University of South Carolina
Scholar Commons

Theses and Dissertations

2015

Commutator Studies in Pursuit of Finite Basis Results

Nathan E. Faulkner
University of South Carolina

Follow this and additional works at: http://scholarcommons.sc.edu/etd

Part of the Mathematics Commons

Recommended Citation
Faulkner, N. E.(2015). *Commutator Studies in Pursuit of Finite Basis Results.* (Doctoral dissertation). Retrieved from http://scholarcommons.sc.edu/etd/3695

This Open Access Dissertation is brought to you for free and open access by Scholar Commons. It has been accepted for inclusion in Theses and Dissertations by an authorized administrator of Scholar Commons. For more information, please contact SCHOLARC@mailbox.sc.edu.

Commutator studies in pursuit of finite basis results

by

Nathan E. Faulkner

Bachelor of Arts
Duke University 2004

Bachelor of Science
Winston-Salem State University 2007

Master of Arts
Wake Forest University 2010

Submitted in Partial Fulfillment of the Requirements

for the Degree of Doctor of Philosophy in

Mathematics

College of Arts and Sciences

University of South Carolina

2015

Accepted by:

George McNulty, Major Professor

Joshua Cooper, Commitee Member

Ralph Howard, Committee Member

Peter Nyikos, Committee Member

Stephen Fenner, Commitee Member

Lacy Ford, Senior Vice Provost and Dean of Graduate Studies

© Copyright by Nathan E. Faulkner, 2015
All Rights Reserved.

Dedication

For Cari

Acknowledgments

[1]Like most, this work would not have been possible without the support, guidance, and encouragement of others.

For whatever the reader finds of worth in this volume, I would like to thank George McNulty, my adviser, for his insight, guidance, teaching, and thought. Just as importantly, but less obviously, I also need to thank him for his patience and care, for his generosity and the example he provides.

I would also like to thank all of my teachers who have carried me to this point. Thank you especially to my committee members, Steve Fenner, Ralph Howard, Peter Nyikos, Hong Wang, and Joshua Cooper, for their support. Thank you not only for your wisdom, but for your kindness.

I thank the Departments of Mathematics at the University of South Carolina, Wake Forest University, and Winston-Salem State University as well as Thomas Cooper Library. Thank you to Ognian Trifonov, Anton Schep, Jerrold Griggs, and Matthew Miller for their leadership during my studies at Carolina. Thank you especially to John Adeyeye at Winston-Salem State, who encouraged me to study math. Thank you, too, to my peers here and at past institutions and friends elsewhere.

Now, if the above thanks "go without saying," these last cannot. This result of five years' effort, not without some anguish, could not have happened without the support of my wife, Cari. As my adviser has suggested, mathematics often requires a bit of courage. My family, Martin, August, and Cari give me mine. Thank you also to my parents and my sisters. Thanks!!

$\alpha\chi\rho\omega$

Abstract

Several new results of a general algebraic scope are developed in an effort to build tools for use in finite basis proofs. Many recent finite basis theorems have involved assumption of a finite residual bound, with the broadest result concerning varieties with a difference term (Kearnes, Szendrei, and Willard (2013+)). However, in varieties with a difference term, the finite residual bound hypothesis is known to strongly limit the degree of nilpotence observable in a variety, while, on the other hand, there is another, older series of results in which nilpotence plays a key role (beginning with those of Lyndon (1952) and Oates and Powell (1964).) Thus, we have chosen to further study nilpotence, commutator theory, and related matters in fairly general settings. Among other results, we have been able to establish the following:

- If variety $\mathcal{V}$ has a finite signature, is generated by a nilpotent algebra and possesses a finite 2-freely generated algebra, then for all large enough N, the variety based on the N-variable laws true in $\mathcal{V}$ is locally finite and has a finite bound on the index of the annihilator of any chief factor of its algebras.

- If variety $\mathcal{V}$ has a finite signature, is congruence permutable, locally finite and generated by a supernilpotent algebra, then $\mathcal{V}$ is finitely based.

We have also established several new results concerning the commutator in varieties with a difference term, including an order-theoretic property, a "homomorphism" property, a property concerning affine behavior, and new characterizations of nilpotence in such a setting—extending work of Smith (1976), Freese and McKenzie (1987), Lipparini (1994), and Kearnes (1995).

Table of Contents

Chapter 1

Introduction

This thesis is concerned with the study of abstract algebraic systems of a general type: sets endowed with operations—all of which we shall assume to be of finite arity (or rank). These given operations—which we shall call *fundamental operations* can (of course) be composed to form new ones, which we shall call *term operations*, and it sometimes happens that a pair of term operations so formed are identical. We associate this coincidence with a syntactical object—namely, an *equation*—in a natural way. To describe this a bit further, consider a class of algebras each of which is endowed with a set of fundamental operations, which is indexed by some set of symbols—which we call the set of *fundamental operation symbols*—with each of which an intended rank is associated; this enhanced indexing is referred to as the *signature* of the class. We refer to such a class of algebras as a *similarity class*. By supplying an adequate supply of symbols for variables, we can also use the signature to index all term operations formed across the class, forming syntactical *terms* to parallel various possible compositions. Unofficially, the use of parentheses is also used to clarify presentation; for instance, the term $x \cdot (y \cdot z)$ is the familiar way to represent one side of the associative property, whether one is viewing this within the context of group theory, monoid theory, or even, a bit unnaturally—if '$\cdot$' is interpreted in the usual manner of '$+$'—addition over the natural numbers (and so forth.) An equation, then, is simply a pair of terms; we usually use a formal symbol for equality to denote this pair, writing, for example $x \cdot (y \cdot z) \approx (x \cdot y) \cdot z$ to denote the associative law, with '$\cdot$' simply a symbol awaiting interpretation as some binary operation in whatever algebraic context we care to consider. (Consult Appendix A for a more rigorous treatment of all the relevant background material.)

Our primary goal with this work is to further the understanding of a class of problems concerned with the set of equations that holds in a given system or systems. However, we have generally pursued strategies concerned with the algebraic structures themselves (rather than more syntactically-minded considerations). On the other hand, there are numerous examples of a class of algebras that are natural to study due, first of all, to some structural property shared among its constituent algebras, but which turn out also to be characterizable by its satisfaction of some set of equations. Thus, most of our results are concerned with the study of some such classes of structures, and while some of the results below are more clearly connected with the primary goal as stated above, others are less clearly so; nevertheless, it seems useful to state at the outset, as we have, what our particular motivation has been.

We shall call a class of algebras defined by its satisfaction of a set of equations, a *variety.* We shall call the set of all equations that hold in a given system its *equational theory.* Given a particular algebra $\mathbf{A}$, the variety based on the equational theory of $\mathbf{A}$ is called *the variety generated by* $\mathbf{A}$. A problem which began with the earliest work in this field is to determine whether and which algebraic systems—or, as we shall say, *algebras*—have equational theories that are axiomatizable by a finite subset of these equations. We shall refer to this body of problems as *finite basis problems.* Any equational theory that may be axiomatized by a finite set of equations we shall call *finitely based.*

An early result of this type was got by Roger Lyndon in 1952, when he showed that every nilpotent group has a finitely based equational theory. Generalizing this result (as well as a subsequent stronger result obtained M.R. Vaughan-Lee (1983) and Ralph Freese (1987)) has been one of our primary motivators. Nilpotence and a related concept, solvability, are group-theoretic concepts, which can be viewed as generalizations of abelianness. Both concepts are typically defined in terms of a two-place operation—the commutator—defined on the set of normal subgroups of a given group, though, nilpotence has other very useful characterizations as well.

A notion of commutator can also be developed for rings; indeed, beginning in the early Nineteen-Seventies and continuing since then, a rather general theory of the commutator has been developed—one which necessarily swaps the group-theoretic study of normal subgroups with the study of congruences—that is, those equivalence relations that are closed under the operations of a given algebra when applied coordinatewise—with which every group-homomorphism and hence every normal subgroup can be associated. Furthermore, the presence of this concept can be noted in most of the existing finite basis results, from Lyndon's to the present day—some of these in a retrospective sense, in view of the fact that the commutator was not available at the time of their initial discovery. For instance, nilpotence plays a crucial role in another result the proof of which has been another of our primary interests, that of Oates and Powell (1964), who proved that every finite group has a finitely based equational theory. It is also known that each finite lattice has a finitely based equational theory, and while the original proof of this fact, supplied by McKenzie (1970) does not refer to the commutator, there was subsequently developed a proof of his result which one can view as concerning the commutator. Indeed, by 2013+, Kearnes, Szendrei, and Willard had managed a proof of a rather broad result that generalizes McKenzie's result as well as—in small part—the theorem of Oates and Powell; their work very explicitly relies on analysis of the commutator. The result of Kearnes, Szendrei, and Willard concerns algebras possessing what is called a "difference term," a ternary term function, which is available in groups, quasigroups, rings, modules, vector spaces, Lie algebras and the like, semi-lattices, and more: a majority of algebraic objects common to mathematical practice. (However, they also adopted a second, strongly limiting assumption.) In groups, for example, the ternary function $d(x, y, z) = xy^{-1}z$ represents the difference term available there; in general, it is rather a technical thing, and so we leave its definition to Appendix A. In Chapter 4, we further the understanding of the commutator in varieties of algebras possessing this ubiquitous term, building on the work of Smith (1976), Freese and McKenzie (1987), Lipparini (1994), and Kearnes (1995).

On the other hand, many algebras have been found with equational theories that are not finitely based. Indeed, the seemingly natural conjecture that perhaps all finite algebras have a finitely based equational theory was proved false early on by Roger Lyndon, when in 1954 he found a 7-element counterexample—not long after the appearance of his 1951 paper, in which he established that all 2-element algebras generate a finitely based variety. Murskiĭ (1965) later provided a 3-element algebra that generates a variety without a finite basis. Thus, the task has shifted to an attempt at characterizing those algebras that do boast a finitely based equational theory. Knowing these results of Lyndon, Tarski asked whether there is an algorithm for deciding, on the input of a finite algebra $\mathbf{A}$ of finite signature, whether $\mathbf{A}$ generates a finitely based variety. In (1996), Ralph McKenzie answered Tarski's longstanding question in the negative. Yet, this does not mean it is out of the question that something of mathematical interest can be said about the body of algebras with a finitely based equational theory. Building tools to tell us more is the purpose of this thesis.

While a certain strong assumption has been employed in the recent result of Kearnes, Szendrei, and Willard, (and those of their predecessors, which they have generalized) we have sought to try to understand further what can be said regarding the finite basis question without the luxury of their strong, secondary assumption (in brief, their secondary assumption entails the availability of a representation of any algebra in terms of a product of some of its *finite* quotients or residues, a very useful tool). We have pursued a line of research which is in some sense orthogonal to that result. Specifically, we have undertaken a further study of the methods first employed by Lyndon in his result concerning nilpotent groups and by Oates and Powell in their result, in order to resolve the open question of the extent to which Lyndon's result on nilpotent groups can be generalized—thus, pursuing knowledge of a class of algebras not well-covered by the recent result of Kearnes, Szendrei, and Willard, whose assumptions strongly limit the type of nilpotence possible in the algebras under their consideration: In fact, the only nilpotent algebras considered under their assumptions are abelian.

However, we are not the first to press with this line of inquiry. M.R. Vaughan-Lee (1983) and, subsequently, Ralph Freese (1987) were able to generalize a part of the result of Lyndon concerning nilpotent groups—that is, that part that concerns *finite*, nilpotent groups—with these latter researchers working under the auspices of a stronger assumption than the availability of a difference term, but one still weak enough to specialize to Lyndon's result in the group setting. Their assumptions are known to force a certain property on the set of congruences of each algebra under their consideration, namely that of *congruence permutability*. For an intuitive picture of what is meant by this, recall from group theory that a product can be imposed on the set of normal subgroups of a group $\mathbf{G}$ and, indeed, for any pair of normal subgroups $\mathbf{H}$ and $\mathbf{K}$ of $\mathbf{G}$, we have that $\mathbf{HK} = \mathbf{KH}$—that is, this product is commutative; furthermore, related computations demonstrate that whenever we have that $HK = G$ and $H \cap K$ is the trivial subgroup, $\mathbf{G}$ factors as the direct product of $\mathbf{H}$ and $\mathbf{K}$. Facts very much parallel hold in any variety of algebras each of which is congruence permutable, which we define now.

Observe that any binary relations, say R and S can be composed in a natural way; we let $R \circ S$ denote the set of all pairs $\langle x, z\rangle$ for which there is some y such that $x \mathrel{R} y \mathrel{S} z$—that is, so that x is R-related to y and y is R-related to z. To say that a given algebra $\mathbf{A}$ is congruence permutable means precisely that this composition operation permutes (or commutes) on the set of congruences of **A**—that is, so that for any congruences α and β on **A**, we have that $\alpha \circ \beta = \beta \circ \alpha$. This property is equivalent to the one just cited for groups—if translated in the appropriate way from the context of normal subgroups into that of congruences—but it also holds in rings, modules, Lie algebras, vector spaces, loops, quasigroups, and more. In fact, in 1954 Anatoli Mal'cev established that

> A variety $\mathcal{V}$ is congruence permutable if and only if there is a ternary term p supplied by the signature of $\mathcal{V}$ such that, for any algebra $\mathbf{A} \in \mathcal{V}$ and any $a, b \in A$, we have that $p(a, b, b) = a = p(b, b, a)$ (or, put another way, **A** *satisfies* the equations $p(x, y, y) \approx x \approx p(y, y, x)$.)

Such a term is called a *Mal'cev term*, and any variety the algebras of which are each congruence permutable we shall either call congruence permutable or *Mal'cev.* In particular, as we shall see, every Mal'cev term is a difference term. In fact, the example given above for the difference term in groups is also a Mal'cev term.

A more exotic and involved example of a Mal'cev term occurs in quasigroups. Recall first that quasigroups are endowed with three binary operations symbolized by $\cdot$, $/$, and $\backslash$ with which we may express the axioms of this class: $(x \cdot y)/y \approx x$, $(x/y) \cdot y \approx x$, $y\backslash(y \cdot x) \approx x$, and $y \cdot (y\backslash x) \approx x$. One can then check that the ternary term p defined in the signature of quasigroups by $p(x, y, z) \approx (x/(y\backslash y)) \cdot (y\backslash z)$ satisfies Mal'cev's equations, given in the display above.

In their finite basis result, Freese and Vaughan-Lee also assumed further a property that is got for free in the case of finite, nilpotent groups, but which is not a property of all nilpotent algebras: that of being representable as a direct product of algebras of prime power order. They found the following (which, however, can be stated more broadly; see Theorem 4.2).

Theorem 1.1. *Let* $\mathbf{A}$ *be a finite, nilpotent algebra with finitely many fundamental operations that generates a congruence permutable variety. Suppose also that* $\mathbf{A}$ *factors as the direct product of algebras of prime power order. Then* $\mathbf{A}$ *has a finitely based equational theory.*

We have been able to broaden this result. It turns out that, in a congruence permutable variety, the property of being nilpotent and a direct product of algebras of prime power cardinality is necessarily associated with the satisfaction of a set of equations. Algebras in a variety that satisfy one such set of equations—depending on the natural number parameter n—we shall call "supernilpotent of class n." We have been able to show the following.

Theorem 1.2. *Let* n *be a natural number. Let* $\mathcal{V}$ *be a locally finite, Mal'cev variety of finite signature consisting solely of algebras supernilpotent of class* n*. Then* $\mathcal{V}$ *has a finitely based equational theory.*

This comes as a trivial consequence of another new result we have been able to obtain: For any natural number n and any locally finite, Mal'cev variety $\mathcal{V}$ consisting solely of algebras of supernilpotence class n, we have that $\mathcal{V}$ is generated by a finite algebra. We have several other contributions to this relatively new study of the concept of supernilpotence, which we give in the next chapter.

We also have many results inspired by the techniques employed in the Oates-Powell proof. Our results add steam to the following open problem, which has been our primary focus.

Problem 1.3. Let $\mathbf{A}$ be a finite nilpotent algebra in a congruence permutable variety of finite signature. Is the variety generated by $\mathbf{A}$ finitely based?

We have pursued the strategy of the Oates-Powell proof and have generalized many of the incremental results feeding into their proof to the setting of our interest (and sometimes broader.) We hope that a few of the results (and questions raised) here concerning this topic may point the way to a solution of this problem.

It is convenient to briefly outline the strategy of the Oates and Powell proof, which is concerned primarily with the concept of critical groups. We have defined (somewhat novelly) a *critical algebra* to be any that is not found in the variety generated by its proper factors, where its *proper factors* are any subalgebra or homomorphic image thereof of cardinality strictly less than the original algebra (see the discussion preceding Theorem A.5 in the appendix). The Oates and Powell proof, then, exploits the fact that if $\mathcal{V}$ is any variety such that all of its finitely generated algebras are finite (a property which we shall refer to as *local finiteness*, moving forward), then $\mathcal{V}$ is generated by its critical algebras. Now, Birkhoff (1935) showed that if $\mathcal{V}$ is any locally finite variety of algebras each of which is endowed with only finitely many fundamental operations, and n is a natural number, then the set of equations that hold across $\mathcal{V}$ and that involve only terms in n or fewer variables has a finite basis (which he provided.)

For a given variety $\mathcal{V}$, let us denote by $\mathcal{V}^{(n)}$ the variety of algebras that satisfy the n-variable equations true in $\mathcal{V}$. It turns out that if for some natural number n we have that $\mathcal{V}^{(n)}$ is locally finite and has a finite bound on the size of its critical algebras, then the same must be true of $\mathcal{V}$. Oates and Powell make use of this along with the fact that if $\mathcal{V}$ is the variety generated by any finite group, then there are natural numbers n, e, m, and c such that $\mathcal{V}^{(n)}$ is locally finite and composed only of algebras of exponent e, the chief factors of which have cardinality at most m, and the nilpotent factors of which are of nilpotence class at most c. (A *chief factor* of a given group $\mathbf{G}$ is the factor group $\mathbf{H}/K$, where $\mathbf{H}$ and $\mathbf{K}$ are normal subgroups of $\mathbf{G}$ such that $K \leq H$ and so that $\mathbf{H}/K$ is minimal in $\mathbf{G}/K$.) They show, using these parameters, which hold across $\mathcal{V}$ but which can also be "lifted" to $\mathcal{V}^{(n)}$, that for high enough n, $\mathcal{V}^{(n)}$ has only finitely many non-isomorphic critical groups. We have sought to use a similar approach applied to Problem 1.3. In fact, we have been able to show the following.

Theorem 1.4. *If* $\mathbf{A}$ *is any nilpotent algebra of finite signature that generates a locally finite congruence permutable variety* $\mathcal{V}$*, then for high enough* n*,* $\mathcal{V}^{(n)}$ *is locally finite and has a bound on its chief factors, depending only on the nilpotence class of* $\mathbf{A}$*.*

By "chief factors" here, we mean something very much parallel to the group-theoretic definition given above, only concerning congruences rather than normal subgroups. (We have also employed what appears to be the natural generalization of the group-theoretic concept of "exponent" in our proofs.) We achieve this result by identifying a set v_n of equations for a fixed congruence modular[1] variety $\mathcal{V}$ that is satisfied in any algebra in $\mathcal{V}$ of cardinality strictly less than n lying in $\mathcal{V}$ and so that, conversely, if $\mathbf{A} \in \mathcal{V}$ satisfies v_n, then the annihilator of any chief factor of $\mathbf{A}$ is strictly less than n. (The annihilator of a chief factor can be defined in terms in the commutator of congruences.) Furthermore, the law v_n is satisfied by a nilpotent algebra in $\mathcal{V}$ if it is of a certain class depending on n. This result is a generalization of one that holds in groups, given as Theorem 52.32 in Neumann (1967), in whose work v_n is called the "chief centralizer law." Using it, we draw several results, giving new proofs of some older results as well as some apparently novel observations.

Now, Freese and McKenzie (1987) give a set Σ of equations that characterize nilpotence of a given class c within a given class $\mathcal{K}$ of algebras, with Σ turning out to be finite if, for instance, $\mathcal{K}$ is locally finite and of finite signature. For this reason, if $\mathbf{A}$ is again taken to be a nilpotent algebra that generates a congruence permutable variety $\mathcal{V}$, "lifting" the nilpotence class of $\mathbf{A}$ to $\mathcal{V}^{(n)}$, for high enough n, is not a problem. However, there are several good reasons for supposing that this

[1]Congruence modularity is defined in the appendix below in terms of the satisfaction of a certain implication (or, equivalently, a certain equation) on the congruence lattices of the algebras in a given variety.

may not supply sufficient data to establish, too, a finite bound on the size of the critical algebras of such a $\mathcal{V}^{(n)}$; rather, we suggest that, as a preliminary heuristic, replacing many of the occurrences of the concept of nilpotence in the Oates-Powell proof with that of supernilpotence may yield an affirmative solution to Problem 1.3. In the Oates-Powell proof, a key theorem provides a consequence of criticality in an arbitrary group, which has implications concerning the structure of certain of its nilpotent factors (we have in mind here Theorem 51.37 from Neumann (1967).) We have found what seems to be a natural generalization of this result, but it concerns instead the notion of supernilpotence. On the other hand, in group theory, nilpotence and supernilpotence coincide. Indeed, it has been established via Aichinger and Mudrinski (2010) and Kearnes (1999) that a given nilpotent algebra in a congruence permutable variety is supernilpotent if and only if it is the direct product of algebras of prime power order, which, as is well known, characterizes nilpotence in the group setting. Furthermore, one can observe in the proof of the Oates-Powell result that this feature of nilpotent groups—that is, that each such is the direct product of its Sylow subgroups—appears to play an apparently indispensable role in their analysis. For this reasons, we suggest further study of the concept of supernilpotence, supplemented by the results of Aichinger and Mudrinski (2010), Kearnes (1999), and what we have been able to establish below may finish the work started here in answering Problem 1.3. In particular, we ask whether some fragments of Sylow theory might extend to quasigroups with operators; work in this direction seems to very new, judging by a recent, relevant paper of Smith (2015), but which may have some useful antecedents and groundwork provided in Kearnes (1999) and others.

Taken as a whole, this thesis can be viewed as a collection of new results in the study of the commutator, nilpotence, and related phenomena in algebras of a fairly general nature. In Chapter 2, we define the higher commutator of Bulatov (2001), via which the concept of supernilpotence is defined. Then, building on the work of Aichinger and Mudrinski (2010) and the very insightful contributions of Opršal (2014+), we establish the results concerning supernilpotence in congruence permutable varieties mentioned above, while, on the way, noting some new results concerning the higher commutator and, employing a slightly modified perspective relative to Opršal's, some new proofs of existing results, which we hope only continue the useful simplifications of Aichinger and Mudrinski's theorems offered by Opršal. We would like to note here, however, that the work we pursued concerning supernilpotence was driven out of a desire to generalize Theorem 51.37, Lemma 33.44, and Lemma 33.37 in Neumann (1967). Indeed, where certain of our results (especially Theorem 2.24) can be viewed as a gloss on Opršal (2014+) they can also be viewed as a close generalization of some work of Graham Higman, as presented in Neumann (1967), p. 88 (especially Lemma 33.44).

In Chapter 3, in addition to establishing Theorem 1.4 and some of its interesting consequences (as well as generalizing other of the results relevant to the Oates-Powell result, as presented in Neumann (1967)) we conduct further analysis of a Frattini congruence, given first by Kiss and Vovsi (1995), while introducing another, as well, which together seem to lend further legitimacy to the claim that such generalizes the group-theoretic concept of Frattini subalgebra. We conclude that chapter by offering a handful of relatively narrow questions the resolution of any of which would resolve Problem 1.3.

In Chapter 4, we publicize an apparently known fact which seems to have mostly been consigned to the folkloric background of the field: that any solvable algebra in a variety with a difference term—and, indeed, with a so-called "weak difference term"—generates a congruence permutable variety. Thus, the result of Freese and Vaughan-Lee, given above as Theorem 1.1, can be more strongly stated (owing also to the fact that nilpotence entails solvability). However, in Chapter 4, we also undertake a novel study of this fact, revealing it to be the consequence of a new "homomorphism" property of the commutator in varieties with a difference term, which we argue might be as sharp a result as can be expected. We obtain this property by first noting two other new results that may be of independent interest: We offer a new (apparently sharp) order-theoretic property of the commutator in difference term varieties and a new result concerning affine behavior in varieties with a difference term. This latter result also enables us to show that the same set of equations given by Freese and McKenzie to characterize nilpotence of fixed class in congruence modular varieties holds also in varieties with a difference term. We do this by newly demonstrating that the natural generalization of nilpotence with reference to the "upward central series" from group theory is equivalent to nilpotence as traditionally defined, provided one is working in a variety with a difference term. (That this last result holds in congruence modular varieties is implicitly given in Freese and McKenzie (1987), but, apparently, has not been previously noted to hold under the weaker assumption of the presence of a difference term.)

We conclude with a selection of questions and problems generated in the course of producing the work in this thesis. We also offer in the appendix a fairly comprehensive presentation of the background material necessary to digest the work to which we now turn.

Chapter 2

On centralizers and commutators of higher order

The following concerns the "higher centralizer" and commutator and the accompanying notion of supernilpotence, concepts first developed by Bulatov (2001), later applied by Aichinger and Mudrinski (2010), and simplified by Opršal (2014+).[1] Building on the work of these authors as well as that of Ralph Freese (1987) and Vaughan-Lee (1983) we obtain a broadening of the finite basis result of Freese and Vaughan-Lee, which shall be given below as Theorem 2.30. In the process, we derive a few other overlooked (or previously unneeded) results concerning the higher centralizer, commutator, and supernilpotence. Furthermore, the technology we develop also lends itself to establishing a "finiteness condition" for critical algebras resembling one got through techniques of Graham Higman (when he supplied a second proof of Lyndon's finite basis result for nilpotent groups) and which is key in the proof of the Oates-Powell result. (It is our hope that this finiteness condition may find a role in an Oates-Powell-style proof of a finite basis result for finite, nilpotent algebras.) We also point out that results concerning supernilpotence lend themselves to a very exact generalization of Higman's Lemma, as given in Neumann (1967) as Corollary 33.44.

Building on the work of Opršal, we are able to give simpler proofs for the results we shall require from Aichinger and Mudrinski, making this exposition fairly independent of these latter researchers (but very close to that of Opršal.)

[1]Thank you to Jakub Opršal, who was game for my bouncing various ideas off of him this spring regarding his December 2014 submission to ArXiv.org.

We begin with the definition of the "higher centralizer" given by Bulatov and others. (See Aichinger and Mudrinski (2010), Definition 3.1.) Below, for a given binary relation R over set A and any natural number ℓ, we shall use R^ℓ to denote $\{\langle \mathbf{a}, \mathbf{b}\rangle \in A^\ell \times A^\ell \mid \mathbf{a}(i) \, R \, \mathbf{b}(i)\}$.

Definition 2.1. For any algebra $\mathbf{A}$ and congruences $\theta_0, \ldots, \theta_{n-1}, \gamma$ on $\mathbf{A}$, we define an $(n+1)$-ary relation on $\operatorname{Con} \mathbf{A}$, denoted by $C^n(\theta_0, \ldots, \theta_{n-1}; \gamma)$. We say that this relation is satisfied by $\theta_0, \ldots, \theta_{n-1}; \gamma$ according to the following conditions.

Let $\ell_0, \ldots, \ell_{n-1}$ be natural numbers. For each $i < n$, let $\langle \mathbf{a}_i, \mathbf{b}_i \rangle \in \theta_i^{\ell_i}$. Let t be a term operation (or, without loss of generality, polynomial) for $\mathbf{A}$ of rank $\sum_{i<n} \ell_i$. Then whenever

$$t(\mathbf{x}_0, \ldots, \mathbf{x}_{n-2}, \mathbf{a}_{n-1}) \, \gamma \, t(\mathbf{x}_0, \ldots, \mathbf{x}_{n-2}, \mathbf{b}_{n-1}),$$

for all choices of

$$\langle \mathbf{x}_0, \ldots, \mathbf{x}_{n-2} \rangle \in \{\mathbf{a}_0, \mathbf{b}_0\} \times \cdots \times \{\mathbf{a}_{n-2}, \mathbf{b}_{n-2}\} \setminus \{\langle \mathbf{b}_0, \ldots, \mathbf{b}_{n-2} \rangle\},$$

we must also have that

$$t(\mathbf{b}_0, \ldots, \mathbf{b}_{n-2}, \mathbf{b}_{n-1}) \, \gamma \, t(\mathbf{b}_0, \ldots, \mathbf{b}_{n-2}, \mathbf{b}_{n-1}).$$

Let us call this the *n-rank term condition.* We shall usually drop the superscript $({}^n)$ decorating its symbol, but its availability is sometimes convenient.

Proposition 2.2. *Let n be a natural number. Let $\mathbf{A}$ be any algebra. Let $\theta_0, \ldots, \theta_{n-1}, \gamma$ be congruences of $\mathbf{A}$. Let σ be any permutation of the set $\{0, \ldots, n-2\}$. Then $C(\theta_0, \ldots, \theta_{n-1}; \gamma)$ holds if and only if $C(\theta_{\sigma(0)}, \ldots, \theta_{\sigma(n-2)}, \theta_{n-1}; \gamma)$ holds.*

Proof. This is evident from the definition above, using also the fact that any term algebra is closed under permutations of its variables. $\square$

It is convenient to frame the rank-n term condition in some other ways as well. But, to do so, we need to build some notation for the manipulation of natural number indices.

For any natural number n, let β_n be the binary ω-tuple associated with the binary expansion of n. That is, for example, we have $\beta_5 = \langle 1, 0, 1, 0, 0, \ldots \rangle$, while $\beta_8 = \langle 0, 0, 1, 0, \ldots \rangle$. Let $\mathbb{B}$ be the set of all β_n, for $n \in \omega$. Let $\underline{2} = \{0, 1\}$. We endow $\underline{2}$ with the boolean operations, a join, meet, and complement, plus the usual binary addition, denoting them, respectively, $\vee$, $\wedge$, $'$, and $\oplus$. Write $\underline{\mathbf{2}} = \langle \underline{2}, \wedge, \vee, ', \oplus \rangle$. Note that $\mathbb{B}$ is a subset of $\underline{2}^\omega$ and, furthermore, that it is closed under the operations just provided.

Now, we let ω inherit the operations on $\mathbb{B}$ via the bijection $\beta : \omega \to \mathbb{B}$ defined by $\beta(n) = \beta_n$. For instance, for any $n, m \in \omega$, we set $n \vee m = \beta^{-1} (\beta_n \vee \beta_m)$. By way of example and using an abbreviated form, note that $\beta_3 = \langle 1, 1, 0 \rangle$ and $\beta_5 = \langle 1, 0, 1 \rangle$, and so we have that

$$3 \vee 5 = \beta^{-1} \langle 1, 1, 1 \rangle = 7,$$

$$3 \wedge 5 = \beta^{-1} \langle 1, 0, 0 \rangle = 1, \text{ and}$$

$$3 \oplus 5 = \beta^{-1} \langle 0, 1, 1 \rangle = 6.$$

For any power indexed by ω, say $P = S^\omega$, for a given set S, we use the structure given to ω above to define three classes of useful maps on P. Let $r \in \omega$ and $f \in P$. We set

$$\rho_r^P f = \rho_r^P \langle f(n) \mid n \in \omega \rangle = \langle f(n \vee r) \mid n \in \omega \rangle;$$

we let

$$\varepsilon_r^P f = \langle f(n \wedge r) \mid n \in \omega \rangle;$$

and we set

$$\pi_r^P f = \langle f(n \oplus r) \mid n \in \omega \rangle.$$

Of course, it is also possible to define these sorts of maps on a given set—rather than a direct power—indexed by ω; we shall do so below for the standard set of variables. Furthermore, for any natural number n and any direct power P indexed by n, we can define a similar set of maps for P.

The following is clear from the nature of the operations for $\underline{2}^{\omega}$.

Proposition 2.3. *Let n be a natural number. Let P be any power indexed by 2^n. The sets $\{\rho_r^P \mid r < 2^n\}$ and $\{\pi_r^P \mid r < 2^n\}$ are generated by maps of the form ρ_r^P and π_r^P, respectively, where $r < 2^n$ and $\beta_r(i) = 1$ for at most one $i \in \omega$—that is, so that $r = 2^j$ for some $j < n$. The set $\{\varepsilon_r^P \mid r < 2^n\}$ is generated by maps of the form ε_r^P with $r < 2^n$ and $\beta_r(i) = 0$ for at most one $i \in \omega$— that is, so that $r = 2^n - 1 - 2^j$ for some $j < n$.*

Definition 2.4. Let $\mathbf{A}$ be an algebra, and let n be a natural number. Let $\theta_0, \ldots, \theta_{n-1}$ be congruences on $\mathbf{A}$. For $n > 0$, we let $P(\theta_0, \ldots, \theta_{n-1})$ be the set of all 2^n-tuples, $\mathbf{a}$, of the form

$$\mathbf{a} = \langle \langle a, b \rangle (\beta_r(i)) \mid r < 2^n \rangle,$$

such that $i < n$ and $\langle a, b \rangle \in \theta_i$. (Note that $\langle a, b \rangle(0) = a$, while $\langle a, b \rangle(1) = b$.) Now, let $\mathbf{Q}(\theta_0, \ldots, \theta_{n-1})$ be the subalgebra of $\mathbf{A}^{2^n}$ generated by $P(\theta_0, \ldots, \theta_{n-1})$. Also, for any $\mathbf{e} \in Q(\theta_0, \ldots, \theta_{n-1})$, write $\mathbf{e}^\circ$ for its projection onto its first $2^n - 1$ coordinates; similarly, let $\mathbf{Q}^\circ(\theta_0, \ldots, \theta_{n-1})$ be the projection of $\mathbf{Q}(\theta_0, \ldots, \theta_{n-1})$ onto its first $2^n - 1$ coordinates.[2]

It is helpful to view an example of a P and Q. Let $\mathbf{A}$ be an algebra with congruences $\theta_0, \theta_1, \theta_2$. Let $\langle a_i, b_i \rangle \in \theta_i$, for each $i < 3$. Typical elements of $P(\theta_0, \theta_1, \theta_2)$ are

$$\mathbf{a}_0 = \langle a_0, b_0, a_0, b_0, a_0, b_0, a_0, b_0 \rangle,$$

$$\mathbf{a}_1 = \langle a_1, a_1, b_1, b_1, a_1, a_1, b_1, b_1 \rangle, \text{ and}$$

$$\mathbf{a}_2 = \langle a_2, a_2, a_2, a_2, b_2, b_2, b_2, b_2 \rangle.$$

[2] $\mathbf{Q}(\theta_0, \ldots, \theta_{n-1})$ is defined also in Opršal; however, it is called $\mathbf{\Delta}(\theta_0, \ldots, \theta_{n-1})$, there. See Definition 3.1 in Opršal (2014+).

Let t be a ternary term operation for $\mathbf{A}$; consider

$$t(\mathbf{a}_0, \mathbf{a}_1, \mathbf{a}_2) = \langle t(a_0, a_1, a_2), t(b_0, a_0, a_2), t(a_0, b_1, a_2), t(b_0, b_1, a_2)$$
$$t(a_0, a_1, b_2), t(b_0, a_1, b_2), t(a_0, b_1, b_2), t(b_0, b_1, b_2)\rangle$$

as an illustrative example of an element of $Q(\theta_0, \theta_1, \theta_2)$.

The following is evident from the definitions, together with Proposition 2.2. (See also Lemmas 3.2 and 3.3 from Opršal (2014+).)

Proposition 2.5. *Let $\mathbf{A}$ be an algebra with congruences $\theta_0, \ldots, \theta_{n-1}$. Then*

$$C(\theta_0, \ldots, \theta_{n-1}; \gamma)$$

holds if and only if for all $\mathbf{e} \in Q(\theta_0, \ldots, \theta_{n-1})$, for all $i < 2^{n-1}$, whenever, for each $j < 2^{n-1}$ with $j \neq i$, we have that $\mathbf{e}(j) \,\gamma\, \mathbf{e}(j + 2^{n-1})$, then we must have that $\mathbf{e}(i) \,\gamma\, \mathbf{e}(i + 2^{n-1})$, as well.

Remark 2.6. For any natural number n, let ν_n be the natural projection of $\mathbf{B} \leq \mathbf{A}^{2^n}$ onto $\mathbf{A}^{2^{n-1}} \times \mathbf{A}^{2^{n-1}}$. It is not difficult to show that for $\mathbf{A} \in \mathcal{V}$, Mal'cev, for any natural number n, and any $\theta_0, \ldots, \theta_{n-1} \in \operatorname{Con} \mathbf{A}$, $\Delta(\theta_0, \ldots, \theta_{n-1}) := \nu_n Q(\theta_0, \ldots, \theta_{n-1})$ is a congruence on $\mathbf{Q}(\theta_0, \ldots, \theta_{n-2})$; in fact, it turns out to be the least congruence on $\mathbf{Q}(\theta_0, \ldots, \theta_{n-2})$ to include the pairs $\nu_n\langle\langle a, b\rangle(\beta_r(n-1)) \mid r < 2^n\rangle$ such that $a \,\theta_{n-1}\, b$. In particular, $\Delta(\theta_0, \theta_1) = \Delta_{\theta_0}^{\theta_1}$ as given in Definition A.36. See Lemma 3.4, from Opršal (2014+), for a related observation.

Proposition 2.7. *Let n be a natural number. For any algebra $\mathbf{A}$ with congruences $\theta_0, \ldots, \theta_{n-1}$ and for all $r < 2^n$, we have that $Q := Q(\theta_0, \ldots, \theta_{n-1})$, is closed under $\rho_r^{A^{2^n}}$, $\varepsilon_r^{A^{2^n}}$, and $\pi_r^{A^{2^n}}$.*

Proof. Let $r < 2^n$. Write $\rho_r = \rho_r^{A^{2^n}}$, $\varepsilon_r = \varepsilon_r^{A^{2^n}}$, and $\pi_r = \pi_r^{A^{2^n}}$. Let $\mathbf{a} \in Q$. Then, for some term t of rank, say r, and tuples $\mathbf{a}_0, \ldots, \mathbf{a}_{r-1} \in P$,

$$\mathbf{a} = \langle t^{\mathbf{A}}(\mathbf{a}_0(s), \ldots, \mathbf{a}_{r-1}(s)) \mid s < 2^n\rangle.$$

Thus, we have that $\rho_r \mathbf{a} = \langle t^{\mathbf{A}}(\mathbf{a}_0(s \vee r), \ldots, \mathbf{a}_{r-1}(s \vee r)) \mid s < 2^n \rangle$ (and similarly for ε_r or π_r substituted for ρ_r). Thus, it is apparent that we need only show that $P := P(\theta_0, \ldots, \theta_{n-1})$ is closed under ρ_r, ε_r, and π_r. To show that P is closed under ρ_r, by Proposition 2.3, we need only show the case of $r = 2^i$ for some $i < n$. So, suppose $\mathbf{a} \in P$. Let $\langle a, b\rangle \in \theta_j$, for some $j < n$, witness this; that is, suppose that $\mathbf{a} = \langle \langle a, b\rangle(\beta_s(j)) \mid s < 2^n\rangle$. Then $\rho_{2^i}\mathbf{a} = \langle \langle a, b\rangle(\beta_{s \vee 2^i}(j)) \mid s < 2^n\rangle$. Now, note that if $j \neq i$, then for any $s < 2^n$, $\beta_{s\vee 2^i}(j) = \beta_s(j)$. On the other hand, for any $s < 2^n$, we have that $\beta_{s \vee 2^i}(i) = 1$. Thus, ρ_{2^i} either leaves $\mathbf{a}$ unchanged or maps it to the constantly-b tuple. In either case, $\rho_{2^i}\mathbf{a} \in P$, and thus, Q is closed under ρ_r.

That P is closed under ε_r involves a similar demonstration, and so we omit it. We now show that P is closed under π_r. Using the same $\mathbf{a}$ from above, we shall show that $\pi_r \mathbf{a} \in P$. Again, by Proposition 2.3, it is sufficient to show the case of $r = 2^i$ for some $i < n$. We consider by cases. First suppose that $j \neq i$. Then we have that, for any $s < 2^n - 1$, $\beta_{s \oplus 2^i}(j) = \beta_s(j)$. Thus, in this case, $\pi_r\mathbf{a} = \mathbf{a}$. On the other hand, we have that

$$\beta_{s\oplus 2^i}(i) = \begin{cases} 0 & \text{if } \beta_s(i) = 1 \\ 1 & \text{if } \beta_s(i) = 0. \end{cases}$$

It follows that

$$\begin{aligned} \pi_r \mathbf{a} &= \pi_r \langle \langle a, b\rangle(\beta_s(i)) \mid s < 2^n - 1\rangle \\ &= \langle \langle a, b\rangle(\beta_{s \oplus r}(i)) \mid s < 2^n - 1\rangle \\ &= \langle \langle b, a\rangle(\beta_s(i)) \mid s < 2^n - 1\rangle. \end{aligned}$$

From this it is clear that $P(\theta_0, \ldots, \theta_{n-1})$ is closed under π_r. □

The following is (nominally) new. I considered this first as a way to generalize Theorem 51.37 from Neumann (1967). However, it is essentially the same as Opršal's "fork-description" of Bulatov's higher centralizer, as given by Opršal (2014+), Proposition 3.6.

Definition 2.8. For any algebra $\mathbf{A}$ and congruences $\theta_0, \ldots, \theta_{n-1}, \gamma$ on $\mathbf{A}$, we define an $(n+1)$-ary relation on $\operatorname{Con}\mathbf{A}$, denoted by $C_2^n(\theta_0, \ldots, \theta_{n-1}; \gamma)$. We say that this relation is satisfied by $\theta_0, \ldots, \theta_{n-1}; \gamma$ whenever given n pairs of tuples (of any length ℓ_i), such that $\langle \mathbf{a}_i, \mathbf{b}_i \rangle \in \theta_i^{\ell_i}$ and given term operations (or, without loss of generality, polynomials) t and s over $\mathbf{A}$ of appropriate rank, if $s(\mathbf{x}_0, \ldots, \mathbf{x}_{n-1}) \,\gamma\, t(\mathbf{x}_0, \ldots, \mathbf{x}_{n-1})$, for all choices of

$$\langle \mathbf{x}_0, \ldots, \mathbf{x}_{n-1} \rangle \in \{\mathbf{a}_0, \mathbf{b}_0\} \times \cdots \times \{\mathbf{a}_{n-1}, \mathbf{b}_{n-1}\} \setminus \{\langle \mathbf{b}_0, \ldots, \mathbf{b}_{n-1} \rangle\},$$

then we must also have that $s(\mathbf{b}_0, \ldots, \mathbf{b}_{n-1}) \,\gamma\, t(\mathbf{b}_0, \ldots, \mathbf{b}_{n-1})$. Let us call this the *n-rank two-term condition.* Again, we will most often drop the superscript $({}^n)$ in its notation.

Proposition 2.9. *Let n be any natural number, and let σ be a permutation of $\{0, \ldots, n{-}1\}$. Let $\mathbf{A}$ be an algebra. Let $\theta_0, \ldots, \theta_{n-1}, \gamma \operatorname{Con}\mathbf{A}$. Then $C_2(\theta_0, \ldots, \theta_{n-1}; \gamma)$ holds if and only if $C_2(\theta_{\sigma(0)}, \ldots, \theta_{\sigma(n-1)}; \gamma)$ holds.*

Proof. This is clear from the definition of C_2^n above and the fact that, the set of terms given by any signature is closed under permutations of the variables. $\square$

The following is also not difficult to see from the definitions.

Proposition 2.10. *Let n be a natural number. Let $\mathbf{A}$ be an algebra with congruences $\theta_0, \ldots, \theta_{n-1}, \gamma$. Then $C_2(\theta_0, \ldots, \theta_{n-1}; \gamma)$ holds if and only if for natural numbers r, for all rank-r terms t and s given by the signature of $\mathbf{A}$, and for all $\mathbf{a}_0, \ldots, \mathbf{a}_{r-1} \in P(\theta_0, \ldots, \theta_{n-1})$, we have that*

$$s^{\mathbf{Q}^\circ}(\mathbf{a}_0^\circ, \ldots, \mathbf{a}_{r-1}^\circ) \,\gamma^{2^n-1}\, t^{\mathbf{Q}^\circ}(\mathbf{a}_0^\circ, \ldots, \mathbf{a}_{r-1}^\circ)$$

implies

$$s^{\mathbf{A}}(\mathbf{a}_0(2^n-1), \ldots, \mathbf{a}_{r-1}(2^n-1)) \,\gamma\, t^{\mathbf{A}}(\mathbf{a}_0(2^n-1), \ldots, \mathbf{a}_{r-1}(2^n-1)).$$

Recall that a quasiequation ϕ is any first order formula of the form

$$\phi = \epsilon_0 \wedge \cdots \wedge \epsilon_{r-1} \to \epsilon_r,$$

where r is a natural number and, for each $i < r$, ϵ_i is an equation. It is well known that (universal) satisfaction of quasiequations is preserved under the formation of subalgebras and products.

Proposition 2.11. *Let n be a natural number. Let $\mathbf{A}$ be any algebra. Then there is a set Σ of (universally quantified) quasiequations such that $C^n(1_A, \ldots, 1_A; 0_A)$ holds if and only if $\mathbf{A} \models \Sigma$. Similarly, there is a set Σ_2 of quasiequations such that $C_2^n(1_A, \ldots, 1_A; 0_A)$ holds if and only if $\mathbf{A} \models \Sigma_2$.*

Proof. We will show the second claim, with the first being similar. We let Σ_2 be the set of all quasiequations ϕ of the form

$$\phi = \epsilon_0 \wedge \cdots \wedge \epsilon_{2^n-2} \to \epsilon_{2^n-1},$$

where, for each $r < 2^n$,

$$\epsilon_r = \delta_r t(\mathbf{x}_0, \ldots, \mathbf{x}_{n-1}) \approx \delta_r s(\mathbf{x}_0, \ldots, \mathbf{x}_{n-1}),$$

where t, s are any terms in the pairwise distinct tuples $\mathbf{x}_0, \ldots, \mathbf{x}_{n-1}$, of pairwise distinct variables, and δ_r is a substitution sending, for each $i < n$,

$$\mathbf{x}_i \mapsto \begin{cases} \mathbf{z}_i & \text{if } \beta_r(i) = 0 \\ \mathbf{x}_i & \text{otherwise} \end{cases},$$

with $\mathbf{z}_0, \ldots, \mathbf{z}_{n-1}$ another list of pairwise distinct tuples of pairwise distinct variables, each of which is assumed also not to appear as a variable in $\mathbf{x}_i$ for any $i < n$. That Σ_2 has the desired property is immediate from Definition 2.8. $\square$

The following is easy, but—apparently—new. See also Proposition 3.6 in Opršal (2014+) for a special case of this.

Proposition 2.12. *Let* $\mathbf{A}$ *be any algebra. Let* $\theta_0, \dots, \theta_{n-1}$*, and* γ *be congruences on* $\mathbf{A}$*. Then* $C_2(\theta_0, \dots, \theta_{n-1}; \gamma) \Rightarrow C(\theta_0, \dots, \theta_{n-1}; \gamma)$*.*

Proof. Assume that $C(\theta_0, \dots, \theta_{n-1}; \gamma)$ holds. Let t be any term operation for $\mathbf{A}$ of rank, say r. Let $\ell_0, \dots, \ell_{r-1}$ be natural numbers so that $\sum \ell_i = r$. For each for $i < n$, take pairs $\langle \mathbf{a}_i, \mathbf{b}_i \rangle \in \theta_i^{\ell_i}$. Suppose that

$$t(\mathbf{x}_0, \dots, \mathbf{x}_{n-1}, \mathbf{a}_{n-1}) \,\gamma\, t(\mathbf{x}_0, \dots, \mathbf{x}_{n-1}, \mathbf{b}_{n-1}),$$

for all $\mathbf{x}_0, \dots, \mathbf{x}_{n-2}$ with $\mathbf{x}_i \in \{\mathbf{a}_i, \mathbf{b}_i\}$ and $\mathbf{x}_i = \mathbf{a}_i$ for at least one $i < n-1$. We need to show that

$$t(\mathbf{b}_0, \dots, \mathbf{b}_{n-2}, \mathbf{a}_{n-1}) \,\gamma\, t(\mathbf{b}_0, \dots, \mathbf{b}_{n-2}, \mathbf{b}_{n-1}).$$

Set $L(\mathbf{x}_0, \dots, \mathbf{x}_{n-1}) := t(\mathbf{x}_0, \dots, \mathbf{x}_{n-2}, \mathbf{a}_{n-1})$ and $R := t$.

Observe that if $\mathbf{x}_{n-1} = \mathbf{a}_{n-1}$, then

$$\begin{aligned} L(\mathbf{x}_0, \dots, \mathbf{x}_{n-1}) &= t(\mathbf{x}_0, \dots, \mathbf{x}_{n-2}, \mathbf{a}_{n-1}) \\ &= R(\mathbf{x}_0, \dots, \mathbf{x}_{n-1}). \end{aligned}$$

On the other hand, if $\mathbf{x}_{n-1} = \mathbf{b}_{n-1}$ but $\mathbf{x}_i = \mathbf{a}_i$ for some $i < n-1$, then, by assumption,

$$\begin{aligned} L(\mathbf{x}_0, \dots, \mathbf{x}_{n-1}) &= t(\mathbf{x}_0, \dots, \mathbf{x}_{n-2}, \mathbf{a}_{n-1}) \\ &\gamma\, t(\mathbf{x}_0, \dots, \mathbf{x}_{n-2}, \mathbf{b}_{n-1}) \\ &= R(\mathbf{x}_0, \dots, \mathbf{x}_{n-1}). \end{aligned}$$

Thus, we see that whenever $\mathbf{x}_i \in \{\mathbf{a}_i, \mathbf{b}_i\}$ for each $i < n$ such that $\mathbf{x}_i = \mathbf{a}_i$ for at least one $i < n$, we get that $L(\mathbf{x}_0, \dots, \mathbf{x}_{n-1}) \,\gamma\, R(\mathbf{x}_0, \dots, \mathbf{x}_{n-1})$. By $C_2(\theta_0, \dots, \theta_{n-1}; \gamma)$, then, we may conclude that

$$\begin{aligned} t(\mathbf{b}_0, \dots, \mathbf{b}_{n-2}, \mathbf{a}_{n-1}) &= L(\mathbf{b}_0, \dots, \mathbf{b}_{n-1}) \\ &\gamma\, R(\mathbf{b}_0, \dots, \mathbf{b}_{n-1}) \\ &= t(\mathbf{b}_0, \dots, \mathbf{b}_{n-1}), \end{aligned}$$

as we wished. □

Proposition 2.13. *Let n be a natural number. Let $\mathcal{V}$ be a variety so that for any $\mathbf{A} \in \mathcal{V}$, $C_2^n(1_A, \ldots, 1_A; 0_A)$ holds. Then, for any critical algebra $\mathbf{C} \in \mathcal{V}$, we have that $|C| \leq |F_{\mathcal{V}}(n)|$. In particular, if $F_{\mathcal{V}}(n)$ is finite, then $\mathcal{V}$ has a finite critical bound.*

Proof. Let $\mathbf{C}$ be a critical algebra in $\mathcal{V}$. Then there is an equation $t \approx s$ in the language of $\mathcal{V}$ that fails to hold in $\mathbf{C}$ but that holds in all proper factors of $\mathbf{C}$. Since any witness of the failure of $t \approx s$ in $\mathbf{C}$ involves finitely many elements of C, we can find a $t \approx s$ with a minimal such failure. Suppose that $t \approx s$ has a minimal witness to its failure, say $\mathbf{a} = \langle a_0, \ldots, a_{k-1} \rangle$. We claim that $k \leq n$. Suppose instead that $k > n$. For each $r < 2^n$, let δ_r be a substitution including, for each $i < n$,

$$\delta x_i = \begin{cases} x_n & \text{if } \beta_r(i) = 0 \text{ and } i < n \\ x_i & \text{otherwise.} \end{cases}$$

Then, by the minimality of k, we have that, for all $r < 2^n - 1$,

$$\delta_r t^{\mathbf{C}}(x_0, \ldots, x_{k-1})[\mathbf{a}] = \delta_r s^{\mathbf{C}}(x_0, \ldots, x_{k-1})[\mathbf{a}] :$$

after all, each of these equations involves at most $k-1$ variables. On the other hand, since $C_2^n(1_C, \ldots, 1_C; 0_C)$ holds, we may conclude that

$$t^{\mathbf{C}}(a_0, \ldots, a_{k-1}) = s^{\mathbf{C}}(a_0, \ldots, a_{k-1}),$$

contrary to our assumptions. Thus, the claim is good. It follows that all critical algebras in $\mathcal{V}$ are at most n-generated, and hence for critical $\mathbf{C} \in \mathcal{V}$, we get the bound $|C| \leq |F_{\mathcal{V}}(n)|$. $\square$

2.1 On cube terms and strong cube terms

The following definition is adapted from Berman, Idziak, Marković, McKenzie, Valeriote, and Willard (2010); see their Definition 2.5.

Suppose that $\mathbf{A}$ is in a variety with a term q of rank $2^n - 1$ and for which the equation

$$q(\langle z, x\rangle(\beta_j(i)) \mid j < 2^n - 1) \approx x, \tag{2.1}$$

holds for every $i < n$. (Note that this implies that q is idempotent.) Thus, for $\mathbf{e} = \langle\langle a, b\rangle(\beta_j(i)) \mid j < 2^n\rangle \in P$, $q^{\mathbf{A}}(\mathbf{e}^\circ) = b$. Consider the example of $n = 3$. We shall call a q of this form an *n-cube term*, following Berman, Idziak, Marković, McKenzie, Valeriote, and Willard (2010). Consider the case of $n = 3$; a 3-cube term q satisfies the equations

$$q(z, x, z, x, z, x, z) \approx x$$

$$q(z, z, x, x, z, z, x) \approx x, \text{ and}$$

$$q(z, z, z, z, x, x, x) \approx x.$$

Lemma 2.14. *Let n be a natural number. Let $\mathbf{A}$ be an algebra in a variety with n-cube term, q. Let $\theta_0, \ldots, \theta_{n-1}, \gamma$ be congruences on $\mathbf{A}$. Let η be the natural quotient map of $\mathbf{A}$ onto $\mathbf{A}/\gamma$. Write $Q = Q(\theta_0, \ldots, \theta_{n-1})$. Then $\eta \circ q^{\mathbf{A}} : Q^\circ \to A/\gamma$ is a homomorphism if and only if, for any $\mathbf{e} \in Q$, $q^{\mathbf{A}}(\mathbf{e}^\circ)\ \gamma\ \mathbf{e}(2^n - 1)$.*

Proof. First, suppose that $\eta \circ q^{\mathbf{A}} : Q^\circ \to A/\gamma$ is a homomorphism. Let $\mathbf{e} \in Q$. Then we can write $\mathbf{e} = t^{\mathbf{Q}}(\mathbf{a}_0, \ldots, \mathbf{a}_{r-1})$ for some term t of whatever rank s and for $\mathbf{a}_0, \ldots, \mathbf{a}_{s-1} \in P$. We need to show that $\eta \circ q^{\mathbf{A}}(\mathbf{e}^\circ) = \eta(\mathbf{e}(2^n - 1))$. We show by inducting on the complexity of t. The basis step is done by noting first that if t is a projection or a constant function, then $\mathbf{e} \in P$: In this case, we have that $q^{\mathbf{A}}(\mathbf{e}(0), \ldots, \mathbf{e}(2^n - 2)) = \mathbf{e}(2^n - 1)$, owing simply to the fact that the n-cube equations hold for q.

Now, for the inductive step, write

$$\mathbf{e} = f^{\mathbf{Q}}(t_0^{\mathbf{Q}}(\mathbf{a}_0, \ldots, \mathbf{a}_{s-1}), \ldots, t_{r-1}^{\mathbf{Q}}(\mathbf{a}_0, \ldots, \mathbf{a}_{s-1})),$$

where f is some fundamental operation symbol of rank r and t_i is a term for each $i < s$. Write $\mathbf{e}_i = t_i^{\mathbf{Q}}(\mathbf{a}_0, \ldots, \mathbf{a}_{s-1})$ for each $i < s$. Then, by (the standard) inductive hypothesis and since $\eta \circ q^{\mathbf{A}}$ restricted to $\mathbf{Q}^{\circ}$ is a homomorphism,

$$\begin{aligned}
\eta \circ q^{\mathbf{A}}(\mathbf{e}^{\circ}) &= \eta \circ q^{\mathbf{A}}(f^{\mathbf{Q}^{\circ}}(\mathbf{e}_0^{\circ}, \ldots, \mathbf{e}_{r-1}^{\circ})) \\
&= f^{\mathbf{A}/\gamma}(\eta \circ q^{\mathbf{A}}(\mathbf{e}_0^{\circ}), \ldots, \eta \circ q^{\mathbf{A}}(\mathbf{e}_{r-1}^{\circ})) \\
&= f^{\mathbf{A}/\gamma}(\eta(\mathbf{e}_0^{\circ}(2^n - 1)), \ldots, \eta(\mathbf{e}_{r-1}^{\circ}(2^n - 1))) \\
&= \eta\Big(f^{\mathbf{A}}(\mathbf{e}_0^{\circ}(2^n - 1)), \ldots, \mathbf{e}_{r-1}^{\circ}(2^n - 1))\Big) \\
&= \eta(\mathbf{e}(2^n - 1)).
\end{aligned}$$

Thus, the forward direction is completed by induction.

Now, suppose that, for any $\mathbf{e} \in Q$, $q^{\mathbf{A}}(\mathbf{e}^{\circ}) \, \gamma \, \mathbf{e}(2^n - 1)$. Let f be a fundamental operation symbol of arity, say, r. Let $\mathbf{e}_0, \ldots, \mathbf{e}_{r-1} \in Q$. Write $\mathbf{e} = f^{\mathbf{Q}}(\mathbf{e}_0, \ldots, \mathbf{e}_{r-1})$. Then, by hypothesis,

$$\begin{aligned}
\eta \circ q^{\mathbf{A}}(f^{\mathbf{Q}^{\circ}}(\mathbf{e}_0^{\circ}, \ldots, \mathbf{e}_{r-1}^{\circ})) &= \eta \circ q^{\mathbf{A}}(\mathbf{e}^{\circ}) \\
&= \eta(\mathbf{e}^{\circ}(2^n - 1)) \\
&= \eta(f^{\mathbf{A}}(\mathbf{e}_0(2^n - 1), \ldots, \mathbf{e}_{r-1}(2^n - 1))) \\
&= f^{\mathbf{A}/\gamma}(\eta(\mathbf{e}_0(2^n - 1)), \ldots, \eta(\mathbf{e}_{r-1}(2^n - 1))) \\
&= f^{\mathbf{A}/\gamma}(\eta \circ q^{\mathbf{A}}(\mathbf{e}_0^{\circ}), \ldots, \eta \circ q^{\mathbf{A}}(\mathbf{e}_{r-1}^{\circ})).
\end{aligned}$$

□

Lemma 2.15. *Let n be a natural number. Let $\mathbf{A}$ be an algebra in a variety with n-cube term, q. Let $\theta_0, \ldots, \theta_{n-1}, \gamma$ be congruences on $\mathbf{A}$. Let η be the natural quotient map of $\mathbf{A}$ onto $\mathbf{A}/\gamma$. Write $Q = Q(\theta_0, \ldots, \theta_{n-1})$. If $\eta \circ q^{\mathbf{A}} : Q^{\circ} \to A/\gamma$ is a homomorphism, then $C_2(\theta_0, \ldots, \theta_{n-1}; \gamma)$ holds (and hence, by Proposition 2.12, $C(\theta_0, \ldots, \theta_{n-1}; \gamma)$ holds, as well).*

Proof. Let s and t be any terms of rank, say, r. Let $\mathbf{a}_0, \ldots, \mathbf{a}_{r-1} \in P(\theta_0, \ldots, \theta_{n-1})$. For each $i < n$, we have a $j_i < n$ and $\langle a_i, b_i \rangle \in \theta_{j_i}$ such that $\mathbf{a}_i = \langle \langle a_i, b_i \rangle (\beta_s(j_i)) \mid s < 2^n \rangle$. Suppose that

$$s^{\mathbf{Q}^{\circ}}(\mathbf{a}_0^{\circ}, \ldots, \mathbf{a}_{r-1}^{\circ}) \, \gamma^{2^n - 1} \, t^{\mathbf{Q}^{\circ}}(\mathbf{a}_0^{\circ}, \ldots, \mathbf{a}_{r-1}^{\circ}).$$

But, then, by Lemma 2.14, we get that,

$$\begin{aligned} s^{\mathbf{A}}(b_0, \ldots, b_{r-1}) \,&\gamma\, q^{\mathbf{A}}(s^{\mathbf{Q}^\circ}(\mathbf{a}_0^\circ, \ldots, \mathbf{a}_{r-1}^\circ)) \\ &\gamma\, q^{\mathbf{A}}(t^{\mathbf{Q}^\circ}(\mathbf{a}_0^\circ, \ldots, \mathbf{a}_{r-1}^\circ)) \\ &\gamma\, t^{\mathbf{A}}(b_0, \ldots, b_{r-1}). \end{aligned}$$

□

Corollary 2.16. *Let n be a natural number. Let $\mathcal{V}$ be a variety with an n-cube term. Suppose also that, for all $\mathbf{A} \in \mathcal{V}$, the restriction of $q^{\mathbf{A}}$ to $Q^\circ = Q_n(1_A, \ldots, 1_A)^\circ$ is a homomorphism. Then, for any critical algebra $\mathbf{C} \in \mathcal{V}$, we have that $|C| \leq |F_{\mathcal{V}}(n)|$. In particular, if $F_{\mathcal{V}}(n)$ is finite, then $\mathcal{V}$ has a finite critical bound.*

Proof. This is immediate from Proposition 2.13 and Lemma 2.15. □

2.1.1 On strong cube terms and congruence permutability

Let $\mathcal{V}$ be a variety with a Mal'cev term, p. Let $X = \{x_n \mid n \in \omega\}$ be the usual set of variables.

For each $r \in \omega$, we can define an endomorphism on $\mathbf{F} = \mathbf{F}_{\mathcal{V}}(\omega)$ by homomorphically extending the maps

$$\rho_r^X x_n = x_{n \vee r}.$$

Let $\bar{\rho}_r$ stand for the endomorphism induced on $\mathbf{F}$ by ρ_r^X. Note that these endomorphisms pairwise commute. (This follows from the fact that $\vee$ is commutative on $\underline{\mathbf{2}}^\omega$.)

Similarly, for each natural number r, we let $\bar{\varepsilon}_r$ stand for the endomorphisms got by homomorphically extending the maps

$$\varepsilon_r^X x_n = x_{n \wedge r}.$$

Again, we get that these maps commute.

Now, we shall recursively build, for each natural number $n > 0$, a term q_n for $\mathcal{V}$ in the variables $\{x_n \mid n < 2^n - 1\}$. Set

$$q_1(x_0) = x_0.$$

Now, for $n > 1$, define

$$q_n(x_0, \ldots, x_{2^n-2}) = p(x_{2^{n-1}-1}, q_{n-1}(x_0, \ldots, x_{2^{n-1}-2}), q_{n-1}(x_{2^{n-1}}, \ldots, x_{2^n-2})).$$

It is also useful to note that $q_2(x_0, x_1, x_2) = p(x_1, x_0, x_2)$ and that

$$\begin{aligned} q_n(x_0, \ldots, x_{2^n-2}) &= q_2(q_{n-1}(x_0, \ldots, x_{2^{n-1}-2}), x_{2^{n-1}-1}, q_{n-1}(x_{2^{n-1},\ldots,x_{2^n-2}})) \\ &= q_2(q_{n-1}(x_0, \ldots, x_{2^{n-1}-2}), x_{2^{n-1}-1}, \bar{\rho}_{2^{n-1}} q_{n-1}(x_0, \ldots, x_{2^{n-1}-2})). \end{aligned}$$

In Opršal (2014+) (see his p. 8), these terms q_n are also defined; he calls them *strong cube terms* there.

Proposition 2.17. *For each $n > 0$, let q_n be the term for variety $\mathcal{V}$ with Mal'cev term p, as defined above. Then, for each $n > 0$ and any $r : 0 < r < 2^n$,*

$$\mathcal{V} \models \bar{\rho}_r q_n(\mathbf{x}) \approx x_{2^n-1}.$$

Proof. We will induct on $n > 0$. For the case $n = 1$, we have that $2^n = 2$ and so we need to verify the claim for $r = 1$; in this case,

$$\bar{\rho}_r q_1(x_0) := \rho_1 x_0 = x_{0\vee 1} = x_1.$$

Now, suppose that the theorem has been verified for the case $n = m - 1$. Get $r : 0 < r < 2^m$. Note that

$$\begin{aligned} \rho_r q_m(\mathbf{x}) = p(&x_{(2^{m-1}-1)\vee r}, \\ &\rho_r q_{m-1}(x_0, \ldots, x_{2^{m-1}-2}), \\ &\bar{\rho}_r \bar{\rho}_{2^{m-1}} q_{m-1}(x_0, \ldots, x_{2^{m-1}-2})). \end{aligned}$$

We show by cases, supposing first that $r < 2^{m-1}$ (in particular, $\beta_r(m-1) = 0$, and hence $2^{m-1} - 1 \vee r = 2^{m-1} - 1$). Then, by inductive hypothesis, we have that

$$\begin{aligned}\mathcal{V} \models p(&x_{(2^{m-1}-1)\vee r}, \bar{\rho}_r q_{m-1}(x_0, \ldots, x_{2^{m-1}-2}), \bar{\rho}_r \bar{\rho}_{2^{m-1}} q_{m-1}(x_0, \ldots, x_{2^{m-1}-2})) \\ &\approx p(x_{2^{m-1}-1}, x_{2^{m-1}-1}, \bar{\rho}_{2^{m-1}} x_{2^{m-1}-1}) \\ &= p(x_{2^{m-1}-1}, x_{2^{m-1}-1}, x_{2^m-1}) \\ &\approx x_{2^m-1}.\end{aligned}$$

Now suppose that $r$is such that $2^{m-1} \leq r < 2^m$. Then, $\beta_r(m-1) = 1$ and so $r \vee 2^{m-1} = r$, while $r \vee (2^{m-1} - 1) = 2^m - 1$. In particular, $\bar{\rho}_r \bar{\rho}_{2^{m-1}} = \bar{\rho}_r$, while $\bar{\rho}_r x_{2^{m-1}-1} = x_{2^m-1}$. Thus,

$$\begin{aligned}\mathcal{V} \models p(&x_{(2^{m-1}-1)\vee r}, \bar{\rho}_r q_{m-1}(x_0, \ldots, x_{2^{m-1}-2}), \bar{\rho}_r \bar{\rho}_{2^{m-1}} q_{m-1}(x_0, \ldots, x_{2^{m-1}-2})) \\ &\approx x_{2^m-1}.\end{aligned}$$

The proposition follows by induction. $\square$

Next is a theorem equivalent to the previous, but which is worth stating in its own right:

Proposition 2.18. *Let n be a natural number. Let q_n be the term for variety $\mathcal{V}$ with Mal'cev term p, as defined above. Then, for any $r < 2^n - 1$,*

$$\mathcal{V} \models \bar{\varepsilon}_r q_n(\mathbf{x}) \approx \bar{\varepsilon}_r x_{2^n-1} = x_r.$$

Proof. We prove by induction on n. If $n = 1$, then $r < 2^n - 1 = 1$ means that $r = 0$. Thus, since $q_1(x_0) = x_0$, this case is trivial. Now, suppose that the proposition has been verified for the $(n-1)$-case. Let $r < 2^n$. By Proposition 2.7, we need only consider the case of r such that $\beta_r(i) = 0$ for just one $i < n$—that is, so that $r = 2^n - 1 - 2^i$ for some $i < n$. We consider by cases, first supposing that $i < n - 1$. Note, then, that $\bar{\varepsilon}_r \bar{\rho}_{2^{n-1}} = \bar{\rho}_{2^{n-1}} \bar{\varepsilon}_r$. Using this and the inductive hypothesis, we calculate that

$$\begin{aligned}\bar{\varepsilon} q_n(x_0,\ldots,x_{2^n-2}) &= \bar{\varepsilon}_r q_2(q_{n-1}(x_0,\ldots,x_{2^{n-1}-2}), x_{2^{n-1}-1}, \bar{\rho}_{2^{n-1}} q_{n-1}(x_0,\ldots,x_{2^{n-1}-2}))\\ &\approx q_2(x_r, x_{2^{n-1}-1-2^i}, \bar{\rho}_{2^{n-1}} x_r)\\ &= q_2(x_r,x_r,x_r) \approx x_r.\end{aligned}$$

Now, suppose that $i = n-1$ and hence that $r = 2^{n-1}-1$. Note, then, that $\bar{\varepsilon}_r$ leaves $q_{n-1}(x_0,\ldots,x_{2^{n-1}-2})$ unchanged while mapping $q_{n-1}(x_{2^{n-1}},\ldots,x_{2^n-2})$ to $q_{n-1}(x_0,\ldots,x_{2^{n-1}-2})$. We thus get that

$$\begin{aligned}\bar{\varepsilon}_r q_n(x_0,\ldots,x_{2^n-2}) &= q_2(\bar{\varepsilon}_r q_{n-1}(x_0,\ldots,x_{2^{n-1}-2}), \bar{\varepsilon}_r x_{2^{n-1}-1}, \bar{\varepsilon}_r q_{n-1}(x_{2^{n-1}},\ldots,x_{2^n-2}))\\ &\approx x_r.\end{aligned}$$

The result follows by induction. □

It is worth noting that, for each natural number n, the term q_n can be used to “complete an n-dimensional hypercube” in the same way that the Mal’cev term—as shown in Mal’cev’s classic result—“completes a parallelogram.” For instance, let $\mathbf{A}$ be any algebra in a variety with a Mal’cev term, p, and congruences α, β. Let $a,b,c \in A$ such that if $b\,\alpha\,a\,\beta\,c$, then $b\,\beta\,p^{\mathbf{A}}(b,a,c)\,\alpha\,c$. In preparation to generalize this, consider an overly-pedantic restatement of this fact: if $\theta_0,\theta_1 \in \operatorname{Con}\mathbf{A}$ and $a_0,a_1,a_2 \in A$ such that, for any $i<2$, and $r,s : 0 \le r < s < 3$ with $\beta_r(i) \neq \beta_s(i)$ and $\beta_r(j) = \beta_s(j)$ for $j \neq i$, we have $a_r\,\theta_i\,, a_s$, then, for each $i<2$, $q_2(a_0,a_1,a_2)\,\theta_i\,a_{3-2^i}$.

We can generalize this procedure and formalize the point we are trying to make. Let n be a natural number. Let $\mathcal{V}$ be a variety. Let $\theta_0,\ldots,\theta_{n-1} \in \operatorname{Con}\mathbf{A}$. Let $D(\theta_0,\ldots,\theta_{n-1})$ be the set of all $\langle a_0,\ldots,a_{2^n-1}\rangle \in A^{2^n}$ such that, for all s,r with $0 \le s \le r < 2^n$, $a_s\theta_i a_r$ whenever, $\beta_s(j) = \beta_r(j)$ for all $j \neq i$ (that is, when their binary expansions differ at most in the i^{th} coordinate). We denote by $D^\circ(\theta_0,\ldots,\theta_{n-1})$ the projection of $D(\theta_0,\ldots,\theta_{n-1})$ onto its first 2^n-1 coordinates and denote by $\mathbf{a}^\circ$ the image of a given element $\mathbf{a} \in A^{2^n}$ under this same sort of projection. We say that $\mathbf{A}$ has the *n-dimensional hyper-parallelogram completion property*—abbreviated $H^{\mathbf{A}}(n)$—provided for any $\theta_0, \ldots, \theta_{n-1} \in \operatorname{Con} \mathbf{A}$, and any $\langle a_0, \ldots, a_{2^n-1} \rangle \in D(\theta_0, \ldots, \theta_{n-1})$, there exists an $a^* \in A$ such that, $\langle a_0, \ldots, a_{2^n-2}, a^* \rangle$ is in $D(\theta_0, \ldots, \theta_{n-1})$. We say that variety $\mathcal{V}$ has the property $H(n)$ provided $H^{\mathbf{A}}(n)$ holds for all $\mathbf{A} \in \mathcal{V}$.

Definition 2.19. Let $\mathcal{V}$ be a variety. Let n be a natural number. Suppose that $\mathcal{V}$ has a term function p_n in $2^n - 2$ variables that satisfies the equations displayed in Proposition 2.18, which we reproduce here: For all $r < 2^n - 1$,

$$\mathcal{V} \models \bar{\varepsilon}_r p_n(x_0, \ldots, x_{2^n-2}) \approx x_r.$$

We say that p_n is a *strong n-cube term for $\mathcal{V}$.*

Theorem 2.20. *Let $\mathcal{V}$ be variety, and let n be a natural number. Then $\mathcal{V}$ has the property $H(n)$ if and only if $\mathcal{V}$ has a strong n-cube term.*

Proof. First, suppose that $\mathcal{V}$ exhibits the property, $H(n)$. Consider $\mathbf{F} := \mathbf{F}_{\mathcal{V}}(2^n - 1)$. For each $r < 2^n$, let $\bar{\varepsilon}_r$ denote the endomorphism of $\mathbf{F}$ similar to that given above. For each $i < n$, let

$$\theta_i = \operatorname{Cg}^{\mathbf{F}}\{\langle x_r, x_s \rangle \mid \beta_r(i) \neq \beta_s(i) \text{ and } \beta_r(j) = \beta_s(j) \text{ for all } j \neq i\}.$$

Then, of course, $\langle x_0, \ldots, x_{2^n-2} \rangle \in D^{\circ}(\theta_0, \ldots, \theta_{n-1})$. Since $\mathbf{F}$ has the property $H^{\mathbf{F}}(n)$, we have some rank-$(2^n - 1)$ term p_n such that

$$\langle x_0, \ldots, x_{2^n-2}, p_n^{\mathbf{F}}(x_0, \ldots, x_{2^n-2}) \rangle \in D(\theta_0, \ldots, \theta_{n-1}).$$

Let $i < n$, and set $r = 2^n - 1 - 2^i$. Note that $\theta_i = \ker \bar{\varepsilon}_r$. Thus,

$$\bar{\varepsilon}_r p_n^{\mathbf{F}}(x_0, \ldots, x_{2^n-2}) = x_r.$$

Now, for arbitrary $r < 2^n-1$, we can write $r = 2^n-1-\sum_{i \in S} 2^i$, with $S \subseteq \{0, \ldots, n-1\}$. By inducting on $|S| > 0$, it is not difficult to show that, for any $r < 2^n - 1$,

$$\bar{\varepsilon}_r p_n^{\mathbf{F}}(x_0, \ldots, x_{2^n-2}) = x_r.$$

We have already seen the basis step. For the inductive step, write $S = \{i_0, \ldots, i_{k-1}\}$, with $1 < k \leq n$. Let $r = 2^n - 1 - \sum_{j=0}^{k-1} 2^{i_j}$ and $r' = 2^n - 1 - \sum_{j=0}^{k-2} 2^{i_j}$. By inductive hypothesis, we may assume that

$$\bar{\varepsilon}_{r'} p_n^{\mathbf{F}}(x_0, \ldots, x_{2^n-2}) = x_{r'}. \tag{2.2}$$

Let $r'' = 2^n - 1 - 2^{i_{k-1}}$. Note that $\bar{\varepsilon}_{r''}\bar{\varepsilon}_{r'} = \bar{\varepsilon}_r$ and also that $\bar{\varepsilon}_{r''} x_{r'} = x_r$. Applying $\bar{\varepsilon}_{r''}$ to both sides of equation 2.2, we thus learn that

$$\bar{\varepsilon}_r p_n^{\mathbf{F}}(x_0, \ldots, x_{2^n-2}) = x_r.$$

Now, since $\mathbf{F}$ is free for $\mathcal{V}$ we thus get that, for all $r < 2^n - 1$,

$$\mathcal{V} \models \bar{\varepsilon}_r p_n^{\mathbf{F}}(x_0, \ldots, x_{2^n-2}) \approx x_r.$$

Thus, $\mathcal{V}$ has a strong n-cube term.

Now, suppose that $\mathcal{V}$ has a strong n-cube term, p_n. Let $\mathbf{A} \in \mathcal{V}$. Let $\theta_0, \ldots, \theta_{n-1}$ be congruences of $\mathbf{A}$, and take

$$\langle a_0, \ldots, a_{2^n-2}\rangle \in D^\circ(\theta_0, \ldots, \theta_{n-1}).$$

Let $a^* = p_n^{\mathbf{A}}(a_0, \ldots, a_{2^n-2})$; we claim that $\langle a_0, \ldots, a_{2^n-2}, a^*\rangle \in D(\theta_0, \ldots, \theta_{n-1})$. Choose an $i < n$ and set $r = 2^n - 1 - 2^i$. We need to show that $p_n^{\mathbf{A}}(a_0, \ldots, a_{2^n-2}) \; \theta_i \; a_r$. We claim that, for each $i < n$,

$$p_n^{\mathbf{A}}(a_0, \ldots, a_{2^n-2}) \; \theta_i \; (\bar{\varepsilon}_r p_n)^{\mathbf{A}}(a_0, \ldots, a_{2^n-2}) = p_n^{\mathbf{A}}(a_{0\wedge r}, \ldots, a_{(2^n-2)\wedge r}),$$

which will prove the claim. We claim that, for any $s < 2^n$, $a_s \; \theta_i \; a_{s\wedge r}$: Note that $\beta_s(j) = \beta_{s\wedge r}(j)$ for all $j < n$ except possibly for $j = i$. Since $\mathbf{a} \in D(\theta_0, \ldots, \theta_{n-1})$, the claim and the result then follow. □

This now gives rise to the following characterization of congruence permutability, an apparently new one.

Theorem 2.21. *Let $\mathcal{V}$ be a variety. Then $\mathcal{V}$ is congruence permutable if and only if there is a natural number n such that the n-dimensional hyper-parallelogram completion property holds across $\mathcal{V}$.*

Proof. Above, for arbitrary congruence permutable $\mathcal{V}$, we used a Mal'cev term to construct a strong n-cube term for $\mathcal{V}$, for each n. Now, as noted in Opršal (2014+), Lemma 4.1, it is also easy to use a strong n-cube term, for any n, to construct a Mal'cev term. Thus, the theorem follows by Mal'cev's characterization of congruence permutability (Theorem A.21) together with Theorem 2.20. □

2.2 "Affine" properties of strong cube terms

In this section, we will prove a generalization of Higman's Lemma (see Neumann (1967), propositions 33.42 and 33.44), involving strong cube terms—indeed, we indicate (in a later section, below Corollary 2.53) how one can verify that the manner in which Higman rewrites any group-term, modulo nilpotence of some class, involves a strong cube term. Furthermore, we characterize this new version of Higman's Lemma in terms of the commutation of the strong cube term with all operations on a hypercube-indexed subpower of a given algebra. We regard this as suggesting a possible generalization of the notion of "affine" or at least as depicting supernilpotence as a generalization of abelianness. We give a second result which we regard as further suggestive of such a notion.

But first, we note the following purely technical observation for convenience.

Proposition 2.22. *Let n be a natural number. Let $\mathbf{A}$ be an algebra in a Mal'cev variety for which the term q_n is defined, as above. Let $\theta_0, \dots, \theta_{n-1} \in \operatorname{Con} \mathbf{A}$. Then for any $r < 2^n$ and any $\mathbf{e} \in Q := Q(\theta_0, \dots, \theta_{n-1})$,*

$$q_n^{\mathbf{A}}((\varepsilon_r^Q(\mathbf{e}))^\circ) = (\bar{\varepsilon}_r q_n)^{\mathbf{A}}(\mathbf{e}^\circ) = \mathbf{e}(r).$$

Proof. This is really a direct corollary of Proposition 2.18; we calculate that

$$\begin{aligned} q_n^{\mathbf{A}}((\varepsilon_r^Q \mathbf{e})^\circ) &= q_n^{\mathbf{A}}(\langle \mathbf{e}(j \wedge r) \mid j < 2^n - 1 \rangle) \\ &= (\varepsilon_r q_n)^{\mathbf{A}}(\langle \mathbf{e}(j) \mid j < 2^n - 1 \rangle) \\ &= \mathbf{e}(r). \end{aligned}$$

□

The next result can be viewed as a partial generalization of Proposition 5.7 from Freese and McKenzie (1987). I think of it as concerning "affine behavior." Its statement and proof should also be compared to that of Opršal (2014+), Lemma 4.2.

Lemma 2.23. *Let* $\mathbf{A}$ *be an algebra in Mal'cev variety* $\mathcal{V}$*. Let* $\theta_0, \ldots, \theta_n, \gamma$ *be congruences on* $\mathbf{A}$*. Let* η *be the natural quotient map of* $\mathbf{A}$ *onto* $\mathbf{A}/\gamma$*. Let* Q *denote* $Q(\theta_0, \ldots, \theta_{n-1})$*. Then* $C(\theta_0, \ldots, \theta_{n-1}; \gamma)$ *implies that* $\eta \circ q_n^{\mathbf{A}} : \mathbf{Q}^\circ \to \mathbf{A}/\gamma$ *is a homomorphism with the property that for any* $\mathbf{a} = \langle a_0, \ldots, a_{2^n-1} \rangle \in Q$*,*

$$\langle q_n(a_0, \ldots, a_{2^n-2}), a_{2^n-1} \rangle \in \gamma.$$

Proof. Take any element $\mathbf{a} \in Q$. Recall that by Proposition 2.7, $\rho_r^{A^{2^n}} a \in Q$ for all $r < 2^n$. Consider

$$\begin{aligned} \mathbf{e} :&= q_n^{\mathbf{Q}}(\rho_0^Q \mathbf{a}, \ldots, \rho_{2^n-2}^Q \mathbf{a}) \\ &= \langle q^{\mathbf{A}}((\rho_0^Q \mathbf{a})(s), \ldots, (\rho_{2^n-2}^Q \mathbf{a})(s)) \mid s < 2^n \rangle \end{aligned}$$

We calculate that

$$\begin{aligned} \mathbf{e}(0) &= q^{\mathbf{A}}((\rho_0^Q \mathbf{a})(0), \ldots, (\rho_{2^n-2}^Q \mathbf{a})(0)) \\ &= q^{\mathbf{A}}(\mathbf{a}(0 \vee 0), \ldots, \mathbf{a}(0 \vee 2^n - 2)) \\ &= q^{\mathbf{A}}(\mathbf{a}(0), \ldots, \mathbf{a}(2^n - 2)). \end{aligned}$$

On the other hand, for $r \in \{1, \dots, 2^n - 1\}$, we find that by Proposition 2.17,

$$\begin{aligned}\mathbf{e}(r) &= q_n^{\mathbf{A}}((\rho_0^Q \mathbf{a})(r), \dots, (\rho_{2^n-2}^Q \mathbf{a})(r)) \\ &= q_n^{\mathbf{A}}(\mathbf{a}(r \vee 0), \dots, \mathbf{a}(r \vee 2^n - 2)) \\ &= \bar{\rho}_r q_n^{\mathbf{A}}(\mathbf{a}(0), \dots, \mathbf{a}(2^n - 2)) \\ &= \mathbf{a}(2^n - 1).\end{aligned}$$

Let $\mathbf{a}^\circ$ denote the image of $\mathbf{a}$ in Q°; that is, let $\mathbf{a}^\circ = \langle a_s \mid s < 2^n - 1\rangle$. For each $r : 0 < r < 2^{n-1}$, we have that $\mathbf{e}(r) = \mathbf{e}(r + 2^{n-1})$. Using that $C(\theta_0, \dots, \theta_{n-1}; \gamma)$ holds and applying Proposition 2.5, we get that

$$q_n^{\mathbf{A}}(\mathbf{a}^\circ) = \mathbf{e}(0)\,\gamma\,\mathbf{e}(2^{n-1}) = \mathbf{a}(2^n - 1). \tag{2.3}$$

Now, take any fundamental operation symbol f. Say that f has rank ℓ. Take, as well, $\mathbf{a}_0, \dots, \mathbf{a}_{\ell-1} \in Q$. Write $\mathbf{b} = f^{\mathbf{Q}}(\mathbf{a}_0, \dots, \mathbf{a}_{\ell-1})$.

We now apply our above findings in two ways. Since γ respects $f^{\mathbf{A}}$ and since, for each $i < \ell$, we have that $\langle q_n(\mathbf{a}_i{}^\circ), \mathbf{a}_i(2^n - 1)\rangle \in \gamma$, we may conclude that

$$\langle f^{\mathbf{A}}(q_n^{\mathbf{A}}(\mathbf{a}_0{}^\circ), \dots, q_n^{\mathbf{A}}(\mathbf{a}_{\ell-1}{}^\circ)), \mathbf{b}(2^n - 1)\rangle \in \gamma.$$

On the other hand, we also have that

$$\langle q_n(\mathbf{b}^\circ), \mathbf{b}(2^n - 1)\rangle \in \gamma.$$

Thus, by the transitivity of γ, we get that

$$\langle f^{\mathbf{A}}(q_n(\mathbf{a}_0{}^\circ), \dots, q_n(\mathbf{a}_{\ell-1}{}^\circ)), q_n(\mathbf{b}^\circ)\rangle \in \gamma.$$

Thus, $\eta \circ q_n : \mathbf{Q}^\circ \to \mathbf{A}/\gamma$ is indeed a homomorphism.

The last claim of the theorem is evident from Proposition 2.14, in light of the fact that every strong n-cube term is a an n-cube term. □

It is appropriate to compare the following to Proposition 3.6 and Lemma 4.2 of Opršal (2014+); the result below is implicit in these results of Opršal. However, it may also be helpful to see this as a very close generalization of Higman's Lemma, which can be found as Corollary 33.44 in Neumann (1967).

Theorem 2.24. *For natural number n, $\mathbf{A}$ in a Mal'cev variety, and any congruences $\theta_0, \ldots, \theta_{n-1}, \gamma$ on $\mathbf{A}$, the following are equivalent.*

(i) $C(\theta_0, \ldots, \theta_{n-1}; \gamma)$

(ii) $q_n(a_0, \ldots, a_{2^n-2}) \,\gamma\, a_{2^n-1}$ *holds for any* $\langle a_0, \ldots, a_{2^n-1}\rangle \in Q(\theta_0, \ldots, \theta_{n-1})$.

(iii) $C_2(\theta_0, \ldots, \theta_{n-1}; \gamma)$

Proof. That (i) implies (ii) is one of the results noted in Lemma 2.23. We get that (ii) implues (iii) from Lemmas 2.14 and 2.15 and the fact that every strong n-cube term is an n-cube term. The fact that (iii) implies (i) follows from Proposition 2.12. $\square$

In Freese and McKenzie (1987) (and elsewhere) it is often used that if $\mathbf{A}$ is in a congruence-permutable variety with Mal'cev term p, and $\alpha, \beta \in \operatorname{Con} \mathbf{A}$, then for any $a, b, c \in A$ with $a \,\alpha\, b \,\beta\, c$, we have that

$$p^{\mathbf{A}}(p^{\mathbf{A}}(a, b, c), c, b) \; [\alpha, \beta] \; a.$$

This fact is closely connected with the affine structure available on blocks of abelian congruences for such an $\mathbf{A}$. We now work toward what appears to be the correct generalization of this, for a term q_n, for a given n, in place of p. We suggest that one might think of p and, for each n, q_n, geometrically (in the way of Gumm) as related to a projection function, though requiring an entire "frame" of coordinates for its input.

Proposition 2.25. *Let n be a natural number. Let $\mathbf{A}$ be an algebra in Mal'cev variety with term q_n as defined above. Let $\theta_0, \ldots, \theta_{n-1} \in \operatorname{Con} \mathbf{A}$. Let $Q = Q(\theta_0, \ldots, \theta_{n-1})$. Let $r < 2^n$. Then for any $\mathbf{e} \in Q$, we have that*

$$(\bar{\pi}_r q_n)^{\mathbf{A}}(\mathbf{e}^{\circ}) \equiv \mathbf{e}(r') \mod S(\theta_0, \ldots, \theta_{n-1}).$$

Proof. Recall from Proposition 2.7 that $Q := Q(\theta_0, \ldots, \theta_{n-1})$ is closed under $\pi_r := \pi_r^{A^{2^n}}$, for each $r < 2^n$. Let $\mathbf{e} \in Q$, and set $\mathbf{e}' := \pi_r \mathbf{e} = \langle \mathbf{e}(s \oplus r) \mid s < 2^n \rangle$. Let $\equiv$ denote $S(\theta_0, \ldots, \theta_{n-1})$. From Theorem 2.23, we have that $q_n^{\mathbf{A}}(\mathbf{e}'^{\circ}) \equiv \mathbf{e}'(2^n - 1)$. Note also that $\mathbf{e}'(2^n - 1) = \mathbf{e}((2^n - 1) \oplus r) = \mathbf{e}(r')$. It follows that

$$\begin{aligned}
(\bar{\pi}_r q_n)^{\mathbf{A}}(\mathbf{e}^{\circ}) &= (\bar{\pi}_r q_n)^{\mathbf{A}}(\langle \mathbf{e}(s) \mid s < 2^n - 1 \rangle) \\
&= q_n^{\mathbf{A}}(\langle \mathbf{e}(s \oplus r) \mid s < 2^n - 1 \rangle) \\
&= q_n^{\mathbf{A}}(\langle \mathbf{e}'(s) \mid s < 2^n - 1 \rangle) \\
&\equiv \mathbf{e}'(2^n - 1) \\
&= \mathbf{e}(r')
\end{aligned}$$

□

Proposition 2.26. *Let n be a natural number. Let $\mathbf{A}$ be an algebra in a Mal'cev variety with term q_n as defined above. Let $\theta_0, \ldots, \theta_{n-1} \in \operatorname{Con} \mathbf{A}$. Let $Q = Q(\theta_0, \ldots, \theta_{n-1})$. Let $r < 2^n$. Let $\mathbf{e} \in Q$, and write $e^* = q_n^{\mathbf{A}}(\mathbf{e}^{\circ})$. Let $\mathbf{a}$ be any assignment of elements of A to the variables in X that includes $x_r \mapsto e^*$ and, for each $i \neq r$, $x_i \mapsto \mathbf{e}(i \oplus r')$. Then*

$$q_n^{\mathbf{A}}(x_0, \ldots, x_{2^n-2})[\mathbf{a}] = \mathbf{e}(r).$$

Proof. Let $\equiv$ stand for $S(\theta_0, \ldots, \theta_{n-1})$. Note that $e^* = q_n^{\mathbf{A}}(\mathbf{e}^{\circ}) \equiv \mathbf{e}(2^n - 1) = \mathbf{e}(r \oplus r')$. Then

$$\begin{aligned}
q_n^{\mathbf{A}}(x_0, \ldots, x_{2^n-2})[\mathbf{a}] &\equiv (\bar{\pi}_{r'} q_n)^{\mathbf{A}}(\mathbf{e}(0 \oplus r'), \ldots, \mathbf{e}((2^n - 2) \oplus r')) \\
&\equiv \mathbf{e}(r)
\end{aligned}$$

□

As an illustration of the previous result, note that, for a given $\mathbf{A}$ in a Mal'cev variety with $\theta_0, \theta_1, \theta_2 \in \operatorname{Con} \mathbf{A}$ and $\mathbf{e} = \langle e_0, \ldots, e_7 \rangle \in Q(\theta_0, \theta_1, \theta_2)$, we get that

$$q_3^{\mathbf{A}}(e_6, q_3^{\mathbf{A}}(e_0, e_1, e_2, e_3, e_4, e_5, e_6), e_4, e_5, e_2, e_3, e_0) \equiv e_1 \mod S(\theta_0, \theta_1, \theta_2).$$

2.3 Supernilpotence and a broadening of the finite basis result of Freese and Vaughan-Lee

Definition 2.27. For any algebra $\mathbf{A}$, natural number n and tuple of congruences $\Theta = \langle\theta_0, \ldots, \theta_{n-1}\rangle$, we define the (ordered) commutator of these congruences, denoted $S_n(\Theta)$ as follows. For $n = 0$—that is, for Θ empty—we set $S_0(\Theta) = 1_A$. For $n = 1$, and so for $\Theta = \langle\theta_0\rangle$, we set $S_1(\Theta) = \theta_0$. Otherwise, we let $S_n(\Theta)$ be the least congruence γ on $\mathbf{A}$ so that $C(\theta_0, \ldots, \theta_{n-1}; \gamma)$. (It is easy to see from the definition of $C(\theta_0, \ldots, \theta_{n-1}; \gamma)$ that one can obtain such.) Typically, for $n > 0$, we'll write $S_n(\Theta) = S(\theta_0, \ldots, \theta_{n-1})$, with the parameter n thus implied. Note that $S_2(\theta_0, \theta_1) = [\theta_0, \theta_1]$.

Definition 2.28. For a given algebra $\mathbf{A}$, and $\theta \in \operatorname{Con}\mathbf{A}$, we say that θ is *supernilpotent of class k* whenever for any $(k+1)$-tuple of congruences, Θ with $\Theta(i) = \theta$ for each $i < k+1$, we have that $S_k(\Theta) = 0_A$. If 1_A is supernilpotent of class k we say that $\mathbf{A}$ is supernilpotent of class k. If $\theta \in \operatorname{Con}\mathbf{A}$ (or $\mathbf{A}$) is supernilpotent of class k for some k, we say that θ (or $\mathbf{A}$) is supernilpotent.

In particular, note that $\mathbf{A}$ is supernilpotent of class 0 if and only if A includes only a single element, while $\mathbf{A}$ is supernilpotent of class 1 if and only if $\mathbf{A}$ is abelian.

Recall the following result of Freese (1987) and Vaughan-Lee (1983).

Theorem 2.29. *(The finite basis result of Freese and Vaughan-Lee) Let $\mathbf{A}$ be a finite, nilpotent algebra in a Mal'cev variety of finite signature. Suppose also that $\mathbf{A}$ is the direct product of algebras of prime power order. Then $\mathbf{A}$ has a finite basis for its equational theory.*

Using their result, we now show that a seemingly broader statement of their result is also true.

Theorem 2.30. *Let n be a natural number. Let $\mathcal{V}$ be a locally finite,*[3] *Mal'cev variety of finite signature consisting solely of class-n supernilpotent algebras. Then $\mathcal{V}$ is finitely based.*

Proof. Since $\mathcal{V}$ is locally finite we have that $F_{\mathcal{V}}(n)$ is finite. By Theorem 2.24 and Proposition 2.13, we have that $\mathcal{V}$ has a finite critical bound. However, since locally finite algebras are generated by their critical algebras, we have that $\mathcal{V}$ is finitely generated. All that remains to show is that finite supernilpotent algebras are nilpotent and can be represented as the direct product of prime power algebras. These fact appear as Lemmas 7.5 and 7.6 in Aichinger and Mudrinski (2010). □

Continuing the work of Opršal, we find that we can simplify many of the proofs of Aichinger and Mudrinski, as well as strengthen some of them in the process. In particular, we offer proofs of those lemmas leading up to the results just cited in the above proof. Along the way, we also derive several properties of higher centralizers and commutators of a fairly basic nature, but which do not seem to have made it into print before now. Below, we shall further apply many of these results.

2.4 Some properties of higher centralizers and commutators, some old and some new

Here are two elementary facts one can deduce directly from Definition 2.27 (together with the definition of $C(\theta_0, \ldots, \theta_{n-1}; \gamma)$), which are not new, but which we shall need.

Proposition 2.31. *(Monotonicity of any higher commutator) Let $\mathbf{A}$ be an algebra with congruences $\theta_0, \ldots, \theta_{n-1}, \theta'_0, \ldots, \theta'_{n-1}$, for some natural number n. Suppose also that $\theta'_i \subseteq \theta_i$ for each $i < n$. Then*

(i) $S(\theta'_0, \ldots, \theta'_{n-1}) \leq S(\theta_0, \ldots, \theta_{n-1})$ *and*

[3] We also show in Theorem 3.7 that one does not need to assume local finiteness here, either: It is enough that $F_{\mathcal{V}}(2)$ is finite.

(ii) $\quad S(\theta_0, \ldots, \theta_{n-1}) \leq \theta_0 \cap \cdots \cap \theta_{n-1}$.

To my knowledge, the next result has not yet appeared in print, though it has an elementary proof.

Proposition 2.32. *Let n be a natural number. Let $\mathbf{A}$ be any algebra. Let $\theta_0, \ldots, \theta_{n-1}$ be congruences on $\mathbf{A}$. Let $k < n-1$. Then, for any $\{i_0, \ldots, i_{k-1}\} \subseteq \{0, \ldots, n-2\}$, we have that*

$$S_n(\theta_0, \ldots, \theta_{n-1}) \subseteq S_{k+1}(\theta_{i_0}, \ldots, \theta_{i_{k-1}}, \theta_{n-1}).$$

In particular, if σ is any permutation of $\{0, \ldots, n-2\}$, then

$$S(\theta_0, \ldots, \theta_{n-1}) = S(\theta_{\sigma(0)}, \ldots, \theta_{\sigma(n-2)}, \theta_{n-1}).$$

Proof. Let φ be an injective map from $\{0, \ldots, k-1\}$ into $\{0, \ldots, n-2\}$ such that for each $j < k$, $i_j = \varphi(j)$. Let $\gamma = S_{k+1}(\theta_{\varphi(0)}, \ldots, \theta_{\varphi(n-2)}, \theta_{n-1})$. By definition of S_n, it is sufficient to show that $C(\theta_0, \ldots, \theta_{n-1}; \gamma)$ holds. Let $\ell_0, \ldots, \ell_{n-1}$ be natural numbers, and, for each $i < n$, let $\mathbf{a}_i$ and $\mathbf{b}_i$ be ℓ_i-tuples of elements from A such that $\mathbf{a}_i \, \theta_i^{\ell_i} \, \mathbf{b}_i$. Let t be any term of rank $\sum \ell_i$. Suppose that, for any

$$\langle \mathbf{u}_0, \ldots, \mathbf{u}_{n-2} \rangle \in \{\mathbf{a}_0, \mathbf{b}_0\} \times \cdots \times \{\mathbf{a}_{n-2}, \mathbf{b}_{n-2}\} \setminus \{\langle \mathbf{b}_0, \ldots, \mathbf{b}_{n-2} \rangle\},$$

we have that $t^{\mathbf{A}}(\mathbf{u}_0, \ldots, \mathbf{u}_{n-2}, \mathbf{a}_{n-1}) \, \gamma \, t^{\mathbf{A}}(\mathbf{u}_0, \ldots, \mathbf{u}_{n-2}, \mathbf{b}_{n-1})$.

Assume that, for each $i < n$, $\mathbf{x}_i$ is a tuple of distinct variables whose entries do not occur in any $\mathbf{x}_j$ for $j \neq i$, $j < n$. Let e be the endomorphism of $\operatorname{Pol} \mathbf{A}$ defined by the following substitutions. For all $i \in \operatorname{im} \varphi$, let $e\mathbf{x}_i = \mathbf{x}_{\varphi^{-1}(i)}$; also, let $e\mathbf{x}_{n-1} = \mathbf{x}_{n-1}$, and, otherwise, set $e\mathbf{x}_i = \mathbf{b}_i$. Let t' be the image of $t^{\mathbf{A}}$ under the map e. It is evident, then, that for all choices of

$$\langle \mathbf{u}_0, \ldots, \mathbf{u}_{k-1} \rangle \in \{\mathbf{a}_{\varphi(0)}, \mathbf{b}_{\varphi(0)}\} \times \cdots \times \{\mathbf{a}_{\varphi(k-1)}, \mathbf{b}_{\varphi(k-1)}\} \setminus \{\langle \mathbf{b}_{\varphi(0)}, \ldots, \mathbf{b}_{\varphi(k-1)} \rangle\},$$

we have that $t'(\mathbf{u}_0, \ldots, \mathbf{u}_{k-1}, \mathbf{a}_{n-1}) \, \gamma \, t'(\mathbf{u}_0, \ldots, \mathbf{u}_{k-1}, \mathbf{b}_{n-1})$. Thus, we find that

$$\begin{aligned} t^{\mathbf{A}}(\mathbf{b}_0, \ldots, \mathbf{b}_{n-2}, \mathbf{a}_{n-1}) &= t'(\mathbf{b}_{\varphi(0)}, \ldots, \mathbf{b}_{\varphi(k-1)}, \mathbf{a}_{n-1}) \\ &\equiv t'(\mathbf{b}_{\varphi(0)}, \ldots, \mathbf{b}_{\varphi(k-1)}, \mathbf{b}_{n-1}) \\ &= t^{\mathbf{A}}(\mathbf{b}_0, \ldots, \mathbf{b}_{n-2}, \mathbf{b}_{n-1}). \end{aligned}$$

The result follows. □

The following is Proposition 6.1 in Aichinger and Mudrinski (2010) and Proposition 5.1 in Opršal (2014+), but it seems worth noting here as a simple consequence of the equivalence of the higher term condition and higher two-term condition in Mal'cev varieties.

Proposition 2.33. *Let* $\mathbf{A}$ *be an algebra in a Mal'cev variety. Let* $\theta_0, \ldots, \theta_{n-1} \in \operatorname{Con} \mathbf{A}$. *Let* σ *be a permutation of* $\{0, \ldots, n-1\}$. *Then*

$$S(\theta_0, \ldots, \theta_{n-1}) = S(\theta_{\sigma(0)}, \ldots, \theta_{\sigma(n-2)}, \theta_{\sigma(n-1)}).$$

Proof. This easily follows from Theorem 2.24, (i) ⇔ (iii) and Proposition 2.9. □

The next result is not difficult, but is also apparently new.

Proposition 2.34. *Let* n *be a natural number. Let* $\mathbf{A}$ *be an algebra in a Mal'cev variety. Let* $\theta_0, \ldots, \theta_{n-1} \in \operatorname{Con} \mathbf{A}$. *Let* $k < n$. *Then, for any* $\{i_0, \ldots, i_{k-1}\} \subseteq \{0, \ldots, n-1\}$, *we have that* $S(\theta_0, \ldots, \theta_{n-1}) \subseteq S(\theta_{i_0}, \ldots, \theta_{i_{k-1}})$.

Proof. This follows immediately from Propositions 2.32 and 2.33. □

The first part of the following theorem is given as Proposition 5.2 in Opršal (2014+) and Lemma 6.2 of Aichinger and Mudrinski (2010). Our proof of this first statement below is essentially the same as that given by Opršal; we have simply paired it with a second easy, but possibly overlooked, observation, to which it is related.

Theorem 2.35. *Let* $\mathbf{A}$ *be an algebra in a Mal'cev variety, and let* $\theta_0, \ldots, \theta_{n-1}$ *and* γ *be congruences of* $\mathbf{A}$*. Then*

$$C(\theta_0, \ldots, \theta_{n-1}; \gamma) \text{ if and only if } S(\theta_0, \ldots, \theta_{n-1}) \geq \gamma.$$

Furthermore, if q_n *is a strong* n*-cube term for* $\mathbf{A}$*, then*

$$S(\theta_0, \ldots, \theta_{n-1}) = \mathrm{Cg}^{\mathbf{A}}\{\langle q_n(a_0, \ldots, a_{2^n-2}), a_{2^n-1}\rangle \mid \mathbf{a} \in Q(\theta_0, \ldots, \theta_{n-1})\}.$$

Proof. Let $\gamma = \mathrm{Cg}^{\mathbf{A}}\{\langle q_n(a_0, \ldots, a_{2^n-2}), a^{2^n-1}\rangle \mid \mathbf{a} \in Q(\theta_0, \ldots, \theta_{n-1})\}$. By Theorem 2.24, we have that $C(\theta_0, \ldots, \theta_{n-1}; \gamma)$ holds. Thus, by definition, $S(\theta_0, \ldots, \theta_{n-1}) \subseteq \gamma$. On the other hand, since $C(\theta_0, \ldots, \theta_{n-1}; S(\theta_0, \ldots, \theta_{n-1}))$, we also get that, from Theorem 2.24, $\gamma \subseteq S(\theta_0, \ldots, \theta_{n-1})$. It follows that $\gamma = S(\theta_0, \ldots, \theta_{n-1})$, as claimed.

Now let γ' be any congruence on $\mathbf{A}$ so that $S(\theta_0, \ldots, \theta_{n-1}) \leq \gamma'$. But, as we have just seen, this puts $\{\langle q_n(a_0, \ldots, a_{2^n-2}, a_{2^n-1})\rangle \mid \mathbf{a} \in Q(\theta_0, \ldots, \theta_{n-1})\} \subseteq \gamma'$. Thus, by Theorem 2.24, we get that $C(\theta_0, \ldots, \theta_{n-1}; \gamma')$. □

The following is recorded in Aichinger and Mudrinski (2010) as Lemma 6.7 and in Opršal (2014+) as Lemma 5.6. Opršal's proof fits with the current exposition (much of which, in fairness, is a reworking of his presentation); we have not found that we could improve in a substantial way Opršal's proof, and so we refer the reader there.

Proposition 2.36. *Let* $\mathbf{A}$ *be an algebra in a Mal'cev variety. Let* n *be a natural number and let* $j < n$*. Let* $\theta_i \in \mathrm{Con}\,\mathbf{A}$ *for* $i < n$ *such that* $i \neq j$*. Let* Λ *be any set and let* $\psi_\lambda \in \mathrm{Con}\,\mathbf{A}$ *for all* $\lambda \in \Lambda$*. Then*

$$S(\theta_0, \ldots, \theta_{j-1}, \bigvee_{\Lambda} \psi_\lambda, \theta j + 1, \ldots, \theta_{n-1}) = \bigvee_{\Lambda} S(\theta_0, \ldots, \theta_{j-1}, \psi_\lambda, \theta_{j+1}, \ldots, \theta_{n-1}).$$

The following appears in Aichinger and Mudrinski (2010), but the proof they supply is arguably more complicated than the one we now offer.

Proposition 2.37. *Let* $\mathbf{A}$ *be an algebra in a Mal'cev variety. Let* n *be a natural number and let* $j < n$*. Let* $\theta_i \in \mathrm{Con}\,\mathbf{A}$ *for* $i < n$ *such that* $i \neq j$*. Let*

Λ *be any set and let* $\psi_\lambda \in \operatorname{Con}\mathbf{A}$ *for all* $\lambda \in \Lambda$. *Also, let* $\gamma \in \operatorname{Con}\mathbf{A}$. *Then* $C(\theta_0, \ldots, \theta_{j-1}, \bigvee_\Lambda \psi_\lambda, \theta_{j+1}, \ldots, \theta_{n-1}; \gamma)$ *if and only if, for all* $\lambda \in \Lambda$,

$$C(\theta_0, \ldots, \theta_{j-1}, \psi_\lambda, \theta_{j+1}, \ldots, \theta_{n-1}; \gamma).$$

Proof. The forward direction is done by monotonicity of the $(n+1)$-place centralizer in its first n coordinates. Now, assume that for all $\lambda \in \Lambda$, we have that $C(\theta_0, \ldots, \theta_{j-1}, \psi_\lambda, \theta_{j+1}, \ldots, \theta_{n-1}; \gamma)$. Then, by Theorem 2.35, we find that, for all $\lambda \in \Lambda$, $\gamma \geq S(\theta_0, \ldots, \theta_{j-1}, \psi_\lambda, \theta_{j+1}, \ldots, \theta_{n-1})$. But, by Theorem 2.36, this means that

$$\gamma \geq \bigvee_\Lambda S(\theta_0, \ldots, \theta_{j-1}, \psi_\lambda, \theta_{j+1}, \ldots, \theta_{n-1}) = S(\theta_0, \ldots, \theta_{j-1}, \bigvee_\Lambda \psi_\lambda, \theta_{j+1}, \ldots, \theta_{n-1}).$$

Thus, using Theorem 2.35, again, we find that

$$C(\theta_0, \ldots, \theta_{j-1}, \bigvee_\Lambda \psi_\lambda, \theta_{j+1}, \ldots, \theta_{n-1}; \gamma).$$

$\square$

Corollary 2.38. *Let* $\mathbf{A}$ *be an algebra in a Mal'cev variety, and let* $\theta_0, \ldots, \theta_{n-1}, \gamma$ *be congruences on* $\mathbf{A}$. *Then* $C(\theta_0, \ldots, \theta_{n-1}; \gamma)$ *holds if and only if*

$$C(\operatorname{Cg}\langle a_0, b_0\rangle, \ldots, \operatorname{Cg}\langle a_{n-1}, b_{n-1}\rangle; \gamma)$$

holds for all $\langle a_i, b_i\rangle \in \theta_i$.

Definition 2.39. Let n be a natural number and let $\mathbf{A}$ be an algebra with congruences $\theta_0, \ldots, \theta_{n-1}, \gamma$. Let $\ell_0, \ldots, \ell_{n-1}$ be natural numbers. We say that

$$C(\ell_0, \ldots, \ell_{n-1}; \theta_0, \ldots, \theta_{n-1}; \gamma)$$

holds when the following test is satisfied. Let $\mathbf{a}_i, \mathbf{b}_i \in A^{\ell_i}$, for each $i < n$, such that $\langle \mathbf{a}_i, \mathbf{b}_i\rangle \in \theta_i^{\ell_i}$. Let t be a polynomial on $\mathbf{A}$ of rank $\sum_{i<n} \ell_i$. Then, whenever

$$t(\mathbf{x}_0, \ldots, \mathbf{x}_{n-2}, \mathbf{a}_{n-1}) \,\gamma\, t(\mathbf{x}_0, \ldots, \mathbf{x}_{n-2}, \mathbf{b}_{n-1}),$$

for all choices of $\langle \mathbf{x}_0, \ldots, \mathbf{x}_{n-2} \rangle \in \{\mathbf{a}_0, \mathbf{b}_0\} \times \cdots \times \{\mathbf{a}_{n-2}, \mathbf{b}_{n-2}\} \setminus \{\langle \mathbf{b}_0, \ldots, \mathbf{b}_{n-2} \rangle\}$, we require also that

$$t(\mathbf{b}_0, \ldots, \mathbf{b}_{n-2}, \mathbf{b}_{n-1}) \,\gamma\, t(\mathbf{b}_0, \ldots, \mathbf{b}_{n-2}, \mathbf{b}_{n-1}).$$

Note that $C(\theta_0, \ldots, \theta_{n-1}; \gamma)$ holds if and only if, for all natural numbers $\ell_0, \ldots, \ell_{n-1}$, $C(\ell_0, \ldots, \ell_{n-1}; \theta_0, \ldots, \theta_{n-1}; \gamma)$ holds.

The following, too, is found in Aichinger and Mudrinski, as Lemma 5.4, but we believe our proof to be easier; the reader may agree that it has made the next result an easy consequence of Corollary 2.38, one other fundamental result, and some simple bookkeeping.

Lemma 2.40. *Let* $\mathbf{A}$ *be an algebra in a Mal'cev variety. Let* $n, \ell_0, \ldots, \ell_{n-1}$ *be natural numbers, and let* $\theta_0, \ldots, \theta_{n-1}, \gamma$ *be congruences of* $\mathbf{A}$*. Then*

$$C(\ell_0, \ldots, \ell_{n-1}; \theta_0, \ldots, \theta_{n-1}; \gamma)$$

if and only if $C(1, \ldots, 1; \theta_0, \ldots, \theta_{n-1}; \gamma)$.

Proof. The forward direction is implicit in Definition 2.39. Now, suppose that

$$C(1, \ldots, 1; \theta_0, \ldots, \theta_{n-1}; \gamma)$$

holds. From Corollary 2.38, it is sufficient to show that for all choices of pairs $\langle a_i, b_i \rangle \in \theta_i$ for $i < n$, $C(\mathrm{Cg}\langle a_0, b_0 \rangle, \ldots, \mathrm{Cg}\langle a_{n-1}, b_{n-1} \rangle; \gamma)$. Take $\langle a_i, b_i \rangle \in \mathrm{Cg}\langle a_i, b_i \rangle$ for $i < n$. We may as well assume that, for each $i < n$, $\theta_i = \mathrm{Cg}^{\mathbf{A}}\langle a_i, b_i \rangle$. Let $\mathbf{a}^i, \mathbf{b}^i$ be tuples of elements from A of length ℓ_i so that $\mathbf{a}^i \,\theta_i^{\ell_i}\, \mathbf{b}^i$ for each $i < n$. Let t be a polynomial over $\mathbf{A}$ of rank $\sum_{i<n} \ell_i$. Suppose that

$$t(\mathbf{x}^0, \ldots, \mathbf{x}^{n-2}, \mathbf{a}^{n-1}) \,\gamma\, t(\mathbf{x}^0, \ldots, \mathbf{x}^{n-2}, \mathbf{b}^{n-1}),$$

for all choices of $\langle \mathbf{x}^0, \ldots, \mathbf{x}^{n-2} \rangle \in \{\mathbf{a}^0, \mathbf{b}^0\} \times \cdots \times \{\mathbf{a}^{n-2}, \mathbf{b}^{n-2}\} \setminus \{\langle \mathbf{b}^0, \ldots, \mathbf{b}^{n-2} \rangle\}$. For each $i < n$ and $j < \ell_i$, we can find a polynomial t^i_j over $\mathbf{A}$ such that $\langle a^i_j, b^i_j \rangle =$

$\langle t^i_j(a_i), t^i_i(b_i)\rangle$. Now consider the polynomial

$$t'(x_0,\dots,x_{n-1}) := t(t^0_0(x_0),\dots,t^0_{\ell_0-1}(x_0),\dots,t^{n-1}_0(x_{n-1}),\dots,t^{n-1}_{\ell_{n-1}-1}(x_{n-1})).$$

By construction, $t'(x_0,\dots,x_{n-1}) = t(\mathbf{x}^0,\dots,\mathbf{x}^{n-1})$ for all choices of

$$\langle\langle x_0,\mathbf{x}^0\rangle,\dots,\langle x_{n-1},\mathbf{x}^{n-1}\rangle\rangle \in \{\langle a_0,\mathbf{a}^0\rangle,\langle b_0,\mathbf{b}^0\rangle\}\times\cdots\times\{\langle a_{n-1},\mathbf{a}^{n-1}\rangle,\langle b_{n-1},\mathbf{b}^{n-1}\rangle\}.$$

Thus, we find that $t'(x_0,\dots,x_{n-2},a_{n-1})\,\gamma\,t'(x_0,\dots,x_{n-2},b_{n-1})$ for all choices

$$\langle x_0,\dots,x_{n-2}\rangle \in \{a_0,b_0\}\times\cdots\{a_{n-2},b_{n-2}\}\setminus\{\langle b_0,\dots,b_{n-2}\}.$$

Thus, by $C(1,\dots,1;\theta_0,\dots,\theta_{n-1};\gamma)$, we get that

$$\begin{aligned} t(\mathbf{b}^0,\dots,\mathbf{b}^{n-2},\mathbf{a}^{n-1}) &= t'(b_0,\dots,b_{n-2},a_{n-1})\\ &\gamma\, t'(b_0,\dots,b_{n-2},b_{n-1})\\ &= t(\mathbf{b}^0,\dots,\mathbf{b}^{n-2},\mathbf{b}^{n-2}). \end{aligned}$$

□

The following appears as Lemma 6.14 of Aichinger and Mudrinski (2010) and Proposition 5.7 of Opršal (2014+). We offer a new proof here, in case the reader should find it more accessible than the others (but we make no promise about this, however.)

Proposition 2.41. *Let* $\mathbf{A}$ *be an algebra in Mal'cev variety* $\mathcal{V}$. *For each natural number* n, *let* q_n *be term defined as above for* $\mathcal{V}$. *Let* n *and* k *be any natural numbers with* $k \le n$. *Let* $\theta_0,\dots,\theta_{n-1} \in \operatorname{Con}\mathbf{A}$. *Then*

$$S(S(\theta_0,\dots,\theta_{k-1}),\theta_k,\dots,\theta_{n-1}) \subseteq S(\theta_0,\dots,\theta_{n-1})$$

Proof. Let t_0 be any term of rank, say, r_0. Let $\mathbf{a}_0,\dots,\mathbf{a}_{r_0-1} \in P(\theta_0,\dots,\theta_{k-1})$, where, for each $i < r_0$,

$$\mathbf{a}_i = \langle\langle a_i,b_i\rangle(\beta_s(j_i)) \mid s < 2^k\rangle,$$

where $j_i < k$ and $\langle a_i, b_i \rangle \in \theta_{j_i}$. Set $a := q_k^{\mathbf{A}}(t_0^{\mathbf{a}^{2^k-1}}(\mathbf{a}_0, \ldots, \mathbf{a}_{r_0-1}))$ and let b denote $t_0^{\mathbf{A}}(b_0, \ldots, b_{r_0-1})$. Let $\theta = \mathrm{Cg}^{\mathbf{A}}\langle a, b \rangle$. By Proposition 2.37 and Theorem 2.35, it is sufficient to show that

$$S(\theta, \theta_k, \ldots, \theta_{n-1}) \subseteq S(\theta_0, \ldots, \theta_{n-1}).$$

Take any term t_1 of rank, say r_1. Let $r = r_0 + r_1$ and let $m = n - k + 1$. Let $\mathbf{a}_{r_0}, \ldots, \mathbf{a}_{r-1} \in P(\theta, \theta_k, \ldots, \theta_{n-1})$, where, for each $i \in \{r_0, \ldots, r-1\}$,

$$\mathbf{a}_i = \langle \langle a_i, b_i \rangle (\beta_s(j_i)) \mid s < 2^m \rangle,$$

where $j_i \in \{k, \ldots, n-1\}$ and $\langle a_i, b_i \rangle \in \theta_{j_i}$. Let φ be mapping from r into n, taking $i \mapsto j_i$, which identifies the $j_i < n$ involved in the definition of each $\mathbf{a}_i$. Let

$$\mathbf{a} = \langle \langle a, b \rangle (\beta_s(0)) \mid s < 2^m \rangle.$$

It is not difficult to see that, by Corollary 2.38 and Theorem 2.35, and by changing to another polynomial t_1, if necessary, it is sufficient to show that

$$c := q_m^{\mathbf{A}}(t_1^{\mathbf{A}^{2^m-1}}(\mathbf{a}, \mathbf{a}_{r_0}, \ldots, \mathbf{a}_{r-1}))$$

is congruent, modulo $\gamma := S(\theta_0, \ldots, \theta_{n-1})$, to

$$t_1^{\mathbf{A}}(b, b_{r_0}, \ldots, b_{r-1}) =: d.$$

We shall use Theorem 2.24 (iii) $\Leftrightarrow$ (ii). To that end, we define two terms L and R of rank r by essentially substituting, for each $i < r$, a variable x_i in place of b_i in the representations of c and d, respectively, given above. We now make this explicit (which is not to say any more clear). For each $i < r_0$, define

$$\mathbf{a}'_i(x_i) := \langle \langle a_i, x_i \rangle (\beta_s(j_i)) \mid s < 2^k \rangle.$$

For each $i \in \{r_0, \ldots, r-1\}$, let

$$\mathbf{a}'_i(x_i) := \langle \langle a_i, x_i \rangle (\beta_s(j_i)) \mid s < 2^m \rangle.$$

Let a' and b' be rank r_0 polynomials on $\mathbf{A}$ given by

$$a'(x_0, \ldots, x_{r_0-1}) = q_k^{\mathbf{A}}(t_0^{\mathbf{a}^{2^k-1}}(\mathbf{a}'_0(x_0), \ldots, \mathbf{a}'_{r_0-1}(x_{r_0-1})))$$

and $b'(x_0, \ldots, x_{r_0-1}) = t_0^{\mathbf{A}}(x_0, \ldots, x_{r_0-1})$. Set

$$\mathbf{a}(x_0, \ldots, x_{r_0-1}) = \langle\langle a'(x_0, \ldots, x_{r_0-1}), b'(x_0, \ldots, x_{r_0-1})\rangle(\beta_s(0)) \mid s < 2^m\rangle.$$

Now, let $L(x_0, \ldots, x_{r-1}) :=$

$$q_m^{\mathbf{A}}(t_1^{\mathbf{A}^{2^m-1}}(\mathbf{a}(x_0, \ldots, x_{r_0-1}), \mathbf{a}'_{r_0}(x_{r_0}), \ldots, \mathbf{a}'_{r-1}(x_{r-1})))$$

and $R(x_0, \ldots, x_{r-1}) := t_1^{\mathbf{A}}(b'(x_0, \ldots, x_{r_0-1}), x_{r_0}, \ldots, x_{r-1})$.

Note that

$$\begin{aligned} L(b_0, \ldots, b_{r-1}) = q_m^{\mathbf{A}}(t_1^{\mathbf{A}^{2^m-1}}(\mathbf{a}(b_0, \ldots, b_{r_0-1}), \mathbf{a}'_{r_0}(b_{r_0}), \ldots, \mathbf{a}'_{r-1}(b_{r-1}))) \\ = q_m^{\mathbf{A}}(t_1^{\mathbf{A}^{2^m-1}}(\mathbf{a}, \mathbf{a}_{r_0}, \ldots, \mathbf{a}_{r-1})), \end{aligned}$$

while

$$R(b_0, \ldots, b_{r-1}) = t_1^{\mathbf{A}}(b'(b_0, \ldots, b_{r_0-1}), b_{r_0}, \ldots, b_{r-1}) = t_1^{\mathbf{A}}(b, b_{r_0}, \ldots, b_{r-1}).$$

Thus, since $C_2(\theta_0, \ldots, \theta_{n-1}; \gamma)$ holds, it is sufficient to show that $L(x_0, \ldots, x_{r-1}) = R(x_0, \ldots, x_{r-1})$ for all choices of

$$\langle x_0, \ldots, x_{r-1}\rangle \in \{a_0, b_0\} \times \{a_{r-1}, b_{r-1}\} \setminus \{\langle b_0, \ldots, b_{r-1}\rangle\},$$

subject to the constraints that for any $i < r$, $x_i = a_i$ if and only if for all i' such that $j_i = j_{i'}$ we have that $x_{i'} = a_{i'}$ and that $x_i = a_i$ for at least one $i < r$. Let $\langle x_0, \ldots, x_{r-1}\rangle$ be chosen according to those contraints. Let $i < r$ so that $x_i = a_i$. We show by cases. First, suppose that $j_i < k$. Then, by Proposition 2.22, we have that $\mathbf{a}(x_0, \ldots, x_{r_0-1})$ is a constant tuple. Thus, by Proposition 2.22, again, we get that $L(x_0, \ldots, x_{r-1}) = R(x_0, \ldots, x_{r-1})$. On the other hand, if $j_j \in \{k, \ldots, n-1\}$, then it is automatic from Proposition 2.22 that $L(x_0, \ldots, x_{r-1}) = R(x_0, \ldots, x_{r-1})$. $\square$

The following is gotten easily from the above, through an inductive argument.

Corollary 2.42. *Let $\theta \in \operatorname{Con} \mathbf{A}$, and let Θ be the constantly-θ ω-tuple. Then for any natural number n,*

$$[\theta)_n \subseteq S_n(\Theta).$$

In particular, if $\mathbf{A}$ is supernilpotent of class n, then it is nilpotent of class n.

Proposition 2.43. *Let $\mathbf{A}$ be an algebra in a Mal'cev variety. Then*

$$S^1(1_A) \geq S^2(1_A, 1_A) \geq \cdots \geq S^n(1_A, \ldots, 1_A) \geq S^{n+1}(1_A, \ldots, 1_A) \geq \cdots.$$

Furthermore, if $S(1_A, 1_A) = 1_A$, then $S^n(1_A, \ldots, 1_A) = 1_A$, for all $n > 1$.

Proof. The first claim is clear from Proposition 2.34. Now, suppose that $S(1_A, 1_A) = 1_A$. If for some $n > 1$, $S^n(1_A, \ldots, 1_A) = 1_A$, then by Proposition 2.41,

$$\begin{aligned} 1_A = S^n(1_A, 1_A, \ldots, 1_A) &= S^n(S(1_A, 1_A), 1_A, \ldots, 1_A) \\ &\leq S^{n+1}(1_A, \ldots, 1_A), \end{aligned}$$

whence the claim follows by induction. □

The following seems to be a new observation, but perhaps previous authors neglected to state it only since they had no use for it.

Theorem 2.44. *Let $\mathcal{V}$ be a Mal'cev variety. Let k be a natural number. Then supernilpotence of class k is preserved under HSP within $\mathcal{V}$. In particular, the subclass of all algebras in $\mathcal{V}$ that are supernilpotent of class k constitutes a subvariety.*

Proof. Closure under H is noted in Corollary 2.46, below. Closure under S and P can be seen from Proposition 2.11 or, alternatively, from Proposition 2.48 and Proposition 2.48, the latter two appearing below.

For yet another way to see this, note that supernilpotence of class k is characterizable by satisfaction of a set of equations, in a Mal'cev variety: This is evident from Theorem 2.24 (i) $\Leftrightarrow$ (ii). □

The following is an easy strengthening—but a useful one—of what appears as Lemma 6.3 in Aichinger and Mudrinski (2010). We also give a slightly different proof.

Theorem 2.45. *Let $\mathbf{A}, \mathbf{B} \in \mathcal{V}$ with $\mathcal{V}$ Mal'cev. Let h be a homomorphism of $\mathbf{A}$ onto $\mathbf{B}$. Let $\theta_0, \ldots, \theta_{n-1}$ be congruences on $\mathbf{A}$ and write $\eta = \ker h$. Then*

$$S(\theta_0, \ldots, \theta_{n-1}) \vee \eta = h^{-1} S(h(\theta_0 \vee \eta), \ldots, h(\theta_{n-1} \vee \eta)),$$

where $h^{-1}\xi$ has the usual interpretation as the set of all pairs that map into $\xi \in \operatorname{Con} \mathbf{B}$.

Proof. By the additivity of the higher commutator and Theorem 2.36, we find that

$$S(\theta_0 \vee \eta, \ldots, \theta_{n-1} \vee \eta) \vee \eta = S(\theta_0, \ldots, \theta_{n-1}) \vee \eta.$$

Thus, it suffices to prove the theorem for the case $\eta \subseteq \cap\{\theta_i \mid i < n\}$. Equivalently, we show that

$$h(S(\theta_0, \ldots, \theta_{n-1}) \vee \eta) = S(h(\theta_0), \ldots, h(\theta_{n-1})).$$

From Theorem 2.35, we have that

$$S(\theta_0, \ldots, \theta_{n-1}) \vee \eta = \mathrm{Cg}^{\mathbf{A}}\{\langle q^{\mathbf{A}}(a_0, \ldots, a_{2^n-2}), a_{2^n-1}\rangle \mid \mathbf{a} \in Q(\theta_0, \ldots, \theta_{n-1})\} \cup \eta,$$

while

$$S(h(\theta_0), \ldots, h(\theta_{n-1})) = \mathrm{Cg}^{\mathbf{B}}\{\langle q^{\mathbf{A}}(b_0, \ldots, b_{2^n-2}), b_{2^n-1}\rangle \mid \mathbf{b} \in Q(h(\theta_0), \ldots, h(\theta_{n-1}))\}.$$

It is not difficult to see, then, that h maps a set of generators for $S(\theta_0, \ldots, \theta_{n-1}) \vee \eta$ onto a set of generators for $S(h(\theta_0), \ldots, h(\theta_{n-1}))$. Thus, by Theorem A.10, we are done. $\square$

In particular, we get the following.

Corollary 2.46. *Let $\mathbf{A}$ be an algebra in a Mal'cev variety $\mathcal{V}$. Suppose that $\mathbf{A}$ is supernilpotent of class k. Then all homomorphic images of $\mathbf{A}$ are supernilpotent of class k.*

Proof. Let η be any congruence on $\mathbf{A}$. Then

$$S(1_{A/\eta}, \ldots, 1_{A/\eta}) = (S(1_A, \ldots, 1_A) \vee \eta)/\eta = \eta/\eta = 0_{A/\eta}.$$

□

The following is elementary (meaning, it can be deduced easily from the definitions);[4]

Proposition 2.47. *Let $\mathbf{A}$ be any algebra and let $\mathbf{B}$ be a subalgebra of $\mathbf{A}$. Let $\theta_0, \ldots, \theta_{n-1}$ be congruences on $\mathbf{A}$. Then*

$$S(\theta_0 \restriction_{\mathbf{B}}, \ldots, \theta_{n-1} \restriction_{\mathbf{B}}) \subseteq S(\theta_0, \ldots, \theta_{n-1}) \restriction_{\mathbf{B}}$$

Proposition 2.48. *Let $\mathbf{A}_i$ be algebras in Mal'cev variety for all $i \in I$. Let n be a natural number greater than 0. For each $j < n$, let Θ_j be an I-tuple of congruences such that $\Theta_j(i) \in \operatorname{Con} \mathbf{A}_i$ for each $j < n$ and $i \in I$. Then*

$$S(\Pi_I \Theta_0(i), \ldots, \Pi_I \Theta_{n-1}(i)) \subseteq \Pi_I S(\Theta_0(i), \ldots, \Theta_{n-1}(i)).$$

Proof. If $n = 1$, then the claim is a trivial result of Definition 2.27. For each $i \in I$, let π_i be the i^{th} projection function. Arguing by elements, we have that for any I-tuple Θ of congruences such that $\Theta(i) \in \operatorname{Con} \mathbf{A}_i$ for each $i \in I$,

$$\Pi_I \Theta(i) = \bigcap_I \pi_i^{-1}(\Theta(i)).$$

Thus, the claim reduces to showing that

$$S\left(\bigcap_I \pi_i^{-1} \Theta_0(i), \ldots, \bigcap_I \pi_i^{-1} \Theta_{n-1}(i)\right) \subseteq \bigcap_I \pi_i^{-1} S(\Theta_0(i), \ldots, \Theta_{n-1}(i)).$$

By Theorem 2.45, we have that

$$\bigcap_I \pi_i^{-1} S(\Theta_0(i), \ldots, \Theta_{n-1}(i)) = \bigcap_I S(\pi_i^{-1} \Theta_0(i), \ldots, \pi_i^{-1} \Theta_{n-1}(i)) \vee \ker \pi_i.$$

[4] Also, I am not aware of it appearing in the literature before now.

Thus, we need only show that for each $j \in I$,

$$S\left(\bigcap_I \pi_i^{-1}\Theta_0(i), \ldots, \bigcap_I \pi_i^{-1}\Theta_{n-1}(i)\right) \subseteq S(\pi_j^{-1}\Theta_0(j), \ldots, \pi_j^{-1}\Theta_{n-1}(j)) \vee \ker \pi_j.$$

But, this last inclusion follows from the monotonicity of any higher commutator. $\square$

2.5 Supernilpotence and commutator polynomials

We now undertake work that will support the results of Aichinger and Mudrinski (2010) that we used in the proof of Theorem 2.30, our broadening of Freese and Vaughan-Lee's finite basis result. We have found that we may be able to more easily present the key lemmas leading into the results of Aichinger and Mudrinski of our present interest. What's more, we have found that we can strengthen several of them.

Lemma 2.49. *Let n be a natural number. Let $\mathbf{A}$ be any algebra in a congruence-regular, Mal'cev variety $\mathcal{V}$. Let q_n be a term for $\mathcal{V}$ as defined above. Then the following are equivalent:*

(i) $C^n(1_A, \ldots, 1_A; 0_A)$

(ii) *Let $b_0, \ldots, b_{n-1}, a, c \in \operatorname{Con} \mathbf{A}$, and let $t \in \operatorname{Pol}_n \mathbf{A}$. Let t' represent the polynomial of rank n on $\mathbf{A}^{2^n-1}$ given by*

$$t'(\mathbf{x}_0, \ldots, \mathbf{x}_{n-1}) = \langle t(\mathbf{x}_0(i), \ldots, \mathbf{x}_{n-1}(i)) \mid i < 2^n - 1\rangle,$$

where $\mathbf{x}_0, \ldots, \mathbf{x}_{n-1} \in A^{2^n-1}$. For each $i < n$, write

$$\mathbf{a}_i = \langle \langle a, b_i\rangle(\beta_j(i)) \mid j < 2^n\rangle.$$

Then $q_n^{\mathbf{A}}(t'(\mathbf{a}_0^\circ, \ldots, \mathbf{a}_{n-1}^\circ)) = t(b_0, \ldots, b_{n-1})$.

(iii) *For all $t, s \in \operatorname{Pol}_n \mathbf{A}$ and all $b_0, \ldots, b_{n-1}, a \in A$, if, for all choices of*

$$\langle x_0, \ldots, x_{n-1}\rangle \in \{a, b_0\} \times \cdots \times \{a, b_{n-1}\} \setminus \{\langle b_0, \ldots, b_{n-1}\rangle\},$$

we have that $s^{\mathbf{A}}(x_0, \ldots, x_{n-1}) = t^{\mathbf{A}}(x_0, \ldots, x_{n-1})$*, then we have that*

$$s^{\mathbf{A}}(b_0, \ldots, b_{n-1}) = t^{\mathbf{A}}(b_0, \ldots, b_{n-1}),$$

as well.

Proof. That (i) $\Rightarrow$ (ii) holds is clear from Theorem 2.24 ((i) $\Rightarrow$ (ii)) of which this is a special case. Showing that (ii) $\Rightarrow$ (iii) involves computation similar to one used in the proof of Lemma 2.15:

Take $s, t \in \operatorname{Pol}_n \mathbf{A}$. Let $b_0, \ldots, b_{n-1}, a \in A$. Suppose that, for all choices of

$$\langle x_0, \ldots, x_{n-1} \rangle \in \{a, b_0\} \times \cdots \times \{a, b_{n-1}\} \setminus \{\langle b_0, \ldots, b_{n-1} \rangle\},$$

we have that $s^{\mathbf{A}}(x_0, \ldots, x_{n-1}) = t^{\mathbf{A}}(x_0, \ldots, x_{n-1})$. For each $i < n$, write $\mathbf{a} = \langle \langle a, b_i \rangle (\beta_j(i)) \mid j < 2^n \rangle$. Let $t', s' \in \operatorname{Pol}_n \mathbf{A}^{2^n - 1}$ be defined as in (ii). Then, we have that

$$\begin{aligned} s(b_0, \ldots, b_{n-1}) &= q_n^{\mathbf{A}}(s'(\mathbf{a}_0^{\circ}, \ldots, \mathbf{a}_{n-1}^{\circ}) \\ &= q_n^{\mathbf{A}}(t'(\mathbf{a}_0^{\circ}, \ldots, \mathbf{a}_{n-1}^{\circ}) \\ &= t(b_0, \ldots, b_{n-1}). \end{aligned}$$

Now, assume that (iii) holds. By Theorem 2.38, to show $C^n(1_A, \ldots, 1_A; 0_A)$, it is sufficient to show that, for all pairs $\langle a_0, b_0 \rangle, \ldots, \langle a_{n-1}, b_{n-1} \rangle \in A^2$,

$$C(\operatorname{Cg}^{\mathbf{A}}\langle a_0, b_0 \rangle, \ldots, \operatorname{Cg}^{\mathbf{A}}\langle a_{n-1}, b_{-1} \rangle; 0_A)$$

holds. However, since $\mathbf{A}$ is congruence regular, we may assume that $a_i = a$ for each $i < n$, for some $a \in A$. We now use a strategy similar to that employed in the proof of Proposition 2.12.

Let $t \in \operatorname{Pol}_n \mathbf{A}$. Suppose that

$$t(x_0, \ldots, x_{n-2}, a) = t(x_0, \ldots, x_{n-2}, b_{n-1}),$$

for all choices of

$$\langle x_0, \dots, x_{n-2}\rangle \in \{a, b_0\} \times \cdots \times \{a, b_{n-2}\} \setminus \{\langle b_0, \dots, b_{n-2}\rangle\}.$$

Let L be the polynomial on $\mathbf{A}$ defined by

$$\ell(x_0, \dots, x_{n-1}) = t(x_0, \dots, x_{n-2}, a).$$

Let $R := t$. Observe that if $x_{n-1} = a$, then, for any $x_0, \dots, x_{n-2} \in A$,

$$L(x_0, \dots, x_{n-1}) = t(x_0, \dots, x_{n-1}, a) = R(x_0, \dots, x_{n-1}).$$

On the other hand, if

$$\langle x_0, \dots, x_{n-1}\rangle \in \{a, b_0\} \times \cdots \times \{a, b_{n-1}\} \setminus \{\langle b_0, \dots, b_{n-1}\rangle\},$$

but with $x_i = a$ for some $i < n-1$ and $x_{n-1} = b_{n-1}$, then, too,

$$L(x_0, \dots, x_{n-1}) = t(x_0, \dots, x_{n-2}, a) = t(x_0, \dots, x_{n-2}, b_{n-1}) = R(x_0, \dots, x_{n-1}).$$

Then, by (iii), we get that

$$t(b_0, \dots, b_{n-2}, a) = L(b_0, \dots, b_{n-1}) = R(b_0, \dots, b_{n-1}) = t(b_0, \dots, b_{n-1}),$$

as we wished. $\square$

Definition 2.50. Let $\mathbf{A}$ be an algebra. Let n be a natural number. Let w be a polynomial for $\mathbf{A}$ in the variables $\{x_0, \dots, x_{n-1}, z\}$. We say that w is a *commutator polynomial of rank n* provided that whenever δ is a substitution that sends x_i to z for at least one $i < n$, we have that for all $b_0, \dots, b_{n-1}, a \in A$

$$\delta w(b_0, \dots, b_{n-1}, a) = a.$$

If w is a term operation, then we say that it is a *commutator term operation.* If $w = z$, then we say that w is trivial.

Theorem 2.51. *Let $\mathbf{A} \in \mathcal{V}$, a variety with Mal'cev term p. Suppose also that there is a ternary term f for $\mathcal{V}$ such that*

$$\mathcal{V} \models f(p(u,x,y),y,x) \approx u \wedge f(u,u,x) \approx x.$$

Then $\mathbf{A}$ is supernilpotent of class n if and only if all commutator polynomials for $\mathbf{A}$ of rank n or higher are trivial.

Proof. Suppose first that $\mathbf{A}$ is supernilpotent of class n. By Theorem 2.24 ((i) $\Leftrightarrow$ (iii)), we have that $C_2^n(1_A,\ldots,1_A;0_A)$ holds. But from this, it is easy to see that all commutator polynomials for $\mathbf{A}$ of rank n or higher are trivial.

For the converse, we shall use Lemma 2.49 ((i) $\Leftrightarrow$ (ii)). Let $t \in \operatorname{Pol}_n \mathbf{A}$. Let t' be defined as in Lemma 2.49, (ii). For each $i < n$, set $\mathbf{x}_i = \langle\langle z, x_i\rangle(\beta_j(i)) \mid j < 2^n\rangle$. Let q_n be the term for $\mathbf{A}$ defined as above. Let $v \in \operatorname{Pol}_{n+1}\mathbf{A}$ be defined by

$$v(\mathbf{x},z) = v(x_0,\ldots,x_{n-1},z) = q_n^{\mathbf{A}}(t'(\mathbf{x}_0,\ldots,\mathbf{x}_{n-1})).$$

Now, set $w(x_0,\ldots,x_{n-1},z) = p^{\mathbf{A}}(v(\mathbf{x},z),t(\mathbf{x}),z)$. We claim that w is a a commutator polynomial for $\mathbf{A}$.

Say that δ is a substitution map for $\operatorname{Pol}\mathbf{A}$ that maps x_i to z, for at least one $i < n$. Let $S = \{i < n \mid \delta x_i = z\}$. Let δ act coordinatewise on $(\operatorname{Pol}\mathbf{A})^I$, for whatever I. Let $r = \sum_{i \notin S} 2^i$, and hence $\beta_r(i) = 0$ if and only if $i \in S$. Note that for any $i < n$ and $j < 2^n$,

$$\begin{aligned}
\delta\mathbf{x}_i(j) &= \delta\langle z, x_i\rangle(\beta_j(i)) \\
&= \begin{cases} z & \text{if } \beta_j(i) = 0 \text{ or if } i \in S \\ x_i & \text{otherwise} \end{cases} \\
&= \begin{cases} z & \text{if } \beta_j(i) = 0 \text{ or if } \beta_r(i) = 0 \\ x_i & \text{otherwise} \end{cases} \\
&= \langle z, x_i\rangle(\beta_{j\wedge r}(i)).
\end{aligned}$$

Thus, for each $i < n$ and $j < 2^n$, $\delta\mathbf{x}_i(j) = \mathbf{x}_i(j \wedge r)$. As a special case of this, note also that, for any $i < n$,

$$\begin{aligned}
\mathbf{x}_i(r) &= \langle z, x_i \rangle(\beta_r(i)) \\
&= \begin{cases} z \text{ if } i \in S \\ \\ x_i \text{ if } i \notin S, \end{cases}
\end{aligned}$$

and hence $t'(\mathbf{x}_0, \ldots, \mathbf{x}_{n-1})(r) = t(\mathbf{x}_0(r), \ldots, \mathbf{x}_{n-1}(r)) = \delta t(x_0, \ldots, x_{n-1}))$. Thus, using also Proposition 2.18, we have that

$$\begin{aligned}
\delta q_n^{\mathbf{A}}(t'(\mathbf{x}_0, \ldots, \mathbf{x}_{n-1})) &= q_n^{\mathbf{A}}(t'(\delta\mathbf{x}_0, \ldots, \delta\mathbf{x}_{n-1})) \\
&= q_n^{\mathbf{A}}(\langle t(\delta\mathbf{x}_0(j), \ldots, \delta\mathbf{x}_{n-1}(j)) \mid j < 2^n - 1) \\
&= q_n^{\mathbf{A}}(\langle t(\mathbf{x}_0(j \wedge r), \ldots, \mathbf{x}_{n-1}(j \wedge r)) \mid j < 2^n - 1\rangle) \\
&= (\bar{\varepsilon}_r q_n)^{\mathbf{A}}(t'(\mathbf{x}_0, \ldots, \mathbf{x}_{n-1})) \\
&= t'(\mathbf{x}_0(r), \ldots, \mathbf{x}_{n-1}(r)) \\
&= \delta t(x_0, \ldots, x_{n-1}).
\end{aligned}$$

Using that p is a Mal'cev term, then, it is easily follows that $\delta w(x_0, \ldots, x_{n-1}, z) = z$; thus, by the choice of δ, w is commutator polynomial. Since w is of rank n, we thus get that $w = z$, by assumption. By hypothesis, then, we get that

$$\begin{aligned}
q_n^{\mathbf{A}}(t'(\mathbf{x}_0, \ldots, \mathbf{x}_{n-1})) &= v(\mathbf{x}, z) \\
&= f^{\mathbf{A}}(p^{\mathbf{A}}(v(\mathbf{x}, z), t(\mathbf{x}), z), z, t(\mathbf{x})) \\
&= f^{\mathbf{A}}(w(\mathbf{x}, z), z, t(\mathbf{x})) \\
&= f^{\mathbf{A}}(z, z, t(\mathbf{x})) \\
&= t(\mathbf{x}).
\end{aligned}$$

By Lemma 2.49 ((i) $\Leftrightarrow$ (ii)), then, we find that $\mathbf{A}$ is supernilpotent of class n. $\square$

Corollary 2.52. *Let n be a natural number. Let $\mathbf{A}$ be an algebra in a Mal'cev variety. Then $\mathbf{A}$ is supernilpotent of class n if and only if it is nilpotent of class n and all of its commutator polynomials of rank n or higher are trivial.*

Proof. The forward direction follows from the above, together with Corollary 2.42. To see the reverse direction, recall that from Theorem A.47, we get a term f for $\mathcal{V} = \operatorname{Var}\mathbf{A}$ as described in the hypotheses of Theorem 2.51. The corollary then follows from this latter result. □

Corollary 2.53. *Let $\mathbf{G}$ be a group. Then $\mathbf{G}$ is nilpotent of class n if and only if it is supernilpotent of class n.*

There is more than one way to see this last result; it can be deduced from Aichinger and Mudrinski (2010), Lemma 7.6, together with the well-known fact that nlipotent groups factor as the direct product of their Sylow subgroups, and so we do not supply a proof here. Rather, we would like to point out that our description of supernilpotence given by Theorem 2.24 (ii) is exactly parallel to a characterization of nilpotence in groups that is implicit in Higman's Lemma, as given in 33.42 and 33.44 in Neumann (1967). That is to say, the terms constructed in 33.42, there, are precisely those given in Theorem 2.24 (ii), but with the identity element appearing in key places. For instance (consider the "$n = 2$" case), 33.44 says (almost) directly that, for any binary term $t(x, y)$ in the language of groups, any group $\mathbf{A}$, and any $x, y \in A$

$$t^{\mathbf{A}}(x, y) \equiv q_2^{\mathbf{A}}(t^{\mathbf{A}}(1, 1), t^{\mathbf{A}}(1, y), t^{\mathbf{A}}(x, 1)) \mod [1_A, 1_A],$$

where $q_2(x, y, z) := y \cdot x^{-1} \cdot z$. A similar expression holds true with another $n > 1$ in place of 2.

2.6 Some possible applications to Problem 1.3

We turn now to some results that we have targeted out of an interest in pursuing an Oates-Powell-proof style strategy in pursuing the question of whether any finite, nilpotent, Mal'cev algebra of finite signature might generate a finitely based variety. Indeed, contained in this section is the result on critical algebras in Mal'cev varieties which was our original motivation for considering the higher two-term condition given above, as well as the strong n-cube terms.

2.6.1 The super-Fitting congruence

In the proof of the finite basis result of Oates and Powell, some key facts concerning the Fitting subgroup of a group come in to play. For further explanation of our interest here, see Neumann (1967), Lemma 52.42. Recall that the Fitting subgroup of a given group $\mathbf{G}$ is the largest nilpotent, normal subgroup of $\mathbf{G}$ (if it has one).

It is our hope that an analysis of the highest supernilpotent congruence of a given, (nilpotent) Mal'cev algebra might reveal combinatorial relationships paralleling those that hold concerning Fitting subgroups. But to begin with, we offer a demonstration of when such an object—a "super-Fitting congruence," if you like—is available.

Theorem 2.54. *Let $\mathbf{A}$ be an algebra in a Mal'cev variety. Then the join of any two supernilpotent congruences of $\mathbf{A}$ is also supernilpotent. Furthermore, if*

(i) every ascending chain in $\operatorname{Con}\mathbf{A}$ contains its least upper bound (which is also its union)

(ii) or if all supernilpotent congruences on $\mathbf{A}$ are of supernilpotence class m,

then $\mathbf{A}$ has a unique highest supernilpotent congruence.

Proof. Let α and β be congruences of $\mathbf{A}$ of supernilpotence class n and m, respectively. We claim that $\alpha \vee \beta$ is supernilpotent of class $n+m$. Let $\theta = \alpha \vee \beta$ and let $\Theta = \langle \theta \mid i \in \omega \rangle$.

By Propositions 2.36 and 2.33, it is not difficult to see that

$$S_{n+m}(\Theta) = \bigvee_{i \leq n+m} S_{n+m}(\Gamma_i),$$

where, for each $i \leq n+m$, we define Γ_i as the $(n+m)$-tuple of congruences given by

$$\Gamma_i(j) = \begin{cases} \alpha & \text{if } j < i \\ \\ \beta & \text{otherwise} . \end{cases}$$

However, by Proposition 2.34, we have that, for $i \geq n$, $S_{n+m}(\Gamma_i) \subseteq S_n(\alpha, \ldots, \alpha) = 0_A$, while, for $i < n$, $S_{n+m}(\Gamma_i) \subseteq S_m(\beta, \ldots, \beta) = 0_A$. Thus, $S_{n+m}(\Theta) = 0_A$, and so $\alpha \vee \beta$ is indeed supernilpotent of class $n+m$, as claimed.

Now, let $\mathcal{F}$ be the set of all supernilpotent congruences of $\mathbf{A}$. Clearly, $\mathcal{F}$ is nonempty, since $0_A \in \mathcal{F}$. Let $\mathcal{C}$ be a nonempty chain in $\mathcal{F}$. If $\mathbf{A}$ is such that every chain of congruences contains its union, then, of course, $\cup\mathcal{C} \in \mathcal{C} \subseteq \mathcal{F}$. On the other hand, it is well known that the union of a chain of congruences is again a congruence. Suppose now that every supernilpotent congruence on $\mathbf{A}$ is of supernilpotence class m. We claim that $\theta := \cup\mathcal{C}$ is as well. We will show that $C^m(\theta, \ldots, \theta; 0_A)$. Let $\ell_0, \ldots, \ell_{m-1}$ be natural numbers, and choose a term t for $\mathbf{A}$ of rank $\sum_{i<m} \ell_i$. For each $i < m$, choose $\mathbf{a}_i, \mathbf{b}_i \in A^{\ell_i}$ such that $\mathbf{a}_i \, \theta^{\ell_i} \, \mathbf{b}_i$. Now, suppose that for each choice of

$$\langle \mathbf{x}_0, \ldots, \mathbf{x}_{m-2} \rangle \in \{\mathbf{a}_0, \mathbf{b}_0\} \times \cdots \times \{\mathbf{a}_{m-2}, \mathbf{b}_{m-2}\} \setminus \{\langle \mathbf{b}_0, \ldots, \mathbf{b}_{m-2} \rangle\},$$

we have that

$$t^{\mathbf{A}}(\mathbf{x}_0, \ldots, \mathbf{x}_{m-2}, \mathbf{a}_{m-1}) = t^{\mathbf{A}}(\mathbf{x}_0, \ldots, \mathbf{x}_{m-2}, \mathbf{b}_{m-1}).$$

Now, since $\theta = \cup\mathcal{C}$, for each $i < m$, we obtain $\theta_i \in \mathcal{C}$ such that $\mathbf{a}_i \, \theta_i^{\ell_i} \, \mathbf{n}_i$. Since $\mathcal{C}$ is a chain, we obtain an $i < n$ such that, for all $j < n$, $\theta_j \subseteq \theta_i$. Let $\psi = \theta_i$. Now, since $\psi \in \mathcal{C}$ is supernilpotent of class m and hence $C^m(\psi, \ldots, \psi; 0_A)$ holds, we may conclude from the equations above that

$$t^{\mathbf{A}}(\mathbf{b}_0, \ldots, \mathbf{b}_{n-2}, \mathbf{a}_{n-1}) = t^{\mathbf{A}}(\mathbf{b}_0, \ldots, \mathbf{b}_{n-2}, \mathbf{b}_{n-1}).$$

Thus, we find, too, that $C^m(\cup\mathcal{C}, \ldots, \cup\mathcal{C}; 0_A)$. Thus, $\cup\mathcal{C} \in \mathcal{F}$.

Thus, in case (i) or (ii) holds, we can apply Zorn's Lemma to obtain a maximal element of $\mathcal{F}$, that is, a maximal supernilpotent congruence on $\mathbf{A}$. But, of course, from the first part of this theorem, this maximal congruence must be unique. $\square$

2.6.2 A promising consequence of criticality in Mal'cev varieties

My own motivation for considering many of the notions in this chapter—especially those concerning the two-term condition and the terms q_n built from a Mal'cev term—was to get the result in this subsection. In the Oates-Powell proof, we find one of the key steps involves a combinatorial feature of any critical group, as seen in Theorem 51.37 and Corollary 51.38 in Neumann (1967). It seems to us that a key deficit in the generalization of the Oates-Powell proof has been a lack of information concerning critical algebras. However, below, we offer what seems to be a satisfactory generalization of Theorem 51.37 from Neumann (1967); it is our hope that it might find application in answering Problem 1.3.

Let $\mathbf{A}$ be any algebra in a congruence regular, Mal'cev variety. Let $\mathbf{L}$ be a subalgebra of $\mathbf{A}$. Let $\theta_0, \dots, \theta_{n-1}$ be congruences of $\mathbf{A}$. For each $i < n$, pick some congruence block B_i of θ_i that intersects L. Since $\mathbf{A}$ is congruence regular, we have that B_i determines θ_i for each $i < n$; that is, $\theta_i = \operatorname{Cg} B_i^2$. Let Z be a set (to symbolize variables) duplicating L. Write $Z = \{z_a \mid a \in L\}$. For each $i < n$, let X^i be a set (to symbolize variables) duplicating B_i. For each $i < n$, write $X^i = \{x_a^i \mid a \in B_i\}$. For each $i < n$, choose a $b_i \in B_i \cap L$. Note that $\operatorname{Cg} B_i^2 = \operatorname{Cg}\{\langle b_i, a\rangle \mid a \in B_i\}$. Let C be a set of symbols duplicating A; these are to symbolize constants. Write $C = \{c_a \mid a \in A\}$.

For each $i < n$ define an endomorphism δ_i on the algebra $\mathbf{T}$ of terms in $Z \cup \bigcup_{i \in \omega} X^i \cup C$ by homomorphically extending its action on the variables, given as follows. For each $i < n$, let

$$\delta_i x_a^i = z_{b_i},$$

for each $a \in B_i$, while fixing all other variables and constants. We also define, for each $r < 2^n$, an endomorphism η_r of $\mathbf{T}$ to be the product of maps, $\eta_r = \delta_0' \cdots \delta_{n-1}'$, where $\delta_i' = \delta_i$ if $\beta_r(i) = 0$ and is the identity map otherwise. Also, for convenience, let $\eta := \eta_0$.

Let α be the assignment map from T into $\mathbf{A}$ given by letting, for any $a \in L$, $\alpha z_a = a$ and, for each $i < n$ and for all $a \in B_i$, $\alpha x^i_a = a$ and, for each $a \in A$, $\alpha c_a = a$.

Now, let T' be the set of all terms t in T such that $\alpha\eta t \in L$. Note that since L is closed under the operations of $\mathbf{A}$ and $\alpha\eta$ is a homomorphism (as an assignment map always is), we get that T' is closed under the operations of $\mathbf{T}$.

Lemma 2.55. *With the notation defined as above, we have that α maps T' onto $L\theta_0 \cdots \theta_{n-1}$, while for each $i < n$, $\alpha\delta_i$ maps T' into $L\theta'_0 \cdots \theta'_{n-2}$, where $\theta'_0, \ldots, \theta'_{n-2}$ is a list of the elements in $\{\theta_0, \ldots, \theta_{n-1}\} \setminus \{\theta_i\}$.*

Proof. Note that since $\mathbf{A}$ is congruence permutable, for any congruences $\gamma_0, \ldots, \gamma_{m-1}$ on $\mathbf{A}$, $L\gamma_0 \cdots \gamma_{m-1} = L\gamma$, with $\gamma = \gamma_0 \vee \cdots \vee \gamma_{n-1}$. Thus, this lemma is easy to see from our construction of T' together with Proposition A.26; we need the fact that $\theta_i = \mathrm{Cg}\{\langle b_i, a\rangle | a \in B_i\}$ for each $i < n$ to show onto. $\square$

Theorem 2.56. *Let $\mathbf{A}$ be any congruence regular algebra in a Mal'cev variety. Let $\mathbf{L} \leq \mathbf{A}$. Let $\theta_0, \ldots, \theta_{n-1}$ be congruences on $\mathbf{A}$ such that $S(\theta_0, \ldots, \theta_{n-1}) = 0_A$, $A = L\theta_0 \ldots \theta_{n-1}$, and for any $i < n$ the expansion of L by $\bigvee\{\theta_0, \ldots, \theta_{n-1}\} \setminus \{\theta_i\}$ is a proper subset of A. Then $\mathbf{A}$ is not critical.*

Proof. By hypothesis, and Lemma 2.55, we have that for each $r : 0 < r < 2^n$, $\mathbf{C}_r := \alpha\eta_r\mathbf{T}'$ is a proper subalgebra of $\mathbf{A}$.

Let $\gamma : T' \to \Pi_{r:0<r<2^n}\mathbf{C}_r$ be given by $\gamma t = \langle \alpha\eta_r t \mid 0 < r < 2^n\rangle$. We claim that $\ker\gamma \subseteq \ker\alpha$. After all, if $\gamma t = \gamma s$ for $s, t \in T'$, we have by $C_2(\theta_0, \ldots, \theta_{n-1}; 0_A)$ that $\alpha t = \alpha s$.

It follows that $\mathbf{A}$ is a homomorphic image of a product of its proper subalgebras. Thus, $\mathbf{A}$ is not critical. $\square$

Chapter 3

Toward a finite basis result for finite, nilpotent, Mal'cev algebras

Recall that to establish that a given locally finite variety of finite signature $\mathcal{V}$ is finitely based, it is sufficient to show that, for some natural number N, $\mathcal{V}^{(N)}$ is locally finite and has a finite critical bound—or, put another way, it has only finitely many critical algebras. (See the discussion following Theorem A.6.)

In fact, we can do the first of these tasks for $\mathcal{V}$ a locally finite, Mal'cev variety of finite signature comprised solely of algebras of uniform nilpotence class n, for some n. We begin this chapter with this result and then continue onward, establishing results inspired by the Oates-Powell proof of the fact that all finite groups have a finitely based equational theory, which may represent the start of an Oates-Powell-style proof answering in the affirmative the question whether or not all finite nilpotent, Mal'cev algebras also have a finitely based equational theory.

3.1 Lifting local finiteness

Theorem 3.1. *Let* $\mathbf{A}$ *be a finitely generated algebra of finite signature with congruence* θ *of finite index. Then* θ *is finitely generated.*

Furthermore, a generating set may be found of size bounded in terms of the size of the finite-generating set of $\mathbf{A}$*, the index of* θ*, the signature of* $\mathbf{A}$*, and the arity of its operation symbols.*

Proof. Suppose $\mathbf{A}$ is generated by finite $X \subseteq A$, and that $\theta \in \operatorname{Con} \mathbf{A}$ is of finite index. Let T be a transversal of the θ-classes. Let Γ_0 be the set of all pairs of the form $\langle b', b\rangle$ where $b' = Q^{\mathbf{A}}(b_0, \ldots, b_{r-1})$ for some fundamental operation symbol Q in the signature of $\mathbf{A}$ (with whatever rank, r), $\{b_0, \ldots, b_{r-1}\} \subseteq T$, and b is the unique θ-representative of b' drawn from T. Let $\Gamma_1 := \{\langle a, b\rangle \in \theta \mid a \in X, b \in T\}$. Let $\Gamma := \Gamma_0 \cup \Gamma_1$, and note that, by our hypotheses, Γ is finite. We shall estimate the size of Γ at the conclusion of the proof. We claim that $\theta = \operatorname{Cg}^{\mathbf{A}} \Gamma$. By construction, $\Gamma \subseteq \theta$; so, we need only verify that $\theta \subseteq \operatorname{Cg}^{\mathbf{A}} \Gamma$.

Take $\langle a, b\rangle \in \theta$. By the symmetry and transitivity of $\operatorname{Cg}^{\mathbf{A}} \Gamma$, we need only show the case that $b \in T$, using, of course, too, that T is a transversal for θ. Since $\mathbf{A}$ is generated by X, we can write $a = t^{\mathbf{A}}(a_0, \ldots, a_{m-1})$ for some term t of rank, say, m and $\{a_0, \ldots, a_{m-1}\} \subseteq X$. Write $\mathbf{a}$ for $\langle a_0, \ldots, a_{m-1}\rangle$.

We induct on the complexity of t. The basis step consists of two cases, corresponding to the two possibilities for t: It is either a variable or a constant. First, suppose that t is a variable. Then, $a = a_i \in X$, for some i, and hence $\langle a, b\rangle \in \Gamma_1$. Now, suppose that t is a constant. Then $a = c^{\mathbf{A}}$, for some nullary operation symbol c in the signature of $\mathbf{A}$. This puts $\langle a, b\rangle \in \Gamma_0$, by construction.

For the inductive step, suppose that $t = Qt_0 \ldots t_{q-1}$ for some fundamental operation symbol Q of rank q and each t_i a term. Adopting an inductive hypothesis, we assume that for each $i < q$, $\langle t_i(\mathbf{a}), b_i\rangle \in \operatorname{Cg}^{\mathbf{A}} \Gamma$, where b_i is the unique θ-representative of $t_i(\mathbf{a})$ in T. Since $\operatorname{Cg}^{\mathbf{A}} \Gamma$ respects the operations of $\mathbf{A}$, we get that

$$a = Q^{\mathbf{A}}(t_0^{\mathbf{A}}(\mathbf{a}), \ldots, t_{q-1}^{\mathbf{A}}(\mathbf{a})) \operatorname{Cg}^{\mathbf{A}} \Gamma \cap \theta \; Q^{\mathbf{A}}(b_0, \ldots, b_{q-1}) \; \Gamma_0 \; b.$$

Thus, by the transitivity of $\operatorname{Cg}^{\mathbf{A}} \Gamma$, we have that $\langle a, b\rangle \in \operatorname{Cg}^{\mathbf{A}} \Gamma$. It follows that, $\theta \subseteq \operatorname{Cg}^{\mathbf{A}} \Gamma$, which proves the first part of the theorem.

For the second part, let n be the cardinality of the generating set X of $\mathbf{A}$. Let p be the number of fundamental operation symbols given by the signature, and let R be their maximum arity. Finally, let $t := |T|$. Then, as we found that θ was generated by

$\Gamma = \Gamma_0 \cup \Gamma_1$, we need only count each of these. It is not difficult to see that $|\Gamma_0| \leq p \cdot t^R$ and that $|\Gamma_1| = n$. Thus, we note, for convenience that $|\Gamma| \leq n + t \cdot p^R$. $\square$

For a given algebra $\mathbf{A}$ and $\alpha, \beta \in \operatorname{Con} \mathbf{A}$, we define a congruence Δ^{α}_{β} on $\boldsymbol{\beta}$ by

$$\Delta^{\alpha}_{\beta} := \operatorname{Cg}^{\boldsymbol{\beta}}\{\langle \langle a, a \rangle, \langle b, b \rangle \rangle \mid a \, \alpha \, b\}.$$

The following is a consequence of Proposition 7.1 from Freese and McKenzie 1987; however, the proof of this particular detail is omitted in their exposition, so we record it here for convenience.

Theorem 3.2. *Let* $\mathbf{A}$ *be any algebra in a variety with a difference term,* d*. Let* ζ *be the center of* $\mathbf{A}$*, and let 1 denote its highest congruence. Then*

$$|A| = \left|\zeta / \Delta^1_{\zeta}\right| \cdot |A/\zeta| \, .$$

Proof. Let T be a transversal of the ζ-classes of A, and write $r(a)$ for the unique ζ-representative from T of a given $a \in A$. We use the following map $\pi : A \to \zeta/\Delta^1_{\zeta} \times A/\zeta$: $\pi(x) = \langle \langle x, r(x) \rangle / \Delta^1_{\zeta}, x/\zeta \rangle$, for a given $x \in A$. Suppose that $\pi(x) = \pi(y)$. Then, evidently, $x \, \zeta \, y$, and hence $r(x) = r(y)$. But, then, by $\langle x, r(x) \rangle \, \Delta^1_{\zeta} \, \langle y, r(y) \rangle$ and Lemma 4.11, we get that $x = y$. Thus, we see that π is one-to-one.

Now, take any $u, v, z \in A$ with $\langle u, v \rangle \in \zeta$. We need to find an element $x \in A$ so that $\langle x, r(x) \rangle \, \Delta^1_{\zeta} \, \langle u, v \rangle$ and $x \, \zeta \, z$. We shall use $x = d(u, v, r(z))$. Note that $x = d(u, v, r(z)) \, \zeta \, r(z) \, \zeta \, z$. It follows also that $r(x) = r(z)$. Now, since ζ is abelian, we can apply d coordinate-wise, "vertically," to the pairs

$$\begin{aligned} \langle u, v \rangle \, &\Delta^1_{\zeta} \, \langle u, v \rangle \\ \langle v, v \rangle \, &\Delta^1_{\zeta} \, \langle u, u \rangle \\ \langle r(z), r(z) \rangle \, &\Delta^1_{\zeta} \, \langle u, u \rangle, \end{aligned}$$

to learn that $\langle x, r(z) \rangle \, \Delta^1_{\zeta} \, \langle u, v \rangle$, as needed. $\square$

The following is also noted by Freese and McKenzie, but it has a brief proof and so is recorded here for convenience.

Lemma 3.3. *Let* $\mathbf{A}$ *be any algebra in a congruence modular variety. Then* $\boldsymbol{\zeta}_A/\Delta_{\zeta_A}^{1_A}$ *is abelian.*

Proof. Write $\boldsymbol{\zeta} = \boldsymbol{\zeta}_A$. Also, write Δ for $\Delta_{\zeta}^{1_A}$. By Proposition 4.32, we need only show that $[1_\zeta, 1_\zeta] \subseteq \Delta$. For $i = 0, 1$, let η_i be the kernel of the i^{th} projection map from ζ onto A. Note that, for any $\langle x_0, x_1\rangle, \langle x_0', y_0'\rangle \in \zeta$, we have that

$$\langle x_0, x_1\rangle \, \eta_0 \, \langle x_0, x_0\rangle \, \Delta \, \langle x_0', x_0'\rangle \, \eta_0 \, \langle x_0', x_1'\rangle;$$

thus, $1_\zeta = \Delta \vee \eta_0$. Similarly, one can show that $1_\zeta = \Delta \vee \eta_1$. Of course, we also have that $[\eta_0, \eta_1] \subseteq \eta_0 \cap \eta_1 = 0_\zeta$. Thus, by Proposition A.31 and the additivity of the commutator in congruence modular varieties (see Theorem A.42), we have that

$$[1_\zeta, 1_\zeta] = [\Delta \vee \eta_0, \Delta \vee \eta_1] \subseteq \Delta,$$

as desired. □

We shall also make use of the following fact, noted in Freese and McKenzie (1987) (see equation 10, p. 83).

Theorem 3.4. *Let* $\mathbf{A}$ *be an abelian algebra in a variety with Mal'cev term* p*. Then for any* t*, a term operation on* $\mathbf{A}$ *of rank, say,* n*,*

$$\mathbf{A} \models t(x_1, \ldots, x_n) \approx t(z, \ldots, z) + \sum_{j=1}^{n} t^{(j)}(x_j, z),$$

where each $t^{(j)}$*,* $j = 1, \ldots, n$*, is a binary term operation defined by*

$$t^{(j)}(u, v) := p(t(v, \ldots, v, u, v, \ldots, v), t(v, \ldots, v), v),$$

and where $x + y := p(x, z, y)$*.*

The above has a straightforward proof that applies only the following well-known result (see McKenzie, McNulty, and Taylor (1987), Theorem 4.155).

Theorem 3.5. *Let* $\mathbf{A}$ *be an abelian algebra in a variety with Mal'cev term* p*. Let* $z \in A$*, and define operations* $x + y := p(x, z, y)$ *and* $-x := p(z, x, z)$*. Let* $R = \{r \in \operatorname{Pol}_1 \mathbf{A} \mid r(z) = z\}$*. Then* $\langle A, +, -, z, r\rangle_{r\in R}$ *is a module with underlying abelian group* $\langle A, +, -, z\rangle$*. Furthermore, for any natural number* r *and any* $s \in \operatorname{Pol}_r \mathbf{A}$ *such that* $s(z, \ldots, z) = z$*, we get the identity*

$$s(x_1, \ldots, x_r) = \sum_{i=1}^{n} s_i(x_i),$$

where each $s_i \in \operatorname{Pol}_1 \mathbf{A}$ *is defined by* $s_i(x) = s(z, \ldots, z, x, z, \ldots, z)$*, with* x *appearing in the* i^{th} *place. (Abelian algebras in a Mal'cev variety are thus called* affine*.)*

Corollary 3.6. *Let* $\mathbf{A}$ *be in* $\mathcal{V}$*, a Mal'cev variety of abelian algebras. Suppose also that* $\mathbf{A}$ *is* n*-generated, for some natural number* n*. Then*

$$|A| \leq |F_{\mathcal{V}}(1)| \cdot |F_{\mathcal{V}}(2)|^n \leq |F_{\mathcal{V}}(2)|^{n+1}.$$

Proof. We can take $F_{\mathcal{V}}(\{z\})$, $F_{\mathcal{V}}(\{y_1, \ldots, y_n\})$, and, for each $i = 1, \ldots, n$, $F_{\mathcal{V}}(\{z, y_i\})$ to be subalgebras of $F_{\mathcal{V}}(\{z, y_1, \ldots, y_n\})$. (We shall let each of the variables $z, y_1, \ldots, y_n$ denote both an index and the projection function indexed by that index; see A.1.1 for details.) Note also that $F_{\mathcal{V}}(\{z\})$ is isomorphic to $F_{\mathcal{V}}(1)$, while, for each $i = 1, \ldots, n$, $F_{\mathcal{V}}(\{z, y_i\})$ is isomorphic to $F_{\mathcal{V}}(2)$. Let S be the subset of $F_{\mathcal{V}}(\{z\}) \times F_{\mathcal{V}}(\{z, y_1\}) \times \cdots \times F_{\mathcal{V}}(\{z, y_n\})$ with elements of the form

$$\langle t(z, \ldots, z), t^{(1)}(y_1, z), \ldots, t^{(n)}(y_n, z)\rangle,$$

where t is any term operation of rank n. By Theorem 3.4, the map from S into $F := F_{\mathcal{V}}(\{y_1, \ldots, y_n\})$ defined by

$$\langle t(z, \ldots, z), t^{(1)}(y_1, z), \ldots, t^{(n)}(y_n, z)\rangle \mapsto t(z, \ldots, z) + \sum_{j=1}^{n} t^{(j)}(y_j, z)$$

is onto. Thus, $|F_{\mathcal{V}}(n)| \leq |F_{\mathcal{V}}(1)| \cdot |F_{\mathcal{V}}(2)|^n$. Since every n-generated algebra in $\mathcal{V}$ is a homomorphic image of $\mathbf{F}$, the result follows. $\square$

Given any variety $\mathcal{V}$ and for each natural number N, let $\mathcal{V}^{(N)}$ denote the variety based on the set of N-variable equations that hold across $\mathcal{V}$.

Theorem 3.7. *Let $\mathcal{V}$ be a Mal'cev variety of finite signature such that $|F_{\mathcal{V}}(2)| = m$, a natural number, and such that each of its algebras is of nilpotence class k. Let p be the number of fundamental operations provided in the signature and let R be the maximum of their ranks. There is a function $F : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ (with its definition depending on m, p, R) so that for all N high enough, for all n-generated $\mathbf{B} \in \mathcal{V}^{(N)}$ of nilpotence class $c \leq k$, $|B| \leq F(n, c)$. In particular, for all high enough N, $\mathcal{V}^{(N)}$ is locally finite, and hence $\mathcal{V}$ itself is locally finite.*

Proof. Let $\mathcal{V}$ be as described in the hypotheses. By Theorems A.21 and 4.48, we can find a natural number $N_0 \geq 2$ such that for all $N > N_0$, $\mathcal{V}^{(N)}$ is Mal'cev and so that for all $\mathbf{B} \in \mathcal{V}^{(N)}$, $\mathbf{B}$ is nilpotent of class c.

We shall define f recursively in the parameter c. For the basis step, note that if $c = 1$, we have that $\mathbf{B}$ is abelian. Then, it is not too difficult to see that we can use Corollary 3.6 to find that $|B| \leq m^{n+1}$. Thus, we set $F(n, 1) = m^{n+1}$. Now, suppose $F(n, c')$ has been defined for all $c' < c$, for some $c \leq k$, and that $F(n, c')$ provides a bound on the n-generated algebras of nilpotence class c' in $\mathcal{V}^{(N)}$. Using Theorem 3.2, we can write $|B| = |\zeta_B / \Delta_{\zeta_B}^{1_B}| \cdot |B/\zeta_B|$. Note that $\mathbf{B}/\zeta_B$ is nilpotent of class $c - 1$ (see Theorem 4.30 and Proposition 4.28) and is also, of course, n-generated. Thus, we have that the index of ζ_B is bounded by $t := F(n, c-1)$. Thus, as shown in the proof of Theorem 3.1, as a congruence, ζ_B is generated by $n + pt^R$ elements. We claim further that, as a subalgebra, $\boldsymbol{\zeta}_B$ is generated by $2n + pt^R$ elements. Indeed, from Theorem A.25, for any Mal'cev algebra $\mathbf{A}$ and $X \subseteq A \times A$, we have that

$\mathrm{Cg}^{\mathbf{A}}\, X = \mathrm{Sg}^{\mathbf{A}\times\mathbf{A}}\, X \cup 0_A$. In light of the fact that 0_A is n-generated in $\mathbf{A} \times \mathbf{A}$, the claim is apparent.

By Lemma 3.3, $\boldsymbol{\zeta}_B/\Delta^{1_B}_{\zeta_B}$ is abelian. As $\boldsymbol{\zeta}_B/\Delta^{1_B}_{\zeta_B}$ is also $(2n + pt^R)$-generated, we may apply Corollary 3.6 to learn that $|\zeta_B/\Delta^{1_B}_{\zeta_B}| \leq m^{2n+pt^R+1}$, and hence $|B| \leq m^{2n+pt^R+1} \cdot t$. Thus, we set

$$F(n, c) = m^{2n+pt^R+1} \cdot t,$$

with $t = F(n, c-1)$. $\square$

3.2 Towards an Oates-Powell-style proof

The general strategy of the Oates-Powell proof, as outlined in the broadest sense by Section A.2 of Appendix A, is supplemented greatly by several properties of varieties of groups. (Our reference here for this result is Neumann (1967)). Essentially, Oates and Powell make use of the fact that for $\mathcal{V}$ a finitely generated variety of groups, there are three parameters for $\mathcal{V}$ that can be "lifted" to $\mathcal{V}^{(N)}$ for all high enough N; these include

- the exponent of $\mathcal{V}$;
- a bound on the nilpotence class of all nilpotent algebras in $\mathcal{V}$;
- a bound on cardinality of the chief factors of $\mathcal{V}$.

Our suggestion, inspired by this, is to replace, wherever helpful, the first two concepts by $|F_{\mathcal{V}}(2)|$ and the maximum supernilpotence class of all supernilpotent algebras of $\mathcal{V}$, respectively. Lifting the first parameter to $\mathcal{V}^{(N)}$ is simple: indeed, we have already put this parameter to use in our proof that $\mathcal{V}^{(N)}$ is locally finite for all high enough N, where $\mathcal{V}$ is a variety with a finite freely 2-generated algebra. However, it is not clear that the second parameter is even a property available in $\mathcal{V}$, for $\mathcal{V}$ a finitely generated Mal'cev variety of nilpotent algebras. Research in this direction appears to be a very new endeavor—however, work by Kearnes (1999) and perhaps Smith (2015) may point the way.

On the other hand, the third parameter above, as we prove below, is indeed available in $\mathcal{V}$ for $\mathcal{V}$ a Mal'cev variety of nilpotent algebras. Furthermore, if the nilpotence class k of algebras in $\mathcal{V}$ is uniformly bounded, then we can also lift this parameter to $\mathcal{V}^{(N)}$ for all large enough N. Of course, we should recall what is meant by "chief factor" in group theory, and then describe how we shall generalize this concept, following the lead of Freese and McKenzie (1981) and Freese and McKenzie (1987). For a group $\mathbf{G}$ with normal subalgebras $\mathbf{M} \prec \mathbf{N}$, $\mathbf{M}/N$ is a chief factor of $\mathbf{G}$; by "bound on the chief factor $\mathbf{M}/N$," then, it is meant a bound on $|M/N|$. Adopting our usual routine of considering congruences in favor of normal subalgebras, given an algebra $\mathbf{A}$, and congruences $\alpha \prec \beta$ of $\mathbf{A}$, we consider instead the supremum over the cardinalities of all β/α-classes in A/α; we denote this by $\operatorname{Ind}(\beta/\alpha)$. Thus, whenever for $\mathcal{V}$ there exists a cardinal κ such that $\operatorname{Ind}(\beta/\alpha) < \kappa$, for all $\mathbf{A} \in \mathcal{V}$ and all $\alpha \prec \beta$ from $\operatorname{Con} \mathbf{A}$, we say that $\mathcal{V}$ has *a bound on its chief factors.* We shall only be interested in the case of κ a natural number, however; in this case, we say that $\mathcal{V}$ has a finite bound on its chief factors.

Shortly, we prove that for any Mal'cev variety $\mathcal{V}$, consisting solely of algebras of nilpotence class k, for some natural number k, $\mathcal{V}$ has a finite bound on its chief factors. Thus, by the discussion above, "lifting" nilpotence of class k to $\mathcal{V}^{(N)}$, for all large enough N, also serves to lift the bound on the chief factors, when $\mathcal{V}$ is a Mal'cev variety of algebras of nilpotence class k. Along the way, however, we establish several other results of independent interest.

3.3 Lifting the bound on the chief factors, and other results

In the exposition of the Oates-Powell proof given in Neumann (1967), the following is noted.

Theorem 3.8. *For each natural number n, there is an equation v_n in the language of groups that is satisfied by every group of cardinality n or less and, conversely, if v_n holds in $\mathbf{G}$, then the index of the centralizer of any chief factor is n or less.*

Recall that if $\mathbf{G}$ is a group with factor $\mathbf{H}/K$, then the centralizer of $\mathbf{H}/K$ is the set of all $a \in G$ such that $ah \equiv ha \mod K$, for all $h \in H$.

Neumann (1967) refers to this v_n as the "chief centralizer law," which, for comparison, we give now. We adopt the usual notation for group operations. Let us abbreviate conjugation, writing x^y in place of $y^{-1}xy$ for variables x, y. We also let $[x, y] = x^{-1}y^{-1}xy$ abbreviate the commutator of variable elements x and y, and recursively define some iterates of this by $[x_0, \dots, x_{n-1}] = [[x_0, \dots, x_{n-2}], x_{n-1}]$, for $n > 2$. For any $n > 1$, Neumann (1967) recursively defines the terms v_n in the variables $x_1, \dots, x_n$, $y_3, \dots, y_n$, and $y_{i,j}$ $(1 \leq i < j \leq n)$ by $v_2 = [x_1, x_2, (x_1^{-1}x_2)^{y_{1,2}}]$ and, for $n > 2$, $v_n = [v_{n-1}, x_n^{y_n}, (x_1^{-1}x_n)^{y_{1,n}}, \dots, (x_{n-1}^{-1}x_n)^{y_{n-1,n}}]$. The law v_n, by usual convention, is formed by equating this term v_n to the symbol for the identity element.

We shall show that for each natural number n and for a fixed congruence modular variety $\mathcal{V}$, we can obtain a similar "chief centralizer law" (depending on $\mathcal{V}$) and a result parallel to Theorem 3.8; we have repurposed the symbol v_n for this law, which we have, in a sense, patterned after that given above. Our chief centralizer law v_n turns out to be a countably infinite set of equations, rather than a single one; on the other hand, for a Mal'cev variety $\mathcal{V}$ of algebras of nilpotence class k, for some natural number k, and for which $F_{\mathcal{V}}(2)$ is finite, we find that the law v_n is implied by a finite set of equations—namely, those given by Freese and McKenzie (1987), characterizing nilpotence of class k (see Theorem 4.48).

We construct the law using the following Mal'cev condition for congruence modular groups, given by Gumm (1983) as well as the work building on this of McKenzie (1987a). The following is

Theorem 3.9. *Let $\mathcal{V}$ be a variety. Then $\mathcal{V}$ is congruence modular if and only if there is a natural number n and ternary terms $q_0, \ldots, q_n, p$ for $\mathcal{V}$ such that the following equations hold in $\mathcal{V}$:*

1. $q_0(x, y, z) \approx x$

2. $q_i(x, y, x) \approx x$ *for* $0 \leq i \leq n$

3. $q_i(x, y, y) \approx q_i(x, y, y)$ *for even* $i < n$

4. $q_i(x, x, y) \approx q_i(x, x, y)$ *for odd* $i < n$

5. $q_n(x, y, y) \approx p(x, y, y)$

6. $p(x, x, y) \approx y$

We shall call such terms—that is, that satisfy these equations—*Gumm terms.*

Remark 3.10. It also turns out that for $\mathcal{V}$ with Gumm terms given above, p is a difference term.

Let $\mathcal{V}$ be a congruence modular variety. Let $p, q_i (i = 0, \ldots, n)$ be a set of Gumm terms for $\mathcal{V}$.

Following McKenzie (1987a), for a given natural number k and term t in $2 + k$ variables, we let S_t be the set of all $4 + k$-rank terms $s(x, y, u, v, \mathbf{z})$ including $p(t(x, u, \mathbf{z}), t(y, u, \mathbf{z}), t(y, v, \mathbf{z}))$ and, for each $i \leq n$, $q_i(t(x, v, \mathbf{z}), t(x, u, \mathbf{z}), t(y, v, \mathbf{z}))$ and $q_i(t(x, v, \mathbf{z}), t(y, u, \mathbf{z}), t(y, v, \mathbf{z}))$.

We shall make use of the following consequence of Theorem 2.7 from McKenzie (1987a).

Theorem 3.11. *Let $\mathbf{A}$ be an algebra in a congruence modular variety, with Gumm terms $p, q_i (i = 0, \ldots, n)$, for some natural number n. Let $a, b, c, d \in A$. Then*

$[\mathrm{Cg}\langle a, b\rangle, \mathrm{Cg}\langle c, d\rangle] = 0_A$ *if and only if for all natural numbers k, for all terms t in $2+k$ variables, and for all $s \in S_t$, we have*

$$s(a, b, c, d, \mathbf{e}) = s(a, b, d, d, \mathbf{e}),$$

for all k-tuples $\mathbf{e}$ of elements of A.

For any given $\mathbf{A} \in \mathcal{V}$ and $a, b, c, d \in A$, let us write $C^{\mathbf{A}}(a, b, c, d)$ if and only if $[\mathrm{Cg}\langle a, b\rangle, \mathrm{Cg}\langle c, d\rangle] = 0_A$. Note also that, by the equations for the Gumm terms fixed above, for any t and any $s \in S_t$,

$$\mathcal{V} \models s(x, x, u, v, \mathbf{z}) \approx s(x, x, v, v, \mathbf{z}). \tag{3.1}$$

Let m be a natural number. Set $\Lambda_m = \{\langle i, j\rangle \mid 0 \leq i < j < m\}$. We impose an order on $\Lambda_m \cup \{\varnothing\}$, by letting $\varnothing$ be its least element, and by letting the rest be ordered arbitrarily (or, if you like, with the dictionary order.) Let X be the usual set of variables, indexed by the natural numbers. For each $\lambda \in \Lambda_m$, let Z_λ be a countably infinite set of distinct variables. Let $Z = \cup Z_\lambda$. Also, let u, v be two more distinct variables. Let T be the set of terms in the variables $X \cup \{u, v\} \cup Z$. For convenience, for a given $\bar{t} \in T^{\Lambda_m}$, set $S^{\bar{t}} = \Pi_{\Lambda_m} S_{t_\lambda}$.

For each $\lambda = \langle i, j\rangle \in \Lambda_m$, let $\langle x_\lambda, x'_\lambda\rangle = \langle x_i, x_j\rangle$. For each $\bar{t} \in T^{\Lambda_n}$, $\bar{s} \in S^{\bar{t}}$, and $\lambda \in \Lambda_m \cup \{\varnothing\}$, we shall define a pair of terms $\ell_\lambda^{(\bar{t},\bar{s})}$ and $r_\lambda^{(\bar{t},\bar{s})}$ in the variables u, v, Z_λ, and x_i, for $i = 0, \ldots, \binom{m}{2} - 1$, . For convenience, however, for each $\lambda \in \Lambda_m \cup \{\varnothing\}$, let us for the moment write $\ell_\lambda = \ell_\lambda^{(\bar{t},\bar{s})}$ and $r_\lambda = r_\lambda^{(\bar{t},\bar{s})}$. Set $\ell_\varnothing(\mathbf{x}, u, v, \mathbf{z}) = u$ and $r_\varnothing(\mathbf{x}, u, v, \mathbf{z}) = v$. For $\lambda \in \Lambda_m$, let

$$\ell_\lambda(\mathbf{x}, u, v, \mathbf{z}) = s_\lambda(x_\lambda, x'_\lambda, \ell_{\lambda^-}, r_{\lambda^-}, \mathbf{z}_\lambda)$$

and

$$r_\lambda(\mathbf{x}, u, v, \mathbf{z}) = s_\lambda(x_\lambda, x'_\lambda, r_{\lambda^-}, r_{\lambda^-}, \mathbf{z}_\lambda),$$

where we have suppressed expression of the dependence of ℓ_{λ^-} and r_{λ^-} on their variables and where λ^- is the immediate predecessor of λ.

Let M be the highest element of Λ_m. Set $\ell^{(\bar{t},\bar{s})} = \ell_M^{(\bar{t},\bar{s})}$ and $r^{(\bar{t},\bar{s})} = r_M^{(\bar{t},\bar{s})}$. Let v_m be the conjunction of all equations $\ell^{(\bar{t},\bar{s})} \approx r^{(\bar{t},\bar{s})}$, for all choices of $\bar{t} \in T^{\Lambda_m}$ and $\bar{s} \in S^{\bar{t}}$.

Let $\mathbf{A} \in \mathcal{V}$. Choose $\bar{t} \in T^{\Lambda_m}$ and $\bar{s} \in S^{\bar{t}}$. Let $\mathbf{a}$ be an assignment of the variables appearing in $\ell := \ell^{(\bar{t},\bar{s})}$ and $r := r^{(\bar{t},\bar{s})}$. Let $e_i = x_i[\mathbf{a}]$, and write $\langle e_\lambda, e'_\lambda \rangle = \langle e_i, e_j \rangle$ for any $\lambda = \langle i, j \rangle \in \Lambda_m$. Suppose that $e_\lambda = e'_\lambda$ for some $\lambda \in \Lambda_m$. We claim that this entails that $\mathbf{A} \models (\ell \approx r)[\mathbf{a}]$. Note that by equation 3.1 we have that $\ell_\lambda[\mathbf{a}] = r_\lambda[\mathbf{a}]$. If λ is the highest element of Λ_m, then we are done. Otherwise, it easily follows that $\ell_{\lambda^+}[\mathbf{a}] = r_{\lambda^+}[\mathbf{a}]$, where λ^+ is the immediate successor of λ. Thus, by induction on the order we imposed on Λ_m we have that $\ell[\mathbf{a}] = r[\mathbf{a}]$.

Theorem 3.12. *Let $\mathcal{V}$ be a congruence modular variety. Let m be a natural number. Fix Gumm terms, $p, q_i (i = 0, \ldots, n)$ for $\mathcal{V}$. Let Λ_m and v_m be as described above. Let $\mathbf{A} \in \mathcal{V}$. If $|A| < m$, then $\mathbf{A} \models v_m$. Conversely, if $\alpha \prec \beta$ are congruences on $\mathbf{A}$ and $\mathbf{A}/\alpha \models v_m$, then $|A/(\alpha : \beta)| < m$.*

Proof. Suppose first that $|A| < m$. Let $\mathbf{a}$ be any assignment of the variables $X \cup \{u, v\} \cup Z$ to elements in $\mathbf{A}$. Let $e_i = x_i[\mathbf{a}]$, and write $\langle e_\lambda, e'_\lambda \rangle = \langle e_i, e_j \rangle$ for any $\lambda = \langle i, j \rangle \in \Lambda_m$. Reasoning as pigeons do, we find that there must be a $\lambda \in \Lambda_m$ so that $e_\lambda = e'_\lambda$. Thus, by the argument preceding this theorem, we have that $\mathbf{A} \models v_m$.

Now, suppose that $\alpha \prec \beta$ are congruences on $\mathbf{A}$ so that $(\alpha : \beta)$ has index m or greater. Without loss of generality, we shall assume that $\alpha = 0_A$: After all, $(\alpha : \beta)/\alpha = (0_{A/\alpha} : \beta/\alpha)$, and so, by the third isomorphism theorem (A.15), $(0_{A/\alpha} : \beta/\alpha)$ has the same index in $\mathbf{A}/\alpha$ as $(\alpha : \beta)$ does in $\mathbf{A}$. Thus, we can write $\beta = \mathrm{Cg}\langle a, b \rangle$ for some $a, b \in A$. List m elements $e_0, \ldots, e_{m-1} \in A$ lying in mutually distinct $(0_A : \beta)$-classes. We shall find a sequence of terms $\bar{t} \in T^{\Lambda_m}$ and $\bar{s} \in S^{\bar{t}}$ and terms $\ell = \ell^{(\bar{t},\bar{s})}$ and $r = r^{(\bar{t},\bar{s})}$, and a witness to the failure of $\ell \approx r$ in $\mathbf{A}$, which shall also represent a failure of v_m in $\mathbf{A}$.

Set $a_\varnothing = a$ and $b_\varnothing = b$. Let $\ell_\varnothing = u$ and $r_\varnothing = v$. Let $\lambda^+ \in \Lambda_m$ with immediate predecessor λ. Suppose that a_λ, b_λ have been chosen so that $\mathrm{Cg}\langle a, b \rangle = \mathrm{Cg}\langle a_\lambda, b_\lambda \rangle$.

Suppose that ℓ_λ and r_λ are terms in the variables $X \cup \{u, v\} \cup Z$ and $\mathbf{c}_{\lambda'}(\lambda' \leq \lambda)$ are elements of A that have been chosen so that, for any assignment $\mathbf{a}$ of elements of A to the variables appearing in ℓ_λ and r_λ that includes $x_i \mapsto e_i$, $u \mapsto a$, $v \mapsto b$, and, for each $\lambda' \leq \lambda$, $\mathbf{z}_{\lambda'} \mapsto \mathbf{c}_{\lambda'}$, we have that $\ell_\lambda[\mathbf{a}] = a_\lambda$ and $r_\lambda[\mathbf{a}] = b_\lambda$. (Note that the basis step, above, clearly satisfies these requirements, if we let $\mathbf{c}_\varnothing$ be arbitrary.)

Since $\neg C^{\mathbf{A}}(e_{\lambda^+}, e'_{\lambda^+}, a_\lambda, b_\lambda)$, by Theorem 3.11 we get a term t, a tuple of elements $\mathbf{c}$ from A, and an $s \in S_t$ so that

$$a_{\lambda^+} := s(e_{\lambda^+}, e'_{\lambda^+}, a_\lambda, b_\lambda, \mathbf{c}) \neq s(e_{\lambda^+}, e'_{\lambda^+}, b_\lambda, b_\lambda, \mathbf{c}) =: b_{\lambda^+}.$$

Set $t_{\lambda^+} = t$, $s_{\lambda^+} = s$, and $\mathbf{c}_\lambda = \mathbf{c}$. Note that, by inductive hypothesis,

$$\langle a_{\lambda^+} b_{\lambda^+} \rangle \in \mathrm{Cg}\langle a_\lambda, b_\lambda \rangle \setminus 0_A = \mathrm{Cg}\langle a, b \rangle \setminus 0_A.$$

But since $0_A \prec \mathrm{Cg}\langle a, b\rangle$, we get that $\mathrm{Cg}\langle a_{\lambda^+}, b_{\lambda^+}\rangle = \mathrm{Cg}\langle a, b\rangle$. Set

$$\ell_{\lambda^+} = s(x_{\lambda^+}, x'_{\lambda^+}, \ell_\lambda, r_\lambda, \mathbf{z}_{\lambda^+})$$

and

$$\ell_{\lambda^+} = s(x_{\lambda^+}, x'_{\lambda^+}, r_\lambda, r_\lambda, \mathbf{z}_{\lambda^+}),$$

and note that, by inductive hypothesis, under any assigment $\mathbf{a}$ that includes $x_i \mapsto e_i$, $u \mapsto a$, $v \mapsto b$, and, for each $\lambda \leq \lambda^+$, $\mathbf{z}_\lambda \mapsto \mathbf{c}_\lambda$, we get that $\ell_{\lambda^+}[\mathbf{a}] = a_{\lambda^+}$ and $r_{\lambda^+}[\mathbf{a}] = b_{\lambda^+}$. Let the construction of this sequence of objects indexed by $\Lambda_m \cup \{\varnothing\}$ then continue through recursion.

Thus, we get a $\bar{t} \in T^{\Lambda_m}$ and $\bar{s} \in S^{\bar{t}}$. For each $\lambda \in \Lambda_m \cup \{\varnothing\}$, set $\ell_\lambda^{(\bar{t},\bar{s})} = \ell_\lambda$ and $r_\lambda^{(\bar{t},\bar{s})} = r_\lambda$. Let $r = r_M$ and ℓ_M, where M is the highest element of Λ_m. Let $\mathbf{a}$ be any assignment of elements in A that includes $x_i \mapsto e_i$, $u \mapsto a$, $v \mapsto b$, and, for each $\lambda \in \Lambda_m$, $\mathbf{z}_\lambda \mapsto \mathbf{c}_\lambda$. By construction, then, we get that $\mathbf{a}$ witnesses the failure of $\ell \approx r$ in $\mathbf{A}$. It is also evident from the construction of r and ℓ that this entails the failure of v_m in $\mathbf{A}$. $\square$

This theorem—and especially its consequences—should be compared with those evident from some results in Chapter 10 of Freese and McKenzie (1987), in particular, their Theorem 10.12 and Theorem 10.16. Kearnes (1996) should also be consulted. We can find several uses for the theorem just given. We now take a look at a few of its immediate consequences, some of which seem to be new results in their own right.

This first consequence is also evident from Freese and McKenzie (1987), Theorem 10.12.

Corollary 3.13. *Let* $\mathbf{A}$ *be a finite algebra that generates a congruence modular variety* $\mathcal{V}$*. Then for any subdirectly irreducible* $B \in \mathcal{V}$ *with nonabelian monolith, we have that* $|B| \leq |A|$*.*

Proof. Let $\mathbf{A}$ and $\mathbf{B}$ be as described. Say that $|A| = n$. Then, by the theorem above, $\mathbf{A} \models v_{n+1}$. Now, since v_{n+1} is just a (countable) set of equations, we have that $\mathcal{V} \models v_{n+1}$ as well. Note that the annihilator of the monolith of $\mathbf{B}$ is 0_B; hence, by the theorem above, we get the result. □

The next is a well-known result, originating from Foster and Pixley (1964).

Corollary 3.14. *Let* $\mathbf{A}$ *be a finite algebra in a congruence distributive variety. Let* $\mathcal{V}$ *be the variety generated by* $\mathbf{A}$*. Then* $\mathcal{V}$ *has a finite residual bound.*

Proof. To see this result as a consequence of Corollary 3.13, one needs to first recall Day's Mal'cev characterization of congruence distributivity, which can be found in Freese and McKenzie (1987), as well as recall the elementary fact that congruence distributivity implies congruence modularity. Secondly, one must recall that any prime congruence quotient for an algebra lying in a congruence distributive variety is nonabelian. This last is a nontrivial, but well-known result (See Hobby and McKenzie (1988), Theorems 5.7 and 9.11, for instance.) □

The following is patterned from the parallel observation made in Neumann (1967), as Corollary 52.34, where it was limited to the case of $\mathcal{V}$ a variety of groups. It appears to be a new result. It is interesting to consider this result alongside that of Kearnes (1996), Theorem 3.7 (iii) $\Rightarrow$ (iv).

Theorem 3.15. *If $\mathbf{A} \in \mathcal{V}$, a congruence modular variety, and $\mathbf{A}$ is a finite, subdirectly irreducible with non-abelian monolith, then $\mathbf{A}$ is critical.*

Proof. Let $\mathbf{A}$ be a finite, subdirectly irreducible algebra in a congruence modular variety $\mathcal{V}$. Say that $|A| = n$. Suppose also that the monolith, say μ, of $\mathbf{A}$ is nonabelian. (See Definition A.43). Then, $(0_A : \mu) = 0_A$; that is, the index of the annihilator of μ is n. Then, by Theorem 3.12, we get that $\mathbf{A} \not\models v_n$. Thus, we get that for some $\bar{t} \in T^{\Lambda_n}$, $\bar{s} \in S^{\bar{t}}$, and $\varphi = \ell^{(\bar{t},\bar{s})} \approx r^{(\bar{t},\bar{s})}$, $\mathbf{A} \not\models \varphi$. On the other hand, by Theorem 3.12, we also get that, if $\mathbf{B}$ is a proper factor of $\mathbf{A}$, then $\mathbf{B} \models v_n$ and hence $\mathbf{B} \models \varphi$. It follows that $\mathbf{A}$ is critical. $\square$

One flaw in our chief centralizer laws v_n as given above, relative to the one given in Neumann (1967), is that ours is potentially an infinite set of equations. On the other hand, the following can be used to show that v_n is implied by a finite set of equations under a certain circumstance in which we are interested. More to the point, v_n holds in any algebra $\mathbf{A}$ in the variety with which v_n is associated provided $\mathbf{A}$ is nilpotent of class $\binom{n}{2}$. This fact and its results are apparently new.

Theorem 3.16. *Let $\mathbf{A} \in \mathcal{V}$, a congruence modular variety. Pick Gumm terms for $\mathcal{V}$; we adopt the notation from above. Let n be a natural number, and pick $\bar{t} \in T^{\Lambda_n}$. Let $\bar{s} \in S^{\bar{t}}$. List the elements, in order, of $\Lambda_n \cup \{\varnothing\}$ as $\lambda_0, \ldots, \lambda_m$, for $m = \binom{n}{2}$. Then for each $k \leq m$ and all assignments $\mathbf{a}$ to the relevant variables, $\ell^{(\bar{t},\bar{s})}_{\lambda_k}[\mathbf{a}]\ (1_A]_k\, r^{(\bar{t},\bar{s})}_{\lambda_k}[\mathbf{a}]$. In particular, if $(1_A]_m = 0_A$, then $\mathbf{A} \models v_n$.*

Proof. For convenience, write $\ell_\lambda = \ell^{(\bar{t},\bar{s})}_\lambda$ and $r_\lambda = r^{(\bar{t},\bar{s})}_\lambda$ for each $\lambda \in \Lambda_n \cup \{\varnothing\}$. Let $\mathbf{a}$ be any assignment of the variables appearing in $\ell_{\lambda_{m-1}}, r_{\lambda_{m-1}}$ to elements of A;

say that $\mathbf{a}$ sends $\langle x_i, u, v, \mathbf{z}_\lambda\rangle_{i\in\omega,\lambda\in\Lambda_n}$ to $\langle e_i, a, b, \mathbf{c}_\lambda\rangle_{i\in\omega,\lambda\in\Lambda_n}$. For $\lambda = \langle i, j\rangle \in \Lambda_n$, let $\langle e_\lambda, e'_\lambda\rangle = \langle e_i, e_j\rangle$.

We shall show by induction that $\ell_{\lambda_k}[\mathbf{a}]\,(1_A]_k\, r_{\lambda_k}[\mathbf{a}]$ for each $k \leq m$. The claim is trivial for $k = 0$. Now, suppose that it has been verified for some $k < m$. Note that from equation 3.1,

$$s_{\lambda_{k+1}}(e_{\lambda_{k+1}}, e_{\lambda_{k+1}}, \ell_{\lambda_k}[\mathbf{a}], r_{\lambda_k}[\mathbf{a}], \mathbf{c}_{\lambda_{k+1}}) = s_{\lambda_{k+1}}(e_{\lambda_{k+1}}, e_{\lambda_{k+1}}, r_{\lambda_k}[\mathbf{a}], r_{\lambda_k}[\mathbf{a}], \mathbf{c}_{\lambda_{k+1}}).$$

Thus, by the inductive hypothesis and the fact that $C(1_A, (1_A]_k; (1_A]_{k+1})$ holds, we get that

$$\begin{aligned}\ell_{\lambda_{k+1}}[\mathbf{a}] = s_{\lambda_{k+1}}(e_{\lambda_{k+1}}, e'_{\lambda_{k+1}}, \ell_{\lambda_k}[\mathbf{a}], r_{\lambda_k}[\mathbf{a}], \mathbf{c}_{\lambda_{k+1}})\,(1_A]_{k+1}& \\ s_{\lambda_{k+1}}(e_{\lambda_{k+1}}, e'_{\lambda_{k+1}}, r_{\lambda_k}[\mathbf{a}], r_{\lambda_k}[\mathbf{a}], \mathbf{c}_{\lambda_{k+1}}) = r_{\lambda_{k+1}}[\mathbf{a}].&\end{aligned}$$

□

It is interesting to compare the above result with Theorem of Freese and McKenzie (1987); the two results seem somewhat orthogonally related.

We shall need the following result, the proof of which is only a slight alteration of what appears in Kearnes, Szendrei, and Willard (2013+) as Lemma 2.8 and McKenzie (1987a) as Lemma 2.16. (That is, the result is not new.) For algebra $\mathbf{A}$ and congruences $\alpha \leq \beta$ on $\mathbf{A}$, we let $\mathrm{Ind}(\beta/\alpha)$ be the supremum of the cardinalities of all β/α-classes in A/α.

Theorem 3.17. *Let $\mathbf{A} \in \mathcal{V}$, a Mal'cev variety, and let $\alpha \prec \beta$ be a pair of congruences on $\mathbf{A}$. Let r be a natural number. If the index of $(\alpha : \beta)$ is r or less, then*

$$\mathrm{Ind}(\beta/\alpha) \leq |F_{\mathcal{V}}(r+1)|.$$

Proof. Affirm the hypotheses. Let p be the Mal'cev term for $\mathcal{V}$. Since $(\alpha : \beta)/\alpha = (0_{A/\alpha} : \beta/\alpha)$, we can use the third isomorphism theorem A.15 to reduce the claim to the case of $\alpha = 0_A$. That is, we may assume that $\beta = \mathrm{Cg}^{\mathbf{A}}\langle a, b\rangle$ for some $a, b \in A$.

Fix a transversal T of the $(0_A : \beta)$-classes of A. Fix also $\mathbf{e}$, a tuple of length r with exactly the elements of T appearing in it.

Let $u \in A$, and choose $v \in u/\beta$. Then, by Theorem A.26, we get a term s so that $\langle v, u \rangle = \langle s(a, \mathbf{e}''), s(b, \mathbf{e}'') \rangle$, for some tuple $\mathbf{e}''$ of elements from A. Now, using that p is a Mal'cev term, we have that

$$p(s(a, \mathbf{e}''), s(b, \mathbf{e}''), u) = p(v, u, u) = v = p(v, v, v) = p(s(a, \mathbf{e}''), s(a, \mathbf{e}''), v).$$

From $C((0_A : \beta), \beta; 0_A)$, we can conclude that

$$p(s(a, \mathbf{e}'), s(b, \mathbf{e}'), u) = p(s(a, \mathbf{e}'), s(a, \mathbf{e}'), v) = v,$$

for any tuple $\mathbf{e}'$ related coordinate-wise by $(0_A : \beta)$ to $\mathbf{e}$. Let $\mathbf{e}'$ be the tuple of the same length as $\mathbf{e}''$ and whose elements are the unique representatives from T of the corresponding elements of $\mathbf{e}''$. It is easy to see that one can use s to construct a term t in $r + 1$ variables such that $s(x, \mathbf{e}') = t(x, \mathbf{e})$ for any $x \in A$. In particular, $\langle u, v \rangle = \langle u, p(t(a, \mathbf{e}), t(b, \mathbf{e}), u)$. On the other hand, given any $t \in \operatorname{Clo}_{r+1} \mathbf{A}$, and we have that $p(t(a, \mathbf{e}), t(b, \mathbf{e}), u) \in u/\beta$.

Thus, we can define a map from $\operatorname{Clo}_{r+1} \mathbf{A}$ into u/β given by

$$t \mapsto p(t(a, \mathbf{e}), t(b, \mathbf{e}), u)$$

and the map is is onto. The result follows. $\square$

Theorem 3.18. *Let m be a natural number. Let $\mathbf{A}$ be an algebra of nilpotence class m (or less) that generates a congruence permutable variety $\mathcal{V}$. Then $\mathbf{A} \models v_n$, where n is any natural number so that $m \leq \binom{n}{2}$—such as $n = \left\lceil \sqrt{2m} \right\rceil + 1$. Thus, for any congruences $\alpha \prec \beta$ of $\mathbf{A}$, $(\alpha : \beta)$ is of index less than n and* $\operatorname{Ind}(\beta/\alpha) \leq |F_{\mathcal{V}}(n)|$.

Proof. Let $n = \left\lceil \sqrt{2m} \right\rceil + 1$. Note that $n \geq 1$ and hence $2n - 1 \geq n$. Thus, $\binom{n}{2} = \frac{n^2-n}{2} \geq \frac{n^2-2n+1}{2} = \frac{(n-1)^2}{2} \geq m$. By, Theorem 3.16, we get that $\mathbf{A} \models v_n$. Let $\alpha, \beta \in \operatorname{Con} \mathbf{A}$ such that $\alpha \prec \beta$. By Theorem 3.12, $(\alpha : \beta)$ has index less or equal to $n - 1$

(noting, of course, that congruence permutability implies congruence modularity.) Therefore, by Theorem 3.17, we conclude that $\mathrm{Ind}(\beta, \alpha) \leq |F_{\mathcal{V}}(n)|$. $\square$

It is by means of the theorem just proved not only that we discover that for any Mal'cev variety of algebras of nilpotence class k, and any $\mathbf{A} \in \mathcal{V}$, we have a bound $\mathrm{Ind}(\beta/\alpha)$ for any prime quotient $\alpha \prec \beta$ of congruences on $\mathbf{A}$, but that we are also able to "lift" this bound to $\mathcal{V}^{(N)}$ for large enough N. In the following sections we shall explore some preliminary suggestions for how to apply this result towards the finite basis result sought. First, we recall some facts concerning nilpotent algebras in a Mal'cev variety, noted by Smith (1976).

3.4 Some useful items adapted from Smith (1976)

While the results and their proofs presented in this section can be found in Smith (1976), he uses somewhat different concepts and language concerning the commutator from that employed in the present paper. Some of these differences may even be of more than a strictly superficial kind, but, in any case, we offer proofs using the notation established earlier in this paper.

Lemma 3.19. *Let $\mathbf{A} \in \mathcal{V}$, a variety with a difference term, d. If $\alpha, \beta \in \mathrm{Con}\,\mathbf{A}$ with $\beta \leq \alpha$ such that $[\beta, \alpha] = 0_A$, then $\langle x, y\rangle \, \Delta^{\alpha}_{\beta} \, \langle u, v\rangle$ implies that $v = d^{\mathbf{A}}(y, x, u)$. If d is also a Mal'cev term, then for any $\alpha, \beta \in \mathrm{Con}\,\mathbf{A}$, $\langle x, y\rangle \, \Delta^{\alpha}_{\beta} \, \langle u, v\rangle$ implies that $v \, [\alpha, \beta] \, d^{\mathbf{A}}(y, x, u)$.*

Proof. Let d denote $d^{\mathbf{A}}$, as well. Let $\alpha, \beta \in \mathrm{Con}\,\mathbf{A}$. Suppose first that $[\beta, \alpha] = 0_A$ and that $\beta \leq \alpha$. Apply d coordinate-wise, "vertically" to the following pairs:

$$\langle y, y\rangle \, \Delta^{\alpha}_{\beta} \, \langle y, y\rangle$$

$$\langle x, y\rangle \, \Delta^{\alpha}_{\beta} \, \langle x, y\rangle$$

$$\langle x, y\rangle \, \Delta^{\alpha}_{\beta} \, \langle u, v\rangle,$$

to yield $\langle d(y,x,x),y\rangle \, \Delta^{\alpha}_{\beta} \, \langle d(y,x,u),v\rangle$. Since $[\beta,\beta] \leq [\beta,\alpha] = 0_A$ and $\langle y,x\rangle \in \beta$, we have that $d(y,x,x) = y$. Thus, the first claim follows by Proposition A.37.

The second claim is even easier, and it follows by a similar computation, and so we omit it. (It is also a consequence of Theorem 2.24 together with Remark 2.6.) □

For any algebra $\mathbf{A}$ and any $B \subseteq A$, we shall say that B is *normal* provided it is the class of some congruence—in particular, of $\mathrm{Cg}^{\mathbf{A}}\, B^2$.

The following is a generalization of Proposition 236 from Smith (1976). The proof is adapted from his, as well.

Theorem 3.20. *Let $\mathbf{A}$ be an algebra in a variety with difference term d. Let ζ be the center of $\mathbf{A}$. Let $\mathbf{M}$ be a subalgebra of $\mathbf{A}$ with the property that $M\zeta = A$. Then M is normal in $\mathbf{A}$, and $\mathbf{A}/\operatorname{Cg} M^2$ is abelian.*

Proof. Let d denote $d^{\mathbf{A}}$. Let $\tilde{\mu}$ be the binary relation on A defined by $\langle a,a'\rangle \in \tilde{\mu}$ if and only if there exist $m,m' \in M$ such that

$$\langle a,m\rangle \, \Delta^{1_A}_{\zeta} \, \langle a',m'\rangle.$$

We claim that $\tilde{\mu}$ is a tolerance (that is, a reflexive, symmetric, binary relation that respects the operations of $\mathbf{A}$. Reflexivity of $\tilde{\mu}$ follows from reflexivity of $\Delta^{1_A}_{\zeta}$ and from the hypothesis that $M\zeta = A$; put another way, $M\zeta = A$ says precisely that given any $a \in A$, we can find an $m \in M$ so that $m \,\zeta\, a$. The symmetry of $\tilde{\mu}$ is also easy to see: One just needs the symmetry of $\Delta^{1_A}_{\zeta}$. That $\tilde{\mu}$ respects the operations of $\mathbf{A}$ is automatic from the facts that M and $\Delta^{1_A}_{\zeta}$ are closed under the operations of $\mathbf{A}$ and $\mathbf{A}^2$, respectively. It easily follows that the transitive closure μ of $\tilde{\mu}$ is a congruence on $\mathbf{A}$.

Now, by the definition of $\Delta^{1_A}_{\zeta}$, we get that for any $m,m' \in M$,

$$\langle m,m\rangle \, \Delta^{1_A}_{\zeta} \, \langle m',m'\rangle,$$

and so $m \,\mu\, m'$. Thus, we see that M is contained in some μ-class.

We claim that M *absorbs* $\tilde{\mu}$: That is, if $m \in M$ and $a \in A$ such that $m \mathrel{\tilde{\mu}} a$, then $a \in M$. Let m and a satisfy these hypotheses. Say that $\langle m, m_0 \rangle \mathrel{\Delta_{\zeta}^{1_A}} \langle a, m_1 \rangle$. Then, it is not hard to see, by Mal'cev's description of congruence generation (see Theorem A.9) that $\langle m_0, m \rangle \mathrel{\Delta_{\zeta}^{1_A}} \langle m_1, a \rangle$, as well. Thus, since $[\zeta, 1_A] = 0_A$, Lemma 3.19 tells us that $a = p(m, m_0, m_1) \in M$. We use this now to show that M absorbs μ. Let $m \in M$ and $a \in A$ such that $m \mathrel{\mu} a$. Then we can write

$$m = a_0 \mathrel{\tilde{\mu}} a_1 \mathrel{\tilde{\mu}} \cdots \mathrel{\tilde{\mu}} a_{k-1} = a,$$

for some natural number k and $a_i \in A$ for $i < k$. Since M absorbs $\tilde{\mu}$, we have that $a_1 \in M$. Thus, by inducting on k, we have that $a \in M$, as well. As we saw above that M is contained in a single μ-block, it now follows that M is a congruence block of μ; hence M is normal.

We claim further that $\mu = \operatorname{Cg} M^2$. Of course, we have just seen that $\operatorname{Cg} M^2 \leq \mu$, and so it remains only to show the reverse inequality. Indeed, using an argument similar to the one just given, we observe that if $\langle a, a' \rangle \in \tilde{\mu}$, then $a' = p(a, m, m')$ for some $m, m' \in M$. Thus,

$$\begin{aligned} \langle a, a' \rangle &= \langle p(a, m, m), p(a, m, m') \rangle \\ &= p(\langle a, a \rangle, \langle m, m' \rangle, \langle m, m' \rangle) \\ &\in \operatorname{Cg} M^2. \end{aligned}$$

Thus, $\tilde{\mu} \leq \operatorname{Cg} M^2$, from which it now follows that $\mu = \operatorname{Cg} M^2$. Note also that since $M\zeta = A$ and M is a block of μ, we get that $\mu \vee \zeta = 1_A$.

It remains to show that $\mathbf{A}/\mu$ is abelian. To do so, by Proposition A.28, it is equivalent to show that $(\mu : 1_A) = 1_A$. Note that since $\mathbf{A}$ is in a difference term variety, we use Theorem 4.38 and the fact that $C(\zeta, 1_A; 0_A)$ to learn that $C(\zeta, 1_A; \mu)$. Thus, $\zeta \leq (\mu : 1_A)$. On the other hand, $C(\mu, 1_A; \mu)$ and so $\mu \leq (\mu : 1_A)$, as well. Thus, $1_A = \mu \vee \zeta \leq (\mu : 1_A)$, as desired. □

The following is given by Smith (1976), as Proposition 236. In fact, he says a little more than we have included here—concerning the Frattini subalgebra of a given nilpotent, Mal'cev algebra $\mathbf{A}$, should it have one.

Theorem 3.21. *Let* $\mathbf{A}$ *be a nilpotent algebra in a Mal'cev variety. Then every maximal subalgebra of* $\mathbf{A}$ *is normal.*

Proof. Let k be the nilpotence class of $\mathbf{A}$. According to Theorem 4.30, since $\mathbf{A}$ is nilpotent, we have that $\zeta^k := \zeta^k_{\mathbf{A}} = 1_A$. Let $\mathbf{M}$ be a maximal (proper) subalgebra of $\mathbf{A}$. Evidently, $M\zeta^k = A$. Let n be the least natural number so that $M\zeta^n = A$. Note that $n > 0$, since $\zeta^0 = 0_A$ and M is a proper subset of A. Also, by the maximality of $\mathbf{M}$, we have that for any $i < n$, $M\zeta^i = M$. In particular, M is a union of ζ^{n-1}-blocks. Let M/ζ^{n-1} denote the set of ζ^{n-1}-blocks contained in M. It is not hard to see that

$$(M/\zeta^{n-1})\zeta_{A/\zeta^{n-1}} = (M/\zeta^{n-1})(\zeta^n/\zeta^{n-1}) = A/\zeta^{n-1}.$$

It follows by Theorem 3.20 (and Definition 4.14) that $\mathbf{M}/\zeta^{n-1}$ is normal in $\mathbf{A}/\zeta^{n-1}$ and that $(\mathbf{A}/\zeta^{n-1})/\operatorname{Cg}(M/\zeta^{n-1})^2$ is abelian. Recall from Theorem A.46, that, since $\mathbf{A}$ is nilpotent and Mal'cev, it is also congruence regular. In particular, $\zeta^{n-1} = \operatorname{Cg}^{\mathbf{A}}\{\langle a, b\rangle \mid b \in a/\zeta^{n-1} \text{ and } a \in M\}$. Thus, $\zeta^{n-1} \leq \operatorname{Cg}^{\mathbf{A}} M^2$. Now, using also that

$$(\operatorname{Cg}^{\mathbf{A}} M^2)/\zeta^{n-1} = \operatorname{Cg}^{\mathbf{A}/\zeta^{n-1}}(M/\zeta^{n-1})^2 \tag{3.2}$$

(which can be seen from Proposition A.10), we can easily show that M is a congruence block of $\operatorname{Cg}^{\mathbf{A}} M^2$; that is, M is normal in $\mathbf{A}$: Let $m \in M$ and $a \in A$ such that $m \operatorname{Cg}^{\mathbf{A}} M^2\, a$. Then,

$$\langle m/\zeta^{n-1}, a/\zeta^{n-1}\rangle \in \operatorname{Cg}^{\mathbf{A}} M^2/\zeta^{n-1} = \operatorname{Cg}^{\mathbf{A}/\zeta^{n-1}}(M/\zeta^{n-1})^2,$$

and hence $a/\zeta^{n-1} \in M/\zeta^{n-1}$, whence $a \in M$. We also observe that from

$$C(1_{A/\zeta^{n-1}}, 1_{A/\zeta^{n-1}}; \operatorname{Cg}^{\mathbf{A}/\zeta^{n-1}}(M/\zeta^{n-1})^2),$$

we can also deduce from 3.2 and Proposition A.28 (e) that

$$C(1_A, 1_A; \operatorname{Cg}^{\mathbf{A}} M^2);$$

that is, $\operatorname{Cg}^{\mathbf{A}} M^2$ is abelian. □

3.5 (Some) Frattini congruences

In group theory, the Frattini subgroup is defined to be the intersection of all maximal subgroups of a given group—if it has any—and otherwise the group itself. (See Scott (1964), section 7.3). In his Proposition 237, Smith (1976) showed that this concept generalizes to Mal'cev nilpotent algebras with favorable results. On the other hand, Smith has a counterexample demonstrating that the intersection of the maximal subalgebras of a nilpotent, Mal'cev algebra may be empty (see p. 45 in Smith (1976)). Kiss and Vovsi (1995) and Kearnes (1996) have argued that the concept of Frattini subgroup is more aptly generalized by a congruence. We give their definition of the Frattini congruence below, but we also offer a second one which we show is equivalent to theirs in any Mal'cev variety of nilpotent algebras.

Let $\mathbf{A}$ be any algebra. Denote by $\mathcal{M}_{\mathbf{A}}$, or, if $\mathbf{A}$ is clear from context, simply, $\mathcal{M}$, the set of all maximal subalgebras of $\mathbf{A}$ (of course, $\mathcal{M}$ may be empty.) For any nonempty subset B of A, let ϕ_B denote the largest congruence so that B is a union of ϕ_B-classes, noting, of course, that an easy computation is needed to justify this definition. Given a subset B of A and a congruence θ on $\mathbf{A}$, we say that θ is *contained in* B provided $B\theta = B$ (see Definition A.12.) (We might also say that "B absorbs θ.") It is not hard to see, then, that for a given $B \subseteq A$, ϕ_B is also the largest congruence contained in B; indeed, for a given $\theta \in \operatorname{Con} \mathbf{A}$, B is a union of θ-classes if and only if $B\theta = B$.

Definition 3.22. For a given algebra $\mathbf{A}$, let ${}^1\Phi_{\mathbf{A}}$ be the congruence on $\mathbf{A}$ defined as follows. If $\mathbf{A}$ has no maximal subalgebras, let ${}^1\Phi_{\mathbf{A}} = 1_A$. Otherwise, let

$$^1\Phi_{\mathbf{A}} = \bigcap\{\phi_M \mid M \in \mathcal{M}_{\mathbf{A}}\}.$$

When it is clear from context, we shall drop the subscript $\mathbf{A}$. We call this the ^{1}*Frattini congruence of* $\mathbf{A}$.

Kiss and Vovsi (1995) and Kearnes (1996) used this to generalize some results from Neumann (1967) concerning critical algebras and other matters. Our interest, too, is critical algebras (albeit, we seek necessary conditions of criticality rather than sufficient ones) and we have found some promise in answer Problem 1.3 through the consideration of the following definition, which turns out to yield the same object as Definition 3.22 in the context of a Mal'cev variety of nilpotent algebras.

Definition 3.23. For a given algebra $\mathbf{A}$, let ${}^2\Phi_{\mathbf{A}}$ be a congruence on $\mathbf{A}$ defined as follows. If $\mathbf{A}$ has no maximal (proper) subalgebras, let ${}^2\Phi_{\mathbf{A}} = 1_A$. Otherwise, we set

$$^2\Phi_{\mathbf{A}} = \bigcap\{\operatorname{Cg}^{\mathbf{A}} M^2 \mid \mathbf{M} \in \mathcal{M}_{\mathbf{A}}\}.$$

When it is clear from context, we shall drop the subscript $\mathbf{A}$. We call this the ^{2}*Frattini congruence of* $\mathbf{A}$.

Proposition 3.24. *Let* $\mathbf{A}$ *be any algebra. If* $\mathbf{A}$ *is congruence regular, then we have that* ${}^1\Phi_{\mathbf{A}} \leq {}^2\Phi_{\mathbf{A}}$. *If* $\mathbf{A}$ *is such that each of its maximal subalgebras are normal, then* ${}^2\Phi_{\mathbf{A}} \leq {}^1\Phi_{\mathbf{A}}$. *In particular, if* $\mathbf{A}$ *is nilpotent and lies in a Mal'cev variety, then* ${}^1\Phi_{\mathbf{A}} = {}^2\Phi_{\mathbf{A}}$.

Proof. Note that if $\mathbf{A}$ is without maximal, proper subalgebras, we have that, by definition, ${}^1\Phi = {}^2\Phi$ (where we have dropped the subscript, $\mathbf{A}$.) So, let us suppose that $\mathcal{M} = \mathcal{M}_{\mathbf{A}}$ is nonempty.

First, suppose that $\mathbf{A}$ is congruence regular. Let $\langle a, b\rangle \in {}^1\Phi$. Let $\mathbf{M} \in \mathcal{M}$. We need to show that $\langle a, b\rangle \in \operatorname{Cg}^{\mathbf{A}} M^2$. Since $\langle a, b\rangle \in {}^1\Phi$, we have that $\operatorname{Cg}^{\mathbf{A}}\langle a, b\rangle \leq \phi_M$.

Thus, $M \operatorname{Cg}^{\mathbf{A}}\langle a, b\rangle \subseteq M\phi_M = M$ and hence M is a union of $\operatorname{Cg}^{\mathbf{A}}\langle a, b\rangle$-classes. But since $\mathbf{A}$ is congruence regular, we thus have that $\operatorname{Cg}^{\mathbf{A}}\langle a, b\rangle \leq \operatorname{Cg}^{\mathbf{A}} M^2$. It follows that ${}^1\Phi \subseteq {}^2\Phi$.

Now, suppose that $\mathbf{A}$ is such that each of its maximal subalgebras is normal. Let $\langle a, b\rangle \in {}^2\Phi$. Let $\mathbf{M} \in \mathcal{M}$. We need to show that $\langle a, b\rangle \in \phi_M$. It is sufficient to show that $M \operatorname{Cg}^{\mathbf{A}}\langle a, b\rangle = M$. By assumption, we have that $\langle a, b\rangle \in \operatorname{Cg}^{\mathbf{A}} M^2$, and hence $\operatorname{Cg}^{\mathbf{A}}\langle a, b\rangle \leq \operatorname{Cg}^{\mathbf{A}} M^2$. Now, we have assumed that $\mathbf{M}$ is normal, and hence we must also have that M is the union of $\operatorname{Cg}^{\mathbf{A}}\langle a, b\rangle$-classes. This puts $\langle a, b\rangle \in \phi_M$. It follows that ${}^2\Phi \subseteq {}^1\Phi$.

To see the final claim of this proposition, recall Theorems A.46 and 3.21. $\square$

As in the case of the study of Frattini subgroups, we have a connection with the ^{1}Frattini congruence and a notion of "nongeneration." See also Kearnes (1996), p. 8.

Definition 3.25. For a given algebra $\mathbf{A}$, we shall call any pair $\langle x, y\rangle \in A^2$ a ^{1}*nongenerator for* $\mathbf{A}$ whenever for any $\mathbf{B} \leq \mathbf{A}$, we have that

$$B \operatorname{Cg}^{\mathbf{A}}\langle x, y\rangle = A \Rightarrow B = A.$$

Theorem 3.26. *Let* $\mathbf{A}$ *be an algebra such that every chain of proper subalgebras of* $\mathbf{A}$ *includes its least upper bound. Then* ${}^1\Phi_{\mathbf{A}}$ *is exactly the set of all* ^{1}*nongenerators for* $\mathbf{A}$.

Proof. Note that, if $\mathbf{A}$ is without maximal, proper subalgebras, then, our hypothesis concerning chains of subalgebras of $\mathbf{A}$ together with Zorn's Lemma, implies that $\mathbf{A}$ is without any proper subalgebras at all. Thus, under this circumstance, every pair of elements from A is a ^{1}nongenerator and so, by definition of ${}^1\Phi$, the claim is satisfied. Thus, we will proceed under the assumption that $\mathcal{M}$ is nonempty.

Let $\langle a, b\rangle \in {}^1\Phi$. Let $\mathbf{B} \leq \mathbf{A}$ and suppose that $\mathbf{B} \operatorname{Cg}\langle a, b\rangle = A$. If $B \neq A$, then, by Zorn's Lemma and our hypothesis concerning chains of subalgebras of $\mathbf{A}$, we can extend $\mathbf{B}$ to a maximal, proper subalgebra $\mathbf{M}$ of $\mathbf{A}$. Note that, since $\langle a, b\rangle \in {}^1\Phi \leq \phi_M$, we also have that $M \operatorname{Cg}\langle a, b\rangle = M$. Altogether, we thus have that $A = B \operatorname{Cg}\langle a, b\rangle \leq M \operatorname{Cg}\langle a, b\rangle = M$, which contradicts the definition of $\mathbf{M}$ as proper. Thus, we are forced to conclude that $\mathbf{B} = \mathbf{A}$, which shows that $\langle a, b\rangle$ is a ^{1}nongenerator for $\mathbf{A}$.

Now, assume that $\langle a, b\rangle$ is a ^{1}nongenerator for $\mathbf{A}$. Let $\mathbf{M} \in \mathcal{M}$. We need to show that $\langle a, b\rangle \in \phi_M$, which is to say, that $M \operatorname{Cg}\langle a, b\rangle = M$. But, of course, the alternative, namely that $M \operatorname{Cg}\langle a, b\rangle = A$ is ruled out by the definition of ^{1}nongenerator, as M is assumed to be a proper subset of $\mathbf{A}$. $\square$

Lemma 3.27. *Let $\mathbf{A}$ be an algebra with regular congruences, and suppose that each of its maximal, proper subalgebras are normal. Then if $\mathbf{M}$ is a maximal (proper) subalgebra of $\mathbf{A}$, then $\operatorname{Cg} M^2$ is a maximal proper congruence of $\mathbf{A}$.*

Proof. Let $\mathbf{A}$ and $\mathbf{M}$ be as described. Denote $\operatorname{Cg} M^2$ by μ. Let θ be a congruence on $\mathbf{A}$ with $\mu < \theta$. Note that M is a block of μ and is also contained within a single θ-block, which is equal to $M\theta$. Since $\mathbf{A}$ has regular congruences, we must have that $M < M\theta = A$. But this entails that all of A is a single θ-block and hence that $\theta = 1_A$. $\square$

Theorem 3.28. *Let $\mathbf{A}$ be an algebra that generates a Mal'cev variety and such that each chain of subalgebras of $\mathbf{A}$ contains its upper bound. Let Φ denote its ^{1}Frattini congruence. Suppose that Φ is finitely generated. Then $\mathbf{A}$ is generated by a transversal of its Φ-classes.*

Proof. Choose a transversal T of the Φ-classes of $\mathbf{A}$. Let $\mathbf{B} = \operatorname{Sg}^{\mathbf{A}} T$. We claim that, in fact, $\mathbf{B} = \mathbf{A}$. Note that $B\Phi = A$.

By our hypotheses, we can write

$$\Phi = \operatorname{Cg}\langle x_0, y_0\rangle \circ \cdots \circ \operatorname{Cg}\langle x_{n-1}, y_{n-1}\rangle$$

for some natural number n and some pairs $\langle x_i, y_i\rangle \in A^2$. Note that

$$B\Phi = B\,\mathrm{Cg}\langle x_0, y_0\rangle \cdots \mathrm{Cg}\langle x_{n-1}, y_{n-1}\rangle$$

By induction and Theorem 3.26, we have that

$$\begin{aligned}
&A = B\,\mathrm{Cg}\langle x_0, y_0\rangle \cdots \mathrm{Cg}\langle x_{n-1}, y_{n-1}\rangle \\
\Rightarrow &A = B\,\mathrm{Cg}\langle x_0, y_0\rangle \cdots \mathrm{Cg}\langle x_{n-2}, y_{n-2}\rangle \\
&\vdots \\
\Rightarrow &A = B
\end{aligned}$$

□

The following is noted by Smith (1976) as Proposition 234.

Theorem 3.29. *Let* $\mathbf{A}$ *be any algebra. If every subalgebra of any algebra* $\mathbf{B}$ *in the variety generated by* $\mathbf{A}$ *is normal, then* $\mathbf{A}$ *is abelian.*

As a partial converse, if $\mathbf{A}$ *is abelian and Mal'cev, then each of its subalgebras is normal in* $\mathbf{A}$*.*

Proof. Suppose that each subalgebra of any algebra $\mathbf{B}$ in $\mathrm{Var}\,\mathbf{A}$ is normal in $\mathbf{B}$. Note that it is not hard to see from Proposition A.37, that $\mathbf{A}$ is abelian if and only if 0_A is normal in $\mathbf{\Delta}_{1_A}^{1_A}$. But, by hypothesis, since $\mathbf{\Delta}_{1_A}^{1_A}$ is a subalgebra of $\mathbf{A}^2$, we have exactly that.

Now, suppose that $\mathbf{A}$ is abelian with Mal'cev term operation p. Let $\mathbf{B}$ be a subalgebra of $\mathbf{A}$. Note that, by Proposition A.25, we have that $\mathrm{Cg}^{\mathbf{A}}\,B^2 = \mathrm{Sg}^{\mathbf{A}\times\mathbf{A}}\,B^2 \cup 0_A$. We claim further that $\mathrm{Sg}^{\mathbf{A}\times\mathbf{A}}\,B^2 \cup 0_A = B^2\Delta_{1_A}^{1_A}$ (see Definition A.12 for an explanation of the notation.) Let $\Delta = \Delta_{1_A}^{1_A}$. Note that, by the reflexivity of Δ, we have that $B^2 \subseteq B^2\Delta$. We claim further that $0_A \subseteq B^2\Delta$: Let $a \in A$. Also, take any $b \in B$. Then $\langle b, b\rangle\,\Delta\,\langle a, a\rangle$ and so, indeed, $0_A \subseteq B^2\Delta$. Since $B^2\Delta$ is closed under the operations of $\mathbf{A}^2$, it follows that $\mathrm{Sg}^{\mathbf{A}\times\mathbf{A}}\,B^2 \cup 0_A \leq B^2\Delta$. Now, take any $\langle a, a'\rangle \in B^2\Delta$.

Then we have some $\langle b, b' \rangle \in B^2$ such that $\langle b, b' \rangle \,\Delta\, \langle a, a' \rangle$. By Proposition 3.19, we have that $a' = p(b', b, a)$. Thus,

$$\langle a, a' \rangle = \langle p^{\mathbf{A}}(b, b, a), p^{\mathbf{A}}(b', b, a) \rangle = p^{\mathbf{A}^2}(\langle b, b' \rangle, \langle b, b \rangle, \langle a, a \rangle),$$

which puts $\langle a, a' \rangle$ in $\operatorname{Sg}^{\mathbf{A}\times\mathbf{A}} B^2 \cup 0_A$. It now follows that $\operatorname{Cg}^{\mathbf{A}} B^2 = B^2\Delta$.

Now, take any $b \in B$ and $a \in A$ such that $b\, B^2\Delta\, a$. Then, for some $b_0, b_1 \in B$, we can write $\langle b, a \rangle \,\Delta\, \langle b_0, b_1 \rangle$. By Proposition 3.19, then, we get that $a = p^{\mathbf{A}}(b_1, b_0, b) \in B$, since B is closed under the operations of $\mathbf{A}$. Thus, B is indeed normal in $\mathbf{A}$. $\square$

The following is apparently new, and includes a generalization of 7.3.3 from Scott (1964); see also Theorem 237 in Smith (1976).

Theorem 3.30. *Let* $\mathbf{A}$ *be an congruence regular algebra in a Mal'cev variety. Suppose also that for all* $\gamma \in \operatorname{Con}\mathbf{A}$ *with* $\gamma \prec 1_A$ *we have that* 1_A *is abelian over* γ *(which means nothing more or less than that* $\mathbf{A}/\gamma$ *is abelian). If all the maximal, proper subalgebras of* $\mathbf{A}$ *are normal, then* ${}^2\Phi_{\mathbf{A}} \geq [1_A, 1_A]$.

Conversely, if ${}^1\Phi_{\mathbf{A}} \geq [1_A, 1_A]$, *then all maximal, proper subalgebras of* $\mathbf{A}$ *are normal, and hence, in fact,* ${}^1\Phi_{\mathbf{A}} = {}^2\Phi_{\mathbf{A}}$.

Proof. Let ${}^1\Phi$ and ${}^2\Phi$ denote the ^{1} and ^{2}Frattini congruences of $\mathbf{A}$, respectively. Let $\mathcal{M}$ be the set of all maximal, proper subalgebras of $\mathbf{A}$. First, assume that all $\mathbf{M} \in \mathcal{M}$ are normal. From Lemma 3.27, for any $\mathbf{M} \in \mathcal{M}$ and $\mu := \operatorname{Cg}^{\mathbf{A}} M^2$, we have that $\mu \prec 1_A$, and hence, by hypothesis, $C(1_A, 1_A; \mu)$ holds. By definition of ${}^2\Phi$ (and Proposition A.28 (a)) we also have that $C(1_A, 1_A; {}^2\Phi)$ holds, which is to say, ${}^2\Phi \geq [1_A, 1_A]$.

Now, suppose that ${}^1\Phi \geq [1_A, 1_A]$. Let $\mathbf{M} \in \mathcal{M}$. Note that M is a union of ${}^1\Phi$-blocks. Let $M/{}^1\Phi = (M\,{}^1\Phi)/{}^1\Phi$ denote the set of all ${}^1\Phi$-blocks contained within M. It is not hard to see that $M/{}^1\Phi$ is closed under the operations of $\mathbf{A}/{}^1\Phi$. Note, also that, by congruence regularity of $\mathbf{A}$, ${}^1\Phi \leq \operatorname{Cg}^{\mathbf{A}} M^2$. (See Theorem A.14.) Now, by Proposition A.28 (e), $C(1_A, 1_A; {}^1\Phi)$ implies that $\mathbf{A}/{}^1\Phi$ is abelian and hence, by Theorem 3.29, $M/{}^1\Phi$ is normal in $\mathbf{A}/{}^1\Phi$. We claim that this entails that M is normal in $\mathbf{A}$. Let $m \in M$ and $a \in A$ such that $m \operatorname{Cg}^{\mathbf{A}} M^2\, a$. Then, by Proposition A.10, we have that

$$\langle m/{}^1\Phi, a/{}^1\Phi\rangle \in (\operatorname{Cg}^{\mathbf{A}} M^2)/{}^1\Phi = \operatorname{Cg}^{\mathbf{A}/{}^1\Phi}(M/{}^1\Phi)^2.$$

Since $M/{}^1\Phi$ is normal, we then get that $a/{}^1\Phi \in M/{}^1\Phi$, which puts $a \in M$. It follows that M is normal. Now, by the second part of Theorem 3.24, we then also discover that ${}^2\Phi \leq {}^1\Phi$. By the first part of Theorem 3.24, we also have that ${}^1\Phi \leq {}^2\Phi$, and hence the two are equal. □

Theorem 3.31. *Let* $\mathbf{A}$ *be a nilpotent algebra in a Mal'cev variety. Denote its* ^{2}*Frattini congruence by* Φ. *Then* $\mathbf{A}/\Phi$ *is abelian.*

Proof. There is more than one way to see this. Note that if $\mathbf{A}$ is without maximal, proper subalgebras, then $\Phi = 1_A$ and so the claim is trivial. So suppose otherwise. Let $\mathbf{M} \in \mathcal{M} := \mathcal{M}_{\mathbf{A}}$. Now, note from Theorem 3.21 and Lemma 3.27, we have that $\operatorname{Cg} M^2 \prec 1_A$. Thus, by Theorem A.48 we get that $\mathbf{A}/\operatorname{Cg} M^2$ is abelian. Now, since

$$\mathbf{A}/\Phi \hookrightarrow_{\mathrm{sd}} \Pi\{\mathbf{A}/\operatorname{Cg} M^2 \mid \mathbf{M} \in \mathcal{M}\}$$

and since abelianness is inherited under SP, the claim follows. (See A.1.1 for notation.) □

3.6 A condition for the finite axiomatizability of supernilpotence of class n

The following result is likely to be a necessary step in addressing the task suggested by the second bullet near the beginning of Section 3.2. That is, while it is not currently known whether the supernilpotence class c of any supernilpotent algebra in a congruence permutable variety generated by an algebra $\mathbf{A}$ (perhaps also assumed to be nilpotent) is controlled by the cardinality of A (or, perhaps, another related parameter), but the following shows that, if this is the case, then such a bound on c can be "lifted" to $\mathcal{V}^{(n)}$ for high enough n, under the circumstances described in the theorem.

Theorem 3.32. *Let n be a natural number. Let $\mathcal{V}$ be a Mal'cev variety of finite signature such that each of its members is nilpotent of class n and so that $F_{\mathcal{V}}(2)$ is finite. Then for all natural numbers k, there is a finite set Σ_k of equations in the language of $\mathcal{V}$ such that for any algebra $\mathbf{A}$ in the same signature as $\mathcal{V}$, we have that if $\mathbf{A} \models \Sigma_k$, then $\mathbf{A}$ is supernilpotent of class k.*

Proof. By Theorem 3.7 we get a natural number $N \geq 2$ such that $\mathcal{V}^{(N)}$ is locally finite (and hence $\mathcal{V}$ is locally finite, too). Let k be any natural number. Let $\mathcal{S}_k$ be the class of all algebras in $\mathcal{V}^{(N)}$ that are supernilpotent of class k. It is also clear that since $N \geq 2$ that $\mathcal{V}^{(N)}$ is Mal'cev (see Theorem A.21). Note from Theorem 2.44 that $\mathcal{S}_k$ is a variety. Since $\mathcal{V}^{(N)}$ is locally finite, we have that $\mathcal{S}_k$ is too. Thus, by Theorem 2.30, $\mathcal{S}_k$ is finitely based. Let Σ_k be its finite basis. It is clear that Σ_k has the property claimed of it in the statement of this theorem. $\square$

See Neumann (1967), Lemma 52.35, for a model of precisely how this result might be used.

3.7 Some strategies for establishing that $\mathcal{V}^{(N)}$ has a finite critical bound for high enough N

Let k be a natural number, and fix a Mal'cev variety $\mathcal{V}$ of finite signature, such that each $\mathbf{A} \in \mathcal{V}$ is nilpotent of class k and so that $F_{\mathcal{V}}(2)$ is finite. By Corollary 4.49, we get a finite set of equations E_k satisfied in $\mathcal{V}$ such that, for any algebra $\mathbf{B}$ of the same signature as $\mathbf{A}$, $\mathbf{B} \models E_k$ if and only if $\mathbf{B}$ is nilpotent of class k. Since E_k is finite, we get an N_0 so that for $N \geq N_0$, $\mathcal{V}^{(N)} \models E_k$. Suppose that $N \geq \max\{N_0, 2\}$.

Since $N \geq 2$, we get that $F_{\mathcal{V}^{(N)}}(2) = F_{\mathcal{V}}(2)$ (see Subsection A.1.1.) So by applying Corollary 4.49, again, we find that each algebra in $\mathcal{V}^{(N)}$ is nilpotent of class k.

By Theorem 3.7, we also learn that there is an N_1 such that for all $N \geq N_1$, $\mathcal{V}^{(N)}$ is locally finite. Let $N \geq \max\{N_1, N_0, 2\}$. Let $\mathbf{C}$ be critical algebra in $\mathcal{V}^{(N)}$. Then $\mathbf{C}$ is finitely generated and hence finite by the local finiteness of $\mathcal{V}^{(N)}$. Thus, by Theorems 3.26, 3.24, and 3.28 it is sufficient to find a bound for C/Φ, where Φ is the ^{2}Frattini congruence of $\mathbf{C}$. We also get that $|C/\Phi| \leq \Pi\{|C/\operatorname{Cg} M^2| \mid \mathbf{M} \in \mathcal{M}\}$, where $\mathcal{M}$ is the set of all maximal, proper subalgebras $\mathbf{M}$ of $\mathbf{C}$. Since $N \geq \max\{N_0, 2\}$, we have that $\mathbf{C}$ is nilpotent of class k. Thus, by Lemma 3.27, for each $\mathbf{M} \in \mathcal{K}$, we have that $\operatorname{Cg}^{\mathbf{C}} M^2$ is maximal in $\operatorname{Con} \mathbf{C}$—that is, $\operatorname{Cg}^{\mathbf{C}} M^2 \prec 1_C$. Now, by Theorem 3.18, for each $\mathbf{M} \in \mathcal{K}$, we have that $|\mathbf{C}/\operatorname{Cg} M^2| \leq |F_{\mathcal{V}}(n)|$, where $n = \left\lceil \sqrt{2m} \right\rceil + 1$, noting that since $\mathcal{V}^{(N)}$ is locally finite, $F_{\mathcal{V}}(n)$ is finite. Thus, we need only bound the number of maximal subalgebras of $\mathbf{C}$ (or, perhaps, the number of maximal, proper congruences of $\mathbf{C}$.) Now, we haven't used the fact that $\mathbf{C}$ is critical, except to argue that it is finite. So, really, unless for some reason we think that $\mathcal{V}$ might have an upper bound on the size of its finite algebras, then we ought to find some further use for the hypothesis that $\mathbf{C}$ is critical. Furthermore, we must recall Example 1 from Vaughan-Lee (1983): We shall not be able to establish a finite critical bound in $\mathcal{V}^{(N)}$ without also assuming that $\mathcal{V}$ is generated by a finite algebra, as he provides an example of a locally finite, Mal'cev variety $\mathcal{V}$ of algebras of nilpotence class 3 such that $\mathcal{V}$ is not finitely based.

Remark 3.33. Let $\mathbf{C}$ be a subdirectly irreducible algebra lying in a congruence permutable variety such that $\mathbf{C}$ is nilpotent. Let β be its monolith. Recall from Theorem A.48, that β is abelian, since $\mathbf{C}$ is nilpotent of class, say, m. From Theorem 3.18, then, we have that $\operatorname{Ind}(\beta : 0_A) \leq |F_{\mathcal{V}}(n)|$, where $n = \left\lceil \sqrt{2m} \right\rceil + 1$. In particular, if $\mathcal{V}$ is a locally finite, finite signature, Mal'cev variety of algebras of nilpotence class m, then by Corollary 4.49 and Theorem A.21, we get the same for $\mathcal{V}^{(N)}$ for all high enough N. From Theorem 3.7, we also have that $\mathcal{V}^{(N)}$ is locally finite for high enough

N. Thus, if we can establish that the index of the monolith of any critical algebra $\mathbf{C} \in \mathcal{V}^{(N)}$ is bounded, then we shall be able to establish a finite critical bound for $\mathcal{V}^{(N)}$. While it is not true, in general, that a bound for the index of the monolith of an arbitrary subdirectly irreducible can be found for $\mathcal{V}$, it may turn out that such a bound does exist for critical algebras. Of course, in the case of $\mathcal{V}$, a variety of groups of nilpotence class m, we do indeed get a finite critical bound for $\mathcal{V}$; this can be seen directly from Corollary 2.53 together with Theorem 2.13 and Theorem 2.24 (among other ways). It is interesting to note that Theorem 3.7 (iii) $\Rightarrow$ (iv) of Kearnes (1996), together with Theorem 3.18 shows that each of one particular class of critical algebras in $\mathcal{V}$—namely those whose monolith equals its annihilator—is of some finite, bounded cardinality. On the other hand, Example 1 from Vaughan-Lee (1983) shows that this class does not always comprise all of the critical algebras in $\mathcal{V}^{(N)}$.

A the very least, perhaps there is a way to bound the height of $(0_C : \beta)$ above β in the lattice $\operatorname{Con}\mathbf{C}$. Theorem 3.18 would then finish the job.

A third strategy is outlined in the following. After giving this result, we shall generalize it, but it still seems helpful to display the proof below, as an example of the general case.

Theorem 3.34. *Let* $\mathbf{C}$ *be a critical algebra in a Mal'cev variety. Then* $\mathbf{C}$ *is either 2-generated, or it is generated by a transversal of its* $\zeta_{\mathbf{C}}$*-classes.*

Proof. Let ζ denote the center of $\mathbf{C}$. We use that the term condition is equivalent to the two-term condition in Mal'cev varieties (a fact which isn't hard to prove directly, but which is also evident from Theorem 2.24). Since $\mathbf{C}$ is critical, there is some equation $t \approx s$ that fails in $\mathbf{C}$ but which is satisfied in all proper factors of $\mathbf{C}$. Since the failure of $t \approx s$ involves a finite witness, say $\mathbf{c} = \langle c_0, \ldots, c_\ell \rangle$, for some natural number ℓ, it is thus evident that $\mathbf{C}$ is generated by $\{c_0, \ldots, c_\ell\}$. Assume that

$t^{\mathbf{C}}(c_0, \ldots, c_\ell) \neq s^{\mathbf{C}}(c_0, \ldots, c_\ell)$ witnesses that $\mathbf{C}$ is critical, but also that ℓ is minimal in this regard.

Suppose that $c_i \, \zeta \, c_j$, for some $i \neq j$. By permuting the variables of t and s, we may assume that $i = 0$ and $j = \ell$. Suppose, too, that $\ell \geq 2$. Let us write c for c_ℓ. Now, from (the contrapositive of) $C_2(\zeta, 1_C; 0_C)$, we learn that one of the following inequalities must hold:

$$t^{\mathbf{C}}(c, c, c, \ldots, c) \neq s^{\mathbf{C}}(c, c, c, \ldots, c),$$
$$t^{\mathbf{C}}(c_0, c, c, \ldots, c) \neq s^{\mathbf{C}}(c_0, c, c, \ldots, c), \text{ or}$$
$$t^{\mathbf{C}}(c, c_1, c_2, \ldots, c_{\ell-1}, c) \neq s^{\mathbf{C}}(c, c_1, c_2, \ldots, c_{\ell-1}, c).$$

But, by the minimality of ℓ, this cannot be. It follows that the elements in $\{c_0, \ldots, c_\ell\}$ must lie in distinct ζ-classes. The claim follows. □

The second part of the theorem just given is worth comparing to Theorem 51.35 of Neumann (1967), which we can now easily generalize:

Theorem 3.35. *If $\mathbf{C}$ is an abelian, critical algebra in a Mal'cev variety $\mathcal{V}$ then $\mathbf{C}$ is 2-generated. If, too, $\mathcal{V}$ is provided with a named constant in its signature, then $\mathbf{C}$ is 1-generated.*

Proof. The first claim is evident from Theorem 3.34. The second claim can be seen by using the named constant in place of c. □

We also find that the previous theorem is a special case of the following, which can be seen as a partial generalization of Proposition 2.13. Let $\mathbf{A}$ be an algebra in a Mal'cev variety. Let n be a natural number. Note that from Theorem 2.37, for any congruences $\theta_0, \ldots, \theta_{n-1}$ on $\mathbf{A}$, we can find a highest $\alpha \in \operatorname{Con} \mathbf{A}$ such that $S_{n+1}(\alpha, \theta_0, \ldots, \theta_{n-1}) = 0_A$. Let $\xi_n(\mathbf{A})$ be the largest $\xi \in \operatorname{Con} \mathbf{A}$ such that $S_{n+1}(\xi, 1_A, \ldots, 1_A) = 0_A$. Note that $\xi_2(\mathbf{A}) = \zeta_{\mathbf{A}}$.

Theorem 3.36. *Let* $\mathbf{C}$ *be a critical algebra in a Mal'cev variety. Then for every natural number* n*,* $\mathbf{C}$ *is either* n*-generated or it is generated by a transversal of its* $\xi_n(\mathbf{A})$*-classes.*

Proof. Let n be a natural number. Denote $\xi_n(\mathbf{A})$ by ξ_n. We use that the higher term condition is equivalent to the higher two-term condition in Mal'cev varieties, as shown in Theorem 2.24. Since $\mathbf{C}$ is critical, there is some equation $t \approx s$ that fails in $\mathbf{C}$ but which is satisfied in all proper factors of $\mathbf{C}$. Since the failure of $t \approx s$ involves a finite witness, say $\mathbf{c} = \langle c_0, \dots, c_\ell \rangle$, for some natural number ℓ, it is thus evident that $\mathbf{C}$ is generated by $\{c_0, \dots, c_\ell\}$: Indeed, the subalgebra generated by this set cannot be proper. Assume that $t^{\mathbf{C}}(c_0, \dots, c_\ell) \neq s^{\mathbf{C}}(c_0, \dots, c_\ell)$ witnesses that $\mathbf{C}$ is critical, but also that ℓ is minimal in this regard.

Suppose that $c_i \; \xi_n \; c_j$, for some $i \neq j$. By permuting the variables of t and s, we may assume that $i = 0$ and $j = \ell$. Suppose, too, that $\ell > n$. For each $r < 2^n - 1$, let δ_r be the endomorphism of the term algebra generated by the usual set of variables with δ_r given by the substitutions

$$\delta_r x_i = x_\ell$$

if $i < n$ and $\beta_r(i) = 0$ or if $i \geq n$ and $\beta_r(n-1) = 0$ but which is otherwise the identity. Now, from (the contrapositive of) $C_2^{n+1}(\xi_n, 1_C, \dots, 1_C; 0_C)$, we learn that for some $r < 2^n - 1$

$$\delta_r s^{\mathbf{C}}(x_0, \dots, x_\ell)[\mathbf{c}] \neq \delta t^{\mathbf{C}}(x_0, \dots, x_\ell)[\mathbf{c}],$$

for else we would have that $s^{\mathbf{C}}(c_0, \dots, c_\ell) = t^{\mathbf{C}}(c_0, \dots, c_\ell)$. But, by the minimality of ℓ, this cannot happen. It follows that the elements in $\{c_0, \dots, c_\ell\}$ must lie in distinct ξ_n-classes. $\square$

Lending more interest to the previous theorem and the strategy it suggests is the following observation.

Proposition 3.37. *Let* $\mathbf{A}$ *be an algebra in a Mal'cev variety. Then*

$$\xi_1(\mathbf{A}) \leq \xi_2(\mathbf{A}) \leq \cdots \leq \xi_n(\mathbf{A}) \leq \xi_{n+1}(\mathbf{A}) \leq \cdots .$$

Proof. For each natural number n, let ξ_n denote $\xi_n(\mathbf{A})$. Let n be any natural number. We wish to show that $\xi_n \leq \xi_{n+1}$. By Proposition 2.32, we find that

$$0_A = S_{n+1}(\xi_n, 1_A, \ldots, 1_A) \geq S_{n+2}(\xi_n, 1_A, \ldots, 1_A),$$

whence the result follows. □

On the other hand, the following would seem to indicate that the strategy given at the beginning of this section is more likely to work that that of Theorem 3.34.

Theorem 3.38. *Let* $\mathbf{A}$ *be a critical algebra in a locally finite Mal'cev variety* $\mathcal{V}$. *Then* $|A| \leq |F_{\mathcal{V}}(n)|$, *where* $n = |F_{\mathcal{V}}(1)|$, *or* $\zeta_{\mathbf{A}} \leq {}^1\Phi_{\mathbf{A}}$.

Proof. Let p be the Mal'cev term for $\mathcal{V}$. Let ζ denote the center of $\mathbf{A}$. Let $\mathbf{M}$ be a maximal, proper subalgebra of $\mathbf{A}$. Suppose that $M\zeta = A$. Since $\mathbf{M}$ is a proper subset of A, we can find a $b \in A \setminus M$. Let $\mathbf{B} = \mathrm{Sg}^{\mathbf{A}}\{b\}$. Note that if $B\zeta = A$, then $\mathbf{A}/\zeta$ is generated by b/ζ: After all, if $a \in A$, then we can find a unary term t such $t^{\mathbf{A}}(b) \mathrel{\zeta} a$ and hence $t^{\mathbf{A}/\zeta}(b/\zeta) = a/\zeta$. By Theorem 3.34, this would entail that $|A| \leq |F_{\mathcal{V}}(n)|$, where $n = |F_{\mathcal{V}}(1)|$. So, we may assume that $B\zeta$ is a proper subset of A.

Let $M \times B\zeta \times_\zeta B$ denote the set of all triples $\langle m, b, b'\rangle \in A^3$ such that $m \in M$, $b \in B\zeta$ and $b' \in B$ such that $b \mathrel{\zeta} b'$. Now, we define a map $\varphi : M \times B\zeta \times_\zeta B \to A$ by $\varphi\langle m, b, b'\rangle = p^{\mathbf{A}}(m, b, b')$. Note that $\mathbf{M} \times \mathbf{B}\zeta \times_\zeta \mathbf{B}$ is a subalgebra of a product of proper factors of $\mathbf{A}$. By Theorem 4.10, it is evident that φ is a homomorphism. We claim that it is also onto. Let $a \in A$. By assumption, we can obtain an $m \in M$ such that $m \mathrel{\zeta} a$. Let $b \in B$. Note then that $p^{\mathbf{A}}(m, a, b) \mathrel{\zeta} b$ and hence $\langle p^{\mathbf{A}}(m, a, b), b\rangle \in B\zeta \times_\zeta B$.

Then by Theorem 4.10 (or Proposition 2.26), we have that

$$\begin{aligned}
p^{\mathbf{A}}(m, p^{\mathbf{A}}(m,a,b), b) &= p^{\mathbf{A}}(p^{\mathbf{A}}(m,a,a), p^{\mathbf{A}}(m,a,b), p^{\mathbf{A}}(a,a,b)) \\
&= p^{\mathbf{A}}(p^{\mathbf{A}}(m,m,a), p^{\mathbf{A}}(a,a,a), p^{\mathbf{A}}(a,b,b)) \\
&= p^{\mathbf{A}}(a,a,a) = a.
\end{aligned}$$

This entails that $\mathbf{A}$ is a homomorphic image of a subalgebra of a product of some of its proper factors, which contradicts the assumption that $\mathbf{A}$ is critical. It follows that $M\zeta = M$, and as $\mathbf{M}$ was an arbitrary maximal, proper subalgebra of $\mathbf{A}$, we have that $\zeta_{\mathbf{A}} \leq {}^1\Phi_{\mathbf{A}}$. □

The following is very similar to the last and, under the conditions of its hypotheses, it is stronger.

Theorem 3.39. *Let k and n be natural numbers so that $k \leq \binom{n}{2}$. Let $\mathbf{C}$ be a critical algebra in a Mal'cev variety $\mathcal{V}$, and suppose that $\mathbf{C}$ is nilpotent of class k. Let $M \in \mathcal{M}_{\mathbf{C}}$, and let $\mu = \mathrm{Cg}^{\mathbf{C}} M^2$. Then either $|\mathcal{M}_{\mathbf{C}}| < 2^m - 1$, where $m = |F_{\mathcal{V}}(n)|$ or, for any $\mathbf{M} \in \mathcal{M}_{\mathbf{C}}$ and $\mu = \mathrm{Cg}^{\mathbf{C}} M^2$, we have that $(0_C : \mu) \leq \mu$. In particular, if $|\mathcal{M}_{\mathbf{C}}| \geq 2^m - 1$, then $\zeta_{\mathbf{C}} \leq \cap\{(0_C : \mathrm{Cg}^{\mathbf{C}} M^2) \mid \mathbf{M} \in \mathcal{M}_{\mathbf{C}}\}$, and $(0_C : \mu)$ is abelian.*

Proof. Let p be a Mal'cev term operation for $\mathbf{A}$. Note first that, by Theorem 3.18, A has at most m μ-classes. Thus, A has at most $2^m - 2$ collections $\mathcal{C}$ of μ-classes such that $\cup\mathcal{C} \notin \{\emptyset, A\}$. Let $\mathcal{M} = \mathcal{M}_{\mathbf{C}}$. Suppose that $|\mathcal{M}| \geq 2^m - 1$. We claim that, for some $\mathbf{M}' \in \mathcal{M}$, $M'\mu = A$. If not, then for all $\mathbf{M}' \in \mathcal{M}$, we have that $M'\mu = M'$, which means that each $M' \in \mathcal{M}$ is a union of M' classes. But, by our initial observation, there is some $\mathbf{M}' \in \mathcal{M}$ that is not a union of μ-classes. Take such an $M' \in \mathcal{M}$, and note that $M'\mu = A$.

Let $\gamma = (0_C : \mu)$, and suppose now that $M\gamma = A$. Now, define $\varphi : M \times_\gamma M \times_\mu M' \to A$ by $\varphi(m_0, m_1, m') = p(m_0, m_1, m')$, where $M \times_\gamma M \times_\mu M'$ denotes the set of all triples $\langle m_0, m_1, m' \rangle \in M \times M \times M'$ such that $m_0 \,\gamma\, m_1 \,\mu\, m'$, noting that it is easily seen to be a subalgebra of $\mathbf{M} \times \mathbf{M} \times \mathbf{M}'$. Note also that by Theorem 2.23 (or by a classic result), φ is a homomorphism. We claim further that φ is onto. Let $a \in \mathbf{A}$. By assumption, we have some $m \in M$ and $m' \in M'$ such that $m \, \gamma \, a \, \mu \, m'$. Note that $m \, \mu \, p(m, a, m') \, \gamma \, m'$ and, in particular, by Theorem 3.21, $p(m, a, m') \in M$. Then, by Lemma 2.23, we have that

$$\begin{aligned} \varphi(m, p(m, a, m'), m') &= p(m, p(m, a, m'), m') \\ &= q(q(a, m, m'), m, m') \\ &= q(q(a, m, m'), q(a, m, a), q(a, a, m')) \\ &= q(a, a, a) = a, \end{aligned}$$

where $q(x, y, z) := p(y, x, z)$. Thus, φ is onto. But, this makes $\mathbf{C}$ a homomorphic image of a subalgebra of a direct product of its proper factors, which contradicts our assumption that $\mathbf{C}$ is critical. It follows that $M(0_C : \mu) = M$. Thus, we have that M is a union of $(0_C : \mu)$-classes, which, since $\mathbf{C}$ is congruence regular (by Theorem A.46), entails that $(0_C : \mu) \leq \mu$. The other claims follow easily. $\square$

Chapter 4

New results on the commutator in varieties with a difference term

We begin with what is unlikely to be a new result, but which is worth promoting here—that is, even if it is not something that has been heretofore overlooked, but simply because it does not seem to have made it into print anywhere and deserves better publicity. Following this, we offer some apparently new results. We shall establish that, in any variety with a difference term, a natural generalization of "upward nilpotence," previously explored (from a somewhat different perspective) by J.D.H. Smith (see Smith (1976), pp. 42-43) as a generalization of the concept of "upward central series" from group theory, is equivalent to the traditional notion of nilpotence—which we shall call "downward nilpotence." Applying this, we show that the set of equations given by Freese and McKenzie (1987) in Theorem 14.2 as a characterization of nilpotence (of fixed class) for congruence modular varieties also works if only the availability of a difference term is assumed. In the process of obtaining these, we also establish further results concerning the commutator in difference term varieties that may be of independent interest. In particular, we offer new order theoretic properties of the commutator in varieties with a difference term, a new condition concerning when homomorphism will commute with the commutator, and a property concerning affine behavior. We also argue that several of these properties are at least nearly "sharp."

4.1 A remark on varieties with a weak difference term

Definition 4.1. Let $\mathcal{V}$ be a variety with ternary term w such that for any $\mathbf{A} \in \mathcal{V}$, any $\theta \in \operatorname{Con} \mathbf{A}$, and any $\langle a, b \rangle \in \theta$, we have that

$$w(a, b, b)\,[\theta, \theta]\,a\,[\theta, \theta]\,w(b, b, a).$$

We say that w is a *weak difference term for* $\mathcal{V}$.

This concept has been studied by Lipparini (1994) and Mamedov (2007); see also Hobby and McKenzie (1988), especially their Theorem 9.6 for a related result.

Recall the finite basis result of Freese and Vaughan-Lee given in Freese and McKenzie (1987) and Vaughan-Lee (1983), and given above as Theorem 2.29. We assert that the following apparent broadening of their result holds.

Theorem 4.2. *Let* $\mathbf{A}$ *be a finite nilpotent algebra in a variety with a weak difference term. Suppose that* $\mathbf{A}$ *is the direct product of algebras of prime power order. Then* $\mathbf{A}$ *has a finitely based equational theory.*

Actually, the theorem of Freese and Vaughan-Lee has something further to say, concerning special terms of the variety generated by $\mathbf{A}$ called commutator terms. We could include a parallel statement here, but we leave this matter until another time. For now, our purpose is simply to point out that this ostensibly new result is a trivial consequence of the following observation, which does not seem to have made it into print.

Theorem 4.3. *Let* $\mathcal{V}$ *be a variety with a weak difference term. Let* $\mathbf{A}$ *be a solvable algebra in* $\mathcal{V}$*. Then* $\mathbf{A}$ *has a Mal'cev term. In particular, since nilpotence always implies solvability, every nilpotent algebra in* $\mathcal{V}$ *also has a Mal'cev term.*

Freese and Vaughan-Lee's result might be said to properly concern Mal'cev algebras; since nilpotent (even solvable) algebras in a congruence modular variety generate a Mal'cev variety, they were able to state it as strongly as they did. Thus, this result, although establishing that the result of Freese and Vaughan-Lee can be stated even more strongly, still properly concerns Mal'cev algebras.

In Exercise 9, Ch. 6, of Freese and McKenzie (1987), we are invited to make the following observations. Given a variety with a difference term d, for each natural number n, we define a ternary term d_n as follows. Let $d_0(x, y, z) = z$, and for $n > 0$, set $d_n(x, y, z) = d(x, d_{n-1}(x, y, y), d_{n-1}(x, y, z))$. Note, of course, that $d_1(x, y, z) = d(x, y, z)$. We first observe that

Proposition 4.4. *Let* $\mathbf{A}$ *be an algebra with a difference term operation* d*. Then for all natural numbers* n*,* $d_n(x, y, y)\,[\theta]_n\,x$ *whenever* $\langle x, y\rangle \in \theta \in \operatorname{Con}\mathbf{A}$*. (See Definitions A.39 and A.45 for clarification.)*

Proof. We shall induct on n. For the basis, note that $[\theta]_0 = \theta$. Thus, the basis is trivial. Now, assuming that the proposition holds for $n = k - 1$, we find that $d_k(x, y, y) = d(x, d_{k-1}(x, y, y), d_{k-1}(x, y, y))\,[\theta]_k\,x$, since d is a difference term. □

The above lends itself immediately to the following.

Corollary 4.5. *Let* $\mathbf{A}$ *be an algebra with a difference term operation. Let* n *be any natural number. If* $\mathbf{A} \in \mathcal{V}$ *is solvable of class* n*, then* d_n *is a Mal'cev term for* $\mathbf{A}$*.*

Proof. In light of Proposition 4.4, we need only note here that

$$\mathbf{A} \models d_n(x, x, y) \approx y.$$

This can easily be shown by inducting on n, using only the fact that this holds for $n = 1$ (solvability is not used in this part of the proof). □

Let $\mathcal{V}$ be a variety with a weak difference term. Through a similar construction, we can also show that any solvable algebra in $\mathcal{V}$ has a difference term operation, and hence a Mal'cev term operation. Define $w_1(x, y, z) = w(x, y, z)$ and for any $n > 1$, let

$$w_n(x, y, z) = w(w_{n-1}(x, y, z), w_{n-1}(y, y, z), z).$$

Lemma 4.6. *Let* $\mathbf{A}$ *be an algebra with a weak difference term operation. Let* θ *be a congruence of* $\mathbf{A}$*, and let* $\langle x, y\rangle \in \theta$*. Then for all natural numbers* $n > 0$*,*

$$w_n(x, y, y)\,[\theta, \theta]\,x,$$

and

$$w_n(x, x, y)\,[\theta]_n\,y.$$

Proof. We induct on n; the basis follows from Definition 4.1. For the inductive step, we observe that, by inductive hypothesis,

$$w_n(x, y, y) = w(w_{n-1}(x, y, y), w_{n-1}(y, y, y), y)\,[\theta, \theta]\,w(x, y, y)\,[\theta, \theta]\,x.$$

Also, by inductive hypothesis, we have that $w_{n-1}(x, x, y)\,[\theta]_{n-1}\,y$. Thus, since w is a weak difference term, we get that

$$w_n(x, x, y) = w(w_{n-1}(x, x, y), w_{n-1}(x, x, y), y)\,[\theta]_n\,y.$$

Thus, the claim follows by induction. □

In particular, the following soon follows.

Theorem 4.7. *Let* $\mathcal{V}$ *be a variety with a weak difference term* w*. Let* $\mathbf{A}$ *be a solvable algebra in* $\mathcal{V}$*. Then* $\mathbf{A}$ *has a difference term operation and hence a Mal'cev term operation.*

Proof. Let n be the solvability class of $\mathbf{A}$. By Proposition 4.6, we have that $\mathbf{A}$ has a difference term $d := w_n$. Then, by Proposition 4.5, we may conclude that d_n is a Mal'cev term for $\mathbf{A}$. Since such is characterized by satisfaction of some equations satisfied by $\mathbf{A}$, we have also that the variety generated by $\mathbf{A}$ is Mal'cev. □

4.2 A new result on affine behavior in difference term varieties

In his 1995 paper, *Varieties with a difference term*, Keith Kearnes obtains, as Lemma 2.9, the following partial generalization of a result of Freese and McKenzie concerning the commutator in congruence modular varieties, given in (1987) as Theorem 5.7.

Theorem 4.8. *For $\mathbf{A} \in \mathcal{V}$, a variety with difference term d and $\alpha \in \operatorname{Con} \mathbf{A}$, the following conditions are necessary and sufficient to exhibit $[\alpha, \alpha] = 0_A$:*

- *For any fundamental operation s (and hence for any term operation) of arity, say, n, and $x_i \,\alpha\, y_i \,\alpha\, z_i$, $i = 1, \ldots, n$,*

  $$d(s(\mathbf{x}), s(\mathbf{y}), s(\mathbf{z})) = s(d(x_1, y_1, z_1), \ldots, d(x_n, y_n, z_n)).$$

  and

- *For any $x \,\alpha\, y$,*

  $$y = d(y, x, x) = d(x, x, y).$$

Remark 4.9. It seems rather clear (though I haven't fastidiously checked it) that for $\mathbf{A} \in \mathcal{V}$, a variety with a weak difference term w, a similar result holds with "weak difference term" replacing "difference term."

Now, it turns out that a stronger version of this theorem is also true—in fact, Theorem 5.7 from Freese and McKenzie (1987) extends intact to varieties with a difference term, as shown in the following. Following its proof, we shall apply this result to extend Freese and McKenzie's characterization of the center of an algebra in a congruence modular varieties to algebras; it works also if one only assumes the presence of a difference term. This latter finding enables us to similarly characterize the upward central series of any algebra in a difference term variety. This, in turn, we use to prove the equivalence of upward and downward nilpotence in a difference term variety, which is enough to implicitly demonstrate that the equational characterization of nilpotence in congruence modular varieties, given by Freese and McKenzie (1987) as Theorem 14.2, works also in difference term varieties. We do give an explicit proof of this, however.

Theorem 4.10. *For* $\mathbf{A} \in \mathcal{V}$*, a variety with difference term* d *and* $\beta \leq \alpha$ *from* $\mathrm{Con}\,\mathbf{A}$*, the following conditions are necessary and sufficient to exhibit* $[\beta, \alpha] = 0_A$*:*

- *For any fundamental operation* s *(and hence for* s *any term operation) of arity, say,* n*, and all* $x_i \,\beta\, y_i \,\alpha\, z_i$*,* $i = 1, \ldots, n$*,*

$$d(s(\mathbf{x}), s(\mathbf{y}), s(\mathbf{z}))) = s(d(x_1, y_1, z_1), \ldots, d(x_n, y_n, z_n)).$$

  and

- *For any* $x \,\beta\, y$*,* $y = d(y, x, x) = d(x, x, y)$*.*

Proof. We begin with a brief

Lemma 4.11. *Let* $\mathbf{A} \in \mathcal{V}$*, a variety with a difference term, and* $\alpha \geq \beta \in \mathrm{Con}\,\mathbf{A}$ *for which* $[\beta, \alpha] = 0_A$*. Then for any* $x, y \in A$*, if*

(i) $\langle x, z\rangle \,\Delta_\alpha^\beta\, \langle y, z\rangle$ *for some* z

or

(ii) $\langle z, x\rangle \,\Delta_\alpha^\beta\, \langle z, y\rangle$ *for some* z

then $x = y$*.*

Proof. We prove that (ii) implies the conclusion, the other case having a similar proof. So suppose (ii) holds for some x, y, and z. In light of Mal'cev's description of congruence generation (Proposition A.9) we get that $x \,\beta\, y$. Thus, using the definition of Δ_α^β, we find that

$$\langle z, x\rangle \,\Delta_\alpha^\beta\, \langle z, x\rangle$$

$$\langle z, x\rangle \,\Delta_\alpha^\beta\, \langle z, y\rangle$$

$$\langle x, x\rangle \,\Delta_\alpha^\beta\, \langle y, y\rangle.$$

Applying d "vertically" (and using also that $[\beta, \beta] \leq [\beta, \alpha] = 0_A$), we get that

$$\langle x, x\rangle \,\Delta_\alpha^\beta\, \langle y, x\rangle.$$

Now, by Remark A.38, the claim holds. $\square$

Let $\mathbf{A} \in \mathcal{V}$ and $\alpha, \beta \in \operatorname{Con} \mathbf{A}$, be as described in the hypotheses. First, suppose that $[\beta, \alpha] = 0_A$. Then since d is a difference term and $[\beta, \beta] \leq [\beta, \alpha] = 0_A$, we get the second bullet immediately. Now, choose fundamental operation s of arity, say, n and $x_i \,\beta\, y_i \,\alpha\, z_i$, $i = 1, \ldots, n$. Also, let $x, y, z \in A$ with $x \,\beta\, y \,\alpha\, z$. Since d is a difference term and $[\beta, \beta] \leq [\alpha, \beta] = 0_A$, we can apply d vertically to

$$\langle x, x\rangle \,\Delta_\alpha^\beta\, \langle y, y\rangle$$

$$\langle y, x\rangle \,\Delta_\alpha^\beta\, \langle y, x\rangle$$

$$\langle z, x\rangle \,\Delta_\alpha^\beta\, \langle z, x\rangle$$

to obtain that $\langle d(x, y, z), x\rangle \,\Delta_\alpha^\beta\, \langle z, y\rangle$. We now apply this observation in two ways. Since $s(\mathbf{x}) \,\beta\, s(\mathbf{y}) \,\alpha\, s(\mathbf{z})$, we have that

$$\langle d(s(\mathbf{x}), s(\mathbf{y}), s(\mathbf{z})), s(\mathbf{x})\rangle \,\Delta_\alpha^\beta\, \langle s(\mathbf{z}), s(\mathbf{y})\rangle.$$

Also, for each $i = 1, \ldots, n$ we have that

$$\langle d(x_i, y_i, z_i), x_i\rangle \,\Delta_\alpha^\beta\, \langle z_i, y_i\rangle.$$

Applying s to the tuple given on the left and right sides of the line above then yields

$$\langle s(d(x_1, y_1, z_1), \ldots, d(x_n, y_n, z_n)), s(\mathbf{x})\rangle \,\Delta_\alpha^\beta\, \langle s(\mathbf{z}), s(\mathbf{y})\rangle.$$

After using transitivity of Δ_{α}^{β}, we can use Lemma 4.11 (ii) to obtain the first bullet.

We now assume that the bulleted conditions hold and prove that $[\beta, \alpha] = 0_A$ (using, of course, too, that $\beta \leq \alpha$). We claim that under our assumptions, we get that

$$\langle x, y\rangle \, \Delta_{\beta}^{\alpha} \, \langle u, v\rangle \text{ if and only if } x \beta \, y \, \alpha \, u \text{ and } v = d(y, x, u).$$

Let Δ' be the binary relation on β characterized by the second part in the line above. Notice first that for $\langle x, y\rangle$ and $\langle u, v\rangle$ as described on the right in the displayed line above, $v = d(y, x, u) \, \beta \, d(y, y, u) = u$, and hence Δ' is indeed a subset of $\beta \times \beta$. It is important to note, too, that, since $\beta \leq \alpha$, we have that $x \; \alpha \; y \; \alpha \; u \; \alpha \; v$, for any $\langle\langle x, y\rangle, \langle u, v\rangle\rangle \in \Delta'$.

We first show that Δ' is a congruence on β. To see that Δ' is reflexive, take any $\langle x, y\rangle \in \beta$. Then, since $\beta \leq \alpha$, we get $x \, \beta \, y \, \alpha \, x$ and, by the second bullet,

$$y = d(y, x, x),$$

which puts $\langle x, y\rangle \, \Delta' \, \langle x, y\rangle$. Now assume that $\langle x, y\rangle \, \Delta' \, \langle u, v\rangle$. Using that $\beta \leq \alpha$, we have that $v = d(y, x, u) \; \alpha \; d(x, x, x) = x$. Thus, $u \, \beta \, v \, \alpha \, x$. Also, by the first bullet, using $d' := d$ in the place of s, we discover that

$$\begin{aligned} d(v, u, x) &= d'(d(y, x, u), d(x, x, u), d(x, x, x)) \\ &= d(d'(y, x, x), d'(x, x, x), d'(u, u, x)) \\ &= d(d'(y, x, x), x, x) = y, \end{aligned}$$

where we have used the second bullet twice to obtain the last equality. Thus, we find that Δ' is symmetric.

To see that it is transitive, suppose that

$$\langle x, y\rangle \, \Delta' \, \langle u, v\rangle \, \Delta' \, \langle z, w\rangle.$$

For ease of reference, notice that this entails that $x \, \beta \, y \, \alpha \, u \, \beta \, v \, \alpha \, z$, $v = d(y, x, u)$, and $w = d(v, u, z)$. Again using that $\beta \leq \alpha$, we have that $y \, \alpha \, z$, and so $x \, \beta \, y \, \alpha z$. Note, too, that $u \,\alpha\, v \,\alpha\, z$. Using the equations just above and the bulleted conditions (again, with $d' := d$ in the place of s), we also have that

$$\begin{aligned} d(y, x, z) &= d'(d(y, x, x), d(x, x, x), d(u, u, z)) \\ &= d(d'(y, x, u), d'(x, x, u), d'(x, x, z)) \\ &= d(v, u, z) = w. \end{aligned}$$

It follows that Δ' is transitive.

That Δ' respects the operations of $\boldsymbol{\beta}$ follows immediately from the first bullet, the fact that β and α respect the operations of $\mathbf{A}$, that operations on $\boldsymbol{\beta}$ are computed coordinate-wise, and that $\beta \leq \alpha$. We observe this computation now. Suppose that f is a fundamental operation of arity n , and $\langle x_i, y_i \rangle \,\Delta'\, \langle u_i, v_i \rangle$ for $i = 1, \ldots, n$. Writing out what this means, we get that for $i = 1, \ldots, n$, $x_i \,\beta\, y_i \,\alpha\, u_i$ and $v_i = d(y_i, x_i, u_i)$. Since α and β respect f, we immediately get that

$$f(\mathbf{x}) \,\beta\, f(\mathbf{y}) \,\alpha\, f(\mathbf{u}).$$

Using the first bullet, with f in the place of s, we also get that

$$f(\mathbf{v}) = f(d(y_1, x_1, u_1), \ldots, d(y_n, x_n, u_n)) = d(f(\mathbf{y}), f(\mathbf{x}), f(\mathbf{u})).$$

Finally, we observe that in $\boldsymbol{\beta}$, we compute that, for any n-tuples $\mathbf{a}$ and $\mathbf{b}$ from A,

$$f^{\beta}(\langle a_1, b_1 \rangle, \ldots, \langle a_n, b_n \rangle) = \langle f^{\mathbf{A}}(\mathbf{a}), f^{\mathbf{A}}(\mathbf{b}) \rangle.$$

Thus, Δ' is a congruence on $\boldsymbol{\beta}$.

Note that for any $x \,\alpha\, y$, reflexivity of β and the equation $y = d(x, x, y)$ puts $\langle x, x \rangle \,\Delta'\, \langle y, y \rangle$; thus we have that the generators of Δ^{α}_{β} are contained in congruence Δ' and hence $\Delta^{\alpha}_{\beta} \subseteq \Delta'$.

Now take $\langle x, y\rangle \,\Delta'\, \langle u, v\rangle$. Then $x \,\beta\, y \,\alpha\, u$ and $v = d(y, x, u)$. In particular, $x \,\alpha\, u$ and so $\langle x, x\rangle \,\Delta^{\alpha}_{\beta}\, \langle u, u\rangle$. Thus, using also the second bullet,

$$\begin{aligned}
\langle x, y\rangle &= \langle d(x, x, x), d(y, x, x)\rangle \\
&= d(\langle x, y\rangle, \langle x, x\rangle, \langle x, x\rangle) \\
&\Delta^{\alpha}_{\beta}\, d(\langle x, y\rangle, \langle x, x\rangle, \langle u, u\rangle) \\
&= \langle d(x, x, u), d(y, x, u)\rangle \\
&= \langle u, v\rangle
\end{aligned}$$

We thus conclude that $\Delta' = \Delta^{\alpha}_{\beta}$, as claimed.

We will use this observation in concert with another claim, which we add now. Under the present assumptions, we hold that

$$[\alpha, \beta] \subseteq \{\langle x, y\rangle \mid \langle x, x\rangle \,\Delta^{\alpha}_{\beta}\, \langle x, y\rangle\}.$$

Let

$$\theta := \{\langle x, y\rangle \in [\alpha, \beta] \mid \langle x, x\rangle \,\Delta^{\alpha}_{\beta}\, \langle x, y\rangle\}.$$

We wish to show that θ comprises the whole of $[\alpha, \beta]$. Using our characterization of Δ^{α}_{β} just given we will then quickly finish the proof.

We first show that θ is a congruence. Reflexivity is immediate from the reflexivity of $[\alpha, \beta]$ and Δ^{α}_{β}. Now, suppose that $\langle x, y\rangle \in [\alpha, \beta]$ and $\langle x, x\rangle \Delta^{\alpha}_{\beta} \langle x, y\rangle$. Using reflexivity of Δ^{α}_{β}, we get that

$$\begin{aligned}
&\langle x, x\rangle \,\Delta^{\alpha}_{\beta}\, \langle x, x\rangle, \\
&\langle x, x\rangle \,\Delta^{\alpha}_{\beta}\, \langle x, y\rangle, \\
&\langle y, y\rangle \,\Delta^{\alpha}_{\beta}\, \langle y, y\rangle.
\end{aligned}$$

Of course, by definition of Δ^{α}_{β}, we have $x \,\beta\, y$, and, using the second bullet, we can apply d "vertically" to the left and right sides above to obtain

$$\langle y, y\rangle \,\Delta^{\alpha}_{\beta}\, \langle y, x\rangle.$$

We now need only notice symmetry of $[\alpha, \beta]$ to conclude that θ is symmetric.

Similarly, to find that θ is transitive, we suppose that $x \,\theta\, y \,\theta\, z$. Immediately, we get $\langle x, z\rangle \in [\alpha, \beta]$, by the transitivity of that relation. We apply d in the same way as above, this time to the left and right sides of

$$\langle x, x\rangle \,\Delta^{\alpha}_{\beta}\, \langle x, y\rangle$$
$$\langle y, y\rangle \,\Delta^{\alpha}_{\beta}\, \langle y, y\rangle$$
$$\langle y, y\rangle \,\Delta^{\alpha}_{\beta}\, \langle y, z\rangle$$

to conclude that $\langle x, x\rangle \,\Delta^{\alpha}_{\beta}\, \langle x, z\rangle$.

That θ respects the operations of $\mathbf{A}$ is an immediate consequence of the facts that $[\alpha, \beta]$ and Δ^{α}_{β} both respect the operations of their respective algebras and that operations are computed coordinate-wise on $\boldsymbol{\beta}$. So, θ is a congruence on $\mathbf{A}$ contained in $[\alpha, \beta]$.

Now, by Theorem A.37, we have that $[\alpha, \beta]$ is the least congruence γ on $\mathbf{A}$ so that $\gamma \cap \beta$ is the union of Δ^{α}_{β}-classes. We contend that θ is also the union of Δ^{α}_{β}-classes. To see this, suppose that $\langle x, y\rangle \in \theta$ and that $\langle x, y\rangle \,\Delta^{\alpha}_{\beta}\, \langle u, v\rangle$. Since $\theta \subseteq [\alpha, \beta]$ and the latter is a union of Δ^{α}_{β}-classes, we get that $\langle u, v\rangle \in [\alpha, \beta]$. But also $\langle x, x\rangle \,\Delta^{\alpha}_{\beta}\, \langle x, y\rangle$ and so, by transitivity of Δ^{α}_{β}, $\langle x, x\rangle \,\Delta^{\alpha}_{\beta}\, \langle u, v\rangle$. By Mal'cev's characterization of congruence generation A.9, we evidently have that $x \,\alpha\, u$. Thus, $\langle u, u\rangle \,\Delta^{\alpha}_{\beta}\, \langle x, x\rangle \,\Delta^{\alpha}_{\beta}\, \langle u, v\rangle$, which puts $\langle u, v\rangle \in \theta$. Thus, the contention is good, and so θ is all of $[\alpha, \beta]$.

Now, take an arbitrary $x \,[\beta, \alpha]\, y$. By Theorem A.40, $x \,[\alpha, \beta]\, y$. Then, as we have just seen, $\langle x, x\rangle \,\Delta^{\alpha}_{\beta}\, \langle x, y\rangle$. But since $\Delta^{\alpha}_{\beta} = \Delta'$, we get that $y = d(x, x, x) = x$. Thus, $[\beta, \alpha] = 0_A$, as claimed. This finishes the proof. □

The following was noted by Kearnes.

Corollary 4.12. *In a variety $\mathcal{V}$ with a difference term, every abelian algebra is affine and, conversely, every affine algebra is abelian.*

For an explanation of what is meant by "affine" see Theorem 3.5.

Theorem 4.10 enables us to construct useful generators for $[\beta, \alpha]$, for any congruences β and α of $\mathbf{A}$ such that $\beta \leq \alpha$, for a given algebra $\mathbf{A}$ in a difference term variety.

Theorem 4.13. *Let $\mathcal{V}$ a be variety with a difference term d and equipped with fundamental operation symbols F. Let $\mathbf{A} \in \mathcal{V}$, and let $\beta, \alpha \in \operatorname{Con} \mathbf{A}$ such that $\beta \leq \alpha$. Then $[\beta, \alpha] = \operatorname{Cg} G$, where*

$$G := \{\langle d^{\mathbf{A}}(f^{\mathbf{A}}(\mathbf{x}), f^{\mathbf{A}}(\mathbf{y}), f^{\mathbf{A}}(\mathbf{z})), f^{\mathbf{A}}(d^{\mathbf{A}}(x_1, y_1, z_1), \ldots, d^{\mathbf{A}}(x_n, y_n, z_n))\rangle \mid \\ f \in F \text{ and } x_i \,\beta\, y_i \,\alpha\, z_i\} \cup \{\langle y, d^{\mathbf{A}}(y, x, x)\rangle \mid x \,\beta\, y\}$$

Proof. Write d for $d^{\mathbf{A}}$. Let $\theta := \operatorname{Cg} G$, where G is as above. Using Theorem 4.10 and a basic commutator fact that holds in any algebra—namely that

$$[\beta/[\beta, \alpha], \alpha/[\beta, \alpha]] = 0_{A/[\beta,\alpha]}$$

—one soon finds that $\theta \subseteq [\beta, \alpha]$: Take any $f \in F$ of arity, say, n. Let us write f for $f^{\mathbf{A}}$, as well. Then, since $[\beta, \alpha] \subseteq \alpha \cap \beta$, we get that given $x_i \,\beta\, y_i \,\alpha\, z_i (i = 1, \ldots, n)$,

$$x_i/[\beta, \alpha] \;\beta/[\beta, \alpha]\; y_i/[\beta, \alpha] \;\beta/[\beta, \alpha]\; z_i/[\beta, \alpha],$$

and so, by Theorem 4.10,

$$d(f(\mathbf{x}), f(\mathbf{y}), f(\mathbf{z})) \;[\beta, \alpha]\; f(d(x_1, y_1, z_1), \ldots, d(x_n, y_n, z_n)).$$

Similarly, if $x \,\beta\, y$, then using the theorem again, we get that

$$y \;[\beta, \alpha]\; d(y, x, x).$$

It follows that $\theta \subseteq [\beta, \alpha]$, and, in particular, $\theta \subseteq \alpha \cap \beta$.

To get the reverse inclusion, we need only check that $C(\beta, \alpha; \theta)$. Now, evidently, by Theorem 4.10 we have that $[\beta/\theta, \alpha/\theta] = 0_{A/\theta}$. Thus, $C(\beta/\theta, \alpha/\theta; 0_{A/\theta})$. By Proposition A.28 we then get that $C(\beta, \alpha; \theta)$. $\square$

4.3 The equivalence of upward and downward nilpotence in varieties with a difference term, and an application

A key result of this section concerns a generalization of the "upper central series" from group theory. A generalization of this was worked out by Smith (1976) (see pages 42-43 in Smith's work) for congruence permutable varieties but does not seem to have been used much since—although, it is certainly implicit in the proof of Theorem 14.2 from Freese and McKenzie (1987). We shall first define the natural generalization of this group theoretic concept, using the term condition to define the center of an algebra.

Throughout this section, for a given algebra $\mathbf{A}$, we shall use $\zeta_{\mathbf{A}}$ to denote the center of $\mathbf{A}$, which is defined as the largest $\zeta \in \operatorname{Con} \mathbf{A}$ such that $C(\zeta, 1_A; 0_A)$ holds. (See Definition A.29 in the appendix.)

Definition 4.14. For a given algebra $\mathbf{A}$, set

$$\zeta_{\mathbf{A}}^0 := 0_A$$

and for $k \geq 1$ define

$$\mathbf{A_k} := \mathbf{A}/\zeta_{\mathbf{A}}^{k-1},$$

and let $\zeta_{\mathbf{A}}^k$ be the (unique) preimage of $\zeta_{\mathbf{A_k}}$ under the isomorphism of the interval $I[\zeta_{\mathbf{A}}^{k-1}, 1_A]$ onto $\operatorname{Con} \mathbf{A_k}$ that is provided by the correspondence theorem.

We say that $\mathbf{A}$ is *upward nilpotent of class k* whenever $\zeta_{\mathbf{A}}^k = 1_A$.

Remark 4.15. . For a given algebra $\mathbf{A}$,

$$0_A = \zeta_{\mathbf{A}}^0 \leq \cdots \leq \zeta_{\mathbf{A}}^k \leq \zeta_{\mathbf{A}}^{k+1} \leq \cdots \leq 1_A.$$

We shall call this chain of congruences the *upper central series of* $\mathbf{A}$.

Recall that for any algebra $\mathbf{A}$ and any $\alpha, \beta \in \operatorname{Con} \mathbf{A}$, we use Proposition A.28 (b) to define $(\alpha : \beta)$ as the highest $\gamma \in \operatorname{Con} \mathbf{A}$ such that $C(\gamma, \beta; \alpha)$. We shall have repeated need of the following fact.

Proposition 4.16. *Let* $\mathbf{A}$ *be an algebra with congruences* α, β*. Then* $(0_{A/\alpha} : \beta/\alpha) = (\alpha : \beta)/\alpha$*.*

Proof. Note that since $C(\alpha, \beta; \alpha)$ always holds (Proposition A.28 (f)) we have that $\alpha \leq (\alpha : \beta)$. Thus, by Proposition A.28 (e) we find that $C((\alpha : \beta)/\alpha, \beta/\alpha; 0_{A/\alpha})$ and hence $(\alpha : \beta)/\alpha \leq (0_{A/\alpha} : \beta/\alpha)$. On the other hand, if γ is the unique congruence above α so that $\gamma/\alpha = (0_{A/\alpha} : \beta/\alpha)$ (provided by the correspondence theorem A.16) then from Proposition A.28 (f) and the fact that $C(\gamma/\alpha, \beta/\alpha; 0_{A/\alpha})$, we may conclude that $C(\gamma, \beta; \alpha)$. Thus, $\gamma \leq (\alpha : \beta)$ and so $(0_{A/\alpha} : \beta) = \gamma/\alpha \leq (\alpha : \beta)/\alpha$. $\square$

Proposition 4.17. *Let* $\mathbf{A}$ *be any algebra. Then, for all natural numbers* k*,* $\zeta_{\mathbf{A}}^{k+1} = (\zeta_{\mathbf{A}}^{k} : 1_A)$*.*

Proof. For convenience, we suppress the subscript $\mathbf{A}$, writing ζ^k for $\zeta_{\mathbf{A}}^k$.

From the definition of ζ^k, we know that $C(\zeta^k/\zeta^{k-1}, 1_{A/\zeta^{k-1}}; 0_{A/\zeta^{k-1}})$. We also have that $\zeta^{k-1} \subseteq \zeta^k$. Thus, by Proposition A.28 (e) and from the obvious fact that $1_{A/\theta} = 1_A/\theta$ for any congruence θ, we deduce that $C(\zeta^k, 1_A; \zeta^{k-1})$. Thus, $\zeta^k \subseteq (\zeta^{k-1} : 1_A)$.

Now, from Proposition A.28 (f), we have that $C(\zeta^{k-1}, 1_A; \zeta^{k-1})$, and hence $\zeta^{k-1} \subseteq (\zeta^{k-1} : 1_A)$. We can then use the correspondence theorem and Proposition A.28 (e), again, to see that

$$C((\zeta^{k-1} : 1_A)/\zeta^{k-1}, 1_{A/\zeta^{k-1}}; 0_{A/\zeta^{k-1}}).$$

By the definition of ζ^k, then, $(\zeta^{k-1} : 1_A) \subseteq \zeta^k$. $\square$

This suggests another nice way of notating the upper central series, which helps to generalize it.

Definition 4.18. Let $\mathbf{A}$ be an algebra. We define $\zeta : \operatorname{Con} \mathbf{A} \to \operatorname{Con} \mathbf{A}$ by $\zeta(\theta) := (\theta : 1_A)$, for any $\theta \in \operatorname{Con} \mathbf{A}$. Let us also write $\zeta(\mathbf{A})$ for $\zeta(0_A) = \zeta_{\mathbf{A}}$. We then iterate ζ in the usual way: For all $\theta \in \operatorname{Con} \mathbf{A}$, let $\zeta^0(\theta) := \theta$ while for $n > 0$ define $\zeta^n(\theta) := \zeta(\zeta^{n-1}(\theta))$.

Note that, for all natural numbers n, $\zeta^n_{\mathbf{A}} = \zeta^n(0_A) = \zeta^n(\mathbf{A})$. We also may very well get some usefulness out of replacing 1_A in the above definition with an arbitrary $\beta \in \operatorname{Con} \mathbf{A}$. We do this now.

Definition 4.19. Let $\mathbf{A}$ be any algebra. Let $\beta \in \operatorname{Con} \mathbf{A}$. Let $\mathcal{Z}_{(\beta)} : \operatorname{Con} \mathbf{A} \to \operatorname{Con} \mathbf{A}$ be given by $\mathcal{Z}_{(\beta)}\alpha = (\alpha : \beta)$, for any $\alpha \in \operatorname{Con} \mathbf{A}$. Now, let $\alpha \in \operatorname{Con} \mathbf{A}$. Set $\mathcal{Z}^0_{(\beta)}\alpha := \alpha$ and for all natural numbers $n > 0$, let $\mathcal{Z}^n_{(\beta)}\alpha := \mathcal{Z}_{(\beta)}\mathcal{Z}^{n-1}_{(\beta)}\alpha$. For example, $\mathcal{Z}^2_{(\beta)}\alpha = \mathcal{Z}_{(\beta)}\mathcal{Z}_{(\beta)}\alpha = \mathcal{Z}_{(\beta)}(\alpha : \beta) = ((\alpha : \beta) : \beta)$. Also, for any $\theta \in \operatorname{Con} \mathbf{A}$ and all natural numbers n, $\zeta^n(\theta) = \mathcal{Z}_{(1_A)}(0_A)$. Let us call these *annihilator operations*.

Remark 4.20. Let $\mathbf{A}$ be any algebra. Let $\alpha, \beta \in \operatorname{Con} \mathbf{A}$. Then

$$\alpha = \mathcal{Z}^0_{(\beta)}\alpha \leq \mathcal{Z}^1_{(\beta)}\alpha \leq \cdots \leq \mathcal{Z}^n_{(\beta)}\alpha \leq \mathcal{Z}^{n+1}_{(\beta)}\alpha \leq \cdots .$$

Proof. Let n be a natural number. By definition $\mathcal{Z}^{n+1}_{(\beta)}\alpha$ is the largest $\gamma \in \operatorname{Con} \mathbf{A}$ such that $C(\gamma, \beta; \mathcal{Z}^n_{(\beta)}\alpha)$. Now, since $C(\mathcal{Z}^n_{(\beta)}\alpha, \beta; \mathcal{Z}^n_{(\beta)}\alpha)$ holds, the claim follows. $\square$

Definition 4.21. Let $\mathbf{A}$ be an algebra. Let $\psi \in \operatorname{Con} \mathbf{A}$. Similarly, let $\mathcal{C}_{(\psi)} : \operatorname{Con} \mathbf{A} \to \operatorname{Con} \mathbf{A}$ be given by $\mathcal{C}_{(\psi)}\theta = [\theta, \psi]$, for any $\theta \in \operatorname{Con} \mathbf{A}$. Now define $\mathcal{C}^n_{(\psi)}$ by iterating this functions in the usual way (with the 0^{th} power denoting the identity function.) In particular, for all natural numbers n, $[1_A)_n = \mathcal{C}^n_{(1_A)}1_A$. (These operators are also defined in McKenzie (1987b), section 3, although his notation would probably not be advisable for use in the context below.)

Proposition 4.22. *Let $\mathbf{A}$ be an algebra with congruences $\psi \leq \psi'$ and $\theta \leq \theta'$. Then for all natural numbers n, $\mathcal{C}^n_{(\psi)}\theta \leq \mathcal{C}^n_{(\psi')}\theta'$.*

Proof. This follows easily from the monotonicity of the commutator (Proposition A.30) and induction. $\square$

On the other hand, the order theoretic properties of an annihilator operation appear to be a bit more complicated. We need use of the following, which appears as Proposition 4.2 in Freese and McKenzie (1987). It has many consequences.

Proposition 4.23. *Let* $\mathbf{A}$ *be an algebra in a congruence modular variety. Let* $\alpha, \beta, \delta \in \operatorname{Con} \mathbf{A}$*. Then* $C(\alpha, \beta; \delta)$ *if and only if* $[\alpha, \beta] \leq \delta$

A restricted version of Proposition 4.23 holds in varieties with a difference term, as we shall see below (and as noted in Kearnes (1995)).

Proposition 4.24. *Let* $\mathbf{A}$ *be an algebra in a congruence modular variety. Let* $\varphi, \theta, \psi \in \operatorname{Con} \mathbf{A}$ *such that* $\varphi \leq \theta$*. Then* $\mathcal{Z}_{(\psi)}\varphi = (\varphi : \psi) \leq (\theta : \psi) = \mathcal{Z}_{(\psi)}\theta$*. Thus, for all natural numbers* n*.* $\mathcal{Z}^n_{(\psi)}\varphi \leq \mathcal{Z}^n_{(\psi)}\theta$

Proof. By Proposition 4.23, we have that for any $\alpha, \beta \in \operatorname{Con} \mathbf{A}$, $C(\alpha, \beta; \varphi)$ implies that $C(\alpha, \beta; \theta)$ holds. Thus, since $C((\varphi : \psi), \psi; \varphi)$ holds we may conclude that $C((\varphi : \psi), \psi; \theta)$ holds. It follows that $(\varphi : \psi) \leq (\theta : \psi)$. □

Proposition 4.25. *Let* $\mathbf{A}$ *be any algebra, and let* $\varphi, \psi, \theta \in \operatorname{Con} \mathbf{A}$*. Then*

(i) *for all natural numbers* n *and* k*,* $\mathcal{C}^k_{(\psi)}\mathcal{Z}^{n+k}_{(\psi)}\theta \leq \mathcal{Z}^n_{(\psi)}\theta$*;*

(ii) *thus, for all natural numbers* m*,* n *and* k*,* $\mathcal{C}^m_{(\psi)}(\varphi) \leq \mathcal{Z}^{n+k}_{(\psi)}\theta$ *implies that* $\mathcal{C}^{m+k}_{(\varphi)}\theta \leq \mathcal{Z}^n_{(\psi)}\theta$*.*

If, furthermore, $\mathbf{A}$ *generates a congruence modular variety, then,*

(iii) *for all natural numbers* n *and* k*,* $\mathcal{C}^m_{(\psi)}\theta \leq \mathcal{Z}^k_{(\psi)}\mathcal{C}^{m+k}_{(\psi)}\theta$*;*

(iv) *thus, for all natural numbers* m*,* n *and* k*,* $\mathcal{C}^{m+k}_{(\psi)}\varphi \leq \mathcal{Z}^n_{(\psi)}\theta$ *implies that* $\mathcal{C}^m_{(\psi)}\varphi \leq \mathcal{Z}^{n+k}_{(\psi)}\theta$*.*

Proof. We first prove (i). We shall induct on k. Note that the basis step is trivial (in this case, $\mathcal{C}^k_{(\psi)}$ is the identity.) Now, suppose that for some natural number k, item (i) has been verified. Then, by Proposition 4.22,

$$\begin{aligned}
\mathcal{C}^{k+1}_{(\psi)}\mathcal{Z}^{n+k+1}_{(\psi)}\theta &= \mathcal{C}_{(\psi)}\mathcal{C}^k_{(\psi)}\mathcal{Z}^{n+k+1}_{(\psi)}\theta \\
&\leq \mathcal{C}_{(\psi)}\mathcal{Z}^{n+1}_{(\psi)}\theta \\
&= [\mathcal{Z}^{n+1}_{(\psi)}\theta, \psi].
\end{aligned}$$

Now, since $\mathcal{Z}^{n+1}_{(\psi)}\theta = (\mathcal{Z}^{n}_{(\psi)}\theta : \psi)$ we have that $C(\mathcal{Z}^{n+1}_{(\psi)}\theta, \psi; \mathcal{Z}^{n}_{(\psi)}\theta)$ and hence

$$[\mathcal{Z}^{n+1}_{(\psi)}\theta, \psi] \leq \mathcal{Z}^{n}_{(\psi)}\theta.$$

Item (i) follows, by induction.

To see (ii), note that if $\mathcal{C}^{m}_{(\psi)}\varphi \leq \mathcal{Z}^{n+k}_{(\psi)}\theta$, then using Proposition 4.22 and then (i), we have that $\mathcal{C}^{m+k}_{(\psi)}\varphi = \mathcal{C}^{k}_{(\psi)}\mathcal{C}^{m}_{(\psi)}\varphi \leq \mathcal{C}^{k}_{(\psi)}\mathcal{Z}^{n+k}_{(\psi)}\theta \leq \mathcal{Z}^{n}_{(\psi)}\theta$.

Suppose now that $\mathbf{A}$ generates a congruence modular variety. We show (iii) by induction on k. Again, the basis step is trivial. Now, assume that the claim has been verified for some natural number k. Then, using Proposition 4.24, we observe that

$$\begin{aligned} \mathcal{Z}^{k+1}_{(\psi)}\mathcal{C}^{m+k+1}_{(\psi)}\theta &= \mathcal{Z}_{(\psi)}\mathcal{Z}^{k}_{(\psi)}\mathcal{C}^{m+k+1}_{(\psi)}\theta \\ &\geq \mathcal{Z}_{(\psi)}\mathcal{C}^{m+1}_{(\psi)}\theta. \end{aligned}$$

Now, since $\mathcal{Z}_{(\psi)}\mathcal{C}^{m+1}_{(\psi)}\theta = (\mathcal{C}^{m+1}_{(\psi)}\theta : \psi)$ and $\mathcal{C}^{m+1}_{(\psi)}\theta = [\mathcal{C}^{m}_{(\psi)}\theta, \psi]$, it follows that

$$C(\mathcal{Z}_{(\psi)}\mathcal{C}^{m+1}_{(\psi)}\theta, \psi; \mathcal{C}^{m+1}_{(\psi)}\theta) \text{ and } C(\mathcal{C}^{m}_{(\psi)}\theta, \psi; \mathcal{C}^{m+1}_{(\psi)}\theta),$$

and hence $\mathcal{Z}_{(\psi)}\mathcal{C}^{m+1}_{(\psi)}\theta \geq \mathcal{C}^{m}_{(\psi)}\theta$. The claim follows.

To see (iv), we use Proposition 4.24 and item (iii). Suppose that $\mathcal{C}^{m+k}_{(\psi)}\varphi \leq \mathcal{Z}^{n}_{(\psi)}\theta$. Then $\mathcal{Z}^{n+k}_{(\psi)}\theta = \mathcal{Z}^{k}_{(\psi)}\mathcal{Z}^{n}_{(\psi)}\theta \geq \mathcal{Z}^{k}_{(\psi)}\mathcal{C}^{m+k}_{(\psi)}\varphi \geq \mathcal{C}^{m}_{(\psi)}\varphi$. □

Corollary 4.26. *If* $\mathbf{A}$ *is an algebra upward nilpotent of class* k*, then* $\mathbf{A}$ *is downward nilpotent of class* k*, as well.*

Proof. Let k be a natural number, and suppose that $\mathbf{A}$ is nilpotent of class k. Then $\mathcal{C}^{0}_{(1_A)}1_A = 1_A = \zeta^k(\mathbf{A}) = \mathcal{Z}^{k}_{(1_A)}0_A$ entails that $[1_A)_k = \mathcal{C}^{k}_{(1_A)}1_A \leq \mathcal{Z}^{0}_{(1_A)}0_A = 0_A$. □

Corollary 4.27. *Let* $\mathbf{A}$ *be an algebra in a congruence modular variety. Then, for all natural numbers* n*,* $[1_A)_n = 0_A$ *if and only if* $\zeta^n(\mathbf{A}) = 1_A$*.*

Proof. Let n be a natural number. That upward nilpotence of class n implies downward nilpotence of class n is true in general, as seen in the previous corollary. Now, suppose that $\mathcal{C}^n_{(1_A)}1_A = [1_A)_n = 0_A = \mathcal{Z}^0_{(1_A)}0_A$. Using Proposition 4.25 (iv), we thus get that $1_A = \mathcal{C}^0_{(1_A)}1_A \leq \mathcal{Z}^n_{(1_A)}0_A = \zeta^n(\mathbf{A})$. $\square$

There is another elementary fact concerning the elements of the upper central series of an algebra worth noting here, which we shall have need of below.

Proposition 4.28. *Let* $\mathbf{A}$ *be an algebra. Let* $\varphi \leq \theta \cap \psi$ *be congruences of* $\mathbf{A}$*. Then for all natural numbers* n*,*

$$\mathcal{Z}^n_{(\psi/\varphi)}(\theta/\varphi) = (\mathcal{Z}^n_{(\psi)}\theta)/\varphi.$$

Thus, if ζ *is the center of* $\mathbf{A}$*, then for all natural numbers* n*,*

$$\zeta^n(\mathbf{A}/\zeta) = \zeta^{n+1}(\mathbf{A})/\zeta.$$

Proof. We induct on n to show the first claim. The basis is trivial, since, in this case, $\mathcal{Z}^n_{(\psi)}$ and $\mathcal{Z}^n_{(\psi/\theta)}$ are identity maps. Now suppose the claim has been verified for some natural number n. Then, using also Proposition 4.16,

$$\begin{aligned}(\mathcal{Z}^{n+1}_{(\psi)}\theta)/\varphi &= (\mathcal{Z}^n_{(\psi)}\theta : \psi)/\varphi \\ &= ((\mathcal{Z}^n_{(\psi)}\theta)/\varphi : \psi/\varphi) \\ &= (\mathcal{Z}^n_{(\psi/\varphi)}(\theta/\varphi) : \psi/\varphi) \\ &= \mathcal{Z}^{n+1}_{(\psi/\varphi)}(\theta/\varphi).\end{aligned}$$

The first claim follows by induction. To see the second claim, observe that

$$\begin{aligned}\zeta^n(\mathbf{A}/\zeta) &= \mathcal{Z}^n_{(1_{A/\zeta})}(\zeta/\zeta) \\ &= (\mathcal{Z}^n_{(1_A)}\zeta)/\zeta \\ &= \zeta^n(\zeta)/\zeta \\ &= \zeta^{n+1}(\mathbf{A})/\zeta.\end{aligned}$$

$\square$

Corollary 4.29. *In a given algebra* $\mathbf{A}$*, for all* $n \geq 1$*,* $\mathbf{A}$ *is upward nilpotent of class* n *if and only if* $\mathbf{A}/\zeta_{\mathbf{A}}$ *is upward nilpotent of class* $n-1$*.*

In Proposition 4.27, we saw that upward and downward nilpotence is equivalent in congruence modular varieties—a fact which was surely known prior to this. It was, at least, proved for congruence permutable varieties, in a similar fashion, by Smith (1976) on pp. 42-43. One of the main results of this section is the following, of which we have already seen the forward direction in Corollary 4.26.

Theorem 4.30. *Let* $\mathbf{A}$ *be an algebra in a variety with a difference term. For all natural numbers* n*,* $\mathbf{A}$ *is upward nilpotent of class* n *if and only if* $\mathbf{A}$ *is (downward) nilpotent of class* n*; in symbols,*

$$\zeta^n(\mathbf{A}) = 1_A \Leftrightarrow [1_A)_n = 0_A.$$

Later in this chapter, we apply this result to show that the same equational characterization of nilpotence of class k for algebras in a congruence modular variety given by Freese and McKenzie (1987) works if we assume only the availability of a difference term.

Theorem 4.30 is not hard to prove, although it may still be a new result. Indeed, we saw in Corollary 4.26 that the "forward direction" of this theorem is automatic, in the sense that we do not need to assume the availability of a difference term.

Consider further the following, to wind up the proof of Theorem 4.30.

Lemma 4.31. *Let* $\mathbf{A}$ *be an algebra in a difference term variety. Suppose also that* $[1_A)_n = 0_A$*. Then* $\zeta^n(\mathbf{A}) = 1_A$*.*

Proof. By Theorem 4.5, $\mathbf{A}$ has a Mal'cev term. Let $\mathcal{V}$ be the variety generated by $\mathbf{A}$. Since such is defined in terms of satisfaction of an equation, we also have that $\mathcal{V}$ is Mal'cev. By Mal'cev's characterization of congruence permutability (Theorem A.21), $\mathcal{V}$ is congruence permutable. Since congruence permutability implies congruence modularity (Proposition A.24), we can apply Corollary 4.27, to wind up the claim. □

4.4 New properties of the commutator in difference term varieties

It is also true that upward and downward nilpotence of a given class k for algebras in a congruence modular variety is easy to check by induction, through the use of the "homomorphism" property of the commutator given as Theorem 4.4 (1) in Freese and McKenzie (1987). For reference, we state this property now.

Proposition 4.32. *Let* $\mathbf{A}$ *be an algebra in a congruence modular variety. Let* $\alpha, \beta, \eta \in \operatorname{Con} \mathbf{A}$. *Then*

$$([\alpha, \beta] \vee \eta)/\eta = [(\alpha \vee \eta)/\eta, (\beta \vee \eta)/\eta].$$

Thus, one might take Theorem 4.30 as a suggestion that a stronger homomorphism property of the commutator exists for varieties with a difference term. We show such a result below, and give a generalization of the "reverse direction" of Theorem 4.30. Thus, a still larger fragment of the commutator theory for congruence modular varieties is found to extend to varieties with only a difference term.

In order to prove this new homomorphism property, we first establish another apparently new result concerning difference term varieties, an order theoretic property of the commutator, which we now give.

The proof of the following is patterned almost exactly after that of Lemma 2.5 from Kearnes (1995). Recall that, for any congruences α, β, θ on a given algebra, we denote by $[\alpha, \beta]_\theta$ the least congruence $\gamma \geq \theta$ such that $C(\alpha, \beta; \gamma)$; see Definition A.33.

Lemma 4.33. *Let* $\mathbf{A}$ *be an algebra in a variety with a difference term* d. *Let* $\alpha, \beta, \theta \in \operatorname{Con} \mathbf{A}$ *such that* $\beta \leq \alpha$. *Then*

$$[\alpha \vee \theta, \beta \vee \theta] \leq [\alpha, \beta] \vee \theta.$$

By the symmetry of the commutator in difference term varieties, it also follows that

$$[\beta \vee \theta, \alpha \vee \theta] \leq [\beta, \alpha] \vee \theta.$$

Proof. Suppose instead that $[\alpha \vee \theta, \beta \vee \theta] \not\leq [\alpha, \beta] \vee \theta$. We shall derive a contradiction. Set $\theta' = [\alpha, \beta] \vee \theta$. Then, by the monotonicity of the commutator, we must have that $[\alpha \vee \theta', \beta \vee \theta'] \not\leq [\alpha, \beta] \vee \theta'$. Thus, by changing notation, we now assume that $[\alpha \vee \theta, \beta \vee \theta] \not\leq [\alpha, \beta] \vee \theta$ and that $[\alpha, \beta] \leq \theta$.

We claim that $\beta \circ \theta \subseteq \theta \circ \beta$. Let $\langle x, z\rangle \in \beta \circ \theta$. Then we obtain $y \in A$ such that $x \,\beta\, y \,\theta\, z$. Then

$$x \, [\beta, \beta] \, d(x, y, y) \, \theta \, d(x, y, z) \, \beta \, d(y, y, z) = z.$$

Now, since $[\beta, \beta] \leq [\alpha, \beta] \leq \theta$, it follows that $\beta \circ \theta \subseteq \theta \circ \beta$, as claimed. It follows from Proposition A.19 that $\beta \vee \theta = \beta \circ \theta$.

Note that $\theta < [\alpha \vee \theta, \beta \vee \theta]_\theta$: After all, if instead $\theta = [\alpha \vee \theta, \beta \vee \theta]_\theta$, then we would have that $C(\alpha \vee \theta, \beta \vee \theta; \theta)$, from which we could conclude that $[\alpha \vee \theta, \beta \vee \theta] \leq \theta = [\alpha, \beta] \vee \theta$, contrary to our assumptions. Now, it must also be that $\theta < [\alpha, \beta \vee \theta]_\theta$: Indeed, $\theta = [\theta, \beta \vee \theta]_\theta$ always holds and so by Proposition A.34 (left semi-distributivity of the commutator), if $\theta = [\alpha, \beta \vee \theta]_\theta$, then we would also get that $\theta = [\alpha \vee \theta, \beta \vee \theta]_\theta$, which we have just ruled out.

From $\theta < [\alpha, \beta \vee \theta]_\theta$ we have that for some natural number k, term t of rank k, and tuples $\langle a, b\rangle \in \alpha$ and $\langle u_i, v_i\rangle \in \beta \vee \theta$, for $i < k$,

$$t(a, \mathbf{u}) \, \theta \, t(a, \mathbf{v}),$$

while

$$t(b, \mathbf{u}) \, [\alpha, \beta \vee \theta]_\theta \setminus \theta \, t(b, \mathbf{v}).$$

Since $\beta \vee \theta = \beta \circ \theta$, for each $i < k$, we may obtain a $w_i \in A$ such that $u_i \,\beta\, w_i \,\theta\, v_i$. Note, then, that $t(a, \mathbf{u}) \, \theta \, t(a, \mathbf{v}) \, \theta \, t(a, \mathbf{w})$. Thus, by definition of $[\alpha, \beta]_\theta$, we may conclude that $c := t(b, \mathbf{u}) \, [\alpha, \beta]_\theta \, t(b, \mathbf{w}) =: e$. On the other hand, $\langle c, e\rangle = \langle t(b, \mathbf{u}), t(b, \mathbf{w})\rangle \notin \theta$, for else we would have $t(b, \mathbf{u}) \, \theta \, t(b, \mathbf{w}) \, \theta \, t(b, \mathbf{v})$, contrary to our assumptions.

Now, let t' be a polynomial on $\mathbf{A}$ defined by $t'(x, \mathbf{y}) = d(t(x, \mathbf{y}), t(x, \mathbf{u}), t(b, \mathbf{u}))$. Note that

$$t'(a, \mathbf{u}) = d(t(a, \mathbf{u}), t(a, \mathbf{u}), t(b, \mathbf{u})) = t(b, \mathbf{u})$$

and, as well,

$$t'(b, \mathbf{u}) = d(t(b, \mathbf{u}), t(b, \mathbf{u}), t(b, \mathbf{u})) = t(b, \mathbf{u}).$$

Using also the symmetry of the commutator in difference term varieties, we thus find that $\langle t'(a, \mathbf{w}), t'(b, \mathbf{w})\rangle \in [\beta, \alpha] = [\alpha, \beta] \subseteq \theta$. Observe further that $c = t(b, \mathbf{u}) = d(t(a, \mathbf{u}), t(a, \mathbf{u}), t(b, \mathbf{u}))\, \theta\, d(t(a, \mathbf{w}), t(a, \mathbf{u}), t(b, \mathbf{u})) = t'(a, \mathbf{w})$, while

$$t'(b, \mathbf{w}) = d(t(b, \mathbf{w}), t(b, \mathbf{u}), t(b, \mathbf{u}))\, [\beta, \beta]\, t(b, \mathbf{w}) = e.$$

Note that $[\beta, \beta] \subseteq [\alpha, \beta] \subseteq \theta$. Altogether, then, we obtain that $c\, \theta\, t'(a, \mathbf{w})\, \theta\, t'(b, \mathbf{w})\, \theta\, e$, which is a contradiction of our finding above regarding these elements. $\square$

Theorem 4.34. *Let $\mathbf{A}$ be an algebra in a variety with a difference term, d. Let $\alpha, \beta \in \operatorname{Con} \mathbf{A}$ such that $\beta \leq \alpha$. Let $h : \mathbf{A} \to \mathbf{B}$ be an epimorphism with kernel θ. Then*

$$h([\alpha, \beta] \vee \theta) = [h(\alpha \vee \theta), h(\beta \vee \theta)].$$

By the symmetry of the commutator in difference term varieties, it also follows that

$$h([\beta, \alpha] \vee \theta) = [h(\beta \vee \theta), h(\alpha \vee \theta)].$$

Proof. Note that Theorem 4.10 gives us sets of generators G and G' for $[\alpha, \beta]$ and $[h(\alpha \vee \theta), h(\beta \vee \theta)]$, respectively. (Of course, it is necessary to note that, by the correspondence theorem, h preserves the lattice order for congruences on $\mathbf{A}$ above θ.) For ease of reference, we have

$$G := \Big\{ \Big\langle d^{\mathbf{A}} \left(f^{\mathbf{A}}(\mathbf{x}), f^{\mathbf{A}}(\mathbf{y}), f^{\mathbf{A}}(\mathbf{z}) \right), f^{\mathbf{A}} \left(d(x_0, y_0, z_0), \ldots, d^{\mathbf{A}}(x_{n-1}, y_{n-1}, z_{n-1}) \right) \Big\rangle \mid$$
$$n \in \omega, f \in F_n, x_i\, \alpha\, y_i\, \beta\, z_i \text{ for } i < n \Big\} \bigcup \Big\{ \langle d^{\mathbf{A}}(x, y, y), x \rangle \mid x\, \beta\, y \Big\}$$

and

$$G' := \Big\{ \Big\langle d^{\mathbf{B}}\left(f^{\mathbf{B}}(\mathbf{x}), f^{\mathbf{B}}(\mathbf{y}), f^{\mathbf{B}}(\mathbf{z})\right), f^{\mathbf{B}}\left(d^{\mathbf{B}}(x_0, y_0, z_0), \ldots, d^{\mathbf{B}}(x_{n-1}, y_{n-1}, z_{n-1})\right) \Big\rangle \mid$$
$$n \in \omega, f \in F_n, x_i \, h(\alpha \vee \theta) \, y_i \, h(\beta \vee \theta) \, z_i \text{ for } i < n \Big\} \bigcup$$
$$\Big\{ \Big\langle d^{\mathbf{B}}(x, y, y), x \Big\rangle \mid x \, h(\beta \vee \theta) \, y \Big\},$$

where, in both expressions, F_n denotes the set of fundamental operation symbols of arity n in the signature of $\mathbf{A}$. In particular, note that $G \cup \theta$ generates $[\alpha, \beta] \vee \theta$.

Take $\langle a', b' \rangle \in h(G)$. That is, suppose that $\langle a', b' \rangle = \langle h(a), h(b) \rangle$ for some pair $\langle a, b \rangle \in G$. We have two cases to consider. First suppose that for some fundamental operation symbol f in the signature of $\mathbf{A}$ of arity, say, n, and for $a_0, \ldots, a_{n-1}, b_0, \ldots, b_{n-1}, c_0, \ldots, c_{n-1} \in A$, such that $a_i \, \alpha \, b_i \, \beta \, c_i$ for each $i < n$, we have

$$\langle a, b \rangle = \Big\langle d^{\mathbf{A}}\Big(f^{\mathbf{A}}(\mathbf{a}), f^{\mathbf{A}}(\mathbf{b}), f^{\mathbf{A}}(\mathbf{c})\Big), f^{\mathbf{A}}\Big(d^{\mathbf{A}}(a_0, b_0, c_0), \ldots, d^{\mathbf{A}}(a_{n-1}, b_{n-1}, c_{n-1})\Big)\Big\rangle.$$

Then

$$\begin{aligned}
\langle ha, hb \rangle &= \Big\langle hd^{\mathbf{A}}\Big(f^{\mathbf{A}}(\mathbf{a}), f^{\mathbf{A}}(\mathbf{b}), f^{\mathbf{A}}(\mathbf{c})\Big), hf^{\mathbf{A}}\Big(d^{\mathbf{A}}(a_0, b_0, c_0)), \ldots, d^{\mathbf{A}}(a_{n-1}, b_{n-1}, c_{n-1})\Big)\Big\rangle \\
&= \Big\langle d^{\mathbf{B}}\Big(f^{\mathbf{B}}(h\mathbf{a}), f^{\mathbf{B}}(h\mathbf{b}), f^{\mathbf{B}}(h\mathbf{c}))\Big), \\
&\qquad f^{\mathbf{B}}\Big(d^{\mathbf{B}}(ha_0, hb_0, hc_0), \ldots, d^{\mathbf{B}}(ha_{n-1}, hb_{n-1}, hc_{n-1}\Big)\Big\rangle.
\end{aligned}$$

Now, since, for each $i < n$, we have that $h(a_i) \, h(\alpha) \, h(b_i) \, h(\beta) \, h(c_i)$; it follows that $\langle h(a), h(b) \rangle \in G'$. The other case can be treated similarly. Thus, we have that $h(G) \subseteq G'$. Note also that $h(G \cup \theta) = h(G) \cup h(\theta) = h(G) \cup 0_B$, and that $O_B \subseteq G'$. It follows from Proposition A.10 that $h([\alpha, \beta] \vee \theta) \subseteq [h(\alpha \vee \theta), h(\beta \vee \theta)]$.

Now, take $\langle a', b' \rangle \in G'$. Again, we have two cases to consider. Suppose that, for some fundamental operation symbol f with arity n and some $a'_0, \ldots, a'_{n-1}, b'_0, \ldots, b'_{n-1}, c'_0, \ldots, c'_{n-1} \in B$ with $a'_i \, h(\alpha \vee \theta) \, b'_i \, h(\beta \vee \theta) \, c'_i$, for each $i < n$, we have that

$$\langle a', b' \rangle = \Big\langle d^{\mathbf{B}}\Big(f^{\mathbf{B}}(\mathbf{a}'), f^{\mathbf{B}}(\mathbf{b}'), f^{\mathbf{B}}(\mathbf{c}')\Big), f^{\mathbf{B}}\Big(d^{\mathbf{B}}(a'_0, b'_0, c'_0)), \ldots, d^{\mathbf{B}}(a'_{n-1}, b'_{n-1}, c'_{n-1})\Big)\Big\rangle.$$

For each i, get $a_i, b_i, c_i \in A$ such that $h(a_i) = a'_i$, $h(b_i) = b'_i$, and $h(c_i) = c'_i$ and so that $a_i \,\alpha \vee \theta\, b_i \,\beta \vee \theta\, c_i$. Then, of course, for

$$\langle a, b\rangle := \Big\langle d^{\mathbf{A}}\Big(f^{\mathbf{A}}(\mathbf{a}), f^{\mathbf{A}}(\mathbf{b}), f^{\mathbf{A}}(\mathbf{c})\Big), f^{\mathbf{A}}\Big(d^{\mathbf{A}}(a_0, b_0, c_0)), \ldots, d^{\mathbf{A}}(a_{n-1}, b_{n-1}, c_{n-1})\Big)\Big\rangle,$$

we have that $\langle h(a), h(b)\rangle = \langle a', b'\rangle$. Now, by Theorem 4.10, we also have that $\langle a, b\rangle \in [\alpha \vee \theta, \beta \vee \theta]$. But, then, by Theorem 4.33, we have that $\langle a, b\rangle \in [\alpha, \beta] \vee \theta$. After treating the second case in a similar fashion, we thus find that $G' \subseteq h([\alpha, \beta] \vee \theta)$. It follows that $[h(\alpha \vee \theta), h(\beta \vee \theta)] \subseteq h([\alpha, \beta] \vee \theta)$, which, together with the opposite inclusion shown above, completes our task. $\square$

Remark 4.35. It appears possible to prove, in a similar manner, that if $\mathbf{A}$ is an algebra in a variety with a difference term, then for all $\alpha, \beta, \theta \in \operatorname{Con} \mathbf{A}$, we have that

$$([\alpha, \beta] \vee \theta)/\theta \leq [(\alpha \vee \theta)/\theta, (\beta \vee \theta)/\theta].$$

Let $\mathbf{A}$ be an algebra in a difference term variety. Let $\alpha, \beta \in \operatorname{Con} \mathbf{A}$. One ought to be able to use Theorem 6.2 from Kearnes, Szendrei, and Willard (2013+) to find generators for $[\alpha, \beta]$, much in the way that we used Theorem 4.10 to find generators for $[\alpha, \beta]$ in the case of $\beta \leq \alpha$. With these generators in hand, a similar proof to that of the first inclusion featured in the proof of Theorem 4.34 should do the trick. We shall see below why the reverse inclusion is not available without additionally implying congruence modularity.

Remark 4.36. Let $\mathbf{A}$ be an algebra in a variety with a weak difference term. In Lipparini (1994), Theorem 4.3 (i), we learn that, for all $\alpha, \theta \in \operatorname{Con} \mathbf{A}$,

$$[\alpha \vee \theta, \alpha \vee \theta] \leq [\alpha, \alpha] \vee \theta.$$

Thus, it seems that one might use the (likely) result of Remark 4.9 together with the proof technique employed to get Theorem 4.34, to learn that, further, for all $\alpha, \theta \in \operatorname{Con} \mathbf{A}$,

$$[(\alpha \vee \theta)/\theta, (\alpha \vee \theta)/\theta] = ([\alpha, \alpha] \vee \theta)/\theta.$$

We now draw some interesting conclusions from this result.

Corollary 4.37. *Let* $\mathbf{A}$ *be an algebra in a variety with a difference term. Let* $\alpha, \theta \in \operatorname{Con} \mathbf{A}$*. Then for all natural numbers* n*,*

$$[(\alpha \vee \theta)/\theta]_n = ([\alpha]_n \vee \theta)/\theta$$

and

$$[(\alpha \vee \theta)/\theta)_n = ([\alpha)_n \vee \theta)/\theta$$

Proof. We shall show the first claim, since the proof of the second is entirely parallel. We shall induct on n. The base case is rather trivial, as seen by computing that

$$[(\alpha \vee \theta)/\theta]_0 = 1_{A/\theta} = 1_A/\theta = (1_A \vee \theta)/\theta = ([\alpha]_0 \vee \theta)\,/\theta.$$

Now, suppose the claim has been verified for some natural number n. Using also the proposition above, we compute that

$$\begin{aligned}
[(\alpha \vee \theta)/\theta]_{n+1} &= [[(\alpha \vee \theta)/\theta]_n, [(\alpha \vee \theta)/\theta]_n] \\
&= [([\alpha]_n \vee \theta)/\theta, ([\alpha]_n \vee \theta)/\theta] \\
&= ([[\alpha]_n, [\alpha]_n] \vee \theta)/\theta \\
&= ([\alpha]_{n+1} \vee \theta)/\theta.
\end{aligned}$$

$\square$

A portion of the following is got from Kearnes (1995), Lemma 2.3 (see his "In particular..."), but not the full result, which has many consequences. In fact, the portion of this proof not covered by Kearnes' previous result seems to be the more useful part.

Theorem 4.38. *Let* $\mathbf{A}$ *be an algebra in a variety with a difference term. Let* $\alpha, \beta, \gamma \in \operatorname{Con} \mathbf{A}$ *such that* $\beta \leq \alpha$*. Then* $C(\alpha, \beta; \gamma)$ *holds if and only if* $[\alpha, \beta] \leq \gamma$*, and* $C(\beta, \alpha; \gamma)$ *holds if and only if* $[\beta, \alpha] \leq \gamma$*. Furthermore,* $C(\alpha, \beta; \gamma)$ *holds if and only if* $C(\beta, \alpha; \gamma)$ *holds.*

Proof. Note that if $C(\alpha,\beta;\gamma)$ holds, then, by definition $[\alpha,\beta] \le \gamma$. Now, suppose that $[\alpha,\beta] \le \gamma$. By Theorem 4.34, we thus have that

$$[(\alpha\vee\gamma)/\gamma,(\beta\vee\gamma)/\gamma] = ([\alpha,\beta]\vee\gamma)/\gamma = \gamma/\gamma = 0_{A/\gamma}.$$

Thus, $C((\alpha\vee\gamma)/\gamma,(\beta\vee\gamma)/\gamma;0_{A/\gamma})$ holds, which, by Proposition A.28 (e), entails that $C(\alpha\vee\gamma,\beta\vee\gamma;\gamma)$ holds. By the monotonicity of the centralizer in its first two coordinates (Proposition A.28 (c)), we thus have that $C(\alpha,\beta;\gamma)$ holds, as desired.

We may also argue in a similar way, using Theorem 4.34, that $C(\beta,\alpha;\gamma)$ holds if and only if $[\beta,\alpha] \le \gamma$.

To see the last claim, observe that $C(\alpha,\beta;\gamma)$ holds if and only if $[\alpha,\beta] \le \gamma$. By Theorem A.40, $[\alpha,\beta] = [\beta,\alpha]$, and so we see that $C(\alpha,\beta;\gamma)$ holds if and only if $C(\beta,\alpha;\gamma)$, as claimed. □

Theorem 4.39. *Let* $\mathbf{A}$ *be an algebra in a variety with a difference term. If* $\alpha_i (i \in I), \beta \in \operatorname{Con}\mathbf{A}$ *such that* $\alpha_i \le \beta$ *for each* $i \in I$*, then*

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

If $\alpha, \beta(i \in I) \in \operatorname{Con}\mathbf{A}$ *such that* $\alpha \le \beta_i$ *for each* $i \in I$*, then*

$$[\alpha,\bigvee_{i\in I}\beta_i] = \bigvee_{i\in I}[\alpha,\beta_i].$$

Proof. We will show the first claim, with the second having a similar proof. By the monotonicity of the commutator, it is always true that

$$\bigvee_{i\in I}[\alpha_i,\beta] \le [\bigvee_{i\in I}\alpha_i,\beta].$$

Thus, we need only show the reverse inequality. To do so, it is sufficient to show that

$$C\left(\bigvee\alpha_i,\beta;\bigvee[\alpha_i,\beta]\right)$$

holds. By Proposition A.28 (b), it is sufficient to show that, for each $i \in I$,

$$C\left(\alpha_i,\beta;\bigvee[\alpha_i,\beta]\right).$$

By definition, for each $i \in I$, we have that $C(\alpha_i, \beta; [\alpha_i, \beta])$. Now, by Theorem 4.38, we have that, for each $i \in I$, $C(\alpha_i, \beta; \bigvee[\alpha_i, \beta])$. The result follows. □

We would further like to observe that Theorems 4.33 and 4.34 are—at least to a degree—sharp. We make this claim precise in the next series of results. The key result we shall use is given by Theorem 3.2 (i) from Lipparini (1994) (which actually says something stronger). We state it here for convenience.

Theorem 4.40. *Let* $\mathbf{A}$ *be an algebra in a variety with a difference term. Suppose that for all* $\alpha, \beta, \gamma \in \operatorname{Con} \mathbf{A}$*, we have that*

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

Then $\operatorname{Con} \mathbf{A}$ *is modular.*

Theorem 4.41. *Let* $\mathbf{A}$ *be an algebra in a variety with a difference term. Suppose also that for all* $\alpha, \beta, \theta \in \operatorname{Con} \mathbf{A}$ *we have that*

$$[(\alpha \vee \theta)/\theta, (\beta \vee \theta)/\theta] = ([\alpha, \beta] \vee \theta)/\theta.$$

Then $\operatorname{Con} \mathbf{A}$ *is modular. In particular, if* $\mathcal{V}$ *is a variety with a difference term, then the above homomorphism property holds across* $\mathcal{V}$ *if and only if* $\mathcal{V}$ *is congruence modular.*

Proof. It is easy to mimic the proof of Theorem 4.38, above, to establish that, under our assumptions, for all $\alpha, \beta, \gamma \in \operatorname{Con} \mathbf{A}$, we have that if $C(\alpha, \beta; \gamma)$ holds if and only if $[\alpha, \beta] \leq \gamma$. From this, it is easy to see that for all $\alpha, \beta, \gamma, \gamma' \in \operatorname{Con} \mathbf{A}$ such that $\gamma \leq \gamma'$, we have that if $C(\alpha, \beta; \gamma)$ then $C(\alpha, \beta; \gamma')$ holds as well. One can then prove, using little more than the basic facts concerning the commutator—that is, which hold in all varieties—that we must have that for all $\alpha, \beta, \gamma \in \operatorname{Con} \mathbf{A}$, $[\alpha \vee \beta, \gamma] = [\alpha, \gamma] \vee [\beta, \gamma]$. (The fact just cited appears in Lipparini (1994) as Proposition 1.6.)

Now, by Theorem 4.40, we may conclude that $\operatorname{Con} \mathbf{A}$ is congruence modular. □

We see from Theorem 4.40 that for a given variety $\mathcal{V}$, the finite additivity of the commutator plus the availability of a difference term implies that $\mathcal{V}$ is congruence modular. Here we note—apparently for the first time—that the finite "subadditivity" of the commutator is enough to force congruence modularity in any difference term variety.

Theorem 4.42. *Let* $\mathbf{A}$ *be an algebra in a variety* $\mathcal{V}$ *with a difference term. Suppose that* $\operatorname{Con}\mathbf{A}$ *is subadditive. That is, suppose that for all* $\alpha, \beta, \theta \in \operatorname{Con}\mathbf{A}$ *we have that*

$$[\alpha \vee \theta, \beta \vee \theta] \leq [\alpha, \beta] \vee \theta.$$

Then $\operatorname{Con}\mathbf{A}$ *is modular. In particular,* $\mathcal{V}$ *is congruence modular if and only if* $\operatorname{Con}\mathbf{A}$ *is subadditive for all* $\mathbf{A} \in \mathcal{V}$.

Proof. Suppose that for all $\alpha, \beta, \theta \in \operatorname{Con}\mathbf{A}$ we have that

$$[\alpha \vee \theta, \beta \vee \theta] \leq [\alpha, \beta] \vee \theta.$$

We may easily mimic the proof of Theorem 4.34 to argue that these assumptions imply that for all $\alpha, \beta, \theta \in \operatorname{Con}\mathbf{A}$, we have that

$$[(\alpha \vee \theta)/\theta, (\beta \vee \theta)/\theta] = ([\alpha, \beta] \vee \theta)/\theta.$$

Thus, that $(i) \Rightarrow (ii)$ follows from Theorem 4.41.

The finish the second claim, one only needs the addivity of the commutator in congruence modular varieties, together with Proposition A.31. $\square$

Theorem 4.34 also provides a (somewhat) interesting proof of Theorem 4.30, independent of Corollary 4.5.

Proof. (of Theorem 4.30) Let $\zeta = \zeta_{\mathbf{A}}$. Suppose that $[1_A)_n = 0_A$. We wish to show that $\zeta_n^A = 1_A$. We shall induct on n. For the base case, observe that $\zeta_{\mathbf{A}}^0 = 0_A = [1_A)_0 = 1_A$. Now, suppose that $n > 0$ and that the $(n-1)$-case has been verified. Note that

$[1_A)_n = 0_A$ entails that $[1_A)_{n-1} \leq \zeta_{\mathbf{A}}$. From Corollary 4.37, we also have that $[1_{A/\zeta})_{n-1} = ([1_A)_{n-1} \vee \zeta)/\zeta$, and hence $[1_{A/\zeta})_{n-1} = 0_{A/\zeta}$. By inductive hypothesis, we have that $\zeta^{n-1}_{\mathbf{A}/\zeta} = 1_{A/\zeta}$. By Proposition 4.28, then, we have that $\zeta^n_{\mathbf{A}} = 1_A$, as claimed. Thus the "reverse direction" follows by induction.

Now suppose that $\zeta^n_{\mathbf{A}} = 1_A$. Again, we induct on n. For the case of $n = 0$, note that $[1_A)_0 = 1_A = \zeta^0_{\mathbf{A}} = 0_A$. Assume that $n > 0$ and the $(n-1)$-case has been verified. We wish to show that $[1_A)_n = 0_A$. This is equivalent to showing that $[1_A)_{n-1} \leq \zeta_{\mathbf{A}}$. By Proposition 4.28, we have that $\zeta^n_{\mathbf{A}} = 1_A$ entails that $\zeta^{n-1}_{\mathbf{A}} = 1_{A/\zeta}$. Thus, by inductive hypothesis, we have that $[1_{A/\zeta})_{n-1} = 0_{A/\zeta}$. By Corollary 4.37, then, we have that

$$([1_A)_{n-1} \vee \zeta)/\zeta = [1_{A/\zeta})_{n-1} = 0_{A/\zeta};$$

thus, by the correspondence theorem A.16, we have that $[1_A)_{n-1} \vee \zeta = \zeta$, which is to say, $[1_A)_{n-1} \leq \zeta$. Thus, this direction follows by induction as well, completing the proof. □

There is a third path to this result, via the following more general fact. First, consider this lemma.

Lemma 4.43. *Let* $\mathbf{A}$ *be an algebra in a variety with a difference term. Let* $\psi, \theta, \varphi \in \operatorname{Con} \mathbf{A}$ *with* $\varphi \leq \theta$ *and such that for all natural numbers* n, $\mathcal{Z}^n_{(\psi)}\theta \leq \psi$. *Then* $\mathcal{Z}_{(\psi)}\varphi = (\varphi : \psi) \leq (\theta : \psi) = \mathcal{Z}_{(\psi)}\theta$ *and hence, for all natural numbers* n, $\mathcal{Z}^n_{(\psi)}\varphi \leq \mathcal{Z}^n_{(\psi)}\theta$.

Proof. From Theorem 4.38, it is easy to see that $C((\varphi : \psi), \psi; \varphi)$ implies that $C((\varphi : \psi), \psi; \theta)$. Thus, $(\varphi : \psi) \leq (\theta : \psi)$. The rest follows by induction. □

Proposition 4.44. *Let* $\mathbf{A}$ *be an algebra in a variety with a difference term. Let* $\psi, \theta, \varphi \in \operatorname{Con} \mathbf{A}$ *such that for all natural numbers* n, $\mathcal{Z}^n_{(\psi)}\theta \leq \psi$. *Then, for all natural numbers* k, m, *and* n,

(i) $\mathcal{C}^m_{(\psi)}\theta \leq \mathcal{Z}^k_{(\psi)}\mathcal{C}^{m+k}_{(\psi)}\theta$ *and*

(ii) $\mathcal{C}^{m+k}_{(\psi)}\varphi \leq \mathcal{Z}^{n}_{(\psi)}\theta$ *implies that* $\mathcal{C}^{m}_{(\psi)}\varphi \leq \mathcal{Z}^{n+k}_{(\psi)}\theta$.

Proof. The same proof as was supplied for Proposition 4.25 (iii) and (iv) works here, substituting the use of Proposition 4.24 in favor of 4.43. □

Corollary 4.45. *Let* $\mathbf{A}$ *be an algebra in a variety with a difference term. Let* $\theta \in \operatorname{Con}\mathbf{A}$. *Then* $\zeta^n(\theta) = 1_A$ *if and only if* $[1_A)_n \leq \theta$.

Proof. This is just an application of Propositions 4.44 and 4.25. □

We have a further use for Theorem 4.10; it enables us to use the same proof of Theorem 14.1 in Freese and McKenzie (1987) to get a new result, with "congruence modular," in the statement of their theorem, replaced by "difference term."

Theorem 4.46. *For* $\mathbf{A} \in \mathcal{V}$, *a variety with a difference term* d, $a\,\zeta_{\mathbf{A}}\,b$ *if and only if*

$$f(d(r_1(a,b), r_1(b,b), c_1), \ldots, d(r_n(a,b), r_n(b,b), c_n)) = \\ d(f(r_1(a,b), \ldots, r_n(a,b)), f(r_1(b,b), \ldots, r_n(b,b)), f(c)) \quad (4.1)$$

and

$$d(r(a,b), r(b,b), r(b,b)) = r(a,b), \quad (4.2)$$

for all fundamental operations f, *all* $\mathbf{c} = \langle c_1, \ldots, c_n\rangle \in A^n$, *and all binary term operations* r *and* r_i.

Proof. The proof supplied by Freese and McKenzie for the case of $\mathcal{V}$ congruence modular goes through intact, replacing only their proposition 5.7 with Theorem 4.10. □

We can also use Theorem 4.46 to find an equational characterization of nilpotence in varieties with a difference term in much the same way that Freese and McKenzie did for congruence modular varieties; in order to make their proofs work, however, we require the fact that upward and downward nilpotence are equivalent in varieties with a difference term.

Definition 4.47. For $\mathcal{V}$, a variety with a difference term, set

$$E_0 := \{x \approx y\},$$

and for $k > 0$ let E_{k+1} be the set of all equations of the form

$$f\left(d(r_1(s,t), r_1(t,t), z_1), \ldots, d(r_n(s,t), r_n(t,t), z_n)\right)$$
$$\approx d\left(f(r_1(s,t), \ldots, r_n(s,t)), f(r_1(t,t), \ldots, r_n(t,t)), f(\mathbf{z})\right)$$

union the set of all equations of the form

$$d(r(s,t), r(t,t), r(t,t)) \approx r(s,t),$$

where f is a basic operation symbol, r and r_i are binary terms, $s \approx t \in E_k$, and the z_i are any variables.

Theorem 4.48. *Let $\mathbf{A} \in \mathcal{V}$, a variety with a difference term. Then for all natural numbers k, $\mathbf{A}$ satisfies E_k if and only if $[1_A)_k = 0_A$.*

.

Proof. We essentially use the proof of Freese and McKenzie, except for added steps that invoke Theorem 4.30 We induct on k. The case of $n = 0$ is clear from the definition of $[1_A)_0$ as 1_A. That is, if $\mathbf{A}$ is nilpotent of class 0, then, evidently, $0_A = [1_A)_0 = 1_A$. This can only happen if A is a singleton, and so we see that $\mathbf{A} \models E_0$.

Now, suppose that the theorem holds for some $k \geq 0$. By Theorem 4.30, we find that $[1_A)_k = 0_A \Leftrightarrow \zeta^k_{\mathbf{A}} = 1_A$. By Corollary 4.29 and a second application of Theorem 4.30, we have that $\zeta^k_{\mathbf{A}} = 1_A \Leftrightarrow \zeta^{k-1}_{\mathbf{A}/\zeta_{\mathbf{A}}} = 1_{A/\zeta_{\mathbf{A}}} \Leftrightarrow [1_{A/\zeta_{\mathbf{A}}})_{k-1} = 0_{A/\zeta_{\mathbf{A}}}$. Now, using the inductive hypothesis and $\mathbf{A}/\zeta_{\mathbf{A}}$ in place of $\mathbf{A}$, we have that $[1_{A/\zeta_{\mathbf{A}}})_{k-1} = 0_{A/\zeta_{\mathbf{A}}}$ if and only if for all evaluations $\langle a, b\rangle$ of any $s \approx t \in E_{k-1}$ in $\mathbf{A}$, we have that $a\,\zeta_{\mathbf{A}}\,b$. By Theorem 4.46, the last condition holds if and only if for all evaluations

$\langle a, b\rangle$ of any $s \approx t \in E_{k-1}$ in $\mathbf{A}$, for all fundamental operations f of any arity n, all binary terms r_i, $(i = 0, \ldots, n)$, and all elements $c_1, \ldots, c_n$ from A,

$$f(d(r_1(a, b), r_1(b, b), c_1), \ldots, d(r_n(a, b), r_n(b, b), c_n)) = \\ d(f(r_1(a, b), \ldots, r_n(a, b)), f(r_1(b, b), \ldots, r_n(b, b)), f(\mathbf{c}))$$

and

$$d(r_0(a, b), r_0(b, b), r_0(b, b)) = r_0(a, b).$$

But, of course, this says precisely that $\mathbf{A} \models E_n$. $\square$

We thus get the following, which parallels Theorem 14.3 from Freese and McKenzie (1987).

Corollary 4.49. *Let $\mathcal{V}$ be a variety of finite signature with a difference term such that $F_{\mathcal{V}}(2)$ is finite. Then for each natural number n, there is a finite set of equations E_n depending only on $F_{\mathcal{V}}(2)$ and the signature of $\mathcal{V}$ such that $\mathbf{A} \in \mathcal{V}$ is nilpotent of class n if and only if $\mathbf{A} \models E_n$.*

Chapter 5

Questions for further study

5.1 Concerning Problem 1.3

The following is known, through a combination of results in Aichinger and Mudrinski (2010) and Kearnes (1999).

Theorem 5.1. *Let* $\mathbf{A}$ *be a nilpotent algebra in a variety with a Mal'cev term. Then the following are equivalent.*

(i) $\mathbf{A}$ *is supernilpotent.*

(ii) $\mathbf{A}$ *has a finite bound on the rank of its nontrivial commutator polynomials.*

(iii) $\mathbf{A}$ *has a finite bound on the rank of its nontrivial commutator terms.*

(iv) $\mathbf{A}$ *factors as the direct product of algebras of prime power order.*

Proof. That (i) implies (ii) is given above as Corollary 2.52 (and was given prior to this as Lemma 7.5 in Aichinger and Mudrinski (2010)). That (ii) implies (iii) is trivial (see Definition 2.50). We get that (iii) implies (iv) from Kearnes (1999), Theorem 3.14. Finally, that (iv) implies (i) is given by Aichinger and Mudrinski (2010) as Lemma 7.6. □

What is left to be desired in the above is a parallel characterization of supernilpotence of class n, for fixed n.

Problem 5.2. For a given natural number n, find a characterization of supernilpotence of class n in a Mal'cev variety that parallels Theorem 5.1. In particular, can we find a bound on the rank of the nontrivial commutator terms for an (finite?) algebra of supernilpotence class n that depends (only?) on n? Is there a combinatorial dependence on the parameter n of the number of factors or the powers associated with the prime power factorization of a Mal'cev algebra of supernilpotence class n?

If we are to follow an Oates-Powell strategy—as discussed in Chapter 3—to solve Problem 1.3, it seems likely that we shall require a generalization of the following facts.

Proposition 5.3. *(see 51.24 (p. 146) in Neumann (1967)) Let* $\mathbf{A}$ *be a group. Then we have that the nilpotence class of any nilpotent group in* $\operatorname{Var}\mathbf{A}$ *is bounded by the highest nilpotence class among nilpotent factors of* $\mathbf{A}$*.*

Proposition 5.4. *For each natural number* n*, there is a finite set* Σ_n *of first order sentences in the language of groups such that an algebra* $\mathbf{A}$ *of the signature of groups is nilpotent of class* n *if and only if* $\mathbf{A} \models \Sigma_n$*.*

Of course, what we have in mind in the above proposition is simply the usual commutator equation. Though something quite of this strength is not necessary, something along these lines, together with Proposition 5.3 is needed to prove the following.

Proposition 5.5. *(See Lemma 52.35 (p. 153) in Neumann (1967)) Let* $\mathbf{A}$ *be a finite group, and let* $\mathcal{V} = \operatorname{Var}\mathbf{A}$*. Suppose that all nilpotent factors of* $\mathbf{A}$ *are nilpotent of class at most* c *(finite). Then, there is a natural number* N *such that for all* $n > N$*, for all nilpotent groups* $\mathbf{B} \in \mathcal{V}^{(n)}$*, we have that* $\mathbf{B}$ *is nilpotent of class* c*.*

Problem 5.6. Establish the following analogy to the above proposition. Let $\mathbf{A}$ be a finite, nilpotent algebra that generates a Mal'cev variety $\mathcal{V}$ of finite signature. Suppose that all supernilpotent factors of $\mathbf{A}$ are supernilpotent of class at most c (finite). Then, is there a natural number N such that for all $n > N$, for all supernilpotent algebras $\mathbf{B} \in \mathcal{V}^{(n)}$, we have that $\mathbf{B}$ is supernilpotent of class c?

In Theorem 3.32, we have undertaken one of the necessary steps to address the above problem. A second would be to find an analogy to Proposition 5.3:

Problem 5.7. Is it true that, given a finite, nilpotent, Mal'cev algebra $\mathbf{A}$ that there is a bound for supernilpotence classes of all supernilpotent algebras in the variety generated by $\mathbf{A}$?

Perhaps the nilpotence class of $\mathbf{A}$ itself bounds the highest supernilpotence class possible in Var $\mathbf{A}$—but I would hazard that it does not. Proposition 5.3 can be proved with reference to Sylow theory (see 51.24 (p. 146) in Neumann (1967)). It does not seem readily apparent how to generalize this approach, but I suggest that further study or adaptation of Kearnes (1999) or perhaps Smith (2015) may yield an answer to this problem.

Now, another approach to its solution is suggested by McKenzie (1987b). Here, we find that, if $\mathbf{A}$ is a finite algebra that generates a congruence modular variety, then there is indeed a bound on the nilpotence class possible in the variety generated by $\mathbf{A}$; see Theorem 3.2 and Corollary 2.12 (or Kiss' improvement on this latter result) in McKenzie's paper for an explanation of how this is established. However, the proof of this fact—as suggested by the results cited in McKenzie (1987b)—appears to depend on the fact that nilpotence is recursively defined, whereas supernilpotence is not apparently so definable. For instance, it is unclear whether a collapse in the middle of the chain

$$1_A \geq S^2(1_A, 1_A) \geq S^3(1_A, 1_A, 1_A) \geq \cdots ,$$

for a given algebra $\mathbf{A}$, will result in the collapse of the remainder:

Problem 5.8. If for a given Mal'cev algebra $\mathbf{A}$ we have that, for some natural number n, $S^n(1_A, \ldots, 1_A) = S^{n+1}(1_A, \ldots, 1_A)$, then, is it the case, too, that $S^m(1_A, \ldots, 1_A) = S^n(1_A, \ldots, 1_A)$ for all $m \geq n$?

On the other hand, Lemma 3.1 of McKenzie (1987b), which feeds into his Theorem 3.2 does appear to work if one exchanges the iterated commutator for the higher commutator. A sort of illustration of this is given in Proposition 2.43. A source of insight into these questions may also be provided by some of the material in Mayr (2011).

Despite Theorem 3.32 or, rather, encouraged by it, one wonders whether supernilpotence of a given class and in a fixed Mal'cev variety can be defined in terms of satisfaction of some finite number of equations given, say, a finite signature and a degree of local finiteness—but independently of Freese and Vaughan-Lee's finite basis.

Problem 5.9. Let $\mathcal{V}$ be a locally finite, Mal'cev variety of finite signature. Let k be a natural number. Find, independent of the finite basis result of Freese and Vaughan-Lee, a finite set σ_k of equations in that language of $\mathcal{V}$ such that for any $\mathbf{A} \in \mathcal{V}$, $\mathbf{A}$ is supernilpotent of class k if and only if $\mathbf{A} \models \sigma_k$.

Perhaps the algorithm developed in Neumann (1967), Lemma 33.37, can be (somehow) adapted to show that the equations given implicitly in Theorem 2.24, only limited to t a term in k variables characterize supernilpotence of class k. An answer to this problem will then lend itself to a new, arguably easier proof of the finite basis result of Freese and Vaughan-Lee: Using Theorem 3.7 and the arguments of Proposition 2.13 (together with Theorem 2.24), one could then show that if $\mathcal{V}$ is a congruence-permutable variety of supernilpotent algebras such that $F_{\mathcal{V}}(2)$ is finite, then $\mathcal{V}^{(n)}$ is a Cross variety, for large enough n.

By consulting pages 156-7 of Neumann (1967), one can observe that our strategy of estimating the cardinality of an algebra in a congruence permutable variety given in Theorem 3.28 has a precedence. For any group $\mathbf{A}$, it is remarked there that $\mathbf{A}$ is generated by a transversal of its Φ-classes, where Φ is the Frattini subalgebra of $\mathbf{A}$. Building on this fact, Neumann is able to establish a bound on the cardinality of any critical group $\mathbf{A}$—under the assumptions of a finite exponent, a bound on the nilpotence class of any of its nilpotent factors, and a bound on it chief factors—by counting each of the factors in the following:

$$|\mathbf{A}/\Phi| = |A/C| \cdot |C/F| \cdot |F/\Phi|, \tag{5.1}$$

where Φ is the Frattini subgroup of $\mathbf{A}$, $\mathbf{F}$ is the Fitting subgroup of $\mathbf{A}$, and $\mathbf{C}$ is the centralizer of $\mathbf{F}/\Phi$. Among other facts, this count relies on the fact that in any finite group, the Frattini subalgebra of a group is nilpotent (and hence contained in the Fitting subgroup of the group, by definition.) (See Scott (1964), 7.4.4.) It is here that Neumann employs Theorem 51.37 (by way of Corollary 51.38), which we have sought to generalize with our Theorem 2.56. Thus, if this program is to be followed, we will need to answer (among other things) the following in the affirmative.

Problem 5.10. Let $\mathbf{A}$ be a finite Mal'cev algebra. By Theorem 2.54, $\mathbf{A}$ has a highest supernilpotent congruence, which we shall label σ. If Φ is the ^{1}Frattini congruence of $\mathbf{A}$, then is $\Phi \leq \sigma$? That is, is the ^{1}Frattini congruence of a finite Mal'cev algebra also supernilpotent?

Again, if we are to follow closely the example set by group theory in establishing this, it may be through an extension of Sylow theory to this more general setting; see Scott (1964), 7.3.13. Together with the desire to understand Problem 5.6, it is more than enough to motivate the next interesting problem. Note also that Theorem A.47 establishes that any nilpotent, Mal'cev algebra is polynomially equivalent to a quasigroup with operators.

Problem 5.11. Find out to what extent Sylow theory can be extended to quasigroups with operators, or, more generally, to congruence regular algebras. In particular, further analysis of (regular) congruences of prime power index (meaning each of its congruence class is of prime power) in any setting is desired.

This project has already been begun implicitly in Kearnes (1999) and Smith (2015), and perhaps elsewhere. This project may be substantial enough, but what may be ultimately needed is a generalization of the result of Gaschütz, given as Lemma 52.42 in Neumann (1967). On the other hand, perhaps only a small part of Sylow theory may be necessary to establish and make use of such a result in the broader setting of, say, nilpotent, Mal'cev algebras. Kearnes (1996) is also worth consulting regarding this question.

One can check by hand that the Mal'cev algebra supplied on p. 45 of Smith (1976) as an example of an algebra with an empty Frattini subalgebra is abelian. (Let me suggest using Remark A.38 to verify this—though there may be an easier way.) In light also of Theorem 237 in Smith (1976), it seems fair to wonder whether any nilpotent, Mal'cev algebra with an empty Frattini subalgebra is in fact abelian. This would make the Frattini subalgebra a potentially useful notion to answer Problem 1.3. For reference, we restate this now.

Problem 5.12. Settle whether or not any nilpotent algebra in a Mal'cev variety that has an empty Frattini subalgebra (as defined by Smith (1976), e.g.: Proposition 235) is abelian.

Finally, there is a subject which I have not touched on in this thesis, though it is well-developed elsewhere. Further study of the notion of what Kearnes (1996) calls normalization may lead to the resolution of Problem 1.3. I believe this to be a promising avenue of study and one which is evidently related to Theorem 3.12, above—at least if one considers their respective consequences. See also Freese and

McKenzie (1987), Chapter 10, for a further discussion of these matters. In particular, I would like to know whether if $\mathbf{A}$ is a subdirectly irreducible algebra that generates a congruence modular variety, then is $\mathbf{A}$ found in the variety generated by its normalization?

5.1.1 A small result and then a question, on the first-order definability of criticality

The strategy of many finite basis results, including McKenzie (1987a), Willard (2000), and Kearnes, Szendrei, and Willard (2013+) can be subsumed under the use of a general fact: that for a given locally finite variety $\mathcal{V}$ of finite signature, if it happens that there is a natural number N and elementary sentences φ and θ in the language of $\mathcal{V}$, such that the class of subdirectly irreducibles in $\mathcal{V}^{(N)}$ is axiomatized by φ, while the class of subdirectly irreducibles in $\mathcal{V}$ is axiomatized by θ, then $\mathcal{V}$ is finitely based. Using Mal'cev's description of congruence generation (Theorem A.9) it is not difficult to see that the concept of subdirect irreducibility is elementarily expressible, although one has to take greater pains and make use of further assumptions to capture such with a single sentence. On the other hand, criticality has historically (see MacDonald and Vaughan-Lee (1978) and Neumann (1967), for instance) included finiteness as part of its definition, which makes it impossible to first-order define. Now, we have shown in the above that it may not be necessary to include finiteness as part of the definition of criticality. On the other hand, as we observed, any critical algebra in a locally finite variety does indeed turn out to be finite. Indeed, our definition also remains resistant to elementary definition, as shown in the following result, which is really just an immediate corollary to work of MacDonald and Vaughan-Lee (1978).

Theorem 5.13. *There is a class $\mathcal{K}$ of algebras of finite signature and a variety $\mathcal{V}$ for which no set Γ of first order sentences exists such that*

$$\operatorname{Crit}\mathcal{V} = \{\mathbf{A} \in \mathcal{K} \mid \mathcal{A} \models \Gamma\}.$$

Proof. In MacDonald and Vaughan-Lee (1978), the authors exhibit a finite algebra $\mathbf{M}$ so that $\operatorname{Var}\mathbf{M}$ contains an infinite chain of critical algebras—in particular, it has no finite critical bound.[1] On the other hand, since $\mathcal{V} := \operatorname{Var}\mathbf{M}$ is locally finite, we have that each of these critical algebras is finite. A routine application of the compactness theorem then demonstrates the result. □

However, the following appears to be an open question.

Problem 5.14. Is there a variety $\mathcal{V}$ without a finite critical bound and yet for which $\operatorname{Crit}\mathcal{V}$ is still first-order definable (noting, as seen in the above, that $\mathcal{V}$ cannot then be locally finite)?

5.2 Concerning the higher centralizer of Bulatov

Is Bulatov's higher centralizer the "right" definition? How would one decide? One possible defect is its lack of symmetry and—what I take to be related—the apparent difficulty presented in discovering what properties and applications it holds outside of the context of congruence permutability. Even some properties, which are simple to prove in the case of the usual term-condition centralizer and commutator, are managed with surprising difficulty for the higher centralizer and commutator. Consider some "symmetrically-defined higher centralizers," by way of an example. Let $\mathbf{A}$ be an algebra with congruences θ_0, θ_1, and θ_2. Let n be any natural number, let t be a term for $\mathbf{A}$ of rank n. Choose natural numbers ℓ_0, ℓ_1, and ℓ_2 that sum to n, and pick tuples $\mathbf{a}_i$ and $\mathbf{b}_i$ of length ℓ_i, for each $i < 3$ such that $\mathbf{a}_i \; \theta_i^{\ell_i} \; \mathbf{b}_i$. One might consider the (four-place) centralizer defined by requiring the following implication to hold for all such choices in $\mathbf{A}$:

[1] 'M' is for Murskii, who invented it.

$$t^{\mathbf{A}}(\mathbf{a}_0, \mathbf{a}_1, \mathbf{a}_2)\,\gamma\, t^{\mathbf{A}}(\mathbf{a}_0, \mathbf{a}_1, \mathbf{b}_2) \text{ and } t^{\mathbf{A}}(\mathbf{b}_0, \mathbf{a}_1, \mathbf{a}_2)\,\gamma\, t^{\mathbf{A}}(\mathbf{b}_0, \mathbf{a}_1, \mathbf{b}_2)$$

$$\Downarrow$$

$$t^{\mathbf{A}}(\mathbf{a}_0, \mathbf{b}_1, \mathbf{a}_2)\,\gamma\, t^{\mathbf{A}}(\mathbf{a}_0, \mathbf{b}_1, \mathbf{b}_2) \text{ and } t^{\mathbf{A}}(\mathbf{b}_0, \mathbf{b}_1, \mathbf{a}_2)\,\gamma\, t^{\mathbf{A}}(\mathbf{b}_0, \mathbf{b}_1, \mathbf{b}_2)$$

Or, perhaps, the following implication would provide a better definition:

$$t^{\mathbf{A}}(\mathbf{a}_0, \mathbf{a}_1, \mathbf{a}_2)\,\gamma\, t^{\mathbf{A}}(\mathbf{a}_0, \mathbf{a}_1, \mathbf{b}_2)\,\gamma\, t^{\mathbf{A}}(\mathbf{b}_0, \mathbf{a}_1, \mathbf{a}_2)\,\gamma\, t^{\mathbf{A}}(\mathbf{b}_0, \mathbf{a}_1, \mathbf{b}_2)$$

$$\Downarrow$$

$$t^{\mathbf{A}}(\mathbf{a}_0, \mathbf{b}_1, \mathbf{a}_2)\,\gamma\, t^{\mathbf{A}}(\mathbf{a}_0, \mathbf{b}_1, \mathbf{b}_2)\,\gamma\, t^{\mathbf{A}}(\mathbf{b}_0, \mathbf{b}_1, \mathbf{a}_2)\,\gamma\, t^{\mathbf{A}}(\mathbf{b}_0, \mathbf{b}_1, \mathbf{b}_2)$$

It may be that a collection of rather more involved implications would be of even greater use. Indeed, the central principal to pay attention to may be the tracking of "collapse" in the dimensionality of the "geometric" arrangement (in the way of Gumm (1983)) of the various congruence relations possible between a so-called matrix of terms. A plausible commutator may come out of any reasonable notion of "collapse" and "projection" so conceived. But, for now, a specific question: Is the alternative centralizer or centralizers here conceived useful? My sense is that restoring the symmetry to the definition of the higher centralizer would yield properties, in the congruence-modular setting, for a higher centralizer and commutator so-defined, properties analogous to those that hold for the term-condition centralizer and commutator there, namely those given in Chapter 4 of Freese and McKenzie (1987). The further question is whether such a symmetrically-defined centralizer would continue to find as impressive applications in congruence permutable varieties; might any of these symmetrical centralizers be equivalent in the congruence permutable setting to the higher centralizer as originally defined?

The main question concerning the Bulatov centralizer and commutator is this: Can the properties that are known to hold for it in Mal'cev vareities be extended to a more general setting. A nice further project would be to see whether, using the 4-ary difference term of Kiss (see Kearnes, Szendrei, and Willard (2013+), section 6) in place of the Mal'cev term, one might be able to establish a part of Theorem 2.24 for varieties with a difference term. That is, by building a sequence of terms q_n through the composition of the Kiss difference term, rather than building these with the Mal'cev term, might we achieve an end as strong or nearly so as got in Theorem 2.24? For instance, with $q := q_2$ the 4-ary difference term of Kiss, for $n > 2$, let

$$q_n(x_0, \dots, x_{2^n-1}) = q(q_{n-1}(x_0, \dots, x_{2^{n-1}-1}), x_{2^{n-1}-1}, q_{n-1}(x_{2^{n-1}}, \dots, x_{2^n-1}), x_{2^n-1}).$$

Theorem 2.24 (i) $\Rightarrow$ (ii) appears to work for this new sequence of q_n's, using the "same proof."

As proof of concept, we now work toward a new result that serves as an illustration and application of what we have in mind. Fix a variety $\mathcal{V}$ with a difference term d. Following Lipparini (1999), we let

$$q(x_0, x_1, x_2, x_3) := d(d(x_1, x_3, x_3), d(x_0, x_2, x_3), x_3).$$

Note that $\mathcal{V} \models q(x, y, x, y) \approx y \approx q(x, x, y, y)$. We also need the following observation from Lipparini (1999). Let $\mathbf{A} \in \mathcal{V}$, and let $\alpha, \beta \in \operatorname{Con} \mathbf{A}$. Let $x, y, z, w, w' \in A$ such that $\langle x, y\rangle, \langle z, w\rangle, \langle z, w'\rangle \in \alpha$ and $\langle x, z\rangle, \langle y, w\rangle, \langle y, w'\rangle \in \beta$. let d denote the difference term operation for $\mathbf{A}$. Note that

$$d(d(w, w, w), d(z, z, w), w) = w \; [\alpha \cap \beta, \alpha \cap \beta] \; d(d(w, w', w'), d(z, z, w'), w').$$

It follows that

$$d(d(y, w, w), d(x, z, w), w) \; [\beta, \alpha \cap \beta] \; d(d(y, w', w'), d(x, z, w'), w').$$

In particular, these terms are $[\beta, \alpha]$-related. That is,

$$q(x, y, z, w) \; [\beta, \alpha] \; q(x, y, z, w').$$

Recall the notation of Theorem 2.24. Let $\theta_0, \theta_1 \in \operatorname{Con}\mathbf{A}$. Let n, ℓ_0, and ℓ_1 be natural numbers so that $\ell_0 + \ell_1 = n$. For $j = 0, 1$, choose $\mathbf{a}_j, \mathbf{b}_j \in A^{\ell_j}$ such that $\mathbf{a}_j \,\theta_j^{\ell_j}\, \mathbf{b}_j$. Let t be any term operation of rank n for $\mathbf{A}$. Let

$$\mathbf{e} = \langle t(\mathbf{a}_0, \mathbf{a}_1), t(\mathbf{b}_0, \mathbf{a}_1), t(\mathbf{a}_0, \mathbf{b}_1), t(\mathbf{b}_0, \mathbf{b}_1)\rangle.$$

Then

$$\begin{aligned}
\bar{\rho}_1 q(\mathbf{e}) &= q(t(\mathbf{b}_0, \mathbf{a}_1), t(\mathbf{b}_0, \mathbf{a}_1), t(\mathbf{b}_0, \mathbf{b}_1), t(\mathbf{b}_0, \mathbf{b}_1)) = t(\mathbf{b}_0, \mathbf{b}_1),\\
\bar{\rho}_2 q(\mathbf{e}) &= q(t(\mathbf{a}_0, \mathbf{b}_1), t(\mathbf{b}_0, \mathbf{b}_1), t(\mathbf{a}_0, \mathbf{b}_1), t(\mathbf{b}_0, \mathbf{b}_1)) = t(\mathbf{b}_0, \mathbf{b}_1), \text{ and}\\
\bar{\rho}_3 q(\mathbf{e}) &= q(t(\mathbf{b}_0, \mathbf{b}_1), t(\mathbf{b}_0, \mathbf{b}_1), t(\mathbf{b}_0, \mathbf{b}_1), t(\mathbf{b}_0, \mathbf{b}_1)) = t(\mathbf{b}_0, \mathbf{b}_1).
\end{aligned}$$

In particular,

$$q(t(\mathbf{b}_0, \mathbf{a}_1), t(\mathbf{b}_0, \mathbf{a}_1), t(\mathbf{b}_0, \mathbf{b}_1), t(\mathbf{b}_0, \mathbf{b}_1)) = q(t(\mathbf{b}_0, \mathbf{b}_1), t(\mathbf{b}_0, \mathbf{b}_1), t(\mathbf{b}_0, \mathbf{b}_1), t(\mathbf{b}_0, \mathbf{b}_1))$$

and hence

$$\begin{aligned}
&q(t(\mathbf{a}_0, \mathbf{a}_1), t(\mathbf{b}_0, \mathbf{a}_1), t(\mathbf{a}_0, \mathbf{b}_1), t(\mathbf{b}_0, \mathbf{b}_1))[\theta_0, \theta_1]\\
&\qquad\qquad q(t(\mathbf{a}_0, \mathbf{b}_1), t(\mathbf{b}_0, \mathbf{b}_1), t(\mathbf{a}_0, \mathbf{b}_1), t(\mathbf{b}_0, \mathbf{b}_1)) = t(\mathbf{b}_0, \mathbf{b}_1).
\end{aligned}$$

Using this observation and previous work, we soon find the following.

Theorem 5.15. *Let $\mathbf{A}$ be an algebra in a variety with a difference term d. Define q as above. Let $\theta_0, \theta_1 \in \operatorname{Con}\mathbf{A}$. Then the following are equivalent:*

(i) $C(\theta_0, \theta_1; 0_A)$*;*

(ii) $q^{\mathbf{A}}(e_0, e_1, e_2, e_3) = e_3$*, for all* $\mathbf{e} \in Q(\theta_0, \theta_1)$ *and if* $\mathbf{e}, \mathbf{e}' \in Q(\theta_0, \theta_1)$ *such that, for* $i < 3$*,* $e_i = e_i'$*, then* $q^{\mathbf{A}}(e_0, e_1, e_2, e_3) = q^{\mathbf{A}}(e_0, e_1, e_2, e_3')$*;*

(iii) $C_2(\theta_0, \theta_1; 0_A)$.

(See Definition 2.4 for notation.)

Proof. In the argument proceeding the statement of this theorem, we saw that (i) implies (ii). That (iii) implies (i) was done in Proposition 2.12.

Now, suppose that (ii) holds. Let n, ℓ_0, and ℓ_1 be natural numbers such that $\ell_0 + \ell_1 = n$. For $j = 0, 1$, choose $\mathbf{a}_j, \mathbf{b}_j \in A^{\ell_j}$ such that $\mathbf{a}_j \; \theta_j^{\ell_j} \; \mathbf{b}_j$. Let t and s be any term operations of rank n for $\mathbf{A}$. Suppose that

$$\begin{aligned} t(\mathbf{a}_0, \mathbf{a}_1) &= s(\mathbf{a}_0, \mathbf{a}_1), \\ t(\mathbf{b}_0, \mathbf{a}_1) &= s(\mathbf{b}_0, \mathbf{a}_1), \text{ and} \\ t(\mathbf{a}_0, \mathbf{b}_1) &= s(\mathbf{a}_0, \mathbf{b}_1). \end{aligned}$$

Then, by (ii), we have that

$$t(\mathbf{b}_0, \mathbf{b}_1) = q^{\mathbf{A}}(t(\mathbf{a}_0, \mathbf{a}_1), t(\mathbf{b}_0, \mathbf{a}_1), t(\mathbf{a}_0, \mathbf{b}_1), t(\mathbf{b}_0, \mathbf{b}_1)) =$$
$$q^{\mathbf{A}}(s(\mathbf{a}_0, \mathbf{a}_1), s(\mathbf{b}_0, \mathbf{a}_1), s(\mathbf{a}_0, \mathbf{b}_1), s(\mathbf{b}_0, \mathbf{b}_1)) = s(\mathbf{b}_0, \mathbf{b}_1),$$

which proves (iii). □

A portion of the above theorem is covered by Lemmas 2.3 and 6.2 from Kearnes, Szendrei, and Willard (2013+).

In order to generalize the above theorem, it may be necessary to first develop a generalization of the 4-difference term of Kiss. I submit the following for further consideration. Let n be a natural number. Fix a variety $\mathcal{V}$. Suppose that q_n is a rank-2^n term for $\mathcal{V}$, such that

$$\mathcal{V} \models \bar{\rho}_r q_n(x_0, \dots, x_{2^n-1}) \approx x_{2^n-1},$$

for each natural number r such that $0 < r < 2^n$. Suppose also that the following condition holds. Let $\mathbf{A} \in \mathcal{V}$, and choose $\theta_0, \dots, \theta_{n-1} \in \operatorname{Con} \mathbf{A}$. Let $\mathbf{e}, \mathbf{e}' \in Q(\theta_0, \dots, \theta_{n-1})$ such that $e_i = e'_i$, for $i < 2^n - 1$. Then we require that

$$q_n^{\mathbf{A}}(e_0, \dots, e_{2^n-1}) \; S(\theta_0, \dots, \theta_{n-1}) \; q_n^{\mathbf{A}}(e'_0, \dots, e'_{2^n-1}).$$

(See Definition 2.27 for notation.) Let us call such a term an n-difference term.

Problem 5.16. Let n be a natural number. Do difference term varieties have an n-difference term? Do congruence modular varieties have an n-difference term?

5.3 Concerning the commutator in varieties with a weak-difference term

In analogy to Theorem 4.42 and Theorem 4.41 in Chapter 4, it would be interesting to know whether the following hold.

Problem 5.17. Let $\mathcal{V}$ be a variety with a weak-difference term. Suppose that for any algebra $\mathbf{A} \in \mathcal{V}$ and any $\alpha, \beta, \theta \in \operatorname{Con} \mathbf{A}$ such that $\beta \leq \alpha$, we have that

$$[\alpha \vee \theta, \beta \vee \theta] \leq [\alpha, \beta] \vee \theta.$$

Does it then follow that $\mathcal{V}$ has a difference term?

Problem 5.18. Let $\mathcal{V}$ be a variety with a weak-difference term. Suppose that for any algebra $\mathbf{A} \in \mathcal{V}$ and any $\alpha, \beta, \theta \in \operatorname{Con} \mathbf{A}$ such that $\beta \leq \alpha$, we have that

$$[(\alpha \vee \theta)/\theta, (\beta \vee \theta)/\theta] = [\alpha \vee \theta, \beta \vee \theta]/\theta.$$

Does it then follow that $\mathcal{V}$ has a difference term?

Bibliography

Aichinger, Erhard and Nebojša Mudrinski (2010). “Some applications of higher commutators in Mal’cev algebras”. In: *Algebra Universalis* 63.4, pp. 367–403. URL: `http://dx.doi.org/10.1007/s00012-010-0084-1`.

Berman, Joel, Paweł Idziak, Petar Marković, Ralph McKenzie, Matthew Valeriote, and Ross Willard (2010). “Varieties with few subalgebras of powers”. In: *Trans. Amer. Math. Soc.* 362.3, pp. 1445–1473. URL: `http://dx.doi.org/10.1090/S0002-9947-09-04874-0`.

Birkhoff, G. (1935). “On the structure of abstract algebras”. In: *Proc. Cambridge Phil. Soc.* 31, pp. 433–454.

— (1944). “Subdirect unions in universal algebra”. In: *Bull. Amer. Math. Soc.* 11, pp. 764–768.

Bulatov, Andrei (2001). “On the number of finite Mal’ tsev algebras”. In: *Contributions to general algebra, 13 (Velké Karlovice, 1999/Dresden, 2000)*. Heyn, Klagenfurt, pp. 41–54.

Foster, Alfred L. and Alden F. Pixley (1964). “Semi-categorical algebras. II”. In: *Math. Z.* 85, pp. 169–184.

Freese, Ralph and Ralph McKenzie (1981). “Residually small varieties with modular congruence lattices”. In: *Trans. Amer. Math. Soc.* 264.2, pp. 419–430. URL: `http://dx.doi.org/10.2307/1998548`.

— (1987). *Commutator theory for congruence modular varieties.* Vol. 125. London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge, pp. iv+227.

Gumm, H. Peter (1983). “Geometrical methods in congruence modular algebras”. In: *Mem. Amer. Math. Soc.* 45.286, pp. viii+79. URL: `http://dx.doi.org/10.1090/memo/0286`.

Hagemann, Joachim and Christian Herrmann (1979). "A concrete ideal multiplication for algebraic systems and its relation to congruence distributivity". In: *Arch. Math. (Basel)* 32.3, pp. 234–245. URL: http://dx.doi.org/10.1007/BF01238496.

Higman, Graham (1959). "Some remarks on varieties of groups". In: *Quart. J. Math. Oxford Ser. (2)* 10, pp. 165–178.

Hobby, David and Ralph McKenzie (1988). *The structure of finite algebras*. Vol. 76. Contemporary Mathematics. American Mathematical Society, Providence, RI, pp. xii+203. URL: http://dx.doi.org/10.1090/conm/076.

Kearnes, Keith A. (1995). "Varieties with a difference term". In: *J. Algebra* 177.3, pp. 926–960. URL: http://dx.doi.org/10.1006/jabr.1995.1334.

— (1996). "Critical algebras and the Frattini congruence. II". In: *Bull. Austral. Math. Soc.* 53.1, pp. 91–100. URL: http://dx.doi.org/10.1017/S0004972700016750.

— (1999). "Congruence modular varieties with small free spectra". In: *Algebra Universalis* 42.3, pp. 165–181. URL: http://dx.doi.org/10.1007/s000120050132.

Kearnes, Keith A., Ágnes Szendrei, and Ross Willard (2013+). "A finite basis theorem for difference term varieties with a finite residual bound". In: *Trans. Amer. Math. Soc.* To appear.

Kiss, Emil W. and S. M. Vovsi (1995). "Critical algebras and the Frattini congruence". In: *Algebra Universalis* 34.3, pp. 336–344. URL: http://dx.doi.org/10.1007/BF01182090.

Lipparini, P. (1999). "A Kiss 4-difference term from a ternary term". In: *Algebra Universalis* 42.1-2, pp. 153–154. URL: http://dx.doi.org/10.1007/s000120050130.

Lipparini, Paolo (1994). "Commutator theory without join-distributivity". In: *Trans. Amer. Math. Soc.* 346.1, pp. 177–202. URL: http://dx.doi.org/10.2307/2154948.

Lyndon, R. C. (1951). "Identities in two-valued calculi". In: *Trans. Amer. Math. Soc.* 71, pp. 457–465.

— (1952). "Two notes on nilpotent groups". In: *Proc. Amer. Math. Soc.* 3, pp. 579–583.

— (1954). "Identities in finite algebras". In: *Proc. Amer. Math. Soc.* 5, pp. 8–9.

MacDonald, Sheila Oates and M. R. Vaughan-Lee (1978). "Varieties that make one Cross". In: *J. Austral. Math. Soc. Ser. A* 26.3, pp. 368–382.

Mal'cev, A. I. (1954). “On the general theory of algebraic systems”. In: *Mat. Sb. N.S.* 35(77), pp. 3–20.

Mamedov, Oktay M. (2007). “Some commutator properties of a variety with a weak difference term”. In: *Trans. Natl. Acad. Sci. Azerb. Ser. Phys.-Tech. Math. Sci.* 27.1, Math. Mech. Pp. 89–94.

Mayr, Peter (2011). “Mal'cev algebras with supernilpotent centralizers”. In: *Alg. Univ.* 65.2, pp. 193–211. URL: http://dx.doi.org/10.1007/s00012-011-0124-5.

McKenzie, Ralph (1970). “Equational bases for lattice theories”. In: *Math. Scand.* 27, pp. 24–38.

— (1987a). “Finite equational bases for congruence modular varieties”. In: *Alg. Univ.* 24.3, pp. 224–250. URL: http://dx.doi.org/10.1007/BF01195263.

— (1987b). “Nilpotent and solvable radicals in locally finite congruence modular varieties”. In: *Algebra Universalis* 24.3, pp. 251–266. URL: http://dx.doi.org/10.1007/BF01195264.

— (1996). “Tarski's finite basis problem is undecidable”. In: *Internat. J. Alg. Comput.* 6, pp. 49–104. URL: http://dx.doi.org/10.1142/S0218196796000040.

McKenzie, Ralph N., George F. McNulty, and Walter F. Taylor (1987). *Algebras, lattices, varieties. Vol. I.* The Wadsworth & Brooks/Cole Mathematics Series. Wadsworth & Brooks/Cole Adv. Books & Software, Monterey, CA, pp. xvi+361.

Murskiĭ, V. L. (1965). “The existence in the three-valued logic of a closed class with a finite basis having no finite complete system of identities”. In: *Dokl. Akad. Nauk SSSR* 163, pp. 815–818.

Neumann, Hanna (1967). *Varieties of groups.* Springer-Verlag New York, Inc., New York, pp. x+192.

Oates, Sheila and M. B. Powell (1964). “Identical relations in finite groups”. In: *J. Algebra* 1, pp. 11–39.

Opršal, Jakub (2014+). “A relational description of higher commutators in Mal'cev varieties”. URL: http://arxiv.org/abs/1412.5776v1.

Scott, W. R. (1964). *Group theory.* Prentice-Hall, Englewood Cliffs, N.J., pp. xi+479.

Smith, Jonathan D. H. (1976). *Mal' cev varieties.* Lecture Notes in Mathematics, Vol. 554. Springer-Verlag, Berlin-New York, pp. viii+158.

Smith, Jonathan D. H. (2015). “Sylow theory for quasigroups”. In: *J. Combin. Des.* 23.3, pp. 115–133. URL: http://dx.doi.org/10.1002/jcd.21415.

Vaughan-Lee, M. R. (1983). “Nilpotence in permutable varieties”. In: *Universal algebra and lattice theory (Puebla, 1982)*. Vol. 1004. Lecture Notes in Math. Springer, Berlin, pp. 293–308. URL: http://dx.doi.org/10.1007/BFb0063445.

Willard, Ross (2000). “A finite basis theorem for residually finite, congruence meet-semidistributive varieties”. In: *J. Symbolic Logic* 65.1, pp. 187–200. URL: http://dx.doi.org/10.2307/2586531.

Appendix A

Fundamentals

A.1 Fundamentals of general (universal) algebra

Following in the footsteps of Garrett Birkhoff, Anatoli Mal'cev, Alfred Tarski and others, we take a permissive view of the appellation "algebra." When we say *algebra* we mean a nonempty set A together with an indexed list, say Φ, (possibly empty) of operations on A. We use boldface for the algebra, as distinguished from the set, as in $\mathbf{A} = \langle A, \Phi \rangle$. In this case, we also call A the *universe* of $\mathbf{A}$. The operations of $\mathbf{A}$, that is, the elements ϕ appearing in Φ, should be viewed as elements of A^{A^κ}, for some cardinal κ where κ is called the *arity* of f. Throughout this text, however, we shall consider only the case of κ a finite cardinal; that is, all operations will be of finite arity. We shall call any one-element algebra *trivial*.

Now, it is useful to consider the class $\mathcal{K}$ of all algebras each of whose list of operations is indexed by the same index set, say F. We call F the set of fundamental operations for $\mathcal{K}$. For each $\mathbf{A} = \langle A, \Phi \rangle \in \mathcal{K}$, we devise an *interpretation* of $f \in F$ in $\mathbf{A}$, by mapping f to the element of Φ indexed by f. The interpretation map so defined is written $f \mapsto f^{\mathbf{A}}$, for a given $\mathbf{A} \in \mathcal{K}$ and $f \in F$. The interpretation of f in $\mathbf{A}$, that is, $f^{\mathbf{A}}$, is called a *fundamental operation* of $\mathbf{A}$. We may also use the symbol $F^{\mathbf{A}}$ in place of Φ in this context.

We shall also like to associate a uniform arity to all fundamental operations indexed by the same symbol. Thus, we require a function, say ρ that assigns to each $f \in F$ its intended arity. Let $\mathcal{K}$ be a class of algebras each of which has fundamental operations indexed by F, with which is associated the arity function ρ. Suppose also that for any $\mathbf{A}, \mathbf{B} \in \mathcal{K}$, and any $f \in F$ of arity, say r, $f^{\mathbf{A}} \in A^{A^r}$ and $f^{\mathbf{B}} \in B^{B^r}$. When this holds, we shall say that $\mathcal{K}$ consists in *similar* algebras or algebras of the same *similarity type*. If you like, the word 'type,' here, refers to the arity function, ρ, which we shall also call the *signature of* $\mathcal{K}$. Thus, we shall typically say that similar algebras are of the same *signature*.

Within the context of a fixed signature, we can develop the standard mathematical notions of homomorphic image, subalgebra, and direct or Cartesian product. Fix any class $\mathcal{K}$ of similar algebras. Given $\mathbf{A}, \mathbf{B} \in \mathcal{K}$, and a map $h : A \to B$, we say that h is a *homomorphism*, provided it respects the indexing of the respective operations, indicating this by modifying the map-notation to include bold print, writing $h : \mathbf{A} \to \mathbf{B}$. That is, $h : A \to B$ is a homomorphism if and only if, for any fundamental operation symbol f (with arity, say, r) and any $a_0, \ldots, a_{r-1} \in A$, $h(f^{\mathbf{A}}(\mathbf{a})) = f^{\mathbf{B}}(h(a_0), \ldots, h(a_{r-1}))$.

Any subset A' of A that is closed under the operations of $\mathbf{A}$ can also be used as the universe of an algebra of the same similarity type; for fundamental operation f, we interpret $f^{\mathbf{A}'}$ to be the restriction of $f^{\mathbf{A}}$ to A'. In this circumstance, $\mathbf{A}'$ is called a *subalgebra* of $\mathbf{A}$.

If $\mathcal{C}$ is a collection of subalgebras of a given algebra $\mathbf{A}$, then $\cap\mathcal{C}$ is also a subalgebra. In particular, if $\mathcal{D}$ is any collection of subalgebras of a given algebra, and $\mathcal{C}$ is the collection of all subalgebras that contains $\cup\mathcal{D}$, then $\cap\mathcal{C}$ is the least subalgebra containing all of them. From these observations, it is established that the set of subalgebras of a given algebra can be given a lattice structure—that is, it is naturally endowed with a partial order (set inclusion) with which we can associate least upper bound and greatest lower bound functions. We remark here, too, that if S is a subset of the universe of some given algebra, then we can obtain a least subalgebra containing S; we call this the *subalgebra generated by* S, and denote it $\mathrm{Sg}^{\mathbf{A}}\, S$.

Now, let I be any (index) set, and let $\mathbf{A}_i \in \mathcal{K}$ for all $i \in I$. We take the direct product $\Pi_{i\in I} A_i$ of these algebras as the universe of an algebra by interpreting a given fundamental operation symbol coordinate-wise: Let r be a natural number, and say that f is a fundamental operation symbol of arity r. Take $\mathbf{a}_0, \ldots, \mathbf{a}_{r-1} \in \Pi_I A_i$; then we set

$$f^{\mathbf{\Pi}_I \mathbf{A}_i}(\mathbf{a}_0, \ldots, \mathbf{a}_{r-1}) := \langle f^{\mathbf{A}}(\mathbf{a}_0(i), \ldots, \mathbf{a}_{r-1}(i)) \mid i \in I \rangle.$$

In the usual fashion, we shall write $\mathbf{A}_0 \times \mathbf{A}_1$ for $\Pi_I \mathbf{A}_i$, when $I = \{0, 1\}$, and so on. Also, when $\mathbf{A}_i = \mathbf{A}$, we write $\Pi_{i\in I} \mathbf{A}_i = \mathbf{A}^I$, calling such a *power of* $\mathbf{A}$.

Let $h : \mathbf{A} \to \mathbf{B}$ be a homomorphism of similar algebras. As is always the case, we can associate with h an equivalence relation on A, denoted by $\ker h$ and defined by $\langle x, y \rangle \in \ker h \Leftrightarrow h(x) = h(y)$. As h respects the indexing of the operations of $\mathbf{A}$ and $\mathbf{B}$, we get also that $\ker h$ respects or is *compatible* with this indexing. That is to say, for $\theta = \ker h$, we have that if f is any fundamental operation symbol of arity, say, r, and $\langle a_0, b_0 \rangle, \ldots, \langle a_{r-1}, b_{r-1} \rangle \in \theta$, then $\langle f^{\mathbf{A}}(a_0, \ldots, a_{r-1}), f^{\mathbf{A}}(b_0, \ldots, b_{r-1}) \rangle \in \theta$. Any equivalence relation θ on $\mathbf{A}$ that respects the operations of $\mathbf{A}$ in this way is called a *congruence* on $\mathbf{A}$. We denote the set of all congruences on $\mathbf{A}$ by $\operatorname{Con} \mathbf{A}$. Note, in particular, that every congruence forms the universe of a subalgebra of $\mathbf{A} \times \mathbf{A}$.

Like the set of all subalgebras of a given algebra, we find that its set of congruences forms a lattice, where, again the partial order is simply set inclusion. As well in this case, we also find that the intersection of any collection of congruences on a given $\mathbf{A}$ is again a congruence. Thus, for any set of pairs $R \subseteq A^2$, we can obtain a least congruence on $\mathbf{A}$ containing R; we call this the *congruence generated by* R, denoting it $\operatorname{Cg}^{\mathbf{A}} R$, often choosing to suppress the mention of $\mathbf{A}$ in the notation.

It is useful to note that the study of congruences parallels the study of normal subgroups in group theory and of ideals in ring theory; indeed, it is adequate to completely replace or reconfigure the study of these concepts in the respective areas mentioned. Indeed, one can view the kernel of a group homomorphism h as simply the equivalence class of the identity element, with the equivalence relation being that induced by the map h. As the presence of a one element subalgebra is not, in general, assured, it is not always possible to associate congruence classes with subalgebras in this way; thus, in most applications, the study of congruences replaces what we might have taken as the generalization of the study of normal subgroups and the like.

As is the case in many areas of mathematics, we also can develop a notion of quotient structure. Fix a signature, say ρ. Let $\mathbf{A}$ be an algebra, and let $\theta \in \operatorname{Con} \mathbf{A}$. For any $a \in A$, we shall denote by a/θ the set $\{b \in A \mid \langle a, b\rangle \in \theta\}$. We shall then let $A/\theta = \{a/\theta \mid a \in A\}$. It is not difficult to verify that the fact that θ respects the operations of $\mathbf{A}$ enables us to define an interpretation of the fundamental operations on A/θ. For any fundamental operation symbol given by ρ, of arity, say, r, and any elements $a_0, \ldots, a_{r-1} \in A$, we let $f^{\mathbf{A}/\theta}(a_0/\theta, \ldots, a_{r-1}/\theta) = f^{\mathbf{A}}(a_0, \cdots a_{r-1})/\theta$. It is also not hard to discover that the natural quotient map from $\mathbf{A}$ into $\mathbf{A}/\theta$ is a homomorphism, and, conversely, any image of $\mathbf{A}$ under a given homomorphism h is isomorphic to the quotient structure on the $\ker h$-classes of A. This series of facts is usually called the Homomorphism Theorem or the First Isomorphism Theorem. Another closely related fact is also easily verified: The image of any homomorphism is a subalgebra of the codomain-algebra. We display these observations here for ease of reference.

Theorem A.1. *(First Isomorphism Theorem) Let $h : \mathbf{A} \to \mathbf{B}$ be a homomorphism. Let $\operatorname{im} h$ denote the image of A under h. Then $B' := \operatorname{im} h$ is closed under the operations of $\mathbf{B}$. Furthermore, $\mathbf{B}'$ is isomorphic to $\mathbf{A}/\ker h$.*

Let $\mathbf{A}$ be any algebra in some class $\mathcal{K}$ of similar algebras, with set of fundamental operation symbols F. As is always the case, we may compose any fundamental operations provided on $\mathbf{A}$ to build new ones, calling these derived operations *term operations*. It is useful to devise an indexing system for these term operations as well. To that end, we choose any set of distinct symbols X duplicating the natural numbers, which we shall call the set of *variables*. We shall write $X = \{x_i \mid i \in \omega\}$. We now let T be smallest set of strings of symbols in the alphabet $X \cup F$ so that

- $T \supset X$ and
- whenever f is a symbol of intended arity r (for whatever r) and $t_0, \ldots, t_{r-1} \in T$, then $ft_0 \ldots t_{r-1} \in T$.

Note that this definition is sound, as, whenever T and T' have the bulleted properties, their intersection does as well. The elements in T are called *terms*. Observe also that we can provide the set T with the structure given by the signature of $\mathcal{K}$; that is, we can interpret each of the fundamental operation symbols for $\mathcal{K}$ as operations on T. Given fundamental operation symbol f of arity, say r, and any $t_0, \ldots, t_{r-1} \in T$, we set $f^{\mathbf{T}}(t_0, \ldots, t_{r-1}) = ft_0 \ldots t_{r-1}$.

We shall extend the meaning of our interpretation map to also include these terms. We do so recursively. For each $x_i \in X$ and for any $\mathbf{A} \in \mathcal{K}$, we let $x_i^{\mathbf{A}} \in A^{A^\omega}$ be the i^{th} projection function. Then, for any $t = ft_0 \ldots t_{r-1}$, where f is a fundamental operation of a given arity r, and t_i is a term operation for each $i < r$, for any ω-tuple $\mathbf{a}$ of elements of A, we let $t^{\mathbf{A}}(\mathbf{a}) = f^{\mathbf{A}}(t_0^{\mathbf{A}}(\mathbf{a}), \ldots, t_{r-1}^{\mathbf{A}}(\mathbf{a}))$.

Even though we interpret each term operation in $\mathbf{A}$ as an element of A^{A^ω}—and are thus all operations of arity ω, apparently—there is a more useful notion of arity to associate with a given term t: that of the number of distinct variables that appear in t. With this basic aim in mind, for set of terms T, we shall let $\mathrm{Rank} : T \to \omega$ be the function that identifies the highest index, plus one, among variables appearing in a given term. Of course, for a given $t \in T$, we shall call $\mathrm{Rank}(t)$, its *rank*. (For instance, if only the variable x_0 appears in a term, then it is of rank 1.) We shall most often adopt a notation for terms to emphasize their rank, writing, for instance, $t = t(x_0, \ldots, x_{r-1})$ for a term t of rank r.

Fix a signature, and an algebra $\mathbf{A}$ of this signature. Let n be a natural number. We shall let $\operatorname{Clo}_n \mathbf{A}$ denote the set of all term operations on $\mathbf{A}$. That is, letting T be the set of terms, as defined above, we set

$$\operatorname{Clo}_n \mathbf{A} = \{t^{\mathbf{A}} \mid \operatorname{Rank}(t) = n\}.$$

We shall also denote by $\operatorname{Clo} \mathbf{A}$ or $\operatorname{Clo}_\omega \mathbf{A}$, the set $\{t^{\mathbf{A}} \mid t \in T\} = \bigcup_{n \in \omega} \operatorname{Clo}_n \mathbf{A}$. It is not difficult to see that $\operatorname{Clo} \mathbf{A}$ and, for any natural number n, $\operatorname{Clo}_n \mathbf{A}$ can provide the universe of an algebra of the same signature as $\mathbf{A}$, and that, furthermore, we get that, for $\alpha \in \omega \cup \{\omega\}$, $\operatorname{Clo}_\alpha \mathbf{A}$ is a subalgebra of $\mathbf{A}^{A^\alpha}$. In fact,

$$\operatorname{Clo}_\alpha \mathbf{A} = \operatorname{Sg}^{\mathbf{A}^{A^\omega}} \{x_n^{\mathbf{A}} \mid n \in \alpha\};$$

that is, $\operatorname{Clo}_\alpha \mathbf{A}$ is the subalgebra of $\mathbf{A}^{A^\omega}$ generated by the set of projection functions, $\{x_n^{\mathbf{A}} \mid n \in \alpha\}$.

Let Λ be any set. For any $\lambda \in \Lambda$, let π_λ be the λ^{th} projection function from A^Λ onto A. We let $\mathbf{Clo}_\Lambda \mathbf{A}$ be the subalgebra of A^{A^Λ} generated by $\{\pi_\lambda \mid \lambda \in \Lambda\}$. We call the algebra $\mathbf{Clo}_\Lambda \mathbf{A}$ the *clone of* $\mathbf{A}$ *over* Λ.

We shall also like to refer to an operation s formed on a given algebra $\mathbf{A}$ by beginning with a term operation and substituting in fixed elements of A for some of its variables; we shall call maps formed in this way, *polynomials.* To be precise, for any $\alpha \in \omega \cup \{\omega\}$, we shall let

$$\operatorname{Pol}_\alpha \mathbf{A} := \operatorname{Sg}^{\mathbf{A}^{A^\omega}} \{x_n^{\mathbf{A}} \mid n \in \alpha\} \cup \{a^{\mathbf{A}} \mid a \in A\},$$

where, for any $a \in A$, $a^{\mathbf{A}} : A^\omega \to A$ is the map defined $a^{\mathbf{A}}(\mathbf{x}) = a$, for all $\mathbf{x} \in A^\omega$.

It will be our most common practice to write term operations and polynomials as if they only depend on the variables of index lower than their rank, as in $t = t(x_0, \ldots, x_{r-1})$ for a term t of rank r.

Now, it may happen, given terms t and s, that $t^{\mathbf{A}} = s^{\mathbf{A}}$. When this occurs we say that *the equation* $t \approx s$ *holds in* $\mathbf{A}$. Thus, by "equation," we mean an ordered pair of terms, but writing it in the manner above. Under this circumstance, we also write $\mathbf{A} \models s \approx t$, reading it as "$\mathbf{A}$ models $s \approx t$" or "φ is true in $\mathbf{A}$." Further, if $\mathcal{K}$ is any class of similar algebras and Σ is any set of equations written using the symbols provided by the signature, then we write $\mathcal{K} \models \Sigma$ provided $\mathbf{A} \models \Sigma$ for all $\mathbf{A} \in \mathcal{K}$, with $\mathbf{A} \models \Sigma$ meaning that $\mathbf{A} \models \varphi$ for all $\varphi \in \Sigma$. Let us call the set of equations associated with a given signature the *language provided by the signature.*

Now, within a class $\mathcal{K}$ of similar algebras, we can consider the subclass of algebras each of which satisfies a given set of equations. Given Σ, a set of equations written in the language associated with the signature, we call the subclass of algebras $\mathbf{A}$ in $\mathcal{K}$, such that $\mathbf{A} \models \Sigma$, *the variety based on* Σ; denote this by $\operatorname{Mod}\Sigma$. On the other hand, for any class $\mathcal{K}$ of similar algebras, we can lay our hands on the set of equations φ such that $\mathbf{A} \models \varphi$ for all $\mathbf{A} \in \mathcal{K}$; let us call this the *equational theory of* $\mathcal{K}$, denoting it $\operatorname{Th}_{\mathrm{eq}}\mathcal{K}$. Further, for a fixed signature, one can begin with Σ, a set of equations in the language provided by the signature, and consider $\Phi = \operatorname{Th}_{\mathrm{eq}}\operatorname{Mod}\Sigma$; we then say that Σ provides a *base* for Φ. We also write $\Sigma \models \Phi$, reading it as "Σ logically implies Φ." Whenever for a given equational theory Φ or variety $\mathcal{V}$ we can find a finite set Σ of equations such that $\Sigma \models \Phi$ or $\mathcal{V} = \operatorname{Mod}\Sigma$, we say that Φ or $\mathcal{V}$ is *finitely based.* One of the fundamental goals with we are concerned with in this thesis is to develop tools that may help in establishing what varieties are finitely based. Such a result we call a finite basis result.

Let us take an arbitrary class $\mathcal{K}$ of similar algebras and denote by $\operatorname{Var}\mathcal{K}$ the class of all algebras satisfying each equation true in $\mathcal{K}$, i.e., $\operatorname{Mod}\operatorname{Th}_{\mathrm{eq}}\mathcal{K}$. (For $\mathcal{K} = \{\mathbf{A}\}$, we shall write $\operatorname{Var} A$ in place of $\operatorname{Var}\mathcal{K}$.) This is the variety generated by $\mathcal{K}$, and, we might remark, represents the structures satisfying a syntactically-framed condition holding in $\mathcal{K}$. It is natural to wonder whether one can obtain a structural, or "semantic," description of such a class of algebras. Indeed, Birkhoff was able to show that $\operatorname{Mod}\operatorname{Th}_{\mathrm{eq}}\mathcal{K}$ is precisely the closure of $\mathcal{K}$ under the formation of products, subalgebras, and homomorphic images; conversely, any class closed under these three class operators is also equationally definable—that is, it is a variety. Thus, Birkhoff gave a semantically-minded description of a natural syntactically-framed notion—unless what he did was provide a syntactical description of a structurally-focused condition that we may find natural to consider, namely closure under the three class operations just mentioned.

To formalize the preceding paragraph, let $\mathcal{K}$ be a class of similar algebras. Let $\mathcal{C}$ be the class of all algebras of that signature. Let

$$H\mathcal{K} = \{\mathbf{A} \mid A = h(B) \text{ for homomorphism } h \text{ and } \mathbf{B} \in \mathcal{K}\}.$$

Let

$$S\mathcal{K} = \{\mathbf{A} \mid \text{ for some } \mathbf{A}' \in \mathcal{K}, \text{ and } \mathbf{B} \in \mathcal{K}, \mathbf{A} \cong \mathbf{A}' \leq \mathbf{B}\},$$

and let

$$P\mathcal{K} = \{\mathbf{A} \mid \text{ for some set } I, \text{ and } \mathbf{A}_i \in \mathcal{K}, \text{ for each } i \in I, \mathbf{A} \cong \Pi_I \mathbf{A}_i\}.$$

What Birkhoff showed, then, is the following.

Theorem A.2. *(Birkhoff's HSP-Theorem) Let $\mathcal{K}$ be a class of similar algebras. Then $\mathcal{K}$ is a variety if and only if $\mathcal{K} = HSP\mathcal{K}$. In particular,* $\operatorname{Var}\mathcal{K} = HSP\mathcal{K}$.

A.1.1 On free algebras

It is useful to prove a part of Birkhoff's HSP-Theorem, as we are able to extract from the proof some further important concepts. Let $\mathcal{V}$ be a variety. Let Φ be the set of all equations that fail in $\mathcal{V}$. Then, for any $\varphi \in \Phi$, we can find an $\mathbf{A}_\varphi \in \mathcal{V}$ such that $\mathbf{A}_\varphi \not\models \varphi$. Let $\mathbf{B} = \Pi_\Phi \mathbf{A}_\varphi$. Note that if φ is any equation that fails in $\mathcal{V}$, then φ fails in $\mathbf{B}$, since term operations and hence equations are computed coordinate-wise. Let κ be any cardinal. Let $\mathbf{F} = \mathbf{Clo}_\kappa \mathbf{B}$. Recall that $\mathbf{Clo}_\kappa \mathbf{B}$ is the subalgebra of $\mathbf{B}^{B^\kappa}$ that is generated by the projection functions $\{\pi_\lambda \mid \lambda < \kappa\}$. We claim that any

κ-generated algebra $\mathbf{A}$ from $\mathcal{V}$ is a homomorphic image of $\mathbf{F}$. To see this, we shall first demonstrate that any equation that fails in $\mathbf{B}$ fails also in $\mathbf{F}$. So, suppose that $t \approx s$ is an equation in the language of $\mathcal{V}$ that fails in $\mathbf{B}$. Suppose that t and s are of rank r (or less), and write $t = t(x_0, \dots, x_{r-1})$ and $s = s(x_0, \dots, x_{r-1})$. Take $b_0, \dots, b_{r-1} \in B$ such that

$$t^{\mathbf{B}}(b_0, \dots, b_{r-1}) \neq s^{\mathbf{B}}(b_0, \dots, b_{r-1}).$$

Now, take any $\lambda_0, \dots, \lambda_{r-1} < \kappa$ and choose any $\mathbf{b} \in B^\kappa$ such that $\mathbf{b}(\lambda_i) = b_i$ for each $i < r$. Observe that

$$\begin{aligned} t^{\mathbf{F}}(\pi_{\lambda_0}, \dots, \pi_{\lambda_{r-1}})(\mathbf{b}) &= t^{\mathbf{B}}(\pi_{\lambda_0}(\mathbf{b}), \dots, \pi_{\lambda_{r-1}}(\mathbf{b})) \\ &= t^{\mathbf{B}}(b_0, \dots, b_{r-1}) \\ &\neq s^{\mathbf{B}}(b_0, \dots, b_{r-1}) \\ &= s^{\mathbf{B}}(\pi_{\lambda_0}(\mathbf{b}), \dots, \pi_{\lambda_{r-1}}(\mathbf{b})) \\ &= s^{\mathbf{F}}(\pi_{\lambda_0}, \dots, \pi_{\lambda_{r-1}})(\mathbf{b}). \end{aligned}$$

We thus have that $t^{\mathbf{F}}(\pi_{\lambda_0}, \dots, \pi_{\lambda_{r-1}}) \neq s^{\mathbf{F}}(\pi_{\lambda_0}, \dots, \pi_{\lambda_{r-1}})$, and hence $\mathbf{F} \not\models t \approx s$, as claimed.

Now, let $\mathbf{A}$ be any algebra in $\mathcal{V}$ that is generated by κ of its elements, say $\{a_\lambda \mid \lambda < \kappa\}$. Let $h_0 : \{\pi_\lambda \mid \lambda < \kappa\} \to \{a_\lambda \mid \lambda < \kappa\}$ be the map defined by $h_0(\pi_\lambda) = a_\lambda$ for each $\lambda < \kappa$. Let $t \approx s$ be any equation that holds in $\mathbf{F}$. As we have just seen, this implies that $\mathbf{B} \models t \approx s$. But, by construction, this entails also that $\mathbf{A} \models t \approx s$: After all, if $\mathbf{A} \not\models t \approx s$, then $t \approx s$ fails in $\mathcal{V}$ and hence in $\mathbf{B}$. Thus, we can define a map h from F onto A as follows. For t, any term for $\mathcal{V}$ of rank, say r, and $\lambda_0, \dots, \lambda_{r-1} < \kappa$, let

$$h(t^{\mathbf{F}}(\pi_{\lambda_0}, \dots, \pi_{\lambda_{r-1}}) = t^{\mathbf{A}}(a_{\lambda_0}, \dots, a_{\lambda_{r-1}}).$$

It is not hard to see that this map is both onto and a homomorphism (and, as we have just established, it also well-defined).

Any κ-generated algebra $\mathbf{F} \in \mathcal{V}$ with the property just demonstrated—namely that any map from its set of generators onto the cardinality-κ generating set of any other algebra in $\mathcal{V}$ extends to a homomorphism—is called a *freely κ-generated algebra for $\mathcal{V}$*. Now, it is clear that any two such algebras will be isomorphic, and so we typically use the definite article in this case—and it is convenient to think of the construction just given as the canonical representative. Indeed, the choices made for each $\mathbf{A}_\varphi \in \mathcal{V}$ with $\varphi \in \Phi$ are immaterial in the sense that any choice will result in an isomorphic copy of that constructed through another choice. We shall denote "this" algebra, then, by $\mathbf{F}_\mathcal{V}(\kappa)$. For an arbitrary set Λ and the algebra $\mathbf{B}$ given above, we write $\mathbf{F}_\mathcal{V}(\Lambda) = \mathbf{Clo}_\Lambda\mathbf{B}$, again noting that this definition is sound, modulo isomorphism.

As a special case, consider $\mathcal{V} = \operatorname{Var}\mathbf{B}$, the variety generated by some given algebra $\mathbf{B}$. Again, $\mathbf{B}$ has the property that for any equation φ in the language of $\mathcal{V}$ and any algebra $\mathbf{A} \in \mathcal{V}$, we have that $\mathbf{B} \models \varphi$ entails that $\mathbf{A} \models \varphi$. Thus, we have that $\mathbf{Clo}_\kappa\mathbf{B}$ is, as it was above, freely generated for $\mathcal{V}$. Now, since $\mathbf{Clo}_\kappa\mathbf{B}$ is a subalgebra of $\mathbf{B}^{B^\kappa}$ and every κ-generated algebra $\mathbf{A}$ in $\mathcal{V}$ is a homomorphic image of $\mathbf{Clo}_\kappa\mathbf{B}$, we have that $|A| \leq |B|^{|B|^\kappa}$. In particular, if κ is a natural number and B is finite, we find that A must be finite also. Thus, we see that in any variety that is generated by a finite algebra—or, which is equivalent, generated by finitely many finite algebras—each of its finitely generated algebras is finite. Any variety with this last property—that is, so that each of its finitely generated algebras is finite—is called *locally finite*.

There is an important, generic finite basis result for certain locally finite varieties—namely, those that are defined by the n-variables laws that hold in a given variety, where n is a natural number. Let $\mathcal{V}$ be any variety. Let n be a natural number. Let Σ_n be the set of equations that hold in $\mathcal{V}$ involving terms of rank at most n. Let $\mathcal{V}^{(n)} = \operatorname{Mod}\Sigma_n$. The following was found by Birkhoff; it has been used in a majority of finite basis results since.

Theorem A.3. *For any natural number n and for any variety $\mathcal{V}$ of finite signature such that $F_{\mathcal{V}}(n)$ is finite, $\mathcal{V}^{(n)}$ is finitely based. In particular, if $\mathcal{V}$ is locally finite and of finite signature, then $\mathcal{V}^{(n)}$ is finitely based for all natural numbers, n, and, furthermore, $\mathcal{V}$ is thereby finitely based if and only if, for some n, $\mathcal{V} = \mathcal{V}^{(n)}$.*

Let S and I be any sets, and let $\Phi = \langle \phi_i \mid i \in I \rangle$ be a system of maps each with S as its domain and, for each $i \in I$ some codomain S_i. We say that Φ *separates points* provided for each $a, b \in S$ such that $a \neq b$, we have some $\phi \in \Phi$ such that $\phi(a) \neq \phi(b)$. The point of this concept is that it provides us with an injection of S into $P := \Pi_{i \in I} S_i$, namely, the natural map defined for $s \in S$ by $s \mapsto \langle \phi_i(s) \mid i \in I \rangle$.

Let $\mathbf{A}$ be any algebra. Let $I = \{\{a, b\} \subseteq A \mid a \neq b\}$. For each $i = \{a, b\} \in I$, using Zorn's Lemma, it is not difficult to lay our hands on a maximal congruence θ_i such that $\langle a, b \rangle \notin \theta$. For each $i \in I$, let ϕ_i be the natural quotient map of $\mathbf{A}$ onto A/θ_i. It is evident that $\Phi = \langle \phi_i \mid i \in I \rangle$ separates points. It is also not hard to see that the map from A into $\Pi_{i \in I} A/\theta_i$ given, for any $a \in A$, by $a \mapsto \langle a/\theta_i \mid i \in I \rangle$ is a homomorphism. Let ϕ stand for this homomorphism. As noted in Theorem A.1, given similar algebras $\mathbf{A}$ and $\mathbf{B}$ and homomorphism $h : \mathbf{A} \to \mathbf{B}$, that $\operatorname{im} h$, the image of A under h, is a subalgebra of $\mathbf{B}$ that is also isomorphic to $\mathbf{A}$. It thus follows from the work above that any algebra $\mathbf{A}$ is isomorphic to a subalgebra $\mathbf{C}$ of a direct product of quotients of $\mathbf{A}$. Furthermore, it is easy to see that this subalgebra has the property that the restriction of any of the projection maps to $\mathbf{C}$ is onto. We call any subalgebra $\mathbf{C}$ of a direct product $\mathbf{D}$ with this latter property a *subdirect product.* To indicate that a given algebra $\mathbf{A}$ is isomorphic to a subdirect product, as in the above, we shall write, for example,

$$\mathbf{A} \hookrightarrow_{\mathrm{sd}} \Pi_{i \in I} \mathbf{A}/\theta_i.$$

Note, also, that, for a given algebra $\mathbf{A}$, for any set $\{\theta_i \mid i \in I\} \subseteq \operatorname{Con} \mathbf{A}$, and for $\theta = \bigcap_{i \in I} \theta_i$, we have that $\mathbf{A}/\theta \hookrightarrow_{\mathrm{sd}} \Pi_{i \in I} \mathbf{A}/\theta_i$.

When $\mathbf{A}$, $\{\theta_i \mid i \in I\}$, and ϕ are given as above, we say that the image of ϕ is a *subdirect representation of* $\mathbf{A}$. This construction was first given by Birkhoff (1944) and is now called Birkhoff's Subdirect Representation Theorem. Note, however, that, for a given $i = \{a, b\} \in I$, there is no reason why we might not have that the equality relation (denoted '=,' of course) on $\mathbf{A}$—that is, the set of all identical pairs from A—is a maximal congruence with respect to the property that $\langle a, b\rangle \notin =$. Note that, then, for any $\theta \in \operatorname{Con}\mathbf{A}$ different from =, we have that $\langle a, b\rangle \in \theta$. We shall call a pair $\langle a, b\rangle \in A^2$ with this property *monolithic for* $\mathbf{A}$ or, simply, *monolithic*; we shall also refer to $\operatorname{Cg}^{\mathbf{A}}\langle a, b\rangle$ as the *monolith of* $\operatorname{Con}\mathbf{A}$, whenever $\langle a, b\rangle$ is monolithic, that is. Thus, when $\operatorname{Con}\mathbf{A}$ has a monolith, the subdirect representation of $\mathbf{A}$ is a trivial thing: $\mathbf{A}$ is one of the factors of the direct product into which we obtain an injection of $\mathbf{A}$. As a result, we call algebras with this property—that is, with a monolithic pair—*subdirectly irreducible.*

For a given class of similar algebras $\mathcal{K}$, let $\operatorname{Sd}\mathcal{K}$ denote the subdirectly irreducible quotients of elements of $\mathcal{K}$. As a direct consequence of Birkhoff's Subdirect Representation Theorem we get the following.

Theorem A.4. *Let $\mathcal{V}$ be any variety. Then $\operatorname{Var}\operatorname{Sd}\mathcal{V} = \mathcal{V}$. In particular, if $\mathcal{W}$ is any variety, then $\mathcal{V} = \mathcal{W}$ if and only if $\operatorname{Sd}\mathcal{V} = \operatorname{Sd}\mathcal{W}$—that is, if and only if they have the same subdirectly irreducible members.*

A.2 Some general strategies of proof for finite basis results

Oates and Powell established in 1964 that all finite groups have a finitely based equational theory. Later, it was found that the same holds for finite rings through the use of a similar argument to that found in the Oates-Powell paper. However, their strategy does not seem to have been used much since. We have sought to remedy that by establishing several results for Mal'cev varieties of nilpotent algebras that parallel those instrumental in the Oates-Powell result. Interestingly, much of the underlying mechanics of their proof owes to work of Graham Higman (1959), which he developed to reprove a result of Lyndon (1952): Every nilpotent group has a finitely based equational theory. See Neumann (1967) for an exposition of Higman's work as well as that of Oates and Powell.

There is another proof-technique for getting finite basis results, which has been used more recently, namely that of establishing that, for a given variety $\mathcal{V}$ and some (sufficiently large) natural number N, the set of subdirectly irreducibles in $\mathcal{V}^{(N)}$ is precisely the same as the set of subdirectly irreducibles in $\mathcal{V}$. By Birkhoff's Subdirect Representation Theorem, any variety is determined by its subdirectly irreducible members. Thus, this is evidently sufficient to get a finite basis result, provided $\mathcal{V}$ is locally finite and has a finite signature, in light of Birkhoff's other work that showed how to find a finite basis for the N-variable laws of any such variety. Any variety that has this property is said to have a *finite residual bound.* Some who have used the technique—such as McKenzie (1987a), Willard (2000), and Kearnes, Szendrei, and Willard (2013+)—have actually added a finite residual bound as an hypothesis. However, as has been observed before, it is not a necessary hypothesis. It is well known that the 8-element quaternion group $\mathbf{Q}$, generates a variety without a finite residual bound. On the other hand, it is indeed finitely based—or "doubly so," to hyperbolize—as can be seen from Lyndon (1952), as $\mathbf{Q}$ forms a group of nilpotence class 2, as well as from Oates and Powell (1964), since they are finite. We have sought to study whether the results of Lyndon and Oates and Powell generalize further than is currently known.

The key fact used in the Oates-Powell result is that any locally finite variety of algebras, say $\mathcal{V}$, is determined by a certain subclass of algebras, the class of all critical algebras in the variety, which we soon define. Let $\mathbf{A}$ be an algebra. We shall say that any element $\mathbf{B}$ of $HS\mathbf{A}$ is a *proper factor of* $\mathbf{A}$ provided its cardinality is strictly less than that of A, while $\mathbf{A}$ is called *critical* provided it is not found in the variety generated by its proper factors.[1] Equivalently, $\mathbf{A}$ is critical if and only if there is an equation φ in the signature of $\mathbf{A}$ so that $\mathbf{A} \not\models \varphi$ and yet, if $\mathbf{B}$ is any proper factor of $\mathbf{A}$, $\mathbf{B} \models \varphi$. Suppose also that $\varphi = s \approx t$ is an equation in the variables $x_0, \ldots, x_{n-1}$. Let $\langle x_0, \ldots, x_{n-1} \rangle \mapsto \langle a_0, \ldots, a_{n-1} \rangle$ be an assignment that witnesses the failure of φ in $\mathbf{A}$. Then, evidently, $\mathbf{A}$ is generated by $S = \{a_0, \ldots, a_{n-1}\}$: after all, by assumption, $\mathrm{Sg}^{\mathbf{A}} S$ is not a proper factor of $\mathbf{A}$. Thus, if $\mathbf{A}$ is critical and lies in a locally finite variety, then $\mathbf{A}$ is finite.

For any class $\mathcal{K}$ of algebras, let $\operatorname{Crit} \mathcal{K}$ be the class of critical factors of algebras in $\mathcal{K}$. For $\mathcal{K} = \{\mathbf{A}\}$, write $\operatorname{Crit} \mathcal{K} =: \operatorname{Crit} \mathbf{A}$.

As mentioned above, we have the following.

Theorem A.5. *Let $\mathcal{V}$ be a locally finite variety. Then $\mathcal{V} = \operatorname{Var} \operatorname{Crit} \mathcal{V}$. Moreover, every nontrivial algebra in $\mathcal{V}$ is contained in the variety generated by its critical factors.*

Proof. Let $\mathbf{A} \in \mathcal{V}$. Let φ be an equation in the signature of $\mathcal{V}$ that fails in $\mathbf{A}$ (hence, we have tacitly assumed that $\mathbf{A}$ is nontrivial). Since this failure involves a finite witness, and $\mathcal{V}$ is locally finite, we may obtain a finite subalgebra $\mathbf{B}$ of $\mathbf{A}$ in which φ fails. Since B is finite, we can also find a minimal, proper factor $\mathbf{C}$ of $\mathbf{B}$—and hence of $\mathbf{A}$—in which φ fails. Evidently, $\mathbf{C}$ is critical, since, if $\mathbf{D}$ is any proper factor of $\mathbf{C}$, φ is satisfied in $\mathbf{D}$, by the minimality of $\mathbf{C}$. Set $\mathbf{C}_\varphi := \mathbf{C}$.

Now, let $\Phi = \{\varphi \mid \mathbf{A} \not\models \varphi\}$, and consider $\mathbf{A}' := \Pi_\Phi \mathbf{C}_\varphi$. We claim that $\mathbf{A}$ is in the variety generated by $\mathbf{A}'$. After all, if $\mathbf{A}' \models \varphi$, then we must have that $\mathbf{A} \models \varphi$: Otherwise, we would have $\varphi \in \Phi$ and hence $\mathbf{C}_\varphi \not\models \varphi$ whence $\mathbf{A}' \not\models \varphi$, contrary to our assumption. We thus see that $\mathbf{A}$ is in the variety generated by its critical factors.

The first part of the theorem then easily follows. □

[1] This is not always how such is defined: In Neumann (1967) and MacDonald and Vaughan-Lee (1978), critical algebras are defined to be finite.

This fact provides an interesting strategy for demonstrating that a given locally finite variety has a finite basis. Recall that for a given variety $\mathcal{V}$ and natural number N, $\mathcal{V}^{(N)}$ is defined to be the variety based on the N-variable equations true in $\mathcal{V}$. Recall also that Birkhoff showed how to find a finite basis for $\mathcal{V}^{(N)}$, provided $\mathcal{V}$ has a finite signature and $F_{\mathcal{V}}(N)$ is finite, which, for instance, occurs whenever $\mathcal{V}$ is locally finite. It turns out, by the following theorem, that $\mathcal{V}$ will inherit the finite basis property for $\mathcal{V}^{(N)}$ provided $\mathcal{V}^{(N)}$ is locally finite and has, up to isomorphism, only finitely many critical algebras. Note also that, in the presence of a finite signature, this last property is equivalent to a finite bound on the cardinality of the critical algebras; this last property is styled "having a *finite critical bound*." Any variety that is finitely based, locally finite, and has, up to isomorphism, only finitely many critical algebras is called a *Cross variety*.

Theorem A.6. *Every subvariety of a Cross variety is also a Cross variety.*

Proof. Let $\mathcal{V}$ be a Cross variety, and let $\mathcal{W}$ be a proper subvariety of $\mathcal{V}$. Let Σ be a finite basis for $\mathcal{V}$.

It is clear that $\mathcal{W}$ is both locally finite and has a finite critical bound. What we need to show is that $\mathcal{W}$ is finitely based. Now, by Theorem A.5, we have that $\operatorname{Crit}\mathcal{W}$ must be a proper subclass of $\operatorname{Crit}\mathcal{V}$. Let f be a choice function for the set of isomorphism classes of $\operatorname{Crit}\mathcal{V}$: for a given $\mathbf{C} \in \operatorname{Crit}\mathcal{V}$, we set $f(\mathbf{C})$ to be the uniquely chosen representative of the isomorphism class of $\mathbf{C}$. Now, let $\mathcal{C} = \{f(\mathbf{C}) \in \operatorname{Crit}\mathcal{V} \mid \mathbf{C} \notin \mathcal{W}\}$. Note that $\mathcal{C}$ is a finite set. Now, for each $\mathbf{C} \in \mathcal{C}$, we can find an equation $\varphi = \varphi_{\mathbf{C}}$ so that $\mathbf{C} \not\models \varphi$, while $\mathcal{W} \models \varphi$. Let $\Phi = \{\varphi_{\mathbf{C}} \mid \mathbf{C} \in \mathcal{C}\}$, noting that Φ is finite.

Note that $\mathcal{W} \subseteq \operatorname{Mod}\Sigma \cup \Phi$. We claim further that $\operatorname{Mod}\Sigma \cup \Phi \subseteq \mathcal{W}$. Let $\mathbf{A} \in \operatorname{Mod}\Sigma \cup \Phi$. Clearly, $\mathbf{A} \in \mathcal{V}$. By Theorem A.5, $\mathbf{A} \in \operatorname{Var}\operatorname{Crit}\mathbf{A}$. Note that $\operatorname{Crit}\mathbf{A} \models \Sigma \cup \Phi$. Thus, $\operatorname{Crit}\mathbf{A} \subseteq \operatorname{Crit}\mathcal{W}$: After all, for $\mathbf{C}' \in \operatorname{Crit}\mathcal{V} \setminus \operatorname{Crit}\mathcal{W}$, there is an equation $\varphi = \varphi_{f(\mathbf{C}')} \in \Phi$ such that $\mathbf{C}' \not\models \varphi$, which entails that $\mathbf{C}' \not\models \Phi$. It follows that $\mathbf{A} \in \mathcal{W}$, as we claimed. Thus, $\mathcal{W} = \operatorname{Mod} \Sigma \cup \Phi$, which demonstrates that $\mathcal{W}$ is finitely based. □

It follows that, in order to show that a given variety $\mathcal{V}$ is finitely based, it is sufficient to show that $\mathcal{V}^{(N)}$ is a Cross variety, for some natural number N. If $\mathcal{V}$ is locally finite and of finite signature, using Birkhoff's finite basis for $\mathcal{V}^{(N)}$, available under these conditions, we find that we need only show that $\mathcal{V}^{(N)}$ is locally finite and has a finite critical bound for all high enough N. We present some results relevant to this strategy in Chapter 3.

A.3 On congruences, the commutator, and related concepts

We shall often be concerned below with lattices and mainly with congruence lattices. It may be helpful to formalize what we mean here, as well as establish some useful notation.

Definition A.7. By a *lattice*, $\mathbf{L}$, we mean an algebra with a signature that provides two binary operations, symbolized by $\wedge$ and $\vee$, referred to as "meet" and "join," respectively. Furthermore, we require that $\wedge$ and $\vee$ are idempotent, commutative, and associative operations. We also require that $\mathbf{L}$ satisfy the equations $(x \wedge y) \vee y \approx y$ and $x \wedge (x \vee y) \approx x$

We can also give any lattice $\mathbf{L}$ a partial order $\leq$ by letting, for $x, y \in L$, $x \leq y$ if and only if $x \wedge y = x$. One can also deduce that $x \leq y$ if and only if $x \vee y = y$. Furthermore, $\wedge$ and $\vee$ represent "greatest lower bound" and "least upper bound" relations, respectively. That is, for instance, for any $x, y \in L$, we have that $x \leq x \vee y$ and $y \leq x \vee y$, while if $z \in L$ with $x \leq z$ and $y \leq z$, then $x \vee y \leq z$.

Let L be any set equipped with a partial order $\leq$ (such as a lattice), and let $x \leq z \in L$. We set $I[x, z] = \{y \in L \mid x \leq y \leq z\}$. Also, suppose that, for any $y \in L$

such that $x \leq y \leq z$, we have that $y \in \{x, z\}$. Then we write $x \prec z$ and say that z *covers* x. We shall call any pair $\langle \alpha, \beta \rangle$ of congruences with $\alpha \leq \beta$ a *quotient*.

Recall from above that the set of all congruences on a given algebra $\mathbf{A}$ can be given a lattice structure, with the order simply that of set inclusion, and that, furthermore, the greatest lower bound of any set of congruences can be found (and, therefore, the least upper bound of any set of congruences on $\mathbf{A}$ can be found as well). Let $\mathbf{A}$ be an algebra, with set of congruences $\operatorname{Con} \mathbf{A}$. We shall denote by 0_A, the least element of $\operatorname{Con} \mathbf{A}$ (that is, the greatest lower bound of the set of all its congruences), namely

$$0_A = \{\langle a, a \rangle \mid a \in A\},$$

often called the diagonal. We shall denote by 1_A the top element of $\operatorname{Con} \mathbf{A}$, that is, A^2. We shall use '$\cap$' for the meet-operation on $\operatorname{Con} \mathbf{A}$, since it is, after all, simply the intersection. For $\mathcal{C} \subseteq \operatorname{Con} \mathbf{A}$, we have that $\vee \mathcal{C} = \bigcap \{\theta \in \operatorname{Con} \mathbf{A} \mid \cup \mathcal{C} \subseteq \theta\}$. For $\mathcal{C} = \{\alpha, \beta\} \subseteq \operatorname{Con} \mathbf{A}$, we shall write $\vee \mathcal{C} = \alpha \vee \beta$.

Recall the notion of congruence generation, which was defined in the first chapter: given an algebra $\mathbf{A}$ and a set of pairs $X \subseteq A^2$, we can find the least congruence containing X; we denote it $\operatorname{Cg}^{\mathbf{A}} X$. For $X = \{\langle a, b \rangle\}$, we write $\operatorname{Cg}^{\mathbf{A}} X = \operatorname{Cg}^{\mathbf{A}} \langle a, b \rangle$. In common with perhaps all mathematical concepts of "generation," there is also a constructive notion of congruence generation. Mal'cev gave a useful description of $\operatorname{Cg}^{\mathbf{A}} X$ of this kind. Before we give it, we need one further technical concept.

Definition A.8. Let $\mathbf{A}$ be an algebra. We shall define the set of *translations* on $\mathbf{A}$ as a set of unary polynomials of a special type. First, we define the notion of basic translation. Let f be a fundamental operation symbol with given arity, say, r. Then for any $i < r$, we say that $\lambda \in \operatorname{Pol}_1 \mathbf{A}$ is a basic translation when $\lambda(x) = f^{\mathbf{A}}(a_0, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_{r-1})$ (with x in the i^{th} position), where $a_0, \ldots, a_{i-1}, a_{i+1}, \ldots, a_{r-1} \in A$. Too, we say that the identity is a basic translation.

We define the set of translations to be the least set of unary polynomials containing the basic translations and closed under composition.

It is easy to see that this definition is sound and that the set of translations can be recursively or constructively described as well.

Proposition A.9. *(Mal'cev (1954): Congruence generation) Let* $\mathbf{A}$ *be any algebra. Let* $X \subseteq A^2$*. Let* θ *be the set of pairs* $\langle a, b\rangle \in A^2$ *for which there exists a natural number* ℓ*, pairs* $\langle a_i, b_i\rangle \in X$ *and translations* λ_i *on* $\mathbf{A}$ *for* $i \leq \ell$ *so that*

- $\lambda_0(a_0) = a$ *and* $\lambda_\ell(b_\ell) = b$ *and*
- $\lambda_i(b_i) = \lambda_{i+1}(a_i)$ *for* $i < \ell$*.*

Then $\theta = \operatorname{Cg}^{\mathbf{A}} X$*.*

We call this arrangement of pairs and translations—the witness of $\langle a, b\rangle \in \operatorname{Cg} X$— a *Mal'cev chain.* It is convenient to formalize such as a pair of tuples, say $\mathcal{C}$, as in

$$\mathcal{C} = \langle\langle\langle a_i, b_i\rangle \mid i \leq \ell\rangle, \langle\lambda_i \mid i \leq \ell\rangle\rangle,$$

for given natural number ℓ; we call $\ell + 1$ the *length of* $\mathcal{C}$.

We shall need the following further fact of an elementary nature concerning congruence generation. In the following, and throughout this text, for any sets A and B and any map $h : A \to B$, any set I, any $X \subseteq A^I$, and any $\mathbf{a} = \langle a_i \mid i \in I\rangle \in X$, we shall abuse notation by writing $h(\mathbf{a}) = \langle h(a_i) \mid i \in I\rangle$ and $h(X) = \{h(\mathbf{a}) \mid \mathbf{a} \in X\}$.

Proposition A.10. *Let* $\mathbf{A}$ *and* $\mathbf{B}$ *be algebras, and let* h *be a homomorphism of* $\mathbf{A}$ *into* $\mathbf{B}$*. Let* θ *be a congruence on* $\mathbf{A}$*, generated by some set* X *of pairs from* A*. Let* $\psi \in \operatorname{Con} \mathbf{B}$ *be generated by* Y*, a set of pairs from* B*. If* $h(X) \subseteq Y$*, then* $h(\theta) \subseteq \psi$*. If, furthermore,* h *is onto and* $\ker h \subseteq \theta$*, then* $Y \subseteq h(X)$ *implies that* $\psi \subseteq h(\theta)$*. In particular, if* h *is onto,* $\ker h \subseteq \theta$*, and* h *maps* X *onto* Y*, then* $h(\theta) = \psi$*.*

Proof. First, suppose that $h(X) \subseteq Y$, and let $\langle b, b' \rangle \in h(\theta)$. Then we can write $\langle b, b' \rangle = \langle h(a), h(a') \rangle$ for some $\langle a, a' \rangle \in \theta$. As $\theta = \mathrm{Cg}^{\mathbf{A}} X$, we obtain a Mal'cev chain of some length $\ell + 1$ witnessing this:

$$\langle \langle \langle x_i, y_i \rangle \mid i \leq \ell \rangle, \langle \lambda_i \mid i \leq \ell \rangle \rangle;$$

that is, we get pairs $\langle x_i, y_i \rangle \in X$ and translations on $\mathbf{A}$, $\lambda_i(x) = t_i^{\mathbf{A}}(x, \mathbf{c}_i)$, for $i \leq \ell$, such that $a = t_0^{\mathbf{A}}(x_0, \mathbf{c}_0)$, $a' = t_\ell^{\mathbf{A}}(y_\ell, \mathbf{c}_\ell)$, and $t_i^{\mathbf{A}}(y_i, \mathbf{c}_i) = t_{i+1}^{\mathbf{A}}(x_{i+1}, \mathbf{c}_{i+1})$ for all $i < \ell$. It is easy to check, then, that the Mal'cev chain

$$\langle \langle \langle h(x_i), h(y_i) \rangle \mid i \leq \ell \rangle, \langle \lambda'_i \mid i \leq \ell \rangle \rangle$$

witness that $\langle b, b' \rangle \in \psi$, where $\lambda'_i(x) = t_i^{\mathbf{B}}(x, h(\mathbf{c}_i))$ for each $i \leq \ell$. Thus, $h(X) \subseteq Y$ implies that $h(\theta) \subseteq \psi$.

Now, assume that h is onto and that $\ker h \subseteq \theta$. Suppose that $Y \subseteq h(X)$. Let $\langle b, b' \rangle \in \psi$, and take a Mal'cev chain witnessing this, say,

$$\langle \langle \langle x'_i, y'_i \rangle \mid i \leq \ell \rangle, \langle \lambda'_i \mid i \leq \ell \rangle \rangle,$$

where $\lambda'_i(x) = t_i^{\mathbf{B}}(x, \mathbf{c}'_i)$, $\langle x'_i, y'_i \rangle \in Y$ for each $i \leq \ell$, and $\langle b, b' \rangle = \langle t_0^{\mathbf{B}}(x'_0, \mathbf{c}'_0), \rangle t_\ell^{\mathbf{B}}(y'_\ell, \mathbf{c}'_\ell)$. Using that h is onto, get $\mathbf{c}_i$ such that $h(\mathbf{c}_i) = \mathbf{c}'_i$ for each $i \leq \ell$. Using that $Y \subseteq h(X)$, get $\langle x_i, y_i \rangle \in X$ so that $\langle h(x_i), h(y_i) \rangle = \langle x'_i, y'_i \rangle$ for each $i \leq \ell$. Let $\langle a, a' \rangle = \langle t_0^{\mathbf{A}}(x_0, \mathbf{c}_0), t_\ell^{\mathbf{A}}(y_\ell, \mathbf{c}_\ell) \rangle$. Using that h is a homomorphism, we have that, for each $i < \ell$,

$$\langle t_i^{\mathbf{A}}(y_i, \mathbf{c}_i), t_{i+1}^{\mathbf{A}}(x_{i+1}, \mathbf{c}_{i+1}) \rangle \in \ker h \subseteq \theta,$$

while, clearly, for each $i \leq \ell$, $t_i^{\mathbf{A}}(x_i, \mathbf{c}_i) \; \theta \; t_i^{\mathbf{A}}(y_i, \mathbf{c}_i)$. Thus, $\langle a, a' \rangle \in \theta$. The second claim now follows. $\square$

Generation of subalgebras is even simpler to characterize than generation of congruences. (After all, congruence generation is a case of subalgebra generation, with added constraints.) Again, we have that the intersection of any nonempty collection of subalgebras on a given algebra $\mathbf{A}$ is again a subalgebra. Thus, we have the following.

Proposition A.11. *Let* $\mathbf{A}$ *be any algebra. Let* $X \subseteq A$. *Then* $\mathrm{Sg}^{\mathbf{A}} X$ *is precisely the set of elements* $t^{\mathbf{A}}(x_0, \ldots, x_{r-1})$ *where* t *is a term of rank, say,* r, *and* $x_i \in X$ *for* $i < r$.

Definition A.12. For any algebra $\mathbf{A}$, any binary relation θ on $\mathbf{A}$, and any subset B of A, we set

$$B\theta = \{a \in A \mid b\,\theta\,a \text{ for some } b \in B\}.$$

We shall call $B\theta$ the *expansion of* B *by* θ.

Now, note that if θ is a congruence on a given algebra $\mathbf{A}$, and $B \subseteq A$, then $B\theta$ is a union of θ-classes, namely, those that intersect B. As such, one can sensibly define the symbol $(B\theta)/\theta$ to mean the set of θ-classes contained in $B\theta$.

Before considering the next theorem, note also the following.

Proposition A.13. *Let* $\mathbf{A}$ *be any algebra. Let* $\mathbf{B}$ *be a subalgebra of* $\mathbf{A}$ *and let* θ *be a congruence of* $\mathbf{A}$. *Then* $\theta \cap B^2$ *is a congruence of* $\mathbf{B}$. *We shall denote it by* $\theta\restriction_{\mathbf{B}}$.

Theorem A.14. *(Second isomorphism theorem, and companion results) Let* $\mathbf{A}$ *be an algebra with subalgebra* $\mathbf{B}$. *Then* $B\theta$ *is closed under the operations of* $\mathbf{A}$, $(B\theta)/\theta$ *is closed under the operations of* $\mathbf{A}/\theta$, *and* $(\mathbf{B}\theta)/\theta \cong \mathbf{B}/(\theta \cap B^2)$.

The following notation and elementary fact will be used in the next two theorems. For any algebra $\mathbf{A}$ and any congruences $\delta \leq \theta$, we have that

$$\theta/\delta := \{\langle a/\delta, b/\delta\rangle \mid a\,\theta\,b\}$$

is a congruence on $\mathbf{A}/\delta$.

Theorem A.15. *(Third isomorphism theorem) Let* $\mathbf{A}$ *be an algebra with congruences* $\delta \leq \theta$. *Then* $(\mathbf{A}/\delta)/(\theta/\delta) \cong \mathbf{A}/\theta$.

Theorem A.16. *(Correspondence theorem) Let* $\mathbf{A}$ *be an algebra, and take any congruence* δ *on* $\mathbf{A}$*. Then the map from* $I[\delta, 1_A]$ *into* $I[0_{A/\delta}, 1_{A/\delta}]$ *given by* $\theta \mapsto \theta/\delta$ *is a lattice isomorphism.*

We shall also occasionally make use of the following concept.

Definition A.17. For a given algebra $\mathbf{A}$ and subset B of A, we say that B is normal provided it is a class of some congruence on $\mathbf{A}$. In particular, then, $B = b/\operatorname{Cg}^{\mathbf{A}} B^2$, for any $b \in B$.

There is another description of the join of congruences we shall give, which involves the following binary operation for binary relations.

Definition A.18. Given two binary relations, R and S on some set A, we let their composition, denoted $R \circ S$ be the set $\{\langle x, y\rangle \mid x\, R\, u\, S\, y, \text{ for some } u \in A\}$.

For a given binary relation R and for each $n > 0$, we shall define R^n recursively by $R^1 := 1$ and $R^{n-1} \circ R$. (Note that this composition operation is associative, as well.)

Proposition A.19. *Let* $\mathbf{A}$ *be an algebra, and let* $\alpha, \beta \in \operatorname{Con} \mathbf{A}$*. Let* $\gamma := \alpha \circ \beta$*. Then* $\alpha \vee \beta = \bigcup_{n>0} \gamma^n$*.*

This description sometimes simplifies, as it does in the following situation.

Definition A.20. Let $\mathbf{A}$ be an algebra. We say that $\mathbf{A}$ is *congruence permutable* provided $\alpha \circ \beta = \beta \circ \alpha$ for all $\alpha, \beta \in \operatorname{Con} \mathbf{A}$. Any class $\mathcal{V}$ such that $\mathbf{A} \in \mathcal{V}$ is congruence permutable for all $\mathbf{A} \in \mathcal{V}$ is also called congruence permutable.

It is not hard to see that if $\mathbf{A}$ is congruence permutable, then for any $\alpha, \beta \in \operatorname{Con} \mathbf{A}$, $\alpha \vee \beta = \alpha \circ \beta$.

It turns out that many familiar classes of algebras are congruence permutable: groups, rings, modules and vector spaces, as are every sort of algebra which has one of these as a reduct (meaning, in the event that some of the structure is ignored), such as Lie algebras and various sorts of structures commonly referred to as "algebras" (meant in the narrow sense) in the literature. As a less common example, quasigroups are also congruence permutable. A *simple algebra* $\mathbf{A}$ is one which has no nontrivial congruences: that is, besides those that are always available, namely 0_A and 1_A. Thus, it is easy to see that all simple algebras are congruence permutable. On the other hand, there are numerous algebras that are not congruence permutable: lattices are not, in general, congruence permutable, nor are semilattices or semigroups.

For all variety $\mathcal{V}$ that are found to be congruence permutable, there is an interesting characterization, given by Mal'cev (1954):

Theorem A.21. *Let $\mathcal{V}$ be a variety. Then $\mathcal{V}$ is congruence permutable if and only if there is a ternary term p for $\mathcal{V}$ such that*

$$\mathcal{V} \models p(x, y, y) \approx x \approx p(y, y, x).$$

A congruence permutable variety is thus often referred to as *Mal'cev*; occasionally we shall also refer an algebra in a congruence permutable variety as Mal'cev, as well. This result of Mal'cev has been imitated in many ways: When various lattice theoretic equations hold in the congruence lattices of algebras across a given variety, this often implies and is implied by the presence of a set of terms, which are given to satisfy certain equations. Results of this type are called *Mal'cev conditions.* There are two generalizations of congruence permutability, important to the present thesis, that have been characterized in this way. The first of these we shall now define by a sentence in the language of lattices; the second is usually defined in terms of the commutator, and so we leave it for below.

Definition A.22. Let $\mathbf{L} = \langle L, \wedge, \vee \rangle$ be a lattice with meet operation $\wedge$, join operation $\vee$, and associated order $\leq$. Let $x, y, z \in L$ such that $z \leq x$. We say that $\mathbf{L}$ is modular provided $x \wedge (y \vee z) = (x \wedge y) \vee z$.

Definition A.23. Any algebra whose congruence lattice is modular is said to be *congruence modular*. For any variety $\mathcal{V}$ such that for all $\mathbf{A} \in \mathcal{V}$ we have that $\mathbf{A}$ is congruence modular, we say that $\mathcal{V}$ is congruence modular, as well.

The following can be shown through an elementary argument.

Proposition A.24. *Congruence permutability entails congruence modularity. That is, if $\mathbf{A}$ is an algebra for which $\operatorname{Con} \mathbf{A}$ is congruence permutable, then $\operatorname{Con} \mathbf{A}$ is also congruence modular.*

In Chapter 4, we shall make use of a Mal'cev-type characterization of congruence modular varieties, given by H.P Gumm, but we defer its statement until then.

Mal'cev varieties (that is, congruence permutable varieties) have many nice properties, and it seems that the theory of Mal'cev varieties has much left to be discovered, as well. As a first, consider the following observation.

Proposition A.25. *Let $\mathbf{A}$ be an algebra in a Mal'cev variety. Any reflexive binary relation that respects the operations of $\mathbf{A}$ is a congruence on $\mathbf{A}$.*

In particular, we have that, for any $X \subseteq A \times A$,

$$\operatorname{Cg}^{\mathbf{A}} X = \operatorname{Sg}^{\mathbf{A} \times \mathbf{A}} X \cup 0_A.$$

We shall often make use of the following easy application of Proposition A.25, as it supplies a nice description of congruence generation in Mal'cev varieties.

Proposition A.26. *Let $\mathbf{A}$ be an algebra in a Mal'cev variety. Let $X \subseteq A \times A$. Then*

$$\operatorname{Cg}^{\mathbf{A}} X = \{\langle s(x_0, \ldots, x_{n-1}), s(y_0, \ldots, y_{n-1})\rangle \mid n \in \omega \text{ and } s \in \operatorname{Pol}_n \mathbf{A}\}.$$

A.3.1 A COMMUTATOR

The commutator, which was originally a group theoretic concept, has found its usefulness extended to more general contexts, though with its definition necessarily adapted. A pioneer in this study was J.D.H. Smith, who, in 1976, extended many of the group-theoretic results concerning the commutator to congruence permutable varieties. Subsequently, a rich theory of the commutator for algebras in a congruence modular variety was developed by Hagemann and Herrmann (1979), Gumm (1983), Freese and McKenzie (1987), and others. Much of the strength of their theory has also been extended to more general settings still. We shall define these more general settings, shortly, as we have made some further contributions to this effort.

There have been a number of different perspectives or notions put forward as a generalized "commutator," each specializing to the concept of the same name when applied to groups (interpreted in the right way), but we shall mostly only consider one or two of these. To give the first, we define the so-called "term condition" (see Freese and McKenzie (1987)).

Definition A.27. (The centralizer relation, or, the "term condition") Given some algebra $\mathbf{A}$, we define a ternary relation C over the set of binary relations on A as follows. For any binary relations α, β and γ on $\mathbf{A}$, we say that $C(\alpha, \beta; \gamma)$ holds if and only if for any natural number n; any n-ary term t; and any pairs $\langle x, y\rangle \in \alpha$ and $\langle u_1, v_1\rangle, \ldots, \langle u_{n-1}, v_{n-1}\rangle \in \beta$, the following implications hold:

$$t(x, \mathbf{u}) \,\gamma\, t(x, \mathbf{v})$$

$$\Updownarrow$$

$$t(y, \mathbf{u}) \,\gamma\, t(y, \mathbf{v}).$$

However, we shall only be concerned with α, β, γ congruences of the given algebra $\mathbf{A}$.

We collect here a selection of elementary (meaning they are derivable from the definition) facts about the centralizer relation, which we put to use in this paper.

Proposition A.28. *For any algebra $\mathbf{A}$ and congruences $\alpha' \leq \alpha, \beta' \leq \beta, \gamma, \gamma_i\,(i \in I)$, $\delta \leq \alpha \cap \beta \cap \gamma$:*

(a) $C(\alpha, \beta; \gamma_i)$, *for each* $i \in I$, *implies that* $C\left(\alpha, \beta; \cap\gamma_i\right)$;

(b) $C(\gamma_i, \beta; \alpha)$, *for each* $i \in I$, *implies that* $C(\vee\gamma_i, \beta; \alpha)$;

(c) $C(\alpha, \beta; \gamma)$ *implies that* $C(\alpha', \beta'; \gamma)$;

(d) $C(\alpha, \beta; \alpha \cap \beta)$ *always holds;*

(e) $C(\alpha, \beta; \gamma)$ *holds if and only if* $C(\alpha/\delta, \beta/\delta; \gamma/\delta) holds$;

(f) *and, finally,* $C(\alpha, \beta; 1_A)$, $C(\alpha, \beta; \alpha)$ *and* $C(\alpha, \beta; \beta)$ *always hold.*

Definition A.29. In light of Proposition A.28 (a) and (f), given algebra $\mathbf{A}$ and any congruences α and β, we obtain the least congruence γ so that $C(\alpha, \beta; \gamma)$, referring to it as *the commutator of* α *and* β and denoting it by $[\alpha, \beta]$.

Similarly, we make use of Proposition A.28 (b) to obtain a largest congruence γ so that $C(\gamma, \beta; \alpha)$. We denote this γ by $(\alpha : \beta)$. This is typically called *the annihilator of* β *over* α. In particular, we shall be interested in the case of $\alpha = 0_A$ and $\beta = 1_A$. In this instance, we write $\zeta_{\mathbf{A}} = (0_A : 1_A)$, referring to this as the *center* of $\mathbf{A}$.

Here are two more elementary facts owing to Proposition A.28.

Proposition A.30. *(Monotonicity of commutator) The commutator respects the lattice order in each coordinate. That is, given algebra* $\mathbf{A}$ *and congruences* $\alpha' \leq \alpha$, $\beta' \leq \beta$,

$$[\alpha', \beta'] \leq [\alpha, \beta].$$

Proposition A.31. *The commutator of congruences is included in their intersection. That is, for given algebra* $\mathbf{A}$ *and congruences* α, β *on* $\mathbf{A}$, $[\alpha, \beta] \subseteq \alpha \cap \beta$.

Here is a third, which is superfluous in the context of congruence modular varieties, but sometimes comes to the rescue when one leaves the convenience of that assumption behind; it is easy to prove using Proposition A.28 (b) and Proposition A.30.

Proposition A.32. *(Left semi-distributivity of the commutator) Let* $\mathbf{A}$ *be any algebra. Let* $\alpha_i, \beta, \gamma \in \operatorname{Con}\mathbf{A}$*, for some index set* I*. If* $[\alpha_i, \beta] = \gamma$*, for each* $i \in I$*, then* $[\bigvee_{i\in I} \alpha_i, \beta] = \gamma$*.*

Definition A.33. Let $\mathbf{A}$ be any algebra with $\alpha, \beta, \theta \in \operatorname{Con}\mathbf{A}$. By Proposition A.28 (a) and (f), it is evident that there is a smallest $\gamma \geq \theta$ such that $C(\alpha, \beta; \gamma)$. We denote this by $[\alpha, \beta]_\theta$.

The following is no more difficult to see than the propositions it refers to.

Proposition A.34. *Let* $\mathbf{A}$ *be any algebra with congruence* θ*. Propositions A.30 (monotonicity of the commutator) and A.32 (left semi-distributivity of the commutator) hold with the commutator* $[\cdot, \cdot]$ *replaced by* $[\cdot, \cdot]_\theta$*.*

There is one other elementary fact that we shall make use of concerning the commutator and its interplay with restriction of congruences to a subalgebra. For any algebra $\mathbf{A}$ with subalgebra $\mathbf{B}$ and $\theta \in \operatorname{Con}\mathbf{A}$, let $\theta \restriction_{\mathbf{B}} = \theta \cap B \times B$. One can easily verify, arguing via elements, that $\theta \restriction_{\mathbf{B}}$ is a congruence on $\mathbf{B}$.

Theorem A.35. *Let* $\mathbf{A}$ *be an algebra with subalgebra* $\mathbf{B}$*. Let* $\alpha, \beta \in \operatorname{Con}\mathbf{A}$*. Then*

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

We shall prove a more general result of this kind later (which has not appeared in print anywhere, to the best of my knowledge); however, both this and the general case are immediate from an *a fortiori* argument concerning the centralizer relation.

There is also a useful relational characterization of the commutator, one which is closer in spirit to its original inception by Smith (1976) and to its elaboration by Gumm (1983).

Definition A.36. Given any algebra $\mathbf{A}$ and congruences α, β on $\mathbf{A}$, we define a congruence on $\boldsymbol{\beta}$ by

$$\Delta_\beta^\alpha = \operatorname{Cg}^{\boldsymbol{\beta}}\{\langle\langle x, x\rangle, \langle y, y\rangle\rangle \mid x \,\alpha\, y\}.$$

Proposition A.37. *For a given algebra* $\mathbf{A}$ *and congruences* α, β, *and* γ *on* $\mathbf{A}$, $C(\alpha, \beta; \gamma)$ *if and only if* $\beta \cap \gamma$ *is the union of* Δ^{α}_{β}*-classes. In particular,* $[\alpha, \beta]$ *is the smallest congruence on* $\mathbf{A}$ *that is the union of* Δ^{α}_{β}*-classes.*

Proof. First, suppose that $C(\alpha, \beta; \gamma)$ holds for congruences α, β, γ of some given algebra. Let $\langle a, b\rangle \in \beta \cap \gamma$ and suppose that $\langle\langle a, b\rangle, \langle c, d\rangle\rangle \in \Delta^{\alpha}_{\beta}$. Using Mal'cev's characterization of congruence generation, we get $x_0, \ldots, x_n$ and $y_0, \ldots, y_n$ such that $\langle x_i, y_i\rangle \in \alpha$ for each i and translations $\mu_0, \ldots, \mu_n$ of $\boldsymbol{\beta}$ so that

$$\begin{aligned} \mu_0\langle x_0, x_0\rangle &= \langle a, b\rangle \\ \mu_i\langle y_i, y_i\rangle &= \mu_{i+1}\langle x_{i+1}, x_{i+1}\rangle, (i = 0, \ldots, n-1) \\ \mu_n\langle y_n, y_n\rangle &= \langle c, d\rangle. \end{aligned}$$

For each translation μ_i and any $\langle x, y\rangle \in \beta$, we may write

$$\mu_i\langle x, y\rangle = \langle t_i(x, \mathbf{u^i}), t_i(y, \mathbf{v^i})\rangle,$$

where t_i is a $k_i + 1$-ary term for some natural number k_i, and $u^i_j \,\beta\, v^i_j$ for each $j < k_i$. In particular, it is immediate that $\langle c, d\rangle \in \beta$. Furthermore, from $\langle a, b\rangle \in \gamma$, we get that

$$t_0(x_0, \mathbf{u^0}) \,\gamma\, t_0(x_0, \mathbf{v^0}).$$

From $C(\alpha, \beta; \gamma)$ we then get that

$$t_1(x_1, \mathbf{u^1}) = t_0(y_0, \mathbf{u^0}) \,\gamma\, t_0(y_0, \mathbf{v^0}) = t_1(x_1, \mathbf{v^1}).$$

Similarly, by induction, we get that

$$c = t_n(y_n, \mathbf{u^n}) \,\gamma\, t_n(y_n, \mathbf{v^n}) = d.$$

This establishes the forward direction.

Now, suppose that $\beta \cap \gamma$ is a union of Δ^{α}_{β}-classes. Pick an arbitrary term t operation of some rank r for $\mathbf{A}$ and suppose that for some a and some $c_i \,\beta\, d_i, (i < r)$,

$$t(a, \mathbf{c}) \,\gamma\, t(a, \mathbf{d}).$$

Take b such that $\langle a, b\rangle \in \alpha$. Let μ be the translation on β defined by

$$\mu\langle x, y\rangle = \langle t(x, \mathbf{c}), t(y, \mathbf{d})\rangle.$$

By the definition of Δ^{α}_{β}, we then get that

$$\langle\langle t(a, \mathbf{c}), t(a, \mathbf{d})\rangle, \langle t(b, \mathbf{c}), t(b, \mathbf{d})\rangle\rangle = \langle\mu\langle a, a\rangle, \mu\langle b, b\rangle\rangle \in \Delta^{\alpha}_{\beta}.$$

Note that

$$\langle t(a, \mathbf{c}), t(a, \mathbf{d})\rangle \in \beta \cap \gamma.$$

Since $\beta \cap \gamma$ is a union of Δ^{α}_{β}-classes, we then get that

$$\langle t(b, \mathbf{c}), t(b, \mathbf{d})\rangle \in \beta \cap \gamma.$$

We may conclude that $C(\alpha, \beta; \gamma)$ holds, from which the result now follows. $\square$

Remark A.38. In particular, we note that, for a given algebra $\mathbf{A}$, $[\alpha, \beta] = 0_A$ if and only if for any $x, y, z \in A$ with $\langle x, y\rangle, \langle x, z\rangle \in \alpha$ and $\langle y, z\rangle \in \beta$ we have that

$$\langle x, x\rangle \, \Delta^{\alpha}_{\beta} \, \langle y, z\rangle \Rightarrow y = z.$$

Indeed, this implication says precisely that 0_A is a union of Δ^{α}_{β}-classes. In particular, a given algebra $\mathbf{A}$ is thus abelian if and only if 0_A is normal in $\mathbf{A}^2$.

The concept of "difference term" is also typically defined with reference to the commutator (although, it does turn out to have other useful characterizations (see Kearnes, Szendrei, and Willard (2013+))—a lattice theoretic characterization as well as a Mal'cev condition.

Definition A.39. We say that $\mathcal{V}$ is a *variety with a difference term* d when d is a ternary term operation for $\mathcal{V}$, so that for $\mathbf{A} \in \mathcal{V}$ and any $a, b \in A$,

$$d(b, b, a) = a \, [\theta, \theta] \, d(a, b, b),$$

where $\theta = \mathrm{Cg}^{\mathbf{A}}\langle a, b\rangle$.

Thus, one can remark that to say that a variety has a difference term is weaker than finding that it has a Mal'cev term; a difference term is, in some sense, "half-Mal'cev." Less obviously, all congruence modular varieties have a difference term.

A.3.2 Some restricted properties of the commutator

Usually, we shall have one further nontrivial property of the commutator available, which we now give. Its proof can be found in Kearnes (1995), Lemma 2.2.

Theorem A.40. *Let* $\mathbf{A}$ *be an algebra in a variety with a difference term. Let* $\alpha, \beta \in \operatorname{Con} \mathbf{A}$*. Then* $[\alpha, \beta] = [\beta, \alpha]$.

We shall call this property *symmetry of the commutator.*

There are two other strong properties of the centralizer relation and commutator available only in congruence modular varieties, which frequently come in handy.

Theorem A.41. *Let* $\mathbf{A}$ *be an algebra in a congruence modular variety. Let* $\alpha, \beta, \gamma \in \operatorname{Con} \mathbf{A}$*. Then* $C(\alpha, \beta; \gamma)$ *holds if and only if* $[\alpha, \beta] \leq \gamma$.

Theorem A.42. *(Additivity of the commutator) Let* $\mathbf{A}$ *be an algebra in a congruence modular variety. Let* $\alpha, \beta_i (i \in I) \in \operatorname{Con} \mathbf{A}$*. Then*

$$[\alpha, \bigvee_{i \in I} \beta_i] = \bigvee_{i \in I} [\alpha, \beta_i].$$

In fact, as noted by Lipparini (1994) as Theorem 3.2, $\mathcal{V}$ is congruence modular if and only if it has a difference term and the commutator is additive, as in Theorem A.42.

A.3.3 Abelian, nilpotence, and solvable congruences

Next, we define abelianness, three types of nilpotence, and solvability.

Definition A.43. Let $\mathbf{A}$ be an algebra, and let $\alpha \leq \beta \in \operatorname{Con}\mathbf{A}$. We say that β is *abelian over* α whenever $C(\beta, \beta; \alpha)$ holds. (Otherwise, we say that the quotient $\langle \alpha, \beta \rangle$ is *nonabelian*.) We say that $\mathbf{A}$ is abelian whenever 1_A is abelian over 0_A.

Definition A.44. For a given algebra $\mathbf{A}$ and $\alpha \in \operatorname{Con}\mathbf{A}$, set

$$[\alpha)_0 := \alpha$$

and for $k \geq 1$

$$[\alpha)_k := [[\alpha)_{k-1}, \alpha].$$

Similarly, set

$$(\alpha]_0 := \alpha$$

and for $k \geq 1$

$$(\alpha]_k := [\alpha, (\alpha]_{k-1}].$$

We say that α is *left nilpotent of class k* whenever $[\alpha)_k = 0_A$. We say that $\mathbf{A}$ is *left nilpotent of class k* whenever $[1_A)_k = 0_A$. We say that algebra $\mathbf{A}$ is *left nilpotent* provided it is left nilpotent of class k for some natural number k.

We can similarly define right nilpotence, if we should find a use for it; however, in varieties for which the commutator is symmetric, these definitions in fact coincide. (One can check this via an easy proof by induction).

We shall also make use of the concept of "solvability," which is a generalization of the concept of the same name from group theory.

Definition A.45. For a given algebra $\mathbf{A}$ and $\alpha \in \operatorname{Con}\mathbf{A}$, we define

$$[\alpha]_0 := \alpha,$$

and for $n \geq 1$

$$[\alpha]_n := [[\alpha]_{n-1}, [\alpha]_{n-1}].$$

In particular, whenever $[1_A]_k = 0_A$ for some natural number k, we say that $\mathbf{A}$ is *solvable of class* k; $\mathbf{A}$ is said to be *solvable* if it is solvable of class k for some k.

Note that by the monotonicity of the commutator and Theorem A.31, for any $\mathbf{A}$, $\alpha \in \operatorname{Con} \mathbf{A}$, and any natural number $n > 0$,

$$\cdots \subseteq [\alpha]_{n+1} \subseteq [\alpha]_n \subseteq [\alpha)_n \subseteq [1_A)_n \subseteq [1_A)_{n-1} \subseteq \cdots \subseteq [1_A)_0 = 1_A.$$

In particular, nilpotence of class n implies solvability of class n.

A.3.4 Regarding nilpotent algebras in a Mal'cev variety

There are many reasons for studying nilpotent algebras in the congruence modular (or, equivalently, weak difference term, difference term, or Mal'cev setting; see Theorem 4.7 in Charpter 4). Now, while the study of nilpotence and solvability in group theory can be viewed as the effort to generalize some of the desirable properties of abelian groups, the assumption of nilpotence in the Mal'cev setting allows one to recover some of the nice properties available in group theory. Among these is the fact noted by Freese and McKenzie (1987).

Theorem A.46. *Let $\mathcal{V}$ be a variety with a Mal'cev term (or, by Theorem 4.7, a weak-difference term), and let $\mathbf{A} \in \mathcal{V}$ be a nilpotent algebra. Then $\mathbf{A}$ has* uniform *and* regular *congruences: that is, for any $\theta \in \operatorname{Con} \mathbf{A}$ and any $a, b \in A$, we have $|a/\theta| = |b/\theta|$ and $\theta = \operatorname{Cg}^{\mathbf{A}} a/\theta$, respectively.*

See Corollaries 7.5 and 7.7 in Freese and McKenzie (1987) for a proof of this theorem. These results of Freese and McKenzie (but which have earlier origins) owe to another result of theirs, which we shall also need.

Theorem A.47. *Let $\mathcal{V}$ be a variety with a Mal'cev term p. Let n be a natural number. Then $\mathcal{V}$ also possesses a ternary term f_n such that for any $\mathbf{A} \in \mathcal{V}$, and $x, b, c \in A$,*

$$f_n^{\mathbf{A}}(p^{\mathbf{A}}(x, b, c), b, c)\ (1_A]_n\ x$$

and

$$p(f_n(x,b,c),b,c)\,(1]_n\,x.$$

Furthermore, one can deduce that if $\mathbf{A}$ *is nilpotent of class* n*, then* $\mathbf{A}$ *satisfies*

$$f_n(z,x,z) \approx f_n(p(x,y,z),y,z) \approx p(f_n(x,y,z),y,z) \approx x.$$

See Theorem 7.3 and Lemma 7.6 of Freese and McKenzie (1987) for proofs of these facts.

The following is known from Hobby and McKenzie (1988), Theorem 7.2, but it is also easy enough to show directly, and so we do so now, for convenience.

Theorem A.48. *Let* $\mathbf{A}$ *be a solvable algebra in a Mal'cev variety. Let* $\alpha, \beta \in \operatorname{Con}\mathbf{A}$ *such that* $\alpha \prec \beta$*. Then* β *is abelian over* α*.*

Proof. We need to show that $C(\beta,\beta;\alpha)$. However, since $\mathbf{A}$ is in a congruence modular variety, by Theorem A.41, it is sufficient to show that $[\beta,\beta] \leq \alpha$. Since $\alpha \prec \beta$ and $[\beta,\beta] \leq \beta$, we have that either $[\beta,\beta] \vee \alpha = \alpha$, as desired, or $[\beta,\beta] \vee \alpha = \beta$. We shall suppose the latter and derive a contradiction.

We claim that, under this assumption, we get that for all $n > 0$, $[\beta]_n \leq [\alpha,\beta] \vee [\beta]_{n+1}$. We shall show this by induction. By the complete additivity (Theorem A.42) and symmetry (Theorem A.40) of the commutator in congruence modular varieties (plus, the fact that congruence permutability entails congruence modularity) we get that

$$\begin{aligned}
[\beta]_1 &= [\beta,\beta] \\
&= [\alpha \vee [\beta,\beta], \alpha \vee [\beta,\beta]] \\
&= [\alpha, \alpha \vee [\beta,\beta]] \vee [[\beta,\beta], \alpha \vee [\beta,\beta]] \\
&= [\alpha, \alpha \vee [\beta,\beta]] \vee [[\beta,\beta], \alpha] \vee [\beta]_2 \\
&= [\alpha,\beta] \vee [\beta]_2,
\end{aligned}$$

establishing the basis. Now let $n > 1$ and assume that the claim has been verified for $n = m - 1$. Then

$$\begin{aligned}
[\beta]_m &= [[\beta]_{m-1}, [\beta]_{m-1}] \\
&\leq [[\alpha, \beta] \vee [\beta]_m, [\alpha, \beta] \vee [\beta]_m] \\
&= [[\alpha, \beta], [\alpha, \beta]] \vee [[\alpha, \beta], [\beta]_m] \vee [\beta]_{m+1} \\
&\leq [\alpha, \beta] \vee [\beta]_{m+1}.
\end{aligned}$$

The claim goes through by induction.

Now, since, by the monotonicity of the commutator we have that $[\beta, \beta] = [\alpha, \beta] \vee [\beta, \beta] = [\alpha, \beta] \vee [\beta]_1$, we can apply the above claim inductively to learn that $[\beta, \beta] \leq [\alpha, \beta] \vee [\beta]_n$ for all $n > 0$. But, of course, since **A** is solvable, we get that for any high enough n, $[\beta]_n \leq [1_A]_n = 0_A$. It follows that $[\beta, \beta] = [\alpha, \beta]$. Thus, we get that $\beta = [\beta, \beta] \vee \alpha = [\alpha, \beta] \vee \alpha = \alpha$, a contradiction which forces $\alpha \vee [\beta, \beta] = \alpha$, as desired. □