

A COURSE ON FINITE BASIS PROBLEMS

By

Petar Marković

Lecture notes

for the course in

Advanced Universal Algebra

held at Charles University, Prague

Spring 2008.

TABLE OF CONTENTS

	Page
TABLE OF CONTENTS	ii
Chapter	
I Introduction	1
II History	3
III Background	7
III.1 Semantics	7
III.2 Syntax	9
III.3 Basic universal algebra	13
IV Baker's finite basis theorem	19
IV.1 Ultrafilters	19
IV.2 Two theorems of Model Theory	20
IV.3 Definable principal congruences	23
IV.4 Jónsson's Lemma	26
IV.5 Baker's Theorem	27
V Willard's finite basis theorem	35
V.1 Prerequisites	35
V.2 Characterization of congruence meet-semidistributivity	38
V.3 Bounding Mal'cev chains	42
V.4 Willard's theorem	46
VI The spiral method	49
VII Undecidability of finite basis	51
Bibliography	53

CHAPTER 1

Introduction

These notes were made as lecture notes for the course in Advanced Universal Algebra I taught at the Charles University in Prague in Spring 2008. They may be freely used for teaching and reference purposes. In my opinion a course based on these notes should be taught only to audience of graduate students who have already seen at least one semester of Universal Algebra.

The main objective of this course is McKenzie's result that there is no algorithm deciding if a finite algebra of finite type has a finite base of equations. Therefore, the results displayed are almost a beeline towards this theorem, often skipping otherwise important results related to finite basis, or proving them in a weaker form (like Willard's theorem). The one notable deviation from this beeline is Baker's theorem, which is proved fully.

The organization of the text is as follows: Chapter III deals with the background Universal Algebra and Lattice Theory facts which the students ought to be familiar with prior to taking the course. I omitted quite a lot of proofs there, proving only the results which I consider more difficult, particularly significant to the main line of the text or likely to be omitted in a basic universal algebra course (these are mostly in Section III.3). Chapter IV proves Baker's finite basis theorem. Chapter V proves a weakened version of the Willard's finite basis theorem. Chapter VI exhibits a construction used for proving inherently non-finitely based results, due to Baker, McNulty and Werner. Chapter VII proves McKenzie's result that finite algebras of finite type which have a finite basis are recursively inseparable from those which don't.

The main source book for the text in Chapters III and IV was [6], Chapter V is based on the papers [37] and [36], Chapter VI on paper [3] and Chapter VII on papers [37], [21] and [22]. Notation is meant to be consistent with [24].

It is quite natural that any text of this form has a large number of errors in its early stages. This one may contain even more than

its fair share, since I was mostly typing it on an unfamiliar keyboard, using an unfamiliar editor. I would be obliged to any readers who electronically report any errors which they find to my email address pera@im.ns.ac.yu.

Petar Marković

CHAPTER 2

History

The questions concerning finite basis of equations are historically one of the most researched topics in universal algebra. The origins can be traced to G. Birkhoff who proved that all equations true in a finite algebra in at most n variables are all corollary of a finite set of such equations. Another possible starting point for history of finite basis was the problem posed by B. H. Neumann [27] in 1937: Does every finite group have a finite base of equations? We give a brief historical overview of the major results divided into three parts: non-finitely based algebras and varieties, finitely based algebras and varieties, results concerning both. Note that questions of finite basis of equations are meaningful only in a finite similarity type, so we make this assumption for the remainder of this overview.

The first finite nonfinitely based algebra was discovered by R. C. Lyndon [15] in 1954. It was a seven element groupoid with a constant. This was improved by V. V. Višin [35] to a four-element algebra and further improved by V. L. Murskii [26] in 1963 to a three-element groupoid. J. Ježek [10] found three more three-element non-finitely based groupoids in 1985. Concerning more 'natural' examples of this sort, R. Park [29] found a commutative idempotent four-element groupoid which is non-finitely based in 1980. A most important example of this sort was discovered by P. Perkins [31] in 1969, who proved that the monoid consisting of the matrices of dimension 2×2 , five of which have at most one entry equal to 1 while remaining entries are equal to 0, the sixth element being the identity matrix, equipped with the multiplication operation, is inherently nonfinitely based. M. V. Sapir [34] proved that Perkins' example is the quintessential example of a inherently nonfinitely based finite semigroup, so that all other such finite semigroups contain it, in a way (it is the only minimal INFB finitely generated variety of semigroups not containing groups). Another paper by Sapir [33] characterized INFB varieties of semigroups in terms of *avoidable words*, an extremely useful approach for various problems. Recently, I. Dolinka [7] (using M. V. Sapir's result [33])

proved that the semiring of binary relations on any finite set with at least two elements is non-finitely based. Another general method for proving INFB using graph algebras and a spiral-like construction was invented by K. A. Baker, G. McNulty and H. Werner [4] in 1989. A very surprising example of a non-finitely based finite algebra was discovered by R. Bryant [5] in 1982: it is a finite group with just one more constant operation. This sharply contrasts with the result [28] and foreshadows that finitely based and nonfinitely based algebras would be hard to distinguish, as we'll see later.

The finite based results start with R. C. Lyndon [14], as well. In 1951 he proved that the algebras on a two-element universe are always finitely based. Murskii's result [26] can be viewed as a statement that this result can't be improved. S. Oates and M. B. Powell [28] solved the original question by Neumann by proving that all finite groups are finitely based. The same result for finite rings was discovered independently by L'vov [13] and Kruse [12] in 1973. Perkins has proved (in the same paper [31] where he found an example of an INFB finite semigroup) that all varieties of commutative semigroups and also all uniformly periodic semigroups satisfying a permutation identity. R. McKenzie [18] in 1970 proved that every finite lattice is finitely based, and generalizing this result, K. A. Baker [1] proved in 1976 that every finite algebra generating a congruence-distributive variety is finitely based. There are two major directions in which Baker's theorem was generalized: In congruence-modular direction there was a series of results by Freese and McKenzie, the final result by McKenzie [20] published in 1987 states that every finite algebra generating a congruence-modular residually finite variety is finitely based. In congruence meet-semidistributive direction, R. Willard [38] proved in 2000 that every finite algebra generating a congruence meet-semidistributive residually strictly finite variety is finitely based. The result by K. Kearnes and R. Willard [11] improves on this by proving that every residually finite locally finite congruence meet-semidistributive variety is residually strictly finite, so now in both cases we can say that residual finiteness implies finite basis. New results by Baker, McNulty and Wang [2] and by Maróti and McKenzie [17] generalize these results to certain locally finite varieties and certain quasivarieties, respectively.

The final class of results and conjectures are concerning simultaneously finitely based and nonfinitely based varieties. In early 1960s A. Tarski posed a famous problem if there is a characterization of all finite finitely based algebras. This problem was partially solved, along with some others, (all in the negative) by R. McKenzie in 1996 in a series of three papers [21], [22] and [23]. There it is proved that given any

Turing machine \mathcal{T} , there is a finite algebra of finite type $\mathbf{A}(\mathcal{T})$ such that $\mathbf{A}(\mathcal{T})$ is finitely based (and residually finite) when \mathcal{T} halts, while it is INFB (and residually infinite) when \mathcal{T} doesn't halt. This means that we can't distinguish finitely based and nonfinitely based finite algebras with any recursive property. A subproblem of Tarski's Finite basis problem is still open, though. As early as 1976, Park [30] conjectured that all residually finite finite algebras of finite type are finitely based. Though there was scant evidence for this conjecture at the time (primarily Baker's theorem), the later results all confirmed this speculation, so that the general feeling among experts today (though by no means unanimous) is that this conjecture 'ought to' be true.

CHAPTER 3

Background

1. Semantics

An *algebraic language*, *similarity type*, or just *type* is any set of symbols \mathcal{F} (these symbols are usually called *operation symbols*). It is always equipped with the *arity* function $ar : \mathcal{F} \rightarrow \omega$. The *ar*-preimage of number $i \in \omega$ is denoted by \mathcal{F}_i , and in the special cases when $i = 0, 1, 2, 3$, \mathcal{F}_i is called the set of constant, unary, binary and ternary [operation] symbols, respectively.

An \mathcal{F} -algebra, or just algebra if \mathcal{F} is understood, is a structure $\mathbf{A} = \langle A; \mathcal{F}^{\mathbf{A}} \rangle$, where $\mathcal{F}^{\mathbf{A}} = \{f^{\mathbf{A}} : f \in \mathcal{F}\}$ and $f^{\mathbf{A}} : A^{ar(f)} \rightarrow A$. Note that formally $A^0 = \{\emptyset\}$, so nullary operations in fact select an element of A (a constant).

Define subalgebra, homomorphism, congruence, lattice, distributive, modular, complete lattice, compact element and algebraic lattice, closure operator and algebraic closure operator. Notation: If $\langle P; \leq \rangle$ is a partially ordered set, $a \uparrow$ will denote the set $\{b \in P : a \leq b\}$. Dually, $a \downarrow$ will denote $\{b \in P : b \leq a\}$. For $X \subseteq P$, $X \uparrow = \bigcup_{x \in X} x \uparrow$ and

$$X \downarrow = \bigcup_{x \in X} x \downarrow.$$

THEOREM 1.1 (Birkhoff and Frink). *Subuniverses of an algebra form an algebraic lattice under inclusion order and every algebraic lattice can be realized in this way.*

PROOF. □

THEOREM 1.2 (Grätzer and Schmidt). *Congruences of an algebra form an algebraic lattice under inclusion order and every algebraic lattice can be realized in this way.*

PROOF. □

DEFINITION 1.3. An element a of the lattice \mathbf{L} is *strictly \wedge -irreducible* if for any $Y \subseteq a \uparrow \setminus \{a\}$, if $\bigwedge Y$ exists, then $\bigwedge Y > a$. \wedge -irreducible elements are those where this requirement is made only for

finite Y , while the dual concepts are called *strictly \vee -irreducible* and *\vee -irreducible*.

THEOREM 1.4 (Birkhoff). *Every element of an algebraic lattice is the infimum of strictly \wedge -irreducible elements above it.*

PROOF. By contradiction. Let a be an element of the algebraic lattice \mathbf{L} and let $a' = \bigwedge\{x \in L : x \text{ is strictly } \wedge\text{-irreducible and } x \geq a\}$. Assume that $a < a'$. By the definition of an algebraic lattice, this means that there must exist a compact element $c \leq a'$ such that $c \not\leq a$.

Let $S = \{x \in L : x \geq a \text{ and } x \not\geq c\} = a \uparrow \setminus c \uparrow$. We see that $S \neq \emptyset$, as $a \in S$. We use Zorn's Lemma to prove S has a maximal element b . So, let $C \subseteq S$ be a chain. If $\bigvee C > c$, then for some finite subset $C' \subseteq C$ it holds that $\bigvee C' > c$, as c is compact. The supremum of the finite chain C' must be one of its elements, all of which are in S , and therefore not greater than or equal to c . Therefore, $\bigvee C \notin c \uparrow$, and since $C \subseteq S \subseteq a \uparrow$, then $\bigvee C \in a \uparrow$, so $\bigvee C \in S$. The conditions of Zorn's Lemma being fulfilled for S , we know that S has a maximal element b .

Now we prove that b is strictly \wedge -irreducible. Indeed, take any $Y \subseteq b \uparrow \setminus \{b\}$. As $b \geq a$, $Y \subseteq a \uparrow$. But since b is a maximal element of S , $Y \cap S = \emptyset$ (each element of Y is strictly greater than b , so outside S). Therefore, $Y \subseteq c \uparrow$, and this means that $c \leq \bigwedge Y$. Hence, $b \neq \bigwedge Y$, as $b \not\geq c$.

This means that b is strictly \wedge -irreducible element of \mathbf{L} , is greater than a , and so $b \geq a' \geq c$. Contradiction. \square

Define subdirectly irreducible algebras and subdirect product.

PROPOSITION 1.5. *If a family of congruences $\{\theta_i : i \in I\}$ of an algebra \mathbf{A} satisfies that $\bigcap_{i \in I} \theta_i = 0_{\mathbf{A}}$, then \mathbf{A} can be subdirectly embedded into $\prod_{i \in I} \mathbf{A}/\theta_i$.*

PROOF. \square

COROLLARY 1.6 (Birkhoff's Subdirect Representation Theorem). *Every algebra is subdirect product of subdirectly irreducible algebras.*

PROOF. If \mathbf{A} is an algebra and $\theta \in \mathbf{Con} \mathbf{A}$ is a strictly \wedge -irreducible element of the lattice $\mathbf{Con} \mathbf{A}$, then the factor algebra \mathbf{A}/θ is subdirectly irreducible. As $\mathbf{Con} \mathbf{A}$ is an algebraic lattice, then by Theorem 1.4, $0_{\mathbf{A}}$ is an intersection of strictly \wedge -irreducible elements of $\mathbf{Con} \mathbf{A}$. Therefore, by Proposition 1.5, the Corollary follows. \square

For a class of (similar) algebras \mathcal{K} , define operators $\mathbf{H}(\mathcal{K})$, $\mathbf{S}(\mathcal{K})$ and $\mathbf{P}(\mathcal{K})$.

PROPOSITION 1.7. $\text{SH}(\mathcal{K}) \subseteq \text{HS}(\mathcal{K})$, $\text{PH}(\mathcal{K}) \subseteq \text{HP}(\mathcal{K})$ and $\text{PS}(\mathcal{K}) \subseteq \text{SP}(\mathcal{K})$.

PROOF. □

DEFINITION 1.8. A class \mathcal{K} of algebras closed under operators \mathbf{H} , \mathbf{S} and \mathbf{P} is called a *variety*. For a class of algebras \mathcal{K} we will call the class $\text{HSP}(\mathcal{K})$ the *variety generated by \mathcal{K}* (it is a variety according to Proposition 1.7) and sometimes denote $\text{HSP}(\mathcal{K})$ by $\mathcal{V}(\mathcal{K})$.

2. Syntax

Let X be a set, elements of which will be called variables. Let \mathcal{F} be an algebraic language disjoint from X . Define the set of *terms* $T(X)$ in the language \mathbf{F} and the \mathcal{F} -algebra $\mathbf{T}(X)$. We fix the language \mathcal{F} for the remainder of this Chapter. The term algebra on a countably infinite set of variables X will be denoted by just \mathbf{T} .

PROPOSITION 2.1. Let \mathbf{A} be an algebra and $S \subseteq A$. Then the subalgebra generated by S , $\text{Sg}_{\mathbf{A}}(S)$ is equal to $\{t^{\mathbf{A}}(s_1, \dots, s_n) : t(x_1, \dots, x_n) \in T \text{ and } s_i \in X \text{ for all } i\}$

PROOF. □

Define for an algebra \mathbf{A} and a mapping $\tau : X \mapsto A$ (an *evaluation* of variables) the homomorphism $v_{\tau} : \mathbf{T}(X) \mapsto \mathbf{A}$. This is an example of the *universal mapping property*.

DEFINITION 2.2. Let \mathcal{K} be a class of algebras, $\mathbf{U}(X)$ an algebra generated by its subset X . We say that $\mathbf{U}(X)$ has the universal mapping property for the class \mathcal{K} over the set X if for any algebra $\mathbf{A} \in \mathcal{K}$ and any mapping $\varphi : X \mapsto A$, there exists a homomorphism $\bar{\varphi} : \mathbf{U} \mapsto \mathbf{A}$ (clearly, since $\text{Sg}_{\mathbf{U}}(X) = \mathbf{U}$, $\bar{\varphi}$ is unique).

From the observation above $\mathbf{T}(X)$ has the universal mapping property for any class \mathcal{K} of algebras.

PROPOSITION 2.3. If $\mathbf{U}(X)$ and $\mathbf{V}(Y)$ have the universal mapping property for \mathcal{K} , $|X| = |Y|$ and $\mathbf{U}, \mathbf{V} \in \mathcal{K}$, then $\mathbf{U} \cong \mathbf{V}$.

PROOF. □

Such algebras are called [$|X|$ -generated] free algebras in \mathcal{K} . They are denoted by $\mathbf{F}_{\mathcal{K}}(n)$, where $n = |X|$ is the cardinal.

LEMMA 2.4. If $|X| > 0$ or $|\mathbf{F}_0| > 0$, \mathcal{K} contains a nontrivial algebra and $\text{SP}(\mathcal{K}) = \mathcal{K}$ then $\mathbf{F}_{\mathcal{K}}(|X|)$ exists.

PROOF. Let $\Theta_{\mathcal{K}}(X) = \bigcap \{ \theta \in \text{Con } \mathbf{T}(X) : (\exists \mathbf{A} \in \mathcal{K})(\exists \tau : X \mapsto A)(\theta = \ker(v_\tau)) \}$. Clearly, for each θ in the above family, $\mathbf{T}(X)/\theta \in \mathbf{S}(\mathcal{K})$. Therefore, $\mathbf{T}(X)/\Theta_{\mathcal{K}}(X) \in \mathbf{SPS}(\mathcal{K}) = \mathcal{K}$. It has the universal mapping property for \mathcal{K} over $\bar{x} = \{x/\Theta_{\mathcal{K}}(X) : x \in X\}$. Since \mathcal{K} contains a nontrivial algebra, for all $x, y \in X$, $x/\Theta_{\mathcal{K}}(X) \neq y/\Theta_{\mathcal{K}}(X)$. \square

Note that any algebra $\mathbf{A} \in \mathcal{K}$ is a homomorphic image of $\mathbf{F}_{\mathcal{K}}(|A|)$, if it exists.

Define identities, $\mathbf{A} \models p \approx q$, $\mathcal{K} \models p \approx q$ and $\Sigma \models p \approx q$.

PROPOSITION 2.5. $\text{Id}(\mathcal{K}) = \text{Id}(\mathbf{H}(\mathcal{K})) = \text{Id}(\mathbf{S}(\mathcal{K})) = \text{Id}(\mathbf{P}(\mathcal{K})) = \text{Id}(\mathcal{V}(\mathcal{K}))$. For some $p, q \in T(X)$, $\mathcal{K} \models p \approx q$ iff $(p, q) \in \Theta_{\mathcal{K}}(X)$ iff $\mathbf{T}(X)/\Theta_{\mathcal{K}}(X) \models p \approx q$. If $\mathbf{F}_{\mathcal{K}}(|X|)$ exists, then $\mathcal{K} \models p \approx q$ iff $\mathbf{F} \models p \approx q$.

PROOF. The last equivalence: let $\mathbf{F} = \mathbf{T}(X)/\Theta_{\mathcal{K}}(X)$, and let $p, q \in T(X)$, $p = p(x_1, \dots, x_n)$ and $q = q(x_1, \dots, x_n)$. If $\mathbf{F} \models p \approx q$, then $p^{\mathbf{F}}(x_1/\Theta_{\mathcal{K}}(X), \dots, x_n/\Theta_{\mathcal{K}}(X)) = q^{\mathbf{F}}(x_1/\Theta_{\mathcal{K}}(X), \dots, x_n/\Theta_{\mathcal{K}}(X))$, so $(p, q) \in \Theta_{\mathcal{K}}(X)$. On the other hand, $\mathbf{F}_{\mathcal{K}}(|X|) \in \mathbf{SP}(\mathcal{K})$ and $\mathcal{K} \models p \approx q$ implies $\mathbf{SP}(\mathcal{K}) \models p \approx q$. The rest is obvious. \square

COROLLARY 2.6. Given a class of algebras \mathcal{K} , terms $p, q \in T(X)$ and $|Y| \geq |X|$, $\mathcal{K} \models p \approx q$ iff $\mathbf{T}(Y)/\Theta_{\mathcal{K}}(Y) \models p \approx q$.

PROOF. Clearly, if $\mathcal{K} \models p \approx q$, then $\mathbf{SP}(\mathcal{K}) \models p \approx q$ and from Lemma 2.4, $\mathbf{T}(Y)/\Theta_{\mathcal{K}}(Y) \in \mathbf{SP}(\mathcal{K})$. Now assume $\mathbf{T}(Y)/\Theta_{\mathcal{K}}(Y) \models p \approx q$. Let $|X'| = |Y|$ and $X \subseteq X'$. Then $\mathbf{T}(X') \cong \mathbf{T}(Y)$ and $\mathbf{T}(X')/\Theta_{\mathcal{K}}(X') \cong \mathbf{T}(Y)/\Theta_{\mathcal{K}}(Y)$, so $\mathbf{T}(X')/\Theta_{\mathcal{K}}(X') \models p \approx q$. As $p, q \in T(X')$, $\mathbf{T}(X')/\Theta_{\mathcal{K}}(X') \models p \approx q$ iff $\mathcal{K} \models p \approx q$. \square

COROLLARY 2.7. Let $|X| = \aleph_0$, \mathcal{K} be a class of algebras and $p, q \in T(Y)$. Then $\mathcal{K} \models p \approx q$ iff $\mathbf{T}(X)/\Theta_{\mathcal{K}}(X) \models p \approx q$.

PROOF. There is a finite set $Y' \subseteq Y$ such that $p, q \in T(Y')$. Now it follows from Proposition 2.5 and Corollary 2.6. \square

THEOREM 2.8. Let $|X| = \aleph_0$. $\mathcal{K} = \mathbf{HSP}(\mathcal{K})$ iff $\mathcal{K} = \text{Mod}(\text{Id}_X(\mathcal{K}))$.

PROOF. Let $\mathcal{K} = \mathbf{HSP}(\mathcal{K})$, $\mathbf{A} \models \text{Id}_X(\mathcal{K})$ and $|Y| = |A|$. Then $(p, q) \in \Theta_{\mathcal{K}}(Y)$ implies that $\mathbf{F}_{\mathcal{K}}(X) \models p \approx q$. Let $p', q' \in T(X)$ be obtained from p, q by renaming of variables, respectively. Clearly, for any algebra \mathbf{B} , $\mathbf{B} \models p \approx q$ iff $\mathbf{B} \models p' \approx q'$. Now, $\mathbf{F}_{\mathcal{K}}(X) \models p \approx q$ implies $\mathbf{F}_{\mathcal{K}}(X) \models p' \approx q'$ implies $p' \approx q' \in \text{Id}_X(\mathcal{K})$ implies $\mathbf{A} \models p' \approx q'$ implies $\mathbf{A} \models p \approx q$ implies $(p, q) \in \Theta_{\mathbf{A}}(Y)$. Therefore, $\Theta_{\mathcal{K}}(Y) \subseteq \Theta_{\mathbf{A}}(Y)$ and since $\mathbf{A} \in \mathbf{H}(\mathbf{T}(Y)/\Theta_{\mathbf{A}}(Y))$, then $\mathbf{A} \in \mathbf{H}(\mathbf{T}(Y)/\Theta_{\mathcal{K}}(Y)) \subseteq$

$\mathbf{H}(\mathbf{SP}(\mathcal{K})) = \mathcal{K}$. Therefore, $\text{Mod}(\text{Id}_X(\mathcal{K})) \subseteq \mathcal{K}$ and $\mathcal{K} \subseteq \text{Mod}(\text{Id}_X(\mathcal{K}))$ is trivial.

Let $\mathcal{K} = \text{Mod}(\text{Id}_X(\mathcal{K}))$. Then $\mathbf{HSP}(\mathcal{K}) \subseteq \text{Mod}(\text{Id}_X(\mathcal{K})) = \mathcal{K}$. \square

COROLLARY 2.9 (Birkhoff's HSP Theorem). *There exists X and $\Sigma \subseteq T(X)^2$ such that $\mathcal{K} = \text{Mod}(\Sigma)$ iff $\mathcal{K} = \mathbf{HSP}(\mathcal{K})$.*

PROOF. If $\mathcal{K} = \mathbf{HSP}(\mathcal{K})$ we can make $\Sigma = \text{Id}_X(\mathcal{K})$ for some countably infinite set X , according to Theorem 2.8. On the other hand, if $\mathcal{K} = \text{Mod}(\Sigma)$ for some Σ , then $\mathcal{K} \models \Sigma$ implies $\mathbf{HSP}(\mathcal{K}) \models \Sigma$, so $\mathbf{HSP}(\mathcal{K}) \subseteq \text{Mod}(\Sigma) = \mathcal{K}$. \square

DEFINITION 2.10. Let \mathbf{A} be an algebra and $\theta \in \text{Con } \mathbf{A}$. We say that θ is *fully invariant* if for every endomorphism $\alpha \in \text{End } \mathbf{A}$ and all $(a, b) \in \theta$, $(\alpha(a), \alpha(b)) \in \theta$. The set of all fully invariant congruences of \mathbf{A} will be denoted by $\text{Con}_{\text{FI}} \mathbf{A}$. The least fully invariant congruence on \mathbf{A} containing $X \subseteq A^2$ will be denoted by $\text{Cg}_{\text{FI}}^{\mathbf{A}}(X)$.

Note that $\text{Con}_{\text{FI}} \mathbf{A} = \text{Con } \mathbf{A}^*$, where \mathbf{A}^* is the algebra \mathbf{A} with each endomorphism of \mathbf{A} added as an unary operation. Therefore $\text{Con}_{\text{FI}} \mathbf{A}$ is an algebraic lattice.

LEMMA 2.11. *Let $\mathbf{T}(X)$ be a term algebra and $\theta \in \text{Con } \mathbf{T}(X)$ a congruence. There exists a class of algebras \mathcal{K} such that $\theta = \Theta_{\mathcal{K}}(X)$ iff $\theta \in \text{Con}_{\text{FI}} \mathbf{T}(X)$.*

PROOF. (\Rightarrow) We need to show that $\Theta_{\mathcal{K}}(X)$ is fully invariant. Let $(p, q) \in \Theta_{\mathcal{K}}(X)$, $p, q \in T(\{x_1, x_2, \dots, x_n\})$ and let $\varphi \in \text{End } \mathbf{T}(X)$. Let $t_i = \alpha(x_i)$ and pick arbitrary $\mathbf{A} \in \mathcal{K}$ and evaluation $\tau : X \rightarrow A$. This evaluation extends to a homomorphism $v_\tau : \mathbf{T}(X) \rightarrow \mathbf{A}$ in the unique way. Let $v_\tau(t_i) = a_i$ for all $i \leq n$. We know that $p^{\mathbf{A}}(a_1, \dots, a_n) = q^{\mathbf{A}}(a_1, \dots, a_n)$, since $(p, q) \in \Theta_{\mathcal{K}}(X)$, so $v_\tau(\varphi(p)) = p^{\mathbf{A}}(v_\tau(t_1), \dots, v_\tau(t_n)) = p^{\mathbf{A}}(a_1, \dots, a_n) = q^{\mathbf{A}}(a_1, \dots, a_n) = q^{\mathbf{A}}(v_\tau(t_1), \dots, v_\tau(t_n)) = v_\tau(\varphi(q))$. Therefore, $(\varphi(p), \varphi(q)) \in \Theta_{\mathcal{K}}(X)$.

(\Leftarrow) Assume $\theta \in \text{Con}_{\text{FI}} \mathbf{T}(X)$ and we desire to prove that $\mathbf{T}(X)/\theta \models p \approx q$ iff $p \theta q$. This would mean that for $\mathcal{K} = \{\mathbf{T}(X)/\theta\}$, $\theta = \Theta_{\mathcal{K}}(X)$. If $\mathbf{T}(X)/\theta \models p \approx q$, then $p(x_1, \dots, x_n)/\theta = p^{\mathbf{T}(X)/\theta}(x_1/\theta, \dots, x_n/\theta) = q^{\mathbf{T}(X)/\theta}(x_1/\theta, \dots, x_n/\theta) = q(x_1, \dots, x_n)/\theta$. On the other hand, if $p \theta q$, then for any evaluation $\tau : X \rightarrow T(X)/\theta$, such that $\tau(x_i) = t_i/\theta$, select $\varphi \in \text{End } \mathbf{T}(X)$ such that $\varphi(x_i) = t_i$. Now, for $p, q \in T(x_1, \dots, x_n)$, $p \theta q$ implies $\varphi(p) \theta \varphi(q)$, so $p^{\mathbf{T}(X)/\theta}(\tau(x_1), \dots, \tau(x_n)) = p(t_1, \dots, t_n)/\theta = \varphi(p)/\theta$ and $q^{\mathbf{T}(X)/\theta}(\tau(x_1), \dots, \tau(x_n)) = q(t_1, \dots, t_n)/\theta = \varphi(q)/\theta$ imply $v_\tau(p) = v_\tau(q)$. \square

We define a closure operator D on $T(X)^2$ such that for $\Sigma \subseteq T(X)^2$, $D(\Sigma)$ is the smallest equivalence θ containing Σ and such that the following two properties hold:

- (Rep):** If $(p, q) \in \theta$ and p is a subterm of t , then $(t, t') \in \theta$, where t' is obtained from t by replacing the subterm p by q .
- (Sub):** If $(p_i, q_i) \in \theta$ for $1 \leq i \leq n$ and $f \in \mathcal{F}_n$, then $(f(p_1, \dots, p_n), f(q_1, \dots, q_n)) \in \theta$.

LEMMA 2.12. *The following are equivalent:*

- (i) $\Sigma \models p \approx q$,
- (ii) $(p, q) \in \text{Cg}_{\text{FI}}^{\mathbf{T}(X)}(\Sigma)$,
- (iii) $p \approx q \in D(\Sigma)$.

PROOF. (i) \Rightarrow (ii) Let $\theta = \text{Cg}_{\text{FI}}^{\mathbf{T}(X)}(\Sigma)$. Since $\theta \in \text{Con}_{\text{FI}} \mathbf{T}(X)$, as in Lemma 2.11 we get $\mathbf{T}(X)/\theta \models \Sigma$, and therefore $\mathbf{T}(X)/\theta \models p \approx q$ and $(p, q) \in \theta = \text{Cg}_{\text{FI}}^{\mathbf{T}(X)}(\Sigma)$.

(ii) \Rightarrow (i) Assume $\mathbf{A} \models \Sigma$. Then $\Sigma \subseteq \Theta_{\mathbf{A}}(X) \in \text{Con}_{\text{FI}}(\mathbf{T}(X))$, so $(p, q) \in \text{Cg}_{\text{FI}}^{\mathbf{T}(X)}(\Sigma) \subseteq \Theta_{\mathbf{A}}(X)$. Therefore, $\mathbf{A} \models p \approx q$.

(ii) \Leftrightarrow (iii) $\text{Cg}_{\text{FI}}^{\mathbf{T}(X)}(\Sigma)$ is an equivalence relation on $\mathbf{T}(X)$ and since it is a congruence, by induction on depth of the occurrence of p in t we can conclude that it satisfies (Rep). On the other hand, if $f \in \mathcal{F}_k$, by k applications of (Rep) we get that $(f(p_1, \dots, p_k), f(q_1, \dots, q_n)) \in D(\Sigma)$ if $(p_i, q_i) \in D(\Sigma)$ for all $i \leq k$. It is clear that (Sub) is equivalent to being fully invariant, as endomorphisms of $\mathbf{T}(X)$ are uniquely characterized by their action on X . \square

We define formal theory of equational logic by putting all $p \approx p$ as axioms, and derivation rules are:

- (Sym):** $p \approx q \vdash q \approx p$,
- (Tr):** $p \approx q, q \approx r \vdash p \approx r$,
- (Rep):** $p \approx q \vdash t \approx t'$ when p a subterm of t and t' is obtained from t by replacing the subterm p by q ,
- (Sub):** $p_1 \approx q_1, \dots, p_k \approx q_k \vdash f(p_1, \dots, p_n) \approx f(q_1, \dots, q_n)$, where $f \in \mathcal{F}_k$.

LEMMA 2.13. $\Sigma \vdash p \approx q$ iff $p \approx q \in D(\Sigma)$.

PROOF. Clearly, $D(\Sigma)$ is closed under all derivation rules of equational logic, by definition. Therefore, we only need to show that $\{p \approx q : \Sigma \vdash p \approx q\}$ is D -closed. This is done by induction on the length of proof. In case of transitivity we glue proofs together, in case of proving symmetry we prove 'reverse' identity for every step in the proof, and replacement and substitution are obvious. \square

THEOREM 2.14 (Completeness of equational logic). $\Sigma \models p \approx q$ iff $\Sigma \vdash p \approx q$.

PROOF. It follows from Lemmas 2.12 and 2.13. \square

THEOREM 2.15 (Compactness for equational logic). *If \mathcal{V} is a variety and $\mathcal{V} = \text{Mod}(\Sigma)$ for some finite Σ , then for any Σ_1 such that $\mathcal{V} = \text{Mod}(\Sigma_1)$ there exists a finite $\Sigma'_1 \subseteq \Sigma_1$ such that $\mathcal{V} = \text{Mod}\Sigma'_1$.*

PROOF. $\Sigma_1 \models \Sigma$, so some finite subset $\Sigma'_1 \models \Sigma$ (by Completeness). Therefore, $\mathcal{V} = \text{Mod}\Sigma'_1$. \square

REMARK 2.1. Note that we could have proved Compactness already when we proved that $\Sigma \models p \approx q$ iff $(p, q) \in \text{Cg}_{\text{SFI}}^{\mathbf{T}(X)}(\Sigma)$, as $\text{Cg}_{\text{SFI}}^{\mathbf{T}(X)}$ is an algebraic closure operator. We will call any set of identities Σ such that $\mathcal{V} = \text{Mod}(\Sigma)$ an *equational base*, or just *base* of \mathcal{V} . Also, note that Compactness allows us to say that having a finite base is a property of a variety, not depending on our choice of base identities. Such varieties will be called *finitely based*.

3. Basic universal algebra

DEFINITION 3.1. The variety \mathcal{V} is *locally finite* if for all $\mathbf{A} \in \mathcal{V}$ and finite $X \subseteq A$, $\text{Sg}^{\mathbf{A}}(X)$ is finite.

LEMMA 3.2. \mathcal{V} is locally finite iff for all $n \in \omega$, $\mathbf{F}_{\mathcal{V}}(n)$ is finite.

PROOF. (\Rightarrow) is trivial. For (\Leftarrow) , let $X \subseteq A$ be finite and $\mathbf{A} \in \mathcal{V}$. Then the subalgebra $\text{Sg}^{\mathbf{A}}(X)$ is a homomorphic image of $\mathbf{F}_{\mathcal{V}}(|X|)$, and is therefore finite. \square

PROPOSITION 3.3. *If \mathbf{A} is a finite algebra, then $\text{HSP}(\mathbf{A})$ is locally finite.*

PROOF. Let X be finite. Then $p, q \in \Theta_{\mathbf{A}}(X)$ iff the functions $p^{\mathbf{A}}$ and $q^{\mathbf{A}}$ from A^X to A are equal. As there are at most $|A|^{|A|^{|X|}}$ many of these, $\Theta_{\mathbf{A}}(X) = \Theta_{\text{HSP}(\mathbf{A})}(X)$ has finitely many blocks, so $F_{\text{HSP}(\mathbf{A})}(X)$ is finite. This implies that $\text{HSP}(\mathbf{A})$ is locally finite, according to Lemma 3.2. \square

DEFINITION 3.4. Let \mathcal{V} be a variety. By \mathcal{V}^n we denote the variety $\text{Mod}(\text{Id}_{\{x_1, \dots, x_n\}}(\mathcal{V}))$.

DEFINITION 3.5. Let \mathcal{V} be a locally finite variety. We will say that \mathcal{V} is *inherently nonfinitely based* when no locally finite variety \mathcal{W} such that $\mathcal{V} \subseteq \mathcal{W}$ is finitely based.

We are already in the situation to prove first, easy results about finite basis.

LEMMA 3.6. *Let \mathcal{V} be a locally finite variety in a finite similarity type \mathcal{F} . Then \mathcal{V}^n is finitely based for all n .*

PROOF. Let $X = \{x_1, \dots, x_n\}$, $\mathbf{F} = \mathbf{F}_{\mathcal{V}}(X)$ and $\theta = \Theta_{\mathcal{V}}(X)$. $|F|$ is finite since \mathcal{V} is locally finite. We may assume that no two constant symbols are equal in θ , otherwise just remove the copies from the language of \mathcal{V} (and add to our finite basis the equations making them equal to original after we are done). We also assume that no two members of X are θ -equal (and consequently, none is θ -equal to a member of \mathcal{F}_0), or $x_1 \approx x_2$ is a basis. We make a representative set R for the partition of $T(X)$ induced by θ so that $X \cup \mathcal{F}_0 \subseteq R$. For $t \in T(X)$, let $t^* \in R$ be such that $t/\theta = t^*/\theta$. Now, for every operation $f \in \mathcal{F}_k$ and $(p_1, \dots, p_k) \in R^k$ put the identity $f(p_1, \dots, p_k) \approx (f(p_1, \dots, p_k))^*$ into our set Σ . This is a set of identities in $T(X)^2$, and since $|R| = |F|$ is finite and \mathcal{F} is also finite, then Σ is finite. Moreover, each of these equations is of the form $t = t^*$, where we know $(t, t^*) \in \theta = \Theta_{\text{vrv}}(X)$ and therefore $\mathcal{V} \models \Sigma$.

Now we claim that for all $t \in T(X)$, $\Sigma \models t \approx t^*$. We prove this by induction on complexity of t . If $t \in X \cup \mathcal{F}_0$, then the claim follows since $t \in R$, so $t = t^*$. If $t = f(p_1, \dots, p_k)$ for some $p_i \in T(X)$ and $f \in \mathcal{F}_k$, then we know by inductive assumption that $\Sigma \models p_i \approx p_i^*$ for all i . Therefore by k applications of Replacement we get that $\Sigma \models t \approx f(p_1^*, \dots, p_k^*)$. As $f(p_1^*, \dots, p_k^*) \approx (f(p_1^*, \dots, p_k^*))^* \in \Sigma$, we get $\Sigma \models t \approx (f(p_1^*, \dots, p_k^*))^*$. Since θ is a congruence, $(t, f(p_1^*, \dots, p_k^*)) \in \theta$, so $t^* = (f(p_1^*, \dots, p_k^*))^*$, and we have that $\Sigma \models t \approx t^*$.

Now let $t_1 \approx t_2 \in \text{Id}_X(\mathcal{V})$. Therefore, $t_1/\theta = t_2/\theta$, so $t_1^* = t_2^*$. As we have proved that $\Sigma \models t_i \approx t_i^*$ for $i = 1, 2$, by symmetry and transitivity we get $\Sigma \models t_1 \approx t_2$. \square

THEOREM 3.7 (Birkhoff). *Let \mathcal{V} be a locally finite variety in a finite similarity type. \mathcal{V} is finitely based iff there exists n such that $\mathcal{V} = \mathcal{V}^n$. \mathcal{V} is inherently nonfinitely based iff for all $n \in \omega$, \mathcal{V}^n is not locally finite.*

PROOF. The direction (\Leftarrow) of the first statement is a consequence of Lemma 3.6. If \mathcal{V} is finitely based, then there exists a finite set of variables X such that all identities used in the finite basis Σ . Clearly, $\Sigma \subseteq \text{Id}_{\mathcal{V}}(X)$ and $\mathcal{V} \subseteq \text{Mod}(\text{Id}_{\mathcal{V}}(X)) \subseteq \text{Mod}(\Sigma) = \mathcal{V}$, so $\mathcal{V} \subseteq \text{Mod}(\text{Id}_{\mathcal{V}}(X))$. If $|X| = n$, this means that $\mathcal{V} = \mathcal{V}^n$.

For the second statement, the direction (\Rightarrow) trivially follows from Lemma 3.6. On the other hand if $\mathcal{V} \subseteq \mathcal{W}$ and \mathcal{W} is locally finite and

finitely based, then according to the first statement of this theorem, $\mathcal{W} = \mathcal{W}^n$, for some n , so \mathcal{W}^n is locally finite. As $\mathcal{V}^n \subseteq \mathcal{W}^n$, then for all m , $\mathbf{F}_{\mathcal{V}^n}(m) \in \mathbf{H}(\mathbf{F}_{\mathcal{W}^n}(\mathbf{m}))$, so $\mathbf{F}_{\mathcal{V}^n}(m)$ is finite. Therefore, \mathcal{V}^n is locally finite. \square

Define polynomials, unary polynomials.

THEOREM 3.8 (Mal'cev chains). *Let \mathbf{A} be an algebra and $X \subseteq A^2$. Then $\text{Cg}^{\mathbf{A}}(X)$ is equal to*

$$\{(x, y) \in A^2 : (\exists x_1, \dots, x_n, y_1, \dots, y_n, z_0, z_1, \dots, z_n \in A)(\exists p_1, \dots, p_n \in \text{Pol}_1 \mathbf{A})(x_i, y_i) \in X \ \& \ x = z_0 \ \& \ y = z_n \ \& \ \{z_{i-1}, z_i\} = \{p_i(x_i), p_i(y_i)\}\}.$$

PROOF. Unary polynomials preserve congruences (since terms do and congruences are reflexive), so we only need to prove that the expression in the statement defines a congruence. The case $n = 0$ insures reflexivity, and the set of pairs is clearly defined to be symmetric and transitive. Let there exist a chain z_0, z_1, \dots, z_ℓ for (a_i, b_i) . Then there exists a chain of the form $f^{\mathbf{A}}(b_1, \dots, b_{i-1}, z_j, a_{i+1}, \dots, a_k)$ for any k -ary operation f . Linking these chains we get a chain from $f^{\mathbf{A}}(a_1, \dots, a_k)$ to $f^{\mathbf{A}}(b_1, \dots, b_k)$. \square

THEOREM 3.9 (Quackenbush's Lemma). *If \mathcal{V} is locally finite and contains an infinite subdirectly irreducible \mathbf{S} , then for any $n \in \omega$, \mathcal{V} contains a finite subdirectly irreducible \mathbf{S}_n such that $|S_n| \geq n$.*

PROOF. Let $(a, b) \in \mu$, where μ is the monolith of \mathbf{S} and $c_1, \dots, c_n \in S$ with $c_i \neq c_j$ for $i \neq j$. Then $(a, b) \in \text{Cg}^{\mathbf{S}}(c_i, c_j)$ for all $i \neq j$. Let d_1, \dots, d_m contain all links in the Mal'cev chains used to prove $(a, b) \in \text{Cg}^{\mathbf{S}}(c_i, c_j)$ and all constants used to construct the unary polynomials in these Mal'cev chains for all $i \neq j$. Then let $\mathbf{A} = \text{Sg}^{\mathbf{S}}(\{a, b\} \cup \{c_1, \dots, c_n, d_1, \dots, d_m\})$. \mathbf{A} is finite since \mathcal{V} is locally finite and $(a, b) \in \text{Cg}^{\mathbf{A}}(c_i, c_j)$ for all $i \neq j$. Let θ be a maximal congruence in $\mathbf{Con} \mathbf{A}$ such that $(a, b) \notin \theta$. From $(a, b) \in \text{Cg}^{\mathbf{A}}(c_i, c_j)$, we get $c_i/\theta \neq c_j/\theta$ for all $i \neq j$. Moreover, if $\alpha > \theta$, then $(a, b) \in \alpha$, so $(a, b) \in \bigwedge \{\alpha \in \mathbf{Con} \mathbf{A} : \alpha > \theta\} \setminus \theta$. Therefore, θ is strictly meet irreducible, and $|\mathbf{A}/\theta| \geq n$. \square

DEFINITION 3.10. We define the *residual bound* of a variety \mathcal{V} , denoted by $\text{resb}(\mathcal{V})$, to be the smallest cardinal n such that all subdirectly irreducible algebras in \mathcal{V} have size smaller than n . If \mathbf{A} is an algebra, $\text{resb}(\mathbf{A})$ is defined to be $\text{resb}(\mathcal{V}(\mathbf{A}))$. We say that a variety (or algebra) is *residually finite* if $\text{resb}(\mathcal{V}) = \aleph_0$ ($\text{resb}(\mathbf{A}) = \aleph_0$).

The following theorem is due to Mal'cev in [16] and the term whose existence is proved is called the Mal'cev term. In general, properties of

varieties which are equivalent to existence of terms in a variety which satisfy a system of equations are called Mal'cev properties, and the equations these terms satisfy Mal'cev conditions. If there is a single term of known arity whose existence is equivalent to a property, then this property is called a strong Mal'cev property (strong Mal'cev condition).

THEOREM 3.11 (Mal'cev term). *Let \mathcal{V} be a variety. \mathcal{V} is congruence permutable iff there exists a ternary term m such that $\mathcal{V} \models m(x, y, y) \approx m(y, y, x) \approx x$.*

PROOF. Assume that \mathcal{V} is congruence permutable and let $\mathbf{F} = \mathbf{F}_{\mathcal{V}}(x, y)$. Denote the elements of \mathbf{F}^2 by vector columns and let

$$\mathbf{G} = \text{Sg}^{\mathbf{F}^2} \left(\begin{bmatrix} x \\ y \end{bmatrix}, \begin{bmatrix} y \\ y \end{bmatrix}, \begin{bmatrix} y \\ x \end{bmatrix} \right).$$

Then denote by $\pi_i : \mathbf{F}^2 \rightarrow \mathbf{F}$ the projection homomorphisms, for $i = 1, 2$ and by $\eta_i = \ker(\pi_i) \cap G^2$. Clearly, $\eta_i \in \text{Con } \mathbf{G}$ and $\begin{bmatrix} x \\ y \end{bmatrix} \eta_2 \circ \eta_1 \begin{bmatrix} y \\ x \end{bmatrix}$. By congruence permutability, there exists $\begin{bmatrix} u \\ v \end{bmatrix} \in G$ such that $\begin{bmatrix} x \\ y \end{bmatrix} \eta_1 \begin{bmatrix} u \\ v \end{bmatrix} \eta_2 \begin{bmatrix} x \\ y \end{bmatrix}$. This implies $u = v = x$ and $\begin{bmatrix} x \\ x \end{bmatrix} \in G$. So, there exists a ternary term m such that

$$m^{\mathbf{F}^2} \left(\begin{bmatrix} x \\ y \end{bmatrix}, \begin{bmatrix} y \\ y \end{bmatrix}, \begin{bmatrix} y \\ x \end{bmatrix} \right) = \begin{bmatrix} x \\ x \end{bmatrix}.$$

So, $m^{\mathbf{F}}(x, y, y) = m^{\mathbf{F}}(y, y, x) = x$, and this implies $\mathcal{V} \models m(x, y, y) \approx m(y, y, x) \approx x$, according to Proposition 2.5.

Now assume the existence of Mal'cev term. Let $\mathbf{A} \in \mathcal{V}$, $\alpha, \beta \in \text{Con } \mathbf{A}$ and $a \alpha \circ \beta b$. Then there exists $c \in A$ such that $a \alpha c$ and $c \beta b$. The first condition implies that $m^{\mathbf{A}}(a, c, b) \alpha m^{\mathbf{A}}(a, a, b) = b$ and the second condition implies that $a = m^{\mathbf{A}}(a, b, b) \beta m^{\mathbf{A}}(a, c, b)$. Therefore, $(a, b) \in \beta \circ \alpha$. \square

THEOREM 3.12 (Jónsson terms). *Let \mathcal{V} be a variety. \mathcal{V} is congruence distributive iff there exist ternary terms p_0, p_1, \dots, p_n such that \mathcal{V} satisfies the following identities*

$$\begin{aligned} p_0(x, y, z) &\approx x, \\ p_n(x, y, z) &\approx z, \\ p_i(x, y, x) &\approx x \text{ for all } i, \\ p_i(x, x, y) &\approx p_{i+1}(x, x, y) \text{ for all even } i, \\ p_i(x, y, y) &\approx p_{i+1}(x, y, y) \text{ for all odd } i. \end{aligned}$$

PROOF. Let \mathcal{V} be congruence distributive and let $\mathbf{F} = \mathbf{F}_{\mathcal{V}}(x, y)$. Denote the elements of \mathbf{F}^3 by vector columns and let

$$\mathbf{G} = \text{Sg}^{\mathbf{F}^2} \left(\begin{bmatrix} x \\ x \\ x \end{bmatrix}, \begin{bmatrix} y \\ x \\ y \end{bmatrix}, \begin{bmatrix} x \\ y \\ y \end{bmatrix} \right).$$

Then denote by $\pi_i : \mathbf{F}^2 \rightarrow \mathbf{F}$ the projection homomorphisms, for $i = 1, 2, 3$ and by $\eta_i = \ker(\pi_i) \cap G^2$. Clearly, $\eta_i \in \text{Con } \mathbf{G}$ and $\begin{bmatrix} x \\ x \\ x \end{bmatrix} \eta_1 \wedge$

$(\eta_2 \circ \eta_3) \begin{bmatrix} x \\ y \\ y \end{bmatrix}$. By congruence distributivity, $\begin{bmatrix} x \\ x \\ x \end{bmatrix} (\eta_1 \wedge \eta_2) \vee (\eta_1 \wedge$

$\eta_3) \begin{bmatrix} x \\ y \\ y \end{bmatrix}$. Hence, there exist ternary terms p_0, p_1, \dots, p_n such that

$$p_i^{\mathbf{G}} \left(\begin{bmatrix} x \\ x \\ x \end{bmatrix}, \begin{bmatrix} y \\ x \\ y \end{bmatrix}, \begin{bmatrix} x \\ y \\ y \end{bmatrix} \right) = \begin{bmatrix} u_i \\ v_i \\ w_i \end{bmatrix} \in G, \text{ for } 0 \leq i \leq n, u_0 = v_0 =$$

$w_0 = u_n = x, v_n = w_n = y$ and for all i , when i is even $\begin{bmatrix} u_i \\ v_i \\ w_i \end{bmatrix} \eta_1 \wedge$

$\eta_2 \begin{bmatrix} u_{i+1} \\ v_{i+1} \\ w_{i+1} \end{bmatrix}$, while when i is odd, $\begin{bmatrix} u_i \\ v_i \\ w_i \end{bmatrix} \eta_1 \wedge \eta_3 \begin{bmatrix} u_{i+1} \\ v_{i+1} \\ w_{i+1} \end{bmatrix}$. Then the

desired equations for p_i follow as in Theorem 3.11.

Now, let \mathcal{V} have Jónsson terms. Assume that $\alpha, \beta, \gamma \in \text{Con } \mathbf{A}$, $\mathbf{A} \in \mathcal{V}$ and that $(a, b) \in \alpha \wedge (\beta \vee \gamma)$. Therefore, there exist $a = c_0, c_1, \dots, c_k = b \in A$ such that $c_i \alpha c_{i+1}$ if i is even and $c_i \beta c_{i+1}$ if i is odd. We wish to prove that for all i , $(p_i^{\mathbf{A}}(a, a, b), p_i^{\mathbf{A}}(a, b, b)) \in (\alpha \wedge \beta) \vee (\alpha \wedge \gamma)$. Indeed, for all j , $p_i^{\mathbf{A}}(a, c_j, b) \alpha p_i^{\mathbf{A}}(a, c_j, a) = a$, for even j , $p_i^{\mathbf{A}}(a, c_j, b) \beta p_i^{\mathbf{A}}(a, c_{j+1}, b)$, while for odd j , $p_i^{\mathbf{A}}(a, c_j, b) \beta p_i^{\mathbf{A}}(a, c_{j+1}, b)$. Hence, $p_i^{\mathbf{A}}(a, a, b) = p_i^{\mathbf{A}}(a, c_0, b) (\alpha \wedge \beta) p_i^{\mathbf{A}}(a, c_1, b) (\alpha \wedge \gamma) p_i^{\mathbf{A}}(a, c_2, b) (\alpha \wedge \beta) \dots p_i^{\mathbf{A}}(a, c_k, b) = p_i^{\mathbf{A}}(a, b, b)$. Finally,

$$\begin{aligned} a &= p_1^{\mathbf{A}}(a, a, b) (\alpha \wedge \beta) \vee (\alpha \wedge \gamma) p_1^{\mathbf{A}}(a, b, b) = \\ & p_2^{\mathbf{A}}(a, b, b) (\alpha \wedge \beta) \vee (\alpha \wedge \gamma) p_2^{\mathbf{A}}(a, a, b) = \dots = p_n^{\mathbf{A}}(a, b, b) = b. \end{aligned}$$

□

A more standard way of proving existence of terms from congruence conditions is via the following Lemma:

LEMMA 3.13. *Let \mathcal{V} be a variety, $X = \{x_1, x_2, \dots, x_n, x_{n+1}\}$ and let $\mathbf{F} = \mathbf{F}_{\mathcal{V}}(X)$ be the free algebra. Denote by $\theta = \text{Cg}^{\mathbf{F}}(x_n, x_{n+1})$. If $(p^{\mathbf{F}}(x_1, x_2, \dots, x_n, x_{n+1}), q^{\mathbf{F}}(x_1, x_2, \dots, x_n, x_{n+1})) \in \theta$, then*

$$\mathcal{V} \models p^{\mathbf{F}}(x_1, x_2, \dots, x_n, x_n) \approx q^{\mathbf{F}}(x_1, x_2, \dots, x_n, x_n).$$

PROOF. Let $\mathbf{G} = \mathbf{F}_{\mathcal{V}}(x_1, x_2, \dots, x_n)$ be the free algebra and $\bar{\alpha} \in \text{hom}(f, g)$ be the homomorphism extending the mapping $\alpha(x_i) = x_i$ for $1 \leq i \leq n$ and $\alpha(x_{n+1}) = x_n$. Then $\theta \subseteq \ker \bar{\alpha}$, so $\bar{\alpha}(p/\Theta_{\mathcal{V}}(X)) = \bar{\alpha}(q/\Theta_{\mathcal{V}}(X))$. This implies the desired identity in \mathcal{V} . \square

We have used the other proof in Theorems 3.11 and 3.12 since it is less well-known, and it also has wide applicability. However, in some kinds of Mal'cev properties it is easier to use the approach via Lemma 3.13 for proving this direction, so we proved here it for future applications.

CHAPTER 4

Baker's finite basis theorem

1. Ultrafilters

We begin by defining some notions in a nontrivial Boolean algebra \mathbf{B} . A lot of the results in this section have more general versions (in distributive lattices, for instance), but for the purposes of our course, we use the Boolean case only. We will mean by \mathbf{B} a Boolean algebra $\mathbf{B} = \langle B; \wedge, \vee, ', 0, 1 \rangle$ with $0 \neq 1$ throughout this section.

DEFINITION 1.1. Let \mathbf{B} be a Boolean algebra. $\emptyset \neq I \subseteq B$ is an *ideal* if $I = I \downarrow$ and for all $x, y \in I$, $x \vee y \in I$. Dually, $\emptyset \neq F \subseteq B$ is a *filter* if $F = F \uparrow$ and for all $x, y \in F$, $x \wedge y \in F$.

Clearly, I is an ideal iff $I' = \{a' : a \in I\}$ is a filter, and F is a filter iff $F' = \{a' : a \in F\}$ is an ideal.

We define the operation of symmetric difference in Boolean algebra by $x + y = (x' \wedge y) \vee (x \wedge y')$ (the notation $+$ suggests that this is the addition of the associated Boolean ring).

THEOREM 1.2. Let θ be a binary relation on \mathbf{B} . θ is a congruence iff there exists an ideal I of \mathbf{B} such that $x + y \in I$ iff $(x, y) \in \theta$.

PROOF. Standard. □

DEFINITION 1.3. A filter F on \mathbf{B} is called an *ultrafilter* when $0 \notin F$ and for any filter G on \mathbf{B} such that $F \subsetneq G$, $G = B$. The dual notion is *maximal ideal*.

THEOREM 1.4. A filter F of \mathbf{B} is ultrafilter iff for all $a \in B$ precisely one of a, a' is in F .

PROOF. (\Rightarrow) Let F be an ultrafilter. Clearly it is impossible for any $a \in B$ that both a and a' are in F , as then $0 = a \wedge a' \in F$, and this means $F = B$. On the other hand, assume that for some $a \in B$ neither a nor a' are in F . Then let $G = \{x \in B : (\exists y \in F)(a \wedge y \leq x)\}$. We have that $G \uparrow = G$, since $x_1 \geq x$ for some $x \in G$ implies that $x_1 \geq x \geq y \wedge a$ for some $y \in F$, so $x_1 \in G$. Moreover, if $x_1, x_2 \in G$, then there exist $y_1, y_2 \in F$ such that $x_i \geq y_i \wedge a$. Therefore, $x_1 \wedge x_2 \geq (y_1 \wedge y_2) \wedge a$ and $y_1 \wedge y_2 \in F$ since F is a filter. Hence, G is a filter. Clearly, $F \subsetneq G$ and

$a \in G$, so $F \subsetneq G$. To get a contradiction, we need to show that $0 \notin G$. So, assume that $0 \in G$. Then there exists $y \in F$ such that $a \wedge y \leq 0$, which is equivalent to $y \leq a'$. Therefore, $a' \in F$, a contradiction.

(\Leftarrow) We have that F is a filter and it is not all of B since at least one of $a, a' \notin F$ for any $a \in B$, so assume that a filter G is such that $F \subsetneq G$. This means that for at least one pair $\{a, a'\}$, both a and a' are in G . Then $0 = a \wedge a' \in G$, and so $B = 0 \uparrow = G$. Therefore, F is an ultrafilter. \square

DEFINITION 1.5. A filter F is *prime* if for all $a, b \in B$, if $a \vee b \in F$, then $a \in F$ or $b \in F$. Prime ideals are defined dually.

COROLLARY 1.6. *A filter is prime iff it is an ultrafilter. Dually, an ideal is prime iff it is a maximal ideal.*

PROOF. (\Rightarrow) Let F be a prime filter. Since for any $a \in B$, $a \vee a' = 1 \in F$, then $a \in F$ or $a' \in F$. Then it follows by Theorem 1.4 that F is an ultrafilter.

(\Leftarrow) Let F be an ultrafilter and assume that $a \vee b \in F$. By Theorem 1.4, $(a \vee b)' = a' \wedge b' \notin F$. Since F is a filter, this implies that $a' \notin F$, or $b' \notin F$ and then using Theorem 1.4 again, we get that $a \in F$ or $b \in F$. \square

THEOREM 1.7. *Let F be a filter on \mathbf{B} and $F \neq B$. Then there exists an ultrafilter U on \mathbf{B} such that $F \subseteq U$.*

PROOF. Let $\mathcal{S} = \{G \subseteq B : G \text{ is a filter on } \mathbf{B}, G \neq B \text{ and } F \subseteq G\}$. Clearly, \mathcal{S} is nonempty as $F \in \mathcal{S}$. If we can prove that \mathcal{S} contains a maximal element under the order \subseteq , then this will also be a maximal proper filter on \mathbf{B} , i. e. an ultrafilter, containing F . We need to prove that for any chain $\mathcal{C} \subseteq \mathcal{S}$ of filters, $\bigcup \mathcal{C}$ is a filter in \mathcal{S} and then Zorn's Lemma will finish the proof. Clearly, $F \subseteq \bigcup \mathcal{C}$ and $0 \notin \bigcup \mathcal{C}$. Assume $a \in \bigcup \mathcal{C}$ and $a \leq b$. Then $a \in G \in \mathcal{C}$ for some G , so since G is a filter, $b \in G \subseteq \bigcup \mathcal{C}$. Hence, $(\bigcup \mathcal{C}) \uparrow = \bigcup \mathcal{C}$. Moreover, if $a, b \in \bigcup \mathcal{C}$ then there exist $G, H \in \mathcal{C}$ such that $a \in G$ and $b \in H$. Since \mathcal{C} is a chain, $G \subseteq H$ or $H \subseteq G$. In either case, a filter in \mathcal{C} contains both a and b , so it contains $a \wedge b$. Therefore, $a \wedge b \in \bigcup \mathcal{C}$, so $\bigcup \mathcal{C}$ is a filter, finishing our proof. \square

2. Two theorems of Model Theory

In this section we prove two basic and fundamental results of Model Theory. Though they hold for arbitrary structures (or models), having relations and operations in their language, we just prove them in case of algebras. The more general results are proved analogously. First we

define a construction used for building new algebras (structures) from a class of algebras (structures) \mathcal{K} which preserves more than just the identities (atomic formulae) of \mathcal{K} .

DEFINITION 2.1. Let $\{\mathbf{A}_i : i \in I\}$ be a family of algebras and $\mathbf{A} = \prod_{i \in I} \mathbf{A}_i$. Then for $\bar{a}_1, \bar{a}_2 \in A$, we denote $\llbracket \bar{a}_1 = \bar{a}_2 \rrbracket = \{i \in I : \bar{a}_1(i) = \bar{a}_2(i)\}$. In general, if $\Phi(x_1, \dots, x_n)$ is a first-order formula and $\bar{a}_1, \dots, \bar{a}_n \in A$, then $\llbracket \Phi^{\mathbf{A}}(\bar{a}_1, \dots, \bar{a}_n) \rrbracket = \{i \in I : \mathbf{A}_i \models \Phi^{\mathbf{A}_i}(\bar{a}_1(i), \dots, \bar{a}_n(i))\}$.

DEFINITION 2.2. Let $\{\mathbf{A}_i : i \in I\}$ be a family of algebras, $\mathbf{A} = \prod_{i \in I} \mathbf{A}_i$ and F a filter on $\mathbf{P}(I)$. $\theta_F \in \text{Con } \mathbf{A}$ by $(\bar{a}_1, \bar{a}_2) \in \theta_F$ iff $\llbracket \bar{a}_1 = \bar{a}_2 \rrbracket \in F$. We call the factor algebra \mathbf{A}/θ_F a *reduced product* of \mathbf{A}_i (modulo F). If F happens to be an ultrafilter, we call \mathbf{A}/θ_F an *ultraproduct* of \mathbf{A}_i (modulo F).

If \mathcal{K} is a class of algebras, denote by $\mathbf{P}_R(\mathcal{K})$ and $\mathbf{P}_U(\mathcal{K})$ the classes of all algebras which are isomorphic to reduced products and to ultraproducts of algebras in \mathcal{K} , respectively. We abuse the terminology slightly by saying F is a filter (ultrafilter) on I , meaning that it is a filter (ultrafilter) on $\mathbf{P}(I)$. Also, sometimes we will write just F (where F is a filter) instead of θ_F , when there is no possibility of confusion. For example, we will write \bar{a}/F , $\prod_{i \in I} \mathbf{A}_i/F$ and so on.

THEOREM 2.3 (Łoś). Let $\{\mathbf{A}_i : i \in I\}$ be a family of algebras, $\mathbf{A} = \prod_{i \in I} \mathbf{A}_i$ and let U be an ultrafilter on $\mathbf{P}(I)$. Then for all formulas $\Phi(x_1, \dots, x_n)$ and $\bar{a}_1, \dots, \bar{a}_n \in A$, $\mathbf{A}/U \models \Phi^{\mathbf{A}/U}(\bar{a}_1/U, \dots, \bar{a}_n/U)$ iff $\llbracket \Phi^{\mathbf{A}}(\bar{a}_1, \dots, \bar{a}_n) \rrbracket \in U$.

PROOF. We prove this by an induction on the complexity of Φ . Assume that $\Phi(x_1, \dots, x_n)$ is an identity $p(x_1, \dots, x_n) \approx q(x_1, \dots, x_n)$. $\mathbf{A}/U \models p^{\mathbf{A}/U}(\bar{a}_1/U, \dots, \bar{a}_n/U) \approx q^{\mathbf{A}/U}(\bar{a}_1/U, \dots, \bar{a}_n/U)$ iff $(p^{\mathbf{A}}(\bar{a}_1, \dots, \bar{a}_n), q^{\mathbf{A}}(\bar{a}_1, \dots, \bar{a}_n)) \in \theta_U$ iff $\llbracket p^{\mathbf{A}}(\bar{a}_1, \dots, \bar{a}_n) = q^{\mathbf{A}}(\bar{a}_1, \dots, \bar{a}_n) \rrbracket \in U$. It is sufficient to prove the induction step for connectives \wedge and \neg and for the quantifier \forall , as other connectives and the quantifier \exists can be expressed by some composition of these.

Let $\Phi(x_1, \dots, x_n) = \Phi_1(x_1, \dots, x_n) \wedge \Phi_2(x_1, \dots, x_n)$. Then $\mathbf{A}/U \models \Phi^{\mathbf{A}/U}(\bar{a}_1/U, \dots, \bar{a}_n/U)$ iff $\mathbf{A}/U \models \Phi_1^{\mathbf{A}/U}(\bar{a}_1/U, \dots, \bar{a}_n/U)$ and $\mathbf{A}/U \models \Phi_2^{\mathbf{A}/U}(\bar{a}_1/U, \dots, \bar{a}_n/U)$ iff (by inductive assumption) $\llbracket \Phi_1^{\mathbf{A}}(\bar{a}_1, \dots, \bar{a}_n) \rrbracket \in U$ and $\llbracket \Phi_2^{\mathbf{A}}(\bar{a}_1, \dots, \bar{a}_n) \rrbracket \in U$ iff (since U is a filter) $\llbracket \Phi_1^{\mathbf{A}}(\bar{a}_1, \dots, \bar{a}_n) \rrbracket \cap \llbracket \Phi_2^{\mathbf{A}}(\bar{a}_1, \dots, \bar{a}_n) \rrbracket = \llbracket \Phi_1^{\mathbf{A}}(\bar{a}_1, \dots, \bar{a}_n) \wedge \Phi_2^{\mathbf{A}}(\bar{a}_1, \dots, \bar{a}_n) \rrbracket \in U$.

Let $\Phi(x_1, \dots, x_n) = \neg\Psi(x_1, \dots, x_n)$. Then $\mathbf{A}/U \models \Phi^{\mathbf{A}/U}(\bar{a}_1/U, \dots, \bar{a}_n/U)$ iff $\mathbf{A}/U \not\models \Psi^{\mathbf{A}/U}(\bar{a}_1/U, \dots, \bar{a}_n/U)$ iff $\llbracket \Psi^{\mathbf{A}}(\bar{a}_1, \dots, \bar{a}_n) \rrbracket \notin U$ iff (since U is an ultrafilter) $\llbracket \Phi^{\mathbf{A}}(\bar{a}_1, \dots, \bar{a}_n) \rrbracket \in U$.

Let $\Phi(x_1, \dots, x_n) = (\forall x)\Psi(x, x_1, \dots, x_n)$. Then $\mathbf{A}/U \models \Phi^{\mathbf{A}/U}(\bar{a}_1/U, \dots, \bar{a}_n/U)$ iff for all $\bar{a} \in A$, $\mathbf{A}/U \models \Psi^{\mathbf{A}/U}(\bar{a}/U, \bar{a}_1/U, \dots, \bar{a}_n/U)$ iff for all $\bar{a} \in A$, $\llbracket \Psi^{\mathbf{A}}(\bar{a}, \bar{a}_1, \dots, \bar{a}_n) \rrbracket \in U$. This is clearly implied by $\llbracket \Phi^{\mathbf{A}}(\bar{a}_1, \dots, \bar{a}_n) \rrbracket \in U$, as $\llbracket \Phi^{\mathbf{A}}(\bar{a}_1, \dots, \bar{a}_n) \rrbracket \subseteq \llbracket \Psi^{\mathbf{A}}(\bar{a}, \bar{a}_1, \dots, \bar{a}_n) \rrbracket$ for all $\bar{a} \in \mathbf{A}$. On the other hand, for each $i \in I$ such that $\Phi^{\mathbf{A}_i}(\bar{a}_1(i), \dots, \bar{a}_n(i))$ fails in \mathbf{A}_i , pick a $\bar{c}(i) \in A_i$ such that $\Psi^{\mathbf{A}_i}(\bar{c}(i), \bar{a}_1(i), \dots, \bar{a}_n(i))$ fails in \mathbf{A}_i . Complete the other coordinates of \bar{c} to a member of A in an arbitrary way, and we found an element $\bar{c} \in A$ such that $\llbracket \Psi^{\mathbf{A}}(\bar{c}, \bar{a}_1, \dots, \bar{a}_n) \rrbracket = \llbracket \Phi^{\mathbf{A}}(\bar{a}_1, \dots, \bar{a}_n) \rrbracket$. Therefore, if for all $\bar{a} \in A$, $\llbracket \Psi^{\mathbf{A}}(\bar{c}, \bar{a}_1, \dots, \bar{a}_n) \rrbracket \in U$, then $\llbracket \Phi^{\mathbf{A}}(\bar{a}_1, \dots, \bar{a}_n) \rrbracket \in U$. \square

The following corollary is a most applicable consequence of Theorem 2.3.

COROLLARY 2.4. *If \mathcal{K} is a class of algebras and Φ is a first-order sentence, then $\mathcal{K} \models \Phi$ implies $\mathbf{P}_U(\mathcal{K}) \models \Phi$.*

PROOF. Obvious. \square

Note that in the above proof we used the property of being an ultrafilter only in closure under negation. If we wrote it out, we would have had to use it also for closure under \forall and \exists . So, any reduced product would satisfy the statement of Theorem 2.3 for all formulae Φ using only \forall and \wedge . Indeed, a slightly stronger result is not hard to prove, that the reduced products preserve quasiidentities, or Horn formulas, which are expressions of the form $(\bigwedge_{i=1}^n (\varepsilon_i)) \Rightarrow \varepsilon$, where ε and all ε_i are identities. We do not need this result, though, as quasiidentities are not a topic of this text, but we may mention that there exists a significant body of results concerning classes of algebras which are models of some set of quasiidentities, so-called quasivarieties, and that Willard's finite basis theorem has been successfully extended in their setting by Maróti and McKenzie [17].

DEFINITION 2.5. We call a class \mathcal{K} of algebras (structures) an *elementary class* if there exists a set Σ of sentences such that $\mathcal{K} = \text{Mod}(\Sigma)$. We say that \mathcal{K} is a *strictly elementary class* if there exists a sentence Φ such that $\mathcal{K} = \text{Mod}(\Phi)$.

Note that varieties are strictly elementary classes, as we can consider each identity as an universally closed atomic formula, while a

finitely based variety is a strictly elementary class, since we can write Φ to be the universal closure of conjunction of the basis equations.

THEOREM 2.6 (Compactness Theorem). *Let Σ be a set of first-order sentences such that for every finite $\Sigma_0 \subseteq \Sigma$ there exists a model of Σ_0 . Then there exists a model of Σ .*

PROOF. Let I be the set of all finite subsets of Σ and for each $i \in I$, let $\mathbf{A}_i \models i$. Let $J_i = \{j \in I : i \subseteq j\}$. Define $F = \{J \subseteq I : J_i \subseteq J\} = \bigcup_{i \in I} J_i \uparrow$.

We wish to prove that F is a proper filter on I . Clearly, $F \uparrow = F$. If $J, K \in F$, then there exist $i, j \in I$ such that $J_i \subseteq J$ and $J_j \subseteq K$. Since $J_i \cap J_j = J_{i \cup j}$, then $J_{i \cup j} \subseteq J \cap K$ and $J_{cap} K \notin J$. Since $i \in J_i$ for all $i \in I$, then all J_i are nonempty, and every $J \in F$ is therefore also nonempty.

So, according to Theorem 1.7, there exists an ultrafilter U on I such that $F \subseteq U$. Now, let $\mathbf{A} = \prod_{i \in I} \mathbf{A}_i / U$. We claim that for all $\Phi \in \Sigma$, $\mathbf{A} \models \Phi$. Let $\Phi \in \Sigma$ be arbitrary and let $\{i_0\} = i_0 \in I$. For all $j \in I$ such that $i_0 \subseteq j$, $\mathbf{A}_j \models \Phi$ (as $\Phi \in j$). Therefore, $J_{i_0} \subseteq \llbracket \Phi \rrbracket$, so $\llbracket \Phi \rrbracket \in F \subseteq U$. Therefore, according to Theorem 2.3, $\mathbf{A} \models \Phi$. \square

The following corollary is used so often that some authors call it the Compactness Theorem. In a way it is justified, as it 'sounds' more like the topological notion of compactness.

COROLLARY 2.7. *Let Σ be a set of sentences and Φ another sentence. If $\Sigma \models \Phi$, then for some finite $\Sigma_0 \subseteq \Sigma$, $\Sigma_0 \models \Phi$.*

PROOF. Assume that for every finite $\Sigma_0 \subseteq \Sigma$, $\Sigma_0 \cup \{\neg\Phi\}$ has a model. Then every finite $\Sigma_1 \subseteq (\Sigma \cup \{\neg\Phi\})$ has a model (any model of $\Sigma_1 \cup \{\neg\Phi\}$ is a model of Σ_1). Therefore, according to Theorem 2.6, $\Sigma \cup \{\neg\Phi\}$ has a model \mathbf{A} , which contradicts $\Sigma \models \Phi$. \square

3. Definable principal congruences

Before proving Baker's result, we take a short detour to prove another finite basis result due to McKenzie in [19].

DEFINITION 3.1. A *principal congruence formula* of similarity type \mathcal{F} is any formula $\pi(x, y, u, v)$ which describes a Mal'cev chain implying that $(x, y) \in \text{Cg}^{\mathbf{A}}(u, v)$ when $\pi(x, y, u, v)$ holds in \mathbf{A} . Formally, π is of the form

$$(\exists \bar{w}) \left(x = p_1(z_1, \bar{w}) \wedge y = p_n(z'_n, w) \wedge \bigwedge_{1 \leq i \leq n} p_i(z'_i, \bar{w}) = p_{i+1}(z_{i+1}, \bar{w}) \right)$$

where $\bar{w} = (w_1, \dots, w_k)$ is a tuple of variables, p_i are terms in $k + 1$ variables and $\{z_i, z'_i\} = \{u, v\}$ for all i , $1 \leq i \leq n$.

Note that we avoid stating that we have to use different parameters by enlarging the variable set over which p_i are defined. We denote the set of all principal congruence formulas of the similarity type \mathcal{F} by Π .

THEOREM 3.2. *Let \mathbf{A} be an \mathcal{F} -algebra and $a, b, c, d \in A$. Then $(a, b) \in \text{Cg}^{\mathbf{A}}(c, d)$ iff there exists $\pi \in \Pi$ such that $\pi(a, b, c, d)$ holds in \mathbf{A} .*

PROOF. This is the same theorem as Theorem III.3.8. \square

DEFINITION 3.3. A class of algebras \mathcal{K} has *definable principal congruences* if there exists a first-order formula $\phi(x, y, z, u)$ such that for all $\mathbf{A} \in \mathcal{K}$ and $a, b, c, d \in a$, $\mathbf{A} \models \phi(a, b, c, d)$ iff $(a, b) \in \text{Cg}^{\mathbf{A}}(c, d)$.

PROPOSITION 3.4. *A variety \mathcal{V} has definable principal congruences iff there exists a finite $\Pi_0 \subseteq \Pi$ such that for all $\mathbf{A} \in \mathcal{V}$ and $a, b, c, d \in A$, $(a, b) \in \text{Cg}^{\mathbf{A}}(c, d)$ iff there exists $\pi \in \Pi_0$ such that $\pi(a, b, c, d)$ holds in \mathbf{A} .*

PROOF. The direction (\Leftarrow) is trivial, as we just take $\phi(x, y, z, u)$ to be $\bigvee_{\pi \in \Pi_0} \pi(x, y, z, u)$.

On the other hand, assume that \mathcal{V} has definable principal congruences realized by a first-order formula $\phi(x, y, z, u)$. Let \mathcal{F}' be the similarity type obtained from \mathcal{F} (the similarity type of algebras in \mathcal{V}) by adding four new constant symbols a, b, c, d into the similarity type \mathcal{F} and let \mathcal{V}' be the class of \mathcal{F}' -algebras defined by $\mathcal{V}' = \{\mathbf{A} : \mathcal{F}\text{-reduct of } \mathbf{A} \text{ is in } \mathcal{V}\}$. In fact, for any system of identities Σ axiomatizing \mathcal{V} , it is also the equational base of \mathcal{V}' , just in the expanded similarity type \mathcal{F}' . (Here by identities we mean the sentences which are universally quantified atomic formulas of equational logic. In this sense, a set of identities which is an equational base of \mathcal{V} axiomatizes \mathcal{V} .) Now take ϕ' to be the \mathcal{F}' -sentence $\neg\phi(a, b, c, d)$ and let Π' be the set of \mathcal{F}' -sentences $\{\neg\pi(a, b, c, d) : \pi(x, y, z, u) \in \Pi\}$. For any $\mathbf{A} \in \mathcal{V}'$ such that $\mathbf{A} \models \Pi'$, we know that $(a^{\mathbf{A}}, b^{\mathbf{A}}) \notin \text{Cg}^{\mathbf{A}}(c^{\mathbf{A}}, d^{\mathbf{A}})$. Therefore, $\mathbf{A} \models \phi'$. By Corollary 2.7, there exists a finite $\Pi_0 \subseteq \Pi$ such that, where

$$\pi'_0 = \bigwedge_{\pi(x, y, z, u) \in \Pi_0} \neg\pi(a, b, c, d),$$

$$\Sigma \cup \pi'_0 \models \phi'.$$

Hence, by deduction theorem and taking the contrapositive,

$$\Sigma \models \phi(a, b, c, d) \Rightarrow \bigvee_{\pi(x, y, z, u) \in \Pi_0} \pi(a, b, c, d).$$

We claim that if $\mathbf{A} \in \mathcal{V}$ and $a', b', c', d' \in A$, $(a', b') \in \text{Cg}^{\mathbf{A}}(c', d')$ iff there exists $\pi \in \Pi_0$ such that $\pi(a', b', c', d')$ holds in \mathbf{A} . The direction (\Leftarrow) trivially holds. On the other hand, take \mathbf{B} to be the \mathcal{F}' -algebra obtained from \mathbf{A} by interpreting $a^{\mathbf{B}} = a'$ and similarly for the other three constants. Since $(a', b') \in \text{Cg}^{\mathbf{A}}(c', d')$, then $\mathbf{B} \models \phi(a, b, c, d)$, and also $\mathbf{B} \models \Sigma$, since $\mathbf{A} \in \mathcal{V}$. Therefore, $\mathbf{B} \models \bigvee_{\pi(x,y,z,u) \in \Pi_0} \pi(a, b, c, d)$, and this means that for some $\pi(x, y, z, u) \in \Pi_0$, $\mathbf{B} \models \pi(a, b, c, d)$. This is the same as saying that $\pi(a', b', c', d')$ holds in \mathbf{A} , as desired. \square

REMARK 3.1. Note that we didn't really need to suppose that \mathcal{V} is a variety in the previous proof, just that it is an elementary class. Moreover, note that we actually proved above that if \mathcal{V} has definable principal congruences, then for some finitely based variety \mathcal{V}' such that $\mathcal{V} \subseteq \mathcal{V}'$, only finitely many principal congruence formulas are needed to establish $(a, b) \in \text{Cg}^{\mathbf{A}}(c, d)$, for all $\mathbf{A} \in \mathcal{V}'$ and $a, b, c, d \in A$.

THEOREM 3.5 (McKenzie). *Let \mathcal{V} be a variety of finite similarity type, having a finite residual bound and definable principal congruences. Then \mathcal{V} is finitely based.*

PROOF. Let $\Pi_0 = \{\pi_1, \dots, \pi_n\}$ be the finite set of principal congruence formulas from Definition 3.1 which witness that \mathcal{V} has definable principal congruences, according to Lemma 3.4, and let $\Phi(x, y, u, v) = \pi_1(x, y, u, v) \vee \dots \vee \pi_n(x, y, u, v)$. We can express by a sentence Ψ_1 the fact that the principal congruence generated by (u, v) consists precisely of pairs (x, y) such that $\Phi(x, y, u, v)$. The idea is to write that for all u, v , the binary relation induced by $\Phi(-, -, u, v)$ is a congruence containing (u, v) (in other words, write that it is an equivalence relation compatible with each of the finitely many operations in the similarity type and containing the pair (u, v)). Since $\Phi(-, -, u, v)$ is always contained in the congruence generated by (u, v) , it must be equal to it. Therefore, $\mathcal{V} \models \Psi_1$.

Then, since \mathcal{V} has a finite residual bound and \mathcal{F} is finite, \mathcal{V} contains only finitely many subdirectly irreducibles $\mathbf{S}_1, \dots, \mathbf{S}_k$, all of them finite. So, express by a sentence Ψ_2 the fact that the algebra is isomorphic to one of \mathbf{S}_i .

Let $\Psi_3 = (\exists x, y)[x \neq y \wedge (\forall u, v)(u \neq v \Rightarrow \Phi(x, y, u, v))]$. Then we claim that $\mathcal{V} \models \Psi_3 \Rightarrow \Psi_2$. Indeed, if $\mathbf{A} \in \mathcal{V}$ and $\mathbf{A} \models \Psi_3$, then there exist $a, b \in A$ such that $a \neq b$ and they are in every congruence generated by a pair of different elements c, d of A . So, $\text{Cg}^{\mathbf{A}}(a, b)$ is the monolith and \mathbf{A} is subdirectly irreducible. Therefore $\mathbf{A} \models \Psi_2$, as well.

Now, let Σ be the set of all identities of \mathcal{V} on a countably infinite set of variables. According to Theorem III.2.9, Σ axiomatizes \mathcal{V} . Since

$\mathcal{V} \models \Psi_1 \wedge (\Psi_3 \Rightarrow \Psi_2)$, then $\Sigma \models \Psi_1 \wedge (\Psi_3 \Rightarrow \Psi_2)$. Therefore, according to Corollary 2.7, there exists a finite set $\Sigma_0 \subseteq \Sigma$ such that $\Sigma_0 \models \Psi_1 \wedge (\Psi_3 \Rightarrow \Psi_2)$. We claim that $\mathcal{V} = \text{Mod}(\Sigma_0)$.

Let \mathbf{A} be any subdirectly irreducible algebra of the same similarity type as \mathcal{F} such that $\mathbf{A} \models \Sigma_0$. Then $\mathbf{A} \models \Psi_1 \wedge (\Psi_3 \Rightarrow \Psi_2)$. Since $\mathbf{A} \models \Psi_1$, we know that for all $a, b, c, d \in A$, $\Phi(a, b, c, d)$ is true in \mathbf{A} iff $(a, b) \in \text{Cg}^{\mathbf{A}}(c, d)$. Since \mathbf{A} is subdirectly irreducible, it has a monolith congruence μ and $\mathbf{A} \models \Psi_2$ with any pair of elements $(a, b) \in \mu \setminus 0_A$ taken as (x, y) . Therefore, we get that $\mathbf{A} \models \Psi_3$, so $\mathbf{A} \in \mathcal{V}$.

We conclude that any \mathcal{F} -algebra \mathbf{B} such that $\mathbf{B} \models \Sigma_0$ is isomorphic to a subdirect product of its subdirectly irreducible factors, which are all in \mathcal{V} . So, $\mathbf{B} \in \mathcal{V}$. \square

4. Jónsson's Lemma

Jónsson's Lemma is one of the most often-used tools in the setting of congruence distributive varieties. Before stating Jónsson's Lemma, we need to prove two easy results.

LEMMA 4.1. *Let $\{\mathbf{B}_1, \dots, \mathbf{B}_k\}$ be a finite set of finite algebras in finite language and let $\{\mathbf{A}_i : i \in I\}$ be a family of algebras such that for all $i \in I$ there exists some j , $1 \leq j \leq k$, so that $\mathbf{A}_i \cong \mathbf{B}_j$. Let $\mathbf{A} = \prod_{i \in I} \mathbf{A}_i / U$ for some ultrafilter U on I . Then $\mathbf{A} \cong \mathbf{B}_j$ for some $1 \leq j \leq k$.*

PROOF. For each finite algebra \mathbf{B}_i we can find a sentence Φ_i such that $\mathbf{A} \models \Phi_i$ iff $\mathbf{A} \cong \mathbf{B}_i$. Then make the sentence $\Psi_j = \Phi_1 \vee \Phi_2 \vee \dots \vee \Phi_j$, for $j \leq k$. Clearly, $\llbracket \Psi_k \rrbracket = I \in U$. Let j be minimal such that $\llbracket \Psi_j \rrbracket \in U$. We want to prove $\llbracket \Phi_j \rrbracket \in U$, which would finish the proof, according to Theorem 2.3. If $j = 1$, then $\llbracket \Phi_1 \rrbracket \in U$, otherwise, from $\llbracket \Psi_j \rrbracket = \llbracket \Psi_{j-1} \vee \Phi_j \rrbracket = \llbracket \Psi_{j-1} \rrbracket \cup \llbracket \Phi_j \rrbracket$ and Theorem 1.6 we get $\llbracket \Phi_j \rrbracket \in U$, since $\llbracket \Psi_{j-1} \rrbracket \notin U$. \square

LEMMA 4.2. *Let $\mathcal{W} \subseteq P(I)$ be such that*

- (i) $I \in \mathcal{W}$
- (ii) $\mathcal{W} \uparrow = \mathcal{W}$
- (iii) *For all $J, K \subseteq I$, if $J \cup K \in \mathcal{W}$, then $J \in \mathcal{W}$ or $K \in \mathcal{W}$.*

Then there exists an ultrafilter $U \subseteq \mathcal{W}$.

PROOF. If $\mathcal{W} = P(I)$, then any ultrafilter will satisfy the Lemma. Otherwise, let $\mathcal{I} = P(I) \setminus \mathcal{W}$. Then \mathcal{I} is an ideal on I and by the dual of Theorem 1.7, there exists a maximal ideal $\mathcal{M} \subseteq P(I)$ such that $\mathcal{I} \subseteq \mathcal{M}$. Then $U = P(I) \setminus \mathcal{M}$ is the desired ultrafilter. \square

DEFINITION 4.3. An algebra \mathbf{A} is finitely subdirectly irreducible if $0_{\mathbf{A}}$ is a \wedge -irreducible element of $\mathbf{Con} \mathbf{A}$. The subclass of all finitely subdirectly irreducible members of a class of algebras \mathcal{K} is denoted by \mathcal{K}_{FSI} .

The following theorem is a slightly strengthened version of the Jónsson's Lemma.

THEOREM 4.4 (Jónsson's Lemma). *Let \mathcal{K} be a class of algebras such that $\mathcal{V} = \mathcal{V}(\mathcal{K})$ is a congruence distributive variety. Then $\mathcal{V}_{SI} \subseteq \mathcal{V}_{FSI} \subseteq \mathbf{HSP}_U(\mathcal{K})$. In particular, $\mathcal{V} = \mathbf{P}_5\mathbf{HSP}_U(\mathcal{K})$.*

PROOF. Let $\mathbf{A} \in \mathcal{V}_{FSI}$. Therefore, there exist algebras $\mathbf{A}_i \in \mathcal{K}$, $i \in I$, an algebra $B \leq \prod_{i \in I} \mathbf{A}_i$ and a \wedge -irreducible congruence $\theta \in \mathbf{Con} \mathbf{B}$ such that $\mathbf{A} \cong \mathbf{B}/\theta$. For $J \subseteq I$, let $\pi_J : \prod_{i \in I} \mathbf{A}_i \rightarrow \prod_{i \in J} \mathbf{A}_i$ be the projection homomorphism and $\alpha_J = \{(\bar{a}_1, \bar{a}_2) \in \prod_{i \in I} A_i : \llbracket a_1 = a_2 \rrbracket \in J\} = \ker \pi_J$. Denote by $\eta_J = \alpha_J \cap B^2$.

Define \mathcal{W} to be $\{J \subseteq I : \eta_J \subseteq \theta\}$. We desire to prove that \mathcal{W} contains an ultrafilter U on I . We know that $I \in \mathcal{W}$, as α_I is the equality relation, so $\eta_I = 0_B \subseteq \theta$. Also, if $J \subseteq K$, then $\eta_K \subseteq \eta_J$, so $\mathcal{W} \uparrow = \mathcal{W}$. Finally, if $J \cup K \in \mathcal{W}$, then $\eta_{J \cup K} \subseteq \theta$. Now, $\theta_{J \cup K} = \theta_J \cap \theta_K$, so $\eta_{J \cup K} = \theta_{J \cup K} \cap B^2 = (\theta_J \cap B^2) \cap (\theta_K \cap B^2) = \eta_J \cap \eta_K$. Therefore, from $\theta = \theta \vee \eta_{J \cup K}$ we get $\theta = \theta \vee (\eta_J \wedge \eta_K) = (\theta \vee \eta_J) \wedge (\theta \vee \eta_K)$ by congruence distributivity. Since θ is \wedge -irreducible, we get that $\theta = \theta \vee \eta_J$ or $\theta = \theta \vee \eta_K$, so $J \in \mathcal{W}$ or $K \in \mathcal{W}$. According to Lemma 4.2, we can select an ultrafilter U on I such that $U \subseteq \mathcal{W}$.

Now, $(\bar{b}_1, \bar{b}_2) \in \theta_U \cap B^2$ implies that for $J = \llbracket \bar{b}_1 = \bar{b}_2 \rrbracket$, $J \in U \subseteq \mathcal{W}$, so $\eta_J \subseteq \theta$ and $(\bar{b}_1, \bar{b}_2) \in \theta$. Therefore, $\mathbf{A} \in \mathbf{H}(\mathbf{B}/(\theta_U \cap B^2))$ and as $\mathbf{B}/(\theta_U \cap B^2) \subseteq \prod_{i \in I} /\theta_U \in \mathbf{P}_U(\mathcal{K})$, the result follows. The last sentence follows from Theorem III.1.6. \square

COROLLARY 4.5. *Let \mathcal{K} be a finite class of finite algebras in a finite language such that $\mathcal{V} = \mathcal{V}(\mathcal{K})$ is a congruence distributive variety. Then $\mathcal{V}_{SI} \subseteq \mathcal{V}_{FSI} \subseteq \mathbf{HS}(\mathcal{K})$.*

PROOF. By application of Lemma 4.1 to the conclusion of Jónsson's Lemma. \square

5. Baker's Theorem

"Though it lacks profundity, it is an interesting fact about finite lattices that each has a finite base. In this section we establish that fact."

This is a quote from McKenzie's paper [19]. The fact which 'lacks profundity' was the starting point for all finite basis research in universal algebra in the following 35 years, and almost all results which were proved were generalizations of it. The first one was Baker's finite basis theorem.

We assume throughout this section that \mathcal{V} is a congruence distributive variety with Jónsson terms p_0, p_1, \dots, p_n and that the language \mathcal{F} of \mathcal{V} is finite. We need an easy corollary of Theorem III.3.12, which gives, in fact, another equivalent condition for congruence distributivity (we will not prove it in this text):

LEMMA 5.1. *There exist terms $p_1 \dots, p_{n-1}$ such that the following hold in \mathcal{V} :*

- (1) $p_i(x, u, x) \approx p_i(x, v, x)$ for all p_i and
- (2) If $x \neq y$ then there exists an i , $0 < i < n$, so that $p_i(x, x, y) \neq p_i(x, y, y)$.

PROOF. We use the Jónsson terms with the same indices. (1) is an immediate corollary of $p_i(x, y, x) \approx x$, while (2) is proved by assuming the opposite: if for all i , $0 < i < n$, $p_i(x, x, y) = p_i(x, y, y)$, then $x = p_1(x, x, y) = p_1(x, y, y) = p_2(x, y, y) = \dots = y$. \square

We will denote by Φ_1 the sentence

$$(\forall x, u, v) \left(\bigwedge_{0 < i < n} p_i(x, u, x) = p_i(x, v, x) \right) \wedge$$

$$(\forall x, y) \left(x \neq y \Leftrightarrow \bigvee_{0 < i < n} p_i(x, x, y) \neq p_i(x, y, y) \right).$$

We now also assume that the language \mathcal{F} contains all p_i , $0 < i < n$, as ternary operation symbols. This assumption is not necessary, but it does make the proof easier to write. The reader can remove this assumption and in the remainder of the section replace every word 'translation' by 'unary polynomial which would have been a translation if p_i were basic operations' and similarly with 'slender term', 'linear term' and other such syntactic notions, and the proof would work just fine. Alternatively, like in [6], one can add new ternary operation symbols t_i to the language of \mathcal{V} and equations $t_i \approx p_i$ and prove that if the new variety has a finite basis, then so does \mathcal{V} .

DEFINITION 5.2. A term is *slender* if it is a variable, or if there exist a k -ary operation symbol f , a slender term p and variables x_1, \dots, x_{k-1} such that $t = f(x_1, \dots, x_{i-1}, p, x_i, \dots, x_{k-1})$. A term is *linear* if there is no variable with more than one occurrence in t .

DEFINITION 5.3. Let $p(x) \in \text{Pol}_1 \mathbf{A}$ be a polynomial. $p(x)$ is a *basic translation* of an algebra \mathbf{A} if $p(x) = f^{\mathbf{A}}(x, a_1, \dots, a_k)$ for some $k + 1$ -ary operation of the language. $p(x)$ is a *translation* of \mathbf{A} if $p(x) = (q_1 \circ \dots \circ q_m)(x)$, for some basic translations q_i of \mathbf{A} . The set of all translations of \mathbf{A} will be denoted by $\text{Tr } \mathbf{A}$.

REMARK 5.1. From Definition 5.3 it follows that $p(x) \in \text{Tr } \mathbf{A}$ iff there exists a slender linear term $t(x, y_1, \dots, y_k)$ such that $p(x) = t^{\mathbf{A}}(x, a_1, \dots, a_k)$ and the (only) occurrence of x in t is at the maximal depth among variables of t . It is not hard to show that if a polynomial $p(x) = t^{\mathbf{A}}(x, a_1, \dots, a_k)$ and t is a linear term, we can find a slender linear term $t_1 = (x, z_1, \dots, z_l)$ such that the only occurrence of x is at maximal depth among the variables in t_1 and $p(x) = t_1^{\mathbf{A}}(x, b_1, \dots, b_l)$ - just write $t = t_1(x, q_1, \dots, q_l)$, where $q_i(y_1, \dots, y_k)$ are subterms of t and let $b_i = q_i^{\mathbf{A}}(a_1, \dots, a_k)$.

LEMMA 5.4. *We can replace $\text{Pol}_1 \mathbf{A}$ by $\text{Tr } \mathbf{A}$ in the statement of Theorem III.3.8.*

PROOF. We need to connect $p(a)$ and $p(b)$ with a chain of images of $\{a, b\}$ under translations. First, we pick a term $t(x, y_1, \dots, y_k)$ such that $p(x) = t^{\mathbf{A}}(x, a_1, \dots, a_k)$. Then let $t_\ell(x_1, \dots, x_r, z_1, \dots, z_m)$ be the linear term with the same term tree as t such that $t = \alpha(t_\ell)$ in the term algebra \mathbf{T} , where α is the substitution which maps all x_i to x while for all z_i , $\alpha(z_i) = y_{j(i)}$. Now, for all i , $1 \leq i \leq m_0$, let $c_i = t_\ell^{\mathbf{A}}(\underbrace{a, \dots, a}_i, \underbrace{b, \dots, b}_{r-i}, a_{j(1)}, \dots, a_{j(m)})$. Now, $a = c_0$, $b = c_r$ and $\{c_{i-1}, c_i\} = \{q_i(a), q_i(b)\}$, where $q_i(x_i)$ is the unary polynomial obtained by substituting all variables of the linear term t_ℓ except for x_ℓ as in the definition of c_i (and c_{i-1}). Now, according to Remark 5.1, $q_i \in \text{Tr } \mathbf{A}$ for all $1 \leq i \leq r$. \square

LEMMA 5.5. *Let \mathbf{A} be any algebra of similarity type \mathcal{F} satisfying Φ_1 and let $a, b, c, d \in A$. Then $\text{Cg}^{\mathbf{A}}(a, b) \cap \text{Cg}^{\mathbf{A}}(c, d) \neq 0_{\mathbf{A}}$ iff there exist $p, q \in \text{Tr } \mathbf{A}$ and i , $0 < i < n$ such that $p_i^{\mathbf{A}}(p(a), q(c), p(b)) \neq p^{\mathbf{A}}(p(a), q(d), p(b))$.*

PROOF. (\Rightarrow) Let $(e, f) \in \text{Cg}^{\mathbf{A}}(a, b) \cap \text{Cg}^{\mathbf{A}}(c, d)$ and $e \neq f$. Then according to Φ_1 , there exist j , $1 < j < n$ such that $p_j^{\mathbf{A}}(e, e, f) \neq p_j^{\mathbf{A}}(e, f, f)$. As $(e, f) \in \text{Cg}^{\mathbf{A}}(a, b)$, this implies that there exists $\hat{p} \in \text{Tr } \mathbf{A}$ such that $e' := p_j^{\mathbf{A}}(e, \hat{p}(a), f) \neq p_j^{\mathbf{A}}(e, \hat{p}(b), f) =: f'$, by Lemma 5.4. Notice that $(e', f') \in \text{Cg}^{\mathbf{A}}(e, f)$, since $(p_j^{\mathbf{A}}(e, \hat{p}(a), f), p_j^{\mathbf{A}}(e, \hat{p}(a), e)) \in \text{Cg}^{\mathbf{A}}(e, f)$, then $p_j^{\mathbf{A}}(e, \hat{p}(a), e) = p_j^{\mathbf{A}}(e, \hat{p}(b), e)$, according to Φ_1 , and

$(p_j^{\mathbf{A}}(e, \hat{p}(b), e), p_j^{\mathbf{A}}(e, \hat{p}(b), f)) \in \text{Cg}^{\mathbf{A}}(e, f)$. Therefore, as $e' \neq f'$ and $(e', f') \in \text{Cg}^{\mathbf{A}}(e, f) \subseteq \text{Cg}^{\mathbf{A}}(c, d)$, we can repeat the argument from the beginning of this proof with c, d, e', f' replacing a, b, e, f , respectively. We get that there exists $q(x) \in \text{Tr } \mathbf{A}$ and $i, 0 < i < n$ so that $p_i^{\mathbf{A}}(e', q(c), f') \neq p_i^{\mathbf{A}}(e', q(d), f')$. Define $p(x) = p_j^{\mathbf{A}}(e, \hat{p}(x), f)$, so $p(x) \in \text{Tr } \mathbf{A}$, $e' = p(a)$ and $f' = p(b)$. This completes the proof of (\Rightarrow) .

(\Leftarrow) According to Φ_1 , $(p_i^{\mathbf{A}}(p(a), q(c), p(b)), p_i^{\mathbf{A}}(p(a), q(d), p(b))) \in \text{Cg}^{\mathbf{A}}(a, b)$, similarly as in the previous paragraph. Obviously, we always have $(p_i^{\mathbf{A}}(p(a), q(c), p(b)), p_i^{\mathbf{A}}(p(a), q(d), p(b))) \in \text{Cg}^{\mathbf{A}}(c, d)$. Therefore, since $p_i^{\mathbf{A}}(p(a), q(c), p(b)) \neq p_i^{\mathbf{A}}(p(a), q(d), p(b))$, $\text{Cg}^{\mathbf{A}}(a, b) \cap \text{Cg}^{\mathbf{A}}(c, d) \neq 0_{\mathbf{A}}$ follows. \square

We define for $m \in \omega$ the set $T_m^* \subseteq T(\{x, y_1, y_2, \dots, y_{m(r-1)}\})$ of \mathcal{F} -terms, where r is the maximal arity of an operation symbol in \mathcal{F} to be all slender and linear \mathcal{F} -terms t in variables $\{x, y_1, y_2, \dots, y_{m(r-1)}\}$ such that the depth of any occurrence of a variable in t is at most m and the occurrence of x is at the maximal depth in t among the variables occurring in t . For all $m \in \omega$, T_m^* is finite,

DEFINITION 5.6. Let $\delta_m(x, y, u, v)$ be the first-order formula

$$\bigvee_{\substack{0 < i < n \\ p, q \in T_m^*}} (\exists \bar{z}, \bar{w}) p_i(p(x, \bar{z}), q(u, \bar{w}), p(y, \bar{z})) \neq p_i(p(x, \bar{z}), q(v, \bar{w}), p(y, \bar{z})).$$

LEMMA 5.7. Let \mathbf{A} be any algebra of similarity type \mathcal{F} satisfying Φ_1 and let $a, b, c, d \in A$. Then $\text{Cg}^{\mathbf{A}}(a, b) \cap \text{Cg}^{\mathbf{A}}(c, d) \neq 0_{\mathbf{A}}$ iff there exist $m \in \omega$ such that $\mathbf{A} \models \delta_m(a, b, c, d)$.

PROOF. Since each $p(x) \in \text{Tr } \mathbf{A}$ can be obtained from some term $t \in T_m^*$ for some $m \in \omega$ by evaluation of all variables except x , according to Remark 5.1, this is just a restatement of Lemma 5.5. \square

DEFINITION 5.8. Let γ_m be the sentence $(\forall x, y, u, v)(\delta_{m+1}(x, y, u, v) \Rightarrow \delta_m(x, y, u, v))$.

LEMMA 5.9. Let \mathbf{A} be any algebra of similarity type \mathcal{F} . Then $\mathbf{A} \models \gamma_m$ implies $\mathbf{A} \models \gamma_{m+1}$. Also if $\mathbf{A} \models \gamma_m$ and for $a, b, c, d \in A$ and $k \in \omega$, $\delta_k(a, b, c, d)$ holds in \mathbf{A} , then $\delta_m(a, b, c, d)$ holds in \mathbf{A} .

PROOF. Assume that $\mathbf{A} \models \gamma_m$ and that for some $a, b, c, d \in A$, $\delta_{m+2}(a, b, c, d)$ holds. Then let the terms $p, q \in T_{m+2}^*$ witnessing δ_{m+2} be such that $p = p'(f(y_{i_1}, \dots, y_{i_{l-1}}, x, y_{i_l}, \dots, y_{i_{k-1}}), y_1, \dots, y_{(m+1)(r-1)})$, $q = q'(g(y_{i'_1}, \dots, y_{i'_{j'-1}}, x, y_{i'_j}, \dots, y_{i'_{r'-1}}), y_1, \dots, y_{(m+1)(r-1)})$ for some $f, g \in \mathcal{F}$, $\{i_1, \dots, i_{k-1}\}, \{i'_1, \dots, i'_{k'-1}\} \subseteq \{y_{(m+1)(r-1)+1}, \dots, y_{(m+2)(r-1)}\}$ and $p', q' \in T_{m+1}^*$. We know that $p_i^{\mathbf{A}}(p^{\mathbf{A}}(a, \bar{z}), q^{\mathbf{A}}(c, \bar{w}), p^{\mathbf{A}}(b, \bar{z})) \neq$

$p_i^{\mathbf{A}}(p^{\mathbf{A}}(a, \bar{z}), q^{\mathbf{A}}(d, \bar{w}), p^{\mathbf{A}}(b, \bar{z}))$ for some $\bar{z}, \bar{w} \in A^{(m+2)(r-1)}$. Let $a' = f^{\mathbf{A}}(z_{i_1}, \dots, z_{i_{i-1}}, a, z_{i_i}, \dots, z_{i_{k-1}})$, $b' = f^{\mathbf{A}}(z_{i_1}, \dots, z_{i_{i-1}}, b, z_{i_i}, \dots, z_{i_{k-1}})$, $c' = g^{\mathbf{A}}(w_{i'_1}, \dots, w_{i'_{j'-1}}, c, w_{i'_{j'}}, \dots, w_{i'_{r'-1}})$ and $d' = g^{\mathbf{A}}(w_{i'_1}, \dots, w_{i'_{j'-1}}, d, w_{i'_{j'}}, \dots, w_{i'_{r'-1}})$. Then $\delta_{m+1}(a', b', c', d')$ holds in \mathbf{A} , so since $\mathbf{A} \models \gamma_m$, $\delta_m(a', b', c', d')$ holds in \mathbf{A} . By returning the substitutions for a', b', c', d' we get that $\delta_{m+1}(a, b, c, d)$ holds in \mathbf{A} .

We see that the tautology $p \Rightarrow p \vee q$ implies $(\forall x, y, z, u) \delta_k(x, y, z, u) \Rightarrow \delta_m(x, y, z, u)$ whenever $k \leq m$. If $k > m$, according to the first part of this Lemma, from $\mathbf{A} \models \gamma_m$ we get $\mathbf{A} \models \gamma_i$ for all $i > m$. Therefore, if $\delta_k(a, b, c, d)$ holds in \mathbf{A} , then $\gamma_{k-1}, \gamma_{k-2}, \dots, \gamma_m$ imply that $\delta_m(a, b, c, d)$ holds in \mathbf{A} . \square

LEMMA 5.10. *If \mathcal{V}_{FSI} is a strictly elementary class, then there exists $n_0 \in \omega$ such that*

- (1) $\mathcal{V}_{FSI} \models (\forall x, y, u, v)(x \neq y \wedge u \neq v) \Rightarrow \delta_{n_0}(x, y, u, v)$
- (2) $\mathcal{V} \models \gamma_{n_0}$
- (3) *If Φ_2 is the formula axiomatizing \mathcal{V}_{FSI} and $\Phi_3 = (\forall x, y, u, v)(x \neq y \wedge u \neq v) \Rightarrow \delta_{n_0}(x, y, u, v)$, then $\mathcal{V} \models \Phi_3 \Rightarrow \Phi_2$.*

PROOF. (1) : Let \mathcal{F}^* be the similarity type $\mathcal{F} \cup \{a, b, c, d\}$ where a, b, c and d are new constant symbols. Let Φ_2 be the \mathcal{F} -sentence such that $\text{Mod}(\Phi_2) = \mathcal{V}_{FSI}$. Let ϕ_m be the \mathcal{F}^* -sentence $\Phi_2 \wedge a \neq b \wedge c \neq d \wedge \neg \delta_m(a, b, c, d)$. We claim that the set of sentences $\{\phi_m : m \in \omega\}$ has no model.

Indeed, for an \mathcal{F}^* -algebra \mathbf{A}^* , $\mathbf{A}^* \models \Phi_2$ means that the \mathcal{F} -reduct of \mathbf{A}^* , $\mathbf{A} \in \mathcal{V}_{FSI}$. As congruence generation is completely independent of having some constant symbols in the similarity type, from $\mathbf{A}^* \models a \neq b \wedge c \neq d$ we get that $\text{Cg}^{\mathbf{A}^*}(a, b) \cap \text{Cg}^{\mathbf{A}^*}(c, d) > 0_{\mathbf{A}^*}$ (we denote $a^{\mathbf{A}^*}$ by a and so on, for the sake of brevity). Since $\mathbf{A} \in \mathcal{V}$, $\mathbf{A}^* \models \Phi_1$, according to Lemma 5.1 (as Φ_1 is an universal sentence, adding new constants can't make it untrue), so for some m , $\delta_m(a, b, c, d)$ holds in \mathbf{A} , and that is the same m for which ϕ_m must fail in \mathbf{A}^* .

Therefore, according to Compactness theorem, there is a finite subset of $S \subseteq \{\phi_m : m \in \omega\}$ such that no \mathcal{F}^* -algebra is a model of S . We may as well assume that $S = \{\phi_m : m \leq n_0\}$ and by taking conjunctions, we get that $\Phi_2 \wedge a \neq b \wedge c \neq d \wedge \bigwedge_{m \leq n_0} \neg \delta_m(a, b, c, d)$ has no model. As $\neg \delta_{n_0}(a, b, c, d) \Rightarrow \neg \delta_m(a, b, c, d)$ for all $m \leq n_0$, we get that $\Phi_2 \wedge a \neq b \wedge c \neq d \wedge \neg \delta_{n_0}(a, b, c, d)$ has no model among \mathcal{F}^* -algebras. Therefore, for any \mathcal{F} -algebra \mathbf{A} such that $\mathbf{A} \models \Phi_2$, it holds that $\mathbf{A} \models (x \neq y \wedge u \neq v) \Rightarrow \delta_{n_0}(x, y, u, v)$, otherwise the \mathcal{F}^* -algebra

obtained from \mathbf{A} by evaluating a, b, c, d as values of x, y, u, v which falsify the implication would be a model for Φ_2 (as the sentence Φ_2 is a \mathcal{F} -sentence true in \mathbf{A}) and also for $a \neq b \wedge c \neq d \wedge \neg \delta_{n_0}(a, b, c, d)$, which is impossible. This proves the first claim in the Lemma statement.

(2) : For the second claim, we need to prove first that $\mathcal{V}_{FSI} \models \gamma_{n_0}$. So, let $\mathbf{A} \in \mathcal{V}_{FSI}$ and $a, b, c, d \in A$ are such that $\delta_{n_0+1}(a, b, c, d)$ holds in \mathbf{A} . According to Lemma 5.1, this means that $a \neq b$ and $c \neq d$ (the second is trivially true). From the first part of this Lemma, it implies that $\delta_{n_0}(a, b, c, d)$ holds in \mathbf{A} , so we have $\mathcal{V}_{FSI} \models \gamma_{n_0}$.

Now assume that $\mathbf{A} \in \mathcal{V}$. We can assume that $\mathbf{A} \leq \prod_{i \in I} \mathbf{A}_i$ is a subdirect product, for some $\mathbf{A}_i \in \mathcal{V}_{SI} \subseteq \mathcal{V}_{FSI}$, according to Theorem III.1.6. Let $\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d} \in A$ be such that $\delta_{n_0+1}(\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d})$ holds in \mathbf{A} . Therefore, for some j , $0 < j < n$, $p, q \in T_{n_0+1}^*$ and $\bar{\mathbf{e}}, \bar{\mathbf{f}} \in A^{(n_0+1)(r-1)}$, $p_j^{\mathbf{A}}(p^{\mathbf{A}}(\mathbf{a}, \bar{\mathbf{e}}), q^{\mathbf{A}}(\mathbf{c}, \bar{\mathbf{f}}), p^{\mathbf{A}}(\mathbf{b}, \bar{\mathbf{e}})) \neq p_i^{\mathbf{A}}(p^{\mathbf{A}}(\mathbf{a}, \bar{\mathbf{e}}), q^{\mathbf{A}}(\mathbf{d}, \bar{\mathbf{f}}), p^{\mathbf{A}}(\mathbf{b}, \bar{\mathbf{e}}))$. So, for some $i \in I$, $p_j^{\mathbf{A}_i}(p^{\mathbf{A}_i}(\mathbf{a}(i), \bar{\mathbf{e}}(i)), q^{\mathbf{A}_i}(\mathbf{c}(i), \bar{\mathbf{f}}(i)), p^{\mathbf{A}_i}(\mathbf{b}(i), \bar{\mathbf{e}}(i))) \neq p_j^{\mathbf{A}_i}(p^{\mathbf{A}_i}(\mathbf{a}(i), \bar{\mathbf{e}}(i)), q^{\mathbf{A}_i}(\mathbf{d}(i), \bar{\mathbf{f}}(i)), p^{\mathbf{A}_i}(\mathbf{b}(i), \bar{\mathbf{e}}(i)))$. Therefore, \mathbf{A}_i satisfies $\delta_{n_0+1}(\mathbf{a}(i), \mathbf{b}(i), \mathbf{c}(i), \mathbf{d}(i))$, and as $\mathbf{A}_i \models \gamma_{n_0}$, since $\mathbf{A}_i \in \mathcal{V}_{FSI}$, then $\delta_{n_0}(\mathbf{a}(i), \mathbf{b}(i), \mathbf{c}(i), \mathbf{d}(i))$ also holds in \mathbf{A}_i .

Therefore, there exist $p_{j'}$, $0 < j' < n$, $p', q' \in T_{n_0}^*$, $\bar{\mathbf{e}}', \bar{\mathbf{f}}' \in A_i^{n_0(r-1)}$ such that they witness $\delta_{n_0}(\mathbf{a}(i), \mathbf{b}(i), \mathbf{c}(i), \mathbf{d}(i))$. We can pick the tuples $\bar{\mathbf{e}}', \bar{\mathbf{f}}' \in A^{n_0(r-1)}$ so that $\mathbf{e}'_s(i) = e_s$ and $\mathbf{f}'_r = f'_r$ for all s, r , since \mathbf{A} is subdirect. Now $p_{j'}, p', q', \bar{\mathbf{e}}', \bar{\mathbf{f}}' \in A_i^{n_0(r-1)}$ will witness $\delta_{n_0}(\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d})$, since the appropriate expressions will evaluate differently at least at the i th coordinate.

(3) : If $\mathbf{A} \in \mathcal{V}$ is such that $\mathbf{A} \models \Phi_3$, that means that for all $a, b, c, d \in A$, if $a \neq b$ and $c \neq d$, then (according to Lemma 5.7) $\text{Cg}^{\mathbf{A}}(a, b) \cap \text{Cg}^{\mathbf{A}}(c, d) \neq 0_A$. Therefore, \mathbf{A} is a finitely subdirectly irreducible algebra, so $\mathbf{A} \models \Phi_2$. \square

THEOREM 5.11. *Let \mathcal{V} be a congruence distributive variety in a finite similarity type, and let \mathcal{V}_{FSI} be a strictly elementary class. Then \mathcal{V} is finitely based.*

PROOF. Let as fix n_0 as in Lemma 5.10 and let Σ be the set of identities of \mathcal{V} on a countably infinite set of variables. According to Theorem III.2.9, Σ axiomatizes \mathcal{V} . According to Lemmas 5.1 and 5.10, $\mathcal{V} \models \gamma_{n_0} \wedge \Phi_1 \wedge (\Phi_3 \Rightarrow \Phi_2)$. Therefore, $\Sigma \models \gamma_{n_0} \wedge \Phi_1 \wedge (\Phi_3 \Rightarrow \Phi_2)$ and we know by Corollary 2.7 that there exists a finite set $\Sigma_0 \subseteq \Sigma$ such that $\Sigma_0 \models \gamma_{n_0} \wedge \Phi_1 \wedge (\Phi_3 \Rightarrow \Phi_2)$. We claim that $\mathcal{V} = \text{Mod}(\Sigma_0)$.

So, let \mathbf{A} be any finitely subdirectly irreducible \mathcal{F} -algebra such that $\mathbf{A} \models \Sigma_0$. We know that $\mathbf{A} \models \Phi_1$, $\mathbf{A} \models \gamma_{n_0}$ and $\mathbf{A} \models \Phi_3 \Rightarrow \Phi_2$. Pick

any $a, b, c, d \in A$ with $a \neq b$ and $c \neq d$. As \mathbf{A} is finitely subdirectly irreducible, $\text{Cg}^{\mathbf{A}}(a, b) \cap \text{Cg}^{\mathbf{A}}(c, d) \neq 0_A$. Since $\mathbf{A} \models \Phi_1$, we can apply Lemma 5.7 to get that $\delta_m(a, b, c, d)$ holds in \mathbf{A} for some m . According to Lemma 5.9, since $\mathbf{A} \models \gamma_{n_0}, \delta_{n_0}(a, b, c, d)$.

We have just proved that $\mathbf{A} \models \Phi_3$, so since $\mathbf{A} \models \Phi_3 \Rightarrow \Phi_2$, $\mathbf{A} \models \Phi_2$ and therefore $\mathbf{A} \in \mathcal{V}_{FSI}$. Therefore, any \mathcal{F} -algebra \mathbf{B} such that $\mathbf{B} \models \Sigma_0$ is isomorphic to a subdirect product of its subdirectly irreducible factors, which are all in \mathcal{V} . So, $\mathbf{B} \in \mathcal{V}$. \square

COROLLARY 5.12 (Baker's Theorem). *Let \mathcal{V} be a finitely generated congruence distributive variety in a finite similarity type. Then \mathcal{V} is finitely based.*

PROOF. Let $\mathcal{V} = \mathcal{V}(\{\mathbf{A}_1, \dots, \mathbf{A}_k\})$, such that all \mathbf{A}_i are finite. According to Corollary 4.5, $\mathcal{V}_{FSI} \subseteq \text{HS}(\{\mathbf{A}_1, \dots, \mathbf{A}_k\})$. As there are only finitely many isomorphism types among $\text{HS}(\{\mathbf{A}_1, \dots, \mathbf{A}_k\})$, all of which are finite, and since the similarity type \mathcal{F} is finite, there is a sentence axiomatizing \mathcal{V}_{FSI} (it is the disjunction of sentences axiomatizing each class of the form $I(\{\mathbf{A}\})$, where \mathbf{A} is a finitely subdirectly irreducible factor of a subalgebra of one of \mathbf{B}_i). Therefore, \mathcal{V}_{FSI} is a strictly elementary class and Theorem IV.5.11 implies that \mathcal{V} is finitely based, \square

CHAPTER 5

Willard's finite basis theorem

In this Chapter we prove the Willard's Finite Basis Theorem. In the course of the proof, we first develop the Mal'cev characterization of congruence meet-semidistributivity, though we need only one of its consequences for the proof of Willard's Theorem. We base our description of Willard terms on the one in [2], rather than on [38] (it is easy to see that the difference is only in notation), as we feel that this is a more intuitive description than the one given by Willard in [38]. On the other hand, we prefer to give an exposition of Willard's original result than the stronger theorem proved in [2], as we feel that Willard's proof is prettier.

1. Prerequisites

Here we prove a few results of independent interest which will be useful in main proof of Willard's Theorem.

PROPOSITION 1.1. *Let \mathcal{V} be a variety in a finite similarity type \mathcal{F} . \mathcal{V} is not finitely based iff for all $k \in \omega$, there exists a subdirectly irreducible algebra $\mathbf{A}_k \notin \mathcal{V}$ which satisfies all identities $p \approx q$ true in \mathcal{V} such that the lengths of terms p and q is at most k .*

PROOF. If \mathcal{V} is finitely based, there is a maximal length of terms k among all terms used in the identities which form a finite basis, so \mathbf{A}_k can't exist. On the other hand, assume that \mathcal{V} is not finitely based. Let us fix $k \in \omega$ and denote the set of \mathcal{F} -terms in a countably infinite set of variables X with length at most k by $\mathbf{T}_{(k)}(X)$. Let n be the maximal arity of a fundamental operation in \mathcal{F} . Where $m = 2n^k$, we easily see that any identity $p \approx q$ in $(\mathbf{T}_{(k)}(X))^2$ has at most m variables occurring in it. So, $p \approx q$ is equivalent to the identity $p' \approx q'$ obtained from $p \approx q$ by injectively mapping all variables occurring in $p \approx q$ to $\{x_1, x_1, \dots, x_m\}$. Therefore, all identities $p \approx q$ true in \mathcal{V} such that $p, q \in \mathbf{T}_{(k)}(X)$ are deductive consequences of identities $p \approx q$ true in \mathcal{V} such that $p, q \in \mathbf{T}_{(k)}(\{x_1, x_1, \dots, x_m\})$. Now, $\mathbf{T}_{(k)}(\{x_1, x_1, \dots, x_m\})$ is a finite set of terms, so \mathcal{V} is not axiomatized by identities of \mathcal{V} which use terms of length at most k . This means that there must exist an

algebra $\mathbf{B}_k \notin \mathcal{V}$ which satisfies all identities of \mathcal{V} with lengths of terms at most k . According to the Subdirect Representation Theorem, \mathbf{B}_k is subdirect product of its subdirectly irreducible factor algebras, so (as \mathcal{V} is closed under SP), one of these, \mathbf{A}_k is not in \mathcal{V} . This finishes the proof, since \mathbf{A}_k satisfies all the identities \mathbf{B}_k does. \square

THEOREM 1.2 (Jónsson's Finite Basis Theorem). *Let \mathcal{V} be a variety of finite similarity type and let $\mathcal{V} \subseteq \mathcal{H}$, where \mathcal{H} is a strictly elementary class. Let there exist an elementary class \mathcal{K} such that $\mathcal{H}_{SI} \subseteq \mathcal{K}$ and such that $\mathcal{V} \cap \mathcal{K}$ is strictly elementary. Then \mathcal{V} is finitely based.*

PROOF. We assume that \mathcal{V} is not finitely based. According to Proposition 1.1, there exist algebras $\mathbf{A}_k \notin \mathcal{V}$ which satisfy all identities of \mathcal{V} with lengths of terms at most k . Let $\mathcal{H} = \text{Mod}(\psi)$ for some sentence ψ and let Σ be a set of identities axiomatizing \mathcal{V} . Since $\mathcal{V} \subseteq \mathcal{H}$, we get that $\Sigma \models \psi$. According to Corollary IV.2.7, there exists a finite set of identities $\Sigma_0 \subseteq \Sigma$ such that $\Sigma_0 \models \psi$. Let n be the maximal depth of terms used in identities in Σ_0 . Now, according to Proposition 1.1, there exist subdirectly irreducible algebras \mathbf{A}_k , $k \in \omega$ such that $\mathbf{A}_k \notin \mathcal{V}$, but \mathbf{A}_k satisfies all identities of \mathcal{V} with lengths of terms at most k . Let $\mathbf{A} = (\prod_{k \in \omega} \mathbf{A}_k)/U$, where U is a nonprincipal ultrafilter on ω . Clearly, for each identity in Σ , almost all \mathbf{A}_k satisfy it, so $\mathbf{A} \in \mathcal{V}$. Also, for all $k \geq n$, $\mathbf{A}_k \in \mathcal{H}$, and since all \mathbf{A}_k are subdirectly irreducible, $\mathbf{A}_k \in \mathcal{K}$ for $k \geq n$. Therefore, each of the sentences axiomatizing \mathcal{K} is true in all \mathbf{A}_k such that $k \geq n$, so $\mathbf{A} \in \mathcal{K}$. As $\mathbf{A} \in \mathcal{K} \cap \mathcal{V} = \text{Mod}(\phi)$ for some sentence ϕ , then $\llbracket \phi \rrbracket \in U$. But that is impossible, since $\mathbf{A}_k \not\models \phi$ for all $k \in \omega$, so $\llbracket \phi \rrbracket = \emptyset$. Contradiction. \square

The following Lemma and Theorem are probably folklore.

LEMMA 1.3. *Let \mathcal{V} be a variety with a finite residual bound n . Then $\mathcal{V}_{FSI} = \mathcal{V}_{SI}$.*

PROOF. Assume that there is an algebra $\mathbf{A} \in \mathcal{V}_{FSI} \setminus \mathcal{V}_{SI}$. As the two notions coincide in case of finite algebras, \mathbf{A} must be infinite. Let $\{a_0, a_1, \dots, a_n\} \subseteq A$ be an $n+1$ -element set. Since \mathbf{A} is finitely subdirectly irreducible, we have $\theta = \bigcap_{i \neq j} \text{Cg}^{\mathbf{A}}(a_i, a_j) > 0_{\mathbf{A}}$, so we can select $b \neq c$ such that $(b, c) \in \theta$. Using Zorn's Lemma it is easy to prove that there is a maximal congruence in **Con** \mathbf{A} which does not contain (b, c) . Indeed, we have already done this during our proof of Theorem III.1.4, if we just recall that **Con** \mathbf{A} is an algebraic lattice and that $\text{Cg}^{\mathbf{A}}(b, c)$ is a compact element of it. Let $\eta_{b,c}$ be a maximal congruence in **Con** \mathbf{A} not containing (b, c) . Then $\eta_{b,c}$ is a strictly \wedge -irreducible element of

Con A (this is also already seen in the proof of Theorem III.1.4) and if $i \neq j$, since $(b, c) \in \text{Cg}^{\mathbf{A}}(a_i, a_j)$, then $(a_i, a_j) \notin \eta_{b,c}$. Therefore, $\mathbf{A}/\eta_{b,c}$ is a subdirectly irreducible algebra and $|A/\eta_{b,c}| \geq n + 1$. Contradiction. \square

THEOREM 1.4. *Let \mathcal{V} be a variety of a finite signature with a finite residual bound n . Let \mathcal{H} be a strictly elementary class such that $\mathcal{V} \subseteq \mathcal{H}$ and for which there exists a formula $M(x, y, z, u)$ with four free variables such that whenever $\mathbf{A} \in \mathcal{H}$ and $a, b, c, d \in A$, $M(a, b, c, d)$ is true in \mathbf{A} iff $\text{Cg}^{\mathbf{A}}(a, b) \cap \text{Cg}^{\mathbf{A}}(c, d) \neq \emptyset$. Then \mathcal{V} is finitely based.*

PROOF. Let ψ be the sentence axiomatizing \mathcal{H} and let ϕ be the sentence ' \mathbf{A} is isomorphic to one of subdirectly irreducible members of \mathcal{V} '. The second sentence is possible since there are only finitely many isomorphism types in \mathcal{V}_{FSI} , all of them finite. Let \mathcal{H}_0 be the strictly elementary class axiomatized by $\psi \wedge [(\forall x, y, z, u)(x \neq y \wedge z \neq u \Rightarrow M(x, y, z, u)) \Rightarrow \phi]$. Clearly, $\mathcal{H}_0 = (\mathcal{H} \setminus \mathcal{H}_{FSI}) \cup \mathcal{V}_{SI}$. Let \mathcal{K} be the strictly elementary class axiomatized by ϕ . Now, $\mathcal{V} \subseteq \mathcal{H}_0$ by Lemma 1.3, $\mathcal{K} = \mathcal{K} \cap \mathcal{V}$ contains precisely all subdirectly irreducible algebras in \mathcal{H}_0 , so $\mathcal{H}_0, \mathcal{K}$ and \mathcal{V} satisfy the conditions of Jónsson's Finite Basis Theorem, so \mathcal{V} is finitely based. \square

Finally, we need the following well-known combinatorial fact:

THEOREM 1.5 (Ramsey). *Let $G = (V, E)$ be a graph (undirected, without loops or multiple edges) and let $|V| = \binom{m+n}{n}$ (where $m, n > 0$). Then G contains a clique (induced subgraph which is a complete graph) of size $m + 1$, or an anticlique (induced subgraph with no edges) of size $n + 1$.*

PROOF. By induction on $m + n$. If $m + n = 2$ this is true, as any graph of 2 vertices is either a 2-clique, or a 2-anticlique. Let the theorem hold for $m + n < k$ and assume $m + n = k$. We may also assume that $m \geq n$ because of symmetricity of our statement (we may exchange words 'clique' and 'anticlique') and because $\binom{m+n}{m} = \binom{m+n}{n}$. If $n = 1$, the statement is true for all m , as the graph on $m + 1$ vertices is either complete (so contains a $m + 1$ -clique), or contains a 2-anticlique. So, let $1 < n \leq m$. Then $\binom{m+n}{n} = \binom{(m-1)+n}{n} + \binom{m+(n-1)}{n-1}$. Select any vertex $v \in V$. By Pigeonhole Principle, v either has $\binom{(m-1)+n}{n}$ neighbors, or it has $\binom{m+(n-1)}{n-1}$ non-neighbors. Say v has $\binom{(m-1)+n}{n}$ neighbors, as the other case is analogous. In the induced subgraph on neighbors of v , by inductive assumption, there either exists a m -clique, which together with v forms a desired $m + 1$ -clique in G , or there exists an $n + 1$ -anticlique, which already satisfies the requirements of the Theorem. \square

2. Characterization of congruence meet-semidistributivity

DEFINITION 2.1. A lattice is meet-semidistributive if it satisfies the following implication: $x \wedge y = x \wedge z \Rightarrow x \wedge y = x \wedge (y \vee z)$. Lattices satisfying the dual property are called join-semidistributive and lattices satisfying both implications are just called semidistributive. Any variety \mathcal{V} such that for all $\mathbf{A} \in \mathcal{V}$, the lattice $\mathbf{Con} \mathbf{A}$ is meet-semidistributive (join-semidistributive) is called a *congruence meet-semidistributive* (*congruence join-semidistributive*) variety.

LEMMA 2.2. Let $\alpha, \beta, \gamma \in \mathbf{Con} \mathbf{A}$. Define two sequences of congruences $\{\beta_n : n \in \omega\}$ and $\{\gamma_n : n \in \omega\}$ inductively by $\beta_0 = \beta$, $\beta_{n+1} = \beta \vee (\alpha \wedge \gamma_n)$, $\gamma_0 = \gamma$ and $\gamma_{n+1} = \gamma \vee (\alpha \wedge \beta_n)$. Then the following hold.

- (1) For all $i \in \omega$, $\beta_i \subseteq \beta_{i+1}$ and $\gamma_i \subseteq \gamma_{i+1}$.
- (2) Define $\beta_\infty = \bigcup_{i \in \omega} \beta_i$ and $\gamma_\infty = \bigcup_{i \in \omega} \gamma_i$, then $\beta_\infty, \gamma_\infty \in \mathbf{Con} \mathbf{A}$.
- (3) $\alpha \wedge \beta_\infty = \alpha \wedge \gamma_\infty$ and if $\beta', \gamma' \in \mathbf{Con} \mathbf{A}$ are such that $\beta \subseteq \beta'$, $\gamma \subseteq \gamma'$ and $\alpha \wedge \beta' = \alpha \wedge \gamma'$, then $\beta_\infty \subseteq \beta'$ and $\gamma_\infty \subseteq \gamma'$.

PROOF. We prove (1) inductively. Clearly, $\beta_0 = \beta \subseteq \beta \vee (\alpha \wedge \gamma) = \beta_1$ and $\gamma_0 = \gamma \subseteq \gamma \vee (\alpha \wedge \beta) = \gamma_1$. Assume that $\beta_k \subseteq \beta_{k+1}$ and $\gamma_k \subseteq \gamma_{k+1}$. Then $\beta_{k+1} = \beta \vee (\alpha \wedge \gamma_k) \subseteq \beta \vee (\alpha \wedge \gamma_{k+1}) = \beta_{k+2}$ and analogously $\gamma_{k+1} \subseteq \gamma_{k+2}$. This immediately implies (2), as union of a chain of congruences is always a congruence.

Assume that $(a, b) \in \alpha \wedge \beta_\infty$. Then $(a, b) \in \alpha$ and for some $n \in \omega$, $(a, b) \in \beta_n$. Therefore, $(a, b) \in \alpha \wedge \beta_n \subseteq \gamma \vee (\alpha \wedge \beta_n) = \gamma_{n+1}$, so $(a, b) \in \alpha \wedge \gamma_{n+1} \subseteq \alpha \wedge \gamma_\infty$. $\alpha \wedge \gamma_\infty \subseteq \alpha \wedge \beta_\infty$ is proved analogously. finally, assume that $\beta \subseteq \beta'$, $\gamma \subseteq \gamma'$ and $\alpha \wedge \beta' = \alpha \wedge \gamma'$. Then we prove inductively that for all n , $\beta_n \subseteq \beta'$ and $\gamma_n \subseteq \gamma'$. The base case $n = 0$ is given. If $\gamma_k \subseteq \gamma'$ then $\beta_{k+1} = \beta \vee (\alpha \wedge \gamma_k) \subseteq \beta' \vee (\alpha \wedge \gamma') = \beta' \vee (\alpha \wedge \beta') = \beta'$. The implication $\beta_k \subseteq \beta' \Rightarrow \gamma_{k+1} \subseteq \gamma'$ is analogous. \square

Let $\Sigma = \{ \}, \{ \}$ and let $P \subseteq \Sigma^*$ be the set of finite words on the alphabet Σ defined by $P = \{w \in \Sigma^* : n_{(}(w) = n_{)}(w) \text{ and for all } u, v \text{ such that } w = uv, |u| > 0 \text{ and } |v| > 0, n_{(}(u) > n_{)}(u)\}$, where $n_{(}(w)$ denotes the number of letters '(' in w , $n_{)}(w)$ denotes the number of letters ')' in w and $|w|$ is the length of the word w . An equivalent way to describe P is to say that it is the smallest set of words over Σ satisfying that $() \in P$ and if $u_1, u_2, \dots, u_n \in P$, then $(u_1 u_2 \dots u_n) \in P$. We will call words in P the *parenthesis terms*. The reader may have seen a different definition of parenthesis terms, one where $n \leq 2$ or $n = 2$ is assumed in the above situation, so we urge the reader not to confuse it with our more general definition. It is easy to prove that if

$w = w_1 w_2 \dots w_{2n}$ is a parenthesis term, where $w_i \in \Sigma$, for each k such that $w_k = ($ (there exists a unique $l > k$ such that $w_k w_{k+1} \dots w_l \in P$ (therefore $w_l =)$, as is easy to see). Define for a parenthesis term w a function $*$: $\{1, \dots, |w|\} \rightarrow \{1, \dots, |w|\}$ so that $k^* = l$ and $l^* = k$, where k, l are as above.

DEFINITION 2.3. Let $w = w_1 w_2 \dots w_{2n} \in P$ be a parenthesis term, where $w_i \in \Sigma$. The sequence s_1, s_2, \dots, s_{2n} of ternary terms will be called *Willard terms parametrized by w* in some variety \mathcal{V} if the following equations hold in \mathcal{V} :

- (1) $s_1(x, y, z) \approx x$,
- (2) $s_{2n}(x, y, z) \approx z$,
- (3) $s_i(x, x, y) \approx s_{i+1}(x, x, y)$ when i is odd,
- (4) $s_i(x, y, y) \approx s_{i+1}(x, y, y)$ when i is even,
- (5) $s_i(x, y, x) \approx s_j(x, y, x)$ when $j = i^*$.

THEOREM 2.4. *The following are equivalent for a variety \mathcal{V} :*

- (1) \mathcal{V} is congruence meet-semidistributive.
- (2) For all $\mathbf{A} \in \mathcal{V}$ and $\alpha, \beta, \gamma \in \text{Con } \mathbf{A}$, $\alpha \wedge (\beta \circ \gamma) \subseteq \beta_\infty$.
- (3) There exists a parenthesis term $w \in P$ such that \mathcal{V} has Willard terms parametrized by w .
- (4) There exist a parenthesis term $w \in P$ and ternary terms $s_1, \dots, s_{|w|}$ such that the equations $s_i(x, y, x) \approx s_{i^*}(x, y, x)$ are satisfied in \mathcal{V} for all $i \leq |w|$, and for any algebra $\mathbf{A} \in \mathcal{V}$ and any elements $a, b \in A$,

$$a = b \text{ iff } [(\forall i \leq |w|)(s_i(a, a, b) = s_{i^*}(a, a, b) \text{ iff } s_i(a, b, b) = s_{i^*}(a, b, b))].$$

- (5) for any algebra $\mathbf{A} \in \mathcal{V}$ and any finite sequence a_0, a_1, \dots, a_n of elements of A such that $a_0 \neq a_n$ there exists an $i < n$ such that $\text{Cg}^{\mathbf{A}}(a_0, a_n) \cap \text{Cg}^{\mathbf{A}}(a_i, a_{i+1}) \neq 0_{\mathbf{A}}$.

PROOF. (1) \Rightarrow (2). Let $\mathbf{A} \in \mathcal{V}$ and $\alpha, \beta, \gamma \in \text{Con } \mathbf{A}$. Then $\alpha \wedge (\beta \circ \gamma) \subseteq \alpha \wedge (\beta_\infty \vee \gamma_\infty) = \alpha \wedge \beta_\infty \subseteq \beta_\infty$ according to Lemma 2.2 and meet-semidistributivity of **Con** \mathbf{A} .

(2) \Rightarrow (3). For $w \in P$, we define alternative Willard terms parametrized by w to be terms satisfying similar equations as Willard terms parametrized by w , except for the switch of equations (3) and (4) in Definition 2.3, so equation (3) holds when i is even and equation (4) holds when i is odd.

Now, assume that (2) holds in \mathcal{V} and let $\mathbf{F} = \mathbf{F}_{\mathcal{V}}(x, y, z)$, $\alpha = \text{Cg}^{\mathbf{F}}(x, z)$, $\beta = \text{Cg}^{\mathbf{F}}(x, z)$ and $\gamma = \text{Cg}^{\mathbf{F}}(y, z)$. According to (2), $(x, z) \in \alpha \wedge (\beta \circ \gamma) \subseteq \beta_\infty$, so for some $n \in \omega$, $(x, z) \in \alpha \wedge \beta_n$. In order to simplify

notation, we denote elements on F by ternary terms, though we are aware that they are just representatives of the equivalence blocks of $\Theta_{\mathcal{V}}(\{x, y, z\})$ which contain them. We prove inductively the following claim:

Claim. If for some $k \in \omega$ and $p, q \in F$, $(p, q) \in \alpha \wedge \beta_k$, then there exists a parenthesis term $w = w_1 w_2 \dots w_{2m}$ and terms $p = s_1, s_2, \dots, s_{2m} = q$ which satisfy equations (3)-(5) of the definition of Willard terms parametrized by w . If $(p, q) \in \alpha \wedge \gamma_k$, then there exists a parenthesis term $w = w_1 w_2 \dots w_{2m}$ and terms $p = s_1, s_2, \dots, s_{2m} = q$ which satisfy equations (3)-(5) of the definition of alternative Willard terms parametrized by w .

The base case when $k = 0$ is clear as then we have $(p, q) \in \alpha \wedge \beta$ and alternatively $(p, q) \in \alpha \wedge \gamma$, which both mean that the parenthesis term $w = ()$ parametrizes the sequence $p = s_1, s_2 = q$, according to Lemma III.3.13. Assume that both statements are true for k and let $(p, q) \in \alpha \wedge \beta_{k+1}$. Since $\beta_{k+1} = \beta \vee (\alpha \wedge \gamma_k)$, there exists a sequence of ternary terms $p = p_1, p_2, \dots, p_{2l} = q$ such that $(p_i, p_{i+1}) \in \beta$ for even i and $(p_i, p_{i+1}) \in \alpha \wedge \gamma_k$ for odd i . The inductive assumption guarantees us sequences of alternative Willard terms between p_i and p_{i+1} for all even i , so by defining $s_1 = p_1 = p, s_2, \dots, s_{2n-1}$ is the concatenation of these sequences of alternative Willard terms (taking first the sequence between p_2 and p_3 , and so on) and $s_{2n} = p_{2l} = q$. We let $w = (v_1 v_2 \dots v_{l-1})$, where v_i parametrizes the alternative Willard sequence between p_{2i} and p_{2i+1} . We get that the desired equations (3) and (4) hold since the adjacent members are either adjacent in the alternative Willard sequence, or are equal to p_i, p_{i+1} for odd i and therefore β -related. Also, s_i and s_{i^*} are either corresponding under $*$ in one of v_i , and then (5) holds by inductive assumption, or $\{s_i, s_{i^*}\} = \{s_1, s_{2n}\} = \{p, q\}$, in which case the equation $p(x, y, x) \approx q(x, y, x)$ follows from $(p, q) \in \alpha$ and Lemma III.3.13. The inductive step in the case when $(p, q) \in \alpha \wedge \gamma_{k+1}$ is analogous.

The Claim applied to $p = x$ and $q = z$ proves the existence of Willard terms.

(3) \Rightarrow (4). We use the same Willard terms and parametrization as above. Therefore, the equations $s_i(x, y, x) \approx s_{i^*}(x, y, x)$ follow from (5). Also, it follows from (5) that if $a = b$ then $s_i(a, a, b) = s_{i^*}(a, a, b)$ and $s_i(a, b, b) = s_{i^*}(a, b, b)$ for all i . So assume that $s_i(a, a, b) = s_{i^*}(a, a, b)$ iff $s_i(a, b, b) = s_{i^*}(a, b, b)$ for all i . We prove by induction on $|i - i^*|$ that $s_i(a, a, b) = s_{i^*}(a, a, b)$ and $s_i(a, b, b) = s_{i^*}(a, b, b)$.

If $|i - i^*| = 1$, this is clear, since one of these equations follows from either (3) or (4) and the other is true since our assumption states that either both hold, or both fail. Let $i < i^*$ and the sequence i_1, i_2, \dots, i_l

be such that $i_1 = i + 1$, $i_j^* + 1 = i_{j+1}$ and $i_l^* + 1 = i^*$ (this sequence is constructed from the parenthesis term $(u_1 u_2 \dots u_l)$ parametrizing the subsequence of s_j between s_i and s_{i^*}). Now, if i is odd, then so are all i_j^* , while i^* and all i_j are even. The identities (3) for Willard terms implies that $s_i(a, a, b) = s_{i_1}(a, a, b)$, $s_{i_j^*}(a, a, b) = s_{i_{j+1}}(a, a, b)$ for all $j < l$ and $s_{i_l^*}(a, a, b) = s_{i^*}(a, a, b)$, while the inductive hypothesis implies that $s_{i_j^*}(a, a, b) = s_{i_j^*}(a, a, b)$ for all $j \leq l$, so by transitivity we get $s_i(a, a, b) = s_{i^*}(a, a, b)$. Then $s_i(a, b, b) = s_{i^*}(a, b, b)$ must also hold by the assumption. If i is even, the proof is analogous, except that we would use identities (4) for Willard terms and inductive hypothesis to prove that $s_i(a, b, b) = s_{i^*}(a, b, b)$ and then obtain $s_i(a, a, b) = s_{i^*}(a, a, b)$ from the assumption.

Finally, we apply the proved equality to $i = 1$. $a = s_1(a, a, b) = s_{1^*}(a, a, b) = s_{2n}(a, a, b) = b$, as desired.

(4) \Rightarrow (5). Assume now that \mathcal{V} is a variety satisfying (4), $\mathbf{A} \in \mathcal{V}$, $a_0, a_1, \dots, a_n \in A$ and $a_0 \neq a_n$. By the second condition in (4), we may assume that there exists s_i such that $s_i(a_0, a_0, a_n) = s_{i^*}(a_0, a_0, a_n)$, while $s_i(a_0, a_n, a_n) \neq s_{i^*}(a_0, a_n, a_n)$ (the other case is analogous). Let j be such that $s_i(a_0, a_j, a_n) = s_{i^*}(a_0, a_j, a_n)$, while $s_i(a_0, a_{j+1}, a_n) \neq s_{i^*}(a_0, a_{j+1}, a_n)$. Denote by $a = s_i(a_0, a_{j+1}, a_n)$, $b = s_{i^*}(a_0, a_{j+1}, a_n)$, $c = s_i(a_0, a_j, a_n)$ and $d = s_i(a_0, a_{j+1}, a_0)$ and define unary polynomials

$$\begin{aligned} f_1(x) &= s_i(a_0, x, a_n) \\ f_2(x) &= s_{i^*}(a_0, x, a_n) \\ g_1(x) &= s_i(a_0, a_{j+1}, x) \\ g_2(x) &= s_{i^*}(a_0, a_{j+1}, x). \end{aligned}$$

Applying the first two polynomials on $\{a_j, a_{j+1}\}$ we get $f_1(\{a_j, a_{j+1}\}) = \{c, a\}$ and $f_2(\{a_j, a_{j+1}\}) = \{c, b\}$, as $s_i(a_0, a_j, a_n) = s_{i^*}(a_0, a_j, a_n)$, so $(a, b) \in \text{Cg}^{\mathbf{A}}(a_j, a_{j+1})$. Also, applying the other two polynomials on $\{a_0, a_n\}$ we get $g_1(\{a_0, a_n\}) = \{d, a\}$ and $g_2(\{a_0, a_n\}) = \{d, b\}$, as $s_i(a_0, a_{j+1}, a_0) = s_{i^*}(a_0, a_{j+1}, a_0)$, so $(a, b) \in \text{Cg}^{\mathbf{A}}(a_0, a_n)$. Finally, note that $a \neq b$, by our choice of j , so $\text{Cg}^{\mathbf{A}}(a_0, a_n) \cap \text{Cg}^{\mathbf{A}}(a_j, a_{j+1}) \neq 0_{\mathbf{A}}$.

(5) \Rightarrow (1). Let \mathcal{V} be a variety satisfying (5), $\mathbf{A} \in \mathcal{V}$ and $\alpha, \beta, \gamma \in \text{Con } \mathbf{A}$. We only need to prove meet-semidistributivity in the case when $\alpha \wedge \beta = \alpha \wedge \gamma = 0_{\mathbf{A}}$, according to the Correspondence Theorem. By the way of contradiction, assume that $a \neq b$ and $(a, b) \in \alpha \wedge (\beta \vee \gamma)$. Then $(a, b) \in \alpha$ and there is a chain $a = a_0, a_1, \dots, a_n = b$ such that $(a_i, a_{i+1}) \in \beta$ for even i , while $(a_i, a_{i+1}) \in \gamma$ for odd i . According to (5), there exists an $i < n$ such that $\text{Cg}^{\mathbf{A}}(a_0, a_n) \cap \text{Cg}^{\mathbf{A}}(a_i, a_{i+1}) \neq 0_{\mathbf{A}}$. But,

this contradicts our assumption as $\text{Cg}^{\mathbf{A}}(a_0, a_n) \cap \text{Cg}^{\mathbf{A}}(a_i, a_{i+1}) \subseteq \alpha \wedge \beta$ for even i and $\text{Cg}^{\mathbf{A}}(a_0, a_n) \cap \text{Cg}^{\mathbf{A}}(a_i, a_{i+1}) \subseteq \alpha \wedge \gamma$ for odd i . \square

3. Bounding Mal'cev chains

We now turn to proving initial results needed for Willard's finite basis theorem. For the next two Sections we fix a congruence meet-semidistributive variety \mathcal{V} in a finite similarity type \mathcal{F} . Like in the proof of Baker's theorem, we assume that the Willard terms for \mathcal{V} are fundamental operations of \mathcal{F} . As in the proof of Baker's theorem, we make this assumption purely for ease of notation, it does not fundamentally change the generality of the result. As we will be making a very involved calculation with respect to the length of translations, we may note now that if the reader prefers not to make this assumption, the calculation would have to multiply every length of a translation by N which is the maximum among lengths of Willard terms s_i in \mathcal{F} .

Recall the definition of translation from Section IV 5. A *basic translation* of an algebra $\mathbf{A} \in \mathcal{V}$ is a unary polynomial of the form $p(x) = f^{\mathbf{A}}(a_1, \dots, a_{i-1}, x, a_{i+1}, \dots, a_n)$ for some n -ary operation symbol $f \in \mathcal{F}$ and $a_i \in A$. Then the set of translations $\text{Tr } \mathbf{A}$ is equal to the monoid generated by the set of basic translations $\text{Tr}_1 \mathbf{A}$ under composition. Also, we define the n -translations, and write $\text{Tr}_n \mathbf{A}$, to be the set of all translations which can be obtained by a composition of length at most n of basic translations. The identity map is the only map in $\text{Tr}_0 \mathbf{A}$.

As in Set Theory, $A^{[2]}$ denotes the set of all subsets of A of size equal to 2. For $\{a, b\}, \{c, d\} \subseteq A$, $\mathbf{A} \in \mathcal{V}$, we denote by $\{a, b\} \rightarrow_k \{c, d\}$ the fact that there exists a k -translation f of \mathbf{A} such that $\{f(a), f(b)\} = \{c, d\}$. We denote by $\{a, b\} \Rightarrow_{k,n} \{c, d\}$ the fact that there exists a sequence of elements $c = c_0, c_1, \dots, c_n$ such that for all $i < n$, $c_i = c_{i+1}$ or $\{a, b\} \rightarrow_k \{c_i, c_{i+1}\}$. $\{a, b\} \Rightarrow_k \{c, d\}$ will denote that there exists $n \in \omega$ such that $\{a, b\} \Rightarrow_{k,n} \{c, d\}$. In a finite similarity type, \rightarrow_k and $\Rightarrow_{k,n}$ are expressible by first-order formulas. The following statements are immediate consequences of the definitions:

- REMARK 3.1. (1) $\{a, b\} \Rightarrow_{k,1} \{c, d\}$ is the same as $\{a, b\} \rightarrow_k \{c, d\}$.
- (2) If $\{a, b\} \Rightarrow_{k,m} \{c, d\} \Rightarrow_{l,n} \{e, f\}$, then $\{a, b\} \Rightarrow_{k+l,mn} \{e, f\}$.
- (3) If $\{a, b\} \rightarrow_{k+l} \{c, d\}$, then there exist $\{u, v\} \subseteq A$ such that $\{a, b\} \rightarrow_k \{u, v\} \rightarrow_l \{c, d\}$. Moreover, they can be chosen so that $f(u) = c$ and $f(v) = d$ for some translation $f \in \text{Tr}_l \mathbf{A}$.

LEMMA 3.1 (Single-sequence Lemma). *If $\mathbf{A} \in \mathcal{V}$ and $a = a_0, a_1, \dots, a_n = b$ is a sequence in A with $a \neq b$, then there exist $\{c, d\} \in A^{[2]}$ and $i < n$ such that $\{a, b\} \Rightarrow_{1,2} \{c, d\}$ and $\{a_i, a_{i+1}\} \Rightarrow_{1,2} \{c, d\}$.*

PROOF. This was proved in Theorem 2.4, (4) \Rightarrow (5). \square

LEMMA 3.2 (Multi-sequence Lemma). *If $\mathbf{A} \in \mathcal{V}$ and $S_i = a_0^{(i)}, a_1^{(i)}, \dots, a_{n_i}^{(i)}$, $1 \leq i \leq N$ are sequences in A with $a_0^{(i)} = a$, $a_{n_i}^{(i)} = b$ and $a \neq b$, then there exist $\{c, d\} \in A^{[2]}$ and $j_i < n_i$ such that $\{a, b\} \Rightarrow_{N,2^N} \{c, d\}$ and $\{a_{j_i}^{(i)}, a_{j_i+1}^{(i)}\} \Rightarrow_{N,2^N} \{c, d\}$.*

The pair $\{a_{j_i}^{(i)}, a_{j_i+1}^{(i)}\}$ will be called the key link of the sequence S_i and it is clear from $c \neq d$ that $\{a_{j_i}, a_{j_i+1}\} \in A^{[2]}$.

PROOF. We prove the Lemma by induction on N . The case $N = 1$ is just the Single-sequence Lemma. Assume that the statement is true for $N - 1$, that is, that there exist $\{c', d'\} \in A^{[2]}$ and key links $\{a_{j_i}^{(i)}, a_{j_i+1}^{(i)}\}$ for $1 \leq i < N$ such that $\{a, b\} \Rightarrow_{N-1,2^{N-1}} \{c', d'\}$ and $\{a_{j_i}^{(i)}, a_{j_i+1}^{(i)}\} \Rightarrow_{N-1,2^{N-1}} \{c', d'\}$ for $1 \leq i < N$.

Let $c' = u_0, u_1, \dots, u_h = d'$ with $h \leq 2^{N-1}$ be the chain of elements of A with $u_i \neq u_{i+1}$ witnessing that $\{a, b\} \Rightarrow_{N-1,2^{N-1}} \{c', d'\}$. Let also $f_i \in \text{Tr}_{N-1} \mathbf{A}$ be such that $\{f_i(a), f_i(b)\} = \{u_i, u_{i+1}\}$. We make a sequence $c' = v_0, v_1, \dots, v_M = d'$ such that u_0, u_1, \dots, u_h is a subsequence of it and such that for all $0 \leq j < M$, there exist $i, k \in \omega$ with $\{f_i(a_k^{(N)}), f_i(a_{k+1}^{(N)})\} = \{v_j, v_{j+1}\}$.

More precisely, $M = hn_N$, $v_{in_N} = u_i$ and if $j = in_N + k$ for some $0 \leq k < n_N$, then

- If $f_i(a) = u_i$ and $f_i(b) = u_{i+1}$, then $v_j = f_i(a_k^{(N)})$ and
- If $f_i(a) = u_{i+1}$ and $f_i(b) = u_i$, then $v_j = f_i(a_{n_N-k}^{(N)})$.

Now, according to the Single-sequence Lemma, there exist $\{c, d\} \in A^{[2]}$ and $0 \leq j < M$ such that $\{c', d'\} \Rightarrow_{1,2} \{c, d\}$ and $\{v_j, v_{j+1}\} \Rightarrow_{1,2} \{c, d\}$. According to our construction there exist $i, k \in \omega$ with $\{f_i(a_k^{(N)}), f_i(a_{k+1}^{(N)})\} = \{v_j, v_{j+1}\}$. Let us denote $k = j_N$. Now, we have

- (1) $\{a, b\} \Rightarrow_{N-1,2^{N-1}} \{c', d'\} \Rightarrow_{1,2} \{c, d\}$, so from Remark 3.1 (2), we obtain $\{a, b\} \Rightarrow_{N,2^N} \{c, d\}$.
- (2) $\{a_{j_i}^{(i)}, a_{j_i+1}^{(i)}\} \Rightarrow_{N-1,2^{N-1}} \{c', d'\} \Rightarrow_{1,2} \{c, d\}$, hence $\{a_{j_i}^{(i)}, a_{j_i+1}^{(i)}\} \Rightarrow_{N,2^N} \{c, d\}$.
- (3) $\{a_{j_N}^{(N)}, a_{j_N+1}^{(N)}\} \rightarrow_{N-1} \{v_j, v_{j+1}\} \Rightarrow_{1,2} \{c, d\}$, so again we have $\{a_{j_N}^{(N)}, a_{j_N+1}^{(N)}\} \Rightarrow_{N,2^N} \{c, d\}$ (since $\Rightarrow_{N,2}$ implies $\Rightarrow_{N,2^N}$).

\square

COROLLARY 3.3. *Let $\mathbf{A} \in \mathcal{V}$, $\{a_1, b_1\}, \dots, \{a_N, b_N\}, \{u, v\} \in A^{[2]}$ and let for all i , $1 \leq i \leq N$, $\{a_i, b_i\} \Rightarrow \{u, v\}$ hold in \mathbf{A} . Then there exist $\{u', v'\} \in A^{[2]}$ and for all $1 \leq i \leq N$, there exist $\{x_i, y_i\} \in A^{[2]}$, such that $\{u, v\} \Rightarrow_{N, 2^N} \{u', v'\}$ and $\{a_i, b_i\} \rightarrow_n \{x_i, y_i\} \Rightarrow_{N, 2^N} \{u', v'\}$.*

PROOF. Let S_i be the sequence $u = a_0^{(i)}, a_1^{(i)}, \dots, a_{n_i}^{(i)} = v$ witnessing the fact that $\{a_i, b_i\} \Rightarrow \{u, v\}$. Then apply the Multi-sequence Lemma to $\{u, v\}$ and the sequences S_i and let $\{x_i, y_i\} = \{a_{j_i}^{(i)}, a_{j_i+1}^{(i)}\}$ guaranteed by the Multi-sequence Lemma. \square

The Corollary just proved allows us to replace \Rightarrow_n with unknown length of Mal'cev chain with a weaker, but first-order definable property $\Rightarrow_{n+N, 2^N}$, which we will habitually do for the remainder of the Chapter. Note that we used only that \mathcal{V} is congruence meet-semidistributive and that the similarity type is finite. In order to be able to define the sentence $\mu(x, y, z, u)$ required by Theorem 1.4, we also need to put a bound on n in \Rightarrow_n , which we refer to as the *depth* of the Mal'cev chain. To do this, we will need to use the finite residual bound. Before getting about it, we need to fix some notation.

Let $m \in \omega$, $m > 0$. We define four functions

- $L(m) = \binom{m+1}{2}$;
- $M(m) = \binom{2^m}{m} - 1$;
- $N(m) = 2^{\binom{M(m)+1}{2}}$;
- $D(m) = N(m) + 3$.

For shortness of notation, with m understood, we will just call them L , M , N and D .

We denote by Φ_m the sentence

$$(\exists x_0, x_1, \dots, x_m, y, z)(y \neq z \wedge \bigwedge_{0 \leq i < j \leq m} \{x_i, x_j\} \Rightarrow_{DM+L, 2^L} \{y, z\})$$

and by $\mu_m(x_1, y_1, x_2, y_2)$ the first-order formula

$$(\exists v, w, r_1, s_1, r_2, s_2)(v \neq w \wedge \bigwedge_{1 \leq i \leq 2} \{x_i, y_i\} \rightarrow_{DM} \{r_i, s_i\} \Rightarrow_{2,4} \{v, w\})$$

The next result will allow us to effectively bound the depth of Mal'cev chains in \mathcal{V} , when we additionally assume that \mathcal{V} has a finite residual bound.

THEOREM 3.4. *Let $\mathbf{A} \in \mathcal{V}$. Then one of the following two statements must hold for \mathbf{A} :*

- (i) $\mathbf{A} \models \Phi_m$.

- (ii) For all $a, b, c, d \in A$, $\mu_m(a, b, c, d)$ holds in \mathbf{A} iff $\text{Cg}^{\mathbf{A}}(a, b) \cap \text{Cg}^{\mathbf{A}}(c, d) \neq 0_{\mathbf{A}}$.

PROOF. Let $\mathbf{A} \in \mathcal{V}$ be such that $\mathbf{A} \not\models \Phi_m$. It is always true that if $a, b, c, d \in A$ are such that $\mu_m(a, b, c, d)$ holds in \mathbf{A} , then $\text{Cg}^{\mathbf{A}}(a, b) \cap \text{Cg}^{\mathbf{A}}(c, d) \neq 0_{\mathbf{A}}$. The only thing left to check is the other implication.

So, assume that $\text{Cg}^{\mathbf{A}}(a, b) \cap \text{Cg}^{\mathbf{A}}(c, d) \neq 0_{\mathbf{A}}$, but $\mu_m(a, b, c, d)$ fails in \mathbf{A} . Since there must exist some $\{u', v'\} \in A^{[2]}$ and $n \in \omega$ such that $\{a, b\} \Rightarrow_n \{u', v'\}$ and $\{c, d\} \Rightarrow_n \{u', v'\}$, then according to Corollary 3.3, there exist $\{r, s\}, \{r', s'\}, \{u, v\} \in A^{[2]}$ such that

$$(*) \quad \{a, b\} \rightarrow_n \{r, s\} \Rightarrow_{2,4} \{u, v\} \text{ and } \{c, d\} \rightarrow_n \{r', s'\} \Rightarrow_{2,4} \{u, v\}.$$

According to our assumption $\mu(a, b, c, d)$ fails, so $n > DM$ for any choice of r, s, r', s', u and v . Let r, s, r', s', u, v be chosen so that $u \neq v$, $(*)$ holds and n is minimal.

Let $t = n - DM$. According to Remark 3.1 (3), we can select $\{a_i, b_i\} \in A^{[2]}$ and $f_i \in \text{Tr}_{D(M-i)}\mathbf{A}$, $0 \leq i \leq M$ such that

$$\{a, b\} \rightarrow_t \{a_0, b_0\} \rightarrow_D \{a_1, b_1\} \rightarrow_D \cdots \rightarrow_D \{a_M, b_M\} = \{r, s\}$$

and such that $f_i(a_i) = r$ and $f_i(b_i) = s$. Analogously, $\{c_i, d_i\} \in A^{[2]}$ and $g_i \in \text{Tr}_{D(M-i)}\mathbf{A}$ can be selected so that $\{c, d\} \rightarrow_t \{c_0, d_0\}$, $g_i(c_i) = r'$ and $g_i(d_i) = s'$.

Fix a Mal'cev chain $u = u_0, u_1, \dots, u_4 = v$ such that for $0 \leq i < 4$, $p_i(\{r, s\})\{u_i, u_{i+1}\}$ for some $p_i \in \text{Tr}_2\mathbf{A}$. Now for any $0 \leq i < j \leq M$ we have a chain $r = f_j(a_j), f_j(a_i), f_j(b_i), f_j(b_j) = s$ which induces a chain $S_{ij} : v_0^{(ij)}, v_1^{(ij)}, \dots, v_{12}^{(ij)}$ from u to v (which contains C as a subsequence) in the following way:

- If $p_k(r) = u_k$ and $p_k(s) = u_{k+1}$, then $v_{3k}^{(ij)} = p_k(f_j(a_j)) = p_k(r) = u_k$, $v_{3k+1}^{(ij)} = p_k(f_j(a_i))$, $v_{3k+2}^{(ij)} = p_k(f_j(b_i))$ and $v_{3k+3}^{(ij)} = p_k(f_j(b_j)) = p_k(s) = u_{k+1}$.
- If $p_k(s) = u_k$ and $p_k(r) = u_{k+1}$, then $v_{3k}^{(ij)} = p_k(f_j(b_j)) = p_k(s) = u_k$, $v_{3k+1}^{(ij)} = p_k(f_j(b_i))$, $v_{3k+2}^{(ij)} = p_k(f_j(a_i))$ and $v_{3k+3}^{(ij)} = p_k(f_j(a_j)) = p_k(r) = u_{k+1}$.

The fact we really need about these chains is that for any chain S_{ij} and $0 \leq k < 12$, one of the following three occurs:

- (1) $\{a_j, a_i\} \rightarrow_{D(M-j)+2} \{v_k^{(ij)}, v_{k+1}^{(ij)}\}$,
- (2) $\{a_i, b_i\} \rightarrow_{D(M-j)+2} \{v_k^{(ij)}, v_{k+1}^{(ij)}\}$, or
- (3) $\{b_i, b_j\} \rightarrow_{D(M-j)+2} \{v_k^{(ij)}, v_{k+1}^{(ij)}\}$.

In the completely analogous way we can define for any $0 \leq i < j \leq M$, chains $R_{ij} : w_0^{(ij)}, w_1^{(ij)}, \dots, w_{12}^{(ij)}$, where $u = w_0^{(ij)}$, $v = w_{12}^{(ij)}$ and for any k , $0 \leq k < 12$, one of the following three occurs:

- (4) $\{c_j, c_i\} \rightarrow_{D(M-j)+2} \{w_k^{(ij)}, w_{k+1}^{(ij)}\}$,
- (5) $\{c_i, d_i\} \rightarrow_{D(M-j)+2} \{w_k^{(ij)}, w_{k+1}^{(ij)}\}$, or
- (6) $\{d_i, d_j\} \rightarrow_{D(M-j)+2} \{w_k^{(ij)}, w_{k+1}^{(ij)}\}$.

So, we have a total of $2^{\binom{M+1}{2}} = N$ sequences from u to v . We apply the Multi-sequence Lemma to these sequences. Therefore, we know that there exist $\{u', v'\} \in A^{[2]}$, and for all $0 \leq i < j \leq n$ there exist x_{ij} , y_{ij} , x'_{ij} and y'_{ij} such that $\{x_{ij}, y_{ij}\} \Rightarrow_{N, 2^N} \{u', v'\}$ and $\{x'_{ij}, y'_{ij}\} \Rightarrow_{N, 2^N} \{u', v'\}$, where $\{x_{ij}, y_{ij}\}$ is a pair of consecutive members of S_{ij} , while $\{x'_{ij}, y'_{ij}\}$ is a pair of consecutive members of R_{ij} . Now, we have two cases:

Case 1: If there exist $0 \leq i < j \leq M$ such that for $\{x_{ij}, y_{ij}\}$ case (2) occurs and also there exist $0 \leq k < l \leq M$ such that for $\{x'_{kl}, y'_{kl}\}$ case (5) occurs, then we will derive a contradiction with minimality of n . Indeed, (2) implies that

$$\{a, b\} \rightarrow_{t+Di} \{a_i, b_i\} \rightarrow_{D(M-j)+2} \{x_{ij}, y_{ij}\} \Rightarrow_{N, 2^N} \{u', v'\},$$

so since $t + Di + D(M - j) + 2 + N = t + DM + N + 2 - D(j - i) \leq n + N + 2 - D = n - 1$, therefore $\{a, b\} \Rightarrow_{n-1} \{u', v'\}$. Similarly, we get from (5) that $\{c, d\} \Rightarrow_{n-1} \{u', v'\}$. Applying Corollary 3.3, we get $\{u'', v''\} \in A^{[2]}$ and $e, f, g, h \in A$ such that $\{a, b\} \rightarrow_{n-1} \{e, f\} \Rightarrow_{2,4} \{u'', v''\}$ and $\{c, d\} \rightarrow_{n-1} \{g, h\} \Rightarrow_{2,4} \{u'', v''\}$. This contradicts the choice of n .

Case 2: We are left with the case when, without loss of generality, case (2) occurs for no $\{x_{ij}, y_{ij}\}$. So, we may define an associated undirected graph $G = (V, E)$ on the vertex set $V = \{0, 1, \dots, M\}$ such that $ij \in E$ iff case (1) occurs for $\{x_{ij}, y_{ij}\}$ (or $\{x_{ji}, y_{ji}\}$, as the case may be). By Ramsey's Theorem, since $|V| = \binom{2m}{m}$, the graph G either contains a clique or an anticlique of size $m + 1$. In case of a clique, we have $0 \leq i_0 < i_1 < \dots < i_m \leq M$ such that for any $j < k$,

$$\{a_{i_j}, a_{i_k}\} \rightarrow_{DM} \{x_{i_j i_k}, y_{i_j i_k}\} \Rightarrow_{N, 2^N} \{u', v'\},$$

so Φ_m holds for $x_j = a_{i_j}$, $y = u'$ and $z = v'$. The case of anticlique produces the satisfaction of Φ_m as well, just with b_{i_j} in place of a_{i_j} . In both subcases we get a contradiction. \square

4. Willard's theorem

We are now ready to prove the Willard's Finite Basis Theorem.

THEOREM 4.1 (Willard's Finite Basis Theorem). *Let \mathcal{V} be a congruence meet-semidistributive variety in a finite similarity type \mathcal{F} and having a finite residual bound. Then \mathcal{V} is finitely based.*

PROOF. Let $\text{resb}(\mathcal{V}) = m + 1$, that is, for all $\mathbf{S} \in \mathcal{V}_{SI}$, $|S| \leq m$. Let also $\mathbf{A} \in \mathcal{V}$ be arbitrary. We wish to prove that $\mathbf{A} \not\models \Phi_m$. Assume $\mathbf{A} \models \Phi_m$ which means that there exist $a_0, a_1, \dots, a_m \in A$ and $\{b, c\} \in A[2]$ such that for all $0 \leq i < j \leq m$, $\{a_i, a_j\} \Rightarrow_{DM+L, 2^L} \{b, c\}$. In particular, this means that $(b, c) \in \text{Cg}^{\mathbf{A}}(a_i, a_j)$, when $0 \leq i < j \leq m$. As we mentioned in the proof of Lemma 1.3, it is easy to prove that there is a maximal congruence θ in **Con** \mathbf{A} among all congruences which do not contain (b, c) and that θ is a strictly \wedge -irreducible. Therefore, \mathbf{A}/θ is subdirectly irreducible and since $(b, c) \notin \theta$ implies $(a_i, a_j) \notin \theta$ for $i \neq j$, then $|A/\theta| \geq m + 1$. This contradicts the assumption that $\text{resb}(\mathcal{V}) = m + 1$.

So, Φ_m fails in every algebra $\mathbf{A} \in \mathcal{V}$. Let \mathcal{W} be the (finitely based) variety in the similarity type \mathcal{F} axiomatized by the identities which say that s_i are Willard terms in \mathcal{V} . Therefore, $\mathcal{V} \subseteq \mathcal{W}$. Let ψ be the sentence which is the conjunction of $\neg\Phi_m$ and all basis equations for \mathcal{W} . If we define the strictly elementary class \mathcal{H} to be the class axiomatized by ψ we get $\mathcal{V} \subseteq \mathcal{H}$. Theorem 3.4 applies to \mathcal{W} , and so for any $\mathbf{A} \in \mathcal{H}$ and $a, b, c, d \in A$, $\text{Cg}^{\mathbf{A}}(a, b) \cap \text{Cg}^{\mathbf{A}}(c, d) \neq 0_{\mathbf{A}}$ iff $\mu_m(a, b, c, d)$ holds in \mathbf{A} , according to Theorem 3.4. Therefore, \mathcal{V} and \mathcal{H} satisfy the assumptions of Theorem 1.4, so \mathcal{V} is finitely based. \square

CHAPTER 6

The spiral method

CHAPTER 7

Undecidability of finite basis

Bibliography

- [1] Baker, K. A., *Finite equational bases for finite algebras in a congruence-distributive equational class*. Advances in Math. **24** (1977) no. 3, 207–243.
- [2] Baker, K. A., McNulty, G. F. and Wang, Ju, *An extension of Willard's finite basis theorem: congruence meet-semidistributive varieties of finite critical depth*, Algebra Universalis **52** (2004) no. 2-3, 289–302.
- [3] Baker, K. A., McNulty, G. F. and Werner, H., *The finitely based varieties of graph algebras*. Acta Sci. Math. (Szeged) **51** (1987), no. 1-2, 3–15.
- [4] Baker, K. A., McNulty, G. F. and Werner, H., *Shift-automorphism methods for inherently nonfinitely based varieties of algebras*, Czechoslovak Math. J. **39(114)** (1989) no. 1, 53–69.
- [5] Bryant, R. M., *The laws of finite pointed groups*, Bull. London Math. Soc. **14** (1982) no. 2, 119–123.
- [6] Burris, S. and Sankappanavar, H.P., *A Course in Universal Algebra*, Graduate Texts in Mathematics, Springer-Verlag, New York, 1981.
- [7] Dolinka, I., *A class of inherently nonfinitely based finite semirings*, to appear in Algebra Universalis.
- [8] Freese, R. and McKenzie, R., *Commutator theory for congruence modular varieties*, London Math. Soc. Lecture Note **125**, 1987.
- [9] Hobby, D. and McKenzie, R. *The structure of finite algebras*, Contemporary Mathematics **76**, American Mathematical Society, Providence, RI 1991.
- [10] Ježek, J., *Nonfinitely based three-element idempotent groupoids*, Algebra Universalis **20** (1985) no. 3, 292–301.
- [11] Kearnes, K. A. and Willard, R., *Residually finite, congruence meet-semidistributive varieties of finite type have a finite residual bound*, Proc. Amer. Math. Soc. **127** (1999) no. 10, 2841–2850.
- [12] Kruse, R. L., *Identities satisfied by a finite ring*, J. Algebra **26** (1973), 298–318.
- [13] L'vov, I. V., *Varieties of associative rings. I, II*, Algebra i Logika **12** (1973), 269–297,
- [14] Lyndon, R. C. *Identities in two-valued calculi*, Trans. Amer. Math. Soc. **71** (1951) 457–465.
- [15] Lyndon, R. C., *Identities in finite algebras*, Proc. Amer. Math. Soc. **5** (1954). 8–9.
- [16] Mal'cev, A. I., *On the general theory of algebraic systems*, Math. Sb. (N. S.) **35** (1954). 3–20.
- [17] Maróti, M. and McKenzie, R., *Finite basis problems and results for quasivarieties*, Studia Logica **78** (2004) no. 1-2, 293–320.
- [18] McKenzie, R., *Equational bases for lattice theories*, Math. Scand. **27** (1970) 24–38.

- [19] McKenzie, R., *Para-primal varieties: a study of finite axiomatizability and definable principal congruences in locally finite varieties*, Algebra Universalis **8** (1978), 336–348.
- [20] McKenzie, R., *Finite equational bases for congruence modular varieties*, Algebra Universalis **24** (1987), 244–250.
- [21] McKenzie, R., *The residual bounds of finite algebras*, Internat. J. Algebra Comput. **6** (1996) no. 1, 1–28.
- [22] McKenzie, R., *The residual bound of a finite algebra is not computable. (English summary)* Internat. J. Algebra Comput. **6** (1996) no. 1, 29–48.
- [23] McKenzie, R., *Tarski's finite basis problem is undecidable. (English summary)* Internat. J. Algebra Comput. **6** (1996) no. 1, 49–104.
- [24] McKenzie, R., McNulty, G. and Taylor, W., *Algebras, Lattices, Varieties, Volume I*, Wadsworth & Brooks/Cole, Monterey, CA, 1987.
- [25] McKenzie, R. and Valeriote, M., *The structure of decidable locally finite varieties*, Birkhäuser, Progress in Mathematics, vol. **79**, 1989.
- [26] Murskiĭ, V. L., *The existence in the three-valued logic of a closed class with a finite basis having no finite complete system of identities*, Dokl. Akad. Nauk SSSR **163** (1965) 815–818.
- [27] Neumann, B. H. *Identical relations in groups. I.*, Math. Ann. **114** (1937), no. 1, 506–525.
- [28] Oates, S. and Powell, M. B., *Identical relations in finite groups*. J. Algebra **1** (1964) 11–39.
- [29] Park, R. E., *A four-element algebra whose identities are not finitely based*, Algebra Universalis **11** (1980) no. 2, 255–260.
- [30] Park, R. E., *Equational classes of non-associative ordered systems*, PhD dissertation, UCLA, 1976.
- [31] Perkins, P., *Bases for equational theories of semigroups*, J. Algebra **11** (1969) 298–314.
- [32] uackebush, R. W., *Equational classes generated by finite algebras*, Algebra Universalis **1** (1971/72) 265–266.
- [33] Sapir, M. V., *Problems of Burnside type and the finite basis property in varieties of semigroups*, Izv. Akad. Nauk SSSR Ser. Mat. **51** (1987) no. 2, 319–340.
- [34] Sapir, M. V., *Inherently non-finitely based finite semigroups*, Mat. Sb. (N.S.) **133(175)** (1987) no. 2, 154–166.
- [35] Višin, V. V., *Identity transformations in a four-valued logic* Dokl. Akad. Nauk SSSR **150** (1963) 719–721.
- [36] Willard, R., *A finite basis theorem, version 0.2B*, manuscript(1997).
- [37] Willard, R., *Tarski's finite basis problem via $\mathbf{A}(\mathcal{T})$* , Trans. Amer. Math. Soc. **349** (1997), no. 7, 2755–2774.
- [38] Willard, R., *A finite basis theorem for residually finite, congruence meet-semidistributive varieties*, J. Symbolic Logic **65** (2000) no. 1, 187–200.