THE CLASS OF SUBDIRECTLY IRREDUCIBLE GROUPS GENERATED BY A FINITE GROUP IS FINITELY AXIOMATIZABLE

GEORGE F. MCNULTY AND JU WANG

In Celebration of the Seventieth Birthday of Jan Mycielski

Abstract. The class of all subdirectly irreducible groups belonging to a variety generated by a finite group can be axiomatized by a finite set of elementary sentences.

1. Introduction

A group is **subdirectly irreducible** provided it has a least nontrivial normal subgroup. Subdirectly irreducible groups are also referred to as **monolithic** groups in the literature. Every simple group is subdirectly irreducible, but there are many subdirectly irreducible groups that are not simple. A **variety** of groups is a class of groups closed with respect to the formation of homomorphic images, subalgebras, and arbitrary direct products. If $\mathbf{G}$ is a group, then the **variety generated by G** is the smallest variety to which $\mathbf{G}$ belongs. We denote this variety by $\mathcal{V}(\mathbf{G})$. According to a classical theorem of Birkhoff [4] varieties are exactly those classes which can be axiomatized by a set of equations. According to another classical theorem of Birkhoff [5] two varieties are the same if they have the same subdirectly irreducible members. For a class $\mathcal{V}$ of groups, we let $\mathcal{V}_{\text{si}}$ denote the class of all subdirectly irreducible groups belonging to $\mathcal{V}$.

The chief result of this paper is:

Main Theorem. *The class of all subdirectly irreducible groups belonging to the variety generated by any finite group is finitely axiomatizable.*

This theorem provides an important property that finite groups share with a surprising assortment of other finite algebras. For this reason we have framed our arguments in the language of general algebra, even though our result lies entirely within group theory. We take an **algebra A** to be a nonempty set A equipped with a system of operations, each taking some finite number of arguments. The notions of subalgebra, homomorphism, and direct product have their natural meanings. A **congruence** on an algebra $\mathbf{A}$ is simply the kernel of some homomorphism. Specifically,

$$\{\langle a, b\rangle : a, b \in A \text{ and } h(a) = h(b)\}$$

is a congruence of $\mathbf{A}$ whenever h is a homomorphism with domain A. In groups, congruences can be replaced by the conceptually simpler notion of normal subgroups. Set-inclusion imposes a lattice ordering on the set of all congruences of an algebra. We use $\operatorname{Con}\mathbf{A}$ to denote the lattice of congreunces of the algebra $\mathbf{A}$. We use $\phi \wedge \psi$ to denote the greatest lower bound or **meet** of the congruences ϕ and ψ (this is just $\phi \cap \psi$) and $\phi \vee \psi$ to denote the least upper bound or **join** of ϕ and ψ (which fails, usually, to be the union). Indeed, any set of congruences of $\mathbf{A}$ has both a least upper bound and a greatest lower bound. An algebra $\mathbf{A}$ is **subdirectly irreducible** provided $\mathbf{A}$ has a least nontrivial congruence, referred to as the **monolith** of $\mathbf{A}$. Usually, we reserve μ to stand for the monolith of a subdirectly irreducible algebra. Subdirectly irreducible algebras are also characterized by the presence of a pair $\langle a, b\rangle$ of distinct elements which belongs to every nontrivial congruence. Such a pair is called a **critical pair**. The two classical theorems of Birkhoff cited

Date: 22 November 2003.

above apply to algebras, not just to groups. For an exposition of the general theory of algebras see [22], [8], and [11]. We follow the notational conventions of [22] most closely. The standard reference for varieties of groups is the excellent book of Hanna Neumann [23].

An algebra $\mathbf{A}$ is said to be **finitely based** if there is a finite set Σ of equations, each true in $\mathbf{A}$, such that every equation true in $\mathbf{A}$ is a logical consequence of Σ. Discovering which finite algebras are finitely based has proven to be a very subtle problem. In groundbreaking work, in 1996 McKenzie [21] solved Tarski's Finite Basis Problem by proving that there is no algorithm for determining which finite algebras are finitely based. Nevertheless, we know that many finite algebras are finitely based.

In 1965, Oates and Powell [24] proved

The Finite Basis Theorem of Oates and Powell

Every finite group is finitely based.

Soon afterward Kruse [14] and L'vov [15], working independently, proved that every finite ring is finitely based. The proofs of the result for finite rings have large overlaps with the proofs of the Theorem of Oates and Powell.

In 1970, McKenzie [18] proved that any finite lattice with finitely many additional operators is finitely based. Shortly thereafter, Baker proved a far-reaching generalization of McKenzie's result:

Baker's Finite Basis Theorem

Let $\mathbf{A}$ be finite algebra with only finitely many fundamental operations. If $\mathcal{V}(\mathbf{A})$ is *congruence distributive*, then $\mathbf{A}$ is finitey based.

Baker's work appeared after a six year delay in [1]. It attracted so much attention that at least four alternate proofs appeared in print prior to [1]. Congruence distributivity means

$$\theta \wedge (\phi \vee \psi) = (\theta \wedge \phi) \vee (\theta \wedge \psi)$$

for all congruences θ, ϕ, and ψ belonging to any algebra in $\mathcal{V}(\mathbf{A})$. The technical condition of congruence distributivity applies to lattices and, indeed, to most of the algebraic structures arising from mathematical logic.

While most groups fail to belong to congruence distributive varieties, all groups do have *modular* congruence lattices—a fact due, in principle, to Dedekind [9]. Modularity is the following weakening of distributivity.

$$\theta \wedge \phi = \phi \implies \theta \wedge (\phi \vee \psi) = (\theta \wedge \phi) \vee (\theta \wedge \psi)$$

However, the prospect of replacing distributivity by modularity in Baker's Finite Basis Theorem (and so arriving at a common generalization of Baker's Theorem and the Oates-Powell Theorem) is frustrated by a series of examples due to Polin [25], Bryant [6], and Isaev [12]. Still, significant progress was possible. It turns out that the theory of the commutator, construed as an operation on pairs of congruences, extends to any variety with modular congruence lattices. Hence, the notions of solvable, nilpotent, and Abelian, familiar in the context of groups, extend to all congruence modular varieties of algebras. See the monograph [10] for an exposition of this important theory. Work of Vaughan-Lee supplemented by work of Freese (cf. [10]) yields:

The Finite Basis Theorem of Vaughan-Lee and Freese

Suppose $\mathbf{A}$ is a finite algebra with only finitely many fundamental operations. If $\mathcal{V}(\mathbf{A})$ is congruence modular and $\mathbf{A}$ is nilpotent and the direct product of algebras of prime power order, then $\mathbf{A}$ is finitely based.

This result extends a part of the Oates-Powell Theorem. In spirit, its proof can be traced to a theorem of Lyndon [16] according to which any variety of nilpotent groups is finitely based. It is well-known that the finite nilpotent groups are exactly those which are direct products of groups of prime power order. This equivalence does not extend to the congruence modular case.

One of the key facts that is employed in all proofs of Baker's Finite Basis Theorem is that there is a finite bound on the cardinalities of the subdirectly irreducible algebras. In the presence of congruence distributivity,

this is a consequence of Jónsson's Lemma [13]. Here are two different generalizations of Baker's Finite Basis Theorem:

McKenzie's Finite Basis Theorem

Suppose $\mathbf{A}$ is a finite algebra with only finitely many fundamental operations. If $\mathcal{V}(\mathbf{A})$ is congruence modular and there is a finite upper bound of the cardinalities of the subdirectly irreducible algebras in $\mathcal{V}(\mathbf{A})$, then $\mathbf{A}$ is finitely based.

This theorem can be found in [20].

McKenzie's Finite Basis Theorem, like the Finite Basis Theorem of Vaughan-Lee and Freese, extends a part of the Oates-Powell Finite Basis Theorem. These two extensions turn out to have little overlap, as McKenzie observed.

Willard's Finite Basis Theorem

Suppose $\mathbf{A}$ is a finite algebra with only finitely many fundamental operations. If $\mathcal{V}(\mathbf{A})$ is congruence meet-semidistributive and there is a finite upper bound of the cardinalities of the subdirectly irreducible algebras in $\mathcal{V}(\mathbf{A})$, then $\mathbf{A}$ is finitely based.

This theorem can be found in [26]. Congruence meet-semidistributivity is the following weakening of congruence distributivity

$$\theta \wedge \phi = \theta \wedge \psi \implies \theta \wedge (\phi \vee \psi) = (\theta \wedge \phi) \vee (\theta \wedge \psi)$$

for all congruences θ, ϕ, and ψ belonging to any algebra in $\mathcal{V}(\mathbf{A})$. The technical condition of congruence meet-semidistributivity holds, for example, in every semilattice with operators.

There is one further finite basis theorem that is germane to our investigations. To state it we need to introduce several more concepts. Let $\mathbf{A}$ be any algebra and let $c, d \in A$. The smallest congruence to which $\langle c, d\rangle$ belongs is called the **principal congruence** generated by $\langle c, d\rangle$ and it is denoted by $\mathrm{Cg}^{\mathbf{A}}(c, d)$. A formula $\Phi(u, v, x, y)$ with four free variables is called a **congruence formula** provided for every algebra $\mathbf{A}$

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

Thus, $\Phi(u, v, c, d)$ describes a part of $\mathrm{Cg}^{\mathbf{A}}(c, d)$. Indeed, it turns out that $\mathrm{Cg}^{\mathbf{A}}(c, d)$ is just the union of all its parts that can be described by congruence formulas. When $\mathbf{A} \models \Phi(a, b, c, d)$, the complexity of the formula $\Phi(u, v, x, y)$ measures how distant $\langle a, b\rangle$ is from $\langle c, d\rangle$. It can happen that $\Phi(u, v, c, d)$ describes all of $\mathrm{Cg}^{\mathbf{A}}(c, d)$. In this event we say that $\Phi(u, v, c, d)$ **defines** the principal congruence $\mathrm{Cg}^{\mathbf{A}}(c, d)$.

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

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

Thus when $\mathcal{K}$ has definable principal subcongruences there will be two congruence formulas Ψ and Φ so that any principal congruence in any algebra in $\mathcal{K}$ is not far (as measured by Ψ) above a principal congruence defined by Φ. This notion, which is a weakening of the notion of definable principal congruences due to Baldwin and Berman [3] (cf. [7, 19]), was introduced by Baker and Wang in [2], where the following theorem in proved.

The Finite Basis Theorem of Baker and Wang

Let $\mathcal{V}$ be a variety with only finitely many fundamental operations and suppose that $\mathcal{V}$ has definable principal subcongruences. Under these assumptions, $\mathcal{V}$ is finitely based if and only if $\mathcal{V}_{\mathrm{si}}$ is finitely axiomatizable.

Baker and Wang demonstrate that varieties generated by finite groups need not have definable principal subcongruences. On the other hand, they also give a direct proof that congruence distributive varieties generated by a finite algebra do have definable principal subcongruences. Thus, they provide the simplest proof to date of Baker's Finite Basis Theorem.

The ambition behind our present line of research is to see all these finite basis theorems as individual manifestations of some small collection of underlying principles. Roughly speaking, Baker's Finite Basis Theorem and its generalizations by McKenzie and Willard stated above are established by developing sufficient information about certain 4-ary relations that are definable by means of elementary formulas and by invoking the finite upper bound on the sizes of the subdirectly irreducible algebras in the variety. A striking difference in the case of finite groups (and of finite rings) is that there need be no such finite bound. Indeed, the variety generated by the quaternion group contains arbitrarily large infinite subdirectly irreducible groups. We believe that the existence of a finite bound on the cardinalities of the subdirectly irreducible algebras is too strong a condition. We propose to replace it by the weaker condition that this class can be axiomatized by a finite set of elementary sentences. Our purpose here is to show that any variety generated by a finite group indeed has this property.

2. A General Theorem

The proof of the theorem below is a variation on the arguments of Baker and Wang [2].

Theorem 0. *If $\mathcal{V}$ is a variety and $\mathcal{V}_{\mathrm{si}}$ has definable principal subcongruences, then $\mathcal{V}_{\mathrm{si}}$ is finitely axiomatizable relative to $\mathcal{V}$. Consequently, if $\mathcal{V}$ is finitely based, then $\mathcal{V}_{\mathrm{si}}$ is finitely axiomatizable.*

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

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

We contend that Θ axiomatizes $\mathcal{V}_{\mathrm{si}}$.

First, suppose $\mathbf{A} \in \mathcal{V}_{\mathrm{si}}$. Let $\langle e, f\rangle$ be a critical pair for $\mathbf{A}$—that is, $e \neq f$ and $\langle e, f\rangle$ belongs to every nontrivial congruence. Now let $c, d \in A$ with $c \neq d$. Because $\mathcal{V}_{\mathrm{si}}$ has definable principal subcongruences, there must be $a, b \in A$ with $a \neq b$ so that $\mathbf{A} \models \Psi(a, b, c, d)$ and $\Phi(x, y, a, b)$ defines $\mathrm{Cg}^{\mathbf{A}}(a, b)$. Because $a \neq b$ and $\langle e, f\rangle$ is critical, we have $\langle e, f\rangle \in \mathrm{Cg}^{\mathbf{A}}(a, b)$. Hence, $\mathbf{A} \models \Phi(e, f, a, b)$. So we have demonstrated that

$$\mathbf{A} \models \exists u, v[u \neq v \mathbin{\mathbb{\wedge}} \forall z, w(z \neq w \implies \exists x, y(\Phi(u, v, x, y) \mathbin{\mathbb{\wedge}} \Psi(x, y, z, w)))]$$

But also $\mathbf{A} \models \Sigma$ since $\mathcal{V}_{\mathrm{si}} \subseteq \mathcal{V}$. Therefore $\mathbf{A} \models \Theta$.

Now suppose $\mathbf{A} \models \Theta$. Then $\mathbf{A} \in \mathcal{V}$ since Σ axiomatizes $\mathcal{V}$. But the second part of Θ entails that $\mathbf{A}$ has a critical pair, since $\Phi(u, v, x, y)$ and $\Psi(x, y, z, w)$ are congruence formulas. Thus $\mathbf{A}$ is subdirectly irreducible. This means $\mathbf{A} \in \mathcal{V}_{\mathrm{si}}$, as desired. □

According to the Theorem of Oates and Powell, every finite group generates a finitely based variety, so to prove our Main Theorem, all we need is the following result.

Theorem 1. *Let $\mathcal{V}$ be the variety generated by some finite group. Then $\mathcal{V}_{\mathrm{si}}$ has definable principal subcongruences.*

The proof of this theorem occupies the remainder of the paper.

3. Preliminaries Concerning Principal Congruences

Let $p(x, y, z) = xy^{-1}z$. Then in any group the following equations hold

$$(\star) \qquad p(x, x, y) \approx y \text{ and } p(x, y, y) \approx x.$$

In 1954, A. I. Maltsev [17] proved that the varieties $\mathcal{V}$ for which there is a term $p(x, y, z)$ such that the equations $(\star)$ holds in $\mathcal{V}$ are precisely the congruence permutable varieties. Congruence permutability means that if ϕ and ψ are congruences of $\mathbf{A} \in \mathcal{V}$, then $\phi \vee \psi = \phi \circ \psi$. Here $\phi \circ \psi$ is the composition of ϕ and ψ as binary relations.

Let $\mathbf{A}$ be a group, let ϕ be a congruence on $\mathbf{A}$, and $a \in A$. We denote the congruence class of a by a/ϕ. That is

$$a/\phi = \{b \mid \langle a, b\rangle \in \phi\}.$$

In particular, $1/\phi$ denotes the normal subgroup of $\mathbf{A}$ associated with the congruence ϕ. This means

$$\langle a, b\rangle \in \phi \text{ if and only if } ab^{-1} \in 1/\phi.$$

Much of our reasoning in this paper applies to algebras belonging to a congruence permutable variety, not just to groups. In particular, this applies to Theorems 2 and 3.

Suppose that $\mathbf{H}$ is a group. By a **unary polynomial** of $\mathbf{H}$ we mean a function $q(x)$ from H into H for which there is a term $r(x, y_0, y_1, \dots)$, built up from the group operations and the variables $x, y_0, y_1, \dots$, and elements $c_0, c_1, \dots \in H$ so that $q(a) = r(a, c_0, c_1, \dots)$ for all $a \in H$. The **complexity** of the polynomial $q(x)$ is the number of occurrences of variables in $r(x, y_0, \dots)$, where $r(x, y_0, \dots)$ is chosen so this number is as small as possible.

The two theorems in this section, which are certainly part of the folklore, will be used repeatedly.

Theorem 2. *Let* $\mathbf{H}$ *be a group and* $a, b \in H$*. Then*

$$\mathrm{Cg}^{\mathbf{H}}(a, b) = \{\langle q(a), q(b)\rangle : \textit{for some unary polynomial } q(x)\}.$$

Proof. Let $T = \{\langle q(a), q(b)\rangle : \text{for some unary polynomial } q(x)\}$. Evidently, $\langle a, b\rangle \in T \subseteq \mathrm{Cg}^{\mathbf{H}}(a, b)$. So we need only argue that T is a congruence.

Now it is well-known that the congruences of $\mathbf{H}$ are exactly those subgroups of $\mathbf{H}\times\mathbf{H}$ which are equivalence relations. T is easily seen to be a subgroup of $\mathbf{H}\times\mathbf{H}$, so it remains to prove that T is an equivalence relation.

For reflexivity, let $c \in H$. Then $p(a, a, c) = c = p(b, b, c)$. So we obtain $\langle c, c\rangle \in T$ by taking $q(x) = p(x, x, c)$.

For symmetry, suppose $\langle c, d\rangle \in T$. Pick a polynomial $s(x)$ so that $c = s(a)$ and $d = s(b)$. Let $q(x) = p(s(a), s(x), s(b))$. Then $d = s(b) = q(a)$ and $c = s(a) = q(b)$. Consequently, $\langle d, c\rangle \in T$.

For transitivity, suppose $\langle c, d\rangle, \langle d, e\rangle \in T$. Pick polynomials $s(x)$ and $t(x)$ so that $c = s(a), d = s(b) = t(a)$ and $e = t(b)$. Take $q(x) = p(s(x), t(a), t(x))$. Then $c = s(a) = p(s(a), t(a), t(a)) = q(a)$ and $e = t(b) = p(s(b), s(b), t(b)) = p(s(b), t(a), t(b)) = q(b)$. This means that $\langle c, e\rangle \in T$. □

We call a condition of the form $\langle a, b\rangle \in \mathrm{Cg}^{\mathbf{H}}(c, d)$ a **membership condition**. When $a = q(c)$ and $b = q(d)$, we say that the membership condition is **witnessed** by the polynomial $q(x)$. The **complexity** of a polynomial $q(x)$ is the length of a shortest term $t(x, y_0, y_1, \dots)$ such that $q(x) = t(x, c_0, c_1, \dots)$ for some $c_0, c_1, \dots \in H$. One of our chief concerns will be the discovery of upper bounds on the complexity of polynomials that are needed to witness various membership conditions.

Theorem 2 asserts that for groups (and more generally, for algebras belonging to congruence permutable vareities) congruence formulas can take a very simple form: disjunctions of formulas of the form

$$\exists u_0, u_1, \dots, u_{n-1}[x \approx t(z, u_0, u_1, \dots, u_{n-1}) \mathbin{\mathbb{A}} y \approx t(w, u_0, u_1, \dots, u_{n-1})]$$

where the disjunction ranges over finitely many terms t.

Theorem 2 can be recast using properties more specific to groups. Evidentally, $\langle a, b\rangle \in \mathrm{Cg}^{\mathbf{H}}(c, d)$ if and only if $\langle ab^{-1}, 1\rangle \in \mathrm{Cg}^{\mathbf{H}}(cd^{-1}, 1)$ for any group $\mathbf{H}$ and any $a, b, c, d \in H$. So we can restrict our attention to membership conditions of the form $\langle u, 1\rangle \in \mathrm{Cg}^{\mathbf{H}}(v, 1)$. For membership conditions of this kind we only need to consider certain kinds of unary polynomials. The set of **conjugate product terms** in x is the smallest set C of terms such that

- $1 \in C$, and
- If $t \in C$ and y is a variable, then both $(yxy^{-1})t$ and $(yx^{-1}y^{-1})t$ belong to C.

A polynomial $\pi(x)$ is called a **conjugate product polynomial** provided $\pi(x)$ is obtained from some conjugate product term $t(x, y_0, \dots, y_k)$ by using elements of the group as values for all the variables other than x.

Theorem 2′. *Let* $\mathbf{H}$ *be a group and* $c \in H$*. Then for all* $a \in H$ *we have*

$$\langle a, 1\rangle \in \mathrm{Cg}^{\mathbf{H}}(c, 1) \text{ if and only if } a = \pi(c) \text{ for some conjugate product polynomial } \pi(x).$$

The observation that $\{\pi(c) \mid \pi(x)$ is a cojugate product polynomial$\}$ is the smallest normal subgroup of $\mathbf{H}$ which contains c is the essence of the proof of this theorem.

Theorem 3. *Let* $\mathbf{A}$ *be a group and* θ *be a congruence relation on* $\mathbf{A}$*. Suppose* $a, b, c, d \in A$*. If* $\langle a/\theta, b/\theta\rangle \in \mathrm{Cg}^{\mathbf{A}/\theta}(c/\theta, d/\theta)$*, then there is* $u \in a/\theta$ *such that* $\langle u, b\rangle \in \mathrm{Cg}^{\mathbf{A}}(c, d)$*.*

Proof. Using Theorem 2 pick a term $s(x, y_0, y_1, \dots)$ and elements $e_0, e_1, \dots \in A$ so that

$$a/\theta = s(c, e_0, e_1, \dots)/\theta, \text{ and}$$
$$b/\theta = s(d, e_0, e_1, \dots)/\theta.$$

Let $q(x) = p(s(x, e_0, e_1, \dots), s(d, e_0, e_1, \dots), b)$. Then

$$q(c) = p(s(c, e_0, e_1, \dots), s(d, e_0, e_1, \dots), b)\ \theta\ p(a, b, b) = a \text{ and}$$
$$q(d) = p(s(d, e_0, e_1, \dots), s(d, e_0, e_1, \dots), b) = b.$$

This means that we can take $u = q(c)$. □

4. Chief Factors and Definability of Atoms of the Congruence Lattice

Let $\mathbf{H}$ be an algebra and let ϕ and ψ be congruences of $\mathbf{H}$ such that $\psi \subseteq \phi$. Then ψ partitions each ϕ congruence class. In general (even in the congruence modular case), different ϕ-classes can be partitioned by ψ into different numbers of blocks, but if $\mathbf{H}$ is a group this partitioning always results in the same number of blocks. In any case, we refer to the least upper bound of the cardinalities of the partitions of the ϕ-classes by ψ as the **size** of ϕ/ψ. Following the practice in group theory, in case ϕ covers ψ—that is $\psi \subseteq \phi, \psi \neq \phi$ and there are no congruences properly between ψ and ϕ—we refer to ϕ/ψ as a **chief factor**. In groups, this comes down to $\mathbf{N}/\mathbf{K}$ where $\mathbf{N}$ is the normal subgroup associated with ϕ and $\mathbf{K}$ is the normal subgroup associated with ψ.

Now suppose that $\mathbf{H}$ is in the variety generated by the finite group $\mathbf{G}$. In the event that $\mathbf{H}$ is finite, it has been noted by H. Neumann in [23] (Theorem 51.23) that $|G|$ is an upper bound on the size of the chief factors of $\mathbf{H}$. More is true. Freese and McKenzie [10] adapted the notion of chief factor to arbitrary congruence modular varieties. According to their Theorem 10.16, the restriction that $\mathbf{H}$ is finite can be eliminated. Freese and McKenzie note that this result was already obtained by J. B. Nation and Walter Taylor in the congruence permutable case—which includes groups.

Let $\mathbf{H}$ be an algebra. The identity relation on H, which we denote by $0_{\mathbf{H}}$, is to smallest congruence on $\mathbf{H}$. Those congruences which cover $0_{\mathbf{H}}$ are referred to as **atoms** of the congruence lattice. Evidently, every atom is a principal congruence. In case $\mathbf{H}$ is subdirectly irreducible, its monolith is an atom.

Theorem 4. *Let* $\mathcal{V}$ *be the variety generated by some finite group. There is a congruence formula* $\Phi(u, v, x, y)$ *such that for every* $\mathbf{H} \in \mathcal{V}$ *and every* $c, d \in H$ *such that* $\mathrm{Cg}^{\mathbf{H}}(c, d)$ *is an atom, it follows that* $\Phi(u, v, c, d)$ *defines* $\mathrm{Cg}^{\mathbf{H}}(c, d)$*.*

The key to the proof of this theorem is the following lemma, which we will also need later.

Lemma 0. *Let* $\mathbf{H}$ *be a group and suppose* $a, b, c, d \in H$ *so that* $\langle a, b\rangle \in \mathrm{Cg}^{\mathbf{H}}(c, d)$*. Then there is a polynomial witnessing this membership condition such that* $4|1/\mathrm{Cg}^{\mathbf{H}}(c, d)| + 1$ *is an upper bound on the complexity of the polynomial, and hence on the number of coefficients needed in the polynomial.*

Proof. This membership condition is equivalent to ab^{-1} belonging to the normal subgroup of $\mathbf{H}$ generated by cd^{-1}. This subgroup is $1/\operatorname{Cg}^{\mathbf{H}}(c,d)$. Consequently, $ab^{-1} = g_0 g_1 \cdots g_{n-1}$ where each g_i is a conjugate either of cd^{-1} or its inverse dc^{-1}. We see that if n is chosen as small as possible, then $g_0, g_0g_1, g_0g_1g_2, \ldots, g_0g_1\cdots g_{n-1}$ will be n distinct elements of the normal subgroup. To obtain a polynomial $q(x)$ witnessing the membership condition replace every occurrence of c in $g_0g_1\cdots g_{n-1}b$ by x. Then $a = q(c)$ and $b = q(d)$. □

Proof of Theorem 4. Let r be a finite upper bound on the size of chief factors in algebras belonging to $\mathcal{V}$. Up to renaming variables there are only finitely many terms with no more than $4r+1$ occurrences of variables. Let $u, v, x, y, w, u_0, \ldots, u_{4r-1}$ be $r+5$ distinct variables and let T be the set of all terms in the variables $w, u_0, dots, u_{4r-1}$ which have no more than $4r+1$ occurrences of variables. Let $\Phi(u,v,x,y)$ be

$$\bigvee_{t\in T} \exists u_0, \ldots, u_{4r-1}[u \approx t(x, u_0, \ldots, u_{4r-1}) \mathbin{\mathbb{\wedge}} v \approx t(z, u_0, \ldots, u_{4r-1})].$$

If $\operatorname{Cg}^{\mathbf{H}}(c,d)$ is an atom, then $\operatorname{Cg}^{\mathbf{H}}(c,d)/0_{\mathbf{H}}$ is a chief factor and $(1/\operatorname{Cg}^{\mathbf{H}}(c,d))/0_{\mathbf{H}}$ has the same number of elements as $1/\operatorname{Cg}^{\mathbf{H}}(c,d)$. According to Lemma 0, a membership condition $\langle a,b\rangle \in \operatorname{Cg}^{\mathbf{H}}(c,d)$ is always witnessed by a polynomial of complexity no more than $4r+1$. Hence $\Phi(a,b,c,d)$ must hold, since one of the disjuncts of $\Phi(u,v,x,y)$ must be fulfilled. Thus, $\Phi(x,y,c,d)$ defines the atom $\operatorname{Cg}^{\mathbf{H}}(c,d)$ as desired. □

In particular, the formula $\Phi(u,v,x,y)$ of Theorem 4 can be used to define the monoliths of each subdirectly irreducible group in the variety. It remains to show that there is a congruence formula Ψ so that in every subdirectly irreducible group in the variety, the monolith is not far below (as measured by Ψ) any other nontrivial principal congruence.

5. Bounding Ladders of Congruences

Let $\mathbf{H}$ be any group. A system $B = \langle B_0, B_1, \ldots, B_{m-1}\rangle$ of subsets of H is said to be a **ladder** provided

(1) $1 \in B_i$ and B_i has at least two elements, for each $i < m$,
(2) $B_i \cap B_j = \{1\}$ for all $i, j < m$ with $i \neq j$,
(3) $\langle z, 1\rangle \in \operatorname{Cg}^{\mathbf{H}}(x,y)$ for all $x \in B_i, y \in B_j$ and $z \in B_k$ with $1 \neq x \neq y$ and for all $i, j, k < m$ with $j, k \leq i$.

The congruences of the form $\operatorname{Cg}^{\mathbf{H}}(x,y)$ where $x \in B_i$ and $y \in B_j$ with $j \leq i < m$ and $x \neq y$ are called the **principal conguences** of the ladder. In view of the symmetry and transitivity of congruence relations, it is a consequence of (3) that this congruence is independent of the choice of $x \in B_i$ or of $y \in B_j$ as long as $1 \neq x \neq y$. We denote $\operatorname{Cg}^{\mathbf{H}}(x,1)$ by φ_i^B, where $x \in B_i$ and $x \neq 1$. To conserve notation, we use φ_i in place of φ_i^B if B can be understood from the context. Evidently, $\varphi_0 \subseteq \varphi_1 \subseteq \cdots \subseteq \varphi_{m-1}$ is chain of congruences. By the **length** of the ladder B we mean the length of this chain of congruences. (Notice that it is possible that $\varphi_i = \varphi_j$ even when $i \neq j$, so the length of B might be less than m.) Now let $i < m$ and let ψ_i be a maximal congruence less than φ_i. The existence of ψ_i is ensured (by Zorn's Lemma) since φ_i is principal.

Observe that ψ_i partitions $1/\varphi_i$ and that $(1/\varphi_i)/\psi_i$ is a chief factor of $\mathbf{H}$. Moreover, the elements of B_i must belong to distinct blocks of this partition. Therefore, $|B_i|$ is bounded above by the size of the chief factor.

In this section we establish

Theorem 5. *Let the variety $\mathcal{V}$ be generated by the finite group $\mathbf{G}$, let $\mathbf{H} \in \mathcal{V}$, and let $\langle B_0, B_1, \ldots, B_{m-1}\rangle$ be a ladder of $\mathbf{H}$. Then $|B_0 \cup B_1 \cup \cdots \cup B_{m-1}| \leq |G|$. Thus $|G|$ is an upper bound on the length of any ladder of $\mathbf{H}$. Moreover, $|G|$ also bounds the length of any chain of completely join irreducible elements of $\operatorname{Con}\mathbf{H}$.*

Lemma 1. *Let $\mathbf{H}$ be a group and suppose that $\varphi_0 < \varphi_1 < \cdots < \varphi_{m-1}$ is a chain of completely join irreducible congruences on $\mathbf{H}$. Then $\mathbf{H}$ has a ladder of length m whose principal congruences are precisely the congruences φ_i for $i < m$.*

Proof. For each $i < m$ let ψ_i be the unique congruence covered by φ_i. Since $\varphi_i > \psi_i$, pick b_i so that $\langle b_i, 1\rangle \in \varphi_i$ but $\langle b_i, 1\rangle \notin \psi_i$. Let $B_i = \{1, b_i\}$.

Suppose $i < j < m$. Then $\varphi_i \leq \psi_j < \varphi_j$. This entails that $\langle b_i, 1\rangle \in \psi_j$, and so $b_i \neq b_j$. Consequently, $B_i \cap B_j = \{1\}$.

Observe that if $\langle x, y\rangle \in \varphi_i$ but $\langle x, y\rangle \notin \psi_i$, then $\varphi_i = \mathrm{Cg}^{\mathbf{H}}(x, y)$, since every congruence properly smaller than φ_i must be contained in ψ_i.

Now suppose that $j \leq i < m$ and that $x \in B_i$ and $y \in B_j$ with $1 \neq x \neq y$. Notice that $x = b_i$. Evidently, $\langle x, 1\rangle, \langle y, 1\rangle \in \varphi_i$ and so $\langle x, y\rangle \in \varphi_i$ by transitivity and symmetry. But it is also clear that $\langle x, y\rangle \notin \psi_i$, since if $y = 1$, then $\langle x, y\rangle \notin \psi_i$ by construction, while if $y \neq 1$, then $\langle y, 1\rangle \in \psi_i$ which would force $\langle x, 1\rangle \in \psi_i$ by transitivity, were $\langle x, y\rangle \in \psi_i$. Therefore $\mathrm{Cg}^{\mathbf{H}}(x, y) = \varphi_i$. Now suppose further that $z \in B_k$ with $k \leq i$. Then $\langle z, 1\rangle \in \varphi_k \subseteq \varphi_i = \mathrm{Cg}^{\mathbf{H}}(x, y)$. This verifies property (3) in the definition of ladder. □

Lemma 2. *Let* $\mathbf{G}$ *be a finite group. If* $\mathbf{F} \in \boldsymbol{SPG}$*, then* $|B_0 \cup B_1 \cup \cdots \cup B_{m-1}| \leq |G|$ *for any ladder* $\langle B_0, B_1, \ldots, B_{m-1}\rangle$ *of* $\mathbf{F}$*.*

Proof. Let $\langle B_0, B_1, \ldots, B_{m-1}\rangle$ be a ladder of $\mathbf{F}$. Notice that property (3) of the definition of a ladder entails that $\langle z, 1\rangle \in \mathrm{Cg}^{\mathbf{F}}(x, y)$ whenever $z \in B_0$ and $x, y \in B_0 \cup B_1 \cup \cdots \cup B_{m-1}$ with $x \neq y$.

Pick $z \in B_0$ with $z \neq 1$. Since $\mathbf{F} \in \boldsymbol{SPG}$, there must be a homomorphism $\eta : \mathbf{F} \to \mathbf{G}$ so that $\eta(z) \neq \eta(1^{\mathbf{F}})$. This means that $\langle z, 1\rangle$ does not belong to the kernel of η. In consequence, $\langle x, y\rangle$ does not belong to the kernel of η, whenever $x \neq y$ and $x, y \in B_0 \cup B_1 \cup \cdots \cup B_{m-1}$. That is, η is one-to-one on $B_0 \cup B_1 \cup \cdots \cup B_{m-1}$. Since η maps H into G, we conclude that $|B_0 \cup B_1 \cup \cdots \cup B_{m-1}| \leq |G|$. □

Lemma 3. *Let* $\mathbf{F}$ *be a finite group,* $\theta \in \mathrm{Con}\,\mathbf{F}$*, and set* $\mathbf{H} = \mathbf{F}/\theta$*. Let* $\langle B_0, B_1, \ldots, B_{m-1}\rangle$ *be a ladder of* $\mathbf{H}$*. There is a ladder* $\langle B_0^*, B_1^*, \ldots, B_{m-1}^*\rangle$ *of* $\mathbf{F}$ *such that* $|B_i| = |B_i^*|$ *for each* $i < m$*,* $\theta < \varphi_i^*$*, and* $\varphi_i = \varphi_j$ *if and only if* $\varphi_i^* = \varphi_j^*$ *for all* $i, j < m$*. Here* φ_i *and* φ_i^* *denote the principal congruences associated with* B_i *and* B_i^* *respectively, for* $i < m$*.*

Proof. We use the following claim repeatedly.

Claim 0. *Let* $i < m$ *and* $b \in B_i$ *be any element such that* $b \neq 1^{\mathbf{H}} = 1^{\mathbf{F}}/\theta$*. Let* $v \in b$*. Let* φ^* *denote* $\mathrm{Cg}^{\mathbf{F}}(v, 1)$*. Then* $1/\varphi^* \cap c$ *is nonempty for every* $c \in B_0 \cup B_1 \cup \cdots \cup B_i$*.*

Proof. Because $\langle B_0, B_1, \ldots, B_{m-1}\rangle$ is a ladder we know that $\langle c, 1\rangle \in \mathrm{Cg}^{H}(1, v/\theta)$. By Theorem 3 pick $u \in c$ such that $\langle u, 1\rangle \in \mathrm{Cg}^{\mathbf{F}}(1, v)$. But then $u \in 1/\varphi^*$, therefore $u \in 1/\varphi^* \cap c$ as desired. □

We will devise a one-to-one map δ on $B_0 \cup B_1 \cup \cdots \cup B_{m-1}$ so that $\langle B_0^*, B_1^*, \ldots, B_{m-1}^*\rangle$ is a ladder of $\mathbf{F}$, where B_i^* is the image of B_i with respect to δ, for every $i < m$. We begin with B_{m-1}. Let b_{m-1} be any element of B_{m-1} other than $1^{\mathbf{H}}$. Using the finiteness of $\mathbf{F}$ pick $u_{m-1} \in b_{m-1}$ so that $\mathrm{Cg}^{\mathbf{F}}(u_{m-1}, 1)$ is minimal. Let $\varphi_{m-1}^* = \mathrm{Cg}^{\mathbf{F}}(u_{m-1}, 1)$. Now suppose that $b_{m-1}, b_{m-2}, \ldots, b_i$ and $u_{m-1}, u_{m-2}, \ldots, u_i$ have been chosen and $\varphi_{m-1}^*, \varphi_{m-2}^*, \ldots, \varphi_i^*$ have been defined so that for all j with $i \leq j < m$

(1) u_j is chosen from $1/\varphi_{j+1}^* \cap b_j$ so that $\mathrm{Cg}^{\mathbf{F}}(u_j, 1)$ is minimal,
(2) $\varphi_j^* = \mathrm{Cg}^{\mathbf{F}}(u_j, 1)$

To get the next lowest stage of the construction, pick $b_{i-1} \in B_{i-1}$ with $b_{i-1} \neq 1^{\mathbf{H}}$. Pick $u_{i-1} \in 1/\varphi_i^* \cap b_{i-1}$ so that $\mathrm{Cg}^{\mathbf{F}}(u_{i-1}, 1)$ is minimal.

Evidently, for $i < j < m$ we have $\theta < \varphi_i^* \leq \varphi_j^*$.

Here is how to define δ on B_i: put $\delta(1^{\mathbf{H}}) = 1^{\mathbf{F}}$, and for each $c \in B_i$ with $c \neq 1^{\mathbf{H}}$ let $\delta(c)$ be any element of $1/\varphi_i^* \cap c$. The map δ is one-to-one since the members of each B_i are disjoint, being congruence classes. Let B_i^* be the image under δ of B_i.

Observe that for each $i < m$ we have $|B_i^*| = |B_i|$, so each B_i^* is a finite subset of F with at least two elements. We also have $1^{\mathbf{F}} \in B_i^*$. So conditions (1) and (2) of the definition of a ladder are secure at this point.

Claim 1. *Let $j \leq i < m$ and let $x \in B_i^*$ and $y \in B_j^*$ with $1 \neq x \neq y$. Then $\mathrm{Cg}^{\mathbf{F}}(x,y) = \mathrm{Cg}^{\mathbf{F}}(u_i, 1)$.*

Proof. First, observe that $\mathrm{Cg}^{\mathbf{F}}(x,y) \subseteq \mathrm{Cg}^{\mathbf{F}}(u_i,1) = \varphi_i^*$ since δ maps $B_0 \cup \cdots \cup B_i$ into the single congruence class $1/\varphi_i^*$.

Notice that $x/\theta \in B_i$ is the preimage of x under δ. Likewise, $y/\theta \in B_j$ is the preimage of y. Since $1 \neq x \neq y$ we have that $1/\theta \neq x/\theta \neq y/\theta$. By property (3) of ladders we see that $\langle 1, u_i/\theta\rangle \in \mathrm{Cg}^{\mathbf{H}}(x/\theta, y/\theta)$. By Theorem 3 pick $u \in u_i/\theta$ so that $\langle 1, u\rangle \in \mathrm{Cg}^{\mathbf{F}}(x,y) \subseteq \mathrm{Cg}^{\mathbf{F}}(u_i,1)$. By the minimality in the choice of u_i, we conclude that $\mathrm{Cg}^{\mathbf{F}}(u,1) = \mathrm{Cg}^{\mathbf{F}}(u_i,1)$. Therefore $\mathrm{Cg}^{\mathbf{F}}(x,y) = \mathrm{Cg}^{\mathbf{F}}(u_i,1)$ as desired. □

For property (3) let $j,k \leq i < m$ and pick $x \in B_i^*, y \in B_j^*$, and $z \in B_k^*$ with $1 \neq x \neq y$. Now by Claim 1 we have both $\mathrm{Cg}^{\mathbf{F}}(x,y) = \varphi_i^*$ and $\langle z, 1\rangle \in \varphi_k^*$. Since we already know by construction that $\varphi_k^* \subseteq \varphi_i^*$, we conclude $\langle z,1\rangle \in \mathrm{Cg}^{\mathbf{F}}(x,y)$, as desired.

Claim 2. *$\varphi_i = \varphi_j$ if and only if $\varphi_i^* = \varphi_j^*$ for all $i < j < m$.*

Proof. Suppose first that $\varphi_i = \varphi_j$. This means $\mathrm{Cg}^{\mathbf{H}}(u_i/\theta, 1/\theta) = \mathrm{Cg}^{\mathbf{H}}(u_j/\theta, 1/\theta)$. So by Theorem 3 there is $u \in F$ so that $u_j/\theta = u/\theta$ and $\langle u, 1\rangle \in \mathrm{Cg}^{\mathbf{F}}(u_i,1)$. So

$$\mathrm{Cg}^{\mathbf{F}}(u,1) \subseteq \mathrm{Cg}^{\mathbf{F}}(u_i,1) \subseteq \mathrm{Cg}^{\mathbf{F}}(u_j,1).$$

By the minimality in the choice of u_j, we conclude that $\mathrm{Cg}^{\mathbf{F}}(u_i,1) = \mathrm{Cg}^{\mathbf{F}}(u_j,1)$. This means that $\varphi_i^* = \varphi_j^*$.

For the reverse inlcusion, suppose that $\varphi_i^* = \varphi_j^*$. So there is a conjufgate product polynomial of $\mathbf{F}$ which witnesses $\langle u_j, 1\rangle \in \mathrm{Cg}^{\mathbf{F}}(u_i,1)$. The image of this polynomial in $\mathbf{H}$ witnesses $\langle u_j/\theta, 1/\theta\rangle \in \mathrm{Cg}^{\mathbf{H}}(u_i/\theta, 1/\theta)$. So $\varphi_j \subseteq \varphi_i$. Since we already have $\varphi_i \subseteq \varphi_j$, we conclude that $\varphi_i = \varphi_j$ as desired. □

□

Proof of Theorem 5. Let $\mathbf{H}$ belong to the variety $\mathcal{V}$ generated by the finite group $\mathbf{G}$. Suppose that $\mathbf{H}$ has a chain of length m of completely join irreducible congruences. By Lemma 1 pick a ladder $\langle B_0, B_1, \ldots, B_{m-1}\rangle$ of length m for $\mathbf{H}$. Each B_i is a finite set, so by condition (3) of the definition of ladders pick a finite subset C of H such that there are polynomials witnessing (3) that have coefficients only from C. Let $\overline{\mathbf{H}}$ be the subalgebra of $\mathbf{H}$ generated by $C \cup B_0 \cup B_1 \cup \cdots \cup B_{m-1}$. Then $\overline{\mathbf{H}}$ is finite, since $\mathcal{V}$ is locally finite, and $\langle B_0, B_1, \ldots, B_{m-1}\rangle$ is a ladder of $\overline{\mathbf{H}}$.

By the HSP Theorem, pick a natural number n, a subalgebra $\mathbf{F}$ of $\mathbf{G}^n$, and a congruence $\theta \in \mathrm{Con}\,\mathbf{F}$ so that $\overline{\mathbf{H}} \cong \mathbf{F}/\theta$. Indeed, we make the harmless assumption that $\overline{\mathbf{H}} = \mathbf{F}/\theta$.

Now by Lemma 3, $\langle B_0^*, B_1^*, \ldots, B_{m-1}^*\rangle$ is a ladder of $\mathbf{F} \in \boldsymbol{SP}\mathbf{G}$ with the same length as $\langle B_0, B_1, \ldots, B_{m-1}\rangle$. Indeed, $|B_0^* \cup \cdots \cup B_{m-1}^*| = |B_0 \cup \cdots \cup B_{m-1}|$ in view of stipulation (2) in the definition of ladder. According to Lemma 2, $|G|$ is an upper bound on this cardinality. It follows that $|G|$ is an upper bound on the length of any ladder of $\mathbf{H}$ as well as an upper bound on the length of any chain of completely join irreducible members of $\mathrm{Con}\,\mathbf{H}$. This completes the proof of Theorem 5. □

6. Reducing the Ladder Height

Let $\mathbf{H}$ be any group and $a \in H$. The **ladder height** of a is the least upper bound on the lengths of ladders all of whose principal congruences are included in $\mathrm{Cg}^{\mathbf{H}}(a,1)$. We will say that such ladders are **below** a. We will denote the ladder height of a in $\mathbf{H}$ by $\rho^{\mathbf{H}}(a)$. Notice that the ladder height of 1 is 0.

Lemma 4. *Let $\mathbf{A}$ be a subdirectly irreducible group and let $a \in A$ with $\rho^{\mathbf{A}}(a) = n$. If $\langle B_0, B_1, \ldots, B_{n-1}\rangle$ is a ladder of length n below a, then φ_0, the principal congruence associated with B_0, is the monolith of $\mathbf{A}$.*

Proof. Suppose that φ_0 is not the monolith. Pick $b \in A$ so that $\langle b, 1\rangle$ is a critical pair. Then $b \notin B_i$ for any $i < m$. Let $M = \{b, 1\}$. It is straightforward to check that $\langle M, B_0, B_1, \ldots, B_{n-1}\rangle$ is a ladder below a. But this ladder has length $n+1$, contradicting the ladder height of a. □

Corollary 6. *Let* $\mathbf{A}$ *be a subdirectly irreducible group and let* $b \in A$*. If* b *has ladder height* 1*, then* $\langle b, 1\rangle$ *is a critical pair.*

Proof. Let $\langle M\rangle$ be a ladder below b. The principal congruence associated with M is the monolith μ. In the case that $b \in M$, we have $\mathrm{Cg}^{\mathbf{A}}(b, 1) = \mu$. In the case that $b \notin M$ it follows easily that $\langle M, \{b, 1\}\rangle$ is also a ladder below b. Since b has ladder height 1, we also have $\mathrm{Cg}^{\mathbf{A}}(b, 1) = \mu$. Therefore, $\langle b, 1\rangle$ is critical. □

In this section our chief task is to prove the following theorem.

Theorem 7. *Let* $\mathbf{G}$ *be a finite group and let* $\mathcal{V}$ *be the variety generated by* $\mathbf{G}$*. There is a finite bound* n *such that for any* $\mathbf{A} \in \mathcal{V}$ *and any* $a \in A$ *with* $\rho^{\mathbf{A}}(a) > 1$*, there is* $b \in A$ *with* $b \neq 1$ *and* $\rho^{\mathbf{A}}(b) < \rho^{\mathbf{A}}(a)$ *such that there is a conjugate product polynomial of complexity no more than* n *which witnesses* $\langle b, 1\rangle \in \mathrm{Cg}^{\mathbf{A}}(a, 1)$*.*

To prove this theorem, we need a version of it for the subdirectly irreducible members of $\mathcal{V}$.

Theorem 8. *Let* $\mathcal{V}$ *be a locally finite variety of groups with finite exponent* e *such that the cardinalities of the chief factors in* $\mathcal{V}$ *have a finite upper bound* r*. Then there is a finite upper bound* n *such that for every subdirectly irreducible group* $\mathbf{F} \in \mathcal{V}$ *and every* $a \in F$ *with* $\rho^{\mathbf{F}}(a) = 2$*, there is* $b \neq 1$ *with* $\langle b, 1\rangle$ *in the monolith of* $\mathbf{F}$ *and there is a conjugate product polynomial of complexity no more than* n *which witnesses that* $\langle b, 1\rangle \in \mathrm{Cg}^{\mathbf{F}}(a, 1)$*.*

First we argue that it is enough to restrict our attention to the finite subdirectly irreducible algebras in $\mathcal{V}$.

Lemma 5. *Let* $\mathcal{V}$ *be a locally finite variety of groups such that the cardinalities of the chief factors in* $\mathcal{V}$ *have a finite upper bound* r*. Suppose* n' *is a finite upper bound such that for every finite subdirectly irreducible group* $\mathbf{H} \in \mathcal{V}$*, every* $a \in H$ *with* $a \neq 1$ *and* $\rho^{\mathbf{H}}(a) < 2r$*, and there is* $b \neq 1$ *with* $\langle b, 1\rangle$ *in the monolith of* $\mathbf{H}$ *such that there is a conjugate product polynomial of complexity no more than* n' *which witnesses that* $\langle b, 1\rangle \in \mathrm{Cg}^{\mathbf{H}}(a, 1)$*. Then there is a finite upper bound* n *such that for every subdirectly irreducible group* $\mathbf{F} \in \mathcal{V}$*, every* $a \in F$ *with* $a \neq 1$ *and* $\rho^{\mathbf{F}}(a) = 2$*, and every* $b \in F$ *with* $b \neq 1$ *and* $\langle b, 1\rangle$ *in the monolith of* $\mathbf{F}$*, there is a conjugate product polynomial of complexity no more than* n *which witnesses that* $\langle b, 1\rangle \in \mathrm{Cg}^{\mathbf{F}}(a, 1)$*.*

Proof. Let $\mathbf{F}$ be a subdirectly irreducible algebra in $\mathcal{V}$ and let $a \in F$ with $a \neq 1$ have ladder height $\rho^{\mathbf{F}}(a) = 2$. Let μ be the monolith of $\mathbf{F}$. Let $\langle M, N\rangle$ be a ladder that witnesses $\rho^{\mathbf{F}}(a)$. Clearly $\mu \leq \varphi$ where φ is the principal congruence associated with M. Were $\mu < \varphi$ then $\langle 1/\mu, M, N\rangle$ would also be a ladder that would force $\rho^{\mathbf{F}}(a)$ to be too big. Therefore, $\mu = \varphi$ and it is harmless to suppose that $M = 1/\mu$. Moreover, we know that $|M|, |N| \leq r$. Further we suppose that N has been chosen so that $|M \cup N|$ is as large as possible. Plainly, $|M \cup N| < 2r$.

By a **membership condition** for $M \cup N \cup \{a\}$ holding over $\mathbf{F}$ we mean a condition of the form $\langle x, y\rangle \in \mathrm{Cg}^{\mathbf{F}}(u, v)$ where $x, y, u, v \in M \cup N \cup \{a\}$. There can be at most $16r^4$ membership conditions.

Pick $p \in M$ and $q \in N$ with $p \neq 1 \neq q$.

For each membership condition for $M \cup N \cup \{a\}$ holding over $\mathbf{F}$, select a polynomial to witness it. Let C be the set of coefficients occurring in these polynomials. C is finite. Let $\mathbf{F}'$ be the subalgebra of $\mathbf{F}$ generated by $C \cup M \cup N \cup \{a\}$. Notice that $\mathbf{F}'$ is finite since $\mathcal{V}$ is locally finite. Now $\langle M, N\rangle$ is a ladder below a for $\mathbf{F}'$ because all the relevant membership conditions have been witnessed over $\mathbf{F}'$.

Let λ be a maximal congruence of $\mathbf{F}'$ subject to the stipulations that $\langle p, 1\rangle \in \lambda$ and that λ separates q and 1. Since $\langle p, 1\rangle \in \mathrm{Cg}^{\mathbf{F}'}(q, 1)$, we see that $\mathbf{F}'/\lambda$ is a finite subdirectly irreducible algebra, that λ collapses M, and that λ separates every pair of distinct elements of N. Moreover, for $d, e \in N$ with $d \neq e$, we know that $\langle d/\lambda, e/\lambda\rangle$ is a critical pair of $\mathbf{F}'/\lambda$.

Claim 3. $\langle a/\lambda, 1/\lambda\rangle$ *is a critical pair of* $\mathbf{F}'/\lambda$*.*

Proof. Suppose not. Let ν denote the monolith of $\mathbf{F}'/\lambda$ and let α denote $\mathrm{Cg}^{\mathbf{F}'/\lambda}(a/\lambda, 1/\lambda)$. Then $\nu < \alpha$. There must be a join irreducible congruence β with $\nu < \beta \leq \alpha$. By Lemma 1 there is a ladder $\langle N', D' \rangle$ of length 2 whose principal congruences are, respectively ν and β, and $|N| \leq |N'|$. By Lemma 3 there is a ladder $\langle N^*, D^* \rangle$ of length 2 below a in $\mathbf{F}'$ with $|N'| = |N^*|$. Moreover, $M \cap N^* = \{1\}$ since λ collapses M. It follows that $\langle M, N^*, D^* \rangle$ is a ladder for $\mathbf{F}$ below a. But this is impossible, since $|M \cup N| < |M \cup N^* \cup D^*|$. □

This means that a/λ and b/λ for each $b \in N$ all belong to the normal subgroup of $\mathbf{F}'/\lambda$ determined by the monolith ν. This normal subgroup has cardinality bounded above by r. So by Lemma 0, all the congruence membership conditions for $N/\lambda \cup \{a/\lambda\}$ which hold over $\mathbf{F}'/\lambda$ can be witnessed by polynomials of complexity bounded by $4r+1$. Let $E \subseteq F'/\lambda$ be the set of coefficients from these polynomials. Then $|E|$ is bounded by $4r+1$. Let $E' \subseteq F'$ be a set consisting of one element from each member of E. Let $\mathbf{F}''$ be the subgroup of $\mathbf{F}'$ generated $E' \cup M \cup N \cup \{a\}$. The size of this group is bounded only in terms of $\mathcal{V}$.

Now pick $\overline{a} \in a/\lambda$ such that $\langle \overline{a}, 1 \rangle \in \mathrm{Cg}^{\mathbf{F}''}(a, 1)$ with $\mathrm{Cg}^{\mathbf{F}''}(\overline{a}, 1)$ minimal subject to these restrictions.

In view of Theorem 3 pick $\overline{q} \in q/\lambda$ such that $\langle \overline{q}, 1 \rangle \in \mathrm{Cg}^{\mathbf{F}''}(\overline{a}, 1)$ with $\mathrm{Cg}^{\mathbf{F}''}(\overline{q}, 1)$ minimal subject to these restrictions.

Again using Theorem 3, for each $d \in N - \{q, 1\}$ pick $\overline{d} \in d/\lambda$ such that $\langle \overline{d}, 1 \rangle \in \mathrm{Cg}^{\mathbf{F}''}(\overline{q}, 1)$. Set $\overline{1} = 1$. Let $\overline{N}$ denote $\{\overline{d} \mid d \in N\}$.

Claim 4. *Let $d, e \in N$ with $d \neq e$. Then $\mathrm{Cg}^{\mathbf{F}''}(\overline{d}, \overline{e}) = \mathrm{Cg}^{\mathbf{F}''}(\overline{q}, 1)$.*

Proof. By construction we know that $\langle \overline{d}, 1 \rangle, \langle 1, \overline{e} \rangle \in \mathrm{Cg}^{\mathbf{F}''}(\overline{q}, 1)$. By transitivity we get $\langle \overline{d}, \overline{e} \rangle \in \mathrm{Cg}^{\mathbf{F}''}(\overline{q}, 1)$. This yields $\mathrm{Cg}^{\mathbf{F}''}(\overline{d}, \overline{e}) \subseteq \mathrm{Cg}^{\mathbf{F}''}(\overline{q}, 1)$. But

$$\langle q/\lambda, 1/\lambda \rangle \in \mathrm{Cg}^{\mathbf{F}''/\lambda}(d/\lambda, e/\lambda).$$

Consequently, there is $w \in F''$ so that $w \in q/\lambda$ and $\langle w, 1 \rangle \in \mathrm{Cg}^{\mathbf{F}''}(\overline{d}, \overline{e}) \subseteq \mathrm{Cg}^{\mathbf{F}''}(\overline{q}, 1) \subseteq \mathrm{Cg}^{\mathbf{F}''}(\overline{a}, 1)$. By the minimality in the choice of $\overline{q}$, we conclude that $\mathrm{Cg}^{\mathbf{F}''}(w, 1) = \mathrm{Cg}^{\mathbf{F}''}(\overline{d}, \overline{e}) = \mathrm{Cg}^{\mathbf{F}''}(\overline{q}, 1)$.

□

By construction, $\langle \overline{q}, 1 \rangle \in \mathrm{Cg}^{\mathbf{F}''}(\overline{a}, 1) \subseteq \mathrm{Cg}^{\mathbf{F}''}(a, 1)$. In view of Claim 4, this means that $\langle \overline{N} \rangle$ is a ladder below a in $\mathbf{F}''$. Because $|F''|$ is bounded only in terms of $\mathcal{V}$, the complexity of the polynomials witnessing the membership conditions for $\overline{N} \cup \{a\}$ are also bounded only in terms of $\mathcal{V}$. Observe that $M \cap \overline{N} = \{1\}$ since λ collapses M. This means that $\langle M, \overline{N} \rangle$ is a ladder below a in $\mathbf{F}$. We also have $|M \cup N| = |M \cup \overline{N}|$ is the maximum size among ladders below a. Moreover, the membership conditions for $\overline{N} \cup \{a\}$ relevant to the notion of ladder still have the same polynomials as witnesses over $\mathbf{F}$.

Now we repeat this process, focussing on M in place of N.

For each membership condition for $M \cup \overline{N} \cup \{a\}$ in $\mathbf{F}$ chose a polynomial of least complexity as a witness. In particular, all the witnesses of $\overline{N} \cup \{a\}$ have complexity bounded in terms only of $\mathcal{V}$. Let K be the set of coefficients occurring in these polynomials. Let $\mathbf{G}'$ be the subgroup of $\mathbf{F}$ generated by $K \cup M \cup \overline{N} \cup \{a\}$. Let θ be a maximal congruence of $\mathbf{G}'$ separating p and 1. Then $\mathbf{G}'/\theta$ is a finite subdirectly irreducible group, θ separates any pair of distinct elements from $M \cup \overline{N} \cup \{a\}$, and for any $c, d \in M$ with $c \neq d$, we know that $\langle c/\theta, d/\theta \rangle$ is critical.

The following hold

(1) $\langle c/\theta, 1/\theta \rangle \in \mathrm{Cg}^{\mathbf{G}'/\theta}(d/\theta, e/\theta)$ for all $c, d, e \in M$ with $d \neq e$.
(2) $\langle c/\theta, 1/\theta \rangle \in \mathrm{Cg}^{\mathbf{G}'/\theta}(\overline{q}/\theta, d/\theta)$ for all $c, d \in M$.

According to Lemma 0, the membership conditions that fall under (1) above can be witnessed by polynomials whose complexity is bounded $4r+1$, since $c/\theta, d/\theta$, and e/θ all belong to the normal subgroup associated with the monolith of $\mathbf{G}'/\theta$, and this is of cardinality bounded by r.

For the membership conditions that fall under (2) above, we contend that $\rho^{\mathbf{G}'/\theta}(\overline{q}d^{-1}/\theta) < 2r$. Otherwise, there would be a ladder of length $2r$ below $\langle \overline{q}/\theta, d/\theta \rangle$. Using Lemma 3 we could obtain a ladder of length $2r$

below $\langle \overline{q}, d\rangle$ in $\mathbf{G}'$. The size of this ladder would be at least $2r+1$. Notice that this system is also a ladder in $\mathbf{F}$ and it is below a. This is impossible, and our contension holds. But this entails, by our main hypothesis, that the membership conditions in (2) above can be witnessed by polynomials of complexity bounded only in terms of $\mathcal{V}$.

Let $J \subseteq G'/\theta$ be the set of coefficients from these least complex polynomials witnessing the membership conditions (1) and (2). Then $|J|$ is bounded only in terms of $\mathcal{V}$. Let J' consist of one element from each member of J together with the elements needed to witness that $\langle \overline{N}\rangle$ is a ladder below a in $\mathbf{G}'$. Observe that $|J'|$ is bounded in terms of $\mathcal{V}$. Let $\mathbf{G}''$ be the subgroup of $\mathbf{G}'$ generated by $J' \cup M \cup \overline{N} \cup \{a\}$. The size of this group is bounded only in terms of $\mathcal{V}$. We abuse notation by using θ to denote $\theta \cap (G'' \times G'')$. Then the following hold:

(1') $\langle c/\theta, 1/\theta\rangle \in \mathrm{Cg}^{\mathbf{G}''/\theta}(d/\theta, e/\theta)$ for all $c, d, e \in M$ with $d \neq e$.

(2') $\langle c/\theta, 1/\theta\rangle \in \mathrm{Cg}^{\mathbf{G}''/\theta}(\overline{q}/\theta, d/\theta)$ for all $c, d \in M$.

Now pick $\hat{a} \in a/\theta$ such that $\langle \hat{a}, 1\rangle \in \mathrm{Cg}^{\mathbf{G}''}(a, 1)$ and $\mathrm{Cg}^{\mathbf{G}''}(\hat{a}, 1)$ is minimal subject to these restrictions.

In view of Theorem 3, we can make the following choices.

Pick $\hat{q} \in \overline{q}/\theta$ such that $\langle \hat{q}, 1\rangle \in \mathrm{Cg}^{\mathbf{G}''}(\overline{q}, 1)$ and $\mathrm{Cg}^{\mathbf{G}''}(\hat{q}, 1)$ is minimal subject to these restrictions.

Pick $\hat{p} \in p/\theta$ such that $\langle \hat{p}, 1\rangle \in \mathrm{Cg}^{\mathbf{G}''}(\hat{q}, 1)$ and $\mathrm{Cg}^{\mathbf{G}''}(\hat{p}, 1)$ is minimal subject to these restrictions.

For each $d \in N - \{q, 1\}$ pick $\hat{d} \in \overline{d}/\theta$ such that $\langle \hat{d}, 1\rangle \in \mathrm{Cg}^{\mathbf{G}''}(\hat{q}, 1)$. Set $\hat{1} = 1$.

For each $c \in M - \{p, 1\}$ pick $\hat{c} \in c/\theta$ such that $\langle \hat{c}, 1\rangle \in \mathrm{Cg}^{\mathbf{G}''}(\hat{p}, 1)$.

Finally, let $\hat{M} = \{\hat{c} \mid c \in M\}$ and $\hat{N} = \{\hat{d} \mid d \in N\}$. The next claims establish that $\langle \hat{M}, \hat{N}\rangle$ is a ladder below a in $\mathbf{G}''$.

Claim 5. *Let $b, c \in M$ with $b \neq c$. Then $\mathrm{Cg}^{\mathbf{G}''}(\hat{b}, \hat{c}) = \mathrm{Cg}^{\mathbf{G}''}(\hat{p}, 1)$. Let $d, e \in N$ with $d \neq e$. Then $\mathrm{Cg}^{\mathbf{G}''}(\hat{d}, \hat{e}) = \mathrm{Cg}^{\mathbf{G}''}(\hat{q}, 1)$.*

Proof. By construction $\langle \hat{b}, 1\rangle, \langle 1, \hat{c}\rangle \in \mathrm{Cg}^{\mathbf{G}''}(\hat{p}, 1)$. By transitivity,$\langle \hat{b}, \hat{c}\rangle \in \mathrm{Cg}^{\mathbf{G}''}(\hat{p}, 1)$ and consequently $\mathrm{Cg}^{\mathbf{G}''}(\hat{b}, \hat{c}) \subseteq \mathrm{Cg}^{\mathbf{G}''}(\hat{p}, 1)$. But

$$\langle p/\theta, 1/\theta\rangle \in \mathrm{Cg}^{\mathbf{G}''/\theta}(b/\theta, c/\theta).$$

Therefore,by Theorem 3, there is $u \in G''$ so that $u \in p/\theta$ and $\langle u, 1\rangle \in \mathrm{Cg}^{\mathbf{G}''}(\hat{b}, \hat{c}) \subseteq \mathrm{Cg}^{\mathbf{G}''}(\hat{p}, 1) \subseteq \mathrm{Cg}^{\mathbf{G}''}(\hat{q}, 1)$. By the minimality in the choice of $\hat{p}$, we conclude $\mathrm{Cg}^{\mathbf{G}''}(u, 1) = \mathrm{Cg}^{\mathbf{G}''}(\hat{b}, \hat{c}) = \mathrm{Cg}^{\mathbf{G}''}(\hat{p}, 1)$.

A similar argument prevails to establish the other part of the claim.

□

Claim 6. *Let $b \in M$. Then $\mathrm{Cg}^{\mathbf{G}''}(\hat{q}, \hat{b}) = \mathrm{Cg}^{\mathbf{G}''}(\hat{q}, 1)$.*

Proof. By construction $\langle 1, \hat{b}\rangle \in \mathrm{Cg}^{\mathbf{G}''}(\hat{q}, 1)$. It is evident that $\langle \hat{q}, 1\rangle \in \mathrm{Cg}^{\mathbf{G}''}(\hat{q}, 1)$. So by transitivity, $\langle \hat{q}, \hat{b}\rangle \in \mathrm{Cg}^{\mathbf{G}''}(\hat{q}, 1)$. But

$$\langle q/\theta, 1/\theta\rangle \in \mathrm{Cg}^{\mathbf{G}''/\theta}(q/\theta, b/\theta).$$

Therefore,again using Theorem 3, there is $u \in G''$ so that $u \in q/\theta$ and $\langle u, 1\rangle \in \mathrm{Cg}^{\mathbf{G}''}(\hat{q}, \hat{b}) \subseteq \mathrm{Cg}^{\mathbf{G}''}(\hat{q}, 1) \subseteq \mathrm{Cg}^{\mathbf{G}''}(\hat{a}, 1)$. By the minimality in the choice of $\hat{q}$, we conclude $\mathrm{Cg}^{\mathbf{G}''}(q, 1) = \mathrm{Cg}^{\mathbf{G}''}(\hat{q}, \hat{b}) = \mathrm{Cg}^{\mathbf{G}''}(\hat{q}, 1)$.

□

Since $\langle \hat{p}, 1\rangle$ is below $\langle \hat{q}, 1\rangle$ which is below $\langle \hat{a}, 1\rangle$ which is below $\langle a, 1\rangle$, it follows from the last two claims that $\langle \hat{M}, \hat{N}\rangle$ is a ladder below a in $\mathbf{G}''$. Since $|G''|$ is bounded in terms only of $\mathcal{V}$, it follows that all the membership conditions relevant to establishing that this is a ladder below a can be witnessed by polynomials of complexity bounded in terms of $\mathcal{V}$ only. Of course, $\langle \hat{M}, \hat{N}\rangle$ is a ladder below a in $\mathbf{F}$ and $|\hat{M} \cup \hat{N}| = |M \cup N|$. But then it follows that $\hat{M}$ must be $1/\mu$, where μ is the monolith of $\mathbf{F}$. That is $\hat{M} = M$. But this means that $\langle b, 1\rangle \in \mathrm{Cg}^{\mathbf{F}}(a, 1)$ can be witnessed by a polynomial of complexity bound in terms of $\mathcal{V}$ only, not matter how b is chosen from M.

□

Lemma 6. *Let $\mathcal{V}$ be a locally finite variety of groups such that the cardinalities of the chief factors in $\mathcal{V}$ have a finite upper bound r.*

(1) Suppose that n'' is a finite upper bound such that for every subdirectly irreducible group $\mathbf{H} \in \mathcal{V}$, every $a \in H$ with $\rho^{\mathbf{H}}(a) = 2$, there is $b \neq 1$ with $\langle b, 1\rangle$ in the monolith of $\mathbf{H}$ such that there is a polynomial of complexity no more than n'' which witnesses that $\langle b, 1\rangle \in \mathrm{Cg}^{\mathbf{H}}(a, 1)$. Then there is a finite upper bound n such that for every $\mathbf{A} \in \mathcal{V}$ and every $a \in A$ with $\rho^{\mathbf{A}}(a) > 1$, there is $b \in A$ with $b \neq 1$ and $\rho^{\mathbf{A}}(b) < \rho^{\mathbf{A}}(a)$ such that there is a polynomial of complexity no more than n which witnesses that $\langle b, 1\rangle \in \mathrm{Cg}^{\mathbf{H}}(a, 1)$.

(2) Suppose that n'' is a finite upper bound such that for every finite subdirectly irreducible group $\mathbf{H} \in \mathcal{V}$, every $a \in H$ with $\rho^{\mathbf{H}}(a) = 2$, there is $b \neq 1$ with $\langle b, 1\rangle$ in the monolith of $\mathbf{H}$ such that there is a polynomial of complexity no more than n'' which witnesses that $\langle b, 1\rangle \in \mathrm{Cg}^{\mathbf{H}}(a, 1)$. Then there is a finite upper bound n such that for every finite $\mathbf{A} \in \mathcal{V}$ and every $a \in A$ with $\rho^{\mathbf{A}}(a) > 1$, there is $b \in A$ with $b \neq 1$ and $\rho^{\mathbf{A}}(b) < \rho^{\mathbf{A}}(a)$ such that there is a polynomial of complexity no more than n which witnesses that $\langle b, 1\rangle \in \mathrm{Cg}^{\mathbf{H}}(a, 1)$.

Proof. We provide a proof for (1). Then (2) follows by noting the appropriate finiteness conditions can be inserted into the proof for (1). Suppose that $a \in A$ with $\rho^{\mathbf{A}}(a) = m > 1$. Select a ladder $\langle B_0, B_1, \ldots, B_{m-1}\rangle$ of length m below a so that $|B_0 \cup B_1 \cup \cdots \cup B_{m-1}|$ has the largest possible value. (Notice this cardinality is bounded above by mr.) Let $\varphi_0 < \varphi_1 < \cdots < \varphi_{m-1}$ be the chain of associated principal congruences.

Let $\theta \in \mathrm{Con}\,\mathbf{A}$ be maximal subject to the restrictions that $\varphi_{m-3} \subseteq \theta < \varphi_{m-2}$. Then $\mathbf{A}/\theta$ is subdirectly irreducible, since φ_{m-2} is principal.

Claim 7. *a/θ has ladder height 2 in $\mathbf{A}/\theta$.*

Proof. Certainly, $\langle B_{m-2}/\theta, B_{m-1}/\theta\rangle$ is a ladder of length 2 below a/θ in $\mathbf{A}/\theta$. So for the sake of contradiction, suppose that there is a ladder of length 3 below a/θ. Let $0 < \psi_0 < \psi_1 < \psi_2$ be the associated principal congruences. By Lemma 3 there is a ladder $\langle C_0, C_1, C_2\rangle$ below a in $\mathbf{A}$ with associated principal congruences $\theta < \psi_0' < \psi_1' < \psi_2'$. Moreover, since $\varphi_{m-3} \subseteq \theta$, we conclude that $\langle B_0, B_1, \ldots, B_{m-3}, C_0, C_1, C_2\rangle$ is ladder of length $m + 1$ beneath a, contrary to our assumption about the ladder height of a. □

Let $\langle M, N\rangle$ be a ladder of length 2 below a/θ. By Lemma 3, let $\langle M^*, N^*\rangle$ be a corresponding ladder below a for $\mathbf{A}$. Then we know that

- $\langle B_0, B_1, \ldots, B_{m-3}, M^*, N^*\rangle$ is a ladder of length m below a for $\mathbf{A}$.
- $M = M^*/\theta$ with $|M| = |M^*|$ and $N = N^*/\theta$ with $|N| = |N^*|$.

It follows, in particular, that every member of M^* has ladder height in $\mathbf{A}$ strictly less than the ladder height of a.

Notice that M is collapsed by the monolith of $\mathbf{A}/\theta$. So there is an upper bound, depending only on $\mathcal{V}$, on complexity of the polynomials needed to witness all the membership conditions of the form $\langle b/\theta, c/\theta\rangle \in \mathrm{Cg}^{\mathbf{A}/\theta}(d/\theta, e/\theta)$ and $\langle b/\theta, 1/\theta\rangle \in \mathrm{Cg}^{\mathbf{A}/\theta}(a/\theta, 1/\theta)$ for $b, c, d, e \in M^*$ with $d \neq e$. Let D be the set of all coefficients occurring in these polynomials. Let $\mathbf{A}''$ be the subgroup of $\mathbf{A}$ generated by $D \cup M^* \cup \{a\}$. Letting θ stand for its restriction to A'', we see that $\langle b/\theta, 1/\theta\rangle \in \mathrm{Cg}^{\mathbf{A}''/\theta}(a/\theta, 1/\theta)$, for each $b \in M^*$. Fix $b \in M^*$ with $b \neq 1$. Using Theorem 3, pick $\overline{b}$ so that $\langle \overline{b}, b\rangle \in \theta$ with $\overline{b} \neq 1$ and $\langle \overline{b}, 1\rangle \in \mathrm{Cg}^{\mathbf{A}''}(a, 1)$. Since the cardinality of $\mathbf{A}''$ is bounded in terms of $\mathcal{V}$ alone, we see that there is an upper bound n on the complexity of the polynomial needed to witness $\langle \overline{b}, 1\rangle \in \mathrm{Cg}^{\mathbf{A}}(a, 1)$.

The proof will be complete once we establish that $\rho^{\mathbf{A}}(\overline{b}) < m = \rho^{\mathbf{A}}(a)$. But let φ^* be the principal congruence of $\mathbf{A}$ associated with M^*. We know that $\theta < \varphi^*$ and that $\varphi^* = \mathrm{Cg}^{\mathbf{A}}(b, 1)$. This entails that $\langle \overline{b}, b\rangle, \langle b, 1\rangle \in \mathrm{Cg}^{\mathbf{A}}(b, 1)$. By transitivity, $\langle \overline{b}, 1\rangle \in \mathrm{Cg}^{\mathbf{A}}(b, 1)$. This means that $\rho^{\mathbf{A}}(\overline{b}) \leq \rho^{\mathbf{A}}(b) < m$. □

Only one piece of the argument for the proofs of Theorem 7 and Theorem 8 remains. It is addressed in the next lemma.

Lemma 7. *Let $\mathcal{V}$ be a locally finite variety of groups of finite exponent e such that the cardinalities of the chief factors in $\mathcal{V}$ have a finite upper bound r. Then there is a finite upper bound n such that for every finite subdirectly irreducible group $\mathbf{F} \in \mathcal{V}$ and every $a \in F$ with $\rho^{\mathbf{F}}(a) = 2$, there is $b \in F$ with $b \neq 1$ such that $\langle b, 1\rangle$ is a critical pair for $\mathbf{F}$ and $\langle b, 1\rangle \in \mathrm{Cg}^{\mathbf{F}}(a, 1)$ can be witnessed by a polynomial of complexity no more than n.*

Proof. Let $\alpha = \mathrm{Cg}^{\mathbf{F}}(a, 1)$ and let μ be the monolith of $\mathbf{F}$. Let ν be any join irreducible congruence so that $\mu < \nu \leq \alpha$. Because $\rho^{\mathbf{F}}(a) = 2$, in view of Lemma 1, we find that ν covers μ. Let $\nu_0, \nu_1, \ldots, \nu_{m-1}$ be distinct covers of μ such that $\alpha = \nu_0 \vee \nu_1 \vee \ldots \vee \nu_{m-1}$ and m is as small as possible. In this way, α is decomposed into a join irredundant system of join irreducible congruences. In particular, no ν_i is below the join of the other ν_j's. Because ν_i covers μ, this means, for example, that

$$\nu_0 \cap (\nu_1 \vee \nu_2 \vee \ldots \vee \nu_{m-1}) \leq \mu,$$

and similarly for each i in place of 0.

Let $i < m$. Now $(1/\nu_i)/\mu$ is a chief factor, therefore $|(1/\nu_i)/\mu| \leq r$. Hence $|1/\nu_i| \leq r|1/\mu| \leq r^2$. It follows from Lemma 0 that $r^2 + 2$ is an upper bound on the complexity of polynomials needed to witness $\langle b, 1\rangle \in \nu_i$ for all $b \in F$ such that $\langle b, 1\rangle$ is critical. Consequently, all we need is a number n' depending only on $\mathcal{V}$ such that there is $i < m$ and $\langle b, 1\rangle \in \nu_i$ with $b \neq 1$ so that $\langle b, 1\rangle \in \mathrm{Cg}^{\mathbf{F}}(a, 1)$ can be witnessed by a polynomial of complexity no more than n'.

From here the proof of our Lemma breaks into two easy cases and one case that requires more work.

Case: $1/\alpha$ is not Abelian.

In this case, our first contention is that there is $i < m$ and $\langle d, 1\rangle \in \nu_i$ so that $ad \neq da$. Suppose otherwise. Let $c \in 1/\alpha$. Then $c = c_0c_1 \ldots c_{m-1}$ where $\langle c_i, 1\rangle \in \nu_i$ for each $i < m$. Consequently, $ac = ac_0c_1 \ldots c_{m-1} = c_0ac_1 \ldots c_{m-1} = c_0c_1 \ldots c_{m-1}a = ca$. This means that a commutes with every element of $1/\alpha$. Now let $t \in A$ and $c \in 1/\alpha$. Since $1/\alpha$ is a normal subgroup of $\mathbf{F}$, pick $d \in 1/\alpha$ so that $c = tdt^{-1}$. Then $tat^{-1}c = tat^{-1}tdt^{-1} = tadt^{-1} = tdat^{-1} = tdt^{-1}tat^{-1} = ctat^{-1}$. Consequently, every conjugate of a commutes with every element of $1/\alpha$. The same applies to all conjugates of a^{-1}. But $1/\alpha$ is just the set of products of conjugates like these. In this way we find that $1/\alpha$ is Abelian, contrary to the stipulation in this case.

So pick $i < m$ and $\langle d, 1\rangle \in \nu_i$ so that $ad \neq da$. Let $b = dad^{-1}a^{-1}$. Observe that $b \neq 1$ while $\langle b, 1\rangle \in \nu_i$ since $\langle d, 1\rangle \in \nu_i$. The polynomial $q(x) = dxd^{-1}x^{-1}$ witnesses $\langle b, 1\rangle \in \mathrm{Cg}^{\mathbf{F}}(a, 1)$. In this case, we can let $n' = 4$.

Case: $1/\alpha$ is Abelian and the order of a is not prime.

Let p be a prime number and $s > 1$ so that ps is the order of a. Let $a' = a^s$. So a' has order p. Let $\alpha' = \mathrm{Cg}^{\mathbf{F}}(a', 1) \subseteq \mathrm{Cg}^{\mathbf{F}}(a, 1)$. So $\rho^{\mathbf{F}}(a')$ is either 1 or 2. The polynomial $q(x) = x^s$ witnesses $\langle a', 1\rangle \in \mathrm{Cg}^{\mathbf{F}}(a, 1)$. The complexity of this polynomial is bounded by the exponent e. If $\rho^{\mathbf{F}}(a') = 1$ we have that $\langle a', 1\rangle \in \mu$. So we can take $b = a'$ and $n' = 2$. On the other hand, if $\rho^{\mathbf{F}}(a') = 2$, the case at hand reduces to the case we consider next.

Case: $1/\alpha$ is Abelian and the order of a is prime.

Let the prime number p be the order of a.

Recalling that $\alpha = \nu_0 \vee \nu_1 \vee \ldots \vee \nu_{m-1}$, let $a = a_0a_1 \ldots a_{m-1}$ where $\langle a_i, 1\rangle \in \nu_i$ for all $i < m$.

Claim 8. *Let η and ν be two distinct members of $\{\nu_0, \nu_1, \ldots, \nu_{m-1}\}$ and let a', a'' be the members of $\{a_0, a_1, \ldots, a_{m-1}\}$ so that $\langle a', 1\rangle \in \eta$ and $\langle a'', 1\rangle \in \nu$. Under these assumptions $\mathrm{Cg}^{\mathbf{F}}(a'a'', 1) = \eta \vee \nu$.*

Proof. Observe that η must be generated by $\langle a', 1\rangle$ since otherwise the congruence generated by $\langle a', 1\rangle$ must be included in μ and hence η can be omitted from the join representation of α. Similarly, $\langle a'', 1\rangle$ generates ν.

Since $\langle a'', 1\rangle \in \alpha$ there is a conjugate product polynomial $\pi(x)$ over $\mathbf{F}$ so that

$$\begin{aligned} a'' &= \pi(a) \\ &= \pi(a_0 a_1 \dots a_{k-1} a_k \dots a_{m-1}) \\ &= \pi(a_0)\pi(a_1)\dots\pi(a')\dots\pi(a'')\dots\pi(a_{m-1}) \end{aligned}$$

This entails that $\langle a'', \pi(a'')\rangle \in \nu \cap \hat{\nu} \subseteq \mu$, where $\hat{\nu}$ is the join of all the ν_i's except ν. Similarly, $\langle \pi(a_j), 1\rangle \in \mu$ for all $a_j \neq a''$. Consequently, $\pi(a'a'') = a''d$ for some d with $\langle d, 1\rangle \in \mu$. It follows that $\mathrm{Cg}^{\mathbf{F}}(\pi(a'a''), 1) = \nu$. So $\nu \subseteq \mathrm{Cg}^{\mathbf{F}}(a'a'', 1)$.

Likewise, we find that $\eta \subseteq \mathrm{Cg}^{\mathbf{F}}(a'a'', 1)$.

Althogether, we have

$$\eta \vee \nu \subseteq \mathrm{Cg}^{\mathbf{F}}(a'a'', 1).$$

But the reverse inclusion is evident, so the proof is complete. □

Claim 9. *Let η and ν be two distinct members of $\{\nu_0, \nu_1, \dots, \nu_{m-1}\}$ and suppose that $\langle b, 1\rangle$ generates η while $\langle c, 1\rangle$ generates ν. Then $\mathrm{Cg}^{\mathbf{F}}(bc, 1) = \eta \vee \nu$.*

Proof. Plainly, $\langle bc, 1\rangle \in \eta \vee \nu$, so $\mathrm{Cg}^{\mathbf{F}}\langle bc, 1\rangle \subseteq \eta \vee \nu$. For the sake of contradiction, suppose that the reverse inclusion fails. So either $\langle b, 1\rangle \notin \mathrm{Cg}^{\mathbf{F}}(bc, 1)$ or $\langle c, 1\rangle \notin \mathrm{Cg}^{\mathbf{F}}(bc, 1)$. But it is clear that each of these two alternatives implies the other. So we have both $\eta \nsubseteq \mathrm{Cg}^{\mathbf{F}}(bc, 1)$ and $\nu \nsubseteq \mathrm{Cg}^{\mathbf{F}}(bc, 1)$.

Now suppose $\langle g, 1\rangle, \langle h, 1\rangle \in \mathrm{Cg}^{\mathbf{F}}(bc, 1) \subseteq \eta \vee \nu$. Further suppose $\langle g_0, 1\rangle, \langle h_0, 1\rangle \in \eta$ and $\langle g_1, 1\rangle, \langle h_1, 1\rangle \in \nu$ so that $g = g_0 g_1$ while $h = h_0 h_1$. (Such factorizations are always possible.) We contend that $\langle g_0, h_0\rangle \in \mu$ if and only if $\langle g_1, h_1\rangle \in \mu$. Otherwise, for instance, $\langle g_0, h_0\rangle \notin \mu$ but $\langle g_1, h_1\rangle \in \mu$. In this situation, $\langle g_0 h_0^{-1}, 1\rangle$ generates η. Using commutativity, we have $gh^{-1} = (g_0 h_0^{-1})(g_1 h_1^{-1})$. So it follows that $\langle g, h\rangle$ generates η, which is impossible. In particular, if $\langle g, h\rangle \notin \mu$, then $\langle g_0, h_0\rangle \notin \mu$ and $\langle g_1, h_1\rangle \notin \mu$.

The following unique factorization property holds:

If $\langle g_0 g_1, h_0 h_1\rangle \in \mu$ where $\langle g_0, h_0\rangle \in \eta$ and $\langle g_1, h_1\rangle \in \nu$, then $\langle g_0, h_0\rangle \in \mu$ and $\langle g_1, h_1\rangle \in \mu$.

Indeed, it follows from the hypothesis of this assertion that $\langle g_0, h_0\rangle \in \nu$ and $\langle g_1, h_1\rangle \in \eta$. But were $\langle g_0, h_0\rangle \notin \mu$, then $\langle g_0, h_0\rangle$ would generate η. This would imply that $\mu < \eta \leq \nu$, and so that $\eta = \nu$.

The observations above allow us to define the maps Ψ_0 from $(1/\mathrm{Cg}^{\mathbf{F}}(bc, 1))/\mu$ to $(1/\eta)/\mu$ and Ψ_1 from $(1/\mathrm{Cg}^{\mathbf{F}}(bc, 1))/\mu$ to $(1/\nu)/\mu$ as follows. Suppose $\langle g, 1\rangle \in \mathrm{Cg}^{\mathbf{F}}(bc, 1)$. Factor $g = g_0 g_1$ where $\langle g_0, 1\rangle \in \eta$ and $\langle g_1, 1\rangle \in \nu$. Let $\Psi_0(g/\mu) = g_0/\mu$ and let $\Psi_1(g/\mu) = g_1/\mu$.

We contend that each of these maps is one-to-one. For suppose $\langle g, 1\rangle, \langle h, 1\rangle \in \mathrm{Cg}^{\mathbf{F}}(bc, 1)$ with $\langle g, h\rangle \notin \mu$. Then we can find $\langle g_0, 1\rangle, \langle h_0, 1\rangle \in \eta$ and $\langle g_1, 1\rangle, \langle h_1, 1\rangle \in \nu$ so that $g = g_0 g_1, h = h_0 h_1$; moreover $\Psi_0(g/\mu) = g_0/\mu$ and $\Psi_0(h/\mu) = h_0/\mu$ while $\Psi_1(g/\mu) = g_1/\mu$ and $\Psi_1(h/\mu) = h_1/\mu$. But we also have $\langle g_0, h_0\rangle \notin \mu$ and $\langle g_1, h_1\rangle \notin \mu$. Therefore $\Psi_0(g/\mu) \neq \Psi_0(h/\mu)$ and $\Psi_1(g/\mu) \neq \Psi_1(h/\mu)$.

We also have that Ψ_0 maps onto $(1/\eta)/\mu$. Indeed, suppose $\langle g_0, 1\rangle \in \eta$. Then there is a conjugate product polynomial $\pi(x)$ so that $g_0 = \pi(b)$. Let $g_1 = \pi(c)$. Then $\langle g_1, 1\rangle \in \nu$. Using commutativity, we see that $g_0 g_1 = \pi(bc)$. Therefore $\langle g_0 g_1, 1\rangle \in \mathrm{Cg}^{\mathbf{F}}(bc, 1)$ and, evidently, $\Psi_0(g_0 g_1/\mu) = g_0/\mu$. Likewise Ψ_1 maps onto $(1/\nu)/\mu$.

Now every element of $1/\alpha$ has the form $\pi(a)$ for some conjugate product polynomial $\pi(x)$. Since the order of a is the prime p, it follows that every element, other than 1, of $1/\alpha$ must have order p. The same must also apply to every element of $1/\eta$ and $1/\nu$. By the Fundamental Theorem for Finite Abelian Groups, we see that $1/\eta$ must be isomorphic to a finite direct power, say the k^{th}, of the cyclic group of order p. Of course, $1/\nu$ must also be isomorphic to the same direct power, since $(1/\eta)/\mu$ and $(1/\nu)/\mu$ have the same finite cardinality. Pick $\langle g_1, 1\rangle, \langle g_2, 1\rangle, \dots, \langle g_{k-1}, 1\rangle \in \eta$ so that $b, g_1, \dots, g_{k-1}$ generate, each individually, the internal direct factors. By using $\Psi_1 \circ \Psi_0^{-1}$ obtain from each g_j an element h_j so that $\langle g_j h_j, 1\rangle \in \mathrm{Cg}^{\mathbf{F}}(bc, 1)$ and $\Psi_0(g_j h_j/\mu) = g_j/\mu$ while $\Psi_1(g_j h_j/\mu) = h_j/\mu$. We can further arrange the choices of the h_j's so that $c, h_1, \dots, h_{k-1}$ generate, each individually, internal direct factors giving a decomposition of $1/\nu$.

Let $a', a'' \in \{a_0, a_1, \ldots, a_{m-1}\}$ so that $\langle a', 1\rangle \in \eta$ and $\langle a'', 1\rangle \in \nu$. So there are natural numbers $s, t_1, t_2, \ldots, t_{k-1} < p$ such that $a' = b^s g_1^{t_1} g_2^{t_2} \ldots g_{k-1}^{t_{k-1}}$. Also, there are natural numbers $u, v_1, v_2, \ldots, v_{k-1} < p$ such that $a'' = c^u g_1^{v_1} g_2^{v_2} \ldots g_{k-1}^{v_{k-1}}$. By Claim 8 there must be a conjugate product polynomial $\pi(x)$ so that $\pi(a'a'') = a''$. From this we deduce $\langle \pi(a'), 1\rangle \in \mu$. It follows that $\langle \pi(b)^s \pi(g_1)^{t_1} \ldots \pi(g_{k-1})^{t_{k-1}}, 1\rangle \in \mu$. From the internal direct representation and the fact that nontrivial elements are of prime order p, it follows that $\langle \pi(b), 1\rangle \in \mu$ and $\langle \pi(g_j), 1\rangle \in \mu$ for all j. This entails, in turn, that $\langle \pi(c), 1\rangle \in \mu$ and that $\langle \pi(h_j), 1\rangle \in \mu$ for all j. Assembling the factors we discover that $\langle \pi(a''), 1\rangle \in \mu$, as well. So $\langle a'', 1\rangle = \langle \pi(a'a''), 1\rangle = \langle \pi(a')\pi(a''), 1\rangle \in \mu$. But this is impossible, and the claim is established. □

Claim 10. *Let $\eta_0, \eta_1, \ldots, \eta_{k-1}$ be any k distinct members of $\{\nu_0, \nu_1, \ldots, \nu_{m-1}\}$ and suppose that $\langle b_j, 1\rangle$ generates η_j for each $j < k$. Then $\mathrm{Cg}^{\mathbf{F}}(b_0 b_1 \ldots b_{k-1}, 1) = \eta_0 \vee \eta_1 \vee \ldots \vee \eta_{k-1}$.*

Proof. We prove this by induction on k. The initial step of the induction is part of the hypotheses of this claim. For the inductive step, we suppose the claim holds for any j of the selected congruences, and argue that it must hold for any $j+1$ of them, say for $\eta_0, \eta_1, \ldots, \eta_j$.

By our inductive assumption $\eta_0 \subseteq \mathrm{Cg}^{\mathbf{F}}(b_0 b_1 \cdots_{j-1}, 1)$. So pick a conjugate product polynomial $\pi(x)$ so that $b_0 = \pi(b_0 b_1 \cdots_{j-1})$. It follows that $\langle \pi(b_0), 1\rangle$ generates η_0 and that $\langle \pi(b_i), 1\rangle \in \mu$ for all i with $1 \leq i < j$. Now consider $\pi(b_0 b_1 \ldots b_{j-1} b_j) = \pi(b_0) d \pi(b_j)$ where $\langle d, 1\rangle \in \mu$. There are two cases:

Case: $\langle \pi(b_j), 1\rangle \in \mu$**.** In this case, we have

$$\eta_0 \subseteq \mathrm{Cg}^{\mathbf{F}}(\pi(b_0 b_1 \ldots b_j), 1\rangle \subseteq \mathrm{Cg}^{\mathbf{F}}(b_0 b_1 \ldots b_j, 1).$$

This means that $\langle b_0, 1\rangle \in \mathrm{Cg}^{\mathbf{F}}(b_0 b_1 \ldots b_j, 1)$. Consequently, $\langle b_1 b_2 \ldots b_j, 1\rangle \in \mathrm{Cg}^{\mathbf{F}}(b_0 b_1 \ldots b_j, 1)$. But by the inductive hypothesis $\eta_1 \vee \eta_2 \vee \ldots \vee \eta_j \subseteq \mathrm{Cg}^{\mathbf{F}}(b_1 b_2 \ldots b_j, 1)$. Therefore,

$$\eta_0 \vee \eta_1 \vee \ldots \vee \eta_j \subseteq \mathrm{Cg}^{\mathbf{F}}(b_0 b_1 \ldots b_j, 1)$$

as desired.

Case: $\langle \pi(b_j), 1\rangle$ **generates** η_j**.** We know that $\pi(b_0 b_1 \ldots b_j) = \pi(b_0)\pi(b_j) d$ where $\langle d, 1\rangle \in \mu$. This means

$$\langle \pi(b_0)\pi(b_j), 1\rangle \in \mathrm{Cg}^{\mathbf{F}}(\pi(b_0)\pi(b_j) d, 1) \subseteq \mathrm{Cg}^{\mathbf{F}}(\pi(b_0 b_1 \ldots b_j), 1) \subseteq \mathrm{Cg}^{\mathbf{F}}(b_0 b_1 \ldots b_j, 1).$$

By Claim 9, we conclude that $\eta_0 \vee \eta_j \subseteq \mathrm{Cg}^{\mathbf{F}}(b_0 b_1 \ldots b_j, 1)$. In particular, $\langle b_j, 1\rangle \in \mathrm{Cg}^{\mathbf{F}}(b_0 b_1 \ldots b_j, 1)$. It follows that $\langle b_0 b_1 \ldots b_{j-1}, 1\rangle \in \mathrm{Cg}^{\mathbf{F}}(b_0 b_1 \ldots b_j, 1)$ as well. By the inductive hypothesis, $\eta_0 \vee \eta_1 \vee \ldots \vee \eta_{j-1} \subseteq \mathrm{Cg}^{\mathbf{F}}(b_0 b_1 \ldots b_j, 1)$. Putting the pieces together, we find

$$\eta_0 \vee \eta_1 \vee \ldots \vee \eta_j \subseteq \mathrm{Cg}^{\mathbf{F}}(b_0 b_1 \ldots b_j, 1),$$

as desired. □

Without loss of generality, assume that $|1/\nu_0| \geq |1/\nu_i|$ for all $i < n$. Now let $\mathbf{F}$ act on $1/\nu_0$ by conjugation. The kernel of this action is γ, the centralizer of ν_0. So

$$\langle t, d\rangle \in \gamma \Leftrightarrow tct^{-1} = dcd^{-1} \text{ whenever } \langle c, 1\rangle \in \nu_0.$$

Evidently, $\mathbf{F}/\gamma$ is embeddable into $\mathrm{Aut}(\mathbf{1}/\boldsymbol{\nu_0})$. Because $|1/\nu_0| \leq r^2$ we have the conclusion that $|F/\gamma| \leq (r^2)!$. Let D be a transversal of F/γ, that is a set of distinct representatives for the congruence classes of γ. Without loss of generality, we place $a_0 \in D$. Let $\mathbf{F}''$ be the subgroup of $\mathbf{F}$ generated by $D \cup \{a\}$. Observe that the cardinality of $\mathbf{F}''$ is bounded above in terms of $\mathcal{V}$ alone. Finally, let α'' denote $\mathrm{Cg}^{\mathbf{F}''}(a, 1)$. Observe that $\alpha'' \subseteq \alpha$.

Pick $u \in F''$ so that $\langle u, 1\rangle \in \alpha''$ and $\langle a_0, 1\rangle \in \mathrm{Cg}^{\mathbf{F}}(u, 1)$ and so that $\langle a_i, 1\rangle \in \mathrm{Cg}^{\mathbf{F}}(u, 1)$ for the least number if i's. Since $\langle u, 1\rangle \in \alpha$, the element u can be decomposed as a product, (after rearranging indices, except for 0, as needed):

$$u = u_0 u_1 \ldots u_{q-1} \text{ where } \langle u_i, 1\rangle \in \nu_i \text{ for all } i < q \leq m,$$

and, moreover, $\langle u_i, 1\rangle$ generates ν_i, for all $i < q$, in view of Claim 10 and the irredundance of the ν_i's.

Claim 11. *If $\langle v, 1\rangle, \langle w, 1\rangle \in \mathrm{Cg}^{\mathbf{F}''}(u, 1)$ so that decompositions of v and w are $v_0 v_1 \dots v_{q-1}$ and $w_0 w_1 \dots w_{q-1}$, and $\langle v_0, w_0\rangle \notin \mu$, then $\langle v_i, w_i\rangle \notin \mu$.*

Proof. Evidently, $\langle vw^{-1}, 1\rangle \in \mathrm{Cg}^{\mathbf{F}''}(u, 1) \subseteq \alpha''$ and we have

$$vw^{-1} = v_0 w_0^{-1} v_1 w_1^{-1} \dots v_{q-1} w_{q-1}^{-1}.$$

Now $\langle v_0 w_0^{-1}, 1\rangle$ generates ν_0 since $\langle v_0, w_0\rangle \notin \mu$. Consequently, $\langle a_0, 1\rangle \in \mathrm{Cg}^{\mathbf{F}}(vw^{-1}, 1)$. Thus, by the minimality of the choice of u, we obtain $\langle v_i, w_i\rangle \notin \mu$ for all $i < q$. □

Now for each $i < q$, let

$$H_i = \{c/\mu \mid \langle c, 1\rangle \text{ generates } \nu_i \text{ and } c \text{ is a canonical factor of } v \text{ for some } v \text{ such that } \langle v, 1\rangle \in \mathrm{Cg}^{\mathbf{F}''}(u, 1)\}$$

Define $\Psi_i : H_i \to H_0$ by $\Psi_i(c/\mu) = b/\mu$ provided there is $\langle v, 1\rangle \in \mathrm{Cg}^{\mathbf{F}''}(u, 1)$ so that $v_i = c$ and $v_0 = b$ in the canonical decomposition of v. This definition of the function Ψ_i is sound according the Claim 11. Evidently, Ψ_i maps H_i onto H_0. Consequently, $|H_i| \geq |H_0|$. On the other hand, because $D \subseteq F''$, the algebra $\mathbf{F}''$ has enough conjugate product polynomials to ensure that $|(1/\nu_0)/\mu| = |H_0| + 1$. So consider these inequalities:

$$|H_i| + 1 \leq |(1/\nu_i)/\mu| \leq |(1/\nu_0)/\mu| = |H_0| + 1.$$

In this way we discover that $|H_i| = |H_0|$ for all $i < q$. Because these numbers are finite, we conclude that Ψ_i maps H_i one-to-one and onto H_0. It also follows that H_i consists exactly of those c's so that $\langle c, 1\rangle$ generated ν_i.

Claim 12. *There is a conjugate product polynomial $\pi(x)$ with all coefficients in D so that*

(1) $\pi(c) \neq 1$ for some c such that $\langle c, 1\rangle \in \nu_0$, and
(2) $\langle \pi(d), 1\rangle \in \mu$ whenever $\langle d, 1\rangle \in \nu_i$ for all $i < q$.

Proof. Let $\langle w, 1\rangle \in \mu$ with $w \neq 1$. As noted in the proof of Claim 9, the group $(1/\nu_0)/\mu$ can be decomposed as the internal direct power (let us say the k^{th} power) of cyclic groups of order p. Let $g_0, g_1, \dots g_{k-1} \in (1/\nu_0)$ so that $g_0/\mu, g_1/\mu, \dots, g_{k-1}/\mu$ will be respective generators of each of these internal direct factors. Since $\langle w, 1\rangle \in \mathrm{Cg}^{\mathbf{F}}(g_0, 1)$ there is conjugate product polynomial $\pi_0(x)$ such that $\pi_0(g_0) = w$. Moreover, we can suppose that all the coefficients of $\pi_0(x)$ belong to D, because D is a transversal of the centralizer. Unless $\langle \pi_0(g_i), 1\rangle \in \mu$ for all $i < k$, we suppose without loss of generality that $\langle \pi_0(g_1), 1\rangle \notin \mu$. So there is a conjugate product polynomial $\kappa_1(x)$ with coefficients in D so that $\kappa_1(\pi_0(g_1)) = w$. Let $\pi_1(x) = \kappa_1(\pi_0(x))$. It follows that $\pi_1(g_1) = w \neq 1$ and $(\pi_1(g_i), 1\rangle \in \mu$ for all $i < 2$. Repeating this process no more than k times will result in a conjugate product polynomial $\pi(x)$ such that $\pi(g_j) = w \neq 1$ for some $j < k$ while $\langle \pi(g_i), 1\rangle \in \mu$ for all $i < k$.

Now let $h \in 1/\nu_0$. Then $h = g_0^{r_0} g_1^{r_1} \dots g_{k-1}^{r_{k-1}}$, by the internal direct decomposition. By invoking the commutativity, we get $\pi(h) = (\pi(g_0))^{r_0} (\pi(g_1))^{r_1} \dots (\pi(g_{k-1}))^{r_{k-1}}$. Therefore $\langle \pi(h), 1\rangle \in \mu$.

At this point we know

- $\pi(c) \neq 1$ for some c such that $\langle c, 1\rangle \in \nu_0$, and
- $\langle \pi(d), 1\rangle \in \mu$ whenever $\langle d, 1\rangle \in \nu_0$.

It remains to prove that $\langle \pi(d), 1\rangle \in \mu$ whenever $\langle d, 1\rangle \in \nu_i$ for all $i < q$. So let $\langle d, 1\rangle \in \nu_0$. Should $\langle d, 1\rangle \in \mu$, our conclusion is immediate. Otherwise, $d/\mu \in H_i$. Let $d'/\mu = \Psi_i(d/\mu)$. Then we know that $\pi(d')/\mu = \Psi_i(\pi(d)/\mu)$. But in view of Claim 11 and the fact that Ψ_i is a one-to-one correspondence between H_i and H_0, we conclude that $\langle \pi(d), 1\rangle \in \mu$ since $\langle \pi(d'), 1\rangle \in \mu$. □

Now the membership condition $\langle u, 1\rangle \in \mathrm{Cg}^{\mathbf{F}''}(a, 1)$ can be witnessed by a polynomial of complexity bounded in terms of $|F''|$, which is in turn bounded in terms of $\mathcal{V}$. Also $\langle c, 1\rangle \in \nu_0 \subseteq \mathrm{Cg}^{\mathbf{F}}(u, 1)$. This means that c can be factored as a product of conjugates of u and u^{-1}. Invoking commutativity, it turns out that

$\pi(c)$ can be expressed as a product of terms of the form $\pi(tut^{-1})$ and $\pi(tu^{-1}t^{-1})$. Because $\pi(c) \neq 1$, one of these factors must also be different from 1. Say $\pi(tut^{-1}) \neq 1$. Now

$$tut^{-1} = e_0 e_1 \dots e_{q-1} \text{ where } e_i = tu_i t^{-1} \text{ and } \langle e_i, 1\rangle \in \nu_i \text{ for all } i < q.$$

Then, by Claim 12

$$\pi(tut^{-1}) = \pi(e_0)\pi(e_1)\dots\pi(e_{q-1}) \in 1/\mu.$$

Let $\mathbf{F}'$ be the subalgebra of $\mathbf{F}$ generated by $D \cup \{a, t\}$. Then $\langle \pi(tut^{-1}), 1\rangle \in \mathrm{Cg}^{\mathbf{F}'}(u, 1) \subseteq \mathrm{Cg}^{\mathbf{F}'}(a, 1)$. Finally, we can take $b = \pi(tut^{-1})$. Because $|F'|$ is bounded in terms of $\mathcal{V}$, there is a polynomial witnessing $\langle b, 1\rangle \in \mathrm{Cg}^{\mathbf{F}}(a, 1)$ of complexity also bounded in terms of $\mathcal{V}$, as desired. □

We are now in a position to prove Theorems 7 and 8.

Proof of Theorem 8. According to Lemma 7 there is a finite upper bound n such that for every finite subdirectly irreducible group $\mathbf{F} \in \mathcal{V}$ and every $a \in F$ with $\rho^{\mathbf{F}}(a) = 2$, there is $b \in F$ with $b \neq 1$ such that $\langle b, 1\rangle$ is a critical pair for $\mathbf{F}$ and $\langle b, 1\rangle \in \mathrm{Cg}^{\mathbf{F}}(a, 1)$ can be witnessed by a polynomial of complexity no more than n. By Lemma 6, applied no more than $2r$ times, there is a finite upper bound n' such that for every finite subdirectly irreducible group $\mathbf{F} \in \mathcal{V}$ and every $a \in F$ with $\rho^{\mathbf{F}}(a) < 2r$, there is $b \in F$ with $b \neq 1$ such that $\langle b, 1\rangle$ is a critical pair for $\mathbf{F}$ and $\langle b, 1\rangle \in \mathrm{Cg}^{\mathbf{F}}(a, 1)$ can be witnessed by a polynomial of complexity no more than n'. Now an application of Lemma 5 finishes the proof. □

Theorem 7 follows immediately from Theorem 5, Theorem 8, and Lemma 6.

Finally, we are in a position to prove Theorem 1 and so complete the proof of our Main Theorem.

Proof of Theorem 1. By Theorem 5 we know that $|G|$ is an upper bound on the ladder height of any element in any algebra in $\mathcal{V}$. By invoking Theorem 7 no more than $|G|$ times we conclude that there is a bound n^* such that for any $\mathbf{A} \in \mathcal{V}$ and any $a \in A$ with $\rho^{\mathbf{A}}(a) > 1$ there is $b \in A$ with $\rho^{\mathbf{A}}(b) = 1$ such that $\langle b, 1\rangle \in \mathrm{Cg}^{\mathbf{A}}(a, 1)$ can be witnessed by a conjugate product polynomial of complexity no more than n^*. Now suppose that $\mathbf{A}$ is subdirectly irreducible. Then, according to Corollary 6, $\langle b, 1\rangle \in \mu$ since $\rho^{\mathbf{A}}(b) = 1$.

Now let S be the set of all conjugate product terms in the variable v of complexity no more than n^* using $y_0, \dots, y_{n^*-1}$ to stand for the coeficients. Take $\Psi(x, y, z, w)$ to be

$$\exists y_0, \dots, y_{n^*-1}[\bigvee_{s\in S} x \approx s(zw^{-1}, y_0, \dots, y_{n^*-1})y].$$

Let $\Phi(u, v, x, y)$ be a congruence formula which defines all the atoms in the congruence lattices of algebras belonging to the variety. This formula is given to us by Theorem 4. The congruence formulas $\Psi(x, y, z, w)$ and $\Phi(u, v, , x, y)$ establish that $\mathcal{V}_{\mathrm{si}}$ has definable principal subcongruences.

This concludes our proof. □

It is worth noting that Theorem 1 can be extended to finite pointed groups. A **pointed group** is an algebra $\langle G, \cdot, ^{-1}, 1, p_0, \dots, p_{n-1}\rangle$ where $p_0, \dots, p_{n-1} \in G$ and $\langle G. \cdot, ^{-1}, 1\rangle$ is a group. Thus, for pointed groups one has the privilege of mentioning in terms certain elements by name. In contrast to the Theorem of Oates and Powell, Roger Bryant [6] has been able to construct of finite pointed group (with just one additional point designated by a constant symbol) which generates a nonfinitely based variety. The extension of Theorem 1 to the case of finite pointed groups is easy since adding additional constant symbols in no way changes the unary polynomials that played such a central role is our arguments. So $\mathcal{B}_{\mathrm{si}}$ has definable principal subcongruences, where $\mathcal{B}$ is the variety generated by Bryant's pointed group. We expect that $\mathcal{B}_{\mathrm{si}}$ will turn out not to be finitely axiomatizable, even though it is axiomatizable by a set of elementary sentences, according to Theorem 0.

References

1. K. A. Baker, *Finite equational bases for finite algebras in congruence distributive varieties*, Advances in Mathematics **24** (1977), 207–243.
2. Kirby A. Baker and Ju Wang, *Definable principal subcongruences*, Algebra Universalis **47** (2002), 145–151.
3. J. T. Baldwin and J. Berman, *On the number of subdirectly irreducible algebras in a variety*, Algebra Universalis **5** (1975), 378–389.
4. Garrett Birkhoff, *On the structure of abstract algebras*, Proc. Cambridge Philos. Soc. **31** (1935), 433–454.
5. ———, *Subdirect unions in universal algebra*, Bull. Amer. Math. Soc. **50** (1944), 764–768.
6. R. Bryant, *The laws of finite pointed groups*, Bull. London Math. Soc. **14** (1982), 119–123.
7. S. Burris, *An example concerning definable principal congruences*, Algebra Universalis **7** (1977), 403–404.
8. S. Burris and H. Sankappanavar, *A Course in Universal Algebra*, Springer-Verlag, New York, 1981.
9. Richard Dedekind, *über dir von drei moduln erzeugte dualgruppe*, Ann. Math. **53** (1900), 371–403.
10. Ralph Freese and Ralph McKenzie, *Commutator theory for congruence modular varieties*, London Mathematical Society Lecture Note Series, vol. 125, Cambridge University Press, 1987.
11. G. Grätzer, *Universal Algebra*, Springer-Verlag, New York, 1979, Second Editon.
12. I. M. Isaev, *Essentially infinitely based varieties of algebras*, Sib. Mat. Zhurnal **30** (1989), 75–77.
13. Bjarni Jónsson, *Algebras whose congruence lattices are distributive*, Math. Scand. **21** (1967), 110–121.
14. R. Kruse, *Identities statisfied by a finite ring*, J. Algebra **26** (1973), 298–318.
15. I. V. L'vov, *Varieties of associative rings*, Algebra i Logika **12** (1973), 269–297; 667–688.
16. R. Lyndon, *Two notes on nilpotent groups*, Proc. Amer. Math. Soc. **3** (1955), 579–583.
17. A. I. Maltsev, *On the general theory of algebraic systems (russian)*, Mat. Sb. (N.S.) **35** (1954), 3–20.
18. R. N. McKenzie, *Equational bases for lattice theories*, Math. Scand. **27** (1970), 24–38.
19. ———, *Para primal varieties: a study of finite axiomatizability and definable principal congruences in locally finite varieties*, Algebra Universalis **8** (1978), 336–348.
20. ———, *Finite equational bases for congruence modular algebras*, Algebra Universalis **24** (1987), 224–250.
21. ———, *Tarski's finite basis problem is undecidable*, Inter. J. Algebra and Comput. **6** (1996), 49–104.
22. R. N. McKenzie, G. F. McNulty, and W. A. Taylor, *Algebras, Lattices, Varieties, Volume 1*, Wadsworth & Brooks/Cole, Monterey, CA, 1987.
23. Hanna Neumann, *Varieties of groups*, Ergebnisse der Mathematik und ihre Grenzengebiete, vol. 37, Springer-Verlag, Berlin, 1967.
24. S. Oates and M. B. Powell, *Identical relations in finite groups*, J. Algebra **1** (1965), 11–39.
25. S. V. Polin, *On the identities of finite algebras*, Sib. Mat. J. **17** (1976), 1365–1366.
26. R. Willard, *A finite basis theorem for residually finite congruence meet-semidistributive varieties*, J. Symbolic Logic **65** (2000), 187–200.

Department of Mathematics, University of South Carolina, Columbia, SC 29208, USA

College of Mathematics and Computer Science, GuangXi Normal University, Guilin 541005, China