2017

Congruence n-permutable varieties

Jiali Li
Iowa State University

Congruence n-permutable varieties

by

Jiali Li

A dissertation submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Major: Mathematics

Program of Study Committee:
Clifford Bergman, Major Professor
Jonathan D.H. Smith
Yiu Tung Poon
Justin Peters
Jennifer Newman

Iowa State University

Ames, Iowa

2017

TABLE OF CONTENTS

LIST OF FIGURES

ACKNOWLEDGEMENTS

I would like to take this opportunity to express my thanks to those who helped me with various aspects of conducting research and the writing of this thesis. First and foremost, thank Professor Clifford Bergman for his patience and guidance during my phd period. Whenever I met the difficulties in the research, Dr. Bergman was always right alongside. Without your dedication, I could not have arrived at this point. I would also like to thank my committee members for their advice in going forward with this thesis. In particular, I would like to dedicate this thesis to my husband Li Lin who always encourages and supports me in my life when I was in any difficulties. Finally, I would like to thank the people of the department of mathematics at Iowa State University for all of their support and making Iowa State a great place to learn and work.

ABSTRACT

Many experts have been doing research on characterizations of congruence n-permutable varieties in many different ways. In 1973 Hagemann and Mitschke, generalizing Maltsev conditions, provided a simple and nice characterization of congruence n-permutable varieties. We offer our own approach to the characterization of congruence n-permutable varieties, inspired by the Kearnes and Tschantz lemma.

CHAPTER 1. BACKGROUND MATERIALS

1.1 Introduction

In 1954, A. I. Maltsev [14] first gave a result that a variety is congruence permutable if and only if the variety satisfies the conditions $p(x, y, y) \approx x$ and $p(x, x, y) \approx y$ for some ternary term $p(x, y, z)$. This is the prototype for what is now known as a "Maltsev condition". From then on, a lot of experts found that many algebraic properties of varieties have been shown to be related to Maltsev conditions, e.g., congruence modularity, congruence distributivity, congruence n-permutability for some positive integer n.

In the early 1980's, Ralph McKenzie and his student David Hobby [8] developed a structure theory for finite algebras and locally finite varieties which they call tame congruence theory. One of the important classes of varieties identified in tame congruence theory is the class of varieties which are congruence n-permutable for some positive integer n. Permutability of congruences had a great influence on the early development of universal algebra and its relation to lattice theory.

Many experts have been doing the research on characterization of congruence n-permutable varieties in many different ways. In 1973, Hagemann and Mitschke [7], generalizing Maltsev conditions, provided a simple and nice characterization of congruence n-permutable varieties. What we are doing is to do some work related to characterization of congruence n-permutable varieties in our own way. In the present chapter, we review the necessary concepts of universal algebra, terms and equation and basic isomorphism theorems. In chapter 2, we give our own result to characterize congruence n-permutable varieties, and the idea is inspired by one result of Dr. Kearnes and Tschantz [12] for the variety which is not congruence permutable, then we present some results for congruence 3-permutable varities. In chapter 3, we will discuss the permutability of the joins and maltsev product of two congruence permutable varieties and state some of our results. The final chapter outlines some possible directions for future research.

1.2 Universal Algebra

By an *algebra*, we mean any structure $\mathbf{A} = \langle A, f_i^{\mathbf{A}}(i \in I)\rangle$ which consists of a nonempty set A, called the *universe* of $\mathbf{A}$, and a system of finitary operations $f_i^{\mathbf{A}}$ over the set A, called the *basic operations* of $\mathbf{A}$. A subset of A that is closed under all the basic operations of $\mathbf{A}$ is called a *subuniverse* of $\mathbf{A}$, and if the subset is nonempty, it will form the universe of a subalgebra of $\mathbf{A}$. The *signature* of $\mathbf{A}$ is the indexed family $\tau = (n_i : i \in I)$, each n_i is the number of variables admitted by each operation $f_i^{\mathbf{A}}$. Algebras of the same signature are said to be *similar*. Operations of $n_i = 0, 1, 2$ are called *nullary* or *constant*, *unary* and *binary* respectively. An algebra whose universe consists of a single element is said to be *trivial*. An algebra with a singe binary operation is referred to as a *binar*.

We begin with some examples of algebras which will be used throughout this work, for notation, examples and proofs of theorems not included here, see [1].

Definition 1.2.1. *A* semigroup *is an algebra $\langle G, \cdot\, \rangle$ of signature $\langle 2\rangle$ satisfying the associative law:*

$$x\cdot (y\cdot z) \approx (x\cdot y)\cdot z\ .$$

Definition 1.2.2. *A* group *is an algebra $\langle G, \cdot\,, ^{-1}, e\rangle$ of signature $\langle 2, 1, 0\rangle$ such that $\langle G, \cdot\, \rangle$ is a semigroup, and the following identities hold:*

$$x\cdot e \approx e\cdot x \approx x,$$

$$x\cdot x^{-1} \approx x^{-1}\cdot x \approx e.$$

Definition 1.2.3. *A quasigroup is an algebra $\langle Q, \cdot\,, /, \backslash\rangle$ of signature $\langle 2, 2, 2\rangle$ such that the following identities hold:*

$$x\backslash(x\cdot y) \approx y, \quad (x\cdot y)/y \approx x,$$

$$x\cdot (x\backslash y) \approx y, \quad (x/y)\cdot y \approx x.$$

Definition 1.2.4. *A* ring *is an algebra* $\langle R, \cdot, +, -, 0\rangle$ *of signature* $\langle 2, 2, 1, 0\rangle$ *such that* $\langle R, +, -, 0\rangle$ *is an Abelian group, and* $\langle R, \cdot\rangle$ *is a semigroup satisfying the distributive laws:*

$$x\cdot (y + z) \approx x\cdot y + x\cdot z,$$

$$(y + z)\cdot x \approx y\cdot x + z\cdot x.$$

Definition 1.2.5. *For a fixed ring* $\boldsymbol{R}$*, an* $\boldsymbol{R}$*-module is an algebra* $\langle M, +, -, 0, \langle r : r \in R\rangle\rangle$ *where each* $r \in R$ *is interpreted as an unary operation,* $\langle M, +, -, 0\rangle$ *is an Abelian group, and for each* $r, s \in R$ *satisfying the identities:*

$$r(x + y) \approx rx + ry,$$

$$(r + s)x \approx rx + sx,$$

$$r(sx) \approx (rs)x.$$

Definition 1.2.6. *A* semilattice *is an algebra* $\langle S, \wedge\rangle$ *of signature* $\langle 2\rangle$ *satisfying the associative law*

$$x \wedge (y \wedge z) \approx (x \wedge y) \wedge z,$$

the idempotent law

$$x \wedge x \approx x,$$

the commutative law

$$x \wedge y \approx y \wedge x.$$

Example 1.2.1. *A typical example of a semilattice is formed by taking* S *to be the collection of all subsets of an arbitrary set with the operation being intersection.*

Example 1.2.2. *Another example is formed by taking* S *to be the compact convex sets on the Euclidean plane and the operation to be the formation of the closed convex hull of the union of two compact convex sets.*

Definition 1.2.7. *A* lattice *is an algebra* $\langle L, \wedge, \vee\rangle$ *with two binary operations such that both* $\langle L, \wedge\rangle$ *and* $\langle L, \vee\rangle$ *are semilattices, and these two basic operations satisfy the absorption laws*

$$x \vee (x \wedge y) \approx x,$$
$$x \wedge (x \vee y) \approx x.$$

The operation $\wedge$ is referred to as **meet**, and the operation $\vee$ is referred to as **join**.

Example 1.2.3. *A typical example of a lattice is formed by taking L to be the collection of all equivalence relations on an arbitrary set, $\wedge$ to be intersection, and $\vee$ to be the transitive closure of the union of two given equivalence relations.*

Example 1.2.4. *Another example is formed by taking L to be the set of all positive integers, $\vee$ to be the formation of the least common multiples, and $\wedge$ to be the formation of the greatest common divisors.*

Lattice is a very important algebra structure, and we will present some properties of this algebra.

Definition 1.2.8. *Let $\boldsymbol{L}$ be a lattice.*

(1) $\boldsymbol{L}$ *is called* distributive *if it satisfies*

$$x \wedge (y \vee z) \approx (x \wedge y) \vee (x \wedge z).$$

(2) $\boldsymbol{L}$ *is called* modular *if it satisfies*

$$z \leq x \Rightarrow x \wedge (y \vee z) \approx (x \wedge y) \vee z.$$

The following proposition can be easily obtained from the above definitions.

Proposition 1.2.1. ([*1*]) *Every distributive lattice is modular.*

Proof. Let L be a distributive lattice and $z \leq x$ in L. Then $x \wedge (y \vee z) \approx (x \wedge y) \vee (x \wedge z) \approx (x \wedge y) \vee z$. □

Besides the definitions of distributive lattice and modular lattice, we can use other ways to check if a lattice is distributive or modular.

Proposition 1.2.2. ([*1*]) *Let $\boldsymbol{L}$ be a lattice. $\boldsymbol{L}$ is distributive if and only if it satisfies*

$$x \vee (y \wedge z) \approx (x \vee y) \wedge (x \vee z).$$

There are two very special lattices with five elements, called $\mathbf{N}_5$ and $\mathbf{M}_3$. They play an important role in the theory of lattices. We can tell from the following theorems. Notice that $\mathbf{M}_3$ is modular and $\mathbf{N}_5$ is not modular.

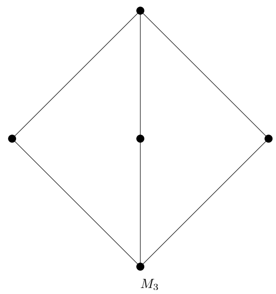

Figure 1.1 Lattice M_3

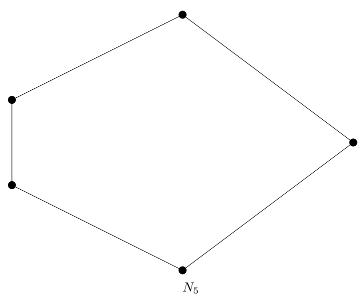

Figure 1.2 Lattice N_5

Theorem 1.2.1. (*Dedekind*) *Let* $\boldsymbol{L}$ *be a lattice. The following are equivalent.*

(1) $\boldsymbol{L}$ *is modular.*

(2) $\boldsymbol{L}$ *satisfies*

$$((x \wedge z) \vee y) \wedge z \approx (x \wedge z) \vee (y \wedge z).$$

(3) $\boldsymbol{L}$ *has no sublattice isomorphic to* $\boldsymbol{N}_5$.

This theorem reveals several things about the class of all modular lattices. The third equivalent condition allows us to determine the modularity of a lattice by considering its Hasse diagram. The second equivalent condition implies that subalgebras, homomorphic images and direct products of modular lattices are also modular.

Similarly, the following theorem reveals several things about the class of all distributive lattices.

Theorem 1.2.2. *(Birkhoff) Let* $\boldsymbol{L}$ *be a lattice. The following are equivalent.*

(1) $\boldsymbol{L}$ *is distributive.*

(2) $\boldsymbol{L}$ *satisfies*

$$(x \wedge y) \vee (x \wedge z) \vee (y \wedge z) \approx (x \vee y) \wedge (x \vee z) \wedge (y \vee z).$$

(3) $\boldsymbol{L}$ *has no sublattice isomorphic to either* $\boldsymbol{N}_5$ *or* $\boldsymbol{M}_3$*.*

The third equivalent condition allows us to determine the distributivity of a lattice by considering its Hasse diagram. The second equivalent condition implies that subalgebras, homomorphic images and direct products of distributive lattices are also distributive.

The two expressions in the second equivalent condition of the above theorem are very interesting in their own right and they have an unique name. Define:

$$m_1(x, y, z) = (x \wedge y) \vee (x \wedge z) \vee (y \wedge z),$$

$$m_2(x, y, z) = (x \vee y) \wedge (x \vee z) \wedge (y \vee z).$$

m_1 and m_2 are called *majority terms.* It is easy to verify that any lattice satisfies the identities

$$m_i(x, x, y) \approx m_i(x, y, x) \approx m_i(y, x, x) \approx x, \text{ for } i = 1, 2.$$

Definition 1.2.9. *A* Boolean Algebra *is an algebra* $\langle B, \wedge, \vee, ', 0, 1\rangle$ *such that* $\langle B, \wedge, \vee\rangle$ *is a distributive lattice with bounds* 0 *and* 1*, and for each* $x \in B$*,* x' *is a complement of* x*, i.e.* $x' \wedge x = 0$ *and* $x' \vee x = 1$*.*

Example 1.2.5. *As an example, take* B *to be the collection of all subsets of an arbitrary set* X*, let the join* $\vee$ *be union, the meet* $\wedge$ *be intersection, and the complementation* $'$ *be the set complementation relative to* X*.*

We have looked at examples of algebra, and naturally the relations on the algebra comes up. Let A be a set, and n a positive integer. A subset of A^n is called an n-ary relation on A. For the moment we will be interested in binary relations, i.e., sets of ordered pairs of elements of A.

Definition 1.2.10. *A binary relation* $\theta \subseteq A \times A$ *is an* equivalence relation *on* A *if for all* $x, y, z \in A$*,*

$$(x,x) \in \theta \quad \textit{(reflexivity)}$$
$$(x,y) \in \theta \Rightarrow (y,x) \in \theta \quad \textit{(symmetry)}$$
$$(x,y) \in \theta \textit{ and } (y,z) \in \theta \Rightarrow (x,z) \in \theta \quad \textit{(transitivity)}$$

Definition 1.2.11. *Let* $f : A \to B$ *be any function. We define*

$$ker(f) = \{(x,y) \in A^2 : f(x) = f(y)\}$$

called the kernel of f .

It is easy to check that $ker(f)$ is always an equivalence relation on A. Moreover, every equivalence relation is the kernel of a function.

Definition 1.2.12. *Let* $\boldsymbol{A}$ *be an algebra. A subset* U *of* A *is called a* subuniverse *of* $\boldsymbol{A}$ *if, for every basic operation* f *of* $\boldsymbol{A}$*, with* $n = rank(f)$*,*

$$u_1, u_2, \cdots, u_n \in U \Longrightarrow f(u_1, u_2, \cdots, u_n) \in U.$$

Definition 1.2.13. *Let* $\boldsymbol{A}$ *is an algebra, a binary relation* θ *on* A *is compatible with* $\boldsymbol{A}$ *if it is a subuniverse of* $\boldsymbol{A} \times \boldsymbol{A}$*, i.e., for every basic operation* f*, with* $n = rank(f)$*, we have*

$$(x_1, y_1), (x_2, y_2), \cdots, (x_n, y_n) \in \theta \Longrightarrow (f(x_1, x_2, \cdots, x_n), f(y_1, y_2, \cdots, y_n)) \in \theta.$$

Compared to equivalence relations, congruence is a more important concept in the universal algebra. It has some special property.

Definition 1.2.14. *A* congruence *relation on an algebra* $\boldsymbol{A}$ *is an equivalence relation on* A *that is compatible with* $\boldsymbol{A}$*.*

Let $\mathbf{A}$ be an algebra. The collection of congruences of $\mathbf{A}$ forms a lattice, denoted by $\mathbf{Con}(\mathbf{A})$, with lattice operations

$$\alpha \wedge \beta = \alpha \cap \beta,$$
$$\alpha \vee \beta = \text{the transitive closure of } \alpha \cup \beta.$$

The equivalence relations on A constitute a lattice $\mathbf{Eqv}(A)$, every congruence relation of $\mathbf{A}$ is an equivalence realtion on A, in fact, $\mathbf{Con}(\mathbf{A})$ is a sublattice of $\mathbf{Eqv}(A)$.

For an algebra $\mathbf{A}$. Let

$$0_A = \{(x, x) : x \in A\}$$

and

$$1_A = A \times A.$$

The equivalence relations 0_A and 1_A are always congruences.

Definition 1.2.15. *A nontrivial algebra possessing exactly two congruences is called* simple.

Definition 1.2.16. *For $\alpha, \beta \in$ **Con(A)**,*

$$\alpha \circ \beta = \{(x, y) : \exists z \in A \textit{ such that } (x, z) \in \alpha \textit{ and } (z, y) \in \beta\}.$$

Then, α and β permute if $\alpha \circ \beta = \beta \circ \alpha$.

Definition 1.2.17. *Let $\nu \subseteq A \times A$. The congruence on **A*** generagted by *ν is*

$$Cg^{\boldsymbol{A}}(\nu) = \bigcap\{\theta \in \boldsymbol{Con}(\boldsymbol{A}) : \nu \subseteq \theta\}.$$

As we recall from our group theory classes, there is a strong relationship between congruences and normal subgroups.

Theorem 1.2.3. [1] *Let $\boldsymbol{G} = \langle G, \cdot, ^{-1}, e\rangle$ be a group.*

(1) *For every normal subgroup N, the relation*

$$\theta_N = \{(x, y) \in G \times G : y^{-1} \cdot x \in N\}$$

*is a congruence on **G**.*

(2) *For every congruence θ, the equivalence class e/θ is a normal subgroup of **G**.*

(3) *The mapping $N \mapsto \theta_N$ is a bijection from the set of normal subgroups to the set of congruences, with inverse map $\theta \mapsto e/\theta$. For normal subgroups N and M,*

$$N \subseteq M \textit{ if and only if } \theta_N \subseteq \theta_M.$$

Given an algebra and its congruence, naturally we can construct a quotient algebra.

Definition 1.2.18. *Let θ be an equivalence relation on A. For $a \in A$ we write*

$$a/\theta = \{x \in A : (a, x) \in \theta\}$$

the equivalence class of a modulo θ*.*

The set of equivalence classes modulo θ is denoted A/θ, called the quotient of A by θ*.*

Definition 1.2.19. *Let $\boldsymbol{A}$ be an algebra and θ a congruence relation on A. The* quotient algebra $\boldsymbol{A}/\theta$ *is the algebra similar to $\boldsymbol{A}$, with universe A/θ and with basic operations defined by*

$$f^{\boldsymbol{A}/\theta}(a_1/\theta, \ldots, a_n/\theta) = f^{\boldsymbol{A}}(a_1, \ldots, a_n)/\theta,$$

where $a_1, \ldots, a_n \in A$.

We note that

$$\mathbf{A}/0_A \cong \mathbf{A}$$

and

$$\mathbf{A}/1_A \text{ is a trivial algebra.}$$

Of course most algebras will contain other congruences besides 0 and 1.

The constructions we have looked at so far, for example, subalgebras and quotient algebras, do not give a means of creating algebras of larger cardinality than what we start with, or of combining several algebras into one.

Definition 1.2.20. *Let $\boldsymbol{A} = \langle A, f_i^{\boldsymbol{A}}(i \in I)\rangle$, $\boldsymbol{B} = \langle B, f_i^{\boldsymbol{B}}(i \in I)\rangle$ be algebras with common signature.*

(1) *A function $h : B \to A$ is a* homomorphism *from $\boldsymbol{B}$ to $\boldsymbol{A}$ if for every $i \in I$ and every $b_1, b_2, \cdots, b_n \in B$,*

$$h(f_i^{\boldsymbol{B}}(b_1, \cdots, b_n)) = f_i^{\boldsymbol{A}}(h(b_1), \cdots, h(b_n)).$$

We say that $\boldsymbol{A}$ *is a* homomorphic image *of* $\boldsymbol{B}$ *if there is a homomorphism from* $\boldsymbol{B}$ *to* $\boldsymbol{A}$ *which is onto.*

(2) $\boldsymbol{B}$ *is a* subalgebra *of* $\boldsymbol{A}$ *if* $B \subseteq A$ *and for every* $f_i^{\boldsymbol{B}} = f_i^{\boldsymbol{A}} \restriction_{B^{n_i}}$.

Definition 1.2.21. *Let* $\boldsymbol{A}_1$ *and* $\boldsymbol{A}_2$ *be similar algebras. Define their* direct product $\boldsymbol{A}_1 \times \boldsymbol{A}_2$ *to be the algebra whose universe is the set* $A_1 \times A_2$, *and with basic operations defined by, such that for* $f \in \mathcal{F}_n$ *and* $a_i \in A_1, b_i \in A_2, 1 \leq i \leq n$, $\mathcal{F}_n$ *is the set of all the n-ary operations,*

$$f^{\boldsymbol{A}_1 \times \boldsymbol{A}_2}((a_1, b_1), \cdots, ((a_n, b_n))) = (f^{\boldsymbol{A}_1}(a_1, \cdots, a_n), f^{\boldsymbol{A}_2}(b_1, \cdots, b_n)).$$

Actually, both $\mathbf{A}_1$ and $\mathbf{A}_2$ are homomorphic images of $\mathbf{A}_1 \times \mathbf{A}_2$.

Definition 1.2.22. *The mapping*

$$p_i : A_1 \times A_2 \to A_i, \text{ for } i \in \{1, 2\},$$

defined by

$$p_i((a_1, a_2)) = a_i, \text{ for } (a_1, a_2) \in A_1 \times A_2, \ i \in \{1, 2\},$$

is called the projection map on the ith coordinate of $A_1 \times A_2$.

Proposition 1.2.3. ([3]) *For* $i = 1$ *or* 2, *the mapping* $p_i : A_1 \times A_2 \to A_i$ *is a surjective homomorphism from* $\boldsymbol{A} = \boldsymbol{A}_1 \times \boldsymbol{A}_2$ *to* $\boldsymbol{A}_i$. *Furthermore, in* $\boldsymbol{Con}(\boldsymbol{A}_1 \times \boldsymbol{A}_2)$, *we have*

$$ker\, p_1 \cap ker\, p_2 = 0_A,$$

$$ker\, p_1 \text{ and } ker\, p_2 \text{ permute},$$

and

$$ker\, p_1 \vee ker\, p_2 = 1_A$$

Definition 1.2.23. *A pair* $\{\alpha, \beta\} \subseteq \boldsymbol{Con}(\boldsymbol{A})$ *is called a pair of* complementary factor congruences *on algebra* $\boldsymbol{A}$ *if*

$$\alpha \cap \beta = 0_A$$

and

$$\alpha \circ \beta = 1_A.$$

The projection kernels on a direct product of two algebras always form a pair of complementary factor congruences.

Theorem 1.2.4. ([*3*]) *If* α *and* β *form a pair of complementary factor congruences on an algebra* $\boldsymbol{A}$*, then*

$$\boldsymbol{A} \cong \boldsymbol{A}/\alpha \times \boldsymbol{A}/\beta$$

under the mapping $a \to (a/\alpha, a/\beta)$*, for* $a \in A$*.*

Conversely, every direct product decomposition arises in this way.

Definition 1.2.24. *A nontrivial algebra is called* directly indecomposable *if it is not isomorphic to a direct product of two nontrivial algebras.*

Equivalently, $\mathbf{A}$ is directly indecomposable if and only if the only pair of complementary factor congruences on $\mathbf{A}$ is $\{0_A, 1_A\}$.

Lemma 1.2.1. ([*1*]) *Suppose that* $\boldsymbol{A} = \boldsymbol{A}_1 \times \boldsymbol{A}_2$*, and let* α_1 *and* α_2 *be the projection kernels. Then*

$$\boldsymbol{A}/\alpha_i \cong \boldsymbol{A}_i \text{ for } i = 1, 2.$$

From the Correspondence Theorem it follows that the lattice $\mathbf{Con}(\mathbf{A}_i)$ is isomorphic to the interval $\mathbf{I}[\alpha_i, 1_A]$ of $\mathbf{Con}(\mathbf{A})$.

Lemma 1.2.2. ([*1*]) *Let* $\boldsymbol{A}$ *and* $\boldsymbol{B}$ *be similar algebras. The mapping*

$$(\alpha, \beta) \mapsto \alpha \times \beta$$

gives an embedding of $\boldsymbol{Con}(\boldsymbol{A}) \times \boldsymbol{Con}(\boldsymbol{B})$ *into* $\boldsymbol{Con}(\boldsymbol{A} \times \boldsymbol{B})$*.*

1.3 Varieties

A major theme in universal algebra is the study of classes of algebras of common signature closed under one or more constructions. Given a class $\mathcal{K}$ of algebras with common signature, we adopt the notation:

$\mathbf{H}(\mathcal{K})$ = the class of all homomorphic images of members of $\mathcal{K}$.

$\mathbf{S}(\mathcal{K})$ = the class of all algebras isomorphic to subalgebras of members of $\mathcal{K}$.

$\mathbf{P}(\mathcal{K})$ = the class of all algebras isomorphic to direct products of members of $\mathcal{K}$.

$\mathbf{P_s}(\mathcal{K})$ = the class of all algebras isomorphic to subdirect products of members of $\mathcal{K}$.

Lemma 1.3.1. ([3]) *The following inequalities hold:* $\boldsymbol{SH} \leq \boldsymbol{HS}$, $\boldsymbol{PS} \leq \boldsymbol{SP}$ *and* $\boldsymbol{PH} \leq \boldsymbol{HP}$.

Definition 1.3.1. *A* variety $\mathcal{V}$ *is a class of algebras over a common signature that is closed under homomorphic images(*$\boldsymbol{H}$*), subalgebras(*$\boldsymbol{S}$*), and direct products(*$\boldsymbol{P}$*).*

The class of groups forms a class of algebras of signature $\langle 2, 1, 0\rangle$ and it is a variety. The class of semilattices forms a class of algebras of signature $\langle 2\rangle$ and it is also a variety.

The intersection of a class of varieties of common signature is a variety.

Definition 1.3.2. *We define the closure operator* $\boldsymbol{V}(\mathcal{K})$ *to be the smallest variety containing* $\mathcal{K}$*.* $\boldsymbol{V}(\mathcal{K})$ *is called the variety generated by* $\mathcal{K}$*. If* $\mathcal{K} = \{\boldsymbol{A}_1, \boldsymbol{A}_2 \cdots, \boldsymbol{A}_k\}$ *is a finite set of algebras, then we often write* $\boldsymbol{V}(\boldsymbol{A}_1, \boldsymbol{A}_2 \cdots, \boldsymbol{A}_k)$ *instead of* $\boldsymbol{V}(\mathcal{K})$*.*

We would like to know how to construct $\mathbf{V}(\mathcal{K})$ directly from $\mathcal{K}$. It would seem as if one would have to iteratively apply the operators **H**, **S** and **P** infinitely many times to generate a variety. Garrett Birkhoff's **HSP** Theorem showed that in order to generate $\mathbf{V}(\mathcal{K})$, it is enough to apply each of **H**, **S** and **P** to $\mathcal{K}$ once, as long as one does it in the correct order.

Theorem 1.3.1. $(Tarski)$ ***V*=*HSP***

Proof. Let $\mathcal{K}$ be some class of algebras. To see that $\mathbf{HSP}(\mathcal{K})$ is a variety, we use Lemma 1.3.1 to compute $\mathbf{H}(\mathbf{HSP}) = \mathbf{HSP}$, $\mathbf{S}(\mathbf{HSP}) \leq \mathbf{HS}^2\mathbf{P} = \mathbf{HSP}$, $\mathbf{P}(\mathbf{HSP}) \leq \mathbf{HSP}^2 = \mathbf{HSP}$. Thus, $\mathbf{HSP} \geq \mathbf{V}$.

On the other hand, with $\mathcal{V} = \mathbf{V}(\mathcal{K})$,

$$\mathbf{HSP}(\mathcal{K}) \subseteq \mathbf{HSP}(\mathcal{V}) = \mathcal{V} = \mathbf{V}(\mathcal{K}),$$

so $\mathbf{HSP} \leq \mathbf{V}$.

□

Definition 1.3.3. (1) *An algebra is called* locally finite *if every finitely generated subalgebra is finite.*

(2) *A variety is* locally finite *if every member is locally finite.*

(3) *A variety is called finitely generated if it is of the form* $\boldsymbol{V}(\mathcal{K})$ *in which* $\mathcal{K}$ *is a finite set of finite algebras.*

Example 1.3.1. *For example, the Abelian group* $\mathbb{Z}$ *is not locally finite since for any* $n \neq 0$, $Sg(n)$ *is infinite. On the other hand, the groups* $\mathbb{Z}(p^\infty)$ *are locally finite.*

Theorem 1.3.2. ([*1*]) *Every finitely generated variety is locally finite.*

Proof. Let $\mathcal{V}$ be a finitely generated variety. Thus $\mathcal{V} = \mathbf{V}(\mathcal{K})$ where $\mathcal{K} = \{\mathbf{A}_1, \mathbf{A}_2, \cdots, \mathbf{A}_n\}$, n is a natural number and each $\mathbf{A}_k$ is finite. Let $\mathbf{B}$ be a finitely generated member of $\mathcal{V}$, say $\mathbf{B}$ is generated by the finite set Y. We must show that B is finite.

Since $\mathbf{B} \in \mathcal{V} = \mathbf{HSP}(\mathcal{K})$, there is an algebra $\mathbf{C}$, a surjective homomorphism $h : \mathbf{C} \to \mathbf{B}$ and algebras $\mathbf{C}_i \in \mathcal{K}$, for $i \in I$, such that $\mathbf{C}$ is isomorphic to a subalgebra of the product $\prod_i \mathbf{C}_i$. Since h is surjective, we can find a subset X of C such that h is a bijection of X with Y. Thus X is finite. By replacing $\mathbf{C}$ with $Sg^{\mathbf{C}}(X)$, we can assume that $\mathbf{C}$ is finitely generated. It suffices to show that C is finite.

Let g denote the embedding of $\mathbf{C}$ into the product and, for each $i \in I$, p_i denote the projection of the product onto the ith factor. For each $k \leq n$, the algebra $\mathbf{A}_k$ is finite. Since $\mathbf{C}$ is finitely generated, $\text{Hom}(\mathbf{C}, \mathbf{A}_k)$ is a finite set. Since $\{p_i \circ g : i \in I\} \subseteq \bigcup_{k=1}^{n} \text{Hom}(\mathbf{C}, \mathbf{A}_k)$, there are actually only finitely many maps $p_i \circ g$. Thus there is a finite subset J of I such that $\{p_i \circ g : i \in I\} = \{p_j \circ g : j \in J\}$. We have $0_C = \bigcap\{ker(p_i \circ g) : i \in I\} = \bigcap\{ker(p_j \circ g) : j \in J\}$. Thus $\mathbf{C}$ embeds into the product $\prod_{j \in J} \mathbf{C}_j$. Since this is a finite product of finite algebras, C, hence B, is finite. □

The converse of the above theorem is false, for example, the variety of p-algebras is locally finite but not finitely generated.

Idempotent algebras and varieties are important for a number of reasons, not the least of which is the role of finite idempotent algebras in the algebraic approach to the Constraint Satifaction Dichotomy Conjecture.

Definition 1.3.4. (1) *An algebra* $\boldsymbol{A}$ *is* idempotent *if each of its fundamental operations* f *satisfies*

$$f(x, x, \cdots, x) \approx x$$

for any $x \in \boldsymbol{A}$.

(2) *A variety* $\mathcal{V}$ *is* idempotent *if each algebra* $\boldsymbol{A}$ *in* $\mathcal{V}$ *is idempotent.*

Orderable algebras will be used in our main theorem, the following is its concept.

Definition 1.3.5. *A partial order on set* A *is a binary relation on* A *which is reflexive, anti-symmetric and transitive,*

An algebra $\boldsymbol{A}$ *is* orderable *if there is a compatible non-trivial partial order on* $\boldsymbol{A}$. *This is equivalent to all of the term operations of* $\boldsymbol{A}$ *being monotone with respect to some non-trivial partial order on* A.

Example 1.3.2. *Every semilattice* $\langle S, \wedge \rangle$ *is an orderable algebra.*

Define a partial order $\preceq$, $a \preceq b$ *if and only if* $a \wedge b = a$. *Then verify it is compatible, for* $a \preceq b$, *and* $c \preceq d$, *we have*

$$(a \wedge c) \wedge (b \wedge d) = (a \wedge b) \wedge (c \wedge d) = a \wedge c,$$

so $a \wedge c \preceq b \wedge d$.

1.4 Terms and Free Algebras

One focus of universal algebra is the study of structural properties of algebras and varieties. By compositions of the fundamental operations, it will lead to terms.

Definition 1.4.1. *Let* X *be a set of distinct objects called variables. Let* $\mathcal{F}$ *be a type of algebras. The set* $T(X)$ *of terms of type* $\mathcal{F}$ *over* X *is the smallest set such that*

$$X \cup \mathcal{F}_0 \subseteq T(X),$$

$$\text{if } p_1, \ldots, p_n \in T(X) \text{ and } f \in \mathcal{F}_n, \text{ then the "string" } f(p_1, \ldots, p_n) \in T(X).$$

Example 1.4.1. *For example,* $\boldsymbol{G} = \langle G, \cdot, ^{-1}, e \rangle$ *is an algebra, we could have a binary term on the algebra* $\boldsymbol{G}$, *mapping* (x, y) *to* $x \cdot y \cdot x^{-1} \cdot y^{-1}$.

Example 1.4.2. *Let $\mathcal{F}$ consist of two binary operation symbols $+$ and $\cdot$, and let $X = \{x, y, z\}$. Then $x, y, x\cdot y, x\cdot(y+z)$, and $(x\cdot y)+(x\cdot z)$.*

Definition 1.4.2. *Let $\mathcal{K}$ be a class of algebras and $\boldsymbol{U}$ an algebra of the same signature as the members of $\mathcal{K}$. Let X be a subset of U.*

(1) *We say that $\boldsymbol{U}$ has the universal mapping property for $\mathcal{K}$ over X if for every $\boldsymbol{A} \in \mathcal{K}$ and every function $h : X \to A$, there is a homomorphism $\bar{h} : \boldsymbol{U} \to \boldsymbol{A}$ such that $\bar{h}_{\restriction X} = h$.*

(2) *We say that $\boldsymbol{U}$ is free for $\mathcal{K}$ over X if $\boldsymbol{U}$ has the universal mapping property and furthermore, $\boldsymbol{U}$ is generated by X.*

(3) *Finally, $\boldsymbol{U}$ is free in $\mathcal{K}$ over X if $\boldsymbol{U}$ is free for $\mathcal{K}$ over X and $\boldsymbol{U}$ is a member of $\mathcal{K}$.*

Proposition 1.4.1. ([*1*]) *Let $\boldsymbol{U}$ be free for $\mathcal{K}$ over X. Then for every $\boldsymbol{A} \in \mathcal{K}$ and $h : X \to A$, the extension $\bar{h}$ of h to $\boldsymbol{U}$ is unique.*

Proposition 1.4.2. ([*1*]) *Let $\boldsymbol{U}_1$ and $\boldsymbol{U}_2$ be free in $\mathcal{K}$ over X_1 and X_2 respectively. If $|X_1| = |X_2|$, then*

$$\boldsymbol{U}_1 \cong \boldsymbol{U}_2.$$

It tells us that up to isomorphism, a free algebra is determined by the cardinality of a free generating set. Every variety has free algebras. The freeness extends upwards from a class $\mathcal{K}$ to its generated variety.

Proposition 1.4.3. ([*1*]) *Let $\boldsymbol{U}$ be free for $\mathcal{K}$ over X. Then $\boldsymbol{U}$ is free for $\boldsymbol{HSP}(\mathcal{K})$ over X.*

Proof. Let $\mathbf{U}$ be free for $\mathcal{K}$ over X. It is enough to show that if $\mathbf{O}$ is one of $\mathbf{H}$,$\mathbf{S}$ or $\mathbf{P}$ then $\mathbf{U}$ has the universal mapping property for $\mathbf{O}(\mathcal{K})$ over X.

Consider the case $\mathbf{A} \in \mathbf{H}(\mathcal{K})$. Then there is $\mathbf{B} \in \mathcal{K}$ and a surjective homomorphism $f : \mathbf{B} \to \mathbf{A}$. Let $h : X \to A$ be a function. We must find an extension of h to a homomorphism from $\mathbf{U}$ to $\mathbf{A}$. For each $x \in X$ choose an element $b_x \in \overleftarrow{f}(h(x))$. Define the function $g : X \to B$ by $g(x) = b_x$. Since $\mathbf{U}$ is free for $\mathcal{K}$ and $\mathbf{B} \in \mathcal{K}$, g extends to a homomorphism $\overline{g} : \mathbf{U} \to \mathbf{B}$. Then $f \circ \overline{g}$ is the desired extension of h.

Now assume that $\mathbf{A} \in \mathbf{S}(\mathcal{K})$. Thus $\mathbf{A} \leq \mathbf{B} \in \mathcal{K}$. A mapping h from X to A is automatically a mapping to B. By freeness, h extends to a homomorphism $h^* : \mathbf{U} \to \mathbf{B}$. Since X generates U,

$$\overrightarrow{h^*}(U) = \overrightarrow{h^*}(Sg^{\mathbf{U}(X)}) = Sg^{\mathbf{B}}(\overrightarrow{h}(X)) \subseteq A.$$

Consequently, h^* is actually a map from $\mathbf{U}$ to $\mathbf{A}$.

Finally, assume that $\mathbf{A} = \prod \mathbf{B}_i$ with each $\mathbf{B}_i \in \mathcal{K}$. If $h : X \to A$ then for each i, $p_i \circ h$ is a mapping from X to B_i. By freeness we get homomorphisms $\overline{h}_i : \mathbf{U} \to \mathbf{B}_i$ which can be reassembled to obtain $\overline{h} = \prod \overline{h}_i : \mathbf{U} \to \mathbf{A}$. □

Example 1.4.3. *As an example, let $\mathbb{Z}_n$ denote the cyclic group of order n. The group $\mathbb{Z}_{30}$ is free for $\mathcal{K} = \{\mathbb{Z}_2, \mathbb{Z}_3\}$ over $\{1\}$. Therefore, $\mathbb{Z}_{30}$ is free for $\mathcal{A}_6 = \boldsymbol{HSP}(\mathcal{K})$, which happens to be the variety of Abelian groups satisfying the identity $6x \approx 0$. But note that $\mathbb{Z}_{30}$ is not a member of $\mathcal{A}_6$. In order to construct an algebra free in $\mathcal{A}_6$, we must resort to a homomorphic image of $\mathbb{Z}_{30}$ that retains the universal mapping property, in this case $\mathbb{Z}_6$. This approach applies quite generally.*

Definition 1.4.3. *Let ρ be a signature. An* identity *or* equation *of signature ρ is an ordered pair of terms, written $p \approx q$. If A is an algebra of signature ρ, we say that A satisfies $p \approx q$ if $p^{\boldsymbol{A}} = q^{\boldsymbol{A}}$. In this situation, we write*

$$\boldsymbol{A} \models p \approx q.$$

If $\mathcal{K}$ is a class of algebras, we write $\mathcal{K} \models p \approx q$ if for every $\boldsymbol{A} \in \mathcal{K}$, $\boldsymbol{A} \models p \approx q$. Finally, if Σ is a set of equations, we write $\mathcal{K} \models \Sigma$ if every member of $\mathcal{K}$ satisfies every member of Σ.

Example 1.4.4. *For example, consider a single binary operation symbol. Let p be the term $x \cdot (y \cdot z)$ and q the term $(x \cdot y) \cdot z$. These terms are distinct. It would never be correct to write $p = q$. However, in any semigroup $\boldsymbol{A}$, the terms should somehow represent the same quantity. That quantity is precisely the term operation $p^{\boldsymbol{A}}$ and it is correct to write $p^{\boldsymbol{A}} = q^{\boldsymbol{A}}$. Observe that the equality of those two term operations exactly captures the fact that for every $a, b, c \in A$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.*

Lemma 1.4.1. ([*1*]) *For any class $\mathcal{K}$, each of the classes $\boldsymbol{S}(\mathcal{K})$, $\boldsymbol{H}(\mathcal{K})$, $\boldsymbol{P}(\mathcal{K})$ and $\boldsymbol{V}(\mathcal{K})$ satisfy exactly the same identities as does $\mathcal{K}$.*

Lemma 1.4.2. ([*1*]) *$\mathcal{K} \models p \approx q$ if and only if for every $\boldsymbol{A} \in \mathcal{K}$ and every homomorphism $h : \boldsymbol{T}(X) \to \boldsymbol{A}$, we have*

$$h(p) = h(q).$$

Proof. First assume that $\mathcal{K} \models p \approx q$. Pick $\mathbf{A}$ and h as in the lemma. Then

$$\mathbf{A} \models p \approx q \Longrightarrow p^{\mathbf{A}} = q^{\mathbf{A}} \Longrightarrow p^{\mathbf{A}}(h(x_1), \cdots, h(x_n)) = q^{\mathbf{A}}(h(x_1), \cdots, h(x_n)).$$

Since h is a homomorphism, we get $h(p^{\mathbf{T}}(x_1, \cdots, x_n)) = h(q^{\mathbf{T}}(x_1, \cdots, x_n))$, i.e., $h(p) = h(q)$. To prove the converse we must take any $\mathbf{A} \in \mathcal{K}$ and $a_1, \cdots, a_n \in A$ and show that $p^{\mathbf{A}}(a_1, \cdots, a_n) = q^{\mathbf{A}}(a_1, \cdots, a_n)$. Let $h_0 : X \to A$ be a function with $h_0(x_i) = a_i$, for $i \leq n$. Then h_0 extends to a homomorphism h from $\mathbf{T}(X)$ to $\mathbf{A}$. By assumption $h(p) = h(q)$. Since $h(p) = h(p^{\mathbf{T}}(x_1, \cdots, x_n)) = p^{\mathbf{A}}(h(x_1), \cdots, h(x_n)) = p^{\mathbf{A}}(a_1, \cdots, a_n)$, the result follows.

□

Definition 1.4.4. *Let $\mathcal{K}$ be a class of algebras and Σ a set of equations. We define*

$$Id(\mathcal{K}) = \{p \approx q : \mathcal{K} \models p \approx q\},$$

$$Mod(\Sigma) = \{A : A \models \Sigma\}.$$

Classes of the form $Mod(\Sigma)$ are called equational classes, and Σ is called an equational base. $Mod(\Sigma)$ is called the class of models of Σ. Dually, a set of identities of the form $Id(\mathcal{K})$ is called an equational theory.

Theorem 1.4.1. ([*1*]) *Every variety is an equational class.*

This theorem is the first truly fundamental result of universal algebra. It is probably the reason that the subject exists at all. It says that the classes closed under **H**, **S** and **P** are precisely the ones definable by equations. The following corollary is a restatement of the theorem. Think of it as giving another description of the algebras that lie in the variety generated by a class of $\mathcal{K}$.

Corollary 1.4.1. ([*1*]) *For any class $\mathcal{K}$ of algebras,*

$$\boldsymbol{V}(\mathcal{K}) = Mod(Id(\mathcal{K})).$$

Corollary 1.4.2. ([*1*]) *Let Y be an infinite set and $\mathcal{V}$ a variety. Then*

$$\mathcal{V} = \boldsymbol{V}(F_{\mathcal{V}}(Y)).$$

Thus, every variety is generated by a single algebra.

1.5 The Isomorphism Theorems

An understanding of the complex interplay of subalgebras, homomorphisms and products is essential to the mastery of universal algebra. We explain tools that allow us to understand how algebras and varieties are put together.

Definition 1.5.1. *Let A and B be sets, and $f : A \to B$ a function. Then f induces two maps on the subsets of A and B as follows.*

$$\overrightarrow{f} : Sb(A) \mapsto Sb(B) \text{ given by } X \mapsto \{f(x) : x \in X\},$$

$$\overleftarrow{f} : Sb(B) \mapsto Sb(A) \text{ given by } Y \mapsto \{a \in A : f(a) \in Y\}.$$

We can call these maps $\overrightarrow{f}$ and $\overleftarrow{f}$ as the direct *and* inverse image *under f.*

For any subsets X and Y of B, and Z and W of A,
$\overleftarrow{f}(X \cap Y) = \overleftarrow{f}(X) \cap \overleftarrow{f}(Y)$, $\overleftarrow{f}(X \cup Y) = \overleftarrow{f}(X) \cup \overleftarrow{f}(Y)$,
$\overleftarrow{f}(\emptyset) = \emptyset$, $\overleftarrow{f}(B) = A$,
$\overrightarrow{f}(W \cup Z) = \overrightarrow{f}(W) \cup \overrightarrow{f}(Z)$,
$\overrightarrow{f}\overleftarrow{f}(X) \subseteq X$, $\overleftarrow{f}\overrightarrow{f}(Z) \supseteq Z$.

Notice that the two inclusions at the bottom become equalities if f is surjective for the first or injective for the second.

Lemma 1.5.1. ([3]) *Let $f : \boldsymbol{A} \to \boldsymbol{B}$ be a homomorphism. Then the image of a subuniverse of $\boldsymbol{A}$ under f is a subuniverse of $\boldsymbol{B}$, and the inverse image of a subuniverse of $\boldsymbol{B}$ is a subuniverse of $\boldsymbol{A}$.*

That means: If $f : \mathbf{A} \to \mathbf{B}$ is a homomorphism, $\mathbf{C}$ is a subalgebra of $\mathbf{A}$ and $\mathbf{D}$ is a subalgebra of $\mathbf{B}$, then $\overrightarrow{f}(\mathbf{C})$ is the subalgebra of $\mathbf{B}$ with universe $\overrightarrow{f}(C)$ and $\overleftarrow{f}(\mathbf{D})$ is the subalgebra of $\mathbf{A}$ with universe $\overleftarrow{f}(D)$.

Lemma 1.5.2. ([3]) *Suppose $f : \boldsymbol{A} \to \boldsymbol{B}$ and $g : \boldsymbol{B} \to \boldsymbol{C}$ are homomorphisms. Then the composition $g \circ f$ is a homomorphism from $\boldsymbol{A}$ to $\boldsymbol{C}$.*

Theorem 1.5.1. ([*1*]) $\boldsymbol{A}$ *and* $\boldsymbol{B}$ *are algebras. Let* $f : \boldsymbol{A} \to \boldsymbol{B}$ *be a homomorphism. Then for any subset* X *of* A*,*

$$\overrightarrow{f}(Sg^{\boldsymbol{A}}(X)) = Sg^{\boldsymbol{B}}(\overrightarrow{f}(X)).$$

Proof. It is easy to check that $\overrightarrow{f}$ is order-preserving. Using that observation,

$$X \subseteq Sg^{\mathbf{A}}(X) \Longrightarrow \overrightarrow{f}(X) \subseteq \overrightarrow{f}(Sg^{\mathbf{A}}(X)) \Longrightarrow Sb^{\mathbf{B}}(\overrightarrow{f}(X)) \subseteq \overrightarrow{f}(Sg^{\mathbf{A}}(X)).$$

Conversely,

$$X \subseteq \overleftarrow{f}\,\overrightarrow{f}(X) \subseteq \overleftarrow{f}(Sg^{\mathbf{B}}(\overrightarrow{f}(X))) \Longrightarrow Sg^{\mathbf{A}}(X) \subseteq \overleftarrow{f}(Sg^{\mathbf{B}}(\overrightarrow{f}(X))) \Longrightarrow$$

$$\overrightarrow{f}(Sg^{\mathbf{A}}(X)) \subseteq \overrightarrow{f}\,\overleftarrow{f}(Sg^{\mathbf{B}}(\overrightarrow{f}(X))) \subseteq Sg^{\mathbf{B}}(\overrightarrow{f}(X)).$$

□

Corollary 1.5.1. ([*1*]) $\boldsymbol{A}$ *and* $\boldsymbol{B}$ *are algebras. Let* $f : \boldsymbol{A} \to \boldsymbol{B}$ *be a homomorphism. The map* $\overrightarrow{f} : Sub\boldsymbol{A} \to Sub\boldsymbol{B}$ *is join-preserving and* $\overleftarrow{f} : Sub\boldsymbol{B} \to Sub\boldsymbol{A}$ *is meet-preserving. Thus, both maps are order-preserving.*

Example 1.5.1. *Let* $\mathbb{R}$ *denote the additive group of real numbers, and define* $f : \mathbb{R}^2 \to \mathbb{R}$ *by* $f(x, y) = x - y$*.* f *is easily seen to be a homomorphism. Let* $X = \mathbb{R} \times \{0\}$ *and* $Y = \{0\} \times \mathbb{R}$ *be subalgebras of* $\mathbb{R}^2$*. Then* $X \cap Y = \{(0, 0)\}$*, so* $\overrightarrow{f}(X \cap Y) = \{0\}$*. But* $\overrightarrow{f}(X) \cap \overrightarrow{f}(Y) = \mathbb{R} \cap \mathbb{R} = \mathbb{R}$*. Thus* $\overrightarrow{f}$ *does not in general preserve meets.*

If $\theta \subseteq A^2$ and $\psi \subseteq B^2$, then we define

$$\overrightarrow{f}(\theta) = \{(f(x), f(y)) : (x, y) \in \theta\},$$

$$\overleftarrow{f}(\psi) = \{(x, y) \in A^2 : (f(x), f(y)) \in \psi\}.$$

Lemma 1.5.3. ([*1*]) $\boldsymbol{A}$ *and* $\boldsymbol{B}$ *are algebras. Let* $f : \boldsymbol{A} \to \boldsymbol{B}$ *be a homomorphism. Then for every* $\psi \in \boldsymbol{Con}(\boldsymbol{B})$*,* $\overleftarrow{f}(\psi)$ *is a congruence on* $\boldsymbol{A}$*.*

Theorem 1.5.2. *(The First Isomorphism Theorem) Let* $\boldsymbol{A}$ *and* $\boldsymbol{B}$ *be similar algebras, and let* $h : \boldsymbol{A} \to \boldsymbol{B}$ *with kernel* θ*. There is a unique injective homomorphsim* $\overline{h} : \boldsymbol{A}/\theta \to \boldsymbol{B}$ *such that* $\overline{h} \circ q_\theta = h$*. If* h *is surjective, then* $\overline{h}$ *is an isomorphism.*

Proof. A typical element of $\mathbf{A}/\theta$ is of the form a/θ, for some $a \in A$. Since $a/\theta = q_\theta(a)$ the condition $\overline{h} \circ q_\theta = h$ requires that $\overline{h}(a/\theta) = h(a)$. That covers the uniqueness clause in the theorem. We must verify that $\overline{h}$ is an injective homomorphism. Consider the chain of equivalences

$$a/\theta = b/\theta \Longleftrightarrow (a,b) \in \theta = kerh \Longleftrightarrow h(a) = h(b) \Longleftrightarrow \overline{h}(a/\theta) = \overline{h}(b/\theta).$$

The left-to-right direction is exactly the assertion that $\overline{h}$ is well-defined, while the right-to-left directions says that $\overline{h}$ is injective. Finally to check that $\overline{h}$ is a homomorphism, let f be an n-ary operation symbol. Then for all $a_1, \cdots, a_n \in A$,

$$\overline{h}(f^{\mathbf{A}/\theta}(\mathbf{a}/\theta)) = \overline{h}(f^{\mathbf{A}}(\mathbf{a})/\theta) = h(f^{\mathbf{A}}(\mathbf{a})) = f^{\mathbf{B}}(h(\mathbf{a})) = f^{\mathbf{B}}(\overline{h}(\mathbf{a}/\theta)).$$

□

Definition 1.5.2. *Let θ and ψ be congruences of $\boldsymbol{A}$, and assume that $\theta \subseteq \psi$. We define a binary relation ψ/θ on A/θ by*

$$\psi/\theta = \{(x/\theta, y/\theta) : (x,y) \in \psi\}.$$

Theorem 1.5.3. *(The Second Isomorphism Theorem) Let $\theta \subseteq \psi$ be congruences on an algebra $\boldsymbol{A}$. Then ψ/θ is a congruence on $\boldsymbol{A}/\theta$. The algebras $(\boldsymbol{A}/\theta)/(\psi/\theta)$ and $\boldsymbol{A}/\psi$ are isomorphic.*

Proof. Define $f : \mathbf{A}/\theta \to \mathbf{A}/\psi$ by $f(a/\theta) = a/\psi$. The condition $\theta \subseteq \psi$ is equivalent to the assertion that f is well-defined. Clearly, f is surjective. A straightforward verification shows that f is a homomorphism and that $kerf = \psi/\theta$. Thus by the fundamental homomorphism theorem,

$$\mathbf{A}/\psi \cong (\mathbf{A}/\theta)/kerf = (\mathbf{A}/\theta)/(\psi/\theta).$$

□

Theorem 1.5.4. *(Correspondence Theorem) Let $\boldsymbol{A}$ be an algebra and let θ be a congruence on $\boldsymbol{A}$. Let $q : \boldsymbol{A} \to \boldsymbol{A}/\theta$ be the canonical homomorphism. Then $\overline{q}$ is a lattice isomorphism of the interval $\boldsymbol{I}[\theta, 1_A]$ of $\boldsymbol{Con}(\boldsymbol{A})$ with $\boldsymbol{Con}(\boldsymbol{A}/\theta)$ mapping ψ to ψ/θ.*

Proof. Suppose that ψ is a congruence on A and that $\theta \subseteq \psi$. It follows directly from the definition that $\overrightarrow{q}(\psi) = \psi/\theta$. We wish to show that $\overrightarrow{q}$ is a lattice isomorphism with inverse $\overleftarrow{q}$.

We already know that both $\overrightarrow{q}$ and $\overleftarrow{q}$ are order-preserving. And according to equations, $\overrightarrow{q} \circ \overleftarrow{q}$ is the identity map. For the other direction

$$(a, b) \in \overleftarrow{q}\,\overrightarrow{q}(\psi) \Longleftrightarrow (q(a), q(b)) \in \overleftarrow{q}(\psi) \Longleftrightarrow$$

$(a/\theta, b/\theta) \in \psi/\theta \Longleftrightarrow (a, b) \in \psi$.

□

CHAPTER 2. CHARACTERIZATION OF CONGRUENCE n-PERMUTABLE VARIETIES

2.1 Congruence n-permutable Varieties

An algebra is said to be congruence permutable if every pair of congruences on the algebra permutes, while a variety is said to be congruence permutable if every one of its members is congruence permutable. The following theorem, due to Maltsev, first provides the link between the structural and sementic sides of the subject.

Definition 2.1.1. *A* Maltsev operation *on a set A is a ternary operation $q(x, y, z)$ satisfying*

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

Theorem 2.1.1. $(Maltsev)$ *Let $\mathcal{V}$ be a variety of algebras. The following are equivalent:*

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

(2) $F_{\mathcal{V}}(3)$ *is* congruence permutable*.*

(3) $\mathcal{V}$ *has a Maltsev term. That is, a ternary term q such that $\mathcal{V}$ satisfies*

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

Proof. (1) $\Rightarrow$ (2). (1) implies (2) a fortiori.

(2) $\Rightarrow$ (3). Let $\mathbf{F} = \mathbf{F}_{\mathcal{V}}(x, y, z)$ and define $\alpha = Cg^{\mathbf{F}}(x, y)$ and $\beta = Cg^{\mathbf{F}}(y, z)$. Then $(x, z) \in \alpha \circ \beta$. Applying (2) we obtain $(x, z) \in \beta \circ \alpha$ which means that there is $u \in F$ such that $(x, u) \in \beta$ and $(u, z) \in \alpha$. Since $\mathbf{F}$ is generated by $\{x, y, z\}$, there is a term q such that $u = q^{\mathbf{F}}(x, y, z)$.

Let A be an arbitrary member of $\mathcal{V}$ and $a, b \in A$. By the freeness of $\mathbf{F}$, there is a homomorphism g: $\mathbf{F} \to \mathbf{A}$ such that $g(x) = g(y) = a$ and $g(z) = b$. Then $(x, y) \in ker(g)$ from which it follows that $\alpha \subseteq ker(g)$. From above we have $(u, z) \in \alpha$. Hence

$$b = g(z) = g(u) = g(q^{\mathbf{F}}(x,y,z)) = q^{\mathbf{A}}(g(x), g(y), g(z)) = q^{\mathbf{A}}(a,a,b).$$

This demonstrates the satisfaction of one of the two identities in (3). The other is proved analogously.

(3) $\Rightarrow$ (1). Assume q is a term satisfying condition (3) and let $\mathbf{A}$ be a member of $\mathcal{V}$, α and β congruences on $\mathbf{A}$, and assume that $(a,b) \in \alpha \circ \beta$. We shall show $(a,b) \in \beta \circ \alpha$ which is enough to prove condition (1).

Since $(a,b) \in \alpha \circ \beta$, there is an element $c \in A$ such that $(a,c) \in \alpha$ and$(c,b) \in \beta$. Then using condition(3),

$$(a = q^{\mathbf{A}}(a,b,b), q^{\mathbf{A}}(a,c,b)) \in \beta, (q^{\mathbf{A}}(a,c,b), q^{\mathbf{A}}(a,a,b) = b) \in \alpha,$$

Therefore $(a,b) \in \beta \circ \alpha$. □

The above result is very useful and has a great impact on universal algebra. Congruence permutable varieties are often called Maltsev varieties, and a term satisfying condition(3) is generally called a Maltsev term. We know many examples of Maltsev varities. The following are some examples.

Example 2.1.1. *For example, groups $\langle G, \cdot, ^{-1}, e\rangle$ are congruence permutable, for let*

$$q(x,y,z) \approx x \cdot y^{-1} \cdot z.$$

Example 2.1.2. *Rings $\langle R, +, \cdot, -, 0\rangle$ are congruence permutable, for let*

$$q(x,y,z) \approx x - y + z.$$

Example 2.1.3. *Quasigroups $\langle Q, \cdot, /, \backslash\rangle$ are congruence permutable, for let*

$$q(x,y,z) \approx (x/(y\backslash y)) \cdot (y\backslash z).$$

Theorem 2.1.2. ([*1*]) *Let $\mathcal{V}$ be a congruence permutable variety and $\boldsymbol{A} \in \mathcal{V}$.*

(1) *Every reflexive subalgebra of $\boldsymbol{A}^2$ is a congruence on $\boldsymbol{A}$.*

(2) *Let $\theta \subseteq A^2$ and $a, b \in A$. The following are equivalent:*

   (*a*) $(a,b) \in Cg^A(\theta)$;

   (*b*) *There are $(\boldsymbol{u}, \boldsymbol{v}) \in \theta$, $\boldsymbol{w} \in A^m$ and $t \in Clo_{n+m}(\boldsymbol{A})$ such that $a = t(\boldsymbol{u}, \boldsymbol{w})$ and $b = t(\boldsymbol{v}, \boldsymbol{w})$;*

   (*c*) *There are $(\boldsymbol{u}, \boldsymbol{v}) \in \theta$ and $p \in Pol_n(\boldsymbol{A})$ such that $a = p(\boldsymbol{u})$ and $b = p(\boldsymbol{v})$.*

Then we move to congruence n-permutable varieties for some n. Some experts have characterized such a variety in a very nice way, such as using congruences, identities, orderable algebras. Let us look at it.

Definition 2.1.2. *Let $\mathcal{V}$ be a variety of algebras and n an integer, $n > 1$.*
A variety $\mathcal{V}$ is congruence n-permutable *if for every $\boldsymbol{A} \in \mathcal{V}$ and for every pair of congruences α and β in $Con(\boldsymbol{A})$,*

$$\alpha \circ_n \beta = \beta \circ_n \alpha$$

where $\alpha \circ_n \beta = \alpha \circ \beta \circ \alpha \circ \beta \cdots$ is the n-fold relational product, there are n-1 occurances of $\circ$ on the right side of equation.

Specially, if n=2, we say that the variety $\mathcal{V}$ is congruence permutable, and a congruence permutable variety is also called a Maltsev variety.

In 1973, Hagemann and Mitschke provided the following classical characterization of congruence n-permutable varieties with several identities and this result is widely used in many ways. Later, Hagemann characterized such a variety using orderable algebras.

Theorem 2.1.3. ([7]) *Fix $n > 1$, n an integer. Let $\mathcal{V}$ be a variety of algebras. $\mathcal{V}$ is congruence n-permutable if and only if there exist ternary terms $p_1, p_2, \ldots, p_{n-1}$ such that the following identities hold:*

$$p_1(x, y, y) \approx x,$$

$$p_i(x, x, y) \approx p_{i+1}(x, y, y) \textit{ for } 1 \le i \le n-2,$$

$$p_{n-1}(x, x, y) \approx y\ .$$

Example 2.1.4. ($Mitschke$) *The variety of implication algebras has a single binary operation symbol, $\rightarrow$, and is defined by the equations:*

$$(x \rightarrow y) \rightarrow x \approx x,$$

$$(x \rightarrow y) \rightarrow y \approx (y \rightarrow x) \rightarrow x,$$

$$x \rightarrow (y \rightarrow z) \approx y \rightarrow (x \rightarrow z).$$

This variety is congruence 3-permutable, since we have two ternary terms $p_1(x,y,z) \approx (z \to y) \to x$ *and* $p_2(x,y,z) \approx (x \to y) \to z$ *satisfying the equations in Hagemann and Mitschke's theorem, i.e.,*

$$p_1(x,y,y) \approx (y \to y) \to x \approx (x \to x) \to x \approx x,$$
$$p_2(x,x,y) \approx (x \to x) \to y \approx (y \to y) \to y,$$
$$p_1(x,x,y) \approx (y \to x) \to x \approx (x \to y) \to y \approx p_2(x,y,y).$$

But it is not congruence permutable, since we can find two congruence α *and* β *such that* $\alpha \circ \beta \approx \beta \circ \alpha$.

Let $\boldsymbol{D}$ *be a 2-element implication algebra,* $D = \{0,1\}$, *defined by the equations*

$$0 \to 0 \approx 0 \to 1 \approx 1 \to 1 \approx 1$$
$$1 \to 0 \approx 0.$$

Then $A = \{(0,1),(1,0),(1,1)\}$ *is a subuniverse of* $\boldsymbol{D}^2$.

Define $\alpha_1, \alpha_2 \in \boldsymbol{Con}(A)$ *by* $((x_1,x_2),(y_1,y_2)) \in \alpha_i \iff x_i = y_i$, *for* $i = 1,2$.

We can tell that $((0,1),(1,0)) \in \alpha_2 \circ \alpha_1$ *and* $((0,1),(1,0)) \notin \alpha_1 \circ \alpha_2$.

Theorem 2.1.4. (*Hagemann*) *A variety* $\mathcal{V}$ *does not contain an orderable algebra if and only if it is congruence* n*-permutable for some* $n > 1$.

That means, a variety contains an orderable algebra if and only if it is not congruence n-permutable for any $n > 1$.

Example 2.1.5. *The variety of semilattices is not congruence* n*-permutable for any* n *since every semilattice is an orderable algebra.*

We are partly inspired by the following lemma to construct the equivalent conditions for congruence n-permutable variety.

Lemma 2.1.1. ([*12*]) *Let* $\mathcal{V}$ *be an idempotent variety that is not congruence permutable. If* $\boldsymbol{F} = \boldsymbol{F}_{\mathcal{V}}(x,y)$ *is the 2-generated free algebra in* $\mathcal{V}$, *then* $\boldsymbol{F}$ *has subuniverses* U *and* V *such that*

(1) $x \in U, y \in V$,

(2) $y \notin U, x \notin V$,

(3) $(U \times F) \cup (F \times V)$ *is a subuniverse of* $\boldsymbol{F} \times \boldsymbol{F}$.

The other direction also holds. The following is the proof for the other direction.

Proof. Assume $\mathcal{V}$ is congruence permutable.

By theorem 2.1.3, there exists a ternary term p_1 such that the following identities hold:

$$p_1(x, y, y) \approx x,\ p_1(x, x, y) \approx y.$$

We know that $(U \times F) \cup (F \times V)$ is a subuniverse of $\mathbf{F} \times \mathbf{F}$, then

$$(y, x) = (p_1(x, x, y), p_1(x, y, y)) \in (U \times F) \cup (F \times V).$$

But we have $y \notin U$ and $x \notin V$, there is a contradiction. □

Definition 2.1.3. *For $k \geq 2$, a k-*edge operation *on a set A is a $(k+1)$-ary operation f on A satisfying the k identities:*

$$f(x, x, y, y, y, \cdots, y, y) \approx y$$
$$f(x, y, x, y, y, \cdots, y, y) \approx y$$
$$f(y, y, y, x, y, \cdots, y, y) \approx y$$
$$f(y, y, y, y, x, \cdots, y, y) \approx y$$
$$\cdots$$
$$f(y, y, y, y, y, \cdots, x, y) \approx y$$
$$f(y, y, y, y, y, \cdots, y, x) \approx y$$

We often characterize algebras by the operations they possess and the identities that they satisfy. The most beautiful and striking results in the subject provide bridges between the structural and the semantic.

Let A be a set. For every positive natural number n, let $Op_n(A)$ denote the set of all n-ary operations on A. Let $Op(A) = \cup_{n \in \mathbb{N}} Op_n(A)$ be the set of all operations on A. For any $k \leq n$, there is an n-ary operation $p_k^n(x_1, \cdots, x_n) = x_k$, called the k-th projection operation.

Let n and k be natural numbers, and suppose that $f \in Op_n(A)$ and $g_1, \cdots, g_n \in Op_k(A)$. Then we define a new k-ary operation $f[g_1, \cdots, g_n]$ by

$$(x_1, x_2, \cdots, x_k) \mapsto f(g_1(x_1, x_2, \cdots, x_k), \cdots, g_n(x_1, x_2, \cdots, x_k))$$

called the generalized composite of f with $g_1, \cdots, g_n$. Note that, unlike the ordinary composition of unary operation, the generalized composite only exists when all of the ranks match up correctly.

Just as the set of unary operations forms a monoid under the operation of composition, we can form a kind of algebraic structure whose elements are members of $Op(A)$ with the operation of generalized composition.

Definition 2.1.4. *Let A be a nonempty set. A* clone *on A is a subset of $Op(A)$ that contains all projection operations and is closed under generalized composition.*

Example 2.1.6. *Here are some examples of clones:*

(1) *$Op(A)$ and $Proj(A) = \{p_k^n : 1 \leq k \leq n\}$ are clones on any set A.*

(2) *The set of $\mathbb{Z}$-linear functions on $\mathbb{Q}$, i.e., the set of all operations of the form $f(x_1, \cdots, x_n) = a_1x_1 + \cdots + a_nx_n$ with $a_i \in \mathbb{Z}$ forms a clone on $\mathbb{Q}$. Similarly, the set of $\mathbb{Z}$-affine functions on $\mathbb{Q}$ forms a clone. $f(x_1, \cdots, x_n)$ is affine if it is of the form $a_1x_1 + \cdots + a_nx_n + b$ for $a_1, \cdots, a_n \in \mathbb{Z}$ and $b \in \mathbb{Q}$.*

(3) *The set of all idempotent operations on A is a clone. Recall that an operation f is idempotent if $f(x, x, \cdots, x) = x$ for all x.*

(4) *Let $\langle P, \leq \rangle$ be a poset. The set of all isotone operations is a clone on P. An operation f is isotone if $x_i \leq y_i$ for $i \leq n$ implies $f(x_1, x_2, \cdots, x_n) \leq f(y_1, y_2, \cdots, y_n)$.*

Let A be a fixed set. The collection of clones on A is ordered by inclusion, and is closed under arbitrary intersection. Therefore, it forms a complete lattice. The smallest and largest elements of this lattice are $Proj(A)$ and $Op(A)$ respectively. There is an associated closure operator, Clo^A. In other words, for any set $F \subseteq Op(A)$, $Clo^A(F)$ is the smallest clone on A containing F.

For any natural number n, the set of n-ary members of a clone C will be denoted $C_{(n)}$. Similarly the set of n-ary members of $Clo(F)$ is denoted $Clo_n(F)$.

Theorem 2.1.5. ([*1*]) *Let A be a set and F a set of operations on A. Define*

$$F_0 = Proj(A),$$

$$F_{n+1} = F_n \cup \{f[g_1, \cdots, g_k] : f \in F, k = rank(f) \quad and$$
$$g_1, \cdots, g_k \in F_n \cap Op_m(A),\ some\ m \in \mathbb{N}\},\ for\ n \in \mathbb{N}.$$

Then $Clo^A(F) = \cup_{n \in \mathbb{N}} F_n$.

Corollary 2.1.1. ([*1*]) *Let* A *be a set and* F *a set of operations on* A*. For any natural number* m*, define*

$$G_0 = \{p_1^m, p_2^m, \cdots, p_m^m\},$$
$$G_{n+1} = G_n \cup \{f[g_1, \cdots, g_k] : f \in F, g_1, \cdots, g_k \in G_n\},\ for\ n \in \mathbb{N}.$$

Then $Clo_m(F) = \cup_{n \in \mathbb{N}} G_n$.

Example 2.1.7. *As an example, let* F *consist of the operations of addition, negation, multiplication and 1(a nullary operation) on the set* $\mathbb{Q}$ *of rational numbers. What are the members of* $Clo_2^{\mathbb{Q}}(F)$*? The set* G_0 *consists of the two projection operations, which we can abbreviate to* $\{x, y\}$*. At level one, we apply each of the members of* F *to* G_0 *obtaining*

$$G_1 = \{x + x, x + y, y + y, -x, -y, x \cdot x, x \cdot y, y \cdot y, 1\}$$
$$= \{2x, x + y, 2y, -x, -y, x^2, xy, y^2, 1\}.$$

Then 1 *in the above set is the binary constant operation with value* 1*.* G_2 *is constructed from* G_1 *in the same way. There are already too many functions to list, but among them are* $3x, x^3, 2x + y, x^2 + 2y, y + 1$*, etc. Note that we will obtain the binary constant operations 0 and 2. Proceeding like this, we can construct integer powers and integer multiples of* x *and* y*, together with their sums and products. In other words*

$$Clo_2^{\mathbb{Q}}(F) = \mathbb{Z}[x, y].$$

Of course, a set A together with a family F of operations is actually an algebra. This motivates the next definition.

Definition 2.1.5. *Let* $\boldsymbol{A} = \langle A, F \rangle$ *be an algebra. The clone of* term operations *on* $\boldsymbol{A}$ *is* $Clo^A(F)$*, which we denote* $Clo(\boldsymbol{A})$*. The clone of* polynomial operations *on* $\boldsymbol{A}$*,* $Pol(\boldsymbol{A})$ *is the clone on* A *generated by* $F \cup Op_0(A)$*.*

We have the theorems for constructing the term operations from the basic operations. The same theorem is also used to construct the polynomial operations. Here is an alternate description of the polynomial clone obtained directly from the terms.

Theorem 2.1.6. ([1]) *Let $\boldsymbol{A}$ be an algebra and let n be a natural number. An operation g is in $Pol_n(\boldsymbol{A})$ if and only if for some $m \in \mathbb{N}$, $f \in Clo_{n+m}(\boldsymbol{A})$ and $a_1, \cdots, a_n \in A$,*

$$g(x_1, \cdots, x_n) = f(x_1, \cdots, x_n, a_1, \cdots, a_m).$$

2.2 Congruence Distributive and Modular Varieties

We turn to congruence distributive varieties. Recall that the variety is called congruence distributive if every member has a distributive congruence lattice. We will give a theorem that is similar in favor to characterization of congruence permutable varieties.

Theorem 2.2.1. *(Jónsson) Let $\mathcal{V}$ be a variety of algebras. The following are equivalent:*

(1) $\mathcal{V}$ *is* congruence distributive*.*

(2) $\boldsymbol{F}_{\mathcal{V}}(3)$ *is* congruence distributive.

(3) *There is a positive integer n and ternary terms $p_0, p_1, \cdots, p_n$ such that $\mathcal{V}$ satisfies the following identities:*

$$p_i(x, y, x) \approx x, \text{ for } 0 \leq i \leq n,$$
$$p_0(x, y, z) \approx x,$$
$$p_n(x, y, z) \approx z,$$
$$p_i(x, x, y) \approx p_{i+1}(x, x, y), \text{ for } i \text{ even},$$
$$p_i(x, y, y) \approx p_{i+1}(x, y, y), \text{ for } i \text{ odd}.$$

Proof. (1) $\Longrightarrow$ (2) is immediate.

(2) $\Longrightarrow$ (3). Let $\mathbf{F}$ denote the free algebra on $\{x, y, z\}$ and define

$$\alpha = Cg^{\mathbf{F}}(x, y), \beta = Cg^{\mathbf{F}}(y, z), \gamma = Cg^{\mathbf{F}}(x, z).$$

By congruence-distributivity $(\alpha \vee \beta) \wedge \gamma = (\alpha \wedge \gamma) \vee (\beta \wedge \gamma)$. Since (x, z) clearly lies in the left hand side of this equation, it lies in the right hand side as well. Therefore, there are elements

$u_0, u_1, \cdots, u_n \in F$ such that $x = u_0(\alpha \wedge \gamma)u_1(\beta \wedge \gamma)u_2(\alpha \wedge \gamma)u_3 \cdots (\beta \wedge \gamma)u_n = z$. Since $\mathbf{F}$ is generated by $\{x, y, z\}$, there are terms p_i for $i = 0, \cdots, n$ such that $u_i = p_i^{\mathbf{F}}(x, y, z)$.

Now to verify that the identities of condition (3) hold in $\mathcal{V}$, let $\mathbf{A} \in \mathcal{V}$ and $a, b, c \in A$. By the freeness of $\mathbf{F}$, there are homomorphisms $f, g, h : \mathbf{F} \to \mathbf{A}$ such that

$$f(x) = f(y) = a, f(z) = b$$
$$g(y) = g(z) = b, g(x) = a$$
$$h(x) = h(z) = a, h(y) = b.$$

Note that

$$ker(f) \supseteq \alpha \supseteq \alpha \wedge \gamma$$
$$ker(g) \supseteq \beta \supseteq \beta \wedge \gamma$$
$$ker(h) \supseteq \gamma \supseteq \alpha \wedge \gamma, \beta \wedge \gamma.$$

For every $i \leq n$, $h(u_i) = h(p_i^{\mathbf{F}}(x, y, z)) = p_i^{\mathbf{A}}(a, b, a)$. Applying h to the expressions in the above,

$$h(x) = h(u_0) = h(u_1) = h(u_2) = \cdots = h(u_n) = h(z)$$

i.e., $a = p_0^{\mathbf{A}}(a, b, a) = p_1^{\mathbf{A}}(a, b, a) = \cdots = p_n^{\mathbf{A}}(a, b, a)$. The fact that $x = u_0$ and $z = u_n$ gives us two equations. For the other two equations, let i be an even index. Then $u_i(\alpha \wedge \gamma)u_{i+1}$. Applying f and using $p_i^{\mathbf{A}}(f(x), f(y), f(z)) = p_{i+1}^{\mathbf{A}}(f(x), f(y), f(z))$, i.e., $p_i^{\mathbf{A}}(a, a, b) = p_{i+1}^{\mathbf{A}}(a, a, b)$. A similar argument works for the odd indices.

(3) $\Longrightarrow$ (1). Assume that the identities in conditions (3) hold in $\mathcal{V}$, and let us prove that $\mathcal{V}$ is congruence distributive. Let $\mathbf{A} \in \mathcal{V}$ and $\alpha, \beta, \gamma \in Con(\mathbf{A})$. We wish to show that $(\alpha \vee \beta) \wedge \gamma \subseteq (\alpha \wedge \gamma) \vee (\beta \wedge \gamma)$. Call the right hand side ν and let $(a, b) \in (\alpha \vee \beta) \wedge \gamma$.

Then $(a, b) \in \gamma$ and there are elements $c_0, c_1, \cdots, c_k$ in A such that $a = c_0 \alpha c_1 \beta c_2 \alpha \cdots \beta c_k = b$. Now let $i \leq n$ and $j \leq k$. We have $(p_i(a, c_j, b), p_i(a, c_j, a) = a) \in \gamma$ and $(b, a) \in \gamma$, therefore $(p_i(a, c_j, b), p_i(a, c_{j+1}, b)) \in \gamma$ for all $j < k$. Also $(p_i(a, c_0, b), p_i(a, c_1, b)) \in \alpha$ and $(p_i(a, c_1, b), p_i(a, c_2, b)) \in \beta \cdots$. Combining these two observations

$$(p_i(a, c_j, b), p_i(a, c_{j+1}, b)) \in \nu, \text{ for } j < k.$$

We claim that for all $i < n$,

$$(p_i(a,a,b), p_i(a,b,b)) \in \nu, \ (p_i(a,b,b), p_{i+1}(a,b,b)) \in \nu.$$

To see the first of these observe that

$$p_i(a,a,b) = p_i(a,c_0,b)\nu p_i(a,c_1,b)\nu \cdots \nu p_i(a,c_k,b) = p_i(a,b,b).$$

For the second,

$$p_i(a,b,b) = p_{i+1}(a,b,b) \text{ for i odd,}$$

$$p_i(a,b,b)\nu p_i(a,a,b) = p_{i+1}(a,a,b)\nu p_{i+1}(a,b,b) \text{ for i even.}$$

Using the two relationships we obtain $a = p_0(a,b,b)\nu p_1(a,b,b)\nu p_2(a,b,b) \cdots \nu p_n(a,b,b) = b$ as desired. □

The terms in the theorem are usually called Jónsson terms. Notice that if $n = 1$ in the above theorem, then in $\mathcal{V}$,

$$x \approx p_0(x,x,y) \approx p_1(x,x,y) \approx y,$$

thus $\mathcal{V}$ is a trivial variety.

The most important case is $n = 2$. This is equivalent to the identities

$$p_1(x,x,y) \approx p_1(x,y,x) \approx p_1(y,x,x) \approx x.$$

Such a term p_1 is called a majority term. In the variety of lattices, the term $m(x,y,z) = (x \wedge y) \vee (x \wedge z) \vee (y \wedge z)$ and its dual both behave as majority terms.

Corollary 2.2.1. ([*1*]) *If a variety admits a majority term, then it is congruence distributive.*

Theorem 2.2.2. (*Alan Day*) *Let $\mathcal{V}$ be a variety of algebras. The following are equivalent:*

(1) $\mathcal{V}$ *is* congruence modular.

(2) $\boldsymbol{F}_{\mathcal{V}}(4)$ *is* congruence modular.

(3) *There is a positive integer n and quatenary terms $p_0, p_1, \cdots, p_n$ such that $\mathcal{V}$ satisfies the following identities:*

$$p_i(x,y,y,x) \approx x, \textit{ for } 0 \leq i \leq n,$$

$$p_0(x,y,z,u) \approx x,$$

$$p_n(x,y,z,u) \approx u,$$

$$p_i(x,x,y,y) \approx p_{i+1}(x,x,y,y), \textit{ for } i \textit{ even},$$

$$p_i(x,y,y,z) \approx p_{i+1}(x,y,y,z), \textit{ for } i \textit{ odd}.$$

The followings are another equivalent conditions for congruence modular.

Theorem 2.2.3. ([3]) *Let $\mathcal{V}$ be a variety of algebras. The following are equivalent:*

(1) $\mathcal{V}$ *is* congruence modular.

(2) *There is a positive integer n and ternary terms $p_0, p_1, \cdots, p_n$ and p such that $\mathcal{V}$ satisfies the following identities:*

$$p_0(x,z,y) \approx x,$$

$$p_i(x,y,x) \approx x, \textit{ for } 2 \leq i \leq n\ ,$$

$$p_i(x,y,y) \approx p_{i+1}(x,y,y), \textit{ for } i \textit{ even},$$

$$p_i(x,x,y) \approx p_{i+1}(x,x,y), \textit{ for } i \textit{ odd},$$

$$p_n(x,y,y) \approx p(x,y,y),$$

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

Lemma 2.2.1. ([3]) *Let $\boldsymbol{A}$ be an algebra and suppose $\theta_1, \theta_2 \in Con(\boldsymbol{A})$. Then the following are equivalent:*

(1) $\theta_1 \circ \theta_2 = \theta_2 \circ \theta_1$,

(2) $\theta_1 \vee \theta_2 = \theta_1 \circ \theta_2$,

(3) $\theta_1 \circ \theta_2 \subseteq \theta_2 \circ \theta_1$.

Theorem 2.2.4. *(Birkhoff) If $\boldsymbol{A}$ is congruence permutable, then $\boldsymbol{A}$ is congruence modular.*

Proof. Let $\theta_1, \theta_2, \theta_3 \in Con(\mathbf{A})$ with $\theta_1 \subseteq \theta_2$. We want to show that

$$\theta_2 \cap (\theta_1 \vee \theta_3) \subseteq \theta_1 \vee (\theta_2 \cap \theta_3).$$

Suppose $(a,b) \in \theta_2 \cap (\theta_1 \vee \theta_3)$, then there is an element c such that $(a,c) \in \theta_1$ and $(c,b) \in \theta_3$. We have $\theta_1 \circ \theta_2 = \theta_2 \circ \theta_1$ since $\mathbf{A}$ is congruence permutable. Using lemma 2.2.1, $\theta_1 \vee \theta_3 = \theta_1 \circ \theta_3$, by symmetry,

$$(c,a) \in \theta_1,$$

hence

$$(c, a) \in \theta_2,$$

then by transitivity,

$$(c, b) \in \theta_2.$$

Thus $(c, b) \in \theta_2 \cap \theta_3$, so from

$$(a, c) \in \theta_1 \text{ and } (c, b) \in \theta_2 \cap \theta_3,$$

we have

$$(a, b) \in \theta_1 \circ (\theta_2 \cap \theta_3),$$

hence

$$(a, b) \in \theta_1 \vee (\theta_2 \cap \theta_3).$$

□

We know that each of the conditions of congruence distributivity and congruence permutability is important in its own right. The combination of the two properties turns out to be particularly important.

Definition 2.2.1. *An algebra is called* arithmetical *if it is both congruence permutable and congruence distributive.*
A variety is arithmetical if every member is arithmetical.

Theorem 2.2.5. (*Pixley*) *Let $\mathcal{V}$ be a variety of algebras. The following are equivalent:*

(1) $\mathcal{V}$ *is* arithmetical.

(2) $\boldsymbol{F}_{\mathcal{V}}(3)$ *is* arithmetical.

(3) *There is a term $p(x, y, z)$ such that $\mathcal{V}$ satisfies the following identities:*

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

The term p in the above theorem is called a *Pixley term.*

Example 2.2.1. *Let us define an* r-lattice *to be an algebra $\langle L, \wedge, \vee, r\rangle$ of signature $\langle 2, 2, 3\rangle$ such that*

$$\langle L, \wedge, \vee \rangle \textit{ is a lattice,}$$

$$y \wedge r(x, y, z) \approx x \wedge y \wedge z,$$

$$y \vee r(x, y, z) \approx x \vee y \vee z.$$

The variety of r-lattices is arithmetical. For a Pixley term, we can take

$$p(x, y, z) \approx r(x, x \vee y, x \vee y \vee z) \wedge r(z, z \vee y, z \vee y \vee x).$$

For then

$$p(x, x, z) \approx r(x, x, x \vee z) \wedge r(z, z \vee x, z \vee x) \approx (x \vee z) \wedge z \approx z,$$

$$p(x, z, z) \approx r(x, x \vee z, x \vee z) \wedge r(z, z, z \vee x) \approx x \wedge (z \vee x) \approx x,$$

$$p(x, y, x) \approx r(x, x \vee y, x \vee y) \wedge r(x, x \vee y, x \vee y) \approx x \wedge x \approx x.$$

Example 2.2.2. *Every Boolean algebra can obviously be made into an r-lattice by defining*

$$r(x, y, z) \approx (y' \vee (x \wedge z)) \wedge (x \vee z),$$

Thus, Boolean algebras are arithmetical.

In the book [1], the variety generated by the six-element ortholattice in Figure 2.1 is arithmetical.

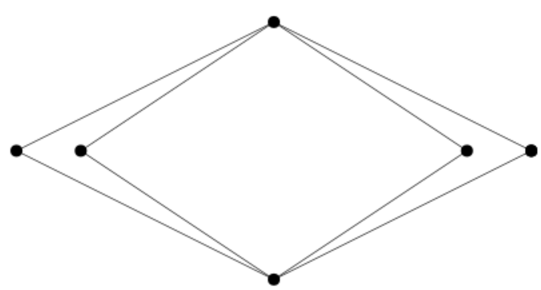

Figure 2.1 Six-element ortholattice

2.3 Main Theorem

Theorem 2.3.1. *Let $\mathcal{V}$ be an idempotent variety, $\boldsymbol{F} = \boldsymbol{F}_{\mathcal{V}}(x, y)$ is the 2-generated free algebra in $\mathcal{V}$. The following are equivalent:*

(1) *$\mathcal{V}$ has a finite orderable algebra.*

(2) *$\mathcal{V}$ has a 2-element orderable algebra.*

(3) *$\boldsymbol{F}$ has subuniverses U and V such that $x \in U$ and $y \in V$, $U \cap V = \phi$, and $(U \times F) \cup (F \times V)$ is a subuniverse of $\boldsymbol{F} \times \boldsymbol{F}$.*

Proof. (2) $\Rightarrow$ (1). It is obvious.

(1) $\Rightarrow$ (2). Suppose $\mathcal{V}$ contains a finite orderable algebra $\mathbf{A}$, that means $\mathbf{A}$ has a non-trivial compatible partial order on $\mathbf{A}$. Denote this partial order as " $\preceq$ ". Since $\mathbf{A}$ is finite, then we can find two elements a, b in A such that $a \preceq b$ and $\{x : a \preceq x \preceq b\} = \{a, b\}$. Define $I[a,b] = \{x : a \preceq x \preceq b\}$, then $I[a,b]$ is a subuniverse, since for any n-ary operation f, and $\forall x_1, x_2, \cdots, x_n \in I[a,b]$,

$$f(a, a, \cdots, a) \preceq f(x_1, x_2, \cdots, x_n) \preceq f(b, b, \cdots, b).$$

By the idempotency of f, $f(a, a, \cdots, a) = a$ and $f(b, b, \cdots, b) = b$, we have

$$a \preceq f(x_1, x_2, \cdots, x_n) \preceq b,$$

so $f(x_1, x_2, \cdots, x_n) \in I[a,b]$ by the definition of $I[a,b]$. Hence $I[a,b]$ is a 2-element orderable algebra.

(2) $\Rightarrow$ (3). Suppose $\mathcal{V}$ contains a 2-element orderable algebra $D = \{c, d\}$. Denote this partial order as " $\preceq$ ", $c \preceq d$. Define a mapping

$$h : F \to D = \{c, d\}$$

by $h(x) = c$ and $h(y) = d$.

Let

$$U = \{u \in F : h(u) = c\}$$

and

$$V = \{v \in F : h(v) = d\}$$

Notice that U and V are subuniverses of $\mathbf{F}$, for any n-ary operation f, and any $u_1, u_2, \cdots, u_n \in U$, $h(f(u_1, u_2, \cdots, u_n)) = f(h(u_1), h(u_2), \cdots, h(u_n)) = f(c, c, \cdots, c) = c$ since f is idempotent. Obviously, $x \in U$ and $y \in V$. Then we will show that

$$U \cup V = F \text{ and } U \cap V = \phi.$$

For any $t \in F$, $h(t) = c$ or $h(t) = d$, then $t \in U$ or $t \in V$, so $F \subseteq U \cup V$. If $t \in U \cap V$, then $h(t) = c$ and $h(t) = d$, it is not possible, so $U \cap V = \phi$.

Finally we will show that $(U \times F) \cup (F \times V)$ is a subuniverse of $\mathbf{F} \times \mathbf{F}$.

We know that

$$(U \times F) \cup (F \times V) = (U \times V) \cup (U \times U) \cup (V \times V),$$
$$D^2 = \{(c,c),(c,d),(d,c),(d,d)\}$$

from $U \cup V = F$ and $D = \{c, d\}$.

Consider the induced mapping from h,

$$h^2 : F^2 \to D^2,$$

by $h^2(a,b) = (h(a), h(b)), (a,b) \in F^2$.

We have

$$(h^2)^{-1}\{(c,c),(c,d),(d,d)\} = (U \times V) \cup (U \times U) \cup (V \times V) = (U \times F) \cup (F \times V).$$

Let $E = \{(c,c),(c,d),(d,d)\}$. Since the inverse of the subuniverse is a subuniverse, in order to prove $(U \times F) \cup (F \times V)$ is a subuniverse of $\mathbf{F}^2$, It suffices to show that $E = \{(c,c),(c,d),(d,d)\}$ is a subuniverse of $\mathbf{D}^2$.

Suppose t is an n-ary term on $\mathbf{F}^2$, $(x_1,y_1),(x_2,y_2),\cdots,(x_n,y_n) \in E$. Without loss of generality, assume $x_1 = \cdots = x_k = c$, $x_{k+1} = \cdots = x_n = d$, then $y_{k+1} = \cdots = y_n = d$ since (d,c) is not in E, so

$$\begin{aligned} & t((x_1,y_1),(x_2,y_2),\cdots,(x_n,y_n)) \\ &= (t(x_1,x_2,\cdots,x_n), t(y_1,y_2,\cdots,y_n)) \\ &= (t(c,\cdots,c,d,\cdots,d), t(y_1,\cdots,y_k,d,\cdots,d)). \end{aligned}$$

Assume $t(c,\cdots,c,d,\cdots,d) = d$ and $t(y_1,\cdots,y_k,d,\cdots,d) = c$, then

$$d = t(c,\cdots,c,d,\cdots,d) \preceq t(y_1,\cdots,y_k,d,\cdots,d) = c, \text{ since } c \preceq y_i.$$

That is a contradiction with $c \preceq d$. Hence $t((x_1, y_1), (x_2, y_2), \cdots, (x_n, y_n)) \in E$, and E is a subuniverse of $\mathbf{D}^2$.

(3) $\Rightarrow$ (2). Suppose we have such U and V in the third equivalent condition. Since (x, x) and (y, y) are both in $(U \times F) \cup (F \times V)$, and x, y are two generators of F, then for any $a \in F$, $(a, a) \in (U \times F) \cup (F \times V)$, we have

$$a \in U \text{ or } a \in V,$$

hence $F \subseteq U \cup V$.

Define $\theta = (U \times U) \cup (V \times V)$.

First we show that θ is an equivalence relation on F. For any $a \in F$, $a \in U$ or $a \in V$, then $(a, a) \in U \times U$ or $(a, a) \in V \times V$, so $(a, a) \in \theta$. If $(a, b) \in \theta$, then $(a, b) \in U \times U$ or $(a, b) \in V \times V$, from that we know $(b, a) \in U \times U$ or $(b, a) \in V \times V$, hence $(b, a) \in \theta$. If $(a, b) \in \theta$ and $(b, c) \in \theta$, then $(a, b) \in U \times U$ or $(a, b) \in V \times V$, $(b, c) \in U \times U$ or $(b, c) \in V \times V$. When $(a, b) \in U \times U$, then $b \in U$ and (b, c) must be in $U \times U$, so $(a, c) \in U \times U \subseteq \theta$; similary, when $(a, b) \in V \times V$, then $b \in V$ and (b, c) must be in $V \times V$, so $(a, c) \in V \times V \subseteq \theta$;

Next we prove that θ is a congruence on F. Let $S = (U \times F) \cup (F \times V) = (U \times V) \cup (U \times U) \cup (V \times V) = \theta \cup (U \times V)$. Suppose f is an n-ary operation on F, $\forall (a_1, b_1), (a_2, b_2), \cdots, (a_n, b_n) \in \theta \subseteq S$, since S is a subuniverse of $\mathbf{F}^2$, then

$$f((a_1, b_1), (a_2, b_2), \cdots, (a_n, b_n)) = (f(a_1, a_2, \cdots, a_n), f(b_1, b_2, \cdots, b_n)) \in S.$$

Assume $(f(a_1, a_2, \cdots, a_n), f(b_1, b_2, \cdots, b_n)) \in U \times V$, then

$$f((b_1, a_1), (b_2, a_2), \cdots, (b_n, a_n)) = (f(b_1, b_2, \cdots, b_n), f(a_1, a_2, \cdots, a_n)) \in V \times U \nsubseteq S.$$

But $f((b_1, a_1), (b_2, a_2), \cdots, (b_n, a_n)) \in S$ since $(b_1, a_1), \cdots, (b_n, a_n) \in \theta \subseteq S$. Hence the assumption is not correct, and $(f(a_1, \cdots, a_n), f(b_1, \cdots, b_n)) \in \theta$.

Consider quotient algebra $\mathbf{F}/\theta$, it has two elements U and V, define a partial order $\preceq$ by $U \preceq V$. Since S is a subuniverse of $\mathbf{F} \times \mathbf{F}$, then $\mathbf{F}/\theta$ is an orderable algebra.

□

Theorem 2.3.2. *Let $\mathcal{V}$ be an idempotent variety. Then $\mathcal{V}$ is not congruence n-permutable for any $n \in \mathbb{N}$ if and only if $\boldsymbol{F} = \boldsymbol{F}_{\mathcal{V}}(x, y)$ is the 2-generated free algebra in $\mathcal{V}$, and $\boldsymbol{F}$ has* *subuniverses U and V such that*

(1) $x \in U$ *and* $y \in V$,

(2) $U \cap V = \phi$,

(3) $(U \times F) \cup (F \times V)$ *is a subuniverse of* $\boldsymbol{F} \times \boldsymbol{F}$.

Proof. " $\Leftarrow$ " Assume $\mathcal{V}$ is congruence $(n+1)$-permutable for some n.

Then by theorem 2.1.3, there exist ternary terms $p_1, \cdots, p_n$ such that

$$p_1(x, y, y) \approx x,$$

$$p_i(x, x, y) \approx p_{i+1}(x, y, y) \text{ for } 1 \leq i \leq n-1,$$

$$p_n(x, x, y) \approx y\ .$$

From those three conditions for U and V, we know that $(x, x), (x, y), (y, y)$ are all in $(U \times F) \cup (F \times V)$, then we apply those n ternary terms to these three pairs,

$$p_n((x, x), (x, y), (y, y)) = (p_n(x, x, y), p_n(x, y, y)) \in (U \times F) \cup (F \times V),$$

$$p_{n-1}((x, x), (x, y), (y, y)) = (p_{n-1}(x, x, y), p_{n-1}(x, y, y)) \in (U \times F) \cup (F \times V),$$

$$\cdots$$

$$p_2((x, x), (x, y), (y, y)) = (p_2(x, x, y), p_2(x, y, y)) \in (U \times F) \cup (F \times V),$$

$$p_1((x, x), (x, y), (y, y)) = (p_1(x, x, y), p_1(x, y, y)) \in (U \times F) \cup (F \times V).$$

Since $p_n(x, x, y) \approx y$ and $y \notin U$, then $p_n(x, y, y) \in V$, that means $p_{n-1}(x, x, y) \in V$ from $p_n(x, y, y) = p_{n-1}(x, x, y)$. So $p_{n-1}(x, x, y) \notin U$ by $U \cap V = \phi$. Proceeding like this, we can get $p_1(x, x, y) \notin U$, then $p_1(x, y, y)$ must be in V, that says that $x \in V$ since $p_1(x, y, y) = x$. That is a contradiction, therefore the assumption is false. Therefore $\mathcal{V}$ is not congruence n-permutable for any $n > 1$.

" $\Rightarrow$ " Suppose $\mathcal{V}$ is not congruence n-permutable for any $n > 1$. Then by Valeriote and Willard's propostion 3.2[18], $\mathcal{V}$ contains an 2-element orderable algebra $\mathbf{A}$, which has a compatible non-trivial partial order on $\mathbf{A}$. By **Theorem 2.3.1**, we could have those subuniverses U and V of $\mathbf{F}$.

□

2.4 Main Results for Congruence 3-permutable Variety

We have generated some results for congruence 3-permutable variety, and try to use them to prove if the variety constructed in some way is congruence 3-permutable variety.

Lemma 2.4.1. *Let $\mathcal{V}$ be an idempotent variety, $\boldsymbol{F} = \boldsymbol{F}_{\mathcal{V}}(x, y)$ is the 2-generated free algebra in $\mathcal{V}$ and $S_0 = Sg^{\boldsymbol{F}^2}\{(x, x), (x, y), (y, y)\}$. $\mathcal{V}$ is congruence 3-permutable if and only if $(y, x) \in S_0 \circ S_0$.*

Proof. " $\Rightarrow$ " Suppose $\mathcal{V}$ is congruence 3-permutable.

By Hagemann and Mitschke's theorem, there exist two ternary terms p_1, p_2 of $\mathcal{V}$ such that

$$p_1(x, y, y) \approx x,$$
$$p_1(x, x, y) \approx p_2(x, y, y),$$
$$p_2(x, x, y) \approx y$$

Since S_0 is a subuniverse,

$$(y, p_2(x, y, y)) \approx (p_2(x, x, y), p_2(x, y, y)) \approx p_2((x, x), (x, y), (y, y)) \in S_0,$$
$$(p_1(x, x, y), x) \approx (p_1(x, x, y), p_1(x, y, y)) \approx p_1((x, x), (x, y), (y, y)) \in S_0.$$

Therefore $(y, x) \in S_0 \circ S_0$ since $p_1(x, x, y) \approx p_2(x, y, y)$.

" $\Leftarrow$ " Suppose $(y, x) \in S_0 \circ S_0$,

then $\exists$ z such that $(y, z) \in S_0$ and $(z, x) \in S_0$.

By the definition of S_0, there exist two terms, say p_1, p_2, such that

$$(y, z) = p_2((x, x), (x, y), (y, y)) = (p_2(x, x, y), p_2(x, y, y)),$$
$$(z, x) = p_1((x, x), (x, y), (y, y)) = (p_1(x, x, y), p_1(x, y, y)).$$

hence

$$y = p_2(x, x, y),$$
$$z = p_2(x, y, y) = p_1(x, x, y),$$
$$x = p_1(x, y, y).$$

By Lemma 4.37 ([1]) and Hagemann and Mitschke's theorem, therefore $\mathcal{V}$ is congruence 3-permutable. □

Lemma 2.4.2. *Let $\mathcal{V}$ be an idempotent variety, $\boldsymbol{F} = \boldsymbol{F}_{\mathcal{V}}(x, y)$ is the 2-generated free algebra in $\mathcal{V}$, and $S_0 = Sg^{\boldsymbol{F}^2}\{(x, y), (x, x), (y, y)\}$. $(y, x) \notin S_0 \circ S_0$ if and only if $F_1 \cap F_2 = \phi$ where $F_1 = \{a : (a, x) \in S_0\}$ and $F_2 = \{b : (y, b) \in S_0\}$, both are subuniverses of $\boldsymbol{F}$.*

Proof. $(y, x) \notin S_0 \circ S_0$ is equivalent to say that for any element $s \in F$, $(y, s) \notin S_0$ or $(s, x) \notin S_0$, which is equivalent to $F_1 \cap F_2 = \phi$, where F_1 and F_2 are defined in the lemma. F_1 and F_2 are subuniverses of **F** since $\mathcal{V}$ is idempotent.

□

For the following lemma, we only prove one direction, actually we are more interesting in the other direction. That is one future direction I will focus on.

Lemma 2.4.3. *Let $\mathcal{V}$ be an idempotent variety. $\boldsymbol{F} = \boldsymbol{F}_{\mathcal{V}}(x, y)$ is the 2-generated free algebra in $\mathcal{V}$, and $\boldsymbol{F}$ has subuniverses U_1, U_2 and V_1, V_2 such that*

(1) $x \in U_1 \cap U_2, \quad y \in V_1 \cap V_2$,

(2) $U_1 \cap U_2 \cap V_1 \cap V_2 = \phi$,

(3) $(U_i \times F) \cup (F \times V_i)$ *is a subuniverse of* $\boldsymbol{F} \times \boldsymbol{F}$, *for* $i = 1, 2$.

Then $\mathcal{V}$ is not congruence 3-permutable.

Proof. Assume $\mathcal{V}$ is congruence 3-permutable.

By Hagemann and Mitschke's theorem, there exist two ternary terms p_1, p_2 of $\mathcal{V}$ such that

$$p_1(x, y, y) \approx x,$$
$$p_1(x, x, y) \approx p_2(x, y, y),$$
$$p_2(x, x, y) \approx y.$$

Notice that $(x, x), (x, y), (y, y)$ are all in $(U_i \times F) \cup (F \times V_i)$ for each $i = 1, 2$.

So

$$(y, p_2(x, y, y)) \approx (p_2(x, x, y), p_2(x, y, y)) \in (U_i \times F) \cup (F \times V_i) \text{ for } i = 1, 2,$$
$$(p_1(x, x, y), x) \approx (p_1(x, x, y), p_1(x, y, y)) \in (U_i \times F) \cup (F \times V_i) \text{ for } i = 1, 2.$$

By $y \notin U_i$ and $x \notin V_i$, we have $p_2(x, y, y) \in V_i$ and $p_1(x, x, y) \in U_i$ for $i = 1, 2$, Since $p_1(x, x, y) \approx p_2(x, y, y)$, we obtain

$$p_1(x,x,y) \in U_1 \cap U_2 \cap V_1 \cap V_2.$$

That is a contradiction with $U_1 \cap U_2 \cap V_1 \cap V_2 = \phi$. Therefore $\mathcal{V}$ is not congruence 3-permutable.

□

Lemma 2.4.4. *Let $\mathcal{V}$ be an idempotent variety, and assume $\mathcal{V}$ is not congruence 3-permutable. Let $\boldsymbol{F} = \boldsymbol{F}_{\mathcal{V}}(x,y)$ be the 2-generated free algebra in $\mathcal{V}$. Then there are two subuniverses F_1 and F_2 of $\boldsymbol{F}$ such that $x \in F_1$, $y \in F_2$ and $F_1 \cap F_2 = \phi$. Moreover $\boldsymbol{F}$ has subuniverses U_1, U_2 and V_1, V_2 such that*

(1) $F_1 \subseteq U_1 \cap U_2, \quad F_2 \subseteq V_1 \cap V_2,$

(2) $(U_i \times F) \cup (F \times V_i)$ *is a subuniverse of $\boldsymbol{F} \times \boldsymbol{F}$, for $i = 1, 2$.*

More specifically, $F_1 = \{a : (a,x) \in S_0\}$ and $F_2 = \{b : (y,b) \in S_0\}$ where $S_0 = Sg^{\boldsymbol{F}^2}\{(x,x),(x,y),(y,y)\}$.

Proof. Suppose $\mathcal{V}$ is not congruence 3-permutable.

By lemma 2.4.1, $(y,x) \notin S_0 \circ S_0$ where $S_0 = Sg^{\mathbf{F}^2}\{(x,y),(x,x),(y,y)\}$. It is equivalent to say that

$$\forall\ z \in F,\ (y,z) \notin S_0 \text{ or } (z,x) \notin S_0.$$

Define

$$F_1 = \{a \in F : (a,x) \in S_0\}, F_2 = \{b \in F : (y,b) \in S_0\}.$$

Obviously, F_1 and F_2 are two subuniverses of $\mathbf{F}$ since $\mathcal{V}$ is idempotent.

Then, we will show that

$$S_0 = Sg^{\mathbf{F}^2}\{F_1 \times F \cup F \times F_2\}.$$

From the definitions of F_1 and F_2, we have $F_1 \times \{x\} \subseteq S_0$ and $\{y\} \times F_2 \subseteq S_0$. Besides $F_1 \times \{y\} \subseteq F \times \{y\} \subseteq S_0$ and $\{x\} \times F_2 \subseteq \{x\} \times F \subseteq S_0$, so we obtain that

$$F_1 \times F \subseteq S_0, \quad F \times F_2 \subseteq S_0.$$

Hence, $Sg^{\mathbf{F}^2}\{F_1 \times F \cup F \times F_2\} \subseteq S_0$. The other direction is obvious.

Extend F_1 to a subuniverse U_1 of $\mathbf{F}$ satisfying that U_1 is maximal such that $(y,x) \notin Sg^{\mathbf{F}^2}\{U_1 \times F \cup F \times F_2\} = S_1$ by Zorn's lemma. Define

$$V_1 = \overrightarrow{P_2}(S_1 \cap \{y\} \times F).$$

$x \in F_1 \subseteq U_1$, $y \in V_1$ since $(y, y) \in S_1$. We will show that

$$(U_1 \times F) \cup (F \times V_1) = S_1.$$

From the definition of V_1, for any $v \in V_1$, $(y, v) \in S_1$. And $(x, v) \in S_1$, so $F \times V_1 \subseteq S_1$, obviously $U_1 \times F \subseteq S_1$, hence $(U_1 \times F) \cup (F \times V_1) \subseteq S_1$.

Take $(p, q) \in S_1 \backslash (U_1 \times F)$. Then $p \notin U_1$. Define $U_1' = Sg^{\mathbf{F}^2}(U_1 \cup \{p\})$. The maximality of U_1 implies that $(y, x) \in Sg^{\mathbf{F}^2}\{U_1' \times F \cup F \times F_2\}$.

We claim that

$$\begin{aligned} & Sg^{\mathbf{F}^2}\{U_1' \times F \cup F \times F_2\} \\ &= Sg^{\mathbf{F}^2}\{U_1' \times F \cup \{y\} \times F_2\} \\ &= Sg^{\mathbf{F}^2}\{U_1' \times F \cup \{y\} \times \{y\}\} \\ &= Sg^{\mathbf{F}^2}\{U_1 \times \{x\} \cup \{(p, x), (x, y), (y, y)\}\}. \end{aligned}$$

Then $\exists$ a term t and $u_1, \cdots, u_k \in U_1$ such that

$$(y, x) = t((u_1, x), \cdots, (u_k, x), (p, x), (x, y), (y, y)).$$

so $y = t(u_1, \cdots, u_k, p, x, y)$ and $x = t(x, \cdots, x, x, y, y)$. We can find a homomorphism f mapping x to q and mapping y to y since $\mathbf{F}$ is free. Then apply f to the equation $x = t(x, \cdots, x, x, y, y)$, we have $q = t(q, \cdots, q, q, y, y)$. Then

$$(y, q) = t((u_1, q), \cdots, (u_k, q), (p, q), (x, y), (y, y)) \in S_1 \cap \{y\} \times F,$$

so $q \in V_1$, $(p, q) \in F \times V_1$, $S_1 \subseteq (U_1 \times F) \cup (F \times V_1)$.

Extend F_2 to a subuniverse V_2 of $\mathbf{F}$ satisfying that V_2 is maximal such that $(y, x) \notin Sg^{\mathbf{F}^2}\{F_1 \times F \cup F \times V_2\} = S_2$ by Zorn's lemma. Define

$$U_2 = \overrightarrow{P_1}(S_2 \cap F \times \{x\}).$$

$y \in F_2 \subseteq V_2$, $x \in U_2$ since $(x, x) \in S_2$. We will show that

$$(U_2 \times F) \cup (F \times V_2) = S_2.$$

From the definition of U_2, for any $u \in U_2$, $(u,x) \in S_2$. And $(u,y) \in S_2$, so $U_2 \times F \subseteq S_2$, obviously $F \times V_2 \subseteq S_2$, hence $(U_2 \times F) \cup (F \times V_2) \subseteq S_2$.

Take $(p,q) \in S_2 \backslash (F \times V_2)$. Then $q \notin V_2$. Define $V_2' = Sg^{\mathbf{F}^2}(V_2 \cup \{q\})$. The maximality of V_2 implies that $(y,x) \in Sg^{\mathbf{F}^2}\{F_1 \times F \cup F \times V_2'\}$.

We claim that

$$\begin{aligned} & Sg^{\mathbf{F}^2}\{F_1 \times F \cup F \times V_2'\} \\ &= Sg^{\mathbf{F}^2}\{F_1 \times \{x\} \cup F \times V_2'\} \\ &= Sg^{\mathbf{F}^2}\{F \times V_2' \cup \{x\} \times \{x\}\} \\ &= Sg^{\mathbf{F}^2}\{\{y\} \times V_2 \cup \{(y,q),(x,y),(x,x)\}\}. \end{aligned}$$

Then $\exists$ a term t and $v_1, \cdots, v_k \in V_2$ such that

$$(y,x) = t((y,v_1), \cdots, (y,v_k), (y,q), (x,x), (x,y)).$$

So $y = t(y, \cdots, y, y, x, x)$ and $x = t(v_1, \cdots, v_k, q, x, y)$. We can find a homomorphism f mapping x to x and mapping y to p since $\mathbf{F}$ is free. Then apply f to the equation $y = t(y, \cdots, y, y, x, x)$, we have $p = t(p, \cdots, p, p, y, y)$. Then

$$(p,x) = t((p,v_1), \cdots, (p,v_k), (p,q), (x,x), (x,y)) \in S_2 \cap F \times \{x\},$$

so $p \in U_2$, $(p,q) \in U_2 \times F$, $S_2 \subseteq (U_2 \times F) \cup (F \times V_2)$.

$\square$

CHAPTER 3. JOINS AND MALTSEV PRODUCT OF MALTSEV VARIETIES

3.1 Introduction

Varieties are classes of similar algebras closed under homomorphic images, subalgebras and direct products. This chapter is concerned with what could be for the joins and Maltsev product of two Maltsev varieties.

Definition 3.1.1. *For two idempotent varieties $\mathcal{V}$ and $\mathcal{W}$, the* maltsev product $\mathcal{V} \circ \mathcal{W}$ *is defined as:*

$$\{\boldsymbol{A} : \exists \theta \in Con(\boldsymbol{A}) \quad with\ \boldsymbol{A}/\theta \in \mathcal{W}\ and\ each\ block\ \ a/\theta \in \mathcal{V}\}.$$

Notice that every a/θ is a subalgebra in an idempotent variety.

Definition 3.1.2. *The* join of two varieties $\mathcal{V}$ *and* $\mathcal{W}$ *is the smallest variety containing* $\mathcal{V}$ *and* $\mathcal{W}$*, denoted by* $\mathcal{V} \vee \mathcal{W}$.

Our class of algebras and varieties that we pay attention to are the idempotent algebras and idempotent varieties.

Lemma 3.1.1. *If an algebra $\boldsymbol{A}$ is idempotent and $\theta \in Con(\boldsymbol{A})$, then for any $a \in A$, a/θ is always a subuniverse of $\boldsymbol{A}$.*

Proof. We know that a/θ is a subset of A,

for any $b_1, \cdots, b_n \in a/\theta$, and f is an n-ary operation on A, then

$$f(b_1, \cdots, b_n)/\theta = f(b_1/\theta, \cdots, b_n/\theta) = f(a/\theta, \cdots, a/\theta) = f(a, \cdots, a)/\theta = a/\theta,$$

since A is idempotent.

Thus $f(b_1, \cdots, b_n) \in a/\theta$, and a/θ is a subuniverse of A. □

As a consequence, we have the following lemma.

Lemma 3.1.2. *If an algebra $\boldsymbol{A}$ is idempotent and has no proper, nontrivial subalgebras, then $\boldsymbol{A}$ is simple.*

Proof. Suppose $\theta \in Con(\mathbf{A})$ and $\theta \neq 0_{\mathbf{A}}$.

Using lemma 3.1.1, we know that a/θ is a trivial algebra for some $a \in A$. Since $a \in a/\theta$, $a/\theta \neq \phi$, then $a/\theta = A$, thus $\theta = 1_{\mathbf{A}}$, and $\mathbf{A}$ is simple. □

Let $h : \mathbf{A} \to \mathbf{B}$ be a homomorphism with kernel α. Let $r \in A$. Then r/α is a subalgebra of $\mathbf{A}$ if and only if $h(r)$ is idempotent in $\mathbf{B}$. This is an immediate consequence of the fact that a direct image of a subalgebra is a subalgebra and the inverse image of a subalgebra is a subalgebra. Another way to say that is that r/α is a subalgebra of $\mathbf{A}$ if and only if for every basic operation f, $f(r, \cdots, r) \in r/\alpha$.

Lemma 3.1.3. *Let $\boldsymbol{A}$ be an algebra, $\alpha, \beta \in Con(\boldsymbol{A})$, $\alpha \subseteq \beta$ and $r \in A$.*

(1) $(r/\alpha)/(\beta/\alpha) = (r/\beta)/\alpha$.

(2) $r/\beta \in Sub(\boldsymbol{A}) \Longleftrightarrow (r/\alpha)/(\beta/\alpha) \in Sub(\boldsymbol{A}/\alpha)$.

Proof. $x/\alpha \in (r/\alpha)/(\beta/\alpha) \Longleftrightarrow x \in r/\beta \Longleftrightarrow x/\alpha \in (r/\beta)/\alpha$.

For the other one, let $h : \mathbf{A} \to \mathbf{A}/\alpha$ be the canonical homomorphism.

By the isomorphism theorem, we can obtain

$$\mathbf{A}/\beta \cong (\mathbf{A}/\alpha)/(\beta/\alpha).$$

Let $g_1 : \mathbf{A} \to \mathbf{A}/\beta$ and $g_2 : \mathbf{A}/\alpha \to (\mathbf{A}/\alpha)/(\beta/\alpha)$ be the canonical homomorphisms.

Then

$$g_2 \circ h = g_1.$$

Therefore,

$$r/\beta \in Sub(\mathbf{A}) \Longleftrightarrow g_1(r) = g_2(h(r)) \text{ is idempotent} \Longleftrightarrow (r/\alpha)/(\beta/\alpha) \in Sub(\mathbf{A}/\alpha).$$

□

3.2 Joins of Maltsev Varieties

Theorem 3.2.1. *($M.Valeriote$) If $\mathcal{V}$ and $\mathcal{W}$ are two idempotent Maltsev varieties, then $\mathcal{V} \vee \mathcal{W}$ is congruence 3-permutable with Hagemann-Mitschke terms*

$$x,$$
$$p(q(x, p(x, y, z), p(x, y, z)), q(x, p(y, z, z), z), q(x, y, z)),$$
$$p(q(x, y, z), q(x, p(x, y, y), z), q(p(x, y, z), p(x, y, z), z)),$$
$$z,$$

where p and q are Maltsev terms for $\mathcal{V}$ and $\mathcal{W}$, respectively.

Valeriote also found algebras that show the above terms are not adequate to show $\mathcal{V} \circ \mathcal{W}$ is congruence 3-permutable.

Theorem 3.2.2. *([5]) If $\mathcal{V}$ and $\mathcal{W}$ are two idempotent Maltsev varieties, then $\mathcal{V} \circ \mathcal{W}$ is congruence 4-permutable with Hagemann-Mitschke terms*

$$x,$$
$$f(x, g(x, y, y), g(x, z, z)),$$
$$g(x, y, z),$$
$$f(g(x, x, z), g(y, y, z), z),$$
$$z,$$

where f and g are Maltsev terms for $\mathcal{V}$ and $\mathcal{W}$, respectively.

Notice that the join of two varieties is included in the maltsev product of two varieties.

We have the example that Maltsev product of two idempotent Maltsev varieties is congruence 4-permutable with Hagemann-Mitschke terms. In fact we will see that their Maltsev product is congruence 3-permutable, however the proof does not produce Hagemann-Mitschke terms. We will see it in next section.

3.3 Maltsev Product of Maltsev Varieties

Theorem 3.3.1. *Let Sq be the variety of binars satisfying the identities:*

$$x^2 \approx x,\ xy \approx yx,\ x(xy) \approx y.$$

Then Sq and $Sq \circ Sq$ has a Maltsev term respectively.

Proof. Define $q(x, y, z) = y(xz)$. It is easy to check that q is a Maltsev term for Sq.

Define $p(x, y, z) = (x(z(xy)))(z(x(zy)))$.

We will verify that p is a Maltsev term for $Sq \circ Sq$.

Let $\mathbf{A} \in Sq \circ Sq$, then

$$\exists \theta \in \mathbf{Con}(\mathbf{A}),\ \mathbf{A}/\theta \in Sq, \text{ and for any } a \in A,\ a/\theta \in Sq.$$

We will show $\mathbf{A}$ satisfies

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

for $x, z \in A$,

$$p(x, x, z) \approx (x(z(x^2)))(z(x(zx))) \approx (x(zx))(z(x(zx))),$$

let $w = x(zx)$, then

$$w/\theta = x/\theta(z/\theta \cdot x/\theta) = x/\theta(x/\theta \cdot z/\theta) = z/\theta,$$

since $a/\theta \in Sq$ for any $a \in A$. So $w, z \in z/\theta \in Sq$, we obtain $zw \approx wz$ and $w(wz) \approx z$. Hence

$$p(x, x, z) \approx w(zw) \approx w(wz) \approx z.$$

For the other one,

$$p(x, z, z) \approx (x(z(xz)))(z(x(z^2))) \approx (x(z(xz)))(z(xz)),$$

let $u = z(xz)$, then

$$u/\theta = z/\theta(x/\theta \cdot z/\theta) = z/\theta(z/\theta \cdot x/\theta) = x/\theta,$$

since $a/\theta \in Sq$ for any $a \in A$. So $u, x \in x/\theta \in Sq$, and

$$xu/\theta = x/\theta \cdot u/\theta = x/\theta \cdot x/\theta = x/\theta.$$

So $xu, x \in x/\theta \in Sq$. We obtain $ux \approx xu$ and $u(xu) \approx (xu)u$. Hence

$$p(x, z, z) \approx (xu)u \approx u(xu) \approx u(ux) \approx x.$$

□

Theorem 3.3.2. (*R.Freese and R.McKenzie*) *The Maltsev product of two idempotent and congruence permutable varieties is congruence* 3*-permutable.*

It is not necessarily true that their Maltsev product is congruence permutable. We will present an example later.

The idea of the proof is to show that if $\mathbf{A}$ is an algebra and $\theta \in Con(\mathbf{A})$ is such that $\mathbf{A}/\theta$ has a Maltsev term $q(x, y, z)$ and there is a term $p(x, y, z)$ which is Maltsev on each block of θ, then the congruences of $\mathbf{A}$ 3-permute. The above theorem will use the following two lemmas.

Lemma 3.3.1. ([5]) *Let $\boldsymbol{A}$ be an algebra, $\theta \in Con(\boldsymbol{A})$.*

(1) *If $\boldsymbol{A}/\theta$ has a Maltsev term, then for all $\psi \in Con(\boldsymbol{A})$,*

$$\psi \circ \theta \circ \psi \subseteq \theta \circ \psi \circ \theta$$

(2) *If $p(x, y, z)$ is a term which is Maltsev on each θ-block, then for $\psi \in Con(\boldsymbol{A})$,*

$$\theta \circ \psi \circ \theta \subseteq \psi \circ \theta \circ \psi.$$

Thus if the hypotheses of both (1) *and* (2) *hold, then θ* 3*-permutes with all $\psi \in Con(\boldsymbol{A})$.*

Proof. First assume the hypothesis of (1) holds and that the Maltsev term is $q(x, y, z)$. Suppose $(a, d) \in \psi \circ \theta \circ \psi$ so there exists b and c such that

$$a \ \psi \ b \ \theta \ c \ \psi \ d,$$

then

$$a \ \theta \ q(a, b, b) \ \theta \ q(a, b, c) \ \psi \ q(b, b, d) \ \theta \ d,$$

so

$$(a, d) \in \theta \circ \psi \circ \theta.$$

Now assume the hypothesis of (2) holds and suppose $(a, d) \in \theta \circ \psi \circ \theta$ so there exists b and c such that

$$a \ \theta \ b \ \psi \ c \ \theta \ d,$$

we calculate

$$a = p(a, b, b) \ \psi \ p(a, b, c) \ \theta \ p(b, b, d) \ \psi \ p(c, c, d) = d.$$

Hence

$$(a, d) \in \psi \circ \theta \circ \psi.$$

□

Lemma 3.3.2. ([5]) *Assume* $\boldsymbol{A}$ *and* θ *satisfy the hypotheses of* (1) *and* (2) *of the above lemma.*

(1) *If* $\alpha, \beta \geq \theta$*, then they permute.*

(2) *If* $\alpha, \beta \leq \theta$*, then they permute.*

Example 3.3.1. ([5]) *First, we exhibit two finite idempotent Maltsev algebras* $\boldsymbol{B}_0$ *and* $\boldsymbol{B}_1$ *whose direct product is not Maltsev. This shows also that neither the join nor the Maltsev product of two idempotent Maltsev varieties need have a Maltsev term. These two algebras will have two ternary operation symbols* $\{p, q\}$*, and* $\{0, 1\}$ *is the universe of both algebras,*

$p^{\boldsymbol{B}_0} = q^{\boldsymbol{B}_1}$ *are Pixley operations and* $q^{\boldsymbol{B}_0}(x, y, z) = p^{\boldsymbol{B}_1}(x, y, z) = x \vee y \vee z$ *(the maximum of the three inputs).*

The set $S = \{0, 1\}^2 \backslash \{(0, 0)\}$ *is a subuniverse of* $\boldsymbol{B} = \boldsymbol{B}_0 \times \boldsymbol{B}_1$*, let* $\boldsymbol{S}$ *be the corresponding subalgebra. The two projection congruences restricted to* $\boldsymbol{S}$ *do not permute. Thus* $\boldsymbol{B}_0 \times \boldsymbol{B}_1$ *has no Maltsev term.*

However, the variety generated by $\boldsymbol{B}$ *is congruence* 3*-permutable with Hagemann-Mitschke terms:*

$$x, \quad p(x, q(x, y, x), q(x, y, z)), \quad p(z, q(y, y, z), q(x, y, z)), \quad z.$$

Theorem 3.3.3. [5] *If* $\mathcal{V}$ *and* $\mathcal{W}$ *be two idempotent, congruence* 3*-permutable varieties, then* $\mathcal{V} \circ \mathcal{W}$ *is congruence* 15*-permutable with Hagemann-Mitschke terms,*

$$h_0(x,y,z) = x,\ h_{15}(x,y,z) = z$$

and

$$h_1(x,y,z) = f_1(x, g_1(x,y,y), g_1(x,z,z))$$

$$h_2(x,y,z) = f_2(x, g_1(x,y,y), g_1(x,z,z))$$

$$h_3(x,y,z) = g_1(x,y,z)$$

$$h_4(x,y,z) = f_1(g_1(x,x,z), g_2(x,y,y), g_2(x,z,z))$$

$$h_5(x,y,z) = f_1(g_1(x,x,z), f_1(x, g_1(x,y,y), g_1(x,z,z)), g_2(x,z,z))$$

$$h_6(x,y,z) = f_1(g_1(x,x,z), f_2(x, g_1(x,y,y), g_1(x,z,z)), g_2(x,z,z))$$

$$h_7(x,y,z) = f_1(g_1(x,x,z), g_1(x,y,z), g_2(x,z,z))$$

$$h_8(x,y,z) = f_2(g_1(x,x,z), g_2(x,y,z), g_2(x,z,z))$$

$$h_9(x,y,z) = f_2(g_1(x,x,z), f_1(g_2(x,x,z), g_2(y,y,z), z), g_2(x,z,z))$$

$$h_{10}(x,y,z) = f_2(g_1(x,x,z), f_2(g_2(x,x,z), g_2(y,y,z), z), g_2(x,z,z))$$

$$h_{11}(x,y,z) = f_2(g_1(x,x,z), g_1(y,y,z), g_2(x,z,z))$$

$$h_{12}(x,y,z) = g_2(x,y,z)$$

$$h_{13}(x,y,z) = f_1(g_2(x,x,z), g_2(y,y,z), z)$$

$$h_{14}(x,y,z) = f_2(g_2(x,x,z), g_2(y,y,z), z)$$

where f_i and g_i for $i = 1, 2$ are Hagemann-Mitschke terms for $\mathcal{V}$ and $\mathcal{W}$, respectively.

Theorem 3.3.4. (*Bergman*) *Let $\mathcal{V}$ and $\mathcal{W}$ be two idempotent varieties. If $\mathcal{V} \vee \mathcal{W}$ is congruence permutable, then $\mathcal{V} \circ \mathcal{W}$ is congruence permutable.*

Proof. Let q be a Maltsev term for $\mathcal{V} \vee \mathcal{W}$. Assume $\mathcal{V} \circ \mathcal{W}$ is not congruence permutable. We shall derive a contradiction. Let $\mathcal{U} = \mathbf{H}(\mathcal{V} \circ \mathcal{W})$. Since $\mathcal{V}$ and $\mathcal{W}$ are idempotent, so is $\mathcal{U}$. Certainly $\mathcal{U}$ is not congruence permutable, so we can apply Kearnes and Tschantz' lemma to $\mathcal{U}$.

So let $\mathbf{F} = \mathbf{F}_{\mathcal{U}}(x, y)$. Let U and V be the subuniverses provided by the lemma, and let $S = (U \times F) \cup (F \times V)$. Since $\mathbf{F}$ is free and $\mathcal{U} = \mathbf{H}(\mathcal{V} \circ \mathcal{W})$, we have $\mathbf{F} \in \mathcal{V} \circ \mathcal{W}$. Hence there is a congruence λ on $\mathbf{F}$ such that $\mathbf{G} = \mathbf{F}/\lambda \in \mathcal{W}$ and $\mathbf{Y} = y/\lambda \in \mathcal{V}$. of course $y \in Y$.

Let $a = (y, x), b = (x, x), c = (x, y)$, and $d = (y, y)$. Note that $a, b, c \in S$ while $d \notin S$. We shall derive a contradiction by showing that, in fact, $d \in S$.

Let $d' = q^{\mathbf{F}^2}(a, b, c) = (p_1, p_2)$. Then $a, b, c \in S$ implies that $d' \in S$ as well. From the definition of S we must have either $p_1 \in U$ or $p_2 \in V$. Without loss of generality, let us assume that

$$p_2 \in V.$$

Now from the definitions of a, b, c and d', we have $p_1 = q^{\mathbf{F}}(y, x, x)$. But $\mathbf{G} = \mathbf{F}/\lambda \in \mathcal{W}$ and q is a Maltsev term for $\mathcal{W}$, hence $p_1/\lambda = q^{\mathbf{G}}(y/\lambda, x/\lambda, x/\lambda) = y/\lambda$, thus

$$p_1 \in Y.$$

Similarly, $p_2/\lambda = q^{\mathbf{G}}(x/\lambda, x/\lambda, y/\lambda) = y/\lambda$, so

$$p_2 \in Y.$$

Now let $e = (x, p_2) \in F \times V \subseteq S$ by $p_2 \in V$.Define $e' = q^{\mathbf{F}^2}(d', e, c) = (p_3, p_4)$. Then e' is a member of S as well. As before, $p_3/\lambda = q^{\mathbf{G}}(p_1/\lambda, x/\lambda, x/\lambda) = p_1/\lambda$, so

$$p_3 \in Y.$$

From $p_2 \in Y$, hence $p_4 = q^{\mathbf{F}}(p_2, p_2, y) = q^{\mathbf{Y}}(p_2, p_2, y) = y$ since q is a Maltsev term for $\mathbf{Y} \in \mathcal{V}$.

Finally, let $f_1 = (y, p_2)$ and $f_2 = (p_3, p_2)$. Then $f_1, f_2 \in F \times V \subseteq S$. Then $q^{\mathbf{F}^2}(f_1, f_2, e') \in S$. But

$$q^{\mathbf{F}^2}(f_1, f_2, e') = (q^{\mathbf{Y}}(y, p_3, p_3), q^{\mathbf{Y}}(p_2, p_2, y)) = (y, y) = d$$

proving that $d \in S$. That is a contradiction. □

Corollary 3.3.1. *Let $\mathcal{V}$ be an idempotent congruence permutable variety. Then $\mathcal{V} \circ \mathcal{V}$ is congruence permutable.*

Proof. Since $\mathcal{V} = \mathcal{V} \vee \mathcal{V}$ and $\mathcal{V}$ is an idempotent congruence permutable variety, by the above theorem, $\mathcal{V} \circ \mathcal{V}$ is congruence permutable.

□

CHAPTER 4. FUTURE DIRECTIONS

4.1 Not Congruence 3-permutable Variety

We have the equivalent conditions for the variety which is not congruence permutable from the following lemma. We are thinking, if the variety is not congruence 3-permutable, can we give some similar equivalent conditions. Moreover, if the variety is not congruence n-permutable for some integer $n > 1$, can we characterize such a variety with similar equivalent conditions.

Lemma 4.1.1. ([*12*]) *Let $\mathcal{V}$ be an idempotent variety that is not congruence permutable. If $\boldsymbol{F} = \boldsymbol{F}_{\mathcal{V}}(x, y)$ is the 2-generated free algebra in $\mathcal{V}$, then $\boldsymbol{F}$ has subuniverses U and V such that*
(1) $x \in U, y \in V$,
(2) $y \notin U, x \notin V$,
(3) $(U \times F) \cup (F \times V)$ *is a subuniverse of* $\boldsymbol{F} \times \boldsymbol{F}$.

Definition 4.1.1. *A* binary cross *on a set A is a subset of A^2 of the form $(U_0 \times A) \cup (A \times U_1)$, where U_0 and U_1 are nonempty proper subsets of A. If $U_0 = U_1$, the cross is called symmetric. If $|U_0| = |U_1| = 1$, the cross is called thin. The sequence (U_0, U_1) is called the base for the cross. If the cross is symmetric, i.e., if the base has the form (U, U), then we also refer to U as the base.*

The definition of a cross can be applied for higher arity relations. For some positive integer d, a d-ary cross is defined as follows:

Definition 4.1.2. *A* d-ary cross *is a subset of A^d of the form*

$$(U_0 \times A \times \cdots \times A) \cup (A \times U_1 \times \cdots \times A) \cup \cdots \cup (A \times A \times \cdots \times U_{d-1}),$$

where $U_0, \cdots, U_{d-1}$ *are nonempty proper subsets of* A*. For d=1, this means that 1-ary cross is a nonempty proper subsets of* A*. The definitions of symmetric cross, thin cross, and base for a* $d-ary$ *cross are the expected ones. The arity of a cross is also called its* dimension.

Conjecture 4.1.1. *Let* $\mathcal{V}$ *be an idempotent variety and* n *is an integer,* $n > 1$*. Then* $\mathcal{V}$ *is not congruence* 3*-permutable if and only if* $\boldsymbol{F} = \boldsymbol{F}_{\mathcal{V}}(x, y)$ *is the 2-generated free algebra in* $\mathcal{V}$*, and* $\boldsymbol{F}$ *has subuniverses* U_1, U_2 *and* V_1, V_2 *such that* $1 \leq i \leq 2$

(1) $x \in U_i$ *and* $y \in V_i$*,*

(2) $U_1 \cap U_2 \cap V_1 \cap V_2 = \phi$*,*

(3) $(U_i \times F) \cup (F \times V_i)$ *is a subuniverse of* $\boldsymbol{F} \times \boldsymbol{F}$*.*

If the above corollary is true, further we want to use such a corollary to prove the following statement.

Conjecture 4.1.2. *Let* $\mathcal{V}$ *and* $\mathcal{W}$ *be two idempotent varieties. If* $\mathcal{V} \vee \mathcal{W}$ *is congruence* 3*-permutable, then* $\mathcal{V} \circ \mathcal{W}$ *is congruence* 3*-permutable.*

If the property of congruence 3-permutable is too strong, alternatively we can define a weak condition as follows.

Definition 4.1.1. *An idempotent variety* $\mathcal{V}$ *is* weakly congruence 3-permutable *if* $\boldsymbol{F} = \boldsymbol{F}_{\mathcal{V}}(x, y)$ *is the 2-generated free algebra in* $\mathcal{V}$*, there does not exsit subuniverses* U_1*,* U_2 *and* V_1*,* V_2 *of* $\boldsymbol{F}$ *such that*

(1) $x \in U_2 \subseteq U_1$*,* $y \in V_1 \subseteq V_2$*,*

(2) $U_2 \cap V_1 = \phi$*,*

(3) $(U_i \times F) \cup (F \times V_i)$ *is a subuniverse of* $\boldsymbol{F} \times \boldsymbol{F}$*, for* $i = 1, 2$*.*

Lemma 4.1.1. *If an idempotent variety* $\mathcal{V}$ *is congruence* 3*-permutable, then* $\mathcal{V}$ *is weakly congruence* 3*-permutable.*

Proof. Assume that the idempotent variety $\mathcal{V}$ is not weakly congruence 3-permutable,

then $\mathbf{F} = \mathbf{F}_{\mathcal{V}}(x, y)$ is the 2-generated free algebra in $\mathcal{V}$, there exist subuniverses U_1, U_2 and V_1, V_2 of $\mathbf{F}$ such that

(1) $x \in U_2 \subseteq U_1$, $y \in V_1 \subseteq V_2$,

(2) $U_2 \cap V_1 = \phi$,

(3) $(U_i \times F) \cup (F \times V_i)$ is a subuniverse of $\mathbf{F} \times \mathbf{F}$, for $i = 1, 2$.

We know that $\mathcal{V}$ is congruence 3-permutable,

then there exist two ternary terms p_1, p_2 of $\mathcal{V}$ such that

$$p_1(x, y, y) \approx x,$$
$$p_1(x, x, y) \approx p_2(x, y, y),$$
$$p_2(x, x, y) \approx y.$$

Note that $(x, x), (x, y), (y, y)$ are all in $(U_i \times F) \cup (F \times V_i)$ for each $i = 1, 2$.

So

$$(y, p_2(x, y, y)) \approx (p_2(x, x, y), p_2(x, y, y)) \in (U_i \times F) \cup (F \times V_i) \text{ for } i = 1, 2,$$
$$(p_1(x, x, y), x) \approx (p_1(x, x, y), p_1(x, y, y)) \in (U_i \times F) \cup (F \times V_i) \text{ for } i = 1, 2.$$

By $y \notin U_i$ and $x \notin V_i$, we have $p_2(x, y, y) \in V_i$ and $p_1(x, x, y) \in U_i$ for $i = 1, 2$, Since $p_1(x, x, y) \approx p_2(x, y, y)$, we obtain

$$p_1(x, x, y) \in U_1 \cap U_2 \cap V_1 \cap V_2 = U_2 \cap V_1.$$

That is a contradiction with $U_2 \cap V_1 = \phi$. Therefore $\mathcal{V}$ is weakly congruence 3-permutable.

□

Then if a variety is weakly congruence 3-permutable, can we characterize such a variety with similar conditions, that is one direction we can do the research.

4.2 Cube Term and Cube-term Blocker

Some charaterizations of algebras with cube-terms is very interesting topic, and it is very useful to settle M. Valeriote's conjecture.

In paper[15], it says that Valeriote's conjecture is equivalent to each of the statements below.

(1) The class of finite and finitely related idempotent algebras generating congruence modular varieties is closed under idempotent expansions.

(2) The class of finite and finitely related idempotent algebras generating congruence modular varieties is closed under forming subalgebras and homomorphic images and every full polynomial expansion of such an algebra is finitely related.

First we present some basic information of it.

Definition 4.2.1. *A* cube operation *over a set A is an operation $c(x_0, \cdots, x_{n-1})$ such that for each $0 \leq i < n$, the algebra $\langle A, c\rangle$ satisfies an equation $c(w_0, \cdots, w_{n-1}) = x$ where $\{w_0, \cdots, w_{n-1}\} \subseteq \{x, y\}$ and $w_i = y$.*

Definition 4.2.2. *An algebra $\boldsymbol{A}$ is said to have a* cube-term *if its clone of term operations contains a cube operation.*

Definition 4.2.3. *An* idempotent operation *over A is a function $f : A^n \to A$ for some n such that the function $g(x) = f(x, \cdots, x)$ is the identity function on A. By an* idempotent algebra *we mean an algebra whose basic operations are idempotent, and thus every term operation of the algebra is idempotent.*

Definition 4.2.4. *Let $\boldsymbol{A}$ be a finite algebra. A* cube-term blocker *in $\boldsymbol{A}$ is any pair (D, S) of subuniverses of $\boldsymbol{A}$ such that $\phi < D < S \leq \boldsymbol{A}$ and such that for every term operation $t(x_1, \cdots, x_n)$ of $\boldsymbol{A}$ there is i, $1 \leq i \leq n$, so that whenever $(s_1, \cdots, s_n) \in S^n$ and $s_i \in D$, then $t(s_1, \cdots, s_n) \in D$.*

Then we construct two small results about cube-term blocker.

Lemma 4.2.1. *Let $\boldsymbol{A}$ be a commutative idempotent binar (CIB), $\phi < D < S \leq \boldsymbol{A}$. Then (D, S) is a cube-term blocker if and only if $s \in S$ and $d \in D$ implies $s \cdot d \in D$.*

Proof. " $\Rightarrow$ " Suppose (D, S) is a cube-term blocker. Let $t(x_1, x_2) = x_1 \cdot x_2$.

For any $s, d \in S$, $d \in D$, by the definition of a cube-term blocker, $t(s, d) = s \cdot d \in D$.

" $\Leftarrow$ " Since $\mathbf{A}$ is a CIB, for each term operation $t(x_1, \cdots, x_n)$, for any $x_1, \cdots, x_n \in S$ and $x_i \in D$, we can write $t(x_1, \cdots, x_n) = \prod_{s \in I}(x_{i_1} \cdot x_{i_2} \cdots x_{i_{k_s}})$, where $i_1, i_2, \cdots, i_{k_s} \in \{1, 2, \cdots, n\}$. Consider each $x_{i_1} \cdot x_{i_2} \cdots x_{i_{k_s}}$, if one of $x_{i_1}, x_{i_2}, \cdots, x_{i_{k_s}}$ is in D, since this binary operation $\cdot$ is idempotent and commutative, then $x_{i_1} \cdot x_{i_2} \cdots x_{i_{k_s}} \in D$, if none of $x_{i_1}, x_{i_2}, \cdots, x_{i_{k_s}}$ is in D, then $x_{i_1} \cdot x_{i_2} \cdots x_{i_{k_s}} \in S$. Similarly $t(x_1, \cdots, x_n) = \prod_{s \in I}(x_{i_1} \cdot x_{i_2} \cdots x_{i_{k_s}}) \in D$, since there is some $s \in I$, $x_{i_1} \cdot x_{i_2} \cdots x_{i_{k_s}} \in D$. □

Lemma 4.2.2. *Let* $\boldsymbol{A}$ *be a commutative idempotent binar* (CIB)*, and let* $\boldsymbol{2}$ *denote the 2-element semilattice. Then* $\boldsymbol{2} \in \boldsymbol{HS}(\boldsymbol{A})$ *if and only if* $\boldsymbol{A}$ *has a cube-term blocker.*

Proof. " $\Leftarrow$ " Suppose **A** is CIB and **A** has a cube-term blocker (D, S).

If $|D| = 1$, let $D = \{d\}$. Pick one element $s \in S \backslash D$, then construct $\mathbf{2} = \{s, d\}$, and obtain

$$\mathbf{2} \leq \mathbf{S}(\mathbf{A}) \subseteq \mathbf{HS}(\mathbf{A}).$$

If $|D| \geq 2$, let $\theta = 1_D \cup 0_S$, then $\theta \in Con(S)$. Pick $d \in D$ and $s \in S \backslash D$. We construct $\mathbf{2} = \{s/\theta, d/\theta\}$, where $d/\theta = D$. Then

$$\mathbf{2} \leq \mathbf{S}(S/\theta) \subseteq \mathbf{SH}(S) = \mathbf{SHS}(\mathbf{A}) = \mathbf{HS}(\mathbf{A}).$$

" $\Rightarrow$ " Suppose $\mathbf{2} \in \mathbf{HS}(\mathbf{A})$, then $\mathbf{2} = \mathbf{B}/\phi$, where $\phi \in Con(\mathbf{B})$, and $\mathbf{B} \in \mathbf{S}(\mathbf{A})$.

Let $\mathbf{B}/\phi = \{s_1/\phi, s_2/\phi\}$. WLOG, $(s_1/\phi) \cdot (s_2/\phi) = (s_1/\phi)$, then let $D = s_1/\phi < B$. Choose any $d \in D$, any $s \in B$, then we have

$$s/\phi = s_1/\phi \text{ or } s/\phi = s_2/\phi.$$

If $s/\phi = s_1/\phi$, then $(d/\phi) \cdot (s/\phi) = (s_1/\phi) \cdot (s_1/\phi) = D$, so $d \cdot s \in D$.

If $s/\phi = s_2/\phi$, then

$$(d/\phi) \cdot (s/\phi) = (s_1/\phi) \cdot (s_2/\phi) = (s_1/\phi) = D,$$

so $d \cdot s \in D$, by lemma 4.2.1, (D, B) is a cube-term blocker.

□

Theorem 4.2.1. ([*11*]) *Let* $\boldsymbol{A}$ *be a finite idempotent algebra. Then* $\boldsymbol{A}$ *has a cube-term if and only if it possesses no cube-term blockers.*

That is another direction for the future research.

BIBLIOGRAPHY

[1] Bergman, C. (2012). *Universal Algebra*, volume 301 of Pure and Applied Mathematics. CRC press, Boca Raton, FL.

[2] Birkhoff, G. (1935). On the structure of abstract algebras. *Proceedings of the Cambridge Philosophical Society*, 31:433 – 454.

[3] Burris, S. and Sankappanavar, H. (1981). *A course in universal algebra*. Graduate texts in mathematics. Springer-Verlag.

[4] Freese, R. (2013). Equations implying congruence n-permutability and semidistributivity. *Algebra universalis*, 70(4):347–357.

[5] Freese, R. and Mckenzie, R. (2013). Maltsev families of varieties closed under join or maltsev product, preprint.

[6] Freese, R. and Valeriote, M. A. (2009). On the complexity of some maltsev conditions. *International Journal of Algebra and Computation*, 19(01):41–77.

[7] Hagemann, J. and Mitschke, A. (1973). On n-permutable congruences. *Algebra Universalis 3*, pages 8–12.

[8] Hobby, D. and McKenzie, R. (1988). The structure of finite algebras(tame congruence theory). *Contemporary Mathematics, American Mathematical Society, Providence, RI.*

[9] Kearnes, K. (1993). Congruence permutable and congruence 3-permutable locally finite varieties. *Journal of Algebra*, 156(1):36 – 49.

[10] Kearnes, K. A. and Kiss, E. W. (2013). The shape of congruence lattices. *Memoirs of the American Mathematical Society Series.*

[11] Kearnes, K. A. and Szendrei, A. (2016). Cube term blockers without finiteness. *ArXiv e-prints*.

[12] Kearnes, K. A. and Tschantz, S. T. (2007). Automorphism groups of squares and of free algebras. *International Journal of Algebra and Computation*, 17(03):461–505.

[13] Kozik, M., Krokhin, A., Valeriote, M., and Willard, R. (2015). Characterizations of several maltsev conditions. *Algebra universalis*, 73(3):205–224.

[14] Maltsev, A. I. (1954). On the general theory of algebraic systems. *Mat. Sb. N. S.*, 35 (77):3 – 20.

[15] Marković, P., Maróti, M., and McKenzie, R. (2012). Finitely related clones and algebras with cube terms. *Order*, 29(2):345–359.

[16] Mitschke, A. (1978). Near unanimity identities and congruence distributivity in equational classes. *Algebra Universalis*, 8:29 – 32.

[17] Plonka, J. (1969). On equational classes of abstract algebras defined by regular equations. *Fund. Math.*, 64:241 – 247.

[18] Valeriote, M. and Willard, R. (2014). Idempotent n-permutable varieties. *Bulletin of the London Mathematical Society*, 46(4):870–880.