \subseteq [\alpha]^{2^r} \circ \beta \circ \alpha$. For any given n, (iii) follows from this for r chosen so that $2^r \geq n$.

To finish we must show that (iii) implies (iv). Choose $\mathbf{F} = \mathbf{F}_{\mathcal{V}}(x, y, z)$ and let $\alpha = \mathrm{Cg}(x, y)$ and $\beta = \mathrm{Cg}(y, z)$. Then

$$(x, z) \in \alpha \circ \beta \subseteq [\alpha]^n \circ \beta \circ \alpha,$$

so there are elements $d, e \in F$ such that

$$x \equiv_{[\alpha]^n} e \equiv_\beta d \equiv_\alpha z.$$

If $d_n(x, y, z)$ and $e(x, y, z)$ are terms representing the elements d and e respectively, then the fact that $(d, z) \in \alpha$ implies that $\mathcal{V} \models d_n(x, x, z) = z$. Since $(e, d) \in \beta$ we have that $\mathcal{V} \models d_n(x, y, y) = e(x, y, y)$. We will be finished if we can show that $\mathcal{V} \models e(x, y, y) \ \equiv_{[\theta]^n} x$ whenever $(x, y) \in \theta$.

Let $\mathbf{G} = \mathbf{F}_{\mathcal{V}}(x, y)$ and define $\phi : \mathbf{F} \to \mathbf{G}$ to be the unique homomorphism extending the map $x \mapsto x$, $y \mapsto y$ and $z \mapsto y$. Let $\psi : \mathbf{G} \to \mathbf{F}$ be the unique homomorphism extending the map $x \mapsto x$, $y \mapsto y$. It is the case that $\phi \circ \psi = id_{\mathbf{G}}$, so we are in the situation of Lemma 2.6. Let $\rho = \mathrm{Cg}^{\mathbf{G}}(x, y)$. Then $\psi^{>}(\rho) = \alpha$, so

$$\begin{aligned} \phi([\alpha]^n) &\subseteq [\phi(\alpha)]^n \\ &= [\phi\psi^{>}(\rho)]^n \\ &= [\rho]^n. \end{aligned}$$

Since $x \equiv_{[\alpha]^n} e^{\mathbf{F}}(x, y, z)$, this implies that

$$x = \phi(x) \ \equiv_{[\rho]^n} \ \phi(e^{\mathbf{F}}(x, y, z)) = e^{\mathbf{G}}(x, y, y).$$

Thus we have $e^{\mathbf{G}}(x, y, y) \ \equiv_{[\rho]^n} \ x$. Choose $\mathbf{A} \in \mathcal{V}$, elements $a, b \in A$ and a congruence $\theta \in \mathrm{Con}\,\mathbf{A}$ with $(a, b) \in \theta$. We need to show that $e^{\mathbf{A}}(a, b, b) \ \equiv_{[\theta]^n} \ a$. From the way the commutator restricts to subalgebras, it is clear that $[\mathrm{Cg}^{\mathbf{B}}(a, b)]^n \subseteq [\theta]^n$ for $\mathbf{B} = \mathrm{Sg}^{\mathbf{A}}(\{a, b\})$. Hence it will be sufficient for us to prove $e^{\mathbf{A}}(a, b, b) \ \equiv_{[\theta]^n} \ a$. in the case where $\mathbf{A}$ is generated by a and b and $\theta = \mathrm{Cg}(a, b)$. We reduce our problem one step further. Let $\lambda : \mathbf{G} \to \mathbf{A}$ be the homomorphism determined by $x \mapsto a$, $y \mapsto b$ and let γ equal the kernel of λ. λ is surjective since $\mathbf{A}$ is generated by a and b and $\lambda^{<}(\theta) = \rho \vee \gamma$. Hence, in order to prove $e^{\mathbf{A}}(a, b, b) \ \equiv_{[\theta]^n} \ a$ we need to verify only that $e^{\mathbf{G}}(x, y, y) \ \equiv_{[\rho \vee \gamma]^n_\gamma} \ x$. By the monotonicity of the commutator (or by the trivial part of Lemma 2.5) we have:

$$\langle e^{\mathbf{G}}(x, y, y), x) \rangle \in [\rho]^n \subseteq [\rho]^n_\gamma \leq [\rho \vee \gamma]^n_\gamma.$$

This proves that $\mathcal{V} \models d(x, y, y) = e(x, y, y) \ \equiv_{[\theta]^n} \ x$ whenever $(x, y) \in \theta$. $\square$

LEMMA 2.8 *Assume that $\mathcal{V}$ has a difference term, $\mathbf{A} \in \mathcal{V}$ and $\alpha_i \in \operatorname{Con} \mathbf{A}$ for $i \in I$. Then*

$$[\bigvee_{i\in I} \alpha_i, \bigvee_{i\in I} \alpha_i] = \bigvee_{i,j\in I} [\alpha_i, \alpha_j].$$

Proof: The inclusion $[\bigvee_{i\in I} \alpha_i, \bigvee_{i\in I} \alpha_i] \geq [\alpha_i, \alpha_j]$ holds for all i and j by the monotonicity of the commutator. Hence

$$[\bigvee_{i\in I} \alpha_i, \bigvee_{i\in I} \alpha_i] \geq \bigvee_{i,j\in I} [\alpha_i, \alpha_j]$$

holds. We shall argue that the reverse inclusion holds when $\mathcal{V}$ has a difference term. Since

$$[\bigvee_{i\in I} \alpha_i, \bigvee_{i\in I} \alpha_i] = \bigcup_{\substack{J \subseteq I \\ J \text{ finite}}} [\bigvee_{i\in J} \alpha_i, \bigvee_{i\in J} \alpha_i]$$

and

$$\bigvee_{i,j\in I} [\alpha_i, \alpha_j] = \bigcup_{\substack{J \subseteq I \\ J \text{ finite}}} \left(\bigvee_{i,j\in J} [\alpha_i, \alpha_j]\right)$$

it follows that we only need to prove the lemma in the case that I is finite. The lemma is trivial for $|I| = 1$, so assume that $I = \{0, \ldots, n-1\}$ for some $n > 1$ and that the lemma holds for $|I| = \ell$ for all $\ell < n$.

Set $\delta = \bigvee_{i,j\in I}[\alpha_i, \alpha_j]$. Our goal will be to show that $C(\vee_I \alpha_i, \vee_I \alpha_i; \delta)$ holds for this will prove that $[\vee_I \alpha_i, \vee_I \alpha_i] \leq \delta$. The assertion that $C(\vee_I \alpha_i, \vee_I \alpha_i; \delta)$ holds is equivalent to the assertion that, for each $k < n$, $C(\alpha_k, \vee_I \alpha_i; \delta)$ holds.

Claim. $\bigvee_{i<n} \alpha_i = \delta \circ \alpha_0 \circ \cdots \circ \alpha_{n-1}$.

Proof of Claim: This is an obvious consequence of the facts:

(*i*) $\delta \circ \alpha_0 \circ \cdots \circ \alpha_{n-1} \subseteq \bigvee_{i<n} \alpha_i \subseteq \bigcup_{\ell<\omega} (\alpha_0 \circ \cdots \circ \alpha_{n-1})^\ell$.

(*ii*) $\alpha_i \circ \alpha_j \subseteq [\alpha_i, \alpha_i] \circ \alpha_j \circ \alpha_i \subseteq \delta \circ \alpha_j \circ \alpha_i$.

(*iii*) $\alpha_i \circ \delta = \delta \circ \alpha_i$.

(*iv*) $\alpha_i \circ \alpha_i = \alpha_i$.

((*i*) and (*iv*) follow from the fact **ConA** is a lattice of equivalence relations. (*ii*) and (*iii*) follow from Lemma 2.7 (*i*) $\Leftrightarrow$ (*ii*). For example, to show (*iii*) one first argues that $\alpha_i \circ \theta \subseteq \delta \circ \alpha_i$ where $\theta = [\alpha_r, \alpha_s]$ is any joinand of δ. This proves $\alpha_i \circ \delta \subseteq \delta \circ \alpha_i$ which is equivalent to (*iii*).)

The previous claim shows that

$$\neg C(\alpha_k, \vee_{i<n} \alpha_i; \delta) \Rightarrow \neg C(\alpha_k, \delta \circ \alpha_0 \circ \cdots \circ \alpha_{n-1}; \delta).$$

But if S is any binary relation, then

$$\neg C(\alpha, \delta \circ S; \delta) \Rightarrow \neg C(\alpha, S; \delta).$$

(To see this, start with a failure of $\neg C(\alpha, \delta \circ S; \delta)$: that is, $p(x, \bar{y}) \in \mathrm{Pol}_{t+1}\mathbf{A}$, $(a, b) \in \alpha$ and $u_i \; \delta \circ S \; v_i$ where

$$p(a, \bar{u}) \; \delta \; p(a, \bar{v})$$

but

$$p(b,\bar{u}) \not\mathrel{\delta} p(b,\bar{v}).$$

Then choosing w_i so that $u_i \ \delta \ w_i \ S \ v_i$ we find that

$$p(a,\bar{w}) \ S \ p(a,\bar{v})$$

but

$$p(b,\bar{w}) \not\mathrel{S} p(b,\bar{v}).$$

Hence $\neg C(\alpha, \delta \circ S; \delta) \Rightarrow \neg C(\alpha, S; \delta)$ as promised.) We conclude that

$$\neg C(\alpha_k, \vee_{i<n}\alpha_i; \delta) \Rightarrow \neg C(\alpha_k, \delta \circ \alpha_0 \circ \cdots \circ \alpha_{n-1}; \delta) \Rightarrow \neg C(\alpha_k, \alpha_0 \circ \cdots \circ \alpha_{n-1}; \delta).$$

If we show that $C(\alpha_k, \alpha_0 \circ \cdots \circ \alpha_{m-1}; \delta)$ holds, then $C(\alpha_k, \vee_{i<n}\alpha_i; \delta)$ will hold as a consequence.

Observe that from the previous claim we even have $\bigvee_{i<n} \alpha_i = \delta \circ \alpha_{\pi(0)} \circ \cdots \circ \alpha_{\pi(n-1)}$ for any permutation π of $\{0, \ldots, n-1\}$. Rearranging the order of the α_is in this composition and renumbering, it is clear that we may assume that $\alpha_k = \alpha_0$. Thus we need to derive a contradiction from the assumption that $C(\alpha_0, \alpha_0 \circ \cdots \circ \alpha_{n-1}; \delta)$ fails and that n is the least natural number for which such a failure occurs. Choose $p(x,\bar{y}) \in \mathrm{Pol}_{t+1}\mathbf{A}$, $(a,b) \in \alpha_0$ and $(u_i, v_i) \in \alpha_0 \circ \cdots \circ \alpha_{n-1}$ such that

$$p(a,\bar{u}) \ \delta \ p(a,\bar{v})$$

but

$$p(b,\bar{u}) \not\mathrel{\delta} p(b,\bar{v}).$$

For $\ell = \lceil \frac{n}{2} \rceil$, choose $\bar{w}$ such that for each j it is the case that

$$u_j \ \alpha_0 \circ \cdots \circ \alpha_{\ell-1} \ w_j \ \alpha_\ell \circ \cdots \circ \alpha_{n-1} \ v_j.$$

Since $1 < n$ we have that $0 < \ell < n$. Define $p'(x,\bar{y}) = d(p(x,\bar{y}), p(x,\bar{w}), p(b,\bar{w}))$ where $d(x,y,z)$ is the difference term for $\mathcal{V}$. We have that

$$p'(a,\bar{w}) = p(b,\bar{w}) = p'(b,\bar{w}),$$

so we can conclude that

$$p'(a,\bar{u}) \ [\theta, \alpha_0] \ p'(b,\bar{u}) \qquad \text{and} \qquad p'(a,\bar{v}) \ [\theta', \alpha_0] \ p'(b,\bar{v})$$

where $\theta = \bigvee_{i=0}^{\ell-1} \alpha_i$ and $\theta' = \bigvee_{i=\ell}^{n-1} \alpha_i$.

Claim. $[\theta, \alpha_0] \leq \delta$ and $[\theta', \alpha_0] \leq \delta$.

Proof of Claim: Recall that $n > 1$. If $n = 2$, then $\theta = \alpha_0$ and $\theta' = \alpha_1$. In these cases the claim follows immediately from the definition of δ. Now assume that $n > 2$.

Subclaim. If $n > 2$, then $\{\alpha_0, \ldots, \alpha_{\ell-1}\}$ and $\{\alpha_0, \alpha_\ell, \ldots, \alpha_{n-1}\}$ are proper subsets of $\{\alpha_0, \ldots, \alpha_{n-1}\}$.

Proof of Subclaim: Since $\ell < n$ we have that

$$\alpha_{n-1} \in \{\alpha_0, \ldots, \alpha_{n-1}\} - \{\alpha_0, \ldots, \alpha_{\ell-1}\}.$$

Next, since $\ell = \lceil \frac{n}{2} \rceil > 1$ we have

$$\alpha_1 \in \{\alpha_0, \ldots, \alpha_{n-1}\} - \{\alpha_0, \alpha_\ell, \ldots, \alpha_{n-1}\}.$$

The argument is complete.

Now we finish off the Claim. The set $S = \{\alpha_0, \dots, \alpha_{\ell-1}\}$ has cardinality less than n, so by induction we have

$$[\bigvee_{\gamma\in S} \gamma, \bigvee_{\gamma\in S} \gamma] = \bigvee_{\gamma,\gamma'\in S} [\gamma, \gamma'].$$

By the monotonicity of the commutator, the left-hand side dominates $[\theta, \alpha_0]$ while the right-hand side is dominated by δ. (In fact, each joinand on the right-hand side is a joinand in the definition of δ.) The argument for $[\theta', \alpha_0] \leq \delta$ is the same. This finishes the proof of the Claim.

From the last Claim and the remarks that precede the statement of the claim, we have

$$p'(a, \bar{u})\ \delta\ p'(b, \bar{u}) \quad \text{and} \quad p'(a, \bar{v})\ \delta\ p'(b, \bar{v}).$$

If $f(x) = d(x, p(a, \bar{w}), p(b, \bar{w}))$, then

$$p'(a, \bar{u}) = f(p(a, \bar{u}))\ \delta\ f(p(a, \bar{v})) = p'(a, \bar{v})$$

since f is a polynomial of $\mathbf{A}$ and $(p(a, \bar{u}), p(a, \bar{v})) \in \delta$. From this we obtain that

$$p'(b, \bar{u})\ \delta\ p'(a, \bar{u})\ \delta\ p'(a, \bar{v})\ \delta\ p'(b, \bar{v}).$$

Since $p(b, \bar{u})\ \not\delta\ p(b, \bar{v})$ it follows that either $p(b, \bar{u})\ \not\delta\ p'(b, \bar{u})$ or else $p(b, \bar{u})\ \not\delta\ p'(b, \bar{u})$ (or perhaps both). In fact, we will show this is not the case and this contradiction will conclude the proof. Both cases are similar, so we shall only describe the contradiction obtained in the case where $p(b, \bar{u})\ \not\delta\ p'(b, \bar{u})$.

Recall that $p'(b, \bar{u}) = d(p(b, \bar{u}), p(b, \bar{w}), p(b, \bar{w}))$. If we let $c = p(b, \bar{u})$ and $e = p(b, \bar{w})$, then we have reduced to the case where $c\ \not\delta\ d(c, e, e)$. But $(c, e) = (p(b, \bar{u}), p(b, \bar{w})) \in \bigvee_{i<\ell} \alpha_i$. Since $\ell < n$, our induction hypothesis implies that

$$\begin{aligned}[\mathrm{Cg}(c, e), \mathrm{Cg}(c, e)] &\leq [\textstyle\bigvee_{i<\ell} \alpha_i, \bigvee_{i<\ell} \alpha_i] \\ &= \textstyle\bigvee_{i,j<\ell} [\alpha_i, \alpha_j] \\ &\leq \delta.\end{aligned}$$

Since d is a difference term, we must have $c\ [\mathrm{Cg}(c, e), \mathrm{Cg}(c, e)]\ d(c, e, e)$ and so $c\ \delta\ d(c, e, e)$. This is the contradiction we sought. $\square$

Generalizing previous notation, we let $\mathbf{A} \times_\alpha \mathbf{A} \times_\alpha \mathbf{A}$ denotes the subalgebra of $\mathbf{A}^3$ whose universe consists of those triples $(a, b, c) \in A^3$ where $a \equiv_\alpha b \equiv_\alpha c$.

LEMMA 2.9 *Assume that $\mathcal{V}$ has a difference term d, that $\mathbf{A} \in \mathcal{V}$ and $\alpha \in \mathrm{Con}\,\mathbf{A}$. Then $[\alpha, \alpha] = 0$ iff*

- *(i) $d(b, b, a) = d(a, b, b) = a$ for all $(a, b) \in \alpha$ and*
- *(ii) $d : \mathbf{A} \times_\alpha \mathbf{A} \times_\alpha \mathbf{A} \to \mathbf{A}$ is a homomorphism.*

Proof: This theorem is proved for congruence modular varieties in [1] (Theorem 5.7). All dependence on congruence modularity can be removed from their argument. Freese and McKenzie show (without using congruence modularity) that properties (i) and (ii) of this theorem allow them to define a congruence Δ' on $\mathbf{A} \times_\alpha \mathbf{A}$ which contains

$$\{\langle (x, x), (y, y) \rangle \mid (x, y) \in \alpha\}$$

and which has the property that the diagonal of $\mathbf{A} \times_\alpha \mathbf{A}$ is a union of Δ'-classes. This is sufficient to prove that $[\alpha, \alpha] = 0$. Part of the other direction of their argument really requires congruence modularity, so we modify the argument here.

Since d is a difference term and $[\alpha, \alpha] = 0$, we have that $d(b, b, a) = d(a, b, b) = a$ whenever $(a, b) \in \alpha$, so (i) holds. Now suppose that $x \; \alpha \; y \; \alpha \; z$. Then $\langle (x, x), (y, y) \rangle \in \Delta_{\alpha,\alpha}$, so

$$(d(x, y, z), x) = d((x, x), (y, x), (z, x)) \; \Delta_{\alpha,\alpha} \; d((y, y), (y, x), (z, x)) = (z, y).$$

If $f(\bar{x})$ is a basic n-ary operation of $\mathbf{A}$ and $x_i \; \alpha \; y_i \; \alpha \; z_i$, $i < n$, then $f(\bar{x}) \; \alpha \; f(\bar{y}) \; \alpha \; f(\bar{z})$. We have from this that

$$(d(f(\bar{x}), f(\bar{y}), f(\bar{z})), f(\bar{x})) \; \Delta_{\alpha,\alpha} \; (f(\bar{z}), f(\bar{y}))$$

and, for each i,

$$(d(x_i, y_i, z_i), x_i) \; \Delta_{\alpha,\alpha} \; (z_i, y_i).$$

Applying f coordinatewise to these latter pairs and using that $\Delta_{\alpha,\alpha}$ is a congruence, we get

$$(f(d(x_0, y_0, z_0), \ldots, d(x_{n-1}, y_{n-1}, z_{n-1})), f(\bar{x})) \; \Delta_{\alpha,\alpha} \; (f(\bar{z}), f(\bar{y})).$$

We conclude that

$$(r, t) := (d(f(\bar{x}), f(\bar{y}), f(\bar{z})), f(\bar{x})) \; \Delta_{\alpha,\alpha} \; (f(d(x_0, y_0, z_0), \ldots, d(x_{n-1}, y_{n-1}, z_{n-1})), f(\bar{x})) =: (s, t).$$

The elements r, s and t defined in this way belong to the same α-class, so

$$(r, s) = d((r, t), (s, t), (s, s)) \; \Delta_{\alpha,\alpha} \; d((s, t), (s, t), (s, s)) = (s, s).$$

But the fact that $[\alpha, \alpha] = 0$ means that the diagonal of $\mathbf{A} \times_\alpha \mathbf{A}$ is a union of $\Delta_{\alpha,\alpha}$-classes. Since $(r, s) \; \Delta_{\alpha,\alpha} \; (s, s)$ we must have $r = s$ or $d(f(\bar{x}), f(\bar{y}), f(\bar{z})) = f(d(x_0, y_0, z_0), \ldots, d(x_{n-1}, y_{n-1}, z_{n-1}))$. This holds for every basic operation f, so d is a homomorphism. □

The next theorem summarizes the basic commutator properties that hold for a variety with a difference term.

THEOREM 2.10 *Let $\mathcal{V}$ be a variety with a difference term. Then the following properties of the commutator hold in $\mathcal{V}$.*

I. (HSP Properties) *Assume $\mathbf{A}, \mathbf{B}, \mathbf{A}_0, \mathbf{A}_1 \in \mathcal{V}$. The following hold.*

(H) *If $\phi_1 : \mathbf{A} \to \mathbf{B}$ is surjective and $\alpha, \beta \in \operatorname{Con} \mathbf{A}$, $\rho, \sigma \in \operatorname{Con} \mathbf{B}$, then*

$$\phi([\alpha, \beta]) \subseteq [\phi(\alpha), \phi(\beta)] \text{ and } \phi^{<}[\rho, \sigma] = [\phi^{<}(\rho), \phi^{<}(\sigma)] \vee \phi^{<}(0_{\mathbf{B}}).$$

If there is a $\psi : \mathbf{B} \to \mathbf{A}$ such that $\phi \circ \psi = id_{\mathbf{B}}$, then

$$\psi^{<}[\psi^{>}(\rho), \psi^{>}(\sigma)] = [\rho, \sigma].$$

(S) *If $\mathbf{B} \leq \mathbf{A}$ and $\alpha, \beta \in \operatorname{Con} \mathbf{A}$, then*

$$[\alpha|_{\mathbf{B}}, \beta|_{\mathbf{B}}] \leq [\alpha, \beta]|_{\mathbf{B}}.$$

(P) *If $\alpha_i, \beta_i \in \operatorname{Con} \mathbf{A}_i$, then in $\mathbf{A}_0 \times \mathbf{A}_1$ we have*

$$[\alpha_0 \times \alpha_1, \beta_0 \times \beta_1] = [\alpha_0, \beta_0] \times [\alpha_1, \beta_1].$$

II. (Order-Theoretic Properties) *For congruences on $\mathbf{A} \in \mathcal{V}$ the following hold.*

(*i*) *If* $\alpha \le \alpha'$ *and* $\beta \le \beta'$*, then* $[\alpha, \beta] \le [\alpha', \beta']$.

(*ii*) $[\alpha, \beta] \le \alpha \wedge \beta$.

(*iii*) $[\alpha, \beta] = [\beta, \alpha]$.

(*iv*) *If* $[\alpha_i, \beta] = \gamma$ *for* $i \in I$*, then* $[\bigvee_{i\in I} \alpha_i, \beta] = \gamma$.

(*v*) $[\alpha \vee \gamma]^n \le [\alpha]^n \vee \gamma$ *for any* n.

(*vi*) $[\bigvee_{i\in I} \alpha_i, \bigvee_{i\in I} \alpha_i] = \bigvee_{i,j\in I}[\alpha_i, \alpha_j]$.

III. (Abelian Congruences)

(*a*) *Abelian algebras in* $\mathcal{V}$ *are affine.*

(*b*) $[\alpha, \alpha] = 0$ *in* $\mathbf{A}$ *iff* $d(y, y, x) = d(x, y, y) = x$ *for all* $(x, y) \in \alpha$ *and* $d : \mathbf{A} \times_\alpha \mathbf{A} \times_\alpha \mathbf{A} \to \mathbf{A}$ *is a homomorphism.*

Proof: All of these properties are either (*i*) true of the commutator in any variety (and well-known), (*ii*) proved for modular varieties in [1] or [3] using only the fact that $\mathcal{V}$ has a difference term or (*iii*) proved in Lemmas 2.2–2.9 above. □

Of the standard properties of the modular commutator, the only property that is weakened when we relax the assumption "$\mathcal{V}$ is congruence modular" to "$\mathcal{V}$ has a difference term" is the additivity of the commutator. Instead of complete additivity, we only have complete $\vee$-semidistributivity. It is not hard to prove that congruence modularity is equivalent to the existence of a difference term together with the additivity of the commutator. Properties II (*iv*) $-$ (*vi*) of Theorem 2.10 are a partial substitute for additivity. (Incidentally, properties II (*v*) and II (*vi*) have a valid natural common generalization that is trivial to prove but non-trivial to write down. The case $n = 2$ may be expressed as

$$[[\bigvee_{i\in I} \alpha_i, \bigvee_{i\in I} \alpha_i], [\bigvee_{i\in I} \alpha_i, \bigvee_{i\in I} \alpha_i]] = \bigvee_{i,j,k,l\in I} [[\alpha_i, \alpha_j], [\alpha_k, \alpha_l]].$$

For higher n the property is that $[\bigvee_{i\in I} \alpha_i]^n$ may be expanded "as if the commutator was completely additive.")

3 Varieties with a Difference term

In this section our first goal is to give a useful characterization of those varieties with a difference term. This is done in Theorem 3.3. We then specialize to locally finite varieties and prove Theorem 1.1. First we show that some results on solvability in locally finite varieties extend to arbitrary varieties with a difference term.

Definition 3.1 If α and β are congruences on $\mathbf{A}$, then we write $\alpha \overset{s}{\sim} \beta$ and say that α and β are **solvably related** if for some n it is the case that $[\alpha \vee \beta]^n \le \alpha \wedge \beta$.

It is not obvious at first glance, but for varieties with a difference term our definition of "solvably related" means that $\alpha \overset{s}{\sim} \beta$ iff $(\alpha \vee \beta)/(\alpha \wedge \beta)$ is a solvable congruence of $\mathbf{A}/(\alpha \wedge \beta)$. To explain why this is true, we first set $\theta = \alpha \vee \beta$ and $\delta = \alpha \wedge \beta$. It is clear from the definition that $\alpha \overset{s}{\sim} \beta$ is equivalent to $\alpha \wedge \beta \overset{s}{\sim} \alpha \vee \beta$, so we only need to show that when $\delta \le \theta$ we have $\delta \overset{s}{\sim} \theta$ iff θ/δ is a solvable congruence of $\mathbf{A}/\delta$. That is, we must show that $[\theta]^n \leq \delta$ for some n is equivalent to $[\theta]_\delta^m = \delta$ for some m. Since $[\theta]^n \leq [\theta]_\delta^n$ for all n, we certainly get that $[\theta]_\delta^n = \delta$ implies $[\theta]^n \leq \delta$. The reverse implication follows from the fact that when $\delta \leq \theta$, then $[\theta]_\delta^n = [\theta]^n \vee \delta$ for all n. (This can be proved by a straightforward induction on n using Lemmas 2.4 and 2.5.)

LEMMA 3.2 *Assume that $\mathcal{V}$ has a difference term and $\mathbf{A} \in \mathcal{V}$. Then*

(i) $\overset{s}{\sim}$ *is a congruence on* **ConA**.

(ii) If $\delta \leq \alpha, \beta$, then $\alpha \overset{s}{\sim} \beta$ iff $\alpha/\delta \overset{s}{\sim} \beta/\delta$ in **ConA**$/\delta$.

(iii) $\overset{s}{\sim}$*-classes are convex sublattices of permuting congruences.*

(iv) **ConA**$/\overset{s}{\sim}$ *is meet-semidistributive.*

Proof: For (i) the definition of $\overset{s}{\sim}$ shows that it is a reflexive, symmetric relation on **ConA**. To prove transitivity we must show that if $[\alpha \vee \beta]^j \leq \alpha \wedge \beta$ and $[\beta \vee \gamma]^k \leq \beta \wedge \gamma$, then for some l it is the case that

$$[\alpha \vee \gamma]^l \leq \alpha \wedge \gamma.$$

First note that

$$[\alpha]^j \leq [\alpha \vee \beta]^j \leq \alpha \wedge \beta \leq \beta$$

and

$$[\beta]^k \leq [\beta \vee \gamma]^k \leq \beta \wedge \gamma \leq \gamma.$$

Together these two lines imply that $[\alpha]^{jk} \leq \gamma$. We trivially have $[\alpha]^{jk} \leq \alpha$, so

$$[\alpha]^{jk} \leq \alpha \wedge \gamma.$$

Similarly, $[\gamma]^{jk} \leq \alpha \wedge \gamma$. But now, using the common generalization of Theorem 2.10 II (v) and II (iv) which we described after the statement of Theorem 2.10, it is easy to see that

$$[\alpha \vee \gamma]^{2n} \leq [\alpha]^n \vee [\gamma]^n.$$

Thus, for us,

$$\begin{aligned}[\alpha \vee \gamma]^{2jk} &\leq [\alpha]^{jk} \vee [\gamma]^{jk} \\ &\leq \alpha \wedge \gamma.\end{aligned}$$

To show that $\overset{s}{\sim}$ is compatible with $\vee$ we must show that if $\alpha \overset{s}{\sim} \beta$, then $\alpha \vee \gamma \overset{s}{\sim} \beta \vee \gamma$ for any γ. The former condition means that $[\alpha \vee \beta]^j \leq \alpha \wedge \beta$ for some j while latter is established by showing that

$$[\alpha \vee \beta \vee \gamma]^k \leq (\alpha \vee \gamma) \wedge (\beta \vee \gamma)$$

for some k. Using the idea of the previous paragraph twice we have

$$\begin{aligned}[(\alpha \vee \beta) \vee \gamma]^{4n} &\leq [\alpha \vee \beta]^{2n} \vee [\gamma]^{2n} \\ &\leq [\alpha]^n \vee [\beta]^n \vee [\gamma]^n.\end{aligned}$$

Hence we can finish this part of the argument by showing that each of $[\alpha]^n$, $[\beta]^n$ and $[\gamma]^n$ is less than or equal to $(\alpha \vee \gamma) \wedge (\beta \vee \gamma)$ for sufficiently large n. Note that

$$\begin{aligned}[\alpha]^j &\leq [\alpha \vee \beta]^j \\ &\leq \alpha \wedge \beta \\ &\leq (\alpha \vee \gamma) \wedge (\beta \vee \gamma).\end{aligned}$$

Similarly, $[\beta]^j \leq (\alpha \vee \gamma) \wedge (\beta \vee \gamma)$. Finally,

$$[\gamma]^m \leq \gamma \leq (\alpha \vee \gamma) \wedge (\beta \vee \gamma)$$

for all m. We get that

$$[\alpha \vee \beta \vee \gamma]^{4j} \leq (\alpha \vee \gamma) \wedge (\beta \vee \gamma)$$

as desired.

To show that $\stackrel{s}{\sim}$ is compatible with $\wedge$, assume that $\alpha \stackrel{s}{\sim} \beta$ which means that $[\alpha \vee \beta]^j \leq \alpha \wedge \beta$ for some j. Then for any γ we clearly have

$$[(\alpha \wedge \gamma) \vee (\beta \wedge \gamma)]^j \leq \gamma$$

and

$$[(\alpha \wedge \gamma) \vee (\beta \wedge \gamma)]^j \leq [\alpha \vee \beta]^j \leq \alpha \wedge \beta,$$

so $[(\alpha \wedge \gamma) \vee (\beta \wedge \gamma)]^j \leq \alpha \wedge \beta \wedge \gamma$. This finishes the proof that $\stackrel{s}{\sim}$ is a congruence.

Next we prove (ii). From the remarks following Definition 3.1, $\alpha \stackrel{s}{\sim} \beta$ iff $(\alpha \vee \beta)/(\alpha \wedge \beta)$ is solvable in $\mathbf{A}/(\alpha \wedge \beta)$ and similarly $\alpha/\delta \stackrel{s}{\sim} \beta/\delta$ iff $((\alpha \vee \beta)/\delta)/((\alpha \wedge \beta)/\delta)$ is solvable in $(\mathbf{A}/\delta)/(\alpha \wedge \beta)/\delta$. The equivalence of $\alpha \stackrel{s}{\sim} \beta$ and $\alpha/\delta \stackrel{s}{\sim} \beta/\delta$ now follows from the Second Isomorphism Theorem.

For (iii), note that since $\stackrel{s}{\sim}$ is a lattice congruence, its classes are convex sublattices. We must show that if $\alpha \stackrel{s}{\sim} \beta$, then $\alpha \circ \beta = \beta \circ \alpha$. Choose n such that $[\alpha \vee \beta]^n \leq \alpha \wedge \beta$. Then $[\alpha]^n \leq \beta$, so Lemma 2.7 $(i) \Leftrightarrow (iii)$ insures that $\alpha \circ \beta \subseteq \beta \circ \alpha$. The opposite inclusion follows similarly, so α and β permute.

Finally we show that $\mathbf{ConA}/\stackrel{s}{\sim}$ is meet-semidistributive. We assume otherwise and argue to a contradiction. The claim that $\mathbf{ConA}$ is not meet-semidistributive is equivalent to the assertion that there exist $\alpha, \beta, \gamma \in \mathrm{Con}\,\mathbf{A}$ such that

$$\alpha \wedge \beta \stackrel{s}{\sim} \alpha \wedge \gamma \quad \text{but} \quad \alpha \wedge \beta \stackrel{s}{\not\sim} \alpha \wedge (\beta \vee \gamma).$$

Let

(i) $\alpha' = \alpha \wedge (\beta \vee \gamma)$,

(ii) $\beta' = \beta \vee (\alpha \wedge \gamma)$ and

(iii) $\gamma' = \gamma \vee (\alpha \wedge \beta)$.

Claim. $\alpha' \wedge \beta' = \alpha' \wedge \gamma'$, but $\alpha' \wedge (\beta' \vee \gamma') = \alpha' \stackrel{s}{\not\sim} \alpha' \wedge \beta'$.

Proof of Claim: First, $\beta' = \beta \vee (\alpha \wedge \gamma) \stackrel{s}{\sim} \beta \vee (\alpha \wedge \beta) = \beta$ and similarly $\gamma' \stackrel{s}{\sim} \gamma$. Define $\theta = \alpha' \wedge \beta'$ and note that $\theta = \alpha' \wedge \beta' = \alpha \wedge \beta' \stackrel{s}{\sim} \alpha \wedge \beta$. Define $\delta = (\alpha \wedge \beta) \vee (\alpha \wedge \gamma)$ and note that $\alpha \wedge \beta \leq \delta \leq \theta \leq \alpha$. In particular, $\theta \stackrel{s}{\sim} \delta \stackrel{s}{\sim} \alpha \wedge \beta$. Using Lemma 2.7 and the fact that $[\delta]^n \leq \alpha \wedge \beta$ for some n we have

$$\delta \circ \beta \subseteq [\delta]^n \circ \beta \circ \delta \subseteq \beta \circ \delta.$$

Hence $\beta \vee \delta = \beta \circ \delta$. But $\beta \vee \delta = \beta' \geq \theta \geq \delta$. If there exists a pair $(a, b) \in \theta - \delta$, then $(a, b) \in \beta \circ \delta - \delta$. For such a pair there is a $c \in A$ such that $a\ \beta\ c\ \delta\ b$. Since $(a, b) \in \theta$ we get $c\ \delta\ b\ \theta\ a$. Hence $(a, c) \in \beta \wedge \theta$ $= \alpha' \wedge \beta = \alpha \wedge \beta \leq \delta$. This proves that $a\ \delta\ c\ \delta\ b$ which contradicts our choice of $(a, b) \notin \delta$. We conclude that $\theta = \delta$. Referring back to the definition of δ and θ, this tells us that

$$\alpha' \wedge \beta' = (\alpha \wedge \beta) \vee (\alpha \wedge \gamma).$$

A symmetric argument with γ' in place of β' shows that

$$\alpha' \wedge \gamma' = (\alpha \wedge \beta) \vee (\alpha \wedge \gamma).$$

Hence $\alpha' \wedge \beta' = \alpha' \wedge \gamma'$ as we claimed.

For the second part of the Claim we observe that $\beta' \vee \gamma' = \beta \vee \gamma$, so $\alpha' \wedge (\beta' \vee \gamma') = \alpha'$. From this and our hypothesis that $\alpha \wedge \beta \overset{s}{\not\sim} \alpha \wedge (\beta \vee \gamma) = \alpha'$ we get that

$$\alpha' \wedge (\beta' \vee \gamma') = \alpha' \overset{s}{\not\sim} \alpha \wedge \beta \overset{s}{\sim} \alpha' \wedge \beta'.$$

(The fact used here that $\alpha' \wedge \beta' = \alpha \wedge \beta' \overset{s}{\sim} \alpha \wedge \beta$ follows immediately from the definitions for α' and β'.) This finishes the proof of the Claim.

To continue with the proof of the lemma, let $\lambda = \alpha' \wedge \beta'$. From the claim we have $\alpha' \wedge \beta' = \lambda = \alpha' \wedge \gamma'$. Hence $C(\beta', \alpha'; \lambda)$ and $C(\gamma', \alpha'; \lambda)$ hold. Thus $C(\beta' \vee \gamma', \alpha'; \lambda)$ holds too. Since $\beta' \vee \gamma' = \beta \vee \gamma \geq \alpha'$, we have $C(\alpha', \alpha'; \lambda)$, so $[\alpha', \alpha'] \leq \lambda = \alpha' \wedge \beta' \leq \alpha'$. This implies $\alpha' \overset{s}{\sim} \alpha' \wedge \beta'$ which is contrary to the previous Claim. The only unjustified assumption that we have made is that $\mathbf{ConA}/\overset{s}{\sim}$ is not meet-semidistributive, so this possibility must be discarded. This proves (iv) and concludes the proof of the lemma. □

We will refer to the fact that $\overset{s}{\sim}$ satisfies Lemma 3.2 (ii) by saying that $\overset{s}{\sim}$ is **preserved by homomorphisms**.

If $\mathbf{A}$ has congruences δ, θ and γ such that $\delta < \theta$, $\delta \vee \gamma \geq \theta$ and $\theta \wedge \gamma \leq \delta$, then $\{\delta, \theta, \gamma\}$ generates a sublattice of $\mathbf{ConA}$ isomorphic to the five element non-modular lattice, $\mathbf{N}_5$. In such a sublattice it is common to call the interval $I[\delta, \theta]$ the **critical interval**. We will call $I[\delta, \theta]$ a **neutral** interval of a congruence lattice if $[\alpha, \beta]_\delta = \alpha \wedge \beta$ holds whenever $\alpha, \beta \in I[\delta, \theta]$. This is equivalent to asserting that $[\alpha, \alpha]_\delta = \alpha$ for all $\alpha \in I[\delta, \theta]$, clearly. It is also equivalent to the assertion that $C(\theta', \theta'; \delta')$ fails whenever $\delta \leq \delta' < \theta' \leq \theta$. In particular, if $I[\delta, \theta]$ is neutral and $\alpha, \beta \in I[\delta, \theta]$ are solvably related congruences, then $\alpha = \beta$.

THEOREM 3.3 *If $\mathcal{V}$ is a variety, then the following conditions are equivalent.*

(a) *$\mathcal{V}$ has a difference term.*

(b) *For each $\mathbf{A} \in \mathcal{V}$ the relation $\overset{s}{\sim}$ is a congruence on $\mathbf{ConA}$ which is preserved by homomorphisms. Furthermore, whenever $\mathbf{N}_5$ is a sublattice of $\mathbf{ConA}$, then the critical interval is neutral.*

(c) *For some n $\mathcal{V}$ has terms $m_0(x, y, z, u), \ldots, m_{3n}(x, y, z, u)$ for which the following equations and relation hold.*

- (i) $m_0(x, y, z, u) = x$, $m_{3n}(x, y, z, u) = u$,
- (ii) $m_i(x, y, y, x) = x$ *for all* i,
- (iii) $m_{3i}(x, x, y, y) = m_{3i+1}(x, x, y, y)$,
- (iv) $m_{3i+1}(x, y, y, u) = m_{3i+2}(x, y, y, u)$,
- (v) $m_{3i+2}(x, y, z, u)\ [\alpha, \alpha]\ m_{3i+3}(x, y, z, u)$ *for any congruence* α *with* $(x, u) \in \alpha$.

Proof: If (a) holds, then we have just finished showing that $\overset{s}{\sim}$ is a congruence which is preserved by homomorphisms. To show that the remainder of condition (b) holds, assume that $\mathbf{A} \in \mathcal{V}$ and that $\mathbf{A}$ has congruences δ, θ and γ such that $\delta < \theta$, $\delta \vee \gamma \geq \theta$ and $\theta \wedge \gamma \leq \delta$. We must show that the interval $I[\delta, \theta]$, which is the critical interval of the $\mathbf{N}_5$ generated by $\{\delta, \theta, \gamma\}$, is neutral. If instead one can find congruences δ', θ' such that $\delta \leq \delta' < \theta' \leq \theta$ such that $C(\theta', \theta'; \delta')$ holds, then $\{\delta', \theta', \gamma\}$ generate a copy of $\mathbf{N}_5$ and now we have $[\theta', \theta'] \leq \delta'$. Changing notation back, we see that it is enough for us to prove from (a) that $\mathbf{ConA}$ has no copy of $\mathbf{N}_5$ with critical interval $I[\delta, \theta]$ where $[\theta, \theta] \leq \delta$.

In order to obtain a contradiction, we assume that $\gamma \vee \delta \geq \theta$, $\gamma \wedge \theta \leq \delta$ and $[\theta, \theta] \leq \delta < \theta$. As is usual, we will write $\alpha \circ_n \beta$ to denote the n-fold composition of the congruences α and β beginning with α. That is,

$$\alpha \circ_n \beta = \underbrace{\alpha \circ \beta \circ \alpha \circ \cdots}_{n-1 \text{ occurrences of } \circ}.$$

Since $\delta < \theta \leq \gamma \vee \delta$, it follows that for some n the set $\theta \cap (\gamma \circ_n \delta)$ properly contains δ. For the rest of this proof we fix n to be the least value for which this is true. This value of n must be odd, for otherwise we obtain that $\theta \cap (\gamma \circ_{n-1} \delta) = \delta$ while there is some $(a, b) \in \theta \cap ((\gamma \circ_{n-1} \delta) \circ \delta) - \delta$. But for this (a, b) we can find a $c \in A$ such that

$$a \; (\gamma \circ_{n-1} \delta) \; c \; \delta \; b$$

and for this c we have $c \; \delta \; b \; \theta \; a$. Therefore $(a, c) \in \theta \cap (\gamma \circ_{n-1} \delta) = \delta$. This gives us that $a \; \delta \; c \; \delta \; b$ which is false since, by our choice, we have $(a, b) \notin \delta$.

Since n is odd, the composition $\gamma \circ_n \delta$ begins and ends with γ. As before, for a given $(a, b) \in \theta \cap (\gamma \circ_n \delta) - \delta$ we can find a $c \in A$ such that

$$a \; (\gamma \circ_{n-1} \delta) \; c \; \gamma \; b.$$

For this c we have

$$a = d(c, c, a) \; \psi^{\cup} \; d(b, a, a) \; [\theta, \theta] \; b.$$

Here $\psi := \gamma \circ_{n-1} \delta$ and $\psi^{\cup}$ is the converse of ψ. Our claim that $(d(c, c, a), d(b, a, a)) \in \psi^{\cup}$ comes from the fact that $\psi^{\cup}$ is a subalgebra of $\mathbf{A} \times \mathbf{A}$ which contains (c, a) (by the choice of c) and (c, b) and (a, a) (since in fact $\gamma \subseteq \psi^{\cup}$).

We arranged things so that $[\theta, \theta] \leq \delta$ and so that $(a, b) \in \theta$. For $e := d(b, a, a)$ our last displayed equation implies that $a = \psi^{\cup} \; e \; \delta \; b \; \theta \; a$ and so

$$(e, a) \in \theta \cap \psi = \delta.$$

But this forces $a \; \delta \; e \; \delta \; b$ which contradicts $(a, b) \notin \delta$. This contradiction shows that it is impossible to have $[\theta, \theta] \leq \delta$ when $I[\delta, \theta]$ is the critical interval in an $\mathbf{N}_5$. The proof that $(a) \Rightarrow (b)$ is complete.

Next we assume that (b) holds and prove (c). Our argument will by a modification of Alan Day's argument which associates a Mal'cev condition to congruence modularity. Let $\mathbf{F} = \mathbf{F}_{\mathcal{V}}(x, y, z, u)$ and define congruences

$$\begin{aligned}
\gamma &:= \mathrm{Cg}^{\mathbf{F}}(\{(x, y), (z, u)\}), \\
\theta &:= \mathrm{Cg}^{\mathbf{F}}(\{(x, u), (y, z)\}), \\
\alpha &:= \mathrm{Cg}^{\mathbf{F}}(x, u), \\
\beta &:= \mathrm{Cg}^{\mathbf{F}}(y, z), \text{ and} \\
\chi &:= \gamma \wedge \theta.
\end{aligned}$$

Let $\delta = \beta \vee \chi$ $(\leq \theta)$. Since $\gamma \wedge \theta \leq \delta$ and $\gamma \vee \delta = \gamma \vee \theta \geq \theta$ it follows that $\delta = \theta$ or $I[\delta, \theta]$ is the critical interval of a copy of $\mathbf{N}_5$ generated by $\{\delta, \theta, \gamma\}$. Now $\theta = \beta \vee \alpha$ so, since $\beta \leq \delta \leq \theta$, we must have $\theta = \delta \vee \alpha$. From this we get

$$\delta \leq \delta \vee [\alpha, \alpha] \overset{s}{\sim} \delta \vee \alpha = \theta.$$

The interval $I[(\delta \vee [\alpha, \alpha]), \theta]$ either has one element or it is a solvable subinterval of the critical interval $I[\delta, \theta]$. But critical intervals of $\mathbf{N}_5$s have no solvable subintervals by condition (b) of the theorem. We conclude that $\delta \vee [\alpha, \alpha] = \theta$. Since $\delta = \beta \vee \chi$, we may rewrite this as

$$\chi \vee \beta \vee [\alpha, \alpha] = \theta.$$

θ is the congruence generated by (x, u) and β, so we may rewrite the previous displayed equality as the following equivalent statement:

$$(x, u) \in \chi \vee \beta \vee [\alpha, \alpha].$$

Better yet, we write: $(x, u) \in (\chi \circ \beta \circ [\alpha, \alpha])^n$ for some n. This yields the existence of elements $m_0, \ldots, m_{3n} \in F$ such that

(1) $m_0 = x$, $m_{3n} = u$,

(2) $m_i \; \theta \; x$ for all i,

(3) $m_{3i} \; \chi \; m_{3i+1}$,

(4) $m_{3i+1} \; \beta \; m_{3i+2}$,

(5) $m_{3i+2} \; [\alpha, \alpha] \; m_{3i+3}$.

For each i let $m_i(x, y, z, u)$ denote a term representing the element m_i. The usual arguments for Mal'cev conditions based on the universal mapping property of $\mathbf{F}$ apply to show that conditions $(1)-(4)$ imply that the terms chosen satisfy the equations listed as $(i) - (iv)$ of the theorem. Admittedly, it is not common to consider conditions like (5). But we showed in the proof of Lemma 2.7 why conditions like (5) imply corresponding conditions like (v) throughout the variety. The same type of argument works here. This explains why (b) implies (c) in the theorem.

Our proof that (c) implies (a) is a modification of Christian Herrmann's construction of a difference term from the Day terms associated with a congruence modular variety. Define $q_0(x, y, z) = z$ and

$$\begin{aligned} q_{2i+1}(x, y, z) &= m_{3i+1}(q_{2i}(x, y, z), x, y, q_{2i}(x, y, z)) \\ q_{2i}(x, y, z) &= m_{3i+3}(q_{2i+1}(x, y, z), y, x, q_{2i+1}(x, y, z)) \end{aligned}$$

and $d(x, y, z) = q_{2n}(x, y, z)$. By equation (ii) from condition (c) we have

$$q_{2i+1}(x, x, y) = m_{3i+1}(q_{2i}(x, x, y), x, x, q_{2i}(x, x, y)) = q_{2i}(x, x, y)$$

and

$$q_{2i+2}(x, x, y) = m_{3i+3}(q_{2i+1}(x, x, y), x, x, q_{2i+1}(x, x, y)) = q_{2i+1}(x, x, y).$$

Since $q_0(x, x, y) = y$ we get by induction that $q_j(x, x, y) = y$ for all j. Hence $d(x, x, y) = y$. We now need to verify that in any algebra $\mathbf{A} \in \mathcal{V}$ we have $d(x, y, y) \; [\lambda, \lambda] \; x$ whenever λ is a congruence on $\mathbf{A}$ which contains (x, y). It will suffice to prove inductively that

$$q_{2i}(x, y, y) \; [\lambda, \lambda] \; m_{3i}(y, y, x, x)$$

and

$$q_{2i+1}(x, y, y) \; [\lambda, \lambda] \; m_{3i+1}(y, y, y, x).$$

(For then $d(x, y, y) \; [\lambda, \lambda] \; m_{3n}(y, y, x, x) = x$.)

Certainly $q_0(x, y, y) = y = m_0(y, y, x, x)$. From equations $(c)(ii)$ and $(c)(iii)$ we have

$$\begin{aligned} m_{3i+1}(m_{3i}(y, y, x, x), x, \underline{x}, m_{3i}(y, y, x, x)) &= m_{3i}(y, y, x, x) \\ &= m_{3i+1}(y, y, x, x) \\ &= m_{3i+1}(m_{3i}(y, y, y, y), y, \underline{x}, m_{3i}(x, x, x, x)). \end{aligned}$$

Changing the $\underline{x}$ to y we obtain

$$m_{3i+1}(m_{3i}(y, y, x, x), x, y, m_{3i}(y, y, x, x)) \; [\mathrm{Cg}(x, y), \mathrm{Cg}(x, y)] \; m_{3i+1}(m_{3i}(y, y, y, y), y, y, m_{3i}(x, x, x, x))$$

and the latter operation simplifies to $m_{3i+1}(y,y,y,x)$. From $q_{2i}(x,y,y)\ [\lambda,\lambda]\ m_{3i}(y,y,x,x)$ we deduce

$$\begin{aligned} q_{2i+1}(x,y,y) &= m_{3i+1}(q_{2i}(x,y,y),x,y,q_{2i}(x,y,y)) \\ &[\lambda,\lambda]\ m_{3i+1}(m_{3i}(y,y,x,x),x,x,m_{3i}(y,y,x,x)) \\ &[\mathrm{Cg}(x,y),\mathrm{Cg}(x,y)]\ m_{3i+1}(m_{3i}(y,y,y,y),y,y,m_{3i}(x,x,x,x)) \\ &= m_{3i+1}(y,y,y,x). \end{aligned}$$

Thus $q_{2i+1}(x,y,y)\ [\lambda,\lambda]\ m_{3i+1}(y,y,y,x)$ follows from $q_{2i}(x,y,y)\ [\lambda,\lambda]\ m_{3i}(y,y,x,x)$.

From $(c)(ii)$ and $(c)(iv)$ we have

$$\begin{aligned} m_{3i+2}(m_{3i+1}(y,y,y,x),y,\underline{y},m_{3i+1}(y,y,y,x)) &= m_{3i+1}(y,y,y,x) \\ &= m_{3i+2}(y,y,y,x) \\ &= m_{3i+2}(m_{3i+1}(y,y,y,y),y,\underline{y},m_{3i+1}(x,x,x,x)). \end{aligned}$$

Changing the $\underline{y}$ to x we obtain

$$m_{3i+2}(m_{3i+1}(y,y,y,x),y,x,m_{3i+1}(y,y,y,x))\ [\mathrm{Cg}(x,y),\mathrm{Cg}(x,y)]\ m_{3i+2}(m_{3i+1}(y,y,y,y),y,x,m_{3i+1}(x,x,x,x)).$$

Using $(c)(v)$ twice we get

$$\begin{aligned} &m_{3i+3}(m_{3i+1}(y,y,y,x),y,x,m_{3i+1}(y,y,y,x)) \\ &[\mathrm{Cg}(x,y),\mathrm{Cg}(x,y)]\ m_{3i+2}(m_{3i+1}(y,y,y,x),y,x,m_{3i+1}(y,y,y,x)) \\ &[\mathrm{Cg}(x,y),\mathrm{Cg}(x,y)]\ m_{3i+2}(m_{3i+1}(y,y,y,y),y,x,m_{3i+1}(x,x,x,x)) \\ &= m_{3i+2}(y,y,x,x) \\ &[\mathrm{Cg}(x,y),\mathrm{Cg}(x,y)]\ m_{3i+3}(y,y,x,x). \end{aligned}$$

From $q_{2i+1}(x,y,y)\ [\lambda,\lambda]\ m_{3i+1}(y,y,y,x)$ we deduce

$$\begin{aligned} q_{2i+2}(x,y,y) &= m_{3i+3}(q_{2i+1}(x,y,y),y,x,q_{2i+1}(x,y,y)) \\ &[\lambda,\lambda]\ m_{3i+3}(m_{3i+1}(y,y,y,x),y,x,m_{3i+1}(y,y,y,x)) \\ &[\mathrm{Cg}(x,y),\mathrm{Cg}(x,y)]\ m_{3i+3}(y,y,x,x). \end{aligned}$$

We get that $q_{2i+2}(x,y,y)\ [\lambda,\lambda]\ m_{3i+3}(y,y,y,x)$ follows from $q_{2i}(x,y,y)\ [\lambda,\lambda]\ m_{3i}(y,y,x,x)$. These calculations hold in any member of $\mathcal{V}$ if λ is a congruence containing (x,y). This completes the proof. □

As promised in the introduction, we now show that in a variety with a difference term the congruence intervals defined by failures of the modular law must be neutral.

COROLLARY 3.4 *If $\mathcal{V}$ has a difference term, then for each $\mathbf{A}\in\mathcal{V}$ and any congruences α,β and γ on $\mathbf{A}$ with $\alpha\geq\gamma$ it is the case that the interval $I=I[(\alpha\wedge\beta)\vee\gamma,\alpha\wedge(\beta\vee\gamma)]$ is neutral.*

Proof: Assume that $\mathcal{V}$ has a difference term. If I has only one element, then it is trivially a neutral interval. Otherwise,

$$\delta=(\alpha\wedge\beta)\vee\gamma<\alpha\wedge(\beta\vee\gamma)=\theta$$

and in this case $\{\delta,\theta,\beta\}$ generates a copy of $\mathbf{N}_5$ which has critical interval I. By Theorem 3.3, this interval is neutral. □

Before restricting our attention to locally finite varieties, let us consider one side issue that is a consequence of Theorem 3.3.

Definition 3.5 If α and β are congruences on $\mathbf{A}$, then we write $\alpha \overset{n}{\sim} \beta$ and say that α and β are **neutrally related** if for some n it is the case that the interval $I[\alpha \wedge \beta, \alpha \vee \beta]$ is neutral.

LEMMA 3.6 *Assume that $\mathcal{V}$ has a difference term and $\mathbf{A} \in \mathcal{V}$. Then*

(*i*) $\overset{n}{\sim}$ *is a congruence on* $\mathbf{ConA}$.

(*ii*) *If $\delta \leq \alpha, \beta$, then $\alpha \overset{n}{\sim} \beta$ iff $\alpha/\delta \overset{n}{\sim} \beta/\delta$ in $\mathbf{ConA}/\delta$.*

(*iii*) $\overset{n}{\sim}$*-classes are convex, meet-semidistributive sublattices.*

(*iv*) $\mathbf{ConA}/\overset{n}{\sim}$ *is modular.*

Hence $\mathbf{ConA}$ *is a subdirect product of of a modular lattice and a meet-semidistributive lattice.*

Proof: We leave the proofs of (i) and (iv) to the reader. It is an elementary exercise in lattice theory to prove the following extension of $(i) + (iv)$: Assume that $\mathbf{L}$ is a lattice and that σ is a congruence on $\mathbf{L}$. Assume that no sublattice of $\mathbf{L}$ which is isomorphic to $\mathbf{N}_5$ has critical interval $I[\delta, \theta]$ such that $(\delta, \theta) \in \sigma$. Then define ρ by $(a, b) \in \rho$ iff $(a, b) \in L^2$ and σ restricts trivially to $I[a \wedge b, a \vee b]$. ρ is a congruence of $\mathbf{L}$ and $\mathbf{L}/\rho$ is modular. Of course, (i) and (iv) follow from this using $\sigma = \overset{s}{\sim}$.

For (ii), we observe that $\alpha \overset{n}{\not\sim} \beta$ iff there exist μ and ν such that $\alpha \wedge \beta \leq \mu < \nu \leq \alpha \vee \beta$ with $C(\nu, \nu; \mu)$. This is equivalent to saying that $(\alpha/\delta \wedge \beta/\delta) \leq \mu/\delta < \nu/\delta \leq (\alpha/\delta \vee \beta/\delta)$ and that $C(\nu/\delta, \nu/\delta; \mu/\delta)$ holds in $\mathbf{A}/\delta$. Therefore, it is equivalent to $\alpha/\delta \overset{n}{\not\sim} \beta/\delta$.

(iii) holds for any neutral interval in a congruence lattice because the commutator is semidistributive over join in its left variable.

The final remark of the lemma is a consequence of the obvious fact that $\overset{s}{\sim} \cap \overset{n}{\sim} = 0$. This completes the proof of the lemma. □

In the previous lemma if $\mathbf{ConA}$ has a maximal chain of finite length, then $(0, 1) \in \overset{s}{\sim} \vee \overset{n}{\sim}$ since $\alpha \overset{s}{\sim} \beta$ or $\alpha \overset{n}{\sim} \beta$ whenever α is covered by β. In this case $\overset{s}{\sim}$ and $\overset{n}{\sim}$ are complementary congruences on $\mathbf{ConA}$.

We now focus on locally finite varieties in order to answer Lipparini's question. An advantage that we have in the locally finite setting is that $\overset{s}{\sim}$ is a congruence on $\mathbf{ConA}$ that is preserved by homomorphisms whenever $\mathbf{A}$ is finite (see Chapter 7 of [6]).

COROLLARY 3.7 *A locally finite variety $\mathcal{V}$ has a difference term iff whenever $\mathbf{A} \in \mathcal{V}_{fin}$ has congruences which generate a copy of $\mathbf{N}_5$ with critical interval $I[\delta, \theta]$, then* $\mathrm{typ}\{\delta, \theta\} \subseteq \{\mathbf{3}, \mathbf{4}, \mathbf{5}\}$.

Proof: In Theorem 3.3 our arguments for the equivalence of $(a) - (c)$ remain valid if we restrict our attention to the 4-generated algebras of $\mathcal{V}$. As we mentioned before the statement of the corollary, for any finite algebra $\overset{s}{\sim}$ is a congruence which is preserved by homomorphisms. Therefore, a locally finite variety has a difference term iff whenever $\mathbf{A} \in \mathcal{V}_{fin}$ has congruences which generate a copy of $\mathbf{N}_5$ with critical interval $I[\delta, \theta]$, then $I[\delta, \theta]$ is neutral. Basic tame congruence theory tells that $I[\delta, \theta]$ is neutral exactly when $\mathrm{typ}\{\delta, \theta\} \subseteq \{\mathbf{3}, \mathbf{4}, \mathbf{5}\}$. □

We leave it to the reader to show how to derive the converse of Corollary 3.4 for locally finite varieties using Corollary 3.7.

THEOREM 3.8 *Assume that $\mathcal{V}$ is a variety with a difference term and that $\mathbf{A} \in \mathcal{V}$ is finite. Then*

(*i*) $\mathbf{1} \notin \mathrm{typ}\{\mathbf{A}\}$ *and*

(*ii*) *all type* $\mathbf{2}$ *minimal sets of* $\mathbf{A}$ *have empty tail.*

Proof: Any difference term for $\mathcal{V}$ is Mal'cev on the blocks of any abelian congruence on any algebra in $\mathcal{V}$. This is enough to force $\mathbf{1} \notin \mathrm{typ}\{\mathbf{A}\}$ for any $\mathbf{A} \in \mathcal{V}$.

To prove that condition (*ii*) holds for any $\mathbf{A} \in \mathcal{V}$ it will suffice to prove that for all $\mathbf{A} \in \mathcal{V}$ and all $\langle 0, \alpha\rangle$-minimal sets U, where $\mathrm{typ}(0, \alpha) = \mathbf{2}$, it is the case that U has empty tail. The ideas in this proof are not new. Everything we use comes from Lemmas 4.20 and 4.25 of [6] except that we use some facts from [9] to shorten the argument.

Choose $e \in E(\mathbf{A})$ such that $e(A) = U$. Let $p(x, y, z) = ed(x, y, z)$ where $d(x, y, z)$ is the difference term for $\mathcal{V}$. Let $N \subseteq U$ be a $\langle 0, \alpha\rangle$-trace. $d(x, y, z)$ is Mal'cev on any α-class, hence on N, so (I) $p(x, y, y) = ed(x, y, y) = x$ on N. We also have (II) $p(x, x, y) = y$ on U since d is a difference term. We shall argue that (I) and (II) are incompatible with the assumption that U has nonempty tail.

Define $v(x, y) = p(x, y, y)$ and iterate $v(x, y)$ k times in its first variable for some $k > 1$ chosen so that

$$v^k(x, y) := v(v(\cdots v(v(x, y), y), \cdots), y)$$

satisfies $v^k(v^k(x, y), y) = v^k(x, y)$. Let B be the body of U. Observe that B is closed under $v^k(x, y)$, since $v^k(x, x) = x$ on U and B is a congruence class of the algebra $\mathbf{A}|_U$. If $n \in N$, then $v(x, n) = x$ on N, so $v^k(x, n) = x$ on N. The polynomial $v^k(x, n)$ is therefore an idempotent permutation of U and so $v^k(x, n) = x$ on U. If b is any other element of B, then the polynomial $v^k(x, b)$ of $\mathbf{A}|_B$ has the same range as $v^k(x, n)$ since $\mathbf{A}|_B$ is a coherent nilpotent algebra. (For more detail: $\mathbf{A}|_B$ is nilpotent by Theorem 4.31 and Lemma 4.36 of [6]. $\mathbf{A}|_B$ omits type $\mathbf{1}$ since it has a Mal'cev polynomial. Any algebra which omits type $\mathbf{1}$ is coherent. It is shown in [9] that a coherent algebra $\mathbf{C}$ is nilpotent iff for all $a, b \in C$ and all $e(x, y) \in \mathrm{Pol}_2\mathbf{C}$ satisfying $e(e(x, y), y) = e(x, y)$ it is the case that $e(x, a)$ and $e(x, b)$ have ranges of the same cardinality. Since $v^k(x, n)$ is a permutation of B, so is $v^k(x, b)$.) Both $v^k(x, n)$ and $v^k(x, b)$ are idempotent permutations of U, so $v^k(x, b) = x$ for all $b \in B$.

For $p'(x, y, z) = v^{k-1}(p(x, y, z), z)$ we have $p'(x, y, y) = v^k(x, y)$. If $b \in B$, then $p'(x, b, b) = x$ on U by the final conclusion of the previous paragraph. Furthermore $p'(x, x, y) = v^{k-1}(p(x, x, y), y) = v^{k-1}(y, y) = y$ for all $x, y \in U$. Now we assume that the tail of U is nonempty and we choose $t \in U - B$. Define $h(x) = p'(x, p'(t, p'(t, x, n), n), n)$. If $m \in N$, then

$$p'(t, m, n) \equiv_\alpha p'(t, n, n) = t.$$

But the $\alpha|_U$-class of t is just $\{t\}$ since $t \in U - B$. Hence $p'(t, m, n) = t$ for all $m \in N$ and we deduce that

$$h(m) = p'(m, p'(t, t, n), n) = p'(m, n, n) = m.$$

Since $h(m) = m$ on N, h is a permutation of U. But

$$\begin{aligned} h(t) &= p'(t, p'(t, p'(t, t, n), n), n) \\ &= p'(t, p'(t, n, n), n) \\ &= p'(t, t, n) \\ &= n = h(n). \end{aligned}$$

This is a contradiction since h is a permutation of U, $n \in N \subseteq B$ and $t \in U - B$. $\square$

THEOREM 3.9 *Let $\mathcal{V}$ be a variety such that $\mathbf{F}_{\mathcal{V}}(2)$ is finite. Then $\mathcal{V}$ has a difference term iff for any finite $\mathbf{A} \in \mathcal{V}$ it is the case that*

(*i*) $\mathbf{1} \notin \mathrm{typ}\{\mathbf{A}\}$ *and*

(*ii*) *all type* $\mathbf{2}$ *minimal sets of* $\mathbf{A}$ *have empty tail.*

Proof: As mentioned in the introduction, it suffices to prove the theorem for locally finite varieties only. If $\mathcal{V}$ has a difference term, then (*i*) and (*ii*) must hold by Theorem 3.8.

Conversely, by Corollary 3.7, we must show that if (*i*) and (*ii*) hold then whenever $\mathbf{A} \in \mathcal{V}_{fin}$ has congruences which generate a copy of $\mathbf{N}_5$ with critical interval $I[\delta, \theta]$, then $\mathrm{typ}\{\delta, \theta\} \subseteq \{\mathbf{3}, \mathbf{4}, \mathbf{5}\}$. In order to prove that the critical interval of any $\mathbf{N}_5$ contains only types from $\{\mathbf{3}, \mathbf{4}, \mathbf{5}\}$ it will suffice to prove that no type $\mathbf{2}$ label occurs in a critical interval. Assume otherwise that some finite algebra $\mathbf{A} \in \mathcal{V}$ has congruences $\delta \leq \alpha \prec \beta \leq \theta$, $\delta \vee \gamma \geq \theta$ and $\theta \wedge \gamma \leq \delta$ and that $\mathrm{typ}(\alpha, \beta) = \mathbf{2}$. Choose $U \in \mathrm{M}_{\mathbf{A}}(\alpha, \beta)$. The restriction map is a lattice homomorphism from $\mathbf{ConA}$ to $\mathbf{ConA}|_U$ and $\delta|_U \leq \alpha|_U < \beta|_U \leq \theta|_U$. It follows that $\{\delta|_U, \theta|_U, \gamma|_U\}$ generate a copy of $\mathbf{N}_5$ in the congruence lattice of $\mathbf{A}|_U$. But U has empty tail by (*ii*) of the theorem. In this case $\mathbf{A}|_U$ has a Mal'cev polynomial (by Theorem 4.31 of [6]) and so $\mathbf{ConA}|_U$ is modular. It is impossible for $\mathbf{ConA}|_U$ to contain a sublattice isomorphic to $\mathbf{N}_5$. We conclude that there is no type $\mathbf{2}$ quotient in the critical interval of any copy of $\mathbf{N}_5$ in $\mathbf{ConA}$. □

We record the following application. It has as a consequence that almost all of modular comutator theory holds for locally finite congruence semimodular varieties which omit type $\mathbf{1}$.

THEOREM 3.10 *The following conditions are equivalent for any congruence semimodular variety for which $\mathbf{F}_{\mathcal{V}}(2)$ is finite.*

(*i*) $\mathcal{V}$ *omits type* $\mathbf{1}$.

(*ii*) $\mathcal{V}$ *has a weak difference term.*

(*iii*) $\mathcal{V}$ *has a difference term.*

Proof: It suffices to prove the equivalence for the locally finite variety $\mathsf{HSP}(\mathbf{F}_{\mathcal{V}}(2))$. Theorem 7.12 of [6] proves the equivalence of (*i*) and (*ii*) for any locally finite variety. (*iii*) certainly implies (*ii*). To prove that (*i*) implies (*iii*) we will use Theorem 3.3 of this paper and Theorem 3.4 of [7]. The latter theorem proves that, in a locally finite congruence semimodular variety, the critical interval of any $\mathbf{N}_5$ occurring in the congruence lattice of a finite member of $\mathcal{V}$ has only type $\mathbf{1}$ and $\mathbf{5}$ labels. But condition (*i*) tells us that $\mathcal{V}$ omits type $\mathbf{1}$. We conclude that the critical interval of any $\mathbf{N}_5$ has only type $\mathbf{5}$ labels. For any finite algebra $\overset{s}{\sim}$ is a congruence preserved by homomorphisms, so Theorem 3.3 (*a*) $\Leftrightarrow$ (*b*) shows that (*iii*) holds. □

We close with a few remarks about weak difference terms. Several results in this paper hold for varieties that only have a weak difference term, but usually the necessary argument to prove these stronger versions is more involved. Lemma 3.2 (*i*) $-$ (*iii*) can be proved under the assumption that $\mathcal{V}$ has a weak difference term. In fact, the conditions 3.2 (*i*) $-$ (*iii*) characterize those *locally finite* varieties which have a weak difference term. We do not know if conditions 3.2 (*i*) $-$ (*iii*) characterize all varieties which have a weak difference term.

For locally finite varieties, condition (*iv*) of Lemma 3.2 also holds if $\mathcal{V}$ has a weak difference term, but we do not know if this happens when $\mathcal{V}$ is not locally finite. Certainly the proof we gave for Lemma 3.2 (*iv*) makes essential use of the fact that $\mathcal{V}$ has a difference term and not just a weak difference term.

Since any variety with a weak difference term satisfies conditions (i) and (ii) of Lemma 3.2, one can rephrase our characterization of varieties with a difference term in a way the does not refer to $\stackrel{s}{\sim}$: $\mathcal{V}$ has a difference term iff

(i) $\mathcal{V}$ has a weak difference term and

(ii) the critical interval of any $\mathbf{N}_5$ in the congruence lattice of a member of $\mathcal{V}$ is neutral.

References

[1] **R. Freese and R. McKenzie,** *Commutator Theory for Congruence Modular Varieties*, **LMS Lecture Notes No. 125, Cambridge University Press, 1987.**

[2] **H. -P. Gumm,** *Congruence modularity is permutability composed with distributivity*, **Archiv der Math. (Basel) 36 (1981), 569–576.**

[3] **H. -P. Gumm,** *Geometrical methods in congruence modular algebras*, **AMS Memoir No. 286, 1983.**

[4] **J. Hagemann and C. Herrmann,** *A concrete ideal multiplication for algebraic systems and its relation to congruence distributivity*, **Archiv der Math. (Basel) 32 (1979), 234–245.**

[5] **C. Herrmann,** *Affine algebras in congruence modular varieties,* **Acta Sci. Math. (Szeged) 41 (1979), 119–125.**

[6] **D. Hobby and R. McKenzie,** *The Structure of Finite Algebras*, **Contemporary Mathematics, American Mathematics Society, Providence, Rhode Island, 1988.**

[7] **K. Kearnes,** *Congruence lower semimodularity and 2-finiteness imply congruence modularity*, **Algebra Universalis 28 (1991), 1–11.**

[8] **K. Kearnes,** *Congruence permutable and congruence 3-permutable locally finite varieties*, **Journal of Algebra 156 (1993), 36–49.**

[9] **K. Kearnes,** *An order-theoretic property of the commutator*, **International Journal of Algebra and Computation, 3 (1993), 1–43.**

[10] **P. Lipparini,** *Commutator theory without join-distributivity*, **preprint.**

[11] **A. I. Mal'cev,** *On the general theory of algebraic systems*, **Mat. Sb. (77) 35 (1954), 3–20.**

[12] **E.W. Kiss and P. Pröhle,** *Problems and results in tame congruence theory*, **Preprint no. 60, Math. Inst. Hung. Acad., 1988.**

[13] **R. McKenzie, G. McNulty and W. Taylor,** *Algebras, Lattices and Varieties, vol. 1*, **Wadsworth & Brooks/Cole, 1987.**

[14] **J. D. H. Smith,** *Mal'cev Varieties*, **Lecture Notes in Math. 554, Berlin, 1976.**

[15] **M. Valeriote and R. Willard,** *A characterization of congruence permutable locally finite varieties*, **Journal of Algebra 140 (1991), 362–369.**

1991 *Mathematics subject classification*: **Primary 08B05, Secondary 08A40.**