FINITE AXIOMATISABILITY OF SUBDIRECTLY IRREDUCIBLE MEMBERS OF CERTAIN NILPOTENT VARIETIES

JOSHUA T. GRICE

(November 6, 2019)

Abstract

Let $\mathcal{V}$ be a congruence modular variety generated by a finite nilpotent algebra $\mathbf{A}$. If $\mathbf{A}$ is a product of algebras of prime power order, then the class $\mathcal{V}_{\mathrm{si}}$ of subdirectly irreducible members of $\mathcal{V}$ can be axiomatised by a finite set of elementary sentences.

1. Introduction

We define an *algebra* as a nonempty set endowed with some collection of finitary operations. A *variety* is a class of algebras that is closed with respect to the formation of homomorphic images, subalgebras, and direct products (all of which are defined in the natural way using the basic operations of the algebras). By a 1935 result of Garrett Birkhoff [3], a variety is also precisely the class of algebras axiomatised by a certain set of elementary sentences. The smallest variety containing a given algebra $\mathbf{A}$ is denoted $\mathcal{V}(\mathbf{A})$, and referred to as the *variety generated by* $\mathbf{A}$.

Groups, rings, vector spaces, Boolean algebras, and lattices are all well-known examples of algebras. The correspondence between the algebraic notions of homomorphic images, subalgebras and direct products and the logical notion of axiomatisability has afforded a different perspective on these algebras that can be used to discover commonalities between these separate kinds of objects.

In group theory and ring theory, much of the structural information of the object of interest comes from the study of special subalgebras: normal subgroups in group theory and two-sided ideals in ring theory. Due to the lack of guaranteed identity elements in general algebras, such special subalgebras often fail to exist. But the identification of normal subgroups and ideals as kernels of homomorphisms can be extended to algebras.

If $h : \mathbf{A} \to \mathbf{B}$ is a homomorphism between algebras with the same basic operations (that is, a map that preserves all of those operations), we define the *relational kernel* of h to be the subalgebra of $\mathbf{A}^2$ given by $\{\langle a, b\rangle \mid h(a) = h(b)\}$. This kernel is a special type of equivalence relation called a *congruence relation.* The congruence relations on an algebra $\mathbf{A}$ are also precisely the equivalence relations on $\mathbf{A}$ that are subalgebras of $\mathbf{A}^2$. The congruences of a given algebra $\mathbf{A}$ form a complete lattice under set inclusion, denoted $\mathrm{Con}(\mathbf{A})$. Given two congruences α and β in this lattice, the greatest lower bound or *meet* of two congruences (which is just their intersection) is denoted by $\alpha \wedge \beta$. Their least upper bound or *join* (the congruence generated by their union) is denoted $\alpha \vee \beta$. A congruence on $\mathbf{A}$ is called *principal* if it the smallest congruence containing a given pair $\langle a, b\rangle$, in which case it is denoted $\mathrm{Cg}^{\mathbf{A}}(a, b)$.

An algebra $\mathbf{A}$ is called *subdirectly irreducible* if it has a smallest nontrivial congruence called its *monolith.* This monolith is principal, as it cannot properly contain any other nontrivial congruences. Any nontrivial pair belonging to the monolith is what we call a *critical pair*: that is, a pair $\langle c, d\rangle$ so that for any nontrivial congruence α on $\mathbf{A}$, we have $\langle c, d\rangle \in \alpha$. Given a variety $\mathcal{V}$, we write $\mathcal{V}_{\mathrm{si}}$ to denote the class of subdirectly irreducible members of $\mathcal{V}$. In 1944, Birkhoff also proved in [4] that two varieties are equal if and only if they share the same subdirectly irreducible members, so the study of $\mathcal{V}_{\mathrm{si}}$ can grant insight into $\mathcal{V}$ itself.

If an algebra or class of algebras is axiomatisable by finitely many equations, we say that it is *finitely based.* Subdirect irreducibility isn't preserved by direct products, so $\mathcal{V}_{\mathrm{si}}$ isn't a variety and therefore cannot be axiomatised by equations. But it might still be axiomatisable by more broad sentences of first-order logic. If an algebra or class of algebras can be axiomatised by elementary sentences (which are built up from equations with the help of logical connectives and quantifiers), we say that it is *finitely axiomatisable.* The main result of this paper shows that this can happen if the algebra $\mathbf{A}$ that generates the variety $\mathcal{V}$ satisfies a few particular hypotheses. Included in these hypotheses is nilpotence, which can be seen as a generalised abelianness, and which we will define below.

Theorem 1.1. *Let* $\mathbf{A}$ *be a finite nilpotent algebra that is a product of algebras of prime power order such that* $\mathcal{V} = \mathcal{V}(\mathbf{A})$ *is a congruence modular variety. Then,* $\mathcal{V}_{\mathrm{si}}$ *is finitely axiomatisable.*

In 1996, Ralph McKenzie in [13] solved Tarski's Finite Basis Problem by proving that there is no algorithm to determine whether a given finite algebra is finitely based. However, much progress has been made in classifying what kinds of algebras and varieties are finitely based or finitely axiomatisable.

In 1964, Oates and Powell proved that any finite group is finitely based [14]. Kruse and L'vov independently extended that result to finite rings in 1973 [7], [8]. In 1970, McKenzie proved in [11] that any finite lattice with finitely many additional basic operations is finitely based. A generalisation of this comes in the form of Baker's Finite Basis Theorem [1], which states that if $\mathbf{A}$ is a fintie algebra with only finitely many basic operations and $\mathcal{V}(\mathbf{A})$ is congruence distributive, then $\mathbf{A}$ is finitely based. Baker's theorem was reproved a number of times by different researchers and inspired much of the investigation into finite basis problems.

Congruence distributivity is one of several algebraic qualities of the congruence lattice of algebras in a variety. We say that $\mathcal{V}$ is *congruence distributive* if for any $\mathbf{A} \in \mathcal{V}$, we have that any congruences $\alpha, \beta, \gamma \in \operatorname{Con}(\mathbf{A})$ satisfy the equation

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

or its equivalent dual. Congruence distributivity is less frequently encountered in the study of the classical types of algebras. Groups, rings, vector spaces, and other types of 19th-century algebras often fail to be congruence distributive. They do, however, satisfy a weakening of the distributive law that was discovered by Dedekind in the late 19th century, which he called the modular law, and is as follows:

$$\alpha \wedge \beta = \beta \Rightarrow \alpha \wedge (\beta \vee \gamma) = (\alpha \wedge \beta) \vee (\alpha \wedge \gamma)$$

A variety $\mathcal{V}$ is called *congruence modular* if any congruences α, β, γ on any algebra $\mathbf{A} \in \mathcal{V}$ satisfy this law. Modularity enables a well-behaved extention of the commutator on groups that can be used to define Abelianness, solvability, and nilpotence. Using these notions, Freese and Vaughan-Lee showed that congruence modular varieties generated by certain finite nilpotent algebras are finitely based. This result is stated as Theorem 2.3 in section 2, after we define nilpotence.

A few finite basis results are contingent upon the variety having a *finite residual bound:* that is, a finite upper bound on the cardinalities of the algebras in $\mathcal{V}_{\text{si}}$. In 1974, Bjarni Jónsson speculated that any variety with a finite residual bound that is generated by a finite algebra with finitely many basic operations is finitely based. Jónsson's speculation is still open in its generality, and was the inspiration for many finite basis results from the last several decades. For instance, McKenzie proved in [12] that if $\mathbf{A}$ is a finite algebra with finitely many basic operations so that $\mathcal{V}(\mathbf{A})$ is congruence modular and has a finite residual bound, then $\mathbf{A}$ is finitely based.

Willard proved a similar result in [15], where he showed that if $\mathbf{A}$ is a finite algebra with finitely many basic operations so that $\mathcal{V}(\mathbf{A})$ is congruence meet-semidistributive and has a finite residual bound, then $\mathbf{A}$ is finitely based. Meet-semidistributivity is yet another weakening of the distributive law:

$$\alpha \wedge \beta = \alpha \wedge \gamma \Rightarrow \alpha \wedge (\beta \vee \gamma) = (\alpha \wedge \beta) \vee (\alpha \wedge \gamma)$$

Many algebraic properties of varieties depend upon the presence of certain terms (which are built of compositions of the basic operations of the variety) that satisfy certain equations. For example, a ternary term $p(x, y, z)$ is called a *difference term* if it satisfies the identity $p(x, x, y) \approx y$ and if $p(a, b, b) = a$ whenever $\langle a, b\rangle$ belongs to an abelian congruence of an algebra in the variety. Kearnes, Szendrei and Willard proved in [6] that if $\mathcal{V}$ is a variety with finitely many basic operations and a finite residual bound, then $\mathcal{V}$ is finitely based.

The condition of $\mathcal{V}$ having a finite residual bound is quite restrictive to the subdirectly irreducible algebras in $\mathcal{V}$. It implies that there are only finitely many algebras in $\mathcal{V}_{\text{si}}$, up to isomorphism. In this way, each of the finite basis results that include a finite residual bound as a hypothesis carry with them a sort of automatic finite axiomatisability of $\mathcal{V}_{\mathrm{si}}$. The result of this paper indicates that such an axiomatisability also happens in the case of certain nilpotent varieties. This result is somewhat orthogonal to McKenzie's in [12], since nilpotent varieties with finite residual bounds only contain abelian algebras.

In 2000, McNulty and Wang circulated a preprint of an ultimately incorrect proof that for any finite group $\mathbf{G}$ and $\mathcal{V} = \mathcal{V}(\mathbf{G})$, $\mathcal{V}_{\mathrm{si}}$ is finitely axiomatisable. The proof has not yet been repaired, but the author has made it partway to McNulty and Wang's conjecture by proving in an unpublished paper that if $\mathbf{G}$ is a finite nilpotent group and $\mathcal{V} = \mathcal{V}(\mathbf{G})$, then $\mathcal{V}_{\mathrm{si}}$ is finitely axiomatisable. Nilpotence can be thought of as a measure of how close to being abelian a group is. It is this result that inspired the current paper, which goes partway to extending the result about nilpotent groups up to nilpotent algebras.

2. Preliminaries

2.1. Nilpotence We will begin by generalising the group theoretic notions of Abelianness and nilpotence to general algebras. Most of the theory in this paper comes from Freese and McKenzie's excellent book on commutator theory in general algebras [5]. Abelianness and nilpotence, both in groups and in algebras, can be defined by use of the commutator operation, or using the notion of a center. We will use the latter, as it is all we will need in the proof, but readers curious about the commutator perspective on things will find enrichment in this book. We will assume, from this point onwards, that any varieties are congruence modular, any algebras generate congruence modular varieties.

A group G is Abelian if all of its elements commute. This property is powerful but rare; in general we can find an Abelian normal subgroup of any given group by taking its center. Given a group G, the *center* of G is defined

$$Z(G) = \{x \in G \mid gx = xg \text{ for any } g \in G\}$$

We can then use the center to define the *upper central series* of G; this is a series

$$\{1\} = Z_0 \lhd Z_1 \lhd Z_2 \lhd \dots$$

of normal subgroups of G so that $Z_{i+1}/Z_i = Z(G/Z_i)$ for each i. If the upper central series terminates, that is, there is some k for which $Z_k = G$, we say that G is *nilpotent of class k.* Since Z_1 is just $Z(G)$, we see that G is Abelian if and only if it is nilpotent of class 1. Lyndon proved in 1952 [9] that the variety generated by any nilpotent group is finitely based.

In general algebras, defining the center becomes a bit trickier. Since the basic operations of an algebra can be much more complicated than the binary multiplication of groups, we have to adjust our definition of Abelianness. We first define Abelian congruences.

Suppose α is a congruence of an algebra $\mathbf{A}$. Then, α is Abelian if for any term $t(\bar{u}, \bar{v})$ and any tuples $\bar{a_1}, \bar{a_2}$ of the same length as $\bar{u}$ and $\bar{b_1}, \bar{b_2}$ of the same length of $\bar{v}$ so that $\langle a_{1_i}, a_{2_i} \rangle \in \alpha$ for each i and $\langle b_{1_j}, b_{2_j} \rangle \in \alpha$ for each j, we have that $t(\bar{a_1}, \bar{b_1}) = t(\bar{a_1}, \bar{b_2}) \to t(\bar{a_2}, \bar{b_1}) = t(\bar{a_2}, \bar{b_2})$. That is, the following diagram holds:

$$\begin{tikzcd}
t(\bar{a_1}, \bar{b_1}) \arrow[r, dash, "\alpha"] \arrow[r, bend left, "="] \arrow[d, dash, "\alpha"] & t(\bar{a_1}, \bar{b_2}) \arrow[d, dash, "\alpha"] \\
t(\bar{a_2}, \bar{b_1}) \arrow[r, dash, "\alpha"] \arrow[r, bend left, dashed, "="] & t(\bar{a_2}, \bar{b_2})
\end{tikzcd}$$

Each algebra $\mathbf{A}$ has at least one abelian congruence called the *center.* The center is the binary relation $\zeta_{\mathbf{A}}$ on $\mathbf{A}$ defined by

$$\langle x, y \rangle \in \zeta_{\mathbf{A}} \Leftrightarrow (\forall t)(\forall \bar{u}, \bar{v})(t(\bar{u}, x) = t(\bar{v}, x) \leftrightarrow t(\bar{u}, y) = t(\bar{v}, y))$$

where the first quantifier is over all term operations on $\mathbf{A}$ and the second over all n-tuples from A, depending on the arity of t. It follows from the definitions that $\zeta_{\mathbf{A}}$ is an abelian congruence on $\mathbf{A}$. An algebra $\mathbf{A}$ is called Abelian if $\zeta_{\mathbf{A}} = 1_{\mathbf{A}}$.

Equipped as we are now with the definition of a center, the above definition of a group's upper central series generalises nicely. We define the *upper central series* of an algebra $\mathbf{A}$ to be the series of congruences

$$0_{\mathbf{A}} = \zeta_0 \leq \zeta_1 \leq \zeta_2 \leq \dots$$

so that $\zeta_{i+1}/\zeta_i = \zeta(\mathbf{A}/\zeta_i)$ for each i, where ζ_{i+1}/ζ_i refers to the image of the congruence ζ_{i+1} under the quotient map that forms ζ_i. If this upper central series terminates so that $\zeta_k = 1_{\mathbf{A}}$ for some k, we say that $\mathbf{A}$ is *nilpotent of class k.* This definition generalises the definition for nilpotence in groups. We will call a variety $\mathcal{V}$ *nilpotent of class k* if all of the algebras belonging to $\mathcal{V}$ are nilpotent of class k.

2.2. Congruence Permutability Groups carry the useful property that if H and K are normal subgroups of G, their products commute; that is, $HK = KH$. This property generalises to congruences of algebras. If α and β are congruences on an algebra $\mathbf{A}$, we define their *composition* as

$$\alpha \circ \beta = \{\langle a, b \rangle \mid \exists c \in A \text{ so that } \langle a, c \rangle \in \alpha \text{ and } \langle c, b \rangle \in \beta\}$$

An algebra $\mathbf{A}$ is called *congruence permutable* if, for any two congruences α and β of $\mathbf{A}$, we have $\alpha \circ \beta = \beta \circ \alpha$. Groups are an example of congruence permutable algebras. We call a variety $\mathcal{V}$ congruence permutable if every algebra contained in $\mathcal{V}$ is congruence permutable.

In [10], Anatoli Mal'tsev proved that a variety $\mathcal{V}$ is congruence permutable if and only if it has a ternary term $m(x, y, z)$ so that

$$m(x, y, y) = x = m(y, y, x)$$

We call such a term a *Mal'tsev term.* For example, any variety of groups has the Mal'tsev term $m(x, y, z) = xy^{-1}z$. Freese and McKenzie in [5] prove a number of results relating nilpotence and congruence permutability. We collapse the information that we need in this paper into one theorem for convenience of presentation.

THEOREM 2.1. *If* $\mathbf{A}$ *is a nilpotent algebra and* $\mathcal{V} = \mathcal{V}(\mathbf{A})$ *is a congruence modular variety, then the following are true:*

1. $\mathcal{V}$ *is congruence permutable and has Mal'tsev term* $m(x, y, z)$*.*
2. *If* $\mathbf{A} \in \mathcal{V}$ *and* $a, b, c \in A$*, then* $\mathrm{Cg}^{\mathbf{A}}(a, b) = \mathrm{Cg}^{\mathbf{A}}(m(a, b, c), c)$
3. $(c, d) \in \mathrm{Cg}^{\mathbf{A}}(a, b)$ *iff there exists a unary polynomial* $p(x)$ *so that* $\{p(a), p(b)\} = \{c, d\}$*.*

We will also make use of the finite basis result of Freese and McKenzie. Given any variety $\mathcal{V}$ and a set X of variables, we define the *free algebra* $\mathcal{F}_{\mathcal{V}}(X)$ to be a set of representatives of terms of $\mathcal{V}$ in the variables in X under the equivalence relation defined by the equations true in $\mathcal{V}$. If $\mathcal{V}$ is generated by a finite algebra, it is *locally finite*, meaning that all its finitely generated algebras are finite; $\mathcal{F}_{\mathcal{V}}(X)$ in particular for any finite X.

Now, suppose $\mathcal{V}$ is a nilpotent congruence modular variety, as in Theorem 2.1. Consider $\mathbf{F} = \mathcal{F}_{\mathcal{V}}(X \cup z)$ for some set X of variables. Define $u + v = m(u, z, v)$ where m is the Mal'tsev term in $\mathcal{V}$. This addition generates a group structure on $\mathcal{F}$. For $x \in X$ define $\delta_x \in \mathrm{End}(\mathbf{F})$ as the map where $\delta_x(x) = z$, $\delta_x(z) = z$, and $\delta(y) = y$ for any $y \in X - \{x\}$. In other words, δ_x fixes every element of $X \cup z$ except for x itself, which it maps to z. Then, given a term $w(x_1, \ldots, x_n, z) \in F$, we say that w is a *commutator word* if $w \circ \delta_x = z$ for any $x \in X$. That is to say, if any of $x_1, \ldots, x_n$ are replaced with z, $w(\bar{x}, z) = z$. Commutator words provide a sort of decomposition for general terms in $\mathcal{V}$, as shown by the following theorem, which is Lemma 14.6 in [5].

THEOREM 2.2. *If* $\mathcal{V}$ *is a congruence permutable variety and* $w(\bar{x}, z)$ *is a term in the free algebra on* $X \cup z$*, then there exist commutator words* c_i *so that*

$$w(\bar{x}, z) \approx w(\bar{z}) + c_1 + c_2 + \ldots + c_m$$

Here, $u + v$ *is defined as* $m(u, z, v)$*, and associates to the right.*

As it turns out, commutator words with enough variables always trivialise in a nilpotent congruence modular varietie generated by a finite algebra. The following is Theorem 14.16 in [5].

THEOREM 2.3. *Let* $\mathbf{A}$ *be a finite nilpotent algebra that is a product of algebras of prime power order such that* $\mathcal{V} = \mathcal{V}(\mathbf{A})$ *is a congruence modular variety. Then,* $\mathcal{V}$ *is finitely based. Morevover, there is an integer* M *such that if* $w(x, z)$ *is a commutator word in more than* M *variables, then* $\mathcal{V} \models w(x, z) \approx z$*.*

This theorem also carries within it a proof that if $\mathbf{A}$ is finite and nilpotent of class k, any other algebra contained within $\mathcal{V}(\mathbf{A})$ is nilpotent of class at most k.

2.3. Definable Principal Subcongruences A first-order formula $\Phi(u, v, x, y)$ with four free variables is called a *congruence formula* for a class $\mathcal{K}$ of algebras provided that for every algebra $\mathbf{A} \in \mathcal{K}$,

$$\text{if } \mathbf{A} \models \Phi(a, b, c, d), \text{ then } \langle a, b\rangle \in \mathrm{Cg}^{\mathbf{A}}(c, d)$$

A class $\mathcal{K}$ of algebras is said to have *definable principal subcongruences* if and only if there are congruence formulas $\Phi(u, v, x, y)$ and $\Psi(u, v, x, y)$ so that for every $\mathbf{A} \in \mathcal{K}$ and every $c, d \in A$ with $c \neq d$, there exist $a, b \in A$ with $a \neq b$ so that

1. $\mathbf{A} \models \Psi(a, b, c, d)$ and
2. $\Phi(u, v, a, b)$ defines $\mathrm{Cg}^{\mathbf{A}}(a, b)$.

In other words, if a principal congruence on any algebra in $\mathcal{K}$ is chosen, the first formula Ψ is capable of finding another principal congruence contained within it that is definable by the second formula Φ. This definition is introduced by Baker and Wang in [2], where they prove another finite basis theorem:

Theorem (Baker, Wang). *Let $\mathcal{V}$ be a variety with only finitely many fundamental operations and suppose that $\mathcal{V}$ has definable principal subcongruences. Then, $\mathcal{V}$ is finitely based if and only if $\mathcal{V}_{\mathrm{si}}$ is finitely axiomatisable.*

A variation on the proof of this theorem yields the following result, whose proof we reproduce from McNulty & Wang's unpublished work.

Theorem 2.4. *If $\mathcal{V}$ is a variety and $\mathcal{V}_{\mathrm{si}}$ has definable principal subcongruences, then $\mathcal{V}_{\mathrm{si}}$ is finitely axiomatisable relative to $\mathcal{V}$. In particular, if $\mathcal{V}$ is finitely based, then $\mathcal{V}_{\mathrm{si}}$ is finitely axiomatisable.*

Proof. Let Σ be a finite set of elementary sentences which axiomatises $\mathcal{V}$, and let $\Phi(u, v, x, y)$ and $\Psi(u, v, x, y)$ be the formulas witnessing that $\mathcal{V}_{\mathrm{si}}$ has definable principal subcongruences. Let Θ be the following set of sentences:

$$\Sigma \cup \{\exists u, v, [u \neq v \wedge \forall z, w(z \neq w \Rightarrow \exists x, y(\Phi(u, v, x, y) \wedge \Psi(x, y, z, w)))]\}$$

We claim that Θ axiomatises $\mathcal{V}_{\mathrm{si}}$.

On one hand, suppose $\mathbf{S} \in \mathcal{V}_{\mathrm{si}}$. Let $\langle c, d\rangle$ be a crticial pair for $\mathbf{S}$. So, $c \neq d$ and $\langle c, d\rangle$ belongs to every nontrivial congruence. Now, let $e, f \in S$ with $e \neq f$. Because $\mathcal{V}_{\mathrm{si}}$ has definable principal subcongruences, there are $a, b \in S$ where $a \neq b$ so that $\mathbf{S} \models \Psi(a, b, e, f)$, and $\Phi(x, y, a, b)$ defines $\mathrm{Cg}^{\mathbf{S}}(a, b)$. Since $a \neq b$ and $\langle c, d\rangle$ is critical pair, $\langle c, d\rangle \in \mathrm{Cg}^{\mathbf{S}}(a, b)$, so $\mathbf{S} \models \Phi(c, d, a, b)$. So,

$$\mathbf{S} \models \{\exists u, v, [u \neq v \wedge \forall z, w(z \neq w \Rightarrow \exists x, y(\Phi(u, v, x, y) \wedge \Psi(x, y, z, w)))]\}$$

Since $\mathbf{S}$ is in $\mathcal{V}$, $\mathbf{S} \models \Sigma$ also. Therefore, $\mathbf{S} \models \Theta$.

Now, suppose $\mathbf{S} \models \Theta$. Then, $\mathbf{S} \in \mathcal{V}$ since Σ axiomatises $\mathcal{V}$. But also, since $\mathbf{S}$ believes the second part of Θ and Φ and Ψ are congruence formulas, there exist $c, d \in S$ so that $c \neq d$ and $\langle c, d\rangle$ is contained within any other principal congruence. So, $\langle c, d\rangle$ is a critical pair for $\mathbf{S}$ and $\mathbf{S}$ is subdirectly irreducible. □

In light of this and of Theorem 2.3, in order to prove our main result, we must prove the following:

Theorem 2.5. *Let* $\mathbf{A}$ *be a finite nilpotent algebra that is a product of algebras of prime power order such that* $\mathcal{V} = \mathcal{V}(\mathbf{A})$ *is a congruence modular variety. Then,* $\mathcal{V}_{\mathrm{si}}$ *has definable principal subcongruences.*

We will do this by using part (3) of Theorem 2.1. Recall that the membership condition $\langle c, d\rangle \in \mathrm{Cg}_{\mathbf{A}}(a, b)$ is equivalent to the presence of some unary polynomial $p(x)$ so that $\{p(a), p(b)\} = \{c, d\}$. In this paper, we define the *complexity* of $p(x)$ as the number of parameters used in p. So, if we can limit the complexity of p in some way that is determined entirely by the variety, we can find a first-order sentence equivalent to the membership condition in question. This will be our strategy to complete the proof of the main result.

3. Finding $\Phi(u, v, x, y)$

We begin with the following handy lemma, which follows directly from the definition of the commutator.

Lemma 3.1. *Let* $\mathcal{V}$ *be any variety. Let* $\mathbf{A} \in \mathcal{V}$*, and let* $\alpha \in \mathrm{Con}(\mathbf{A})$ *be an abelian congruence. Suppose* $\langle a, b\rangle \in \alpha$*, and let* $r(u, v, \bar{y})$ *be a term so that* $r^{\mathbf{A}}(b, b, \bar{d}) = b$ *for any sequence* $\bar{d}$ *of parameters. Then, it is also the case that* $r^{\mathbf{A}}(a, b, \bar{d}) = r^{\mathbf{A}}(a, b, \bar{e})$ *for any sequences of parameters* $\bar{d}$ *and* $\bar{e}$*. In other words,* r *only depends on the first two coordinates.*

Proof. Let r be as above. Then, since $\langle a, b\rangle \in \alpha$ and α is an abelian congruence, the following diagram holds:

$$\begin{array}{lllllll}
r(b,b,\bar{d}) = b & \alpha & & & & & b = r(b,b,\bar{e}) \\
\alpha & & & & & & \alpha \\
r(a,b,\bar{d}) & \alpha & r(b,b,\bar{d}) = b & \alpha & b = r(b,b,\bar{e}) & \alpha & r(a,b,\bar{e})
\end{array}$$

So, by the definition of the commutator and since $\langle r(b, b, \bar{d}), r(b, b, \bar{e})\rangle \in 0_{\mathbf{A}}$, we have $\langle r(a, b, \bar{d}), r(a, b, \bar{e})\rangle \in 0_{\mathbf{A}}$ also. □

This tells us the following information regarding commutator words, which will be useful later.

Corollary 3.2. *Let* $w(x, \bar{y}, z)$ *be a commutator word in* $\mathcal{V}$ *with* z *as its neutral element. Let* $\alpha \in \mathrm{Con}(\mathbf{A})$ *be an abelian congruence. Then, for any* $\langle a, b\rangle \in \alpha$ *and any parameters* $\bar{d}$*, we have that* $w(a, \bar{d}, b) = b$*.*

Proof. Suppose $w(x, \bar{y}, z)$ is a commutator as above. Set $r(u, v, \bar{y}) = w(u, \bar{y}, v)$, and let $a, b \in \alpha$ and $\bar{d}$ be any sequence of parameters. Since w is a commutator word, $w(z, \bar{y}, z) \approx z$, so $r^{\mathbf{A}}(b, b, \bar{d}) = b$. So, by Lemma 3.2, w only depends on its first and last coordinates. So, $w(a, \bar{d}, b) = w(a, b, \ldots, b, b) = b$ since w is a commutator word. □

Now, we prove the existence of our desired Φ.

Theorem 3.3. *Let $\mathcal{V}$ be a locally finite, nilpotent, congruence modular variety. Then, there exists a congruence formula $\Phi(u, v, x, y)$ so that for any $\mathbf{A} \in \mathcal{V}$ and abelian principal congruence $\alpha = \mathrm{Cg}^{\mathbf{A}}(a, b)$, α is defined by $\Phi(u, v, a, b)$.*

Proof. Let $\mathcal{V}$ and $\mathbf{A}$ be as stated, and $\alpha = \mathrm{Cg}^{\mathbf{A}}(a, b)$. First, we observe that since $\mathcal{V}$ is congruence permutable with Mal'cev term m,

$$\begin{aligned}\langle c, d\rangle \in \mathrm{Cg}^{\mathbf{A}}(a, b) &\Leftrightarrow \mathrm{Cg}^{\mathbf{A}}(c, d) \subseteq \mathrm{Cg}^{\mathbf{A}}(a, b) \\ &\Leftrightarrow \mathrm{Cg}^{\mathbf{A}}(m(c, d, b), b) \subseteq \mathrm{Cg}^{\mathbf{A}}(a, b) \\ &\Leftrightarrow \langle m(c, d, b), b\rangle \in \mathrm{Cg}^{\mathbf{A}}(a, b)\end{aligned}$$

So, we only have to worry about characterising membership conditions of the form $\langle c, b\rangle \in \mathrm{Cg}^{\mathbf{A}}(a, b)$. We claim that such a membership can be witnessed by a binary term.

Suppose, indeed, that $\langle c, d\rangle \in \mathrm{Cg}^{\mathbf{A}}(a, b)$. Then, there is a unary polynomial $p = s(x, \bar{d})$ witnessing the membership. Suppose without loss of generality that $p(a) = c$ and $p(b) = b$. Now, set

$$r(u, v, \bar{y}) = m(s(u, \bar{y}), s(v, \bar{y}), v)$$

Now, for any parameters $\bar{e}$, we have that $r(b, b, \bar{e}) = m(s(b, \bar{e}), s(b, \bar{e}), b) = b$. So, by Lemma 3.1 $r(a, b, \bar{d}) = r(a, b, \bar{b}) = c$ and $r(b, b, \bar{d}) = r(b, b, \bar{b}) = b$ where $\bar{b}$ is the sequence of the same length as $\bar{e}$ with b in every coordinate. Define $t(x, y) := r(x, y, y, \ldots, y)$. Then, $t(a, b) = c$ and $t(b, b) = b$. So the polynomial $t(x, b)$ witnesses the membership condition.

Now, let T be a set of representatives for all congruence classes of terms in the free algebra in $\mathcal{V}$ on two generators. This free algebra is finite, since $\mathcal{V}$ is locally finite. So, we can set $\Phi(u, v, x, y)$ to be the sentence

$$\bigvee_{t \in T} (t(x, y) \approx m(u, v, y) \wedge t(y, y) \approx y)$$

□

4. Finding $\Psi(u, v, x, y)$

The monolith of a nilpotent algebra is always ableian and principal, so 3.3 gets us halfway to definable principal congruences. Now, we must find Ψ to link any given principal congruence to the monolith.

Theorem 4.1. *Let $\mathbf{A}$ be a finite nilpotent algebra that is the product of algebras of prime power order such that $\mathcal{V} = \mathcal{V}(\mathbf{A})$ is a congruence modular variety. Then, there exists a congruence formula $\Psi(u, v, x, y)$ so that for any $a \neq b \in S$ where $\mathbf{S} \in \mathcal{V}_{\text{si}}$, there is a critical pair $\langle c, d\rangle$ of $\mathbf{S}$ so that $\Psi(c, d, a, b)$ is satisfied in $\mathbf{S}$.*

This theorem is a direct result of the following:

Theorem 4.2. *Let $\mathbf{A}$ be a finite nilpotent algebra that is the product of algebras of prime power order such that $\mathcal{V} = \mathcal{V}(\mathbf{A})$ is a congruence modular variety. Suppose $\mathbf{S} \in \mathcal{V}_{\text{si}}$. Then, for any $a \neq b \in S$, there exists some c so that $\langle c, b\rangle$ is a critical pair, and the membership $\langle c, b\rangle \in \mathrm{Cg}^{\mathbf{S}}(a, b)$ can be witnessed by a unary polynomial whose complexity is bounded entirely in terms of $\mathcal{V}$.*

Proof. Let V and $\mathbf{S}$ be as stated above. Let

$$0_{\mathbf{S}} = \zeta_0 \leq \zeta_1 \leq \ldots \leq \zeta_k = 1_{\mathbf{S}}$$

be the upper central series of $\mathbf{S}$. Since $\mathbf{S}$ belongs to $\mathcal{V}$, the nilpotence degree k of $\mathbf{S}$ is dependent entirely on $\mathcal{V}$. Recall that $\zeta_{i+1}/\zeta_i = \zeta(\mathbf{S}/\zeta_i)$ for each $i < k$.

Claim 1) For $i > 0$, given $a \neq b$ so that $\langle a, b\rangle \in \zeta_{i+1}$, there is some $c' \neq b$ so that $\langle c', b\rangle \in \zeta_i$ and $\langle c', b\rangle \in \mathrm{Cg}^{\mathbf{S}}(a, b)$ can be witnessed by a unary polynomial based on a commutator word.

Certainly, there exists some c so that $\langle c, b\rangle \in \zeta_i$: since the monolith μ is contained in ζ_i, we can pick c from b/μ. We know that there is $c \neq b$ in this congruence class, since nilpotent subdirectly irreducible algebras are congruence uniform. So, if no such c existed, $\mathbf{S}$ would be a trivial algebra.

So, $\langle c, b\rangle \in \zeta_i$. Pick a unary polynomial and parameters $p(x) = s(x, \bar{d})$ so that $p(a) = c$ and $p(b) = b$. Now, define $r(x, \bar{y}, z) := m(s(x, \bar{y}), s(z, \bar{y}), z)$. Note that r now satisfies the following three criteria:

1. $r(a, \bar{d}, b)\ \zeta_i\ r(b, \bar{d}, b)$
2. $r(b, \bar{d}, b) = b$
3. $r(a, \bar{d}, b) \neq b$

We claim that (1-3) can be satisfied by a commutator word, also. By 2.2, there exist commutator words $w_1, \ldots, w_m$ with neutral element z so that

$$r(x, \bar{y}, z) \approx r(z, \ldots, z) + w_1(x, \bar{y}, z) + \ldots + w_m(x, \bar{y}, z)$$

We claim that each w_i satisfies (1) and (2). The latter is clear, since w_i is a commutator word and therefore satisfies $w_i(z, \bar{y}, z) \approx z$. For the former, recall that by construction, ζ_{i+1}/ζ_i is an abelian congruence in $\mathbf{S}/\zeta_i$. So, we can apply Corollary 3.2 to $\langle a/\zeta_i, b/\zeta_i\rangle \in \zeta_{i+1}/\zeta_i$ and see that

$$w(a, \bar{d}, b)/\zeta_i = w(a/\zeta_i, \bar{d}/\zeta_i, b/\zeta_i) = b/\zeta_i = w(b, \bar{d}, b)/\zeta_i$$

We also claim that there is at least one w_j for which $w_j(a, \bar{d}, b) \neq b$. Suppose not. Then, using $x +_b y$ as shorthand for $m(x, b, y)$,

$$\begin{aligned} r(a, \bar{d}, b) &= r(b, \ldots, b) +_b w_1(a, \bar{d}, b) +_b \ldots +_b w_m(a, \bar{d}, b) \\ &= r(b, \ldots, b) +_b b +_b b +_b \ldots, +_b b \\ &= r(b, \ldots, b) \end{aligned}$$

But, $r(b, \ldots, b) = r(b, \bar{d}, b) = b$. So, $r(a, \bar{d}, b) = b$, contradicting item (3) from above. So, w_j does indeed satsify (1-3). Now, we can set c' to be $w_j(a, \bar{d}, b)$, and the claim is satisfied.

Claim 2) Given $a \neq b$ so that $\langle a, b\rangle \in \zeta_1$, there is some c so that $\langle c, b\rangle$ is a critical pair, and the membership condition $\langle c, b\rangle \in \mathrm{Cg}^{\mathbf{S}}(a, b)$ can be witnessed by a unary polynomial built from some binary term.

Let $\langle a, b\rangle \in \zeta_1$ as above. Pick some c so that $\langle c, b\rangle$ is a critical pair. Similar to the proof in claim 1, choose a unary polynomial $p(x) = s(x, \bar{d})$ so that $p(a) = c$ and $p(b) = b$. Now, set $r(u, v, \bar{y}) = m(p(u, \bar{y}), p(v, \bar{y}), v)$. Then, $r(b, b, \bar{e}) = b$ for any sequence $\bar{e}$ of parameters. So, since $\langle a, b\rangle \in \zeta_1$ and ζ_1 is abelian, lemma 3.1 applies and $c = r(a, b, \bar{d}) = r(a, b, \bar{e})$ for any parameters $\bar{e}$. So, set $t(x, y) = r(x, y, y, \ldots, y)$. Then, $t(a, b) = c$ and $t(b, b) = b$, so the unary polynomial $q(x) = t(x, b)$ witnesses the membership condition.

With these two claims, we can prove the theorem. Let $a \neq b \in S$. Trivially, $\langle a, b\rangle \in \zeta_k$. Apply claim 1 to obtain c_1 so that $\langle c_1, b\rangle \in \zeta_{k-1}$, as witnessed by a unary polynomial based on a commutator word. Then, iterate claim 1 on c_1 and its descendents to obtain a sequence $c_1, \ldots, c_{k-1}$ so that for each i, $\langle c_i, b\rangle \in \zeta_{k-i}$, and each of these membership conditions is realised by a unary polynomial $q_i(x)$ based on a commutator word. None of these commutator words are trivial, so by Theorem 2.3, they all use no more than M parameters.

Then, apply claim 2 to c_{k-1} to get c so that $\langle c, b\rangle$ is a critical pair, and this membership condition is realised by a unary polynomial $q_k(x)$ built from a binary term.

The composition of a two unary polynomials is again unary, so composing each q_i together, we now have a unary polynomial $q(x)$ so that $q(a) = c$ and $q(b) = b$, realising the condition $\langle c, b\rangle \in \mathrm{Cg}^{\mathbf{S}}(a, b)$. This polynomial is a composition of at most k many polynomials of complexity no more than M , and one polynomial with complexity 2. Since k and M both depend on the variety $\mathcal{V}$, not on $\mathbf{S}$, this proves the theorem. □

Now, we can prove Theorem 4.1.

Proof. Given $a \neq b$ in $\mathbf{S}$, there is a critical pair $\langle c, d\rangle$ so that $\langle c, d\rangle \in \mathrm{Cg}^{\mathbf{S}}(a, b)$ is witnessed by a unary polynomial of complexity bounded above by some n depending on $\mathcal{V}$ by Theorem 4.2. Let T be a set of representatives for all congruence classes of terms in the free algebra in $\mathcal{V}$ on n generators. This free algebra is finite, since $\mathcal{V}$ is locally finite. So, $\Phi(u, v, x, y)$ is the sentence

$$\bigvee_{t \in T} (t(x, y) \approx m(u, v, y) \wedge t(y, y) \approx y)$$

□

5. Future Research

A number of natural extensions of our result beg investigation. Firstly, the hypothesis of Theorem 1.1 that the generating algebra must be a product of algebras of prime power order is somewhat restrictive; getting rid of it would be preferable. This would also generalise the author's other work on varieties of groups.

Problem 5.1. *Let $\mathcal{V}$ be a congruence modular variety generated by a finite nilpotent algebra $\mathbf{A}$. Then, is it true that $\mathcal{V}_{\mathrm{si}}$ is finitely axiomatisable?*

This question can be generalised; what hypotheses can nilpotence be replaced by to still preserve the result?

Problem 5.2. *Let $\mathcal{V}$ be a variety generated by a finite algebra $\mathbf{A}$. What properties does $\mathcal{V}$ need to have in order for $\mathcal{V}_{\mathrm{si}}$ to be finitely axiomatisable?*

By Baker and Wang's Theorem 2.4 shows that if $\mathcal{V}$ is finitely based and has definable principal subcongruences, then $\mathcal{V}_{\mathrm{si}}$ is finitely based as well. However, there is not much available in the literature to tell us when the converse might be true. This begs investigation as well.

Problem 5.3. *Let $\mathcal{V}$ be a variety so that $\mathcal{V}_{si}$ is finitely axiomatisable. What properties does $\mathcal{V}$ need to have so that $\mathcal{V}$ is finitely based?*

References

[1] Kirby A. Baker, 'Finite equational bases for finite algebras in a congruence-distributive equational class', *Advances in Math.* (3) **24** (1977), 207–243.

[2] Kirby A. Baker and Ju Wang, 'Definable principal subcongruences', *Algebra Universalis* (2) **47** (2002), 145–151.

[3] Garrett Birkhoff, 'On the structure of abstract algebras', *Mathematical Proceedings of the Cambridge Philosophical Society* (4) **31** (1935), 433–454.

[4] ———, 'Subdirect unions in universal algebra', *Bull. Amer. Math. Soc.* **50** (1944), 764–768.

[5] Ralph Freese and Ralph McKenzie, *Commutator theory for congruence modular varieties*, volume 125 of *London Mathematical Society Lecture Note Series* (Cambridge University Press, Cambridge, 1987).

[6] Keith Kearnes, Ágnes Szendrei and Ross Willard, 'A finite basis theorem for difference-term varieties with a finite residual bound', *Trans. Amer. Math. Soc.* (3) **368** (2016), 2115–2143.

[7] Robert L. Kruse, 'Identities satisfied by a finite ring', *J. Algebra* **26** (1973), 298–318.

[8] I. V. L'vov, 'Varieties of associative rings. I, II', *Algebra i Logika* **12** (1973), 269–297, 363; ibid. 12 (1973), 667–688, 735.

[9] R. C. Lyndon, 'Two notes on nilpotent groups', *Proc. Amer. Math. Soc.* **3** (1952), 579–583.

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

[11] Ralph McKenzie, 'Equational bases for lattice theories', *Math. Scand.* **27** (1970), 24–38.

[12] ———, 'Finite equational bases for congruence modular varieties', *Algebra Universalis* (3) **24** (1987), 224–250.

[13] ———, 'Tarski's finite basis problem is undecidable', *Internat. J. Algebra Comput.* (1) **6** (1996), 49–104.

[14] Sheila Oates and M. B. Powell, 'Identical relations in finite groups', *J. Algebra* **1** (1964), 11–39.

[15] Ross Willard, 'A finite basis theorem for residually finite, congruence meet-semidistributive varieties', *J. Symbolic Logic* (1) **65** (2000), 187–200.

University of South Carolina
Department of Mathematics