Equations implying congruence n-permutability and semidistributivity

Ralph Freese

Abstract. In [3] T. Dent, K. Kearnes and Á. Szendrei define the *derivative*, Σ', of a set of equations Σ and show, for idempotent Σ, that Σ implies congruence modularity if Σ' is inconsistent ($\Sigma' \models x \approx y$). In this paper we investigate other types of derivatives that give similar results for congruence n-permutable for some n, and for congruence semidistributivity.

1. Introduction

In a recent paper [3] T. Dent, K. Kearnes and Á. Szendrei study Maltsev conditions which imply congruence modularity from the point of view of the equations. Given a set of equations Σ they define the *derivative* Σ' of Σ. (The definition is given below.) $\Sigma' \supseteq \Sigma$ and if Σ is idempotent then, if Σ' is inconsistent (that is, $\Sigma' \models x \approx y$), then any variety $\mathcal{V}$ that *realizes* Σ (each function symbol in Σ can be interpreted as a term of $\mathcal{V}$ such that the equations of Σ are satisfied) is congruence modular. While the converse is not true in general, they show that it is true if Σ is a set of *linear*, idempotent equations. So in particular if Σ consists of Day's equations [2] (for a fixed n) or Gumm's equations [6], then Σ' is inconsistent.

They use these results to prove interesting new results and give easy proofs of several existing theorems. One nice example: one of the equations in Day's characterization of congruence modularity [2] involves three variables:

$$m_i(x,u,u,y) \approx m_{i+1}(x,u,u,y) \qquad \text{for } i \text{ odd}$$

J. B. Nation wondered if there is a two-variable condition for congruence modularity. In [14] he showed that this is the case.

Using their results, the authors of [3] show that the above equation can be replaced by either

$$m_i(x,x,x,y) \approx m_{i+1}(x,x,x,y) \qquad \text{for } i \text{ odd}$$

or

$$m_i(x,y,y,y) \approx m_{i+1}(x,y,y,y) \qquad \text{for } i \text{ odd}$$

Presented by ...
Received ...; accepted in final form ...
2010 *Mathematics Subject Classification*: Primary: 08B05; Secondary: 08B10.
Key words and phrases: n-permutability, semidistributivity, congruence lattice.

and the resulting set of identities is still implies congruence modularity, and since these identities are weaker than Day's, they are also a Maltsev condition for congruence modularity.

The principal results of [3] for congruence modularity (CM) are summarized in the next theorem. Σ *idempotent* means $\Sigma \models f(x,\dots,x) \approx x$ for all operation symbols f occurring in Σ; it is *linear* if there is no nested composition in the terms occurring in Σ. If $\Sigma \models x \approx f(\mathbf{w})$, where $\mathbf{w}$ is a sequence of not necessarily distinct variables, then f is *weakly independent* of its i^{th} place for each i with $w_i \neq x$. (So a Maltsev term is weakly independent of all of its places.) The *derivative*, Σ', is the augmentation of Σ by equations that say that f is independent of its i^{th} place whenever Σ implies f is weakly independent of its i^{th} place.

Theorem 1 ([3])**.** *Let Σ be an idempotent set of equations. Then*

(1) *If Σ' is inconsistent then any variety that realizes Σ is congruence modular (CM).*
(2) *If $\mathcal{V}$ is a CM variety, then $\mathcal{V}$ realizes some Σ such that Σ' is inconsistent. (The Day terms work.)*
(3) *The converse of the first statement is not true in general but it is true if Σ is linear.*
(4) *For a finite linear, idempotent Σ one can effectively decide if Σ implies CM.*

The authors also show this theorem remains true if "congruence modularity" is replaced by "satisfies some nontrivial congruence identity" and "Σ' inconsistent" is replaced by "some iterated derivative of Σ in inconsistent."

For n-permutability we introduce another derivative, the order derivative, denoted Σ^+. We show the theorem above remains true if "congruence modularity" is replaced by "congruence n-permutable for some n" and "Σ' inconsistent" is replaced by "some iterated order derivative of Σ in inconsistent."

For semidistributivity we define the weak derivative, denoted Σ^*. In this case the analogs of conditions (1) and (2) hold, but (the second part of) (3) fails. Nevertheless we able to establish (4), both for semidistributivity and meet semidistributivity.

Part (4) of the above theorem and its variants show that for several properties one can effectively decide if a linear, idempotent Σ implies the property; that is every variety that realizes Σ has the property. A list of such properties is given near the end of the paper. This decidability contrasts the general result of G. McNulty [13] that without linearity all of these problems are undecidable.

The author would like to thank Ágnes Szendrei and Keith Kearnes for several helpful comments.

2. n-Permutability

A variety $\mathcal{V}$ is congruence n-permutable if for every $\mathbf{A} \in \mathcal{V}$ and every pair of congruences α and β, $\alpha \circ_n \beta = \beta \circ_n \alpha$, where $\alpha \circ_n \beta = \alpha \circ \beta \circ \alpha \circ \beta \circ \cdots$ is the n-fold relational product (there are $n-1$ occurrences of $\circ$).

Theorem 2. *The following are equivalent for a variety $\mathcal{V}$ and an integer n at least 2.*

(1) *$\mathcal{V}$ is congruence n-permutable.*
(2) *There are 3-place terms $p_0, \ldots, p_n$ such that the following hold in $\mathcal{V}$*

$$p_0(x,y,z) \approx x, \text{ and } p_n(x,y,z) \approx z$$
$$p_i(x,x,y) \approx p_{i+1}(x,y,y) \text{ for all } i.$$

(3) *The subalgebra of $\mathbf{F}^2_{\mathcal{V}}(x,y)$ generated by (x,x), (x,y) and (y,y) contains elements (a_i,b_i), $i = 0, \ldots n$, with $(y,y) = (a_0,b_0)$, $(x,x) = (a_n,b_n)$, and $b_i = a_{i+1}$.*

Proof. The first two are equivalent by the result of Hagemann and Mitschke [7]. They are equivalent to the third by a standard argument: if (2) holds, let $a_i = p_{n-i}(x,x,y)$ and $b_i = p_{n-i}(x,y,y)$. Then $(a_i,b_i) = p_{n-i}((x,x),(x,y),(y,y))$ and the properties of (3) hold. Conversely if (3) holds the terms giving the (a_i,b_i)'s, indexed backwards, satisfy (2). □

Theorem 3. *The following are equivalent for an idempotent variety $\mathcal{V}$.*

(1) *$\mathcal{V}$ is not congruence n-permutable for any n.*
(2) *$\mathcal{V}$ contains a nontrivial member $\mathbf{A}$ which has a bounded compatible order (one having a least and greatest element).*

Proof. Assume $\mathcal{V}$ is not n-permutable for any n. Let $\mathbf{F}$ be the free $\mathcal{V}$ algebra freely generated by x and y. Let $\mathbf{R}$ be the subalgebra of $\mathbf{F}^2$ generated by $\{(x,x),(x,y),(y,y)\}$ and let $\mathbf{T}$ be the transitive closure of $\mathbf{R}$. $\mathbf{T}$ is also a subalgebra of $\mathbf{F}^2$ and is reflexive and transitive so is a compatible quasiorder on $\mathbf{F}$. Clearly $(x,y) \in T$.

Suppose $(y,x) \in T$. Then there are elements $w_j \in F$, $j = 0, \ldots, n$, such that $w_0 = y$, $w_n = x$ and $(w_j, w_{j+1}) \in R$, $j < n$. Thus

$$(y,y),(y,w_1),(w_1,w_2),\ldots,(w_{n-1},x),(x,x)$$

are all in $\mathrm{Sg}_{\mathbf{F}^2}((x,x),(x,y),(y,y))$. By (3) of Theorem 2, $\mathcal{V}$ is n-permutable, a contradiction. Thus there is a compatible quasiordering $\leq$ on $\mathbf{F}$ with $x \leq y$ and $y \not\leq x$.

Let

$$\theta = \{(a,b) \in \mathbf{F}^2 : a \leq b \text{ and } b \leq a\}$$

be the equivalence relation associated with $\leq$. Since $\leq$ is compatible, θ is a congruence. Let $\mathbf{A} = \mathbf{F}/\theta$. $\mathbf{A}$ is nontrivial since $(x,y) \notin \theta$. And $\mathbf{A}$ has a compatible ordering which we also denote $\leq$. Using that $\mathcal{V}$ is idempotent, it

is easy to see that $0 = x/\theta$ is the least element and $1 = y/\theta$ is the greatest element in this ordering. This proves (1) $\implies$ (2).

For the other implication suppose $\mathbf{A} \in \mathcal{V}$ is nontrivial and has a compatible order with 0 and 1. If $\mathcal{V}$ has Hagemann-Mitschke terms then

$$1 = p_0^{\mathbf{A}}(1,1,0) = p_1^{\mathbf{A}}(1,0,0) \leq p_1^{\mathbf{A}}(1,1,0) = \cdots = p_n^{\mathbf{A}}(1,0,0) = 0,$$

a contradiction. □

Remark 4. This theorem remains true without the assumption that $\mathcal{V}$ is idempotent if (2) is changed to $\mathbf{A}$ having a compatible order which is not an antichain.

Let Σ be an idempotent set of equations. Define the *order derivative* of Σ, denoted Σ^+, to be the augmentation of Σ by additional equations as follows. If

$$\Sigma \models x \approx f(\mathbf{w})$$

where $\mathbf{w}$ is a vector of not necessarily distinct variables and f is an operation symbol occurring in Σ, then Σ^+ contains all equations

$$x \approx f(\mathbf{w}')$$

where for each i, $w_i' = x$ or w_i.

Theorem 5. *Let Σ be a idempotent set of equations and $\mathcal{V}$ a variety. Then*

(1) *If $\mathcal{V}$ realizes Σ and some iterated order derivative of Σ is inconsistent then $\mathcal{V}$ is congruence n-permutable for some n.*
(2) *If $\mathcal{V}$ is congruence n-permutable for some n then $\mathcal{V}$ realizes some Σ whose k^{th} iterated order derivative is inconsistent for some k.*

Proof. First we note that (1) holds for $\mathcal{V}$ if and only if it holds for $\mathcal{V}_\Sigma$, the variety presented by Σ, by a standard argument. Hence we may assume $\mathcal{V}$ is idempotent. To see (1) assume $\mathcal{V}$ realizes Σ and is not congruence n-permutable for any n. By Theorem 3 there is an $\mathbf{A} \in \mathcal{V}$ having a bounded compatible order with least element 0 and greatest element 1.

Suppose Σ implies

$$x \approx f(\mathbf{u}, y, \mathbf{v}) \tag{+}$$

Where $\mathbf{u}$ and $\mathbf{v}$ are vectors of not necessarily distinct variables. For each variable z_i occurring in $\mathbf{u}$ or $\mathbf{v}$ except x and y we substitute an element $c_i \in A$. For x we substitute an element $a \in A$. Let $\mathbf{u}(b)$ be $\mathbf{u}$ with the above substitution and substituting b for y. $\mathbf{v}(b)$ is defined similarly. By (+)

$$\begin{aligned} a &= f(\mathbf{u}(0), 0, \mathbf{v}(0)) \\ &\leq f(\mathbf{u}(b), a, \mathbf{v}(b)) \\ &\leq f(\mathbf{u}(1), 1, \mathbf{v}(1)) = a \end{aligned}$$

showing $\mathbf{A}$ satisfies $x \approx f(\mathbf{u}, x, \mathbf{v})$. Repeated applications of this argument show that $\mathbf{A}$ is a model of Σ^+. Hence Σ^+ is consistent and, by Theorem 3,

does not imply n-permutability for any n. Repeating this argument we see that every order derivative of Σ is consistent.

For (2) suppose that $\mathcal{V}$ is congruence n-permutable. Then $\mathcal{V}$ realizes the Hagemann-Mitschke terms of Theorem 2(2). An easy inductive arguments shows that the k^{th} order derivative of Σ implies that $x \approx p_k(x, x, y)$. Thus the n^{th} order derivative implies $x \approx p_n(x, x, y) \approx y$. □

Example 6. Recall that an algebra is *congruence regular* if whenever two congruences have a common block, they are equal. A variety is congruence regular if all of its members are. This property can be characterized by a Maltsev condition [1, 5, 16]: a variety $\mathcal{V}$ is congruence regular if and only if, for some n, it realizes Σ, where Σ is:

$$\begin{aligned} g_i(x, x, z) &\approx z \qquad 1 \leq i \leq n \\ x &\approx f_1(x, y, z, z, g_1(x, y, z)) \\ f_1(x, y, z, g_1(x, y, z), z) &\approx f_2(x, y, z, z, g_2(x, y, z)) \\ f_2(x, y, z, g_2(x, y, z), z) &\approx f_3(x, y, z, z, g_3(x, y, z)) \\ &\vdots \\ f_n(x, y, z, g_n(x, y, z), z) &\approx y \end{aligned}$$

Clearly Σ^+ has the equation $g_i(z, x, z) \approx z$. Using this and substituting $z \mapsto x$ we see

$$f_i(x, y, x, x, g_i(x, y, x)) \approx f_i(x, y, x, g_i(x, y, x), x)$$

From this we see $\Sigma^+ \models x \approx y$. Thus Σ^+ is inconsistent and so congruence regular varieties are k-permutable, for some k.

Of course Σ^+ inconsistent implies Σ' is. Thus congruence regular varieties are also congruence modular. Both of these results are unpublished results of J. Hagemann.

Since the first derivative of Σ being inconsistent has special meaning (congruence modularity), one wonders if having the first order derivative, Σ^+, inconsistent implies some well known property. A first guess would be congruence permutability. But if Σ is the Hagemann-Mitschke equations for 3-permutability, it is easy to see that Σ^+ is inconsistent. So a second guess is Σ^+ inconsistent implies 3-permutability. However in [15], E. T. Schmidt gave an example of a regular variety that was not permutable. For any given n, this example can be modified to give an example of an $(n+1)$-permutable, but not n-permutable congruence regular variety. *Thus Σ^+ inconsistent does not imply any fixed level of permutability even though it does imply n-permutability for some n.* The situation could be different when Σ is linear.

For an example showing that the converse of Theorem 5(1) is not true we can take Σ to be the equations defining the variety of idempotent quasigroups. The operations symbols are $\cdot$, $/$, and $\backslash$. Besides the idempotent laws, Σ has

the equations

$$x \cdot (x \setminus y) \approx y \qquad (x/y) \cdot y \approx x$$
$$x \setminus (x \cdot y) \approx y \qquad (x \cdot y)/y \approx x$$

This variety is nontrivial: for $a \neq 0$ or 1 in a field, let $x \cdot y = ax + (1-a)y$ and $x/y = y \setminus x = a^{-1}x + (1-a^{-1})y$. It is also congruence permutable. For example

$$p(x,y,z) = (x/(y \setminus y)) \cdot (y \setminus z) \approx (x/y) \cdot (y \setminus z)$$

is a Maltsev term; see [4]. However, since the operation symbols are all binary it is easy to see that $\Sigma^+ = \Sigma$.

On the other hand, as in [3], when Σ is linear we do have a converse:

Theorem 7. *The following are equivalent for a set Σ of linear idempotent equations.*

(1) *Some iterated order derivative is inconsistent.*
(2) *Any variety that realizes Σ is congruence n-permutable for some n.*
(3) *The variety $\mathcal{V}_\Sigma$ axiomatized by Σ is congruence n-permutable for some n.*

Proof. (1) implies (2) follows from the last theorem and (2) implies (3) is clear. To see (3) implies (1) suppose (1) fails. So assume every iterated order derivative is consistent. Let Ω be the union of all the order derivatives. Then $\Omega^+ = \Omega$.

Let $\mathbf{V}$ be the algebra on $\{0,1\}$ such that for each operation symbol f occurring in Ω we have $f^{\mathbf{V}}(v_1, \dots, v_n) = 1$ if and only if

$$\Omega \models f(x_{v_1}, \dots, x_{v_n}) \approx x_1. \tag{1}$$

Using a theory developed by David Kelly [12], Kearnes, Kiss and Szendrei show that $\mathbf{V}$ is a model of Ω; see [3]. Using $\Omega^+ = \Omega$, it is easy to see that the operations of $\mathbf{V}$ preserve the order on $\mathbf{V}$. Thus by Theorem 3(2) $\mathcal{V}_\Omega$ is not congruence n-permutable for any n. Since $\mathcal{V}_\Omega \subseteq \mathcal{V}_\Sigma$ it is also not congruence n-permutable for any n. □

The following theorem was proved in [8] for locally finite varieties.

Theorem 8. *For a variety $\mathcal{V}$ the following are equivalent.*

(1) *$\mathcal{V}$ is congruence n-permutable for some n.*
(2) *There is a linear idempotent set of equations Σ such that $\mathcal{V}$ realizes Σ but the variety of distributive lattices $\mathcal{D}$ does not.*

Proof. The Hagemann-Mitschke terms witness that (1) implies (2).

For the other direction suppose $\mathcal{V}$ is not n-permutable for any n and that $\mathcal{V}$ realizes a linear idempotent set of equations Σ. By Theorem 7 every iterated order derivative of Σ is consistent. As in the proof of that theorem let Ω be the union of all order derivatives of Σ and let $\mathbf{V}$ be the algebra on $\{0,1\}$ given in that proof that models Ω. As before all of the operations are order preserving. Thus for the operation symbol f occurring in Ω, the operation

$f^{\mathbf{V}}$ preserves order. Every nonconstant, order-preserving function on the two element lattice is a term function, so there is a lattice term that is equal to $f^{\mathbf{V}}$. Thus the variety $\mathcal{D}$ of distributive lattices realizes Ω and hence Σ. □

A straightforward modification of the proof of Corollary 5.3 in [3] shows that the truth of the conditions of Theorem 7 is decidable for Σ a set of linear idempotent equation. Hence we get the following corollary.

Corollary 9. *The following problem is decidable: for a finite set Σ of idempotent linear equations determine if the realization of Σ in a variety implies congruence n-permutability for some n.*

3. Semidistributivity

A variety $\mathcal{V}$ is *congruence join semidistributive* if all of the congruence lattices of all of its members are join semidistributive; that is, satisfy

$$x \vee y = x \vee z \implies x \vee y = x \vee (z \wedge z) \qquad (\mathrm{SD}_\vee)$$

We shall make use of a Maltsev condition for congruence join semidistributivity due to the author, which is a slight variant of the usual one given in [8] and [11]. (In the Hobby-McKenzie, Kearnes-Kiss version, (1) and (2) hold when i is even; (3) when i is odd.)

Theorem 10. *A variety $\mathcal{V}$ is congruence join semidistributive if and only if there is a positive integer k and ternary terms $d_0, \dots, d_k$ such that $\mathcal{V}$ satisfies $d_0(x,y,z) \approx x$, $d_k(x,y,z) \approx z$, and*

(1) $d_i(x,y,y) \approx d_{i+1}(x,y,y)$ *if* $i \equiv 0$ *or* $1 \mod 3$*;*
(2) $d_i(x,y,x) \approx d_{i+1}(x,y,x)$ *if* $i \equiv 0$ *or* $2 \mod 3$*;*
(3) $d_i(x,x,y) \approx d_{i+1}(x,x,y)$ *if* $i \equiv 1$ *or* $2 \mod 3$*;*

Define the *weak derivative* of Σ, denoted Σ^*, to be the augmentation of Σ by equations expressing f is independent of its i^{th} place if Σ implies

$$f(x, \dots, x, y, x, \dots, x) \approx x, \qquad (*)$$

with y in the i^{th} place. This concept is both interesting and disappointing for the same reason: an analog of Theorem 4.2 of [3] and Theorem 5 of this paper hold but the analog of Theorem 5.2 of [3] and Theorem 7 do not. Despite this we will show that there is a recursive procedure to decide if a finite, idempotent, linear set of equations imply congruence semidistributivity (and congruence meet semidistributivity).

Lemma 11. *Let Σ be an idempotent set of equations. Then the following are equivalent.*

(1) *If a variety $\mathcal{V}$ realizes Σ, then $\mathcal{V}$ is congruence meet semidistributive.*
(2) *$\mathcal{V}_\Sigma$ is congruence meet semidistributive.*
(3) *Σ is not realized in any nontrivial variety of modules.*

Proof. This is just part of Theorem 8.1 of [11] from the point of view of Σ: (1) $\Leftrightarrow$ (2) by a standard argument; Theorem 8.1 (10) $\Rightarrow$ (1) gives (3) $\Rightarrow$ (2); (1) $\Rightarrow$ (2) is clear since no nontrivial variety of modules is congruence meet semidistributive. $\square$

We also need the following very important theorem from [11].

Theorem 12 (Kearnes-Kiss)**.** *A variety is congruence join semidistributive if and only if it is both congruence meet semidistributive and satisfies a nontrivial congruence identity.*

Theorem 13. *Let Σ be an idempotent set of equations. Then*

(1) *If $\mathcal{V}$ realizes Σ and some iterated weak derivative of Σ is inconsistent then $\mathcal{V}$ is congruence semidistributive.*
(2) *If $\mathcal{V}$ is congruence semidistributive then $\mathcal{V}$ realizes some Σ whose k^{th} iterated weak derivative is inconsistent for some k.*

Proof. To see (1) assume $\mathcal{V}$ is not congruence semidistributive but realizes a set of equations Σ whose k^{th} iterated weak derivative is inconsistent. Since $\Sigma^* \subseteq \Sigma'$, if all derivatives of Σ are consistent then so are all weak derivatives. So we can assume some derivative is inconsistent and thus $\mathcal{V}$ satisfies a nontrivial congruence identity. We are assuming $\mathcal{V}$ is not congruence semidistributive so, by Theorem 12, $\mathcal{V}$ is not congruence meet semidistributive. By Lemma 11, Σ must be realized in some nontrivial variety of modules $\mathcal{M}$. But if f is a module term and $(*)$ holds it is easy to see that f is independent of its i^{th} place. Thus $\mathcal{M}$ also satisfies Σ^* and all of iterated weak derivatives. In particular, all iterated weak derivatives are consistent.

For (2) suppose $\mathcal{V}$ is congruence semidistributive and let $d_i(x, y, z)$ be the terms of Theorem 10. Assume by induction on i that some iterated weak derivative of Σ implies $x \approx d_i(x, y, z)$. If (1) and (2) of Theorem 10 hold then the next weak derivative implies that $d_{i+1}(x, y, z)$ is independent of its second and third variable and so $d_{i+1}(x, y, z) \approx d_{i+1}(x, x, x) \approx x$. If, say, (1) and (3) hold, then the next weak derivative implies that $d_{i+1}(x, y, z)$ is independent of its third variable and this together with the third equation implies the second equation. (So two weak derivatives were needed to go from i to $i + 1$ in this case.) So some iterate of the weak derivative implies $x \approx d_k(x, y, z) \approx z$. $\square$

As mentioned above, the analogs of Theorem 5.2 of [3] and Theorem 7 do not hold. Here's an example showing that it may not be easy to get something that works: consider Σ to be the equations

$$\begin{aligned} f(x,x,x,y) &\approx f(x,x,y,x) \approx f(x,y,x,x) \approx f(y,x,x,x) \\ g(x,x,y) &\approx g(x,y,x) \approx g(y,x,x) \\ f(x,x,x,x) &\approx g(x,x,x) \approx x \\ f(x,x,x,y) &\approx g(x,x,y) \end{aligned} \tag{2}$$

(f and g are weak near unanimity terms.) These equations cannot be realized in a nontrivial variety of modules (as we shall see below) and so they imply congruence meet semidistributivity. (We could add a Maltsev term if we wanted a set of equations that imply semidistributivity.) But without the last equation, they do not. This seems to indicate that a derivative condition for congruence semidistributivity could not just look at the function symbols individually.

On the other hand we will show that there is a simple recursive procedure to decide if (the realization of) Σ implies congruence semidistributivity (or meet semidistributive) when Σ is linear (and idempotent). By Theorem 12 Σ will imply congruence semidistributivity if and only if it implies both congruence meet semidistributivity and a nontrivial congruence identity. By the results of [3] we can effectively decide if Σ implies a nontrivial congruence identity. So we need an effective procedure to decide if Σ implies meet semidistributivity; that is, if there is no ring $\mathbf{R}$ such that Σ can be realized in the variety of $\mathbf{R}$-modules. The simple form of module terms allows us to translate this problem into existential ring equations. This is best illustrated with some examples. Taking one of the equations from (2), we let

$$\Sigma = \{g(x,x,x) \approx x, g(x,x,y) \approx g(x,y,x) \approx g(y,x,x)\}$$

An $\mathbf{R}$-module term for g has the form $g(x,y,z) = r_1x + r_2y + r_3z$. The first equation implies $r_1 + r_2 + r_3 = 1$ and the others imply $r_1 = r_2 = r_3$. So Σ is realized by $\mathbf{R}$-modules if and only if 3 is invertible in $\mathbf{R}$.

For f from (2), its equations are realized by $\mathbf{R}$-modules if and only if 4 is invertible in $\mathbf{R}$. If the last equation of (2) is also realized, then $1/3 = 1/4$, which implies $0 = 1$. So the equations of (2) cannot be satisfied in any nontrivial variety of $\mathbf{R}$-modules and hence imply congruence meet semidistributivity.[1]

When Σ is linear (as in the above example) the existential ring equations do not involve any products of ring variables. In this case techniques from classical algebra can be applied to effectively determine if Σ can be realized by some nontrivial variety of $\mathbf{R}$-modules. In the linear case, each equation is the sum of integer multiples of the ring variables equal to an integer. This can be put in matrix form:

$$AX = B$$

where A is an $m \times n$ matrix over $\mathbb{Z}$, B is a column vector over $\mathbb{Z}$, and X is a column vector of ring variables. Let D be the Smith Normal Form of A. So D is diagonal and $d_{i,i} \mid d_{i+1,i+1}$, $d_{i,i} > 0$ for $i = 1, \ldots, r$ and $d_{i,i} = 0$ for $i > r$. The $d_{i,i}$ are the invariant factors. Also there are matrices $P \in \mathrm{GL}(m, \mathbb{Z})$ and $Q \in \mathrm{GL}(n, \mathbb{Z})$ with

$$D = PAQ.$$

[1] Matthew Valeriote and several coauthors have shown the converse is true for finitely generated varieties: *a finitely generated variety is congruence meet semidistributive if and only if it realizes* (2).

See [10]. Let $C = PB$ and $Y = Q^{-1}X$. Then, since $Q^{-1}X$ has integer entries, $AX = B$ can be solved in $\mathbf{R}$ if and only if $DY = C$ can.

If $c_j = 0$ for $j > r$ then $DY = C$ can be solved over $\mathbb{Q}$. If $c_j \neq 0$ for some $j > r$ then any ring satisfying $DY = C$ must have characteristic dividing c_j. So one can now test if $DY = C$ has a solution in $\mathbb{Z}/p\mathbb{Z}$ for each prime dividing c_j.

This proves the following theorem:

Theorem 14. *Given a finite set of linear equations Σ one can recursively decide if there is a nontrivial ring $\mathbf{R}$ such that the variety of $\mathbf{R}$-modules realizes Σ.*

In [9], Hutchinson and Czedli give a a more thorough analysis. In particular they characterize for exactly which rings $\mathbf{R}$, the $\mathbf{R}$-modules satisfy Σ.

The next corollary summarizes properties P such that it is known to be decidable, given a finite set Σ of linear idempotent equations, if every variety that realizes Σ satisfies P. The first two are from [3]. The proof is a straightforward modification of Corollary 5.3 in [3].

Corollary 15. *Each of the following problems is decidable: for a finite set Σ of idempotent, linear equations, determine for a variety if*

(1) *the realization of Σ implies congruence modularity.*
(2) *the realization of Σ implies a nontrivial congruence identity.*
(3) *the realization of Σ implies congruence n-permutability, for some n.*
(4) *the realization of Σ implies congruence meet semidistributivity.*
(5) *the realization of Σ implies congruence semidistributivity.*
(6) *the realization of Σ implies congruence distributivity.*

We close with an example illustrating some of these concepts. Let Σ_1 be

$$t(x,x,x,x,y) \approx t(x,x,x,y,x) \approx t(x,x,y,x,x) \approx x$$
$$t(x,x,y,y,y) \approx t(x,y,y,y,y) \approx t(y,x,y,y,y)$$

and let Σ_2 be

$$s(x,x,x,x,y) \approx s(x,x,x,y,x) \approx x$$
$$s(x,x,x,y,y) \approx s(x,x,y,y,y) \approx s(x,y,x,y,y) \approx s(y,x,x,y,y)$$

These are part of a system of sets of equations that all imply $\mathrm{SD}_\vee$. They come from the paper by Matthew Valeriote and others mentioned in the footnote above. Both s and t imply a nontrivial congruence identity. This can be proved by showing the iterated derivatives are inconsistent or just noting both are Hobby-McKenzie terms. Neither can be realized in a nontrivial module. Hence they imply congruence semidistributivity. Do they imply CD?

Σ_1' is inconsistent so by Theorem 3.2 Σ_1 implies modularity and hence distributivity: the top equations imply Σ_1' gives that t is independent of its last 3 variables. So

$$x \approx t(x,x,*,*,*) \approx t(x,y,*,*,*) \approx t(y,x,*,*,*)$$

Reversing x and y gives $y \approx t(x, y, *, *, *) \approx t(y, x, *, *, *)$, so $x \approx y$.

On the other hand Σ_2 does not imply distributivity. Let $\mathbf{V}$ be the two-element algebra defined by (1) in the proof of Theorem 7 with $\Omega = \Sigma_2$ and let $\mathbf{V}'$ be the algebra defined with $\Omega = \Sigma_2'$. Both of these satisfy Σ_2 but $\mathbf{Con}(\mathbf{V} \times \mathbf{V}')$ is $\mathbf{N}_5$.

References

[1] B. Csákány, *Characterizations of regular varieties*, Acta Sci. Math. (Szeged) **31** (1970), 187–189.

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

[3] Topaz Dent, Keith Kearnes, and Ágnes Szendrei, *An easy test for congruence modularity*, Algebra Universalis **67** (2012), 375–392.

[4] Ralph Freese and Ralph McKenzie, *Commutator theory for congruence modular varieties*, London Mathematical Society Lecture Note Series, vol. 125, Cambridge University Press, Cambridge, 1987, Online version available at: `http://www.math.hawaii.edu/~ralph/papers.html`.

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

[6] H. P. Gumm, *Congruence modularity is permutability composed with distributiveity*, Arhc. Math. (Basel) **36** (1981), 569–576.

[7] J. Hagemann and A. Mitschke, *On n-permutable congruences*, Algebra Universalis **3** (1973), 8–12.

[8] D. Hobby and R. McKenzie, *The structure of finite algebras (tame congruence theory)*, Contemporary Mathematics, American Mathematical Society, Providence, RI, 1988.

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

[10] Nathan Jacobson, *Basic algebra. I*, second ed., W. H. Freeman and Company, New York, 1985.

[11] Keith A. Kearnes and Emil W. Kiss, *The shape of congruence lattices*.

[12] D. Kelly, *Basic equations: word problems and Mal'cev conditions*, Abstract 701-08-4, Notices Amer. Math. Soc. **20** (1973), A–54.

[13] G. McNulty, *Undecidable properties of finite sets of equations*, J. Symbolic Logic **41** (1976), 589–604.

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

[15] E. T. Schmidt, *Über reguläre Mannigfaltigkeiten*, Acta Sci. Math. (Szeged) **31** (1970), 197–201.

[16] R. Wille, *Kongruenzklassengeometrien*, Springer-Verlag, New York, 1970, Lecture Notes in Mathematics, vol. **113**.

Ralph Freese

Department of Mathematics, University of Hawaii, Honolulu 96822, USA
e-mail: `ralph@math.hawaii.edu`
URL: `http://math.hawaii.edu/~ralph/`