AN EASY TEST FOR CONGRUENCE MODULARITY

TOPAZ DENT, KEITH A. KEARNES, AND ÁGNES SZENDREI

Abstract. We describe an easy way to determine whether the realization of a set of idempotent identities guarantees congruence modularity or the satisfaction of a nontrivial congruence identity. Our results yield slight strengthenings of Day's Theorem and Gumm's Theorem, which each characterize congruence modularity.

1. Introduction

Given a set Σ of identities, how does one determine whether the variety axiomatized by Σ is congruence modular? One natural approach is to look for Day terms (see [3] or Theorem 3.1 below). In this paper we will exhibit an easier method, which works when Σ is a set of *idempotent* identities. By this, we mean that for every function symbol F appearing in Σ, it is the case that $\Sigma \models F(x, \ldots, x) \approx x$.

For a set Σ of idempotent identities we shall define the notion of a *derivative*, Σ', which is a superset of idempotent identities in the same language. One of our main theorems is that Σ axiomatizes a congruence modular variety if and only if the derivative of Σ is inconsistent. Our other main theorem is that Σ axiomatizes a variety that satisfies some nontrivial congruence identity if and only if its n-th derivative is inconsistent for some n. (In fact, we prove our results not only for the variety $\mathcal{V}$ axiomatized by Σ, but also any variety that "interprets $\mathcal{V}$".)

2. Definitions

Let Σ be a set of identities. Σ is *inconsistent* if $\Sigma \models x \approx y$, otherwise Σ is *consistent*. Σ is *idempotent* if for every function symbol F appearing in Σ it is the case that $\Sigma \models F(x, x, \ldots, x) \approx x$. F is *weakly independent of its first variable* if $\Sigma \models F(y, \mathbf{w}) \approx x$ for variables $x \neq y$ and some sequence of not necessarily distinct variables $\mathbf{w}$. F is *independent of its first variable* if $\Sigma \models F(x, \mathbf{z}) \approx F(y, \mathbf{z})$, where x, y, and all variables in the sequence $\mathbf{z}$ are distinct. Define independence and weak independence of each of the other variables in the same way. (If Σ is idempotent and F is independent of its first variable, then F is weakly independent of its first variable. This is because the assumptions that Σ is idempotent and some F is independent of its first variable yield $\Sigma \models F(y, x, x, \ldots, x) \approx F(x, x, x, \ldots, x) \approx x$, which suffices

This material is based upon work supported by the Hungarian National Foundation for Scientific Research (OTKA) grant no. K77409.

to show that F is weakly independent of its first variable.) The concepts of weak independence and ordinary independence are defined relative to Σ, so when it is not obvious we will specify explicitly which set Σ is involved.

Σ is *realized* by an algebra $\mathbf{A}$ (or variety $\mathcal{V}$) if it is possible to interpret each function symbol appearing in Σ as a term of $\mathbf{A}$ (respectively $\mathcal{V}$) such that all identities in Σ are satisfied by $\mathbf{A}$ (respectively $\mathcal{V}$).

Let Σ be a set of idempotent identities, and let $\mathcal{P}$ be the set of pairs (F, i) where F is a function symbol appearing in Σ that is weakly independent of its i-th variable. The *derivative* Σ' of Σ is the set of identities obtained by adding to Σ all identities asserting that F is independent of its i-th variable for all pairs $(F, i) \in \mathcal{P}$. (I.e., Σ' strengthens each instance of weak independence to an instance of independence.) The n-th derivative of Σ is denoted $\Sigma^{(n)}$.

For example, if Σ is the set consisting of the two identities (i) $F(y, y, x) \approx x$ and (ii) $F(x, y, y) \approx x$, then from (i) we derive that F is weakly independent of its first and second variable, while from (ii) we derive that F is weakly independent of its second and third variable. Hence Σ' will contain identities (iii) $F(x, z_2, z_3) \approx F(y, z_2, z_3)$, (iv) $F(z_1, x, z_3) \approx F(z_1, y, z_3)$ and (v) $F(z_1, z_2, x) \approx F(z_1, z_2, y)$, which assert that F is independent of all of its variables. In this example, Σ' is inconsistent, since $\Sigma' \models x \approx F(x, y, y) \approx F(y, y, y) \approx y$, where the first instance of $\approx$ is from Σ, the second follows from (iii) by variable replacement, and the third follows from (i) by variable replacement.

3. Testing for congruence modularity

In the introduction we raised the question of how to determine whether the variety axiomatized by a set of identities Σ is congruence modular. Rather than consider the variety axiomatized by Σ we shall consider varieties that realize Σ, since this is more general. (The variety axiomatized by Σ also realizes Σ, since we may interpret each function symbol appearing in Σ as itself.) This generalization is important, because it offsets our requirement that Σ be idempotent. Namely, if we state our results for varieties *axiomatized* by idempotent Σ, then we only characterize congruence modularity for idempotent varieties; but if we state our results for varieties that *realize* idempotent Σ, then we characterize all congruence modular varieties.

We start with Alan Day's characterization of congruence modularity.

Theorem 3.1. [3] *The following are equivalent for a variety $\mathcal{V}$.*

(1) *$\mathcal{V}$ is congruence modular.*
(2) *There exist 4-variable terms $m_0, \ldots, m_n$ such that the following identities hold in $\mathcal{V}$:*
   (a) *$m_0(x, u, v, y) \approx x$ and $m_n(x, u, v, y) \approx y$,*
   (b) *$m_i(x, y, y, x) \approx x$,*
   (c) *$m_i(x, u, u, y) \approx m_{i+1}(x, u, u, y)$ for i odd, and*

(d) $m_i(x, x, y, y) \approx m_{i+1}(x, x, y, y)$ *for i even.*

From this we derive our first main result.

Theorem 3.2. *$\mathcal{V}$ is congruence modular if and only if $\mathcal{V}$ realizes some set Σ of idempotent identities whose derivative is inconsistent.*

Proof. [$\Rightarrow$] Assume that $\mathcal{V}$ is congruence modular, and that Σ is the set of identities guaranteed by Theorem 3.1. The identities in part (2)(b) suffice to guarantee that this is a set of idempotent identities. Moreover, the identities of type (2)(b) suffice to guarantee that Σ' will contain identities expressing that each $m_i(x, u, v, y)$ is independent of its middle two variables. In light of this, the identities of type (2)(c) and (2)(d) together assert that $\Sigma' \models m_i(x, *, *, y) \approx m_{i+1}(x, *, *, y)$ for all i, where the asterisks indicate that the identity holds for any middle values. This and (2)(a) yield

$$\Sigma' \models x \approx m_0(x, *, *, y) \approx m_1(x, *, *, y) \approx \cdots \approx m_n(x, *, *, y) \approx y,$$

so Σ' is inconsistent.

[$\Leftarrow$] Conversely, assume that there is a variety $\mathcal{V}$ realizing Σ that is not congruence modular. We need to prove that Σ' is consistent. Without loss of generality we may assume that $\mathcal{V}$ is the variety axiomatized by Σ. For, if $\mathcal{V}$ contains an algebra $\mathbf{A}$ whose congruence lattice is nonmodular, then the reduct of $\mathbf{A}$ to the symbols in Σ is an algebra in the variety axiomatized by Σ whose congruence lattice is nonmodular.

Now we follow Day's proof of Theorem 3.1, and show how to extract a nontrivial model of Σ' from a failure of congruence modularity. Let $\mathbf{F} = \mathbf{F}_{\mathcal{V}}(a, b, c, d)$ be a 4-generated $\mathcal{V}$-free algebra. Define congruences

$$\alpha = \theta((a, b), (c, d)),\ \beta = \theta((a, d), (b, c)), \text{ and } \gamma = \theta(b, c).$$

Day's theorem proves that $\mathcal{V}$ is congruence modular if and only if

$$\beta = (\alpha \wedge \beta) \vee \gamma. \tag{3.1}$$

Since $\mathcal{V}$ is idempotent, we can simplify the situation. Let $\mathbf{T} = \mathbf{F}_{\mathcal{V}}(r, s)$ be a 2-generated $\mathcal{V}$-free algebra. The congruences α and β are the kernels of the homomorphisms $A, B \colon \mathbf{F} \to \mathbf{T}$ defined by $A\colon a, b \mapsto r; c, d \mapsto s$ and $B\colon a, d \mapsto r; b, c \mapsto s$. Hence $\alpha \wedge \beta$ is the kernel of the homomorphism

$$A \times B \colon \mathbf{F} \to \mathbf{T}^2 \colon a \mapsto (r, r);\ b \mapsto (r, s);\ c \mapsto (s, s);\ d \mapsto (s, r).$$

$A \times B$ is surjective, since if $p = p(r, s)$ and $q = q(r, s) \in T$ are arbitrarily chosen, then $m = p(q(a, b), q(d, c)) \in F$ is an element such that $(A \times B)(m) = (p, q)$. The kernel of $A \times B$ is $\alpha \wedge \beta$, so

$$\mathbf{F}/(\alpha \wedge \beta) \cong \mathbf{T}^2. \tag{3.2}$$

Since both sides of (3.1) contain $\alpha \wedge \beta$, we can express Day's conclusion in terms of the algebra $\mathbf{T}^2$. If η_1 and η_2 are the coordinate projection kernels of $\mathbf{T}^2$, then η_1

corresponds to $\alpha/(\alpha \wedge \beta)$ and η_2 corresponds to $\beta/(\alpha \wedge \beta)$ under the isomorphism (3.2), and $\delta = \theta((r,s),(s,s))$ corresponds to $\gamma/(\alpha \wedge \beta)$. Day's conclusion is that $\mathcal{V}$ is congruence modular if and only if $\eta_2 = \delta$. Since we are assuming that $\mathcal{V}$ is not congruence modular, and since η_2 contains δ by definition, it follows that $((r,r),(s,r)) \in \eta_2 \setminus \delta$.

Since $\mathcal{V}$ is idempotent, each congruence class is a subuniverse of $\mathbf{T}^2$. Let $\mathbf{G} \leq \mathbf{T}^2$ be the subalgebra whose universe is the η_2-class of (r,r). We argue that the nontrivial algebra $\overline{\mathbf{G}} = \mathbf{G}/\delta|_G$ is a model of Σ'.

Let F be an n-place function symbol appearing in Σ and suppose that

$$\Sigma \models F(y, \mathbf{w}) \approx x \tag{3.3}$$

where $x \neq y$ and $\mathbf{w}$ is a sequence of not necessarily distinct variables. Let $U \subseteq \{1, \dots, n\}$ be the set of places of F where x occurs in this identity.

Claim 3.3. *Choose any $(g_1, r), \dots, (g_n, r) \in G$. Define*

$$r_i = \begin{cases} r & \text{if } i \in U; \\ s & \text{else.} \end{cases}$$

Then

$$F^{\mathbf{T}^2}((g_1, r), \dots, (g_n, r)) = F^{\mathbf{T}^2}((g_1, r_1), \dots, (g_n, r_n)). \tag{3.4}$$

That both sides of (3.4) are equal in the first coordinate is trivial. In the second coordinate we must establish that the value on the left-hand side, which is $F^{\mathbf{T}}(r, \dots, r) = r$, is the same as the value $F^{\mathbf{T}}(r_1, \dots, r_n)$ on the right-hand side, which is obtained by evaluating $F^{\mathbf{T}}$ on an $\{r, s\}$-tuple with r's substituted in position i for each $i \in U$ and s's substituted in all other positions. This follows from (3.3).

Claim 3.4. *For any $w \in T$, $((w, s), (s, s)) \in \delta$.*

If $w(x, y)$ is a binary term such that $w = w(r, s)$, then

$$(w, s) = (w(r, s), w(s, s)) = w((r, s), (s, s)) \equiv_\delta w((s, s), (s, s)) = (s, s).$$

Now we prove that F is independent of its first variable modulo δ on $\mathbf{G}$. Choose $(g_1, r), \dots, (g_n, r), (h, r) \in G$ arbitrarily. By Claim 3.3,

$$F^{\mathbf{T}^2}((g_1, r), (g_2, r), \dots, (g_n, r)) = F^{\mathbf{T}^2}((g_1, r_1), (g_2, r_2), \dots, (g_n, r_n)),$$

and similarly

$$F^{\mathbf{T}^2}((h, r), (g_2, r), \dots, (g_n, r)) = F^{\mathbf{T}^2}((h, r_1), (g_2, r_2), \dots, (g_n, r_n)).$$

Now $r_1 = s$, since $1 \notin U$ according to (3.3), so by Claim 3.4 we have $(g_1, s) \equiv_\delta (h, s)$. Therefore

$$\begin{aligned} F^{\mathbf{T}^2}((g_1,r),(g_2,r),\dots,(g_n,r)) &= F^{\mathbf{T}^2}((g_1,s),(g_2,r_2),\dots,(g_n,r_n)) \\ &\equiv_\delta F^{\mathbf{T}^2}((h,s),(g_2,r_2),\dots,(g_n,r_2)) \\ &= F^{\mathbf{T}^2}((h,r),(g_2,r),\dots,(g_n,r)). \end{aligned}$$

This proves that F is independent of its first variable modulo δ on G, so

$$\mathbf{G}/\delta|_{\mathbf{G}} \models F(x,\mathbf{z}) \approx F(y,\mathbf{z})$$

where x, y, and all variables in the sequence $\mathbf{z}$ are distinct. □

Corollary 3.5. *Day's Theorem (Theorem 3.1) remains true if one weakens*

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

to either

(c)′ $m_i(x,x,x,y) \approx m_{i+1}(x,x,x,y)$ *for* i *odd, or*
(c)″ $m_i(x,y,y,y) \approx m_{i+1}(x,y,y,y)$ *for* i *odd.*

In particular, congruence modularity can be characterized by identities involving only the variables x *and* y*.*

Proof. We can obtain (c)′ and (c)″ from (c) by replacing the variable u by either x or y, so (c)′ and (c)″ are formally weaker than (c). If you take Σ to be the set of identities of Theorem 3.1 with (c) replaced by either (c)′ or (c)″, then Σ' is inconsistent by the same argument used in the proof of direction [⇒] of Theorem 3.2. Thus, the weakened identities still imply congruence modularity.

For the last statement of the corollary, we can delete the terms m_0 and m_n from the list of Day terms and just use x and y in their place. Then, with (c) replaced by either (c)′ or (c)″, the identities involve only x and y. □

We believe that the first published proof that congruence modularity can be characterized by 2-variable identities appears in [22] by J. B. Nation (see the corollary on page 85 of that paper). Nation's 2-variable identities use 5-variable terms.

Example 3.6. A lattice is *p-modular* if it satisfies the identity

(3.5) $$(x \vee (y \wedge z)) \wedge (z \vee (y \wedge x)) = (z \wedge (x \vee (y \wedge z))) \vee (x \wedge (z \vee (y \wedge x))).$$

This identity is satisfied by all modular lattices and some nonmodular lattices. (It is the conjugate identity for a 10-element splitting lattice.)

Eva Gedeonová characterized the satisfaction of (3.5) as a congruence identity with the following theorem.

Theorem 3.7. [7] *The following are equivalent for a variety* $\mathcal{V}$*.*

1. $\mathcal{V}$ *satisfies (3.5) as a congruence identity.*
2. *There exist 6-variable terms* $g_0, \dots, g_n$ *such that the following identities hold in* $\mathcal{V}$*:*

(a) $g_0(x,s,t,u,v,y) \approx x$ *and* $g_n(x,s,t,u,v,y) \approx y$,
(b) $g_i(x,x,y,y,x,x) \approx g_i(x,y,x,x,y,x) \approx x$ *for all* i,
(c) $g_i(x,s,x,y,s,y) \approx g_{i+1}(x,s,x,y,s,y)$ *for* i *odd, and*
(d) $g_i(x,x,s,s,y,y) \approx g_{i+1}(x,x,s,s,y,y)$ *for* i *even.*

Although the p-modular law is strictly weaker than the modular law as a lattice identity, Day was able to show in [4] that any variety realizing the set Σ of identities of Theorem 3.7 (2) is congruence modular. His argument involved nonobvious calculations with the congruences of the 4-generated free algebra in a variety realizing these identities.

We will derive Day's result from our Theorem 3.2. Gedeonová's identity (b) implies that Σ is idempotent, hence our theorem applies. Identity (b) also implies that each g_i is weakly independent of its middle four variables relative to Σ. Hence

$$\Sigma' \models x \overset{\text{(a)}}{\approx} g_0(x,*,*,*,*,y) \overset{\text{(d)}}{\approx} g_1(x,*,*,*,*,y) \overset{\text{(c)}}{\approx} \cdots \approx g_n(x,*,*,*,*,y) \overset{\text{(a)}}{\approx} y.$$

Σ' is inconsistent, so any congruence p-modular variety is congruence modular.

Example 3.8. The paper [2] introduces the concept of a "cube term", which is a common generalization of a Maltsev term and a near unanimity term. A cube term is a term $F(x_1,\ldots,x_n)$, for some $n \geq 3$, satisfying an idempotent set of identities Σ which expresses exactly that F is weakly independent of each of its variables.

It is proved in [2] that a variety with a cube term (i.e., a variety realizing Σ) is congruence modular. The method of proof is to show first that a variety with a cube term has an "edge term", and then that a variety with an edge term has Day terms. The first step of the proof is long ($\approx$ 5 journal pages) and highly nontrivial. The second step is short and easy to verify, but it is easy to imagine that it required ingenuity to discover.

We can prove the combination of both steps with no ingenuity. Since Σ asserts that F is weakly independent of all variables, Σ' expresses that F is constant. At the same time, Σ' expresses that F is idempotent (since $\Sigma' \supseteq \Sigma$). Thus Σ' proves that $F(x,x,\ldots,x)$ interprets simultaneously as a constant function and as the identity function on any algebra realizing Σ. It follows that Σ' has no models of size greater than one. Hence Theorem 3.2 applies, showing that any variety realizing Σ is congruence modular.

Example 3.9. A variety is congruence n-permutable if, for any two congruences α and β on any algebra $\mathbf{A} \in \mathcal{V}$, it is the case that the $(n-1)$-fold relational product $\alpha \circ_{n-1} \beta$ equals $\beta \circ_{n-1} \alpha$. This property was characterized by J. Hagemann and A. Mitschke in the following way.

Theorem 3.10. [9] *The following are equivalent for a variety* $\mathcal{V}$*.*

(1) $\mathcal{V}$ *is congruence* n*-permutable.*

(2) *There exist* 3*-variable terms* $p_0, \ldots, p_n$ *such that the following identities hold in* $\mathcal{V}$*:*
   (a) $p_0(x, u, y) \approx x$ *and* $p_n(x, u, y) \approx y$*,*
   (b) $p_i(x, x, y) \approx p_{i+1}(x, y, y)$ *for all* i*.*

Bjarni Jónsson proved in [11] that any congruence 3-permutable variety is congruence modular. On the other hand, there exist congruence 4-permutable varieties that are not congruence modular. The first of these statements can be proved by a computation, but we derive it from Theorem 3.2.

A congruence 3-permutable variety realizes

$$\Sigma = \{x \approx p_1(x, y, y),\ p_1(x, x, y) \approx p_2(x, y, y),\ p_2(x, x, y) \approx y\}.$$

Σ' contains Σ along with (i) identities asserting that p_1 is independent of its second and third variables (from the first identity of Σ) and (ii) identities asserting that p_2 is independent of its first and second variables (from the third identity of Σ). Hence

$$\Sigma' \models x \stackrel{\Sigma}{\approx} p_1(x, y, y) \stackrel{\text{(i)}}{\approx} p_1(x, x, y) \stackrel{\Sigma}{\approx} p_2(x, y, y) \stackrel{\text{(ii)}}{\approx} p_2(x, x, y) \stackrel{\Sigma}{\approx} y,$$

showing that Σ' is inconsistent.

It can also be proved from Theorem 3.2 that congruence 4-permutability does *not* imply congruence modularity. For this one must show that if

$$\begin{aligned}\Sigma = \{x \approx p_1(x, y, y),\ & p_1(x, x, y) \approx p_2(x, y, y),\\ & p_2(x, x, y) \approx p_3(x, y, y),\ p_3(x, x, y) \approx y\},\end{aligned}$$

then Σ' is consistent. For this it is necessary that we identify *all* instances of weak independence in order to construct Σ', and then to show that $\Sigma' \not\models x \approx y$. Both of these can be accomplished in a mechanical way with the help of David Kelly's Completeness Theorem, described in [18, 15]. We do not include the details here.

Example 3.11. In [1], Wolfram Bentz investigated varieties $\mathcal{V}$ whose T_0 topological algebras are Hausdorff. It is conjectured that these varieties are exactly the congruence modular varieties that are congruence n-permutable for some n. (This conjecture, called "the congruence modularity conjecture", is still open.)

Let Σ_1 be the set consisting of the following identities involving the 3-variable terms q_1, q_2, p:

(1) $x \approx q_1(x, y, y)$,
(2) $q_1(x, x, y) \approx q_2(x, x, y)$,
(3) $q_2(x, y, x) \approx x$ and $q_2(x, y, y) \approx p(x, y, y)$,
(4) $p(x, x, y) \approx y$.

(These are the Gumm identities for congruence modularity, from [8], for $n = 2$ *minus* the Gumm identity $q_1(x, y, x) \approx x$.) Now let $\mathcal{P}_n$ be the set of identities listed in Theorem 3.10 (2). Bentz proved that any variety realizing $\Sigma_1 \cup \mathcal{P}_n$, for any given n, has the property that its T_0 topological algebras are Hausdorff. In light of the congruence modularity conjecture, this led him to raise the question of whether varieties realizing $\Sigma_1 \cup \mathcal{P}_n$ must be congruence modular.

The question raised by Bentz was answered in [17], where it was shown that any variety realizing Σ_1 must already be congruence modular. The proof was accomplished by defining

$$\begin{aligned}
m_0(x,u,v,y) &:= x,\\
m_1(x,u,v,y) &:= x,\\
m_2(x,u,v,y) &:= q_1(x, q_2(x,v,u), p(x,u,v)),\\
m_3(x,u,v,y) &:= q_2(x,u,y),\\
m_4(x,u,v,y) &:= q_2(x,v,y),\\
m_5(x,u,v,y) &:= p(u,v,y),\\
m_6(x,u,v,y) &:= y,
\end{aligned}$$

and showing that it is provable from Σ_1 that the Day identities of Theorem 3.1 hold for these new terms.

Here we give a different proof that any variety realizing Σ_1 is congruence modular, based on Theorem 3.2. Identities (1), (3) and (4) from the definition of Σ_1 suffice to prove that Σ_1 is idempotent, so the theorem applies. Identity (1) shows that q_1 is weakly independent of its last two variables relative to Σ_1; identity (3) shows that q_2 is weakly independent of its middle variable relative to Σ_1; identity (4) shows that p is weakly independent of its first two variables relative to Σ_1. Therefore, relative to Σ_1' we get that (5) $q_1(x,u,y) \approx q_1(x,x,x) \approx x$, (6) $p(x,u,y) \approx p(y,y,y) \approx y$, and (7) q_2 is independent of its middle variable. Hence

$$\Sigma_1' \models x \overset{(5)}{\approx} q_1(x,x,y) \overset{(2)}{\approx} q_2(x,x,y) \overset{(7)}{\approx} q_2(x,y,y) \overset{(3)}{\approx} p(x,y,y) \overset{(6)}{\approx} y,$$

showing that Σ_1' is inconsistent.

The argument from Example 3.11 actually establishes the following theorem, a slight strengthening of H. P. Gumm's Theorem from [8].

Theorem 3.12. *The following are equivalent for a variety $\mathcal{V}$.*

(1) *$\mathcal{V}$ is congruence modular.*
(2) *There exist 3-variable terms $q_0, \ldots, q_n, p$ such that the following identities hold in $\mathcal{V}$:*
   (a) $q_0(x,u,y) \approx x$,
   (b) $q_i(x,y,x) \approx x$ *for i in the interval* $[2,n]$,
   (c) $q_i(x,y,y) \approx q_{i+1}(x,y,y)$ *for i even,*
   (d) $q_i(x,x,y) \approx q_{i+1}(x,x,y)$ *for i odd,*
   (e) $q_n(x,y,y) \approx p(x,y,y)$, *and*
   (f) $p(x,x,y) \approx y$.

If Σ is the set of identities in Theorem 3.12, then these are exactly Gumm's identities from [8] *minus* the identity $\varepsilon : q_1(x, y, x) \approx x$. The theorem asserts that we can delete this single identity from Gumm's set and still have a set of identities forcing congruence modularity. The 'reason' for this is that the only role played by this identity ε in our method is to prove that q_1 is weakly independent of its middle variable relative to the Gumm identities $\Sigma \cup \{\varepsilon\}$. But this can be deduced another way, directly from Σ, using $\Sigma \models x \overset{\text{(a)}}{\approx} q_0(x, y, y) \overset{\text{(c)}}{\approx} q_1(x, y, y)$.

4. Testing for a nontrivial congruence identity

Our result about congruence modular varieties has an analogue for varieties that satisfy a nontrivial congruence identity. First we recall one Maltsev characterization for this class of varieties.

Theorem 4.1. [14] *The following are equivalent for a variety $\mathcal{V}$.*

1. *$\mathcal{V}$ satisfies a nontrivial congruence identity.*
2. *There exist 4-variable terms $M_0, \dots, M_n$ such that the following identities hold in $\mathcal{V}$:*
   - (a) *$M_0(x, u, v, y) \approx x$ and $M_n(x, u, v, y) \approx y$,*
   - (b) *$M_i(x, x, y, y) \approx M_{i+1}(x, x, y, y)$ and $M_i(x, y, x, y) \approx M_{i+1}(x, y, x, y)$ for i odd, and*
   - (c) *$M_i(x, y, y, y) \approx M_{i+1}(x, y, y, y)$ for i even.*

There are other Maltsev characterizations of the class of varieties satisfying nontrivial congruence identities given in Definition 2.17, Theorem 5.23 and Theorem 8.13 of [14], which could be used just as easily in this paper. We chose the one above, which is part of Theorem 5.28 of [14], since it is the characterization that most resembles the characterization of congruence modularity in Theorem 3.1.

Theorem 4.2. *$\mathcal{V}$ satisfies a nontrivial congruence identity if and only if $\mathcal{V}$ realizes some set Σ of idempotent identities whose n-th derivative is inconsistent for some n.*

Proof. [$\Rightarrow$] Assume that $\mathcal{V}$ satisfies a nontrivial congruence identity, and that Σ is the set of identities guaranteed by Theorem 4.1. The consequence of these identities that results from replacing all variables with x is

$$\Sigma \models x \approx M_0(x, x, x, x) \approx M_1(x, x, x, x) \approx \cdots \approx M_n(x, x, x, x),$$

showing that Σ is idempotent.

Claim 4.3. $\Sigma^{(i)} \models M_i(x, u, v, y) \approx x$ *for all i.*

The claim holds for $i = 0$ by identity (2)(a) of Theorem 4.1. Let's assume that the claim holds for some $k \geq 0$, and prove it for $k + 1$. If k is odd, then from (2)(b) of

Theorem 4.1 we derive

$$\begin{array}{ll}\Sigma^{(k)} \models & x \approx M_k(x,x,y,y) \approx M_{k+1}(x,x,y,y) \qquad \text{and} \\ \Sigma^{(k)} \models & x \approx M_k(x,y,x,y) \approx M_{k+1}(x,y,x,y),\end{array}$$

from which we conclude that $M_{k+1}(x,u,v,y)$ is weakly independent of its second, third and fourth variables relative to $\Sigma^{(k)}$. Hence

$$\Sigma^{(k+1)} \models M_{k+1}(x,u,v,y) \approx M_{k+1}(x,x,x,x) \approx x, \tag{4.1}$$

as claimed. If k is even, then from (c) we derive

$$\Sigma^{(k)} \models \quad x \approx M_k(x,y,y,y) \approx M_{k+1}(x,y,y,y),$$

from which we conclude that $M_{k+1}(x,u,v,y)$ is weakly independent of its second, third and fourth variables relative to $\Sigma^{(k)}$. Just as in (4.1), this finishes the claim in the case where k is even.

It follows from the claim and identity (2)(a) of Theorem 4.1 that $\Sigma^{(n)} \models x \approx M_n(x,u,v,y) \approx y$, so $\Sigma^{(n)}$ is inconsistent. This concludes the proof of [$\Rightarrow$].[1]

[$\Leftarrow$] We will argue that if Σ is idempotent and the realization of Σ by $\mathcal{V}$ does not force $\mathcal{V}$ to satisfy a nontrivial congruence identity, then the same properties are true for Σ'.

If Σ is idempotent, then so if Σ', since it extends Σ and it involves no new function symbols.

If the realization of Σ by $\mathcal{V}$ does not force a nontrivial congruence identity, then the variety $\mathcal{V}_\Sigma$ axiomatized by Σ does not satisfy a nontrivial congruence identity. The combination of Theorems 2.16 and 7.15 (1)$\Leftrightarrow$(2) of [14] implies that $\mathcal{V}_\Sigma$ has no "Hobby-McKenzie term". In this situation, the contrapositive of Lemma 2.5 of [13] proves that $\mathcal{V}_\Sigma$ has a subvariety term equivalent to the variety of sets or the variety of semilattices. In either case, this means that Σ can be realized by a 2-element meet semilattice, $\mathbf{S} = \langle\{0,1\};\wedge\rangle$. If F is weakly independent of its first variable relative to Σ, then $\Sigma \models F(y,\mathbf{w}) \approx x$ for $y \neq x$ and some sequence of not necessarily distinct variables $\mathbf{w}$. By setting $x=1, y=0$ and $\mathbf{w}=\mathbf{s}$ we obtain $F^{\mathbf{S}}(0,\mathbf{s}) = 1$, where $F^{\mathbf{S}}$ is a semilattice term (equivalent to a meet of variables). Necessarily $F^{\mathbf{S}}$ does not depend on its first variable. Thus $\mathbf{S} \models F(x,\mathbf{z}) \approx F(y,\mathbf{z})$ where x, y, and all variables in the sequence $\mathbf{z}$ are distinct. This shows that $\mathbf{S}$ is a model of Σ'. This is enough to prove that the realization of Σ' also does not force the satisfaction of a nontrivial congruence identity (since the variety of semilattices does not satisfy a nontrivial congruence identity, [5]).

We have shown that if Σ is idempotent and the realization of Σ does not force the satisfaction of a nontrivial congruence identity, then both properties hold for Σ',

[1]In fact, it is possible to show that $\Sigma^{(\lceil n/2\rceil)}$ is inconsistent by working inward from both ends of the sequence $M_0,\ldots,M_n$ at the same time, but this does not add anything useful to this proof.

hence for $\Sigma^{(n)}$ for any n. In particular, $\Sigma^{(n)}$ is consistent for any n. This is the contrapositive of [$\Leftarrow$]. $\square$

Example 4.4. Lemma 3.10 of [12], which is credited to Day, proves that a congruence n-permutable variety with a semilattice operation satisfies a nontrivial congruence identity. In other words, if Σ_1 is the set of identities from Theorem 3.10 (2) and Σ_2 is the set of identities expressing that some binary term $s(x, y)$ is a semilattice operation, then any variety realizing the (idempotent) set of identities $\Sigma_1 \cup \Sigma_2$ satisfies a nontrivial congruence identity.

Later, in Theorem 9.19 of [10], D. Hobby and R. McKenzie proved that any locally finite congruence n-permutable variety satisfies a nontrivial congruence identity. (No assumption is made about the existence of a semilattice term.)

The full result, that any congruence n-permutable variety satisfies a nontrivial congruence identity, was established by P. Lipparini in [20]. He went on to publish alternative proofs of this theorem in [19] and [21].

Another proof that any congruence n-permutable variety satisfies a nontrivial congruence identity was found by K. A. Kearnes and J. B. Nation in [16].

Here we show how to derive this theorem from Theorem 4.2. Let Σ denote the set of identities in Theorem 3.10 (2).

Claim 4.5. $\Sigma^{(i)} \models p_i(x, u, y) \approx x$ *for all* i.

The claim holds for $i = 0$ by identity (2)(a) of Theorem 3.10. Assume that the claim holds for some $k \geq 0$. From this, by identity (2)(b) of Theorem 3.10, we derive that $\Sigma^{(k)} \models x \approx p_k(x, x, y) \approx p_{k+1}(x, y, y)$, so p_{k+1} is weakly independent of its last two variables relative to $\Sigma^{(k)}$. Thus p_{k+1} is fully independent of its last two variables relative to $\Sigma^{(k+1)}$, and this means that $\Sigma^{(k+1)} \models p_{k+1}(x, u, y) \approx p_{k+1}(x, x, x) \approx x$. This proves the claim.

Combining the claim with Theorem 3.10 (2)(a), we get that $\Sigma^{(n)} \models x \approx p_n(x, u, y) \approx y$, hence $\Sigma^{(n)}$ is inconsistent. Now apply Theorem 4.2.

References

[1] Bentz, W., *Topological implications in varieties.* Algebra Universalis **42** (1999), 9–16.

[2] Berman, J., Idziak, P., Marković, P., McKenzie, R., Valeriote, M., Willard, R., *Varieties with few subalgebras of powers.* Trans. Amer. Math. Soc. **362** (2010), no. 3, 1445–1473.

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

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

[5] Freese, R. and Nation, J. B., *Congruence lattices of semilattices.* Pacific J. Math. **49** (1973), 51–58.

[6] García, O. C. and Taylor, W., *The lattice of interpretability types of varieties.* Mem. Amer. Math. Soc. **50** (1984), no. 305.

[7] Gedeonová, E., *A characterization of p-modularity for congruence lattices of algebras.* Acta Fac. Rerum Natur. Univ. Comenian. Math. Publ. **28** (1972), 99–106.
[8] Gumm, H.-P., *Congruence modularity is permutability composed with distributivity.* Arch. Math. (Basel) **36** (1981), 569–576.
[9] Hagemann, J.; Mitschke, A., *On n-permutable congruences.* Algebra Universalis **3** (1973), 8–12.
[10] Hobby, D., McKenzie, R., *The structure of finite algebras.* Contemporary Mathematics, **76**. American Mathematical Society, Providence, RI, 1988.
[11] Jónsson, B., *On the representation of lattices.* Math. Scand. **1**, (1953), 193–206.
[12] Jónsson, B., *Congruence varieties.* Algebra Universalis **10** (1980), 355–394.
[13] Kearnes, K. A., *Almost all minimal idempotent varieties are congruence modular.* Algebra Universalis **44** (2000), 39–45.
[14] Kearnes, K. A. and Kiss, E. W., *The Shape of Congruence Lattices.* http://spot.colorado.edu/ kearnes/Papers/cong.pdf
[15] Kearnes, K. A., Kiss, E. W., and Szendrei, Á., *Growth rates of finite algebras.* manuscript.
[16] Kearnes, K. A. and Nation, J. B., *Axiomatizable and nonaxiomatizable congruence prevarieties.* Algebra Universalis **59** (2008), 323–335.
[17] Kearnes, K. A. and Sequeira, L., *Hausdorff properties of topological algebras.* Algebra Universalis **47** (2002), 343–366.
[18] Kelly, D., *Basic equations: word problems and Mal'cev conditions.* Abstract 701-08-4, Notices Amer. Math. Soc. **20** (1973), A-54.
[19] Lipparini, P., *Congruence identities satisfied in n-permutable varieties.* Boll. Un. Mat. Ital. B (7) **8** (1994), no. 4, 851–868.
[20] Lipparini, P., *n-permutable varieties satisfy nontrivial congruence identities.* Algebra Universalis **33** (1995), 159–168.
[21] Lipparini, P., *Every m-permutable variety satisfies the congruence identity $\alpha\beta_h = \alpha\gamma_h$.* Proc. Amer. Math. Soc. **136** (2008), no. 4, 1137–1144.
[22] Nation, J. B., *Varieties whose congruences satisfy certain lattice identities.* Algebra Universalis **4** (1974), 78–88.

(Topaz Dent) Department of Mathematics, University of Colorado, Boulder, CO 80309-0395, USA

E-mail address: `Topaz.Dent@Colorado.EDU`

(Keith Kearnes) Department of Mathematics, University of Colorado, Boulder, CO 80309-0395, USA

E-mail address: `Keith.Kearnes@Colorado.EDU`

(Ágnes Szendrei) Department of Mathematics, University of Colorado, Boulder, CO 80309-0395, USA

E-mail address: `Agnes.Szendrei@Colorado.EDU`