Wreath Decompositions of Algebras

Joel VanderWerf

June, 1995

Abstract

We generalize to finite algebras the Krohn-Rhodes wreath decomposition theory of finite (transformation) semigroups. (An algebra here is a set with a clone of operations.) Our methods are essentially categorical, following the lead of B. Tilson's approach to the Krohn-Rhodes theory. We define wreath products and relational morphisms of algebras. Associated with a relational morphism is a many-sorted algebra, called the derived algebra, analogous with Tilson's derived category. Many-sorted algebras are ordered by division, which is similar to Tilson's division ordering of categories. (For one-sorted algebras, being a divisor means being a quotient of a subreduct.) As in Tilson's work, these notions are linked by a Covering Lemma, which establishes an adjoint-like connection between the derived algebra and wreath product constructions. Using this lemma, finding a decomposition of an algebra (that is, finding a wreath product which the algebra divides) amounts to finding a relational morphism whose image is the right-hand wreath factor and whose derived algebra divides the left-hand wreath factor.

For finite unary algebras, the resulting decomposition theory is essentially the "one-sided" decomposition theory of finite transformation semigroups, as per Krohn-Rhodes. For finite semigroups considered as algebras with a binary multiplication operation, the resulting decomposition theory is related to the "two-sided" theory of Rhodes-Weil. All decompositions using their double semidirect product can be simulated with the new wreath product by adding certain unary operations (specifically, endomorphisms) to the clone of operations of the left-hand wreath factor. In fact, adding certain other unary operations (constants) leads to a new and simplified proof of the Rhodes-Weil decomposition theorem for the new product. The methods used suggest that the new decomposition theory might be stronger than the Rhodes-Weil theory. That is, the complexity of a finite semigroup—the minimum number of groups required to decompose it—might in some cases be strictly lower using the new product. However, counting groups in this manner is meaningless for decompositions involving nonsolvable group factors, for, by a theorem of G. Bergman, every finite algebra divides some nonsolvable group with an extra unary operation of the kind needed to simulate the double semidirect product.

This observation leads us to restrict our attention to algebras which are aprimal—no matrix power has a nonsolvable group divisor. (Matrix powers generalize the construction taking a module M over a ring R to the module M^k over the ring of $k \times k$ matrices over R.) Every such algebra decomposes into simple algebras of (tame congruence theory) type 1, 2, or 5. By theorems of Hobby-McKenzie, simple algebras of type 1 and 2 divide matrix powers of sets and cyclic groups, respectively. Analysis of the type 5 case begins with the order structure found by Hobby-McKenzie. We show that if the order has a maximum element, then the algebra is aperiodic—no matrix power has a group divisor. Such orderings appear frequently in derived algebras in the type 5 case. This suggests that aprimal algebras might decompose into simple type 1 and 2 algebras and aperiodic algebras. A stronger conjecture substitutes "matrix

powers of semilattices" for "aperiodic algebras". Counting type 2 factors in decompositions leads to a nontrivial complexity theory for aprimal finite algebras.

Algebras recognize languages by way of programs over algebras, generalizing Barrington's programs over semigroups. The notions of division, matrix power, and wreath product (slightly modified) give an algebraic analogue of oracle reduction of languages. Hence part (perhaps all) of NC^1 circuit complexity theory is a "homomorphic image" of the complexity theory of aprimal algebras.

Contents

Introduction

A fundamental problem in general algebra is classification. As the generality of the structures of interest increases, the likelihood of their being completely understood decreases. We must settle for a partial understanding, which means that we must decide what differences matter and what differences do not. We must decide not what is important for all purposes but only what is important for a particular purpose. This investigation begins with the manifesto that what matters about finite algebras is what they can compute.

An algebra (A, F) can be thought of as a computer in the following way: the elements of A are the data objects—that is, the states which variables range over—and the operations F are the primitive instructions. The algebra is specified in terms of generators (usually finitely many) for F, but what is essential to the algebra is the clone they generate, which is to say the functions that they can compute. This idea has its roots in the idea of an automaton, which is essentially a finite transformation monoid, which is essentially a unary algebra. Most of the basic ideas in this work come from looking at algebras as generalized transformation monoids or generalized automata.

Our first step should be a way of ordering algebras that corresponds to how much they can compute, since that is what we care about. A computer with fewer programs and with fewer data objects should be lower in the ordering, as should a computer made by forgetting (in a consistent way) the difference between certain data objects. This is the ordering of division: (A, F) divides (B, G) if (A, F) is a quotient of a subalgebra of a reduct of (B, G).

We should also have ways of building large computers out of small ones. The main construction tools are wreath product and matrix power. The wreath product idea appears in both automata and group theory. The automata version is the one that finds its place here. Wreath products model sequential computation. The paradigmatic example is base 10 arithmetic, in which calculation of digits of higher significance depends on the calculations with digits of lower significance. The matrix power idea comes (by way of tame congruence theory) from rings of matrices but also has a computational significance. Matrix powers are not sequential, which means that data flows in both directions between coordinates, and hence are a model for parallel processing.

These tools, taken together, do lead to a classification of finite algebras, via what John Rhodes calls a global theory. In general, a global decomposition theory uses some set of constructions to build all objects of interest out of

primary objects, which are not built out of any smaller objects. An initial classification arises from considering which primary objects are pieces of a given object. In other words, we study classes which are closed under the constructions and which exclude certain primary objects. A more refined classification comes from asking how many pieces and what kinds of pieces we need to build objects. In other words, we use our constructions to build new classes out of the classes defined by exclusion. Determining which such classes an algebra belongs to is a way of measuring the complexity of the algebra.

The constructions we use for a global theory of algebras are wreath product, matrix power, and division. Many of the basic building blocks of global semigroup decomposition theory reappear here—simple groups and two-element semigroups—but a complete list is not known. Two of the classes defined by excluding certain of these primes, the classes of solvable and of strongly solvable algebras, were originally studied in tame congruence theory. Two new classes, of aprimal and of aperiodic algebras, are rich with examples; their global decomposition theories promise to be interesting.

Chapter 0

Preliminaries

This list of definitions is not intended to be complete but rather to supplement the standard definitions found in many textbooks (see, for example, [4] or [12]). The variations should be noted carefully. Most are not dictated by personal preference but are derived from the particular subject matter in the chapters ahead.

0.1 Sets, functions, and relations

Functions are usually written to the right of their arguments; parentheses are used to group complex expressions for the argument or function and may be omitted in simple cases; composition is from left to right and is denoted by juxtaposition or by $\cdot$ when required for clarity.

The product operation on sets is denoted $\times$; the projection $A^i \to A$ on the j-th factor is denoted $\pi_{i,j}$. Given functions $f : A \to B$ and $g : A \to C$, we use $f \times g$ to mean the product map $A \to B \times C$, which sends $a \mapsto (af, ag)$. For $f : A \to B$ and $g : A' \to C$, we use (f, g) to mean the map $A \times A' \to B \times C$ which sends $(a, a') \mapsto (af, a'g)$.

A relation $R \subseteq A \times B$ is *fully defined* if for all $a \in A$ there is a $b \in B$ such that aRb; R is *injective (from A to B)* if aRb and $a'Rb$ together imply $a = a'$. The inverse of R, that is, $\{(x, y) : yRx\}$ is denoted R^{-1}. If $R \subseteq A^2$, then a *block* of R is a subset $X \subseteq A$ such that $X^2 \subseteq R$ and no larger set has this property. If R is an equivalence relation, the blocks of R are the equivalence classes.

A variable representing an n-tuple is written with an overbar, and its components are accessed with subscripts: for example, $\bar{a} \in A^n$ means $\bar{a}$ is an n-tuple of elements of A and $\bar{a} = (a_1, \ldots, a_n)$. We sometimes (abusively) write $(\bar{a}, \bar{b})$ for $((a_1, b_1), ..., (a_n, b_n))$ and aRb for $a_1Rb_1, \ldots, a_nRbn$, and so on. Juxtaposition of sequences means concatenation:

$$(a, b, ...)(p, q, ...) = (a, b, ..., p, q, ...),$$

and

$$(a, b, ...)^n = (a, b, ...)(a, b, ...)...(a, b, ...) \text{ (n times).}$$

0.2 Operations, clones, and algebras

Some of the definitions here are not standard. They belong to an approach to general algebra known as non-indexed algebra. This approach is used here because it is the most natural setting in which to think of algebras as "n-ary transformation monoids." This fiction yields most of the definitions in Chapter 1.

An *operation* on a set A is simply a function $A^n \to A$ for some $n \geq 0$. The number n is known as the *arity* of the operation. A *clone* is a collection F of operations on a set A such that (i) F includes all projection maps $\pi_{n,i}$ and (ii) F is closed under composition, that is, whenever $f_1, \ldots, f_n : A^m \to A$ and $g : A^n \to A$ are all in F, the m-ary operation $(f_1 \times \ldots \times f_n)g$ is also in F. For $n \geq 0$, F_n denotes the set of n-ary opertions in F. We call F *n-ary* (or *essentially n-ary*) if F is generated (under (i) and (ii) of the definition of clone) by F_n. A *subclone* of F is a clone G such that $G \subseteq F$.

An *algebra* is a pair (A, F) where F is a clone of operations on A. Elements of F are referred to as *operations* of (A, F); A is called the *universe* of (A, F). (Note that, under these conventions, a semigroup is equal to its opposite semigroup, even though the two need not even be isomorphic in the ordinary sense.) In describing the universe of an algebra, we sometimes use the usual definition of an ordinal n as the set $\{0, \ldots, n-1\}$.

We frequently express a clone in terms of generators: if $f, g, \ldots$ are operations on A and $F, G, \ldots$ are sets of operations on A, the notation $(A, f, g, \ldots, F, G, \ldots)$ means the algebra whose clone is generated by $\{f, g, \ldots\} \cup F \cup G \cup \ldots$. When we need to explicitly refer to the clone of an algebra specified in this way, we use the notation Clo (A, F) or Clo$_n$ (A, F) for just the n-ary members of Clo (A, F). Note that, under our convention, $(A, \emptyset)$ means the algebra whose clone is the least clone on A, that is, the clone consisting precisely of the projections. These algebras are sometimes referred to as sets.

An algebra is called *primal* if its clone is the clone of all operations on the universe; the primal algebra with universe A is denoted (A, P_A). We use the notations F_A, S_A, and C_A to denote the set of all unary functions, permutations, and constant maps, respectively, on A. If $a \in A$, then c_a denotes the constant map $A \to A$ with value a. Operations of (A, F, C_A) are called *polynomials* of the algebra (A, F); the clone they form is denoted Pol (A, F); the set of n-ary members of this clone is denoted Pol$_n$ (A, F). An algebra (A, F) is called *polynomially complete* if $(A, F, C_A) = (A, P_A)$. We say that (A, F) and (A, G) are *polynomially equivalent* if Pol $(A, F) =$ Pol (A, G).

0.3 Subalgebras, reducts, quotients, and products

Let (A, F) be an algebra. For $X \subseteq A$, we use XF to denote the image of X under the operations in F, that is $XF = \{(a_1, \ldots, a_n)f : a_1, \ldots, a_n \in A, f \in F_n \text{ for some } n\}$. If F is a clone, $(XF)F = XF$, and XF is known as the *subuniverse* generated by X under the action of F. A *subalgebra* of (A, F) is an algebra (B, F) with $B \subseteq A$ and $BF = B$. A *reduct* of (A, F) is an algebra (A, G) with $G \subseteq F$. If $X \subseteq A$, then we set $F|_X = \{f|_X : f \in F_n \text{ for some } n \text{ and } X^n f \subseteq X\}$. Here, $f|_X$ denotes the usual restriction of f to X^n, which is in general a function $X^n \to A$. Note that $(X, F|_X)$ is a subalgebra of a reduct of (A, F); in fact it has the largest clone of any subreduct of (A, F) with universe X. The *induced* algebra of (A, F) on a subset X is the algebra $(X, (\text{Pol } (A, F))|_X)$, which we sometimes denote by $(A, F)|_X$.

A *homomorphism* from (A, F) to (B, G) is a pair (φ, ψ) where $\varphi : A \to B$ and ψ is a sequence of maps $\psi_0 : F_0 \to G_0, \psi_1 : F_1 \to G_1, \ldots$ such that for each $n \geq 0$ and $a_1, \ldots, a_n \in A$, we have

$$(a_1, \ldots, a_n)f\varphi = (a_1\varphi, \ldots, a_n\varphi)(f\psi_n).$$

In this case, we write $(\varphi, \psi) : (A, F) \to (B, G)$. In practice, subscripts on the ψ_n are omitted, and just one letter is used for both φ and ψ. An *isomorphism* is, as usual, an invertible homomorphism. We say (A, F) *embeds* in (B, G) and write $(A, F) \leq (B, G)$ if (A, F) is isomorphic to a subreduct of (B, G).

If $\varphi : (A, F) \to (B, G)$ is a homomorphism, then its *kernel*, $\ker \varphi$, is the binary relation $\{(x, y) \in A^2 : x\varphi = y\varphi\}$. The binary relations obtained in this way are called *congruences*; the set of congruences of (A, F) is denoted by $\text{Con } (A, F)$. Alternately, a congruence is a reflexive, symmetric, transitive binary relation θ on A such that whenever $x_1 \theta y_1, \ldots, x_n \theta y_n$ and $f \in F_n$ we have $(x_1, \ldots, x_n)f\theta(y_1, \ldots, y_n)f$. Given $\theta \in \text{Con } (A, F)$, $a \in A$, and $f \in F_n$, we let $a/\theta = \{a' : a\theta a'\}$ and $A/\theta = \{a/\theta : a \in A\}$; we define $f/\theta : (A/\theta)^n \to A/\theta$ by $(a_1/\theta, \ldots, a_n/\theta)(f/\theta) = ((a_1, \ldots, a_n)f)/\theta$; and we let $F/\theta = \{f/\theta : f \in F\}$. The maps $x \mapsto x/\theta$ and $f \mapsto f/\theta$ describe a homomorphism $\varphi : (A, F) \to (A/\theta, F/\theta)$ with $\ker \varphi = \theta$. We call $(A/\theta, F/\theta)$ the *quotient by* θ or the *quotient modulo* θ of (A, F).

The *non-indexed* product of algebras (A, F) and (B, G) is the algebra $(A, F) \times (B, G) = (A \times B, F \times G)$, where $A \times B$ is the usual product of sets and $(F \times G)_n = \{(f, g) : f \in F_n, g \in G_n\}$ (one easily checks that $F \times G$ is a clone—it is in fact the product of F and G in the category of clones). Note that $(A, F) \leq (A, F) \times (B, G)$ and, symmetrically, $(B, G) \leq (A, F) \times (B, G)$. (To see this, note that $(A, F) \cong (A, F) \times (b, \emptyset)$ for any $b \in B$ and the latter algebra is a subreduct of the full product.)

The k-th non-indexed power of (A, F) is denoted $(A, F)^k$. The usual direct product of algebras is not definable in the non-indexed setting. Nevertheless, the k-th direct power may be defined as $(A^k, (f, \ldots, f) : f \in F)$, where $(f, \ldots, f)$

acts coordinatewise, i.e.,

$$((a_{1,1},\ldots,a_{1,k}),\ldots,(a_{n,1},\ldots,a_{n,k}))(f,\ldots,f)$$
$$=((a_{1,1},\ldots,a_{n,1})f,\ldots,(a_{1,k},\ldots,a_{n,k})f),$$

assuming the arity of f is n. This algebra is denoted by (A^k,F). Note that $(A^k,F)\leq(A,F)^k$. Use of the same letter for the clone of an algebra and of its direct powers is abusive, but it is acceptable because these clones are isomorphic. For notational simplicity, we are being vague about whether F is a collection of specific operations on A or an abstract entity which is "represented on" A by means of some functor.

Similar reasoning justifies the following conventions:

1. Suppose $B\subseteq A$ and $BF=B$. Then (B,F) is shorthand for $(B,F|_B)$, the subalgebra of (A, F) with universe B.

2. Suppose $\theta\in$ Con (A,F). Then $(A/\theta,F)$ is shorthand for $(A/\theta,F/\theta)$, the quotient algebra of (A,F) by θ.

Chapter 1

The Covering Lemma

This chapter owes an enormous debt to Bret Tilson, whose 1987 paper "Categories as algebra: An essential ingredient in the theory of monoids" presents the ideas leading up to his original version of the covering lemma. His setting is the "one-sided" decomposition theory of monoids: the theory of decompositions using the standard wreath product of monoids. This is essentially a decomposition theory of transformation monoids (tms), though Tilson's presentation is in terms of abstract monoids. The concepts in this chapter result from viewing unary algebras as tms in the obvious way and boosting the definitions up into higher arities. The concrete approach (transformations or operations on a set) has some advantages over the abstract approach Tilson used: the concrete wreath product is associative, and the covering lemma is essentially a biconditional.

1.1 Relational morphisms of algebras

Definition A *relation* φ between algebras (A, F) and (B, G) is a subreduct of their non-indexed product, that is, $\varphi \leq (A, F) \times (B, G)$. If $a \in A$ and $b \in B$, we write $a\varphi b$ just when (a, b) belongs to the universe of φ. If $f \in F_n$ and $g \in G_n$, we write $f\varphi g$ just when (f, g) is an n-ary operation of φ. A *relational morphism* φ from (A, F) to (B, G) is a relation between (A, F) and (B, G) which is *fully defined* (on (A, F)), that is, which satisfies

1. for each $a \in A$ there is a $b \in B$ such that $a\varphi b$; and
2. for each $f \in F$ there is a $g \in G$ such that $f\varphi g$.

In this case, we write $\varphi : (A, F) \to (B, G)$.

Note that a relational morphism is a homomorphism just when its universe is a function. Relational morphisms can be thought of as many-valued homomorphisms. One can define a relational morphism from (A, F) to (B, G) as a homomorphism to the power algebra of (B, G) (excluding the empty element).

To define a relation $\varphi \leq (A, F) \times (B, G)$, we typically specify a set X of pairs of elements and a set Y of pairs of operations which together generate φ. For this relation to be a relational morphism, the following must hold:

1. $\{a : (a, b) \in X \text{ for some } b\}$ generates A under the action of F; and
2. $\{f : (f, g) \in Y \text{ for some } g\}$ generates F.

Definition If $\varphi \leq (A, F) \times (B, G)$, then φ^{-1} denotes the relation, called the *inverse* of φ, between (B, G) and (A, F) such that

1. for each $(a, b) \in A \times B$, $b\varphi^{-1}a$ if and only if $a\varphi b$; and
2. for each $(f, g) \in F \times G$, $g\varphi^{-1}f$ if and only if $f\varphi g$.

Also, we define $a\varphi = \{b : a\varphi b\}$, $f\varphi = \{g : f\varphi g\}$.

Note that the inverse of a homomorphism is, in general, a relation of algebras. Such relations, when fully defined, are typical examples of injective relational morphisms, defined below.

Definition A relational morphism $\varphi : (A, F) \to (B, G)$ is said to be *injective* if, whenever $a \neq a' \in A$, we have $a\varphi \cap a'\varphi = \emptyset$. We say that φ is *surjective* if $b\varphi^{-1} \neq \emptyset$ for all $b \in B$ and $g\varphi^{-1} \neq \emptyset$ for all $g \in G$

One can easily show that an injective relational morphism is also injective on operations, in the sense that, whenever $f \neq f' \in F$, we have $f\varphi \cap f'\varphi = \emptyset$.

1.2 Many-sorted algebras and division

A many-sorted algebra is essentially a concrete category with finite products, that is, a category with finite products together with a functor, preserving finite products, from it to the category of sets and functions. A one-sorted algebra is a concrete category with finite products such that every object is a finite power of a single base object. Keeping this in mind will help the reader make sense of the upcoming definitions.

Definition A *many-sorted algebra (msa)* is an indexed family of the form $\mathbf{A} = (A_i : i \in I; F_{\bar{\imath},j} : \bar{\imath} \in I^n, n \geq 0, j \in I)$, where

1. I is a set, called the *index set* of the msa,
2. for $i \in I$, A_i is a set, referred to as the *sort* (or *universe*) indexed by i,
3. for $\bar{\imath} = (i_1, \ldots, i_n) \in I^n$ and $j \in I$, $F_{\bar{\imath},j}$ is a set of functions $A_{i_1} \times \cdots \times A_{i_n} \to A_j$, known as the *(n-ary) operations of signature* $\bar{\imath} \to j$,
4. if $i_m = j$ (notation as above) for some m then $F_{\bar{\imath},j}$ includes the m-th projection operation, denoted $\pi_{\bar{\imath},i_m}$ or simply $\pi_{\bar{\imath},m}$, and

5. if $g \in F_{\bar{\jmath},k}$, $\bar{\jmath} = (j_1, \ldots, j_n) \in I^n$, $\bar{\imath} \in I^m$, and $f_1 \in F_{\bar{\imath},j_1}$, $\ldots$, $f_n \in F_{\bar{\imath},j_n}$, then $(f_1 \times \cdots \times f_n)g \in F_{\bar{\imath},k}$.

A msa is called *finite* if its set of sorts is finite and each sort is itself finite (and hence the set of operations of a particular signature is finite). A *local algebra* of the above msa is an algebra of the form (A_i, G) where $G_n = F_{(i,\ldots,i),i}$ for each n. This algebra is sometimes denoted by $\mathbf{A}_i$ or by $\mathbf{A}|_i$. If a msa has just one sort, we identify the msa with its unique local algebra.

Notation (i) We will frequently use the set of sorts itself as the index set. (ii) As with algebras, we define the operations of a msa by specifying generators. Therefore $(A_1, A_2, \ldots; \emptyset)$ means the msa with sorts $A_1, A_2 \ldots$ and no operations but the various projection operations required by the definition (these operations are easily seen to be closed under composition).

Remark Index sets are used here primarily to eliminate one level of subscripts from the notation. They are not preserved by morphisms of msas.

An important way of comparing msas is division, which Tilson invented for categories (without representation or product structure). Actually, a division is a special kind of relational morphism of msas, which is a special kind of relation of msas, which is a subreduct of a product of msas. Since none of these other concepts are needed in this work, we define division directly.

Definition A *division* from a msa $\mathbf{A} = (A_i : i \in I; F_{\bar{\imath},j} : \bar{\imath} \in I^n, n \geq 0, j \in I)$ to a msa $\mathbf{B} = (B_k : k \in K; G_{\bar{k},l} : \bar{k} \in K^n, n \geq 0, l \in K)$ is an aggregate $\mathbf{\Delta} = (\delta, \delta_i : i \in I, \delta_{\bar{\imath},j} : \bar{\imath} \in I^n, n \geq 0, j \in I)$ such that

1. δ is a function from I to K,
2. δ_i is a fully defined, injective relation from A_i to $B_{i\delta}$,
3. $\delta_{\bar{\imath},j}$ is a fully defined, injective relation from $F_{\bar{\imath},j}$ to $G_{\bar{\imath}\delta,j\delta}$,
4. whenever $\bar{\imath}\delta\bar{k}$ (that is, $i_1\delta k_1, i_2\delta k_2, \ldots i_n\delta k_n$), we have $\pi_{\bar{\imath},m}\delta_{\bar{\imath},i_m}\pi_{\bar{k},m}$,
5. whenever $a_1\delta_{i_1}b_1, \ldots, a_n\delta_{i_n}b_n$, and $f\delta_{\bar{\imath},j}g$, we have $\bar{a}f\delta_j\bar{b}g$, and
6. whenever $f_1\delta_{\bar{\imath},j_1}g_1, \ldots, f_n\delta_{\bar{\imath},j_n}g_n$, and $f_0\delta_{\bar{\jmath},j\prime}g_0$, we have $\bar{f}f_0\delta_{\bar{\imath},j\prime}\bar{g}g_0$.

In this situation, we write $\mathbf{\Delta} : \mathbf{A} \prec \mathbf{B}$. In general, we say that $\mathbf{A}$ *divides* $\mathbf{B}$, or $\mathbf{A}$ is a *divisor* of $\mathbf{B}$, written $\mathbf{A} \prec \mathbf{B}$, if there exists a division $\mathbf{\Delta} : \mathbf{A} \prec \mathbf{B}$.

If the δ_i and $\delta_{\bar{\imath},j}$ are in fact functions, we say that $\mathbf{A}$ *embeds in* $\mathbf{B}$ and write $\mathbf{A} \leq \mathbf{B}$.

Notation By convention, we frequently omit the subscripts from the components of a division, and just use one letter, δ, say, for the entire division. For example, this permits us to rewrite (5) above as:

5'. whenever $\bar{a}\delta\bar{b}$ and $f\delta g$, we have $\bar{a}f\delta\bar{b}g$.

Note that here we are also using the convention, established in (Chapter 0) under which $\bar{a}\delta\bar{b}$ means $a_1\delta b_1, \ldots, a_n\delta b_n$. This convention is suggested by the categorial approach to msas and divisions.

Remark about defining divisions. As long as δ satisfies (1)-(5) above, the closure of δ under compositions as in (6) will still satisfy (1)-(5), as well as (6). Therefore, we usually don't bother to check (6). Also, we needn't check that the $\delta_{\bar{\imath},j}$ relations are injective (condition (3)), since this is implied by the other conditions: if two distinct operations of the same signature have a common δ-image it is easy to show (using (2) and (5)) that there are distinct elements in some sort which have a common δ-image.

Just as one-sorted msas may be identified with algebras, divisions of one-sorted msas may be identified with injective relational morphisms. Since an injective relational morphism is just the inverse of a surjective homomorphism defined on a subreduct, we have

Proposition 1 $(A, F) \prec (B, G)$ *iff* (A, F) *is a quotient of a subreduct of* (B, G).□

Also, the notion of embedding in the definition of division is consistent with the meaning of "embed" introduced for algebras in Chapter 0: (A, F) is isomorphic to a subreduct of (B, G) iff there is an embedding in the sense just defined.

Definition When $\mathbf{A}$ and $\mathbf{B}$ are msas such that $\mathbf{A} \prec \mathbf{B}$ and $\mathbf{B} \prec \mathbf{A}$, we say that $\mathbf{A}$ and $\mathbf{B}$ are *divisionally equivalent*, written $\mathbf{A} \sim \mathbf{B}$. If $\mathbf{A}$ is divisionally equivalent to a trivial algebra, then we say that $\mathbf{A}$ is *divisionally trivial*.

Proposition 2

1. *For finite algebras, divisional equivalence is the same as isomorphism:*

$$(A, F) \sim (B, G) \Leftrightarrow (A, F) \cong (B, G).$$

2. $\mathbf{A}$ *is divisionally trivial iff each sort of* $\mathbf{A}$ *is a singleton.* □

In general, divisionally equivalent msas are not isomorphic and need not even have the same number of sorts. However their local algebras are related by the following.

Proposition 3 *If* $\delta : \mathbf{A} \prec \mathbf{B}$*, then for each index* i *of* $\mathbf{A}$*,* $\mathbf{A}_i \prec \mathbf{B}_{i\delta}$*. Hence,* $\mathbf{A} \sim \mathbf{B}$ *implies each* $\mathbf{A}_i$ *divides some* $\mathbf{B}_j$ *and vice versa.* □

Warning It does not follow from $\mathbf{A} \sim \mathbf{B}$ that each $\mathbf{A}_i$ is divisionally equivalent to some $\mathbf{B}_j$. Also, the converse of the proposition is not true: let $\mathbf{A} = (\{0\}, \{1, 2\}; \emptyset)$ and $\mathbf{B} = (\{0\}, \{1, 2\}; f_1, f_2)$ where $f_i : \{0\} \to \{1, 2\}$ is the

constant map with value i. Then $\mathbf{A}_{\{0\}} = \mathbf{B}_{\{0\}} = (\{0\}, \emptyset)$ and $\mathbf{A}_{\{1,2\}} = \mathbf{B}_{\{1,2\}} = (\{1,2\}, \emptyset)$. However, $\mathbf{B}$ has two distinct unary operations of signature $\{0\} \to \{1,2\}$, whereas $\mathbf{A}$ has no pair of distinct unary operations having the same signature. This implies that there is no division $\mathbf{B} \prec \mathbf{A}$.

This example is familiar to monoid theorists. However, contrary to monoid theory, there are divisionally nontrivial algebras which $\mathbf{B}$ does not divide, such as $(\{0,1\}, \emptyset)$. The latter is (up to isomorphism) the smallest divisionally nontrivial algebra and is, furthermore, (up to divisional equivalence) the smallest divisionally nontrivial msa.

1.3 The derived algebra of a relational morphism

The derived algebra (msa, actually) of a relational morphism is a sort of kernel, analogous with the normal subgroup kernel of a homomorphism of groups. Unlike the kernel congruence in universal algebra, however, it has an algebraic structure that is typically weaker than the domain algebra. As in group theory, it is useful to think of the kernel as encapsulating the information "lost" by the morphism. The purpose of division is to make these vague measurements precise.

Definition Suppose $\varphi : (A, F) \to (B, G)$ is a relational morphism. The *derived algebra* of φ, denoted by D_φ, is a msa whose set of sorts is indexed by B. The sort with index $b \in B$ is the set $\{(a, b) : a \in A, a\varphi b\}$. For $\bar{b} \in B^n$ and $b_0 \in B$, operations of signature $\bar{b} \to b_0$ are given by triples $(f, g, \bar{b})$ with $f \in F_n, g \in G_n, f\varphi g$, and $\bar{b}g = b_0$. The action of $(f, g, \bar{b})$ on pairs $(\bar{a}, \bar{b})$ with $\bar{a}\varphi\bar{b}$ follows the rule

$$(\bar{a}, \bar{b})(f, g, \bar{b}) = (\bar{a}f, \bar{b}g) = (\bar{a}f, b_0).$$

The operations specified in the definition are easily seen to be closed under compositions. The next lemma shows that the clone of the derived algebra is generated by triples formed from the pairs which generate the morphism. This fact will be used frequently and without mention in subsequent descriptions of derived algebras.

Lemma 4 *Suppose $\varphi : (A, F) \to (B, G)$ is a relational morphism. Let X generate the operations of φ. Then the operations of D_φ are generated by the set of triples of the form $(f, g, \bar{b})$ with $(f, g) \in X$.* □

Warning about indexing the derived algebra

In the setting of indexed algebras, we could define, in the obvious way, an indexed derived algebra. (Associated with an n-ary symbol f and the n-tuple of sorts $(b_1, \ldots, b_n)$ is an n-ary operation from those sorts to the sort $(b_1, \ldots, b_n)f^B \ldots$.) One could then speak of the identities satisfied by the derived algebra and easily show that these identities would include those satisfied by (A, F). However, one can find a finite group G with an abelian normal

subgroup N such that the derived algebra of the quotient morphism does not satisfy the abelian law. To do this, it is sufficient that there is an inner automorphism of G that is not the identity map on N. For then there are $g \in G$ and $n \in N$ such that $ng \neq gn$. It follows that the binary multiplication operation $Ng \times Ng \to Ng^2$, which sends $(ng, 1g) \mapsto ngg$ and $(1g, ng) \mapsto gng$, is not abelian.

Additionally, there is a finite semigroup S with an ideal I which is in fact a group such that the derived algebra of the quotient morphism does not satisfy any identity of the form $xx^n = x$ with $n > 0$. In this case, it suffices that the semigroup not be a union of groups.

By contrast, we will see in later chapters that the derived algebra in the first example, stripped of indexing information, divides the abelian group N with certain added unary operations. This new algebra is abelian in the sense of universal algebra (see [8]). In the second example, the nonindexed derived algebra divides the group I with certain added unary operations, and these added operations do not interfere with such propertiers as being abelian or solvable.

The conclusion I draw from these examples is that the indexing information should not be included in the derived algebra, because this information "remembers" too much about the domain algebra. The derived algebra should remember no more than does the kernel of a group homomorphism.

The following lemma has a trivial proof, but it says something important: the operations at a local algebra of D_φ correspond to the operations of G which "stabilize" elements of B.

Lemma 5 *In the notation of the previous lemma, the operations of the local algebra at b are just the triples $(f, g, (b, \ldots, b))$ where $f\varphi g$ and $(b, \ldots, b)g = b$.*□

Proposition 6 *Suppose $\varphi : (A, F) \to (B, G)$ is a relational morphism. Then:*

1. *$D_\varphi \leq (A, F)$.*
2. *If φ is injective, D_φ is divisionally equivalent to a trivial algebra.*
3. *If (B, G) is trivial, then $D_\varphi \cong (A, F)$.*

Proof. For (1), define a relation δ from D_φ to (A, F) by $(a, b)\delta a$ and $(f, g, b)\delta f$. It is easy to see that δ is closed, is fully defined, and is an injective function on each sort. Part (2) follows from the observation that $|b\varphi^{-1}| = 1$ for all $b \in B$. For (3), note that if (B, G) is trivial, then D_φ is isomorphic to (A, F) via the division in (1). □

Lemma 7 *Suppose $\varphi : (A, F) \to (B, G)$ and $\varphi' : (A, F) \to (B', G')$ are relational morphisms with $(B', G') \leq (B, G)$ and $\varphi' \leq \varphi$. Then $D_{\varphi'} \prec D_\varphi$.* □

This lemma is often used when we are given a set $\{f_1, f_2, \ldots\}$ which generates F and a set $\{g_1, g_2, \ldots\} \subseteq G$ such that $f_1\varphi g_1, f_2\varphi g_2, \ldots$, in which case we can obtain a morphism φ' generated by $\{(f_1, g_1), (f_2, g_2), \ldots\}$ without making the image algebra or the derived algebra of φ' any larger than those of φ. In particular, in the decomposition theory of an algebra with one basic operation we need consider only relational morphisms to algebras with one basic operation. Also, we can use this lemma to assume that relational morphisms are surjective both on elements and on operations.

1.4 The wreath product

Definition Let (C, H) and (B, G) be algebras. Their wreath product, denoted $(C, H) \circ (B, G)$, is the algebra with universe $C \times B$ having, for each n, each $\bar{h} \in H_n^{B^n}$, and each $g \in G_n$, an n-ary operation $(\bar{h}, g)$, which acts by

$$(\bar{c}, \bar{b})(\bar{h}, g) = (\bar{c}(\bar{b}\bar{h}), \bar{b}g).$$

It is easy to see that these operations form a clone. This clone is written $H \circ_B G$, and so $(C, H) \circ (B, G)$ can be written $(C \times B, H \circ_B G)$.

Lemma 8 *Suppose $|B|$ is finite.*

1. *$H \circ_B G$ is generated by the following list of operations:*
   (a) *each $(\bar{h}, g)$ where $\bar{h} : B^n \to H_n$ is a constant function, and*
   (b) *for each $b \in B$, the ternary operation q_b defined by*

$$((y_1, x_1), (y_2, x_2), (y_3, x_3))q_b = \begin{cases} (y_2, x_1) & \text{if } x_1 = b \\ (y_3, x_1) & \text{otherwise.} \end{cases}$$

2. *If H and G are finitely generated, then $H \circ_B G$ is finitely generated.* □

Sketch of proof. For (1), let $(\bar{h}, g) \in (H \circ_B G)_n$. Write $B = \{b_1, b_2, \ldots b_m\}$. To construct $(\bar{h}, g)$ in terms of the specified operations, first use the q_b operations to construct the m^n-ary operation

$$((y_1, x_1), \ldots, (y_{m^n}, x_{m^n})) \mapsto \begin{cases} (y_1, x_1) & \text{if } x_1 = b_1, x_2 = b_1, \ldots, x_n = b_1 \\ (y_2, x_1) & \text{if } x_1 = b_2, x_2 = b_1, \ldots, x_n = b_1 \\ (y_3, x_1) & \text{if } x_1 = b_3, x_2 = b_1, \ldots, x_n = b_1 \\ \vdots & \vdots \\ (y_{m^n}, x_1) & \text{if } x_1 = b_m, x_2 = b_m, \ldots, x_n = b_m \end{cases}$$

Next, compose this with the operations of the form $(x_1, \ldots, x_n)\bar{h}$, substituting $(b_1, \ldots, b_1)\bar{h}$ for y_1, and so on. Choose some operation of the form $(\ldots, g)$ and put this together with the result of the previous composition using the binary decomposition operation

$$(\pi_1, \pi_2) : ((y_1, x_1), (y_2, x_2)) \mapsto (y_1, x_2).$$

For (2), observe that the operations in part (a) of the list in (1) are generated by a finite sublist:

1. each $(\bar{h}, \pi_1)$ where $\bar{h}$ is a constant with value a generator of H,
2. each (π_1, g) where $g \in G$, and
3. the binary decomposition operation (π_1, π_2).

The operations of part (b) are finite in number because $|B|$ is finite. □

Remark The first collection of operations is just the set of operations of the non-indexed product $(C, H) \times (B, G)$.

Two points bear thinking about here. First, the wreath product is an essentially non-indexed kind of product. Applying the wreath product to pairs of algebras drawn from two varieties produces a class of algebras that is not even contained in a variety. (The number of operations in $H \circ_B G$ grows with $|B|$.) However, there is a related product that is defined on varieties. Also, the wreath product is defined on hypervarieties. This is investigated in Chapter ???

Second, algebras isomorphic to a wreath product are clearly very special. (We examine their congruences and other structural properties in the next chapter.) Therefore, we cannot expect wreath decompositions to lead to any sort of classification up to isomorphism. We will instead classify algebras using the relation of division. This relation is extremely broad; its looseness will pose a serious problem when we consider such algebras as lattices, nonsolvable groups and semigroups, Boolean algebras, and so on.

This difficulty will lead us to study the class of aprimal algebras which excludes these algebras. A more general theory may require a more sophisticated product which can be applied directly to msas (possibly as in Tilson's recent research) or a finer notion to replace reduct or both.

The wreath product defined here is closely related to the various products considered by semigroup theorists. We may, as mentioned earlier, identify unary algebras with transformation monoids: the unary algebra (A, F) corresponds to the transformation monoid $(A, \mathrm{Clo}_1\ (A, F))$; the wreath product of unary algebras corresponds to the wreath product of tms. The wreath product of algebras is also related, but in a less straightforward way, to the "two-sided" products of semigroups. We may simulate the double semidirect product (and therefore the block product as well) as follows. Let $(S, +)$ and $(T, \cdot)$ be semigroups (the $+$ is not necessarily commutative). Let α be a double action of T on S. (For details, see [Rhodes-Tilson].) Then the double semidirect product of $(S, +)$ and $(T, \cdot)$ is

$$(S, +) * *_\alpha (T, \cdot) = (S \times T, ((s, t), (s', t')) \mapsto (st' + ts', tt')),$$

where st' denotes the result of t' acting on the right of s, and so on. This is easily expressed as a subreduct of

$$(S, +, x \mapsto xt : t \in T, x \mapsto tx : t \in T) \circ (T, \cdot).$$

The first algebra is not a semigroup but rather a semigroup with added unary operations that happen to be endomorphisms. This topic is explored further in Chapter 7, which includes a version of the Krohn-Rhodes theorem based not on the above simulation but on more straightforward decompositions obtained by adding polynomial operations.

The wreath product of algebras is also related to the shift product defined by McKenzie in [8], which is a reduct of the wreath product.

Observe that wreath product is sequential, that is, the right-hand coordinate of the output of an operation depends only on the right-hand coordinates of the inputs and the right-hand coordinate of the operation itself, whence the next proposition.

Proposition 9 *The projection map $C \times B \to B$ induces a homomorphism $\pi : (C, H) \circ (B, G) \to (B, G)$.* □

It is easy to show that there is, in general, no projection morphism onto the left factor. (In fact, in the next chapter we will determine the congruence lattice of a wreath product and see that all congruences are comparable with $\ker \pi$.) Therefore, we may safely refer to π as *the projection homomorphism* of $(C, H) \circ (B, G)$.

Proposition 10 *The wreath product is a monoid operation on isomorphism classes of algebras, with the identity element represented by a trivial algebra:*

1. $(1, \emptyset) \circ (A, F) \cong (A, F) \circ (1, \emptyset) \cong (A, F)$.
2. $((C, H) \circ (B, G)) \circ (A, F) \cong (C, H) \circ ((B, G) \circ (A, F))$.

Proof. The proof of (1) is left to the reader. The proof of (2) is messy but not hard. An n-ary operation of $((C, H) \circ (B, G)) \circ (A, F)$ is given by a pair $(\bar{h} \times \bar{g}, f)$ with $\bar{h} \times \bar{g} \in (H_n^{B^n} \times G_n)^{A^n}, \bar{h} \in (H_n^{B^n})^{A^n}, \bar{g} \in G_n^{A^n}$, and $f \in F_n$. This operation acts by the rule

$$((\bar{c}, \bar{b}), \bar{a})(\bar{h} \times \bar{g}, f) = ((\bar{c}, \bar{b})(\bar{a}(\bar{h} \times \bar{g})), \bar{a}f) = ((\bar{c}(\bar{b}(\bar{a}\bar{h})), \bar{b}(\bar{a}\bar{g})), \bar{a}f).$$

An n-ary operation of $(C, H) \circ ((B, G) \circ (A, F))$ is given by a pair $(\bar{k}, (\bar{g}, f))$ with $\bar{k} \in H_n^{(B \times A)^n}, \bar{g} \in G_n^{A^n}$, and $f \in F_n$. This operation acts by the rule

$$(\bar{c}, (\bar{b}, \bar{a}))(\bar{k}, (\bar{g}, f)) = (\bar{c}((\bar{b}, \bar{a})\bar{k}), (\bar{b}(\bar{a}\bar{g}), \bar{a}f)).$$

The isomorphism is given by the following maps:

$$((c, b), a) \mapsto (c, (b, a))$$

$$(\bar{h} \times \bar{g}, f) \mapsto (\bar{k}, (\bar{g}, f)),$$

where $(\bar{b}, \bar{a})\bar{k} = \bar{b}(\bar{a}\bar{h}))$. □

The wreath product is not in general commutative, as one can easily show by example (or by the fact that only one of the projection functions induces a homomorphism).

Proposition 11 *The wreath product has the following additional properties.*

1. $(C,H)\times(B,G)$ *is a reduct of* $(C,H)\circ(B,G)$*, and hence* (C,H) *and* (B,G) *are both subreducts of* $(C,H)\circ(B,G)$*.*
2. $(C,H)\leq(C',H')$ *and* $(B,G)\leq(B',G')$ *together imply*
$$(C,H)\circ(B,G)\leq(C',H')\circ(B',G').$$
3. $(C,H)\prec(C',H')$ *and* $(B,G)\prec(B',G')$ *together imply*
$$(C,H)\circ(B,G)\prec(C',H')\circ(B',G').$$
4. $((C,H)\circ(B,G))\times((C',H')\circ(B',G'))$
$$\leq((C,H)\times(C',H'))\circ((B,G)\times(B',G')).$$

Proof. For (1), observe that $(H\times G)_n$ consists of all operations (h,g) of $(H\circ_B G)_n$ such that h is a constant function $B^n\to H_n$. The rest of (1) now follows from the remarks in (???0.2) concerning the non-indexed product. For (2), simply restrict operations of $H'\circ_{B'}G'$ to (the embedded image of) $C\times B$.

We now prove (3). We may assume (C,H) is the quotient mod θ of some subreduct (C'',H'') of (C',H') and (B,G) is the quotient mod ψ of some subreduct (B'',G'') of (B',G'). Let $\theta\times\psi$ denote the equivalence relation $\{((x,y),(u,v)) : x\theta u \text{ and } y\psi v\}$ on $C''\times B''$. Note that $\theta\times\psi$ need not be a congruence on $(C'',H'')\circ(B'',G'')$. In essence, the proof will find a reduct of $(C'',H'')\circ(B'',G'')$ for which $\theta\times\psi$ is a congruence and the quotient by $\theta\times\psi$ is $(C,H)\circ(B,G)$.

We define a division $\delta : (C,H)\circ(B,G)\prec(C'',H'')\circ(B'',G'')$ as follows. First, for $(c,b)\in C\times B$, we define $(c,b)\delta=\{(c',b') : c'/\theta=c, b'/\psi=b\}$. Observe that this is an injective relation from $C\times B$ to $C''\times B''$.

Now, let $(\bar h,g)\in(H\circ_B G)_n$. Choose $g''\in G''_n$ so that $g''/\psi=g$. Define $\bar h'' : B''^n\to H''_n$ as follows. For $(b'_1,\dots,b'_n)\in B''^n$, choose $(b''_1,\dots,b''_n)\bar h''\in H''_n$ so that $((b''_1,\dots,b''_n)\bar h'')/\theta=(b''_1/\psi,\dots,b''_n/\psi)\bar h$. Clearly, $(\bar h'',g'')\in(H''\circ_B G'')_n$. Take $(\bar h,g)\delta(\bar h'',g'')$. (As usual, such δ-related pairs of operations are understood as the generators for all pairs in the relation from $H\circ_B G$ to $H''\circ_{B''}G''$.)

We now check that δ-related elements are preserved by δ-related operations. Suppose $(c_1,b_1)\delta(c''_1,b''_1),\dots,(c_n,b_n)\delta(c''_n,b''_n)$ and $(\bar h,g)\delta_n(\bar h'',g'')$. Then $b_1=b''_1/\psi$, …, $b_n=b''_n/\psi$, so (since ψ is a congruence)
$$(b_1,\dots,b_n)g=((b''_1,\dots,b''_n)g'')/\psi.$$
We also have
$$((b''_1,\dots,b''_n)\bar h'')/\theta=(b''_1/\psi,\dots,b''_n/\psi)\bar h=(b_1,\dots,b_n)\bar h.$$
Therefore,
$$\begin{aligned}((c''_1,\dots,c''_n)(b''_1,\dots,b''_n)\bar h'')/\theta &= (c''_1/\theta,\dots,c''_n/\theta)((b''_1,\dots,b''_n)\bar h'')/\theta\\ &= (c_1,\dots,c_n)(b_1,\dots,b_n)\bar h.\end{aligned}$$

This shows that

$$(\bar{c}, \bar{b})(\bar{h}, g) \; \delta \; (\bar{c}'', \bar{b}'')(\bar{h}'', g'').$$

Since δ is injective, by the observation above, it follows that δ is a division.

To prove (4), we must find an embedding from

$$((C \times B) \times (C' \times B'), (H \circ_B G) \times (H' \circ_B G'))$$

into

$$((C \times C') \times (B \times B'), (H \times H') \circ_{B \times B'} (G \times G')).$$

On elements, the map is $((c, b), (c', b')) \mapsto ((c, c'), (b, b'))$. On n-ary operations, the map is $((\bar{h}, g), (\bar{h}', g')) \mapsto (\bar{k}, (g, g'))$, where $((b_1, b'_1), \ldots, (b_n, b'_n))\bar{k} = ((b_1, \ldots, b_n)\bar{h}, (b'_1, \ldots, b'_n)\bar{h}')$. The map on elements is clearly injective, and routine calculations show that the maps on elements and on operations together form a morphism. □

Lemma 12 *Let $\pi : (C, H) \circ (B, G) \to (B, G)$ be the projection. Each local algebra of D_π is isomorphic to (C, H).*

Proof. Operations of the local algebra with elements $C \times b$ are of the form $(\bar{h}, g, (b, \ldots, b))$, where $(b, \ldots, b)g = b$. So we have an isomorphism $D_\pi|_b \cong (C, H)$ sending $(c, b) \mapsto c$ and $(\bar{h}, g, (b, \ldots, b)) \mapsto (b, \ldots, b)\bar{h}$. □

1.5 The Covering Lemma

The Covering Lemma ties together the concepts of relational morphism, derived algebra, division and wreath product. It does so by saying that the derived algebra of a morphism specifies (via the division preorder) exactly the information needed to reconstruct the domain algebra (up to division) from the image algebra using the wreath product. In the subsequent chapters, the Covering Lemma is used to find decompositions by constructing morphisms and consolidating their derived algebras, which is usually easier than directly finding divisions into a wreath product.

In a sense, the Covering Lemma converts a many-to-many coordinate system (a relational morphism) into a one-to-many coordinate system (a division into a wreath product)....

Lemma 13 (The Covering Lemma) *Let π denote the projection homomorphism $(C, H) \circ (B, G) \to (B, G)$.*

1. *Suppose $\varphi : (A, F) \to (B, G)$ is a relational morphism with $D_\varphi \prec (C, H)$. Then there is a division $\delta : (A, F) \prec (C, H) \circ (B, G)$, and $\delta\pi = \varphi$.*

2. *Suppose $\delta : (A, F) \prec (C, H) \circ (B, G)$. Then $D_{\delta\pi} \prec (C, H)$.*

Proof. (1) Let ε denote the division $D_\varphi \prec (C, H)$. Define the relation δ as follows. For $a \in A$, $b \in B$, $c \in C$, we put $a\delta(c, b)$ whenever $a\varphi b$ and $(a, b)\varepsilon c$. For $f \in F_n$, $g \in G_n$, $\bar{h} \in H_n^{B^n}$, we put $f\delta_n(\bar{h}, g)$ whenever $f\varphi_n g$ and for all $\bar{b} \in B^n$ we have $(f, g, \bar{b})\varepsilon_n \bar{b}\bar{h}$. Since φ and ε are both fully defined, so is δ. Clearly, $\delta\pi = \varphi$.

Observe that if $\{a, a'\}\delta(c, b)$ then $\{(a, b), (a', b)\}\varepsilon c$. Since ε is injective, $a = a'$. Therefore, δ is injective on elements and, by earlier remarks, on operations, as well.

To show that δ is admissible, suppose that $a_1\delta(c_1, b_1)$, ..., $a_n\delta(c_n, b_n)$ and that $f\delta_n(h, g)$. Then $a_1\varphi b_1, \ldots, a_n\varphi b_n$ and $f\varphi_n g$, and so $\bar{a}f\varphi\bar{b}g$. Also, $(a_1, b_1)\varepsilon c_1$, ..., $(a_n, b_n)\varepsilon c_n$ and $(f, g, \bar{b})\varepsilon_n \bar{b}\bar{h}$. Applying the pair of operations to the pairs of elements, we get $(\bar{a}f, \bar{b}g)\varepsilon\bar{c}(\bar{b}\bar{h}))$, and so $\bar{a}f\delta(\bar{c}(\bar{b}\bar{h}), \bar{b}g)$. Therefore, δ is a division.

(2) Define $\varepsilon : D_{\delta\pi} \prec (C, H)$ as follows. Set $(a, b)\epsilon c$ whenever $a\delta(c, b)$ and set $(f, g, \bar{b})\varepsilon\bar{b}\bar{h}$ whenever $f\delta(\bar{h}, g)$. If (a, b) belongs to a sort of $D_{\delta\pi}$, then $a\delta\pi b$, and so there is a $c \in C$ such that $a\delta(c, b)$, and so $(a, b)\varepsilon c$. If $(f, g, \bar{b})$ is an n-ary operation of $D_{\delta\pi}$, then $f\delta\pi g$, and so there is an $\bar{h} \in H_n^{B^n}$ such that $f\delta(\bar{h}, g)$, and so $(f, g, \bar{b})\varepsilon\bar{b}\bar{h}$. These remarks show that ε is fully defined.

To see that ε is injective, let (a, b) and (a', b) belong to the same sort of $D_{\delta\pi}$. Suppose $(a, b)\varepsilon c$ and $(a', b)\varepsilon c$. Then $a\delta(c, b)$ and $a'\delta(c, b)$, which, since δ is injective, implies that $a = a'$.

For admissibility, let $(a_1, b_1)\varepsilon c_1$, ..., $(a_n, b_n)\varepsilon c_n$ and $(f, g, \bar{b})\varepsilon_n \bar{b}\bar{h}$, where $\bar{h} \in H_n^{B^n}$. Then $a_1\delta(c_1, b_1)$, ..., $a_n\delta(c_n, b_n)$ and $f\delta_n(\bar{h}, g)$. Applying the pair of operations to the pairs of elements, we have $\bar{a}f\delta(\bar{c}(\bar{b}\bar{h}), \bar{b}g)$, and so $(\bar{a}f, \bar{b}g)\varepsilon\bar{c}(\bar{b}\bar{h})$. □

Remark Replacing "relational morphism" with "homomorphism" and $\prec$ with $\leq$ preserves the truth of both parts of the Covering Lemma, with little change in the proof.

Corollary 14 *Let π be projection $(C, H) \circ (B, G) \to (B, G)$. Then $D_\pi \sim (C, H)$.*

Proof. Applying the Covering Lemma to $\delta = \mathrm{id} : (C, H) \circ (B, G) \prec (C, H) \circ (B, G)$, we have $D_\pi \prec (C, H)$. By Lemma 1.12, any local algebra of D_π is isomorphic to (C, H), so $(C, H) \prec D_\pi$. □

Chapter 2

Methods of decomposition

The work of decomposition theory involves finding relational morphisms and consolidating their derived algebras in order to use the Covering Lemma. Finding a relational morphism $\varphi : (A, F) \to (B, G)$ can be difficult, because we typically need both D_φ and (B, G) to be somewhat less complex (in terms of division) than (A, F) itself. We can obtain a rough approximation to a relational morphism by means of a structure that is in some sense internal to (A, F). Such a structure, called a cover, is a system of subsets which cover the universe and are preserved by the operations. To a certain degree, covers are to relational morphisms what congruences are to homomorphisms. However, the cover of a relational morphism does not determine the relational morphism up to isomorphism, in the way that a congruence determines a homomorphism. Nevertheless, the derived algebra of any relational morphism having a specified cover is bounded above by (divides) the derived algebra of the cover.

The image of the relational morphism is how (A, F) "acts on" the cover. In many examples, semigroups for instance, F acts ambiguously on the cover, and constructing the morphism involves making choices to resolve this ambiguity. The problem becomes still more subtle when we consider morphisms with multiplicities: elements in the image having the same inverse image sets.

Consolidating a many-sorted algebra means finding a division into a one-sorted algebra. One cannot expect to do this in general without the latter being more complex than the former. The $()^{[\mathrm{alg}]}$ construction introduced in this chapter does this in a canonical way, preserving many essential properties of the msa. The resulting algebra is no more complex than a matrix power of any other consolidation. (The $()^{[\mathrm{alg}]}$ construction is itself a kind of matrix power.) Therefore, making full use of the construction will force us into the perspective that matrix power does not change complexity. This statement is justified and its consequences examined in this chapter and in Chapter 4.

2.1 Covers

Let (A, F) be an algebra, and let $\mathcal{P}(A)$ denote the power set of A. A family $\mathcal{C} \subseteq \mathcal{P}(A)$ is called *admissible* if whenever $n \geq 0$, $f \in F_n$, and $C_1, \ldots, C_n \in \mathcal{C}$, there is a $C \in \mathcal{C}$ such that $(C_1 \times \cdots \times C_n)f \subseteq C$. Given any morphism $\varphi : (A, F) \to (B, G)$, the family $\mathcal{C}_\varphi = \{b\varphi^{-1} : b \in B\}$ is admissible. If φ is a homomorphism, $\mathcal{C}_\varphi$ is a partition. This is not true for morphisms in general (nor is the converse true), but $\mathcal{C}_\varphi$ always has two properties: it is admissible and the union of its members is A. A family $\mathcal{C}$ with the latter properties is called an *admissible cover*, or simply a *cover*, of the algebra, and we say that $\mathcal{C}$ *covers*[1] (A, F). Covers may be compared by the following relation: we write $\mathcal{C} \leq \mathcal{D}$ if each $C \in \mathcal{C}$ is contained in some $D \in \mathcal{D}$ and we write $\mathcal{C} \sim \mathcal{D}$ if $\mathcal{C} \leq \mathcal{D}$ and $\mathcal{D} \leq \mathcal{C}$. Let ∇_A denote the cover $\{A\}$ and let Δ_A denote the cover $\{\{a\} : a \in A\}$. If for each cover $\mathcal{C}$ of (A, F) either $\mathcal{C} \sim \nabla_A$ or $\mathcal{C} \sim \Delta_A$, we call (A, F) *cover simple*.

Proposition 15 *Suppose $\varphi : (A, F) \to (B, G)$. Then $\mathcal{C}_\varphi \sim \Delta_A$ iff $\mathcal{C}_\varphi = \Delta_A$ iff φ is a division. Also, $\mathcal{C}_\varphi \sim \nabla_A$ iff there is a $b \in B$ such that $b\varphi^{-1} = A$. If (A, F) is finite and C_1 and C_2 are covers, then $C_1 \sim C_2$ iff C_1 and C_2 have the same maximal elements.* □

Lemma 16 *(A, F) and $(A, \mathrm{Pol}\ (A, F))$ have the same covers.* □

Proposition 17 *If (A, F) is finite and has a Mal'cev polynomial then every cover C is equivalent to $\mathcal{C}_\varphi$ for some homomorphism φ. If such an algebra is simple, then it is cover simple as well.*

Proof. Let m be the Mal'cev polynomial and $\mathcal{C}$ a cover for (A, F). By the lemma, we may assume m is a term.

Let $D, E \in \mathcal{C}$ be maximal. If $D \cap E \neq \emptyset$, then, choosing $x \in D \cap E$, we have

$$(D \times \{x\} \times E)m \supseteq (\{x\} \times \{x\} \times E)m \cup (D \times \{x\} \times \{x\})m = E \cup D.$$

Since D and E are maximal in $\mathcal{C}$, we get $D = E \cup D = E$. This shows that the maximal sets in $\mathcal{C}$ form a partition. This partition must be admissible. □

In particular, polynomially complete algebras and finite simple groups are cover simple, as are two-element algebras, of course. For lattices, being cover simple is equivalent to having no proper nontrivial tolerances, which is equivalent to being tight plus simple, which is equivalent to being polynomially order complete (see [8]). In general, cover simple implies simple but not conversely. A useful criterion is given by the following. A *tolerance* on an algebra is a binary relation which is reflexive, symmetric, and preserved by the operations.

Proposition 18 *Suppose (A, F) is finite. Then the following are equivalent:*

1. *(A, F) is cover simple.*

[1] This terminology is not related to the name of the Covering Lemma

2. $(\forall\{a,b\} \subseteq A, a \neq b)(\exists f \in \text{Pol } (A,F))(\{a,b\} \times \cdots \times \{a,b\})f = A.$

3. *Both of the following conditions hold:*

   (a) (A,F) *has no proper, nontrivial tolerances, and*

   (b) $(\exists\{a_1,b_1\},\ldots,\{a_n,b_n\} \subseteq A)(\exists f \in F)(\{a_1,b_1\}\times\cdots\times\{a_n,b_n\})f = A.$

Proof. $(1 \Rightarrow 2)$ Suppose $\{a,b\}$ is a counterexample to (2). Define

$$\mathcal{C} = \{(\{a,b\} \times \cdots \times \{a,b\})f : f \in \text{Pol } (A,F)\}.$$

By hypothesis, $A \notin \mathcal{C}$. Also, $\mathcal{C}$ is trivially preserved by F. Hence $\mathcal{C}$ is a proper, nontrivial (because $\{a,b\} \subseteq \mathcal{C}$) cover on (A,F). $(2 \Rightarrow 1)$ and $(2 \Rightarrow 3)$ are left to the reader. $(3 \Rightarrow 2)$ Let $\{a,b\} \subseteq A, a \neq b$. The tolerance ρ generated by (a,b) is A^2, by (3a). Therefore, for each $i \in 1,\ldots,n$, there is a $g_i \in F$ such that $(\{a,b\} \times \cdots \times \{a,b\})g_i \supseteq \{a_i,b_i\}$ Then $(g_1 \times \cdots \times g_n)f$ satisfies (2). □

Associated with an admissible k-ary relation on (A, F), that is, a subalgebra of (A^k,F), we have a cover

$$\mathcal{C}_\rho = \{X \subseteq A : x_1,\ldots,x_k \in X \Rightarrow (x_1,\ldots,x_k) \in \rho, \text{ and } X \text{ is maximal with this property}\}.$$

In other words, $\mathcal{C}_\rho$ consists of the blocks of ρ as defined in Chapter 0.

Recall (from [12] or [4]) that a *majority operation* is a ternary operation m satisfying the equations

$$xxym = xyxm = yxxm = x.$$

It is well known that an algebra with such a term (a lattice, for example) generates a congruence-distributive variety.

Proposition 19 *If (A,F) is finite and has a majority polynomial m, then every cover $\mathcal{C}$ is equivalent to $\mathcal{C}_\rho$ for some tolerance ρ.*

Proof. Let m be the majority polynomial and $\mathcal{C}$ a cover for (A,F). By Lemma 2.2, we may assume m is a term.

Set $a\rho b$ iff $\{a,b\}$ is contained in a member of $\mathcal{C}$. Clearly, $\mathcal{C} \leq \mathcal{C}_\rho$.

For the converse, we must show that blocks of $\mathcal{C}_\rho$ (which are the same as the blocks of ρ as defined in Chapter 0) are contained in blocks of $\mathcal{C}$. This follows easily from the following statement, which we prove by induction on n:

For all $a_1,\ldots,a_n,b \in A$,

$$\{a_1,\ldots,a_n\} \text{ is contained in a member of } \mathcal{C} \text{ and, for all } i,\ b\rho a_i$$
$$\Downarrow$$
$$\{b,a_1,\ldots,a_n\} \text{ is contained in a member of } \mathcal{C}.$$

For $n = 1$, the hypothesis is just that $b\rho a_1$, whence $\{b, a_1\}$ is contained in a member of $\mathcal{C}$ by the definition of ρ.

For $n > 1$, suppose $\{a_1, \ldots, a_n\}$ is contained in a member of $\mathcal{C}$ and, for all i, $b\rho a_i$. Define, for each i, $X_i = \{b, a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n\}$. By inductive assumption, each X_i is contained in a member of $\mathcal{C}$. Hence

$$X \stackrel{\text{def}}{=} (\{a_1, \ldots, a_n\} \times X_1 \times X_2)m$$

is contained in a member of $\mathcal{C}$. But $b = a_1bbm \in X$, $a_1 = a_1ba_1m \in X$, $a_2 = a_2a_2bm \in X$, and, for $i > 2$, $a_i = a_ia_ia_im \in X$. Hence $X \supseteq \{b, a_1, \ldots, a_n\}$. □

The last proposition does not appear to be true when m is replaced by the Jónsson terms, which exactly characterize congruence distributivity.

We now turn from the study of covers as systems of subsets to the study of the algebraic structure induced on covers.

Definition If $\mathcal{C}$ covers (A, F), then $D_{\mathcal{C}}$, the *derived algebra* of the cover $\mathcal{C}$, is the msa

$$(\mathcal{C}, \{F|_{(C_1,\ldots,C_n),C_0} : C_1, \ldots, C_n, C_0 \in \mathcal{C}\})$$

where

$$F|_{(C_1,\ldots,C_n),C_0} = \{f|_{C_1\times\cdots\times C_n} : (C_1 \times \cdots \times C_n)f \subseteq C_0\}.$$

If $\theta \in \text{Con}\,(A, F)$, we define $D_\theta = D_{\mathcal{C}}$ where $\mathcal{C}$ is the partition corresponding to θ.

The next lemma can be useful to get an upper bound on D_φ.

Lemma 20 *Suppose* $\varphi : (A, F) \to (B, G)$. *Then* $D_\varphi \prec D_{\mathcal{C}_\varphi}$. □

Warning $\mathcal{C}_1 \leq \mathcal{C}_2 \not\Rightarrow D_{\mathcal{C}_1} \prec D_{\mathcal{C}_2}$.

We now turn to the problem of reversing the construction of $\mathcal{C}_\varphi$, that is, the problem of converting a given cover into relational morphism. Of course, an admissible partition leads to the usual quotient homomorphism. Therefore, a natural question to ask is: when does a cover $\mathcal{C}$ on (A, F) induce a relational morphism to an algebra in the variety generated by (A, F)? For partitions, the answer is affirmative. A more general answer requires that we find a way for F to act on $\mathcal{C}$, so that we have a morphism from (A, F) to $(\mathcal{C}, F)$ given by the membership relation $A \to \mathcal{C}$ and a clone homomorphism on F.

One case in which we can do this is when $\mathcal{C}$ covers (A, F) and for all $f \in F_n$ and $C_1 \ldots C_n \in \mathcal{C}$ there is a unique $C \in \mathcal{C}$ such that $C \supseteq (C_1 \times \cdots \times C_n)f$. Then F acts on $\mathcal{C}$ in a natural way. Specifically, we have an algebra $(\mathcal{C}, F)$ with action given by $(C_1, \ldots, C_n)f = C$, where C is the unique $C \in \mathcal{C}$ such that $C \supseteq (C_1 \times \cdots \times C_n)f$). Such a cover we call *definite* or *unambiguous*.

2.2 The structure of wreath product algebras

Let (C, H) and (B, G) be algebras and let π denote projection $(C,H)\circ(B,G) \to (B,G)$. The cover $\mathcal{C}_\pi = \{C \times \{b\} : b \in B\}$ of this morphism neatly separates the structure of $(C,H)\circ(B,G)$ into two levels, the lower deriving its structure from (C,H) and the upper from (B,G).

Proposition 21 *Assume C is finite. Suppose $\mathcal{E} \subseteq \mathcal{P}(C \times B)$ and $\bigcup \mathcal{E} = (C \times B)$. Then $\mathcal{E}$ is a cover on $(C,H)\circ(B,G)$ iff either*

1. *$\mathcal{E} \sim \{J \times \{b\} : J \in \mathcal{J}, b \in B\}$ for some cover $\mathcal{J}$ of (C,H), or*
2. *$\mathcal{E} \sim \{C \times I : I \in \mathcal{I}\}$ for some cover $\mathcal{I}$ of (B,G).*

Note that in (1) $\mathcal{E} \leq \mathcal{C}_\pi$ and in (2) $\mathcal{E} \geq \mathcal{C}_\pi$.

Proof. The "if" part is left to the reader. For "only if," assume that $\mathcal{E}$ is a cover.

First, suppose $\mathcal{E} \leq \mathcal{C}_\pi$. Then any $E \in \mathcal{E}$ can be written $E = J \times \{b\}$ for some $J \subseteq C$ and $b \in B$. For $b \in B$, let $\mathcal{J}_b = \{J \subseteq C : J \times \{b\} \in \mathcal{E}\}$. Clearly, $\mathcal{J}_b$ is a cover of (C,H). Now let $b_0, b_1 \in B$ and suppose $J \in \mathcal{J}_{b_0}$. Let $d \in H \circ_B G$ be the binary operation $((c,b),(c',b')) \mapsto (c,b')$. Since $\mathcal{E}$ is a cover, $(J \times \{b_0\}) \times (\{c\} \times \{b_1\})d = J \times \{b_1\}$ is contained in some member of $\mathcal{E}$ (for any c). So J is contained in a member of $\mathcal{J}_{b_1}$. Arguing dually and combining, we conclude $\mathcal{J}_{b_0} \sim \mathcal{J}_{b_1}$ for any $b_0, b_1 \in B$. Hence $\mathcal{E} \sim \{J \times \{b\} : J \in \mathcal{J}_{b_0}, b \in B\}$.

Now, suppose $\mathcal{E} \not\leq \mathcal{C}_\pi$. This means that there are $(c_1,b_1),(c_2,b_2) \in E$, for some $E \in \mathcal{E}$, with $b_1 \neq b_2$. Hence $\mathcal{I} \stackrel{\text{def}}{=} \{E\pi : E \in \mathcal{E}\}$ is a nontrivial cover on (B,G).

Suppose $J \times \{b\}$ and $J' \times \{b'\}$ are contained in members of $\mathcal{E}$. Define a ternary operation f of $H \circ_B G$ by

$$((y_0,x_0),(y_1,x_1),(y_2,x_2)) \mapsto \begin{cases} (y_1,x_1) & \text{if } x_0 = b_1 \\ (y_2,x_1) & \text{if } x_0 = b_2 \end{cases}.$$

Then

$$\{(c_1,b_1),(c_2,b_2)\} \times (J \times \{b\}) \times (J' \times \{b'\})f \supseteq (J \cup J') \times \{b\}.$$

Since $\mathcal{E}$ is a cover, $(J \cup J') \times \{b\}$ is contained in a member of $\mathcal{E}$. Since C is finite and $\mathcal{E}$ is a cover, repeating this argument shows that $C \times b$ is contained in a member of $\mathcal{E}$. Given $I \in \mathcal{I}$, choose $E \in \mathcal{E}$ so that $E\pi = I$. Then, with d the binary operation defined above, we have $((C \times b) \times E)d = C \times I$ contained in a member of $\mathcal{E}$. Therefore, $\mathcal{E} \geq \{C \times I : I \in \mathcal{I}\}$. The opposite relation is clear, and the desired equivalence follows. □

In Chapter 5, this proposition will be used in combination with the observation about covers of Mal'cev algebras (Lemma 2.3) to show that solvable-aperiodic complexity is unbounded.

The next Corollary follows directly from the last proposition when C is finite. The Corollary can be proved without the finiteness assumption using the ideas of the above proof and the fact that a congruence is transitive.

Corollary 22 *For any equivalence relation θ on $C \times B$, $\theta \in \text{Con}\,(C,H) \circ (B,G)$ iff either*

1. *$\theta \leq \ker \pi$ and there is a $\psi \in \text{Con}\,(C,H)$ such that*

$$\theta = \{((c,b),(c',b')) : b = b', c \psi c'\} \text{ or}$$

2. *$\theta \geq \ker \pi$ and there is a $\rho \in \text{Con}\,(B,G)$ such that*

$$\theta = \{((c,b),(c',b')) : b \rho b'\}.$$

By this proposition, $\text{Con}\,(C,H) \circ (B,G)$ is the result of gluing $\text{Con}\,(B,G)$ on top of $\text{Con}\,(C,H)$, identifying only the top element of $\text{Con}\,(C,H)$ with the bottom element of $\text{Con}\,(B,G)$. This proposition actually follows from an analogous result in [11] about the shift product, since the latter is a reduct of the wreath product.

2.3 Matrix powers

We will need another construction tool to supplement the wreath product in order to get a satisfactory decomposition theory for any large class of algebras. This is not surprising, given the diversity of algebras. A closely related construction, the $()^{[\text{alg}]}$ construction, provides an easy way of consolidating derived msas.

As far as I know, matrix powers first appeared in full generality in [8].

Definition Let (A,F) be an algebra and let k be a natural number. Then the k-th matrix power of (A,F) is $(A,F)^{[k]} = (A^k, F^{[k]})$, where

$$(F^{[k]})_n = \{f_1 \times \cdots \times f_k : f_i \in F_{kn}, \text{ for each } i\}.$$

To unwind this definition a bit, let $f_1, \ldots, f_k \in F_{kn}$ and $a_1, \ldots, a_n \in A^k$. Then the n-ary operation $f_1 \times \cdots \times f_k$ of the matrix power acts as follows.

$$(\bar{a}_1, \ldots, \bar{a}_n)(f_1 \times \cdots \times f_k) = ((\bar{a}_1, \ldots, \bar{a}_n)f_1, \ldots, (\bar{a}_1, \ldots, \bar{a}_n)f_k).$$

(By abuse of notation, we use $(\bar{a}_1, \ldots, \bar{a}_n)$ to mean both an n-tuple of k-tuples—on the left-hand side of the equation—and the nk-tuple formed by concatenating the k-tuples $a_1, \ldots, a_n$—on the right-hand side.) Notice that each coordinate of the output can depend on any coordinates of the input, unlike operations in the wreath product. The computational intuition here is that the "program" $f_1 \times \cdots \times f_k$ "runs" the programs $f_1, \ldots, f_k$ in parallel on the same input data and combines their outputs into a k-tuple.

The "matrix" terminology comes from the case of R-modules, that is, algebras of the form $(M, +, ()^{-1}, 0, R)$ where $(M, +, ()^{-1}, 0)$ is an Abelian group and R is a ring added to the clone as unary operations. In this setting, $(M, +, ()^{-1}, 0, R)^{[k]}$ is essentially the module $(M^k, +, (--)^{-1}, 0, R^{k\times k})$, where $R^{k\times k}$ denotes the ring of k by k matrices over R acting on M^k in the usual way.

If we think of an algebra (A, F) as a concrete category with finite products such that each object is a finite power of a single object $\mathbf{a}$, then $(A, F)^{[k]}$ is simply the full subcategory on finite powers of $\mathbf{a}^k$.

The following proposition expresses the k-th non-indexed power $(A, F)^k$ as the k-th direct power (A^k, F) with an additional "diagonal" operation and expresses the k-th matrix power $(A, F)^{[k]}$ as the k-th direct power with two added operations: the diagonal operation and a coordinate shift operation.

Proposition 23 *Let (A, F) be an algebra and let $k > 0$. Define $d : A^{k^2} \to A^k$ by*

$$(x_{1,1}, \ldots, x_{1,k}, x_{2,1}, \ldots, x_{2,k}, \ldots, x_{k,1}, \ldots, x_{k,k})d = (x_{1,1}, x_{2,2}, \ldots, x_{k,k}).$$

Define $s : A^k \to A^k$ by

$$(x_1, \ldots, x_k)s = (x_2, \ldots, x_k, x_1).$$

Then:

1. $(A, F)^k = (A^k, F, d)$, *and*
2. $(A, F)^{[k]} = (A^k, F, d, s)$.

In particular, (A^k, F) is a reduct of $(A, F)^k$, which is a reduct of $(A, F)^{[k]}$.

Proof. (1) Clearly, $d = (\pi_{k,1}, \ldots, \pi_{k,k})$ is an operation of $(A, F)^k$. Conversely, any operation $(f_1, \ldots, f_k)$ of $(A, F)^k$ can be expressed as $(f_1, \ldots, f_k) = ((f_1, \ldots, f_1), \ldots, (f_k, \ldots, f_k))d$.

(2) As before, d is an operation of $(A, F)^{[k]}$, as is $s = \pi_{k,2} \times \cdots \times \pi_{k,k} \times \pi_{k,1}$. Conversely, any n-ary operation $f_1 \times \cdots \times f_k$ of $(A, F)^{[k]}$ can be expressed as follows. Let $\bar{x}_1, \ldots, \bar{x}_n \in A^k$. Then

$$(\bar{x}_1, \ldots, \bar{x}_n)(f_1 \times \cdots \times f_k) =$$

$$(\bar{x}_1 s^0, \ldots, \bar{x}_1 s^{k-1}, \bar{x}_2 s^0, \ldots, \bar{x}_2 s^{k-1}, \ldots, \bar{x}_n s^0, \ldots, \bar{x}_n s^{k-1})(f_1, \ldots, f_k).$$

(Recall that applying $(f_1, \ldots, f_k)$ to a nk-tuple of k-tuples means applying the nk-ary operation f_1 to the first coordinates of the k-tuples, applying f_2 to the second coordinates of the k-tuples, and so on.) Expressing $(f_1, \ldots, f_k)$ using d as before completes the proof. □

Corollary 24 *Let (A, F) be an algebra.*

1. Con $(A, F)^k \cong (\text{Con } (A, F))^k$.

2. Con $(A,F)^{[k]} \cong$ Con (A,F).

3. Pol $(A,F)^{[k]} \cong$ (Pol (A,F))$^{[k]}$.

Proof. Exercise. □

Note that Con (A^k,F) is not in general constructible from Con (A,F) in any uniform lattice theoretic way. Consider the group $(2,+)$, for instance.

Lemma 25

1. $(A,F)^{[k]} \leq (A,F)^{[m]}$ *for* $k \leq m$.

2. *If* $(A,F) \prec (B,G)$, *then* $(A,F)^{[k]} \prec (B,G)^{[k]}$.

Proof. For (1), choose $a \in A$. We embed $(A,F)^{[k]} \leq (A,F)^{[m]}$ via the map

$$(x_1,\ldots,x_k) \mapsto (x_1,\ldots,x_k,a,\ldots,a)$$

and, for $f_1,\ldots,f_k \in F_{kn}$,

$$f_1 \times \cdots \times f_k \mapsto f_1' \times \cdots \times f_k' \times \pi \times \cdots \times \pi,$$

where each $f_i' \in F_{mn}$ and is defined by

$$((x_{11},\ldots,x_{1m}),\ldots,(x_{n1},\ldots,x_{nm}))f_i' = ((x_{11},\ldots,x_{1k}),\ldots,(x_{n1},\ldots,x_{nk}))f_i,$$

and π is the projection map

$$((x_{11},\ldots,x_{1m}),\ldots,(x_{n1},\ldots,x_{nm}))\pi = x_{nm}.$$

For (2), first suppose (A,F) is a subreduct of (B,G). Then clearly $(A,F)^{[k]}$ is a subreduct of $(B,G)^{[k]}$. Now suppose $(A,F) = (B/\theta,G)$ for some $\theta \in$ Con (B,G). Define a congruence $\psi \in$ Con $(B,G)^{[k]}$ by

$$(x_1,\ldots,x_k)\psi(y_1,\ldots,y_k) \iff x_1\theta y_1,\ldots,x_k\theta y_k.$$

Then $(B,G)^{[k]}/\psi \cong (B/\theta,G)^{[k]} = (A,F)^{[k]}$. □

Lemma 26 *The matrix power and wreath product constructions commute:*

$$((C,H) \circ (B,G))^{[k]} \cong (C,H)^{[k]} \circ (B,G)^{[k]}.$$

Proof. On elements, we map

$$((c_1,b_1),\ldots,(c_k,b_k)) \mapsto ((c_1,\ldots,c_k),(b_1,\ldots,b_k)).$$

On n-ary operations, we map

$$(\bar{h}_1,g_1) \times \cdots \times (\bar{h}_k,g_k) \mapsto (\bar{f},g_1 \times \cdots \times g_k),$$

where

$$(\bar{b}_1, \ldots, \bar{b}_n)\bar{f} = (\bar{b}_1, \ldots, \bar{b}_n)\bar{h}_1 \times \cdots \times (\bar{b}_1, \ldots, \bar{b}_n)\bar{h}_k.$$

It is easy to check that this map is a homomorphism and is bijective both on elements and on operations. □

From the category theoretic point of view, the last proposition seems natural. Matrix powers commute with most "arrow-theoretic" ideas. See McKenzie's paper on Morita equivalence of varieties. We will use (and prove) the fact that matrix powers preserve the congruence lattice and its type labelling in the upcoming sections on aprimal algebras.

McKenzie shows that matrix powers induce functors on varieties which preserve many ideas. However, matrix powers and subreducts are particularly powerful in combination, preserving fewer ideas, as the following propositions reveal. The first says that matrix powers and subreducts can be used to construct polynomial closures of clones.

Proposition 27 *Let (A, F) be a finitely generated algebra, generated by some k elements. Then $(A, F, C_A) \leq (A, F)^{[k+1]}$.*

Proof. Let $X = \{a_1, \ldots, a_k\}$ generate A under F. Consider the full subreduct of $(A, F)^{[k+1]}$ on $A \times \{a_1\} \times \cdots \times \{a_k\}$. This algebra is isomorphic to $(A, F, C_X) = (A, F, C_A)$. □

Although matrix powers preserve the labelled congrence lattice of tame congruence theory, the types occuring in reducts of an algebra are not preserved, as shown by the next two facts. The first is from [10].

Theorem 28 (Maurer-Rhodes) *If $(S, \cdot)$ is a simple nonabelian group, then $(S, \mathrm{Pol}\ (S, \cdot))$ is primal. Therefore, $(S, \cdot)^{[|S|+1]}$ has a primal subreduct.*

Proposition 29 *$(2, \wedge, \vee)^{[2]}$ has a primal subreduct.*

Proof. Consider the subreduct with elements $(0, 1)$ and $(1, 0)$ and operations

$$(\wedge, \vee) : ((x_1, y_1), (x_2, y_2)) \mapsto (x_1 \wedge x_2, y_1 \vee y_2)$$

and

$$\pi_{2,2} \times \pi_{2,1} : (x, y) \mapsto (y, x).$$

On $\{(0, 1), (1, 0)\}$, the former is a semilattice operation and the latter is the nonidentity permutation. Hence the subreduct is a two-element Boolean algebra. □

I am indebted to Pawel Idziak for showing me how to obtain this fact using only the second matrix power. One consequence is that any algebra with a type 4 (or 3) congruence interval has a matrix power with a primal divisor and hence has a matrix power with any given divisor. The indecomposability theorems

of the next chapter show that no nonindexed power (or even wreath power) of $(2, \wedge, \vee)$ has a primal subreduct.

The next lemma tells us how high a matrix power we must look at to tell whether $(A, F)^{[k]}$ has a given subreduct.

Lemma 30 *Let (A, F) and (B, G) be finite algebras with $(B, G) \leq (A, F)^{[k]}$ for some k. Then $(B, G) \leq (A, F)^{[|A^B|]}$ and $(B, G) \leq (A, F, C_A)^{[|A^B|-|A|]}$.*

Proof. Write $B = \{b_1, \ldots, b_n\}$. Choose k minimal so that $(B, G) \leq (A, F)^{[k]}$. Assume $B \subseteq A^k$. If, for some $i \neq j$, we have $((b_1)_i, \ldots, (b_n)_i) = ((b_1)_j, \ldots, (b_n)_j)$, then projection onto coordinates $\{1, \ldots, k\} \setminus \{i\}$ induces an embedding $(B, G) \leq (A, F)^{[k-1]}$, which is impossible, by choice of k. Since the number of distinct n-tuples of elements of A is $|A^n|$, this proves that $k \leq |A^n|$, from which follows the first part of the lemma.

Now choose k minimal so that $(B, G) \leq (A, F, C_A)^{[k]}$. Assume $B \subseteq A^k$. If, for some i and for some $a \in A$, we have $((b_1)_i, \ldots, (b_n)_i) = (a, \ldots, a)$, then projection onto coordinates $\{1, \ldots, k\} \setminus \{i\}$ induces an embedding $(B, G) \leq (A, F, C_A)^{[k-1]}$. Since the number of distinct nonconstant n-tuples of elements of A is $|A^n| - |A|$, this proves that $k \leq |A^n| - |A|$, from which follows the second part of the lemma. □

The exponent in the lemma might not be optimal, but we cannot in general reduce it very much, as shown by examples in Chapter 4. In general, there is no such theorem for division in place of subreduct. Of course, there will be such a theorem for any (B, G) which satisfies the following: for all (A, F), if $(B, G) \prec (A, F)$ then $(B, G) \leq (A, \mathrm{Pol}\ (A, F))$. Cyclic groups of prime order, the two-element primal algebra (i.e., the two-element Boolean algebra), the two-element lattice, and the two-element semilattice all have this property, by theorems in tame congruence theory. This will be discussed in Chapter 4.

Proposition 31 *A matrix power of a primal algebra is primal.* □

2.4 The $()^{[\mathrm{alg}]}$ consolidation

Unlike the consolidations used in semigroup theory, $()^{[\mathrm{alg}]}$ introduces no unnatural zero elements. In fact, providing we are working in a setting in which matrix powers preserve "complexity" (whatever that is), finding the complexity of an algebra requires only decompositions obtained from $()^{[\mathrm{alg}]}$ and the Covering Lemma. It is therefore possible (but a bit less elegant) to approach decomposition theory in such a setting without the use of msas.

In this section all algebras and msas are finite.

Definition Let $(\mathbf{A}, \mathbf{F})$ be a msa. We define $(\mathbf{A}, \mathbf{F})^{[\mathrm{alg}]}$ to be the algebra

$$(\times \mathbf{A}, \mathbf{F}_{(\times \mathbf{A})^n, \times \mathbf{A}} : n = 0, 1, 2 \ldots).$$

In other words, $(\mathbf{A},\mathbf{F})^{[\mathrm{alg}]}$ is algebra whose universe is $A_1\times\cdots\times A_m$, (where $\mathbf{A}=\{A_1,\ldots,A_m\}$) and whose n-ary operations are those of the form $f_{A_1}\times\cdots\times f_{A_m}$, where each f_{A_i} is an mn-ary operation of $\mathbf{F}$ with signature

$$(\underbrace{A_1,\ldots,A_m,A_1,\ldots,A_m,\ldots,A_1,\ldots,A_m}_{n\text{ copies of }A_1,\ldots,A_m})\to A_i.$$

A specialized version of this construction was devised by M. Valeriote, who applied it to many-sorted unary algebras to obtain a class of type 1 algebras in the McKenzie-Valeriote structure theory for decidable locally finite varieties [???]. The general version used here was suggested to me by R. McKenzie.

Thinking of $(\mathbf{A},\mathbf{F})$ as a concrete category with finite products each of whose objects is a product of copies of objects $\mathbf{a}_1,\ldots,\mathbf{a}_k$, $(\mathbf{A},\mathbf{F})^{[\mathrm{alg}]}$ is the full subcategory on powers of $\mathbf{a}_1\times\cdots\times\mathbf{a}_k$. From this point of view, the proof of the next proposition becomes obvious: we simply restrict the given division to the full subcategory on powers of $\mathbf{a}_1\times\cdots\times\mathbf{a}_k$.

Lemma 32 *If $(\mathbf{A},\mathbf{F})\prec(B,G)$ then $(\mathbf{A},\mathbf{F})^{[\mathrm{alg}]}\prec(B,G)^{[k]}$ where k is the number of sorts of $(\mathbf{A},\mathbf{F})$.* □

Next we show that $()^{[\mathrm{alg}]}$ does indeed produce consolidations.

Lemma 33 $(\mathbf{A},\mathbf{F})\prec(\mathbf{A},\mathbf{F})^{[\mathrm{alg}]}$.

Proof. Let $\{1,\ldots,k\}$ index $(\mathbf{A},\mathbf{F})$. We construct a division $\delta:(\mathbf{A},\mathbf{F})\prec(\mathbf{A},\mathbf{F})^{[\mathrm{alg}]}$ as follows. On a sort A_i, we define

$$x\delta=\{\bar{y}\in\times\mathbf{A}:y_i=x\}.$$

For operations of signature $(i_1,\ldots,i_n)\to j$, we define

$$f\delta=\{\bar{g}\in\mathrm{Clo}_n\ (\mathbf{A},\mathbf{F})^{[\mathrm{alg}]}:(x_{1,1},\ldots,x_{n,k})g_j=(x_{1,i_1},\ldots,x_{n,i_n})f\}.$$

It follows easily that δ is a division. □

Corollary 34 (The Covering Lemma with $()^{[\mathrm{alg}]}$) *Let π denote the projection homomorphism $(C,H)\circ(B,G)\to(B,G)$.*

1. *If $\varphi:(A,F)\to(B,G)$ is a relational morphism, then*

$$(A,F)\prec D_{\varphi}^{[\mathrm{alg}]}\circ(B,G).$$

2. *If $(A,F)\overset{\delta}{\prec}(C,H)\circ(B,G)$, then*

$$D_{\delta\pi}^{[\mathrm{alg}]}\prec(C,H)^{[|B|]}.$$

Proof. Use the previous lemma and the Covering Lemma. (For (2) note that the number of sorts of $D_{\delta\pi}$ is $|B|$.) □

When φ is a homomorphism, $D_\varphi^{[\mathrm{alg}]}$ depends only on $\ker\varphi$ and can be expressed in the following way, which simplifies notation in some of the upcoming proofs.

Lemma 35 *Suppose $\varphi : (A, F) \to (B, G)$ is a homomorphism. Write $B = \{b_1, \ldots, b_k\}$, $A_1 = b_1\varphi^{-1}, \ldots, A_k = b_k\varphi^{-1}$. Then*

$$D_\varphi^{[\mathrm{alg}]} \cong (A_1 \times \cdots \times A_k, H)$$

where

$$\begin{aligned} H_n \quad = \quad & \{h_1 \times \cdots \times h_k : \textit{ for all } i,\ h_i = f_i|_{(A_1\times\cdots\times A_k)^n} \\ & \textit{for some } f_i \in F_{nk} \textit{ with } (A_1 \times \cdots \times A_k)^n f_i \subseteq A_i\}. \end{aligned}$$

Proof. Exercise. □

Following the example of Proposition 2.15, we can construct a msa which doesn't have a primal divisor, but whose $()^{[\mathrm{alg}]}$ does. To do so, let $\mathbf{A} = \{A_1, A_2\}$ with $A_1 = \{0, 1\} = A_2$. Let $\mathbf{F}$ be generated by the following operations

$$u : A_1 \to A_2, 0u = 0, 1u = 1,$$

$$v : A_2 \to A_1, 0v = 0, 1v = 1,$$

$$f : A_1 \times A_2 \to A_1, (x, y)f = x \wedge y,$$

$$g : A_1 \times A_2 \to A_1, (x, y)g = x \vee y.$$

It's easy to see that $(\mathbf{A}, \mathbf{F})^{[\mathrm{alg}]} \cong (2, \wedge, \vee)^{[2]}$. The point of this example (in combination with the lemma comparing $()^{[\mathrm{alg}]}$ with $()^{[k]}$) is that $()^{[\mathrm{alg}]}$ is "safe"—it does not introduce primal algebras—precisely when $()^{[k]}$ is. Another way to say this is: if (A, F) can be decomposed into algebras from various classes closed under matrix powers, then the last corollary also gives a decomposition into algebras from the classes. This is one motivation for the study of classes closed under matrix power and division, which we will take up at length in Chapter 4.

We now show that the construction $\varphi \rightsquigarrow D_\varphi \rightsquigarrow D_\varphi^{[\mathrm{alg}]}$ preserves an important congruence-lattice property.

Lemma 36 *If $\varphi : (A, F) \to (B, G)$ is a homomorphism such that $\ker\varphi$ is minimal among the nonzero elements of $\mathrm{Con}\,(A, F)$, then the algebra $D_\varphi^{[\mathrm{alg}]}$ is simple.*

Proof. Write $B = \{b_1, \ldots, b_k\}, A_1 = b_1\varphi^{-1}, \ldots, A_k = b_k\varphi^{-1}$. Let $(x_1, \ldots, x_k)$ and $(y_1, \ldots, y_k)$ be two distinct elements of $D_\varphi^{[\mathrm{alg}]}$ (or, rather, of the isomorphic algebra defined in Lemma 2.21, with which algebra we shall henceforth work).

We may assume that $x_1 \neq y_1$. By the minimality of $\ker\varphi$ we have sequences

$$\begin{aligned} x_1 = z_{1,1}, z_{1,2}, \ldots, z_{1,m} = y_1, \\ \vdots \\ x_k = z_{k,1}, z_{k,2}, \ldots, z_{k,m} = y_k, \end{aligned}$$

such that each $\{z_{i,j}, z_{i,j+1}\}$ is the image of $\{x_1, y_1\}$ under some unary polynomial of (A, F). Since $\{x_1, y_1\}$ is contained in the congruence class A_1 and $z_{i,1} \in A_i$, $\{z_{i,1}, z_{i,2}\} \subseteq A_i$. Inducting, we get $\{z_{1,1}, z_{1,2}, \ldots, z_{1,m}\} \subseteq A_i$. Hence $(z_{1,j}, \ldots, z_{k,j}) \in A_1 \times \cdots \times A_k$.

It is not hard to see that any pair $\{(z_{1,j}, \ldots, z_{k,j}), (z_{1,j+1}, \ldots, z_{k,j+1})\}$ is the image of $\{(x_1, \ldots, x_k), (y_1, \ldots, y_k)\}$ under some unary polynomial of $D_\varphi^{[\mathrm{alg}]}$. □

In fact, in the setting of the Lemma, D_φ is itself simple in a natural sense. In general, we may study tame congruence theory in the category of msas and their morphisms. A thorough development of these ideas would probably be worthwhile but would be tangential to the present work.

By applying this lemma and the Covering Lemma, we can decompose any finite algebra (A, F) into simple algebras. Furthermore, the types of this sequence of simple algebras may be chosen to correspond to the types of intervals in a maximal chain of Con (A, F) (we will prove this in Chapter 6). This fact appears useful but cannot be the prime decomposition theorem we seek. First, simple algebras are wild—much more so than in semigroup theory. Decomposing them further is where the bulk of the work will take place. Second, every algebra divides algebras of types 3, 4, and 5 (the type 3 and 4 cases were handled in this chapter; for the type 5 case, see Chapter 6). So the "fact" is really a triviality. The aprimal setting (Chapter 4) is the largest setting in which this method of decomposition is nontrivial.

Chapter 3

Indecomposable algebras

In semigroup theory, the wreath indecomposables are easy to classify. In the general setting, the only way to obtain a reasonably small set of "primes" is to allow matrix powers in our decompositions. Before we investigate this technique, we prove as much as possible about wreath indecomposables and give some examples.

Definition Let (A, F) be a finite algebra. Then (A, F) is said to be *morphism indecomposable* if, whenever $\varphi : (A, F) \to (B, G)$ is a relational morphism to a finite algebra, either

1. $(A, F) \prec D_\varphi$, or
2. $(A, F) \prec (B, G)$.

We say that (A, F) is *wreath indecomposable* if, whenever $(A, F) \prec (C, H) \circ (B, G)$, with C and B finite, we have either

1. $(A, F) \prec (C, H)$, or
2. $(A, F) \prec (B, G)$.

We say that (A, F) is *indecomposable up to matrix powers* if, whenever $(A, F) \prec (C, H) \circ (B, G)$, with C and B finite, we have either

1. $(A, F) \prec (C, H)^{[k]}$ for some k, or
2. $(A, F) \prec (B, G)^{[k]}$ for some k.

Note that, by the Covering Lemma, morphism indecomposability implies wreath indecomposablity. Also, wreath indecomposability implies indecomposability up to matrix powers. There are algebras which are not wreath indecomposable but are indecomposable up to matrix powers. Wreath indecomposability is here only for comparison and plays no major role in the decomposition theory. All wreath indecomposable algebras I know of can be shown to be morphism

indecomposable. My conjecture is that the two are distinct. Evidence for this is the fact that the $()^{[\mathrm{alg}]}$ construction can introduce new divisors, as shown in the previous chapter. To prove strong theorems, we always try to find wreath decompositions (as opposed to just relational morphisms) and show morphism indecomposability.

Proposition 37 *The two-element set $(2, \emptyset)$ is morphism indecomposable.*

Proof. Divisionally, $(2, \emptyset)$ is the smallest nontrivial algebra. □

3.1 Indecomposability and iterable operations

Some more general proofs of morphism indecomposability hinge on the notion of an iterable operation. To give a clear definition of this concept we need a kind of exponentiation for operations.

Definition Suppose $f : A^n \to A$. We define, for each i, an operation $f^i : A_{n_i} \to A$ recursively as follows. First, $f^0 = \mathrm{id}_A$. Next, for $i > 0$, we set

$$(x_1, \ldots, x_{n^i})f^i = \\ ((x_1, \ldots, x_n)f, (x_{n+1}, \ldots, x_{2n})f, \ldots, (x_{n^i-n+1}, \ldots, x_{n^i})f)f^{i-1}.$$

This notation, when $n = 1$, agrees with the usual exponentiation of operations $A \to A$. Also, many properties of exponentiation hold for this generalization: $(f^k)^l = f^{kl}$, in $(A, F) \times (B, G)$ we have $(f, g)^n = (f^n, g^n)$, etc.

Definition An operation $f : A^n \to A$ is called *iterable* if, for any $i > 0$, f^i generates f (equivalently, for any $i > 0$, $(A, f^i) = (A, f)$).

The next proposition says that iterable includes two familiar senses of the word "idempotent", the first from semigroup theory and the second from universal algebra.

Proposition 38 *Let A be a finite set.*

1. *Suppose $f : A \to A$. Then f is iterable if and only if $f^2 = f$.*
2. *Suppose $f : A^n \to A$ and, for all $a \in A$, $(a, \ldots, a)f = a$. Then f is iterable.*

Proof. The "if" part in (1) is obvious. For the converse, suppose f is iterable. Since f is unary, f is iterable if and only if $(\forall i > 0)(\exists j > 0)f^{ij} = f$. Since A is finite, we may choose $i > 0$ such that $(f^i)^2 = f^i$. Find $j > 0$ such that $f^{ij} = f$. But then $f^2 = (f^{ij})^2 = f^{ij} = f$.

To prove (2) for a given i, observe that

$$(x_1, \ldots, x_n)f = (x_1, \ldots, x_n, x_1, \ldots, x_n, \ldots, x_1, \ldots, x_n)f^i$$

follows from the hypothesis by an easy inductive argument. □

If $\varphi : (A, F) \to (B, G)$ is a relational morphism, then the subalgebra structure of (B, G) tells us how the sorts of D_φ "connect", i.e., whether there is an "arrow" from one given sort to another. The next lemma reduces the class of relational morphisms one has to look at to give certain proofs of indecomposability to a class in which this sort of connectivity is universal: there is communication between every pair of sorts, in both directions. First we need a technical definition that is needed in the proof of the lemma.

Definition Let (A, F) be an algebra, and $X \subseteq F$. We define the *tree-composites* of operations in X recursively as follows.

Each $g \in X$ is a tree-composite of X.

If $f_1, \ldots, f_n$ are m-ary tree-composites of X and $g \in X$, then the operation given by

$$(x_{1,1}, \ldots, x_{n,m}) \mapsto ((x_{1,1}, \ldots, x_{1,m})f_1, \ldots, (x_{n,1}, \ldots, x_{n,m})f_n)g$$

is a tree-composite of X.

Note that, if all operations in X are surjective, then all tree-composites of X are surjective. Also, f^k is a tree-composite of $\{f\}$.

Lemma 39 *Let (A, F) be a finite cover simple algebra such that F is generated by a set X of surjective operations. If $\varphi : (A, F) \to (B, G)$ is a relational morphism with B finite and φ not injective, then there is a relational morphism $\varphi' : (A, F) \to (B', G')$ with $(B', G') \leq (B, G)$ and $\varphi' \leq \varphi$ such that*

1. *$D_{\varphi'} \prec D_\varphi$,*
2. *(B', G') has no proper, nonempty subalgebras,*
3. *$A\varphi' B'$, that is, $a\varphi' b$ for all $a \in A$ and $b \in B'$,*
4. *for all $b, b' \in B'$, there is a surjective operation in $D_{\varphi'}$ of signature $(b)^n \to b'$ for some n, and*
5. *G' is generated by $X\varphi'$.*

Proof. Since φ is not injective, $\mathcal{C}_\varphi \neq \Delta_A$. Therefore, since (A, F) is cover simple, $\mathcal{C}_\varphi \sim \nabla_A$, and there is a $b_0 \in B$ such that $b_0\varphi^{-1} = A$.

Let B' be a minimal nonempty subuniverse of $(b_0(X\varphi), X\varphi)$. Let G' be the clone generated by $\{g|_{B'} : g \in X\varphi\}$. Statement (2) follows immediately.

For $a \in A$ and $b \in B'$, set $a\varphi' b$ iff $a\varphi b$. Let the clone of φ' be generated by $\{(f, g|_{B'}) : f \in X, f\varphi g\}$. Since X generates F, φ' is fully defined on F. Statement (5) is obvious.

Suppose $b \in B'$. Since $B' \subseteq b_0(X\varphi)$, we can find $(f, g) \in \varphi'$ such that $b = (b_0, \ldots, b_0)g$ and f is a tree-composite of operations in X. Then f is surjective since the operations in X are. So from $A\varphi b_0$ we deduce

$$A \;=\; (A \times \cdots \times A)f \;\; \varphi \;\; (b_0, \ldots, b_0)g \;=\; b.$$

This proves (3), and, moreover, shows that φ is fully defined on A. Statement (1) follows from Lemma 1.7.

Suppose $b, b' \in B'$. By minimality, $b' \in bG'$, and there is a pair $(f, g) \in \varphi'$ such that f is a tree composite of X and $(b, \ldots, b)g = b'$. So f is surjective, as is the operation $(f, g, (b, \ldots, b))$ of $D_{\varphi'}$. This proves (4). □

An operation f on A is said to be *idempotent* if, for all $a \in A$, $(a, \ldots, a)f = a$. Note that if F is generated by indempotent operations then F is generated by surjective operations. In fact, all operations in F are idempotent and hence surjective.

Theorem 40 *Let (A, F) be a finite cover simple algebra such that F is generated by surjective operations. Then (A, F) is morphism indecomposable if either*

1. *F is generated by a single iterable operation, or*
2. *F is generated by idempotent operations.*

Proof. (1) Write $(A, F) = (A, f)$, with f iterable. Suppose $\varphi : (A, f) \to (B, g)$ is a relational morphism to a finite algebra. If φ is injective, then $\varphi : (A, f) \prec (B, g)$. If φ is not injective, then we apply the lemma to get $\varphi' : (A, f) \to (B', G')$. Choose $g' \in G'$ with $f\varphi' g'$. Since B' is finite, we can find $b \in B'$ and $i > 0$ such that $(b, \ldots, b)g'^i = b$. So $D_{\varphi'}|_b$ has the operation $(f^i, g'^i, (b, \ldots, b))$. But since f is iterable, this operation generates an operation of the form $(f, h, (b, \ldots, b))$ for some $h \in G'$. Since $b\varphi^{-1} = A$, $(A, f) \prec D_{\varphi'} \prec D_\varphi$.

(2) Assume F is idempotent and $(A, F) \to (B, G)$ is a relational morphism to a finite algebra. If φ is injective, then $\varphi : (A, F) \prec (B, G)$. If φ is not injective, then we apply the Lemma to get $\varphi' : (A, F) \to (B', G')$. By (4) of the Lemma, there is an identity map between each pair of sorts of D'_φ. Choose a sort b and compose each $(f, g, (b, \ldots, b))$ with the appropriate identity map so that the image is in sort b. This shows that $(D_{\varphi'})|_b \cong (A, F)$. But by the lemma, $D_{\varphi'} \prec D_\varphi$. □

Example 1 The following algebras are morphism indecomposable.

1. A finite simple group $(G, \cdot)$. One way to see this is to let $n = |G|$ and replace binary multiplication with n-ary multiplication $f : (x_1, \ldots, x_n) \mapsto x_1 \cdot \ldots \cdot x_n$. Since a group of order n satisfies $x^n = 1$, $(x, \ldots, x)f = 1$, and so c_1 (the constant map with value one) is in the clone generated by f. Since $(x, y, 1, \ldots, 1)f = x \cdot y$, f generates the original group operation $\cdot$, and $(G, \cdot) = (G, f)$. We now show that f is iterable. Let $i > 0$. Clearly,

$(x, \ldots, x)f^i = 1$, so f^i generates c_1. Composing f^i with sufficiently many copies of c_1 produces f again. Finite simple groups are cover simple, so now we apply part (1) of the theorem.

2. A simple algebra (A, f) with f a Mal'cev operation (i.e., we have $(xyy)f = x = (yyx)f$). Recall from Chapter 2 that a simple algebra with a Maltsev operation is cover simple. A Maltsev operation is idempotent. Apply part (2) of the theorem.

3. The two-element semilattice $(2, \wedge)$ and the two-element lattice $(2, \wedge, \vee)$. Meet and join are idempotent.

4. A tight, simple lattice. Tight plus simple implies cover simple, and lattice operations are idempotent.

Warning A simple nonabelian group with a proper nontrivial subgroup of constant operations is not wreath indecomposable (and therefore not morphism indecomposable). More precisely, let $(G, \cdot)$ be any group with a subgroup H. Then

$$(G, \cdot, C_H) \prec (G, \cdot, A_H) \circ (H, \cdot, C_H),$$

where

$$A_H = \{x \mapsto hxh^{-1} : h \in H\}.$$

To see this, define $\varphi : (G, \cdot, C_H) \to (H, \cdot, C_H)$ by

$$\begin{array}{rcll} g & \varphi & h & \text{for all } g \in G \text{ and all } h \in H \\ \cdot & \varphi & \cdot & \\ c_h & \varphi & c_h & \text{for all } h \in H. \end{array}$$

Then we have $\delta : D_\varphi \prec (G, \cdot, A_H)$, by setting

$$\begin{array}{rcll} (g, h) & \delta & gh^{-1} & \text{for all } g \in G \text{ and all } h \in H \\ c_h & \delta & c_1 & \text{for all } h \in H \\ (\cdot, \cdot, (h, h')) & \delta & f_h & \text{for all } h, h' \in H, \end{array}$$

where f_h is given by $(x, y) \mapsto xhyh^{-1}$. Note that $c_1 \in \text{Clo}\,(G, \cdot, A_H)$ since $(G, \cdot)$ satisfies $x^n = 1$ for some n.

Of course, such a decomposition doesn't really get anywhere. When $(G, \cdot)$ is simple, $(G, \cdot, C_H)$ is indecomposable up to matrix powers. Also, when $H = \{1\}$, $(G, \cdot, C_H) = (G, \cdot)$, which is morphism indecomposable, as shown in the examples above. When $H = G$, $(G, \cdot, C_H)$ is primal. We usually use (n, P_n) to denote the primal algebra on n elements. These algebras are also morphism indecomposable, but we cannot show this by the above methods. (I know of no way to conclude from the noninjectivity of a morphism $\varphi : (n, P_n) \to (B, G)$ that $(n, P_n) \prec D_\varphi$.) Actually, the previous theorem can be used to show that primal algebras are indecomposable up to matrix powers, because (n, P_n) is the polynomial closure of (n, d) where d is a discriminator operation, (n, d) is cover

simple, and d is Mal'cev. Indecomposability up to matrix powers is sufficient for the remainder of this work; nevertheless, the following proof of morphism indecomposability is of some interest.

Theorem 41 *The primal algebra (n, P_n) is morphism indecomposable for all n.*

Proof. Consider the n-valued Post algebra $(n, \wedge, ')$, where $x \wedge y = \min(x, y)$ and $x' = (x + 1) \bmod n$. A little work (using Rosenberg's theorem, for example) reveals this to be primal, so $(n, \wedge, ') = (n, P_n)$. Observe that $\wedge$ and $'$ are surjective. Also, primal algebras are cover simple, so primal algebras satisfy the hypotheses of Lemma 3.3. Hence for the present proof we need consider only morphisms satisfying the conclusions of the lemma.

Let $\varphi : (n, P_n) \to (B, G)$ be a relational morphism such that (B, G) has no proper, nonempty subalgebras, $n\varphi B$, and so on. Now we use the identity $(n, P_n) = (n, s, c_0, \ldots, c_{n-1})$, where $c_i : n \to n$ is the constant map with value i and s is the 4-ary switching operation:

$$(u, v, x, y)s = \begin{cases} x & \text{if } u = v \\ y & \text{if } u \neq v. \end{cases}$$

We may assume that G is generated by $s\varphi \cup c_0\varphi \cup \ldots \cup c_{n-1}\varphi$. The proof now falls into two cases.

First, we suppose that whenever $c_i\varphi g$, $c_j\varphi h$, and $i \neq j$, we have $\mathrm{Im}\,(g) \cap \mathrm{Im}\,(h) = \emptyset$. Let

$$B_i = \{b \in B : b \in \mathrm{Im}\,(g) \text{ for some } g \in c_i\varphi\}.$$

The B_i are pairwise disjoint, by the supposition. Observe that $B_j(c_i\varphi) \subseteq B_i$. Also,

$$(B_i \times B_j \times B_k \times B_l)(s\varphi) \subseteq \begin{cases} B_k & \text{if } i = j \\ B_l & \text{if } i \neq j. \end{cases}$$

Let $B' = B_1 \cup \ldots \cup B_{n-1}$. In particular, B' is closed under G, because $s\varphi \cup c_0\varphi \cup \ldots \cup c_{n-1}\varphi$ generates G. Furthermore, the above remarks show that the partition $\{B_1, \ldots, B_{n-1}\}$ is a cover of (B', G) and that this cover induces a quotient morphism from (B', G) onto (n, P_n).

Second, we suppose that there are pairs $c_i\varphi g$ and $c_j\varphi h$ with $i \neq j$ and $\mathrm{Im}\,(g) \cap \mathrm{Im}\,(h) \neq \emptyset$. So we have operations (c_i, g, b_0) and (c_j, h, b_1) in D_φ with $b_0 g = b_1 h$. Since B has no proper, nonempty subalgebras and c_i and c_j are constant operations, we may assume $b_0 = b_1$. Since (n, P_n) is cover simple, we can find $b \in B$ and, for each m, a constant operation (c_m, g_m, b_0) with $b_0 g_m = b$. Iterating s starting from the sort indexed by b leads to a sort b' such that there is an identity map $b \to b'$ and the local algebra at b' has s. Using the identity maps, the local algebra also has all constants, completing the proof. □

More generally, it is possible to prove that adding constant operations preserves morphism indecomposability for the algebras shown to be morphism indecomposable by the theorem before the preceding one. The proof is similar to the above proof.

Conjecture 1 *Matrix powers preserve morphism (and wreath) indecomposability.*

3.2 Indecomposability up to matrix powers

In the following chapters we study classes of algebras closed under division, matrix power, and wreath product. In this setting it is natural to study algebras indecomposable up to matrix powers, of which we have the following characterization.

Lemma 42 *Let (A, F) be a finite algebra. The following are equivalent:*

1. *(A, F) is indecomposable up to matrix powers.*
2. *Whenever $\varphi : (A, F) \to (B, G)$ is a relational morphism to a finite algebra, either*
   (a) *$(A, F) \prec (D_\varphi^{[\mathrm{alg}]})^{[k]}$ for some k, or*
   (b) *$(A, F) \prec (B, G)^{[k]}$ for some k.*

Proof. Use the Covering Lemma and the properties of $()^{[\mathrm{alg}]}$ and $()^{[k]}$. □

I know of no way to show all cover simple algebras are indecomposable up to matrix powers (or in any other sense). However, in the case of one basic operation, we have the following.

Theorem 43 *Let (A, f) be cover simple and finite. Then (A, f) is indecomposable up to matrix powers.*

Proof. Clearly, f is surjective. Suppose $\varphi : (A, f) \to (B, g)$ is a relational morphism to a finite algebra. If φ is not injective, then there is a $b \in B$ such that $b\varphi^{-1} = A$. Define $xd = (x, \ldots, x)g$. Find $b \in B$ and $k > 0$ so that $bd^k = b$. Let n be the arity of f. Then we have an embedding $(A^k, h) \leq D_\varphi^{[\mathrm{alg}]}$ where h is n-ary and acts by

$$((x_{1,1}, \ldots, x_{1,k}), \ldots, (x_{n,1}, \ldots, x_{n,k}))h = \\ ((x_{1,2}, \ldots, x_{n,2})f, \ldots, (x_{1,k}, \ldots, x_{n,k})f, (x_{1,1}, \ldots, x_{n,1})f).$$

Let $C = \{(a, \ldots, a) : a \in A\}$. Then C is closed under h, and $(C, h) \cong (A, f)$. This shows that $(A, f) \leq D_\varphi^{[\mathrm{alg}]}$. □

I expect that the converse is false. The proof of the theorem is useful beyond the lemma itself: for (A, f) cover simple and finite, any $\varphi : (A, f) \to (B, g)$ for which there is a $b \in B$ such that $b\varphi^{-1} = A$ will have $(A, F) \prec D_\varphi^{[\mathrm{alg}]}$.

Chapter 4

Aprimal algebras

There are a number of reasons for studying classes closed under matrix power and division:

- Algebras are enormously general. Varieties go some of the way towards sorting out this generality. Classes closed under matrix power and division go somewhat farther. Another way of saying this is that, up to matrix power and division, there are fewer "primes".
- Wreath decomposition tools work well in this setting. Division allows us to decompose simple algebras. (Simple algebras cannot usefully be embedded in wreath products, because of the projection homomorphism.) Matrix powers are needed for the $()^{[alg]}$ construction and for the decomposition theorems for simple type 1 and 2 algebras (see Chapter 6).
- Such classes correspond to classes of computers closed under simulation and parallelism. Division is simulation. Matrix power is parallel processing. (See ???)
- Looking at algebras as concrete categories, division and matrix power together constitute a broad notion of being "inside" an algebra.
- Some well known classes are of this kind: the solvable and strongly solvable classes of Hobby-McKenzie [8].
- The resulting classification agrees with a useful classification of semigroups (see Chapter 7).

There are of course drawbacks inherent in this approach: a nonsolvable group, a nontrivial lattice, or a nontrivial Boolean algebra generates the largest class, the class of all finite algebras.

In this chapter, all algebras are finite, and indecomposable means indecomposable up to matrix power.

4.1 Classes defined by exclusion and by construction

In Birkhoff's setting of indexed algebras, the most interesting classes are those closed under the homomorphic image, subalgebra, and direct product constructions. In our nonindexed setting, we make more algebras isomorphic by ignoring the way in which generators for the clone are chosen. The interesting classes are therefore larger. The nonindexed analogues of Birkhoff's constructions are division and nonindexed product. To make the classes even larger, we use matrix power. Our wreath decomposition theory studies classes closed under these operations and classes formed by taking wreath products of such classes. Basic theorems connect classes maximal among those excluding various indecomposables with classes generated by other indecomposables.

Definition Let $\mathcal{K}$ be a class of algebras. We define

1. $\mathbf{I}\mathcal{K} = \{(B,G) : \text{ for some } (A,F) \in \mathcal{K}, (B,G) \cong (A,F)\}$
2. $\mathbf{M}\mathcal{K} = \{(A,F)^{[l]} : (A,F) \in \mathcal{K}, l \geq 0\}$
3. $\mathbf{R}\mathcal{K} = \{(A,G) : \text{ for some } (A,F) \in \mathcal{K}, G \subseteq F\}$
4. $\mathbf{S}\mathcal{K} = \{(B,F|_B) : \text{ for some } (A,F) \in \mathcal{K}, B \subseteq A \text{ and } BF \subseteq B\}$
5. $\mathbf{H}\mathcal{K} = \{(B,G) : \text{ for some } (A,F) \in \mathcal{K}, \text{there is a surjective homomorphism } (A,F) \to (B,G)\}$
6. $\mathbf{D}\mathcal{K} = \mathbf{HSR}\mathcal{K} = \{(B,G) : (B,G) \prec (A,F) \text{ for some } (A,F) \in \mathcal{K}\}$.

Lemma 44 *Let $\mathcal{K}$ be a class of algebras.*

1. *If $\mathbf{O}$ is any operator from the definition above, then $\mathbf{O}\mathcal{K} \supseteq \mathcal{K}$.*
2. *$\mathbf{IMM}\mathcal{K} = \mathbf{IM}\mathcal{K}$, $\mathbf{RR}\mathcal{K} = \mathbf{R}\mathcal{K}$, $\mathbf{SS}\mathcal{K} = \mathbf{S}\mathcal{K}$, $\mathbf{HH}\mathcal{K} = \mathbf{H}\mathcal{K}$.*
3. *$\mathbf{SH}\mathcal{K} \subseteq \mathbf{HS}\mathcal{K}$, $\mathbf{RH}\mathcal{K} \subseteq \mathbf{HR}\mathcal{K}$, $\mathbf{RS}\mathcal{K} \subseteq \mathbf{SR}\mathcal{K}$.*
4. *$\mathbf{D}\mathcal{K} = \mathbf{HSR}\mathcal{K}$, hence by (1), (2), and (3) $\mathbf{DD}\mathcal{K} = \mathbf{D}\mathcal{K}$.*
5. *$\mathbf{MD}\mathcal{K} \subseteq \mathbf{DM}\mathcal{K}$, hence by (4) $\mathbf{DMDM}\mathcal{K} = \mathbf{DM}\mathcal{K}$.*

Proof. Proofs of (1-3) are identical or similar to ones in Birkhoff's theory. Statement (1) for $\mathbf{O} = \mathbf{M}$ requires that we identify $(A,F)^{[1]}$ with (A,F). Statements (4) and (5) follow by lemmas in Chapter 2. □

Definition Let (A,F) be an algebra. We define $\mathbf{Excl}(A,F)$, the *exclusion class* of (A,F), to be the largest class $\mathcal{K}$ of algebras such that $(A,F) \notin \mathcal{K}$ and $\mathbf{DM}\mathcal{K} = \mathcal{K}$. More generally, let $\mathcal{L}$ be a class of algebras. We define $\mathbf{Excl}(\mathcal{L})$, the exclusion class of $\mathcal{L}$, to be the largest class $\mathcal{K}$ of algebras such that $\mathcal{K} \cap \mathcal{L} = \emptyset$ and $\mathbf{DM}\mathcal{K} = \mathcal{K}$.

Of course, to show $\mathbf{DM}\mathcal{K} = \mathcal{K}$ we need show only $\mathbf{DM}\mathcal{K} \subseteq \mathcal{K}$.

Definition Let $\mathcal{K}$ and $\mathcal{L}$ be classes of algebras. We define

1. $\mathcal{K} \circ \mathcal{L} = \{(A, F) \circ (B, G) : (A, F) \in \mathcal{K}$ and $(B, G) \in \mathcal{L}\}$.
2. $\mathbf{W}\mathcal{K} = \mathcal{K} \cup \mathcal{K} \circ \mathcal{K} \cup \mathcal{K} \circ \mathcal{K} \circ \mathcal{K} \cup \ldots$.
3. $\mathcal{K} \times \mathcal{L} = \{(A, F) \times (B, G) : (A, F) \in \mathcal{K}$ and $(B, G) \in \mathcal{L}\}$.

Note that $\circ$ is associative on classes of algebras just as it is on algebras. The product in (3) is essentially the varietal product studied in universal algebra.

Lemma 45 *Let $\mathcal{K}$ be a class of algebras.*

1. $\mathbf{WM}\mathcal{K} = \mathbf{MW}\mathcal{K}$
2. $\mathbf{WD}\mathcal{K} \subseteq \mathbf{DW}\mathcal{K}$

Proof. By Chapter 2. □

The next lemma says that exclusion classes of indecomposable algebras are closed under wreath product. Recall that here indecomposable means indecomposable up to matrix powers.

Lemma 46 *If $\mathcal{L}$ consists entirely of indecomposable algebras, then* $\mathbf{Excl}(\mathcal{L}) \circ \mathbf{Excl}(\mathcal{L}) \subseteq \mathbf{Excl}(\mathcal{L})$*, and therefore* $\mathbf{W}(\mathbf{Excl}(\mathcal{L})) \subseteq \mathbf{Excl}(\mathcal{L})$.

Proof. Let $(C, H), (B, G) \in \mathbf{Excl}(\mathcal{L})$. Suppose $(A, F) \in \mathcal{L}$ and $(A, F) \prec (C, H) \circ (B, G)$. Then either $(A, F) \prec (C, H)^{[k]}$, for some k, or $(A, F) \prec (B, G)^{[k]}$, for some k. But since $\mathbf{Excl}(L)$ is closed under $\mathbf{DM}$, $(A, F) \in \mathbf{Excl}(L)$, a contradiction. □

I expect that classes of finite algebras closed under finite nonindexed product and under taking divisors will be describable as "pseudo-hypervarieties", that is, classes of finite algebras defined by pseudo-hyperidentities. A hyperidentity is an ordinary identity universally quantified over all element and operation symbols occurring in it or, to put it another way, an identity in the language of clones. A pseudo-hyperidentity would likely involve implicit operations on the clone, in addition to the explicit operations on the clone given by the composition operations and the nullary operations whose values are projection operations. (See Reiterman, etc.) It should be interesting to ask how closure under $\mathbf{M}$ affects the pseudo-hyperidentites holding in a class. Also, what pseudo-hyperidentities define the classes discussed in the next section?

4.2 Four primary classes

In this section, we consider the class of solvable algebras and the class of strongly solvable algebras, which were defined (differently) in [8], and describe these classes in terms of **Excl** and in terms of **DMW**, using theorems from tame congruence theory. We also investigate two new exclusion classes, that of aprimal (or "weakly solvable") algebras and that of aperiodic algebras (generalizing aperiodic semigroups). Chapter 6 takes some first steps toward understanding these two classes in terms of **DMW**.

Definition

1. $Solv = \mathbf{Excl}(2, \wedge)$.
2. $StrSolv = \mathbf{Excl}\{(2, \wedge), (p, +) : p \text{ is prime}\}$.
3. $Aper = \mathbf{Excl}\{(p, +) : p \text{ is prime}\})$.
4. $Aprim = \mathbf{Excl}(2, \wedge, \neg)$.

Algebras in *Solv* are termed *solvable*; algebras in *StrSolv*, *strongly solvable*; algebras in *Aper*, *aperiodic*; algebras in *Aprim*, *aprimal*. Note that excluding cyclic groups is the same as excluding all groups, and excluding the two-element semilattice (or Boolean algebra) is the same as excluding all semilattices (or Boolean algebras). Also, by Lemma 4.3, these classes are in fact **DMW** classes.

An immediate consequence of the definition of *Aprim* is that, if $(A, F), (B, G) \notin Aprim$, then $\mathbf{DM}\{(A, F)\} = \mathbf{DM}\{(B, G)\}$. Hence there is only one **DM**-class properly containing *Aprim*, namely, the class of all finite algebras. We will soon prove that no nontrivial **DMW**-class is properly contained in *StrSolv*.

Proposition 47 *We have the following relations among the classes:*

1. $StrSolv = Aper \cap Solv$
2. $Aper \cup Solv \subseteq Aprim$

Proof. To show $Aper \subseteq Aprim$, use the fact that $(2, +) \leq (2, \wedge, \neg)$. □

Since *Aprim* is closed under wreath products, $\mathbf{W}(Aper \cup Solv) \subseteq Aprim$. It seems reasonable to guess that $\mathbf{W}(Aper \cup Solv) = Aprim$. This is in fact true for semigroups in *Aprim*, as we will see in Chapter 7, when we give a version of the Krohn-Rhodes theorem for semigroups using the wreath product of algebras. Hence the conjecture would, if true, amount to a analogue of the Krohn-Rhodes theorem for aprimal algebras. Also, the conjecture would lead to a complexity measure (see Chapter 5) on aprimal algebras by counting the minimal number of solvable factors in any decomposition involving only solvable and aperiodic algebras. This measure is defined for semigroups, is bounded above by the "two-sided" complexity of semigroups studied in [14] and [15]. There are aprimal algebras of arbitrary solvable aperiodic complexity (see Chapter 5).

Examples 2

1. All unary algebras are strongly solvable. Strongly solvable can be thought of as a generalization of unary.

2. A group is solvable in this sense iff it is solvable in the usual sense.

3. Aperiodic semigroups are exactly those with no nontrivial subgroups. For proofs and characterizations of aprimal, solvable, and strongly solvable semigroups, see Chapter 7.

4. Lattices, Boolean algebras, discriminator algebras, and so on are not aprimal by examples in Chapter 2.

The next two theorems connect the definitions of *Solv* and *StrSolv* above with the descriptions in Hobby-McKenzie of solvable and strongly solvable algebras. Parts of their proofs require terminology from tame congruence theory. However, the statements of these theorems do not involve such terminology, so a brief review of tame congruence theory is postponed until Chapter 6, where it is needed to state some theorems.

Theorem 48 *Let (A, F) be an algebra. The following are equivalent:*

1. $(A, F) \in \mathbf{Excl}\{(2, \wedge), (p, +) : p \text{ is prime}\} = StrSolv$.

2. $(A, F) \in \mathbf{DMW}\{(2, \emptyset)\}$.

3. *There do not exist distinct $a, b \in A$ and $f \in \mathrm{Pol}_2\ (A, F)$ with $(a, b)f = (b, a)f = a$ and $(b, b)f = b$.*

4. $(2, \wedge) \not\leq (A, \mathrm{Pol}\ (A, F))$ *and, for all p,* $(p, +) \not\leq (A, \mathrm{Pol}\ (A, F))$

Proof. To see that (1) $\Rightarrow$ (4), note that *StrSolv* is by definition closed under matrix powers and subreducts. Hence, by Lemma 2.13, whenever $(A, F) \in StrSolv$, we also have $(A, \mathrm{Pol}\ (A, F)) \in StrSolv$.

In the language of tame congruence theory, (4) implies that the types in Con (A, F) are all **1**. By Theorem 7.2 of [8], (3) is true.

Suppose (3). By Theorem 7.2 of [8], all types in the congruence lattice are **1**. We will prove in Chapter 6 that this implies (2).

Now assume (2). If we had $(2, \wedge) \prec (A, F)^{[k]}$, then

$$(2, \wedge) \prec (2, \emptyset)^{[k_1]} \circ \ldots \circ (2, \emptyset)^{[k_n]}.$$

Since $(2, \wedge)$ is indecomposable, $(2, \wedge) \prec (2, \emptyset)^{[k_i]}$ for some i. But $(2, \emptyset)^{[k_i]}$ is strongly solvable in the sense of Chapter 3 of [8], and $(2, \wedge)$ is not. The same argument works for group divisors, and we have proved (1). □

Note that (2) of the Theorem implies that *StrSolv* is contained in any nontrivial **DMW** class, since $(2, \emptyset)$ is the smallest nontrivial algebra (with respect

to division). Intuitively, strongly solvable algebras contain very little information. One way to say this is that complexity measures over aprimal algebras should not count the strongly solvable factors appearing in a wreath decomposition. Computationally, operations in a strongly solvable algebra correspond to the record-keeping tasks that any nontrivial machine can do whether or not it is capable of any kind of arithmetic or logical operations. (Here what a machine "can do" includes what it can do if it is run in parallel with copies of itself or in a sequential product with copies of itself.)

Theorem 49 *Let (A, F) be an algebra. The following are equivalent:*

1. $(A, F) \in \mathbf{Excl}(2, \wedge) = Solv$.
2. $(A, F) \in \mathbf{DMW}\{(p, +) : p \text{ is prime}\}$.
3. *There do not exist distinct $a, b \in A$ and $f \in \mathrm{Pol}_2\ (A, F)$ with $(a, a)f = (a, b)f = (b, a)f = a$ and $(b, b)f = b$.*
4. $(2, \wedge) \not\leq (A, \mathrm{Pol}\ (A, F))$

Proof. To see that (1) $\Rightarrow$ (4), note that *Solv* is by definition closed under matrix powers and subreducts. Hence, whenever $(A, F) \in Solv$, we also have $(A, \mathrm{Pol}\ (A, F)) \in Solv$. Obviously, (3) $\Leftrightarrow$ (4). For (3) $\Rightarrow$ (2), we use Theorem 7.2 of [8] to show that all types in Con (A, F) are **1** or **2**. Then we apply the decomposition theorem in Chapter 6.

Now assume (2). If we had $(2, \wedge) \prec (A, F)^{[k]}$, then

$$(2, \wedge) \prec (p_1, +)^{[k1]} \circ \cdots \circ (p_n, +)^{[k_n]}.$$

Since $(2, \wedge)$ is indecomposable, $(2, \wedge) \prec (p_i, +)^{[k_i]}$ for some i. But $(p_i, +)^{[k_i]}$ is solvable in the sense of Chapter 3 of [8], and $(2, \wedge)$ is not. □

Part (3) of either theorem is the primary means of checking membership; in particular, we can use it to decide membership in *StrSolv* and *Solv*. The membership problem of *Aprim* is slightly more difficult and that of *Aper* is much more difficult than those of *StrSolv* and *Solv*. Also, *Aper* and *Aprim* have not yet been characterized in terms of **DMW**.

Lemma 50 *Let $(2, G) \in \{(2, \wedge), (2, \wedge, \vee), (2, \wedge, \neg), (p, +) : p \text{ is prime}\}$. For any algebra (A, F), if $(2, G) \prec (A, F)$, then $(2, G) \leq (A, \mathrm{Pol}\ (A, F))$.*

Proof. This follows (with a little work) from Lemmas 4.15, 4.17, 4.20, and 9.14 of [8]. See the proof of Theorem 4.10. □

Theorem 51 *Let (A, F) be an algebra. The following are equivalent:*

1. $(A, F) \in \mathbf{Excl}(2, \wedge, \neg) = Aprim$.
2. $(A, F) \in \mathbf{Excl}(2, \wedge, \vee)$.

3. $(A, F) \in \mathbf{Excl}(B, G)$, *where* (B, G) *is a primal algebra with* $|B| > 1$.

4. $(A, F) \in \mathbf{Excl}(S, \cdot)$, *where* $(S, \cdot)$ *is a simple nonabelian group.*

5. $(2, \wedge, \neg) \not\leq (A, F)^{[|A|^2]}$.

Proof. (1) $\Rightarrow$ (2) is because $(2, \wedge, \neg) \leq (2, \wedge, \vee)^{[2]}$. (See 2.?) (2) $\Rightarrow$ (1) is because $(2, \wedge, \vee)$ is a reduct of $(2, \wedge, \neg)$. (1) $\Leftrightarrow$ (3) is because every primal algebra is isomorphic to a matrix power of $(2, \wedge, \neg)$ and $(2, \wedge, \neg)$ divides every primal algebra. (3) $\Rightarrow$ (4) is because $(S, \cdot, C_S)$ is primal and this algebra is a subreduct of a matrix power of $(S, \cdot)$. (4) $\Rightarrow$ (3) is because $(S, \cdot)$ divides a sufficiently large primal algebra. (1) $\Rightarrow$ (5) is by definition. To prove (5) $\Rightarrow$ (1), assume $(2, \wedge, \neg) \prec (A, F)^{[k]}$. By the lemma, $(2, \wedge, \neg) \leq (A, F)^{[k]}$. By Lemma 2.16, $(2, \wedge, \neg) \leq (A, F)^{[|A|^2]}$. □

In the language of tame congruence theory, aprimal algebras are those whose matrix powers have no type **3** (or, equivalently, type **4**) divisors. Be warned, however, that there are type **5** algebras which have type **3** divisors and are therefore not aprimal (see Example 6.2). Algebras which are not aprimal can be thought of as computationally complete. See ???.

The exponent in (5) may not be optimal, but we cannot in general reduce it below $(|A| - 1)/2$, as the following example shows.

Example 3 Let $k > 0$. We construct an algebra (A, F) with $(2, \wedge, \neg) \leq (A, F)^{[k]}$, but $(2, \wedge, \neg) \not\prec (A, F)^{[k-1]}$, and $|A| = 2k + 1$.

Let $A = \{0, a_1, \ldots, a_k, b_1, \ldots, b_k\}$. For $i = 1, \ldots, k$, define $f_i : A^{2k} \to A$ as follows:

$$(a_1, \ldots, a_k, a_1, \ldots, a_k)f_i = (a_1, \ldots, a_k, b_1, \ldots, b_k)f_i = \\ (b_1, \ldots, b_k, a_1, \ldots, a_k)f_i = b_i \\ (b_1, \ldots, b_k, b_1, \ldots, b_k)f_i = a_i$$

and f_i otherwise takes the value 0. Let F be the clone generated by $f_1, \ldots, f_k$. Then, in $(A, F)^{[k]}$, the binary operation $f_1 \times \cdots \times f_k$ is a Sheffer operation on $\{(a_1, \ldots, a_k), (b_1, \ldots, b_k)\}$. However, F_{2k-1} has no operations other than the projections and the constant c_0, because each f_i takes the value zero if any two of its $2k$ inputs are equal. The binary operations of $(A, F)^{[k-1]}$ are built from operations of F_{2k-2}, and so $(A, F)^{[k-1]}$ has no Boolean divisors.

Corollary 52 *For algebras with finitely generated clones, membership in Aper, Solv, and StrSolv are all decidable.*

Proof. Let (A, F) be an algebra such that F is finitely generated. Solvability and strong solvability of (A, F) can be checked as follows. Compute $\mathrm{Pol}_2(A, F)$. An effective method of doing this is given in Theorem 4.3 of [12]. If there is a pair $(a, b) \in A^2$ with $a \neq b$ and a polynomial $f \in \mathrm{Pol}_2(A, F)$ such that f is a semilattice operation on $\{a, b\}$, then (A, F) is not solvable; otherwise,

(A, F) is solvable. To check strong solvability, look for distinct $a, b \in A$ and $f \in \mathrm{Pol}_2\ (A, F)$ with $(a, b)f = (b, a)f = a$ and $(b, b)f = b$.

To check whether (A, F) is aprimal, we must check whether $(2, \wedge, \neg) \leq (A, F)^{[|A|^2]}$. But this is equivalent to following condition:

> there exist $f_1, \ldots, f_{|A|^2} \in F_{2|A|^2}$ and $\bar{a}, \bar{b} \in A^{|A|^2}$ such that
>
> > the operation $f_1 \times \cdots \times f_{|A|^2} : A^{2|A|^2} \to A^{|A|^2}$ is a Sheffer operation on $\{\bar{a}, \bar{b}\}$.

So we compute $F_{2|A|^2}$ (as in Thm. 4.3 of [12]) and then check, for each choice of $f_1, \ldots, f_{|A|^2} \in F_{2|A|^2}$ and $\bar{a}, \bar{b} \in A^{|A|^2}$ with $\bar{a} \neq \bar{b}$, whether this operation is a Sheffer operation. □

The following theorem gives the best criterion for aperiodic that I know.

Theorem 53 *Let (A, F) be an algebra. The following are equivalent:*

1. $(A, F) \in \mathbf{Excl}\{(p, +) : p \text{ is prime}\} = \mathit{Aper}$.
2. $(p, +) \not\leq (A, F)^{[k]}$ *for all prime p and all k.*

Proof. (1) ⇒ (2) is trivial. For (2) ⇒ (1), suppose $(p, +) \prec (A, F)^{[k]}$. By definition, there is $(B, G) \leq (A, F)^{[k]}$ and $\theta \in \mathrm{Con}\ (B, G)$ such that $(B, G)/\theta \cong (p, +)$. The interval $(\theta, 1_B)$ is type **2**. By Lemma 4.20 of [8], there is $(C, g) \leq (B, G)$ such that g is a Mal'cev operation on C (that is, (C, g) satisfies the identity $xxyg = y = yxxg$.) By Theorem 9.14 of [8], every type in $\mathrm{Con}\ (C, g)$ is **2** or **3**. In paticular, the interval $(0_C, \delta)$ is type **2** or **3**, where δ is a minimal nonzero congruence on (C, g). But then the $(0_C, \delta)$-traces are are either groups or two-element boolean algebras. Since these algebras are subreducts of $(C, \mathrm{Pol}\ (C, g)) \leq (B, \mathrm{Pol}\ (B, G)$, they are also (by Lemma 2.13) subreducts of $(B, G)^{[l]} \leq (A, F)^{[kl]}$ for some l. □

I do not know whether the property of being aperiodic is decidable. (Aperiodicity of semigroups *is* decidable, because our notion of aperiodic agrees with the traditional one—see Chapter 7.) The difficulty checking aperiodic results from the following two facts:

1. *Aper* is defined as the exclusion class of an infinite set of algebras (namely, the cyclic groups of prime order) which cannot be reduced, and
2. excluding these algebras requires checking arbitrarily high matrix powers, by an example analogous to Example 4.2.

There may be a bound on the size of prime numbers occuring as the orders of cyclic group divisors of matrix powers of a given aprimal algebra (with a finitely generated clone), and it seems likely that such a bound would be computable from the parameters of the algebra (the size of the universe, the number and

arities of basic operations, the operation tables themselves). Decidability of aperiodicity would follow in this case, for, by the methods used in the proof of 4.8, we can decide whether a *particular* prime occurs as the order of a cyclic group divisor of a matrix powers of the given algebra.

Decidability would also follow from a decomposition theorem for aperiodic algebras. For, on one hand, if every aperiodic algebra decomposes into algebras drawn from some recursively enumerable set of aperiodic algebras, then the set of isomorphism classes of aperiodic algebras can itself be enumerated by enumerating the basic aperiodics, their matrix powers, wreath products, divisors, and so on. On the other hand, (isom. classes of) non-aperiodic algebras can be enumerated by enumerating all algebras while looking for groups in their matrix powers.

However, the examples Chapter 7 suggest that the decomposition theory of aperiodics is quite involved. For instance, some aperiodics do not decompose into matrix powers of semilattices (though aperiodic semigroups do). The algebra of Example 6.3 has this property, but it does decompose into a semilattice and a group. This phenomenon suggests that finding a basic set into which all aperiodics decompose may become a significantly harder problem if we require that algebras in the basic set be aperiodic. Yet we must make this requirement if we wish to obtain a decomposition theorem of the kind required for a proof of decidability along the lines of the preceeding paragraph.

Chapter 6

Decomposing aprimal algebras

All algebras in this chapter are finite.

6.1 A little tame congruence theory

We review a enough ideas from tame congruence theory to make the statements, if not the proofs, of the upcoming theorems intelligible to the neophyte. For the complete treatment, see [8].

We say that $M \subseteq A$ is a *minimal set* of (A, F) if:

1. $|M| > 1$,
2. there is a $g \in \mathrm{Pol}_1\ (A, F)$ with $Ag = M$, and
3. if $h \in \mathrm{Pol}_1\ (A, F)$ and $Ah \subseteq Ag$, then either $Ah = Ag$ or $|Ah| = 1$.

Two subsets X, Y of A are said to be *polynomially isomorphic in* (A, F) if there are $f, g \in \mathrm{Pol}_1\ (A, F)$ with $Xf = Y$ and $Yg = X$. A basic theorem of tame congruence theory says that if (A, F) is simple, then all of its minimal sets are polynomially isomorphic. It follows that the algebras $(M, \mathrm{Pol}\ (A, F)|_M)$ are all isomorphic, where M ranges over minimal sets. Such algebras are known as *minimal* (or *permutational*). Any unary operation of a minimal algebra is either constant or a permutation. Up to polynomial equivalence, algebras with this property fall into five *types*, via the work of Pálfy (Thm. 4.7 of [8]), as follows:

type 1 unary algebras

type 2 vector spaces

type 3 $(2, \wedge, \neg)$

type 4 $(2, \wedge, \vee)$

type 5 $(2, \wedge)$.

(Note that, since all minimal sets in the type **5**—or **3** or **4**—case have two elements, condition (3) of the definition above is vapid in type **5**.) Hobby and McKenzie make use of these properties to assign a type in **1**..**5** to simple algebras and, more generally, to certain intervals in congruence lattices.

6.2 The D_φ and $()^{[\mathrm{alg}]}$ constructions preserve type

Among the intervals which can be assigned a unique type are the two-element intervals. In this section, we show that if φ is a homomorphism and $\ker\varphi$ is a minimal congruence, then $D_\varphi^{[\mathrm{alg}]}$ is a simple algebra of the same type as the two-element interval $(0, \ker\varphi)$.

Lemma 54 *If $\varphi : (A, F) \to (B, G)$ is a homomorphism such that $\ker\varphi$ is minimal among the nonzero elements of $\mathrm{Con}\,(A, F)$, and the interval $(0, \ker\varphi)$ has type $\mathbf{t}$, then the algebra $D_\varphi^{[\mathrm{alg}]}$ is simple and has type $\mathbf{t}$.*

Proof. We showed in Chapter 2 (Lem. 2.22) that, under these hypotheses, $D_\varphi^{[\mathrm{alg}]}$ is simple. We show here that this algebra has type **t**.

Let $\theta = \ker\varphi$, let $A_1, \ldots, A_k$ be the θ-classes, let M be a $(0,\theta)$-minimal set, and let N be a $(0,\theta)$-trace of M (that is, a nontrivial θ-class of M). Then, by Lemma 2.21, we may identify $D_\varphi^{[\mathrm{alg}]}$ with $(A_1 \times \cdots \times A_k, H)$, where

$$H_n = \left\{ h_1 \times \cdots \times h_k : \begin{array}{l} \text{for all } i,\ h_i = f_i|_{(A_1\times\cdots\times A_k)^n} \text{ for some } f_i \in \\ F_{nk} \text{ with } (A_1 \times \cdots \times A_k)^n f_i \subseteq A_i \end{array} \right\}.$$

We may assume $N = A_1 \cap M$. Now choose $a_2 \in A_2, \ldots, a_k \in A_k$, and consider the set $N' = N \times \{a_2\} \times \cdots \times \{a_k\}$. We show that N' is a minimal set of $(A_1 \times \cdots \times A_k, H)$.

Let $e \in \mathrm{Pol}_1\,(A, F)$ be an idempotent with $Ae = M$. Then $A_1 e \subseteq M$ and $A_1 e \supseteq Ne = N$. Since A_1 is a θ-class, $A_1 e \subseteq A_1$. Putting all this together, $N \subseteq A_1 e \subseteq A_1 \cap M = N$, whence $A_1 e = N$. So N' is the image of the unary polynomial $(x_1, \ldots, x_k) \mapsto (x_1 e, a_2, \ldots, a_k)$ of $(A_1 \times \ldots \times A_k, H)$. This proves part (2) of the definition of minimal set.

For part (3), we must show that there is no nontrivial polynomial image properly contained in N'. Assuming this fails, let P be minimal among such images. Then, since $(A_1 \times \cdots \times A_k, H)$ is simple, Lemma 2.8 of [8] says that $P = (A_1 \times \cdots \times A_k)h$, where $h = (h_1, \ldots, h_k) \in \mathrm{Pol}_1\,(A_1 \times \cdots \times A_k, H)$ and $h^2 = h$. Now consider the unary polynomial $f : x \mapsto (x, a_2, \ldots, a_k)h_1$ of (A, F) We have $Nf = (N \times \{a_2\} \times \cdots \times \{a_k\})h_1 = N'h_1$. But, since $Ph = P$, $P = N'h_1 \times \{a_2\} \times \cdots \times \{a_k\}$ is nontrivial and properly contained in $N' = N \times \{a_2\} \times \cdots \times \{a_k\}$. So $N'h_1 = Nf$ is nontrivial and properly contained in N. This contradicts the fact that N is inside the minimal set M.

Finally, we must show that the type of the minimal set N' is **t**. This follows from the easy observation that $(N', \mathrm{Pol}\,(A_1\times\cdots\times A_k, H)|_{N'}) \cong (N, \mathrm{Pol}\,(A, F)|_N)$. □

A similar proof shows that matrix power preserves not only the congruence lattice, but the type labelling on it. We prove a special case of this below.

6.3 Decomposing solvable and strongly solvable algebras

Suppose (A, F) is solvable. By the previous section, we can decompose (A, F) into simple algebras corresponding in a natural way to the two-element intervals in a maximal chain of Con (A, F). By theorems in [8], each interval is of type **1** or **2**, so the simple algebras are of type **1** or **2**, and we can embed these algebras in matrix powers of $(2, \emptyset)$ or $(p, +)$, for appropriate p, respectively.

Theorem 55

1. *If (A, F) is simple and type* **1**, *then $(A, F) \leq (2, \emptyset)^{[k]}$, for some k.*
2. *If (A, F) is simple and type* **2**, *then $(A, F) \leq (p, +)^{[k]}$, for some prime p and some k. Furthermore, $(p, +) \leq (A, \mathrm{Pol}\ (A, F))$.*

Proof. These statements follow easily from Theorems 13.3 and 13.5 in [8], using Lemma 2.13 to obtain polynomials in a subreduct of a sufficiently high matrix power. □

Theorem 56

1. *If (A, F) is strongly solvable, $(A, F) \leq (2, \emptyset)^{[k_1]} \circ \cdots \circ (2, \emptyset)^{[k_n]}$ for some $k_1, \ldots, k_n$.*
2. *If (A, F) is solvable, $(A, F) \leq (p_1, +)^{[k_1]} \circ \cdots \circ (p_n, +)^{[k_n]}$ for some primes $p_1, \ldots, p_n$ and integers $k_1, \ldots, k_n$. Unless (A, F) is strongly solvable, we can choose each p_i so that $(p_i, +) \leq (A, \mathrm{Pol}\ (A, F))$.*

Proof. If (A, F) is solvable, then we know from Theorem 7.2 in [8] that all types in the congruence lattice are **1** or **2**. Let θ be a minimal nonidentity congruence. Applying the Covering Lemma to the corresponding quotient morphism φ, $(A, F) \leq D_\varphi^{[\mathrm{alg}]} \circ (A/\theta, F)$. But $D_\varphi^{[\mathrm{alg}]}$ is simple and of type **1** or **2** by Lemma 6.1.

If the type is **1**, then $D_\varphi^{[\mathrm{alg}]} \leq (2, \emptyset)^{[k_1]} \leq (p_1, +)^{[k_1]}$, for some k_1 and any p_1. Unless (A, F) is strongly solvable, we may choose p_1 so that $(p_1, +) \leq (A, \mathrm{Pol}\ (A, F))$.

If the type is **2**, then $D_\varphi^{[\mathrm{alg}]} \leq (p_1, +)^{[k_1]}$, for some p_1 and k_1. By the previous theorem, $(p_1, +) \leq (A, \mathrm{Pol}\ (A, F))$.

In each case, we apply the Covering Lemma to obtain $(A, F) \leq (p_1, +)^{[k_1]} \circ (A/\theta, F)$. Since $(A/\theta, F)$ is solvable, (2) follows by induction.

The proof of (1) is easier, and is left as an exercise. □

Actually, applying the Covering Lemma to the homomorphism φ in the proof yields a division which need not be an embedding. However, there is such an embedding when $(A, F) = (A, \mathrm{Pol}\,(A, F))$ (see Chapter 2). Since $(A, \mathrm{Pol}\,(A, F))$ is solvable if (A, F) is, and $(A, F) \leq (A, \mathrm{Pol}\,(A, F))$, the general statement of the theorem follows.

Since wreath product and matrix power commute, we could have written the decomposition in (1) as $(A, F) \prec ((2, \emptyset) \circ \cdots \circ (2, \emptyset))^{[k]}$, where $k = \max\{k_1, \ldots, k_n\}$. A similar remark holds for (2).

When (2) is applied to a solvable group (Hobby-McKenzie's sense of solvable agrees with the usual notion for groups), the groups $(p_1, +), \ldots, (p_n, +)$ are the Jordan-Hölder factors (up to repetitions).

Exercise A Coordinate System for Solvable Algebras Show that an algebra is solvable iff it is a subalgebra of some algebra of the following form. Let $k_1, \ldots, k_n$ be positive numbers, and let $p_1, \ldots, p_n$ be prime. The universe is $\{0, \ldots, p_1 - 1\}^{k_1} \times \cdots \times \{0, \ldots, p_n - 1\}^{k_n}$. Each binary operation has the following form:

$$
\begin{aligned}
&((\bar{x}_1, \ldots, \bar{x}_{k-2}, \bar{x}_{k-1}, \bar{x}_k), (\bar{y}_1, \ldots, \bar{y}_{k-2}, \bar{y}_{k-1}, \bar{y}_k)) \mapsto \\
&\quad (L_1(\bar{x}_1, \ldots, \bar{x}_k, \bar{y}_1, \ldots, \bar{y}_k) \cdot \bar{x}_1 + M_1(\bar{x}_1, \ldots, \bar{x}_k, \bar{y}_1, \ldots, \bar{y}_k) \cdot \bar{y}_1, \\
&\quad \vdots \\
&\quad L_{k-2}(\bar{x}_{k-1}, \bar{x}_k, \bar{y}_{k-1}, \bar{y}_k) \cdot \bar{x}_{k-2} + M_{k-2}(\bar{x}_{k-1}, \bar{x}_k, \bar{y}_{k-1}, \bar{y}_k) \cdot \bar{y}_{k-2}), \\
&\quad L_{k-1}(\bar{x}_k, \bar{y}_k) \cdot \bar{x}_{k-1} + M_{k-1}(\bar{x}_k, \bar{y}_k) \cdot \bar{y}_{k-1}), \\
&\quad L_k \cdot \bar{x}_k + M_k \cdot \bar{y}_k)
\end{aligned}
$$

where $\bar{x}_i, \bar{y}_i \in \{0, \ldots, p_i - 1\}^{k_i}$ and the L_i and M_i are functions from tuples of integers to square matrices of integers of the appropriate size. (Note that that algebra does not necessarily have *all* such operations.) Operations of other arities have an analogous form.

6.4 Properties of simple type 5 algebras

Consider the problem of finding a decomposition of a aprimal algebra (A, F) into aperiodic and solvable pieces. By the Covering Lemma and Lemma 6.1, we can reduce this problem to simple algebras all having types from Con (A, F). Types **3** and **4** do not occur in a aprimal algebra. So (A, F) decomposes into simple algebras of types **1**, **2**, and **5**. Having type **1** or **2** yields strong global properties for a simple algebra (the embeddings into matrix powers of $(2, \emptyset)$ or $(p, +)$).

Hence we can reduce our problem to the case of simple algebras of type **5**. These algebras are very problematic. There is no matrix representation for simple algebras of type **5**, except of course for the embedding in a matrix power of $(2, \wedge, \neg)$. Such an embedding can be found for any algebra. This cannot be improved upon in general: as Example 6.2 below shows, there are

simple type **5** algebras in which $(2, \wedge, \neg)$ itself embeds. Of course, such an algebra is not aprimal. We can, however, construct simple type **5** algebras with arbitrary (aprimal) subreducts (see Example 6.2, below). So no useful matrix representation can hold for simple type **5** algebras in general. In a sense, the reduction to the simple type **5** case is no reduction at all!

In semigroup theory, this case is handled with an ordering; the cover of maximal principal $\mathcal{H}$-order ideals leads to a decomposition. Tame congruence theory provides a generalization of this ordering (Theorem 6.4, which we can try to use to obtain decompositions. The motivation for this project is Corollary 6.10, which says that if the inverse image sets of a relational morphism each lie below a maximal element of the ordering, then the derived algebra is aperiodic.

A relation $R \subseteq A^n$ is called an *admissible* relation of an algebra (A, F) if R is closed under the operations of (A^n, F).

Theorem 57 (Hobby-McKenzie, Thm. 13.6) *Let (A, F) be any finite simple algebra of type* **4** *or* **5**. *There are six subalgebras $\rho_0, \rho_1, \zeta_0, \zeta_1, \xi_0, \xi_1$ of (A^2, F) such that $0_A \subset \rho_i \subseteq \zeta_i \subseteq \xi_i (i = 0, 1), \rho_1 = \rho_0^{-1}, \zeta_1 = \zeta_0^{-1}, \xi_1 = \xi_0^{-1}, \xi_0 \cap \xi_1 = 0_A$, and*

1. *ρ_0 and ρ_1 are the minimal reflexive admissible relations on (A, F), and $\rho_0 \cup \rho_1 = 0_A \cup \{N^2 : N$ is a minimal set of $(A, F)\}$;*
2. *ζ_0 and ξ_0 are connected partial orderings of A, and ζ_0 is the transitive closure of ρ_0;*
3. *for every admissible partial ordering μ of (A, F) such that $0_A < \mu$, either $\zeta_0 \leq \mu \leq \xi_0 or \zeta_1 \leq \mu \leq \xi_1$.*

At the moment, we are interested only in type **5**. In this case, for each minimal set N, the algebra $(N, \text{Pol } (A, F)|_N))$ is isomorphic to $(2, \wedge, c_0, c_1)$. If, for this particular N, the zero element of the semilattice $(N, \text{Pol } (A, F)|_N))$ is ρ_0-below the unit element, then the same is true for any minimal set N' (because N and N' are polynomially isomorphic and polynomials preserve admissible relations). If, on the other hand, the zero of N is ρ_0-above the unit, then the same is true for any minimal set N', and the zero of N is ρ_1-below the unit. By convention, we assume that ρ_0 is the one which "orients" the minimal algebras with the zero below the unit. Then ζ_0 is referred to as the *natural ordering* of (A, F), and we frequently drop the subscript. Similarly, ρ_0 is referred to simply as ρ. For clarity, we often write $x \leq_\zeta y$ when $x \zeta y$ and $x \leq_\rho y$ when $x \rho y$.

Lemma 58 *Suppose (A, F) is simple and of type* **5**. *Then $(A, F)^{[k]}$ is simple and of type* **5**.

Proof. First, $(A, F)^{[k]}$ is simple because Con $(A, F)^{[k]} \cong$ Con (A, F), by Corollary 2.10.

Suppose the type of (A, F) is **5**. This means that (A, F) has a minimal set $\{a, b\}$ of type **5**. Equivalently, we have $\{a, b\} \subseteq A$ and $g \in \text{Pol}_1 (A, F)$ with

1. $\{a, b\} = Ag$, and
2. $(\{a, b\}, \text{Pol } (A, F)|_{\{a,b\}}) \cong (2, \wedge)$.

We construct a minimal set for $(A, F)^{[k]}$. Let $\bar{a} = (a, a, \ldots, a), \bar{c} = (b, a, \ldots, a) \in A^k$. Define $g' : A^k \to A^k$ by $(x_1, \ldots, x_k) \mapsto (x_1 g, a, \ldots, a)$. Then $A^k g' = \{\bar{a}, \bar{c}\}$. By Corollary 2.10, $g' \in \text{Pol}_1 (A, F)^{[k]}$. So $\{\bar{a}, \bar{c}\}$ is a minimal set of $(A, F)^{[k]}$.

To prove that the type is **5**, we construct an isomorphism

$$\varphi : (\{\bar{a}, \bar{c}\}, \text{Pol } (A, F)^{[k]}|_{\{\bar{a},\bar{c}\}}) \to (a, b, \text{Pol } (A, F)|_{\{a,b\}}) \cong (2, \wedge).$$

Let $\bar{a}\varphi = a$ and $\bar{c}\varphi = b$. If $\bar{f} \in \text{Pol}_n (A, F)^{[k]}|_{\{\bar{a},\bar{c}\}}$, we may write $\bar{f} = f_1 \times c_a \times \cdots \times c_a$ for some $f_1 \in \text{Pol}_{nk} (A, F)|_{\{a,b\}}$. Define $f : \{a, b\}^n \to \{a, b\}$ by $(x_1, \ldots, x_n)f = ((x_1, a, \ldots, a), \ldots, (x_n, a, \ldots, a))f_1$. It is easy to see that $f \in \text{Pol}_n (A, F)$ and also $\{a, b\}^n f \subseteq \{a, b\}$. Hence $f \in \text{Pol } (A, F)|_{\{a,b\}}$. Let $\bar{f}\varphi f$. The pair $\bar{f}\varphi f$ preserves the pairs $\bar{a}\varphi a$ and $\bar{c}\varphi b$, so φ is a morphism. Showing that φ surjects on operations is left to the reader. This isomorphism shows that the minimal set $\{\bar{a}, \bar{c}\}$ is of type **5** and therefore $(A, F)^{[k]}$ is of type **5**. □

Lemma 59 *Suppose (A, F) is simple of type* **5**, *with natural ordering ζ. Then the minimal sets of $(A, F)^{[k]}$ are precisely the sets of the form*

$$\{(a_1, \ldots, a_k), (b_1, \ldots, b_k)\},$$

where

1. *for some i, $a_i \neq b_i$, and*
2. *for each i, either $a_i = b_i$ or $\{a_i, b_i\}$ is a minimal set of (A, F) with $a_i \zeta b_i$.*

Proof. First, let $\{\bar{a}, \bar{b}\}$ be a set of the specified form. By (1), $a \neq b$. Choose a minimal set $\{c, d\}$ with $c\zeta d$ and choose $g \in \text{Pol}_1 (A, F)$ with $Ag = \{c, d\}$. Using (2) and the definition of minimal, we can find $g_1, \ldots, g_k \in \text{Pol}_1 (A, F)$ such that, for each i, if $a_i = b_i$ then $g_i = c_{a_i}$ and if $a_i \neq b_i$ then $cg_i = a_i$ and $dg_i = b_i$. Then $\{\bar{a}, \bar{b}\}$ is the image of A^k under the map $(x, \ldots) \mapsto (xgg_1, \ldots, xgg_k)$, and this map is in $\text{Pol}_1 (A, F)^{[k]}$. Therefore $\{\bar{a}, \bar{b}\}$ is a minimal set.

Now suppose M is a minimal set of $(A, F)^{[k]}$. By the previous lemma, the type of $(A, F)^{[k]}$ is **5**, so all minimal sets have two elements. Write $M = \{\bar{a}, \bar{b}\}$. By definition, we have $\bar{g} = g_1 \times \ldots \times g_k \in \text{Pol}_1 (A, F)^{[k]}$ with $A^k \bar{g} = \{\bar{a}, \bar{b}\}$. Each g_i is a k-ary polynomial of (A, F). If g_1 depends on some variable, say the j-th, choose $d_1, \ldots, d_k$ so that the operation h_1 defined by $xh_1 = (d_1, \ldots, d_{j-1}, x, d_{j+1}, \ldots, d_k)g_1$ is not constant. Otherwise, let h_1 be the unary constant map whose value is the constant value of g_1. Define $h_2, \ldots, h_k$ similarly. Since $\bar{g}$ is not constant, some g_i depends on some variable. So $\bar{h} = h_1 \times \cdots \times h_k$ is not constant. Clearly $A^k \bar{h} \subseteq A^k \bar{g}$. Therefore $A^k \bar{h} = A^k \bar{g}$. By our construction, each h_i depends on at most one variable. If any h_i and $h_{i'}$ depend on distinct variables, then $A^k \bar{h}$ would have at least four elements. So there is a j

such that each h_i either is constant or depends on the j-th variable. Choose i so that h_i is nonconstant. Choose $c, d \in A$ so that $c\zeta d$ and h_i is nonconstant on $\{(c,\dots,c),(d,\dots,d)\}$. (This can be done because ζ is connected and h_i preserves ζ.) Then $\{(c,\dots,c),(d,\dots,d)\}\bar{h} = \{\bar{a},\bar{b}\}$. We may assume that $(c,\dots,c)\bar{h} = \bar{a}$ and $(d,\dots,d)\bar{h} = \bar{b}$. Since $\bar{a} \neq \bar{b}$, (1) is satisfied. Also, for each i, if $a_i \neq b_i$, then h_i is nonconstant, and (a_i, b_i) is the image of (c, d) under the unary polynomial $(x,\dots,x)h_i$. Therefore, $\{a_i, b_i\}$ is a minimal set of (A, F) and, since $c\zeta d$, $a_i\zeta b_i$. □

In the following, if ζ is a binary relation on a set A then ζ^k denotes the binary relation $\{((x_1,\dots,x_k),(y_1,\dots,y_1)) : x_1\zeta y_1,\dots,x_k\zeta y_k\}$ on A^k.

Lemma 60 *Suppose (A, F) is simple type* **5** *with natural ordering ζ. Then the natural ordering of $(A, F)^{[k]}$ is ζ^k.*

Proof. We must show that ζ^k is the transitive closure of $\{(\bar{a},\bar{a}) : \bar{a} \in A^k\} \cup \{(\bar{a},\bar{b}) : \{\bar{a},\bar{b}\}$ is a minimal set of $(A, F)^{[k]}$ and a is the zero of the induced semilattice$\}$. This follows easily from the previous lemma. □

6.5 Which simple type 5 algebras are aperiodic?

Theorem 61 *Suppose (A, F) is simple type* **5**. *If the natural ordering ζ on (A, F) has a maximum element, then (A, F) is aperiodic.*

Proof. By Theorem 4.10, (A, F) is aperiodic if and only if $(A, F)^{[k]}$ has no group subreducts, for all k. However, if (A, F) satisfies the hypotheses of the theorem, then so does $(A, F)^{[k]}$, by the preceding lemmas and by the observation that if ζ has a maximum element then so does ζ^k. Hence to prove the theorem it suffices to show that, for all (A, F) satisfying the hypotheses, (A, F) has no group subreducts.

Let (A, F) satisfy the hypotheses. Denote the maximum element by 1. Suppose that there is a nontrivial group (C, f) with $C \subseteq A$ and $f \in F_2$. Let $D = \{x \in A :$ for all $c \in C, c \leq_\zeta x\}$. Clearly, $1 \in D$, so D is nonempty.

Claim 1: $(C \times D)f \subseteq D$ and $(D \times C)f \subseteq D$. Let $c_0 \in C$, $d_0 \in D$. For any $c \in C$, $c = (c_0, (c_0^{-1}, c)f)f \leq_\zeta (c_0, d_0)f$, where $^{-1}$ denotes inverse in the group. So $(c_0, d_0)f \in D$. This proves the first half of the claim, and the second half is proved symmetrically.

Claim 2: $(D \times D)f \subseteq D$. Let $d_0, d_1 \in D$. For any $c \in C$, $c = (c, u)f \leq_\zeta (d_0, d_1)f$, where u denotes the identity element of the group. This proves the claim.

Define a binary relation θ on $C \cup D$ by $\theta = (C \times C) \cup (D \times D)$. Note that $C \cap D = \emptyset$. (If not, there is a $c_0 \in C$ such that, for any $c \in C$, we have $c \leq_\zeta c_0$. This contradicts the facts that f is a nontrivial group operation on C and that f preserves $\leq_\zeta$.) So θ is an equivalence relation.

Claims 1 and 2, together with the fact that $(C \times C)f \subseteq C$, show that θ is admissible and therefore a congruence of $(C \cup D, f)$, and that $((C \cup D)/\theta, f)$

is a semilattice with absorbing element D/θ. By Lemma 4.15 of [8], there are $c \in C$, $d \in D$, and an operation $p \in \mathrm{Pol}_2\ (A, F)$ with table

p	c	d
c	c	d
d	d	d

Since $c \leq_\zeta d$, we can choose a, b with $c \leq_\zeta a \leq_\rho b \leq_\zeta d$ and a', b' with $c \leq_\zeta a' \leq_\rho b' \leq_\zeta d$ such that p takes values as follows, for some e:

p	c	a'	b'	d
c	c			d
a		e	d	
b		d	d	
d	d			d

(Here, ρ corresponds to ζ as in 6.4.) Since ρ is preserved by unary polynomials, $e \leq_\rho d$, and $\{e, d\}$ is a trace of (A, F). Consequently, there are polynomial isomorphisms between $\{a, b\}$, $\{a', b'\}$, and $\{e, d\}$. Therefore, the induced algebra $(A, F)|_{\{e,d\}}$ is a lattice, contradicting the assumption that (A, F) is type **5**. □

Corollary 62 *Semilattices are aperiodic.*

Proof. Trivially, $(2, \wedge)$ is simple type **5**. The natural ordering is the usual semilattice ordering with $0 < 1$, so Theorem 6.8 shows that $(2, \wedge)$ is aperiodic. Any semilattice is in $\mathbf{DMW}(2, \wedge)$. □

This corollary suggests the question: is $Aper = \mathbf{DMW}(2, \wedge)$? For semigroups, this is true (see Chapter 7). However, it is not true in general, by Example 6.3.

The main application of Theorem 6.8 lies in showing that a broad class of relational morphisms defined on simple type **5** algebras have aperiodic derived algebras. More precisely, the following corollary shows that, if each inverse image set of a relational morphism lies below one of the maximal elements of $\leq_\zeta$, then the $()^{[\mathrm{alg}]}$ of the derived algebra is aperiodic.

Let (A, F) be simple type **5**. Observe that the principal order-ideals of $\leq_\zeta$ form a cover[1]

$$\mathcal{C}_\zeta = \{\{x : x \leq_\zeta a\} : a \in A\}.$$

It is easy to see that $D^{[\mathrm{alg}]}_{\mathcal{C}_\zeta}$ is aperiodic. ($D^{[\mathrm{alg}]}_{\mathcal{C}_\zeta}$ is simple type **5** with ordering equal to the product of the orderings on the principal order-ideals, and so we can apply 6.8.) The next corollary is a much stronger statement but also much harder to prove.

[1]The *maximal* principal order-ideals likewise form a cover, and this cover is equivalent to $\mathcal{C}_\zeta$, but the more refined cover has certain technical advantages.

Corollary 63 *Let (A, F) be a simple type* **5** *algebra with natural ordering $\leq_\zeta$. If $\varphi : (A, F) \to (B, G)$ is a relational morphism with $\mathcal{C}_\varphi \leq \mathcal{C}_\zeta$, then $D_\varphi^{[\mathrm{alg}]}$ is aperiodic.*

Sketch of proof. Much as in the proof of 6.8, we need only show that, in all situations satisfying the hypotheses, D_φ has no group subreducts in any local algebra. (It is left to the reader to show that if $(D_\varphi^{[\mathrm{alg}]})^{[l]}$ has a group subreduct then $D_{\varphi^{kl}}$ (where $k = |B|$) has a group subreduct in some local algebra, for a naturally defined $\varphi^{kl} : (A, F)^{[kl]} \to (B, G)^{[kl]}$ satisfying the hypotheses.)

Assume $\varphi : (A, F) \to (B, G)$ satisfies the hypotheses and $(p, +) \leq D_\varphi$ for some prime p. By Prop. 1.6, $D_\varphi \leq (A, F)$. Let $g_0, \ldots, g_{p-1} \in A$ be the images under the aforementioned embeddings of $0, \ldots, p-1$, respectively. Choose $f \in F_p$ such that f induces p-fold addition (that is, the operation $(x_1, \ldots, x_p) \mapsto x_1 + \cdots + x_p$) on the embedded group elements $g_0, \ldots, g_{p-1}$.

Observe that $\{g_0, \ldots, g_{p-1}\}$ lies under some $s \in A$, by the hypothesis that $\mathcal{C}_\varphi \leq \mathcal{C}_\zeta$. Define, for $x \in A$, $xd = (x, \ldots, x)f$. Choose $t \in \{s, sd, sd^2, \ldots\}$ such that $td^n = t$ for some $n > 0$. Observe that, for each i, $g_i \leq_\zeta t$, by the definition of d, the fact that f preserves ζ, and the fact that f is a group operation and hence surjective on $\{g_0, \ldots, g_{p-1}\}$.

Since $(t, \ldots, t)f^n = td^n = t$, it follows that f^n (exponentiation as in Chapter 3) induces an operation on the local algebra of $D_{\mathcal{C}_\zeta}$ at $\{x \in A : x \leq_\zeta t\}$. But since p-fold addition is iterable (See Chapter 3), the operation that f^n induces on $\{g_0, \ldots, g_{p-1}\}$ generates p-fold addition, which in turn generates ordinary binary addition in the group. This contradicts the easy observation that $D_{\mathcal{C}_\zeta}^{[\mathrm{alg}]}$ is aperiodic. □

6.6 "Filling in the blanks"

With Corollary 6.10 in hand, the approach to decomposing a simple type **5** algebra (A, F) is as follows. If the natural ordering $\leq_\zeta$ has a top element, then the algebra is aperiodic. If not, consider the partial algebra structure F induces on the set of maximal elements. If this partial algebra is in fact total, then Lemma 6.11 below shows how to decompose the algebra in terms of an aperiodic and the subalgebra formed by the top elements.

In general, however, we have to deal with a properly partial algebra. In a special case, we can construct a relational morphism with aperiodic derived algebra by "filling in the blanks" of the partial algebra (Lemma 6.12). The crucial question is: can we fill in the blanks in such a way that the resulting algebra is no more (and preferably less) complex than the original algebra? There are examples showing that sometimes we can, and sometimes we can't. In cases where we can't, but where there is nevertheless a satisfactory decomposition, it appears that a more sophisticated version of filling in the blanks is at work.

Lemma 64 *Let (A, F) and ζ be as above. Suppose $B \subseteq A$ is closed under F and every $\leq_\zeta$-maximal $x \in A$ is in B. Then $(A, F) \in \mathbf{D}(Aper \circ \{(B, F)\})$.*

Proof. Define $\varphi : (A, F) \to (B, F)$ as follows. Set $a\varphi b$ whenever $a \leq_\zeta b$ and set $f\varphi f$ for all $f \in F$. Then φ is a relational morphism, because operations preserve ζ and every $a \in A$ is below some $b \in B$. Since $\mathcal{C}_\varphi \leq \mathcal{C}_\zeta$, Cor. 6.10 implies that $D_\varphi^{[\mathrm{alg}]}$ is aperiodic. □

Of course, the last lemma says nothing useful when $A = B$.

An element 0 of an algebra (A, F) is called absorbing if

$$(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots x_n)f = 0$$

for all $i, n, x_1, \ldots, x_n \in A, f \in F$.

Lemma 65 *Let (A, F) be a simple type* **5** *algebra such that $A = B \cup 0$, with $0 \notin B$. Assume that the ordering ζ is height 1, elements of B are atoms, 0 is a minimum element, and 0 is absorbing. Suppose (B, F') is an algebra such that for each $f \in F_n$ there is an $f' \in F'_n$ with $(b_1, \ldots, b_n)f' = (b_1, \ldots, b_n)f$ whenever $(b_1, \ldots, b_n)f \neq 0$. Then $(A, F) \in \mathbf{D}(Aper \circ (B, F'))$.*

Proof. Repeat the proof of 6.11, but take $f\varphi f'$ for all $f \in F$ and $f' \in F'$. Note that $0\varphi B$, so when $(b_1, \ldots, b_n)f = 0$, we have $(b_1, \ldots, b_n)f\varphi(b_1, \ldots, b_n)f'$. □

6.7 Examples

Example 4 Let $(A, F) = (\{0, a, b\}, f, u)$, where f is the binary operation with the following table:

f	a	b	0
a	a	b	0
b	b	a	0
0	0	0	0

and u is the unary operation $a \mapsto 0$, $b \mapsto b$, $0 \mapsto 0$. Then (A, F) has the following properties:

1. (A, F) is aprimal. (One can show this directly, using Theorem 4.8, or simply decompose it into algebras which are already known to be aprimal, as we do below.)

2. (A, F) is simple and of type **5**. The minimal sets are $\{0, a\}$ and $\{0, b\}$. The natural ordering is determined by $0 \leq_\zeta a$, $0 \leq_\zeta b$.

3. No type other than **5** occurs in the variety generated by (A, F) (this takes a little work).

4. $(A, F) \in \mathbf{D}(Aper \circ Solv)$. (In fact, $(A, F) \prec (2, \wedge, c_0) \circ (2, +)$. One can do this by filling in the blank $u : a \mapsto 0$ with $u' : a \mapsto a$, so that u' is the identity map.)

Example 5 Embedding arbitrary algebras in simple type 5 algebras Let (B, G) be any algebra. Define an algebra (A, F) as follows. The elements are B plus a new zero: $A = B \cup \{0\}$, where $0 \notin B$. For $g \in G_n$, define $g' : A^n \to A$ by $g'|_B = g$ and $(x_1, \ldots, x_n)g' = 0$ if any x_i is 0. For $b \in B$, define $e_b, f_b : A \to A$ by

$$xe_b = b \text{ if } x \neq 0 \qquad 0e_b = 0$$
$$xf_b = 0 \text{ if } x \neq b \qquad bf_b = b$$

Take F to be the clone generated by $\{g' : g \in G\} \cup \{e_b : b \in B\} \cup \{f_b : b \in B\}$.

Then (A, F) is simple because of the e_b and f_b operations. The minimal sets are pairs $\{0, b\}$ with $b \in B$, and the induced algebra $(\{0, b\}, \text{Pol } (A, F)|_{\{0,b\}})$ is a semilattice, so (A, F) is type **5**. However, $(B, G) \leq (A, F)$. We can decompose (A, F) much as in the previous example: $(A, F) \prec (2, \wedge, c_0) \circ (B, G, C_G)$. The details are left to the reader (the constant operations come from the e_b and f_b operations). This decomposition implies that (A, F) is aprimal (or aperiodic) if (B, G) is.

Example 6 Consider the algebra $(A, f) = (\{a, b, 0\}, f)$, where f is the ternary operation given by

$(a,-,-)f$	a	b	0
a	a	0	0
b	0	b	0
0	0	0	0

$(b,-,-)f$	a	b	0
a	0	b	0
b	b	a	0
0	0	0	0

$(0,-,-)f$	a	b	0
a	0	0	0
b	0	0	0
0	0	0	0

A fair amount of work proves the following properties.

1. (A, f) is simple type **5**.
2. (A, f) is aperiodic.
3. Any decomposition obtained by filling in blanks requires a factor which is not aprimal.
4. $(A, f) \prec (2, \wedge, c_0) \circ (3, +)$, so $(A, F) \in \mathbf{D}(\{(2, \wedge, c_0)\} \circ \mathit{Solv})$
5. (A, f) does not decompose into matrix powers of semilattices (use the fact that f is iterable).

This example shows that *Aper* is a complicated class, more so than the class of aperiodic semigroups, which decompose into matrix powers of semilattices. Also, it suggests that aprimal algebras may decompose into semilattices and groups, even though (as the example shows) aperiodic algebras do not necessarily decompose into semilattices.

Chapter 7

The decomposition theory of semigroups

A semigroup is an algebra $(S, \cdot)$ where $\cdot$ is binary and associative. The original wreath decomposition theory of semigroups, due to K. Krohn and J. Rhodes [9], works with transformation semigroups (using what is essentially the wreath product of unary algebras as defined here). Another version (the "two-sided theory") is based on a reversal invariant product in place of the wreath product [14] and [15]. (A product $\star$ is reversal invariant if $(S, \cdot)^{\text{rev}} \star (T, \cdot)^{\text{rev}} \cong ((S, \cdot) \star (T, \cdot))^{\text{rev}}$, where $(S, \cdot)^{\text{rev}}$ is the reverse semigroup $(S, (x, y) \mapsto y \cdot x)$.) The decomposition theory developed here uses the wreath product of algebras. Since algebras are sets with clones of operations, a semigroup is equal to its reverse, and $\circ$ is trivially reversal invariant. Additionally, the wreath product of algebras is associative, whereas the two-sided products of [13] are not.

The wreath product of algebras is in no sense identical to the (left, right, or double) semidirect products or the block product of [13]. In fact, if $(S, \cdot)$ and $(T, \cdot)$ are semigroups, $(S, \cdot) \circ (T, \cdot)$ is rarely a semigroup. The wreath products of algebras can, however, simulate semidirect products, as mentioned in Chapter 1, by adding endomorphisms to the clone of the left factor. This suggests that the factors in a semigroup decomposition theory will not be semigroups, but semigroups with certain additional operations. The decompositions in this section add polynomials rather than endomorphisms.

7.1 Ideals

Ideals (left, right, and two-sided) provide a way of using covers to decompose semigroups. We review the definitions of ideals and the standard theorems about them briefly here. Let $(S, \cdot)$ be a semigroup. For $X, Y \subseteq S$, we define $XY = \{xy : x \in X, y \in Y\}$. By $(S^1, \cdot)$ we mean the semigroup $(S \cup 1, \cdot)$ where 1 is a new element not in S and multiplication extends the multiplication in S by taking $1x = x1 = x$ for all $x \in S^1$. This construction is called *adjoining a*

unit. By $(S^0, \cdot)$ we mean the semigroup $(S \cup 0, \cdot)$ where 0 is a new element not in S and multiplication extends the multiplication in S by taking $0x = x0 = 0$ for all $x \in S^0$. This construction is called *adjoining a zero*.[1] If $(S, \cdot)$ satisfies $xy = 0$ for all $x, y \in S$, then $(S, \cdot)$ is called *null*.

A nonempty subset $I \subseteq S$ is called a *left ideal* if $SI \subseteq I$, a *right ideal* if $IS \subseteq I$, and a *two-sided ideal* (or simply *ideal*) if $S^1IS^1 \subseteq I$. If $(S, \cdot)$ has a zero 0, then $\{0\}$ is a two-sided ideal, known as the *zero* ideal or simply 0, which is contained in all ideals. A two-sided ideal I gives rise to a congruence θ_I whose classes are I and all singleton sets not contained in I. (The quotient by θ_I is known as the *Rees quotient* determined by I). We sometimes use $(S/I, \cdot)$ to denote $(S/\theta_I, \cdot)$. The collection of two-sided ideals of $(S, \cdot)$ will be denoted by Rees $(S, \cdot)$. As is easily seen, the operation $X \mapsto S^1XS^1$ is an algebraic closure operation on subsets of S; the nonempty closed sets are precisely the two-sided ideals. Rees $(S, \cdot)$ is an algebraic lattice (the least element is the intersection of all two-sided ideals). Also, Rees $(S, \cdot)$ embeds into the lattice Con $(S, \cdot)$ via the map $I \mapsto \theta_I$. Left and right ideals do not in general yield congruences, but see Lemma 7.5 below.

Lemma 66 *Let $(S, \cdot)$ be a finite semigroup. Suppose $(S, \cdot)$ has no left or right ideal different from S and 0. Then $(S, \cdot)$ is either a group, a group with a zero adjoined, or a null semigroup.*

Proof. Suppose $(S, \cdot)$ is not null. Choose $s, t \in S$ such that $st \neq 0$. Then St is a left ideal different from 0, $St = S$, and the map $x \mapsto xt$ is a permutation of S. Therefore $tt \neq 0$. Then tS is a right ideal different from 0, $tS = S$, and the map $x \mapsto tx$ is a permutation of S. Choose $n > 0$ so that $x \mapsto xt^n$ and $x \mapsto t^n x$ are both the identity map. This shows that $(S, \cdot)$ has a unit, namely t^n, denoted hereafter by 1. It follows that, for all nonzero $x \in S$, xS and Sx are nonzero ideals, hence are equal to S. So, for all nonzero $x \in S$, there are $y, z \in S$ such that $yx = 1 = xz$. Since $y = y(xz) = (yx)z = z$, the non-zero elements of S form a group. □

Let V be a left ideal of $(S, \cdot)$. A *right coset* of V is a set Vs, with $s \in S^1$; Vs is a left ideal. The set of right cosets of V is denoted $V\backslash S$. Note that if $VS^1 = S$, then $V\backslash S$ covers S. Also, if $(S, \cdot)$ has a zero, then zero is a coset of V. Since $(Vs)(Vt) \subseteq Vt$, for all $s, t \in S^1$, $(S, \cdot)$ induces a semigroup structure on $V\backslash S$; the structure is just projection on the right: $(Vs)(Vt) = Vt$, for all $s, t \in S^1$. (The equality is in $V\backslash S$, not S.) Hence $(V\backslash S, \cdot) = (V\backslash S, \emptyset)$. The natural action of S on the right of $V\backslash S$ is denoted $(V\backslash S, \cdot S)$. Left cosets of a right ideal W are treated analogously: they form a set S/W which has a natural left action by S denoted $(S/W, S\cdot)$.

[1] In the following discussion, we will often consider statements involving zero, even though the semigroup is not assumed to have a zero. If the semigroup in question has no zero, then the statement should be evaluated after adjoining a zero to the semigroup. Alternately, one can prove the decomposition theorems just for semigroups with zero and then derive the general theorems using the natural embedding $(S, \cdot) \leq (S^0, \cdot)$.

A *minimal nonzero* (left/right/two-sided) ideal of $(S, \cdot)$ is one which contains no smaller (left/right/two-sided) ideal of $(S, \cdot)$ different from zero. Note that a left (for instance) ideal V is minimal nonzero iff for any $v \in V$, $v \neq 0$ implies $S^1 v = V$. Note that two left ideals intersect in a left ideal (or the empty set), and similarly for two right ideals, but a left and a right ideal do not necessarily intersect in any kind of ideal. However, intersecting cosets of a left and a right ideal produces a congruence, under the assumption of minimality, as shown by Lemma 7.5 below. We will also show that translations by elements of $(S, \cdot)$ on such an intersection form a group (possibly with zero adjoined), known as the Schützenberger group.

Lemma 67 *Suppose V is a minimal nonzero left ideal of $(S, \cdot)$. Let $t \in S^1$. Then the left ideal Vt is either zero or minimal nonzero. The dual statement holds for a left coset of a minimal right ideal.*

Proof. Suppose $Vt \neq 0$. Let $vt \in Vt$, $vt \neq 0$, with $v \in V$. Since $v \neq 0$, $S^1 v$ is a nonzero left ideal contained in V and therefore equal to V. Then $S^1 vt = Vt$. □

Lemma 68 *Assume $(S, \cdot)$ is finite. Let V and W be minimal nonzero left and right (respectively) ideals of $(S, \cdot)$. Let $s, t \in S^1$. If $0 \neq s(V \cap W)t \subseteq V \cap W$, then $s(V \cap W) = V \cap W = (V \cap W)t$. In particular, a map $V \cap W \to V \cap W$ of the form $x \mapsto sx$ or $x \mapsto xt$ is either zero or a permutation.*

Proof. Assume $0 \neq s(V \cap W)t \subseteq V \cap W$. Since $s(V \cap W)t \subseteq sWt \subseteq sW$, we have $0 \neq s(V \cap W)t \subseteq W \cap sW$. The set $W \cap sW$ is a nonzero right ideal, so by minimality $W = W \cap sW = sW$. Therefore $s(V \cap W) \subseteq sV \cap sW \subseteq V \cap W$. Equality follows because $sV = V$ and because W is finite, hence $x \mapsto sx$ permutes W. A dual argument shows that $V \cap W = (V \cap W)t$. □

Lemma 69 *Assume $(S, \cdot)$ is finite. Let I be a minimal nonzero two-sided ideal of $(S, \cdot)$, and let V be a minimal nonzero left ideal contained in I. Then, for all $t \in S^1$ such that $Vt \neq 0$, there is a $t' \in S^1$ such that $Vtt' = V$. Furthermore, we may choose t' so that $x \mapsto xtt'$ is the identity on V. Dual statements apply to a minimal nonzero right ideal contained in I.*

Proof. If $Vt \neq 0$, then, since V is minimal nonzero, Vt is minimal nonzero, by Lemma 7.2. Since I is minimal, $VtS^1 = I$. Therefore there is a $t' \in S^1$ such that $Vtt' \cap V \neq 0$ and hence $Vtt' = V$. The second statement of the lemma follows by exponentiating tt'. □

Note that given I as in the previous lemma, such a V always exists, although it may be equal to I.

Lemma 70 *Suppose V and W are minimal nonzero left and right (respectively) ideals of $(S, \cdot)$. Let μ be the binary relation whose blocks are $(sW \cap Vt) \setminus 0$, for $s, t \in S^1$, together with all singleton sets not contained in one of these blocks.*

Then μ is a congruence. If V and W are contained in a minimal two-sided ideal I, then the congruence is independent of the choice of V and W; we denote this congruence by μ_I.

Proof. Clearly, μ is reflexive and symmetric. For transitivity, we must show that, for any $s,t,q,r \in S^1$, $sW \cap Vt$ and $qW \cap Vr$ either are equal or intersect in zero. We have $(sW \cap Vt) \cap (qW \cap Vr) = (sW \cap qW) \cap (Vt \cap Vr)$. By minimality, either $Vt \cap Vr = Vt = Vr$ or $Vt \cap Vr = 0$. Similarly, either $sW \cap qW = sW = qW$ or $sW \cap qW = 0$. If at least one of $Vt \cap Vr$ and $sW \cap qW$ is zero, then so is $(sW \cap Vt) \cap (qW \cap Vr)$. If neither are zero, then $sW \cap Vt = qW \cap Vr$.

To finish the proof that μ is a congruence, we must show that μ is admissible or, equivalently, that products of blocks are contained in blocks. We have the following inclusions:

$$\begin{aligned} (sW \cap Vt) \cdot (qW \cap Vr) &\subseteq (sW \cap Vr) \\ u(sW \cap Vt) &\subseteq (usW \cap Vt) \\ (sW \cap Vt)u &\subseteq (sW \cap Vtu). \end{aligned}$$

We must also show that, for $x \mu x'$ and $y \mu y'$, if $xy = 0$ then $x'y' = 0$. This is true because by minimality $S^1x = S^1x'$ and $yS^1 = y'S^1$. So if $xy = 0$ then $x'y' \in S^1x'y'S^1 = S^1xyS^1 = 0$.

For the second assertion, observe that if V' and W' are minimal nonzero left and right (resp.) ideals contained in I, then by minimality of I we have $VS^1 = I$ and so $Vt \cap V' \neq 0$ for some t. By minimality of Vt and V', $Vt = V'$, and similarly for W'. So V and V' have the same cosets, as do W and W'. $\square$

The theory developed so far in this section is (despite slightly different terminology) a fragment of the Green-Rees-Shuskevych picture of a minimal nonzero two-sided ideal. For details, see [5]. The following lemma, while not standard in semigroup theory, is needed to classify the basic and nearly basic pieces produced in semigroup decompositions using the wreath product of algebras.

Lemma 71 *Let $(S,\cdot)$ be finite and suppose V and W are minimal nonzero left and right (respectively) ideals of $(S,\cdot)$. Then $(V \cap W, (\text{Pol } (S,\cdot))|_{V\cap W})$ is polynomially equivalent to either a group, a group with a zero adjoined, or a set with a group action.*

Proof. Suppose $(\text{Pol } (S,\cdot))|_{V\cap W}$ is essentially unary. A unary polynomial xf can be written $(x,\dots,x)g$ where $(x_1,\dots,x_n)g = s_0x_1s_1x_2\dots s_{n-1}x_ns_n$, and $s_0,\dots,s_n \in S^1$. Suppose $0 \neq (V \cap W)f \subseteq V \cap W$. Then $(V \cap W)f \subseteq V \cap Vs_n$, and hence $V \cap Vs_n \neq 0$. Therefore $Vs_n = V$. Dually $s_0W = W$. Since $(V \cap W) \setminus 0$ is a congruence class (by the previous lemma), $(V \cap W)^n g \subseteq (V \cap W)$. Therefore $g \in (\text{Pol } (S,\cdot))|_{V\cap W}$, and so g depends on only one variable, say x_i. By substituting arbitrary constants for the other variables we may write $xf = (x,\dots,x)g = sxt$ with $s,t \in S^1$. Thus the clone $(\text{Pol } (S,\cdot))|_{V\cap W}$ is generated by (constants together with) some set of maps of the form $x \mapsto sxt$, with $s,t \in S^1$. By Lemma 7.3, if $x \mapsto sxt$ is in this clone then so are $x \mapsto sx$ and

$x \mapsto xt$, and furthermore each of the latter maps is either zero or a permutation. Thus $(V \cap W, (\text{Pol } (S,\cdot))|_{V\cap W})$ is polynomially equivalent to a set with a group action.

We may now assume that $(\text{Pol } (S,\cdot))|_{V\cap W}$ has an operation g which is not essentially unary. Without loss of generality we can write $(x,y,\ldots)g = \ldots xty\ldots$ for some $t \in S^1$, where g depends on both x and y. For $x, y \in V \cap W$, $xty \in V \cap W$. Therefore, $(\text{Pol } (S,\cdot))|_{V\cap W}$ has the operation h defined by $(x,y)h = xty$. Note that h is associative: $xt(ytz) = (xty)tz$. Also, h is not the zero map, since g is not.

First, we show that $(V\cap W, h)$ is a group or a group with zero. By Lemma 7.3, $x \mapsto xty$ is either a permutation or zero on $V \cap W$, and similarly for $y \mapsto xty$. Suppose that, for some $y_0 \neq 0$, the map $x \mapsto xty_0$ is zero. Then, for all x, then map $y \mapsto xty$ takes the value zero at 0 and at y_0, hence at all y. But this would imply that h is always zero. Therefore, for $y \neq 0$, $x \mapsto xty$ is nonzero and, similarly, for $x \neq 0$, $y \mapsto xty$ is nonzero. Hence left and right translations by nonzero elements in $(V \cap W, h)$ are permutations, so the semigroup is in fact a group or a group with zero adjoined, by Lemma 7.1.

All we have left to show is that $(\text{Pol } (S,\cdot))|_{V\cap W} = \text{Pol } (V \cap W, h)$. It is clear that the former contains the latter. Let $p \in (\text{Pol}_n\ (S,\cdot))|_{V\cap W}$. We can write

$$(x_1,\ldots,x_n)p = s_0 x_{i_1} s_1 x_{i_2} s_2 \ldots s_{k-1} x_{i_k} s_k,$$

with $s_0 \ldots s_k \in S^1$. Let e denote the identity of the group $(V \cap W, h)$. Then $x \mapsto etx$ and $x \mapsto xte$ are each the identity map on $V \cap W$. For $x_1,\ldots,x_n \in V \cap W$, we have

$$\begin{aligned}(x_1,\ldots,x_n)p &= et((etx_1te,\ldots,etx_nte)p)te \\ &= (ets_0e)tx_{i_1}t(es_1e)tx_{i_2}t(es_2e)t\ldots t(es_{k-1}e)tx_{i_k}t(es_kte).\end{aligned}$$

Observe that, for $s \in S^1$, $ese \in V \cap W$, since $e \in V \cap W$. Therefore, $p \in \text{Pol } (V \cap W, h)$. □

7.2 Semigroup decompositions using minimal ideals

Let $(S,\cdot)$ be a finite nontrivial semigroup. In this section we obtain a decomposition of $(S,\cdot)$ by exploiting the properties of a minimal two-sided ideal I. The basic idea is to apply the covering lemma to the corresponding quotient homomorphism. However, the derived algebra of this map must itself be decomposed.

Lemma 72 *Let I be a minimal nonzero two-sided ideal of $(S,\cdot)$. Choose minimal nonzero left and right ideals V and W (resp.) contained in I. Set $G = V \cap W \setminus 0$. Then*

$$\begin{aligned}(S,\cdot) \prec\ & (G, \text{Pol } (S,\cdot)|_G) \circ (2, \wedge, c_0, c_1) \\ & \circ ((S/W, S\cdot, C_{S/W}) \times (V\backslash S, \cdot S, C_{V\backslash S})) \circ (S,\cdot)/\theta_I.\end{aligned}$$

Proof. Consider the quotient homomorphism $(S,\cdot) \to (S,\cdot)/\theta_I$. By lemmas in Chapter 2,

$$\begin{array}{rcl} D_{\theta_I}^{[\mathrm{alg}]} & \cong & (I,\cdot,\{x \mapsto sx, x \mapsto xs : s \in S \setminus I\},\{c_{st} : s,t \in S \setminus I, st \in I\}) \\ & \leq & (I, \mathrm{Pol}\ (S,\cdot)|_I), \end{array}$$

so we can complete the proof by decomposing the latter algebra into the first three factors of the wreath product in the statement of the Lemma.

Consider the relational morphism

$$\varphi : (I,\cdot,\{x \mapsto sx, x \mapsto xs : s \in S \setminus I\}) \to (S/W, S\cdot, C_{S/W}) \times (V\backslash S, \cdot S, C_{V\setminus S})$$

defined by

$$\begin{array}{rcc} x \in sW \cap Vt & \mapsto & (sW, Vt) \\ \cdot & \mapsto & ((sW,Vt),(s'W,Vt')) \mapsto (sW,Vt') \\ x \mapsto xr & \mapsto & (sW,Vt) \mapsto (sW,Vtr) \\ x \mapsto rx & \mapsto & (sW,Vt) \mapsto (rsW,Vt) \\ c_x, x \in sW \cap Vt & \mapsto & (c_{sW}, c_{Vt}). \end{array}$$

Note that φ is many valued at the zero, if there is one. Also, the operation $((sW,Vt),(s'W,Vt')) \mapsto (sW,Vt')$ is just the diagonal operation present in any non-indexed product.

The $x \mapsto sx$ and $x \mapsto xs$ operations, for $s \in S$, induce isomorphisms of the nonzero sorts of $D\varphi$. Therefore, by the Retraction Lemma of Chapter ???2, we have a division $D\varphi \prec (V \cap W, (\mathrm{Pol}\ (S,\cdot))|_{V\cap W})$, the latter algebra being one of the local algebras of $D\varphi$. If $(S,\cdot)$ has no zero, this is just $(G, (\mathrm{Pol}\ (S,\cdot))|_G)$. Otherwise, we use the congruence $\mu_I|_{V\cap W}$ to obtain the decomposition

$$(V \cap W, (\mathrm{Pol}\ (S,\cdot))|_{V\cap W}) \prec (G, (\mathrm{Pol}\ (S,\cdot))|_G) \circ (2, \wedge, c_0, c_1).$$

□

A careful examination of the proof turns up the following. If $(S,\cdot)$ has no zero, the $(2,\wedge,c_0,c_1)$ factor may be omitted from the decomposition. If I is null, $(2,\wedge,c_0,c_1)$ can be replaced with $(2,c_0)$. If neither of these two conditions hold, $(2,\wedge,c_0,c_1)$ divides $(S, \mathrm{Pol}\ (S,\cdot))$. The first and last factors always divide $(S, \mathrm{Pol}\ (S,\cdot))$. The remaining factor is a product of unary algebras. By the previous lemma, the $(G, (\mathrm{Pol}\ (S,\cdot))|_G)$ factor is either a group (no zero) or a unary algebra.

Theorem 73 *Let $(S,\cdot)$ be a finite semigroup. We have a decomposition $(S,\cdot) \prec (A_n,F_n) \circ \cdots \circ (A_1,F_1)$, where each factor is either*

1. *a unary algebra, or*
2. *(up to pol. equiv.) a group or a two-element semilattice which divides $(S, \mathrm{Pol}\ (S,\cdot))$.*

*Proof.*Apply the lemmas inductively. □

Note that the two-element semilattice is indecomposable. Unary algebras can be further decomposed by the Krohn-Rhodes theorem. Groups can be further decomposed by the next section.

7.3 Groups

Our decompositions of groups will roughly parallel the traditional theory. However, the indecomposable pieces we break groups down into will have slightly more complicated clones than the Jordan-Hölder factors, being direct powers of the latter with some added unary operations.

Recall that $N \lhd G$ (i.e., N a normal subgroup of G) is said to *split* if G has a subgroup H such that $NH = G$ and $N \cap H = \{1\}$.

Lemma 74 *Let $(G, \cdot)$ be a group, $N \lhd G$. Then*

$$(G, \cdot) \prec (N, \cdot, \{x \mapsto gxg^{-1} : g \in G\}, \{x \mapsto xn : n \in N\}) \circ (G/N, \cdot).$$

Furthermore, if $N \lhd G$ splits via $H \leq G$, then

$$(G, \cdot) \prec (N, \cdot, \{x \mapsto hxh^{-1} : h \in H\}) \circ (G/N, \cdot).$$

Proof. Let φ denote the quotient map $(G, \cdot) \to (G/N, \cdot)$. To apply the covering lemma, we must show that D_φ divides the left factor of the appropriate wreath product. The sorts of D_φ are the cosets of N; the operations are (generated by) all restrictions of $\cdot$ to pairs of cosets: for $g, g' \in G$, there is an operation $Ng \times Ng' \to Ngg'$ sending $(ng, n'g') \mapsto ngn'g'$. To consolidate the msa, we choose a set R of coset representatives, with $R = H$ if the extension splits. If the extension does not split, let H be the subgroup generated by R. Then we define a msa D_φ^+ by adding to D_φ right translations by elements of H (and closing the new msa under compositions, of course).

We compute the local algebra at N of D_φ^+. An operation f of this algebra is of the form $t_1 h_1 t_2 h_2 \dots t_n h_n$ where each t_i is a term operation in $\cdot$ and each $h_i \in H$. Applying the group identity $xy = xyx^{-1}x$, we can write this as $(\dots(t_{n-2}h_{n-1}(t_{n-1}h_n(t_n)h_n^{-1})h_{n-1}^{-1})\dots)(h_1 h_2 \dots h_n)$. Since $1 \in N$ and f is an operation in the local algebra at N, we have $h_1 h_2 \dots h_n = (1, \dots, 1)f \in N$. Also, $h_1 h_2 \dots h_n \in H$. Since the local algebras at Nr_1 and Nr_2 are isomorphic via translations by $r_1^{-1}r_2$ and $r_2^{-1}r_1$, we can apply the Retraction Lemma (2.???) to D_φ^+ to obtain

$$D_\varphi \prec D_\varphi^+ \sim (N, \cdot, \{x \mapsto hxh^{-1} : h \in H\}, \{x \mapsto xg : g \in H \cap N\}).$$

Note that if the extension splits, $H \cap N = \{1\}$. □

Notes:

(1) The division produced by the proof is in fact an embedding, given explicitly as follows. Let R and H be as before. Let, for $g \in G$, $C(g)$ be the unique element of N such that $C(g)g \in R$. Then the embedding is

$$\begin{array}{rcl} nr & \mapsto & (n, Nr) \text{ (for } r \in R) \\ \cdot & \mapsto & ((n, Nr), (n', Nr')) \mapsto (nrn'r^{-1}C(rr')^{-1}, Nrr') \end{array}$$

In the split case, $C(rr') = 1$. In general $C(rr') \in H \cap N$.

(2) When the extension splits the decomposition is similar to the corresponding semidirect decomposition of groups. When, more generally, the subgroup H generated by R as in the proof is proper, we can still get a proper decomposition $(G, \cdot) \prec (N, \cdot, \{x \mapsto hxh^{-1} : h \in H\}) \circ (H, \cdot)$ even though the extension is not split. The relational morphism corresponding to this decomposition is not a homomorphism, and the division is not an embedding. (The morphism $(G, \cdot) \to (H, \cdot)$ is $nh \mapsto h$ for $n \in N$, $h \in H$ and $\cdot \mapsto \cdot$. Note that this is many-valued on elements.)

(3) If $(N, \cdot)$ is finite simple nonabelian, then the left factor in the decomposition in the lemma is polynomially equivalent to $(N, \cdot)$, by the theorem of Maurer-Rhodes. If $(N, \cdot)$ is abelian, the left factor, even up to polynomial equivalence, is not necessarily a group but a module over a subring of the ring of inner automorphisms of $(G, \cdot)$.

(4) The type of a tame congruence is the same as the type of the corresponding normal subgroup and this is not changed by adding the unary operations as in the lemma.

Lemma 75 *Let N be a minimal normal subgroup of a finite group $(G, \cdot)$. Then $(N, \cdot) \cong (S^k, \cdot)$, for some k and some simple group $(S, \cdot)$.*

Proof. Let H be a minimal normal subgroup of $(N, \cdot)$. If $H = N$, then N is simple. Otherwise, H is a proper normal subgroup of N whose G-conjugates $H_1, \ldots, H_n$ together generate N. Each H_i is a minimal normal subgroup of $(N, \cdot)$, so $H_i \cap H_j = \{1\}$ for $i \neq j$. So $(N, \cdot) \cong (H^k, \cdot)$, for some $k \leq n$. If H is simple, we're done. If not, repeat. □

Note that, in the situation of the lemma, the group $(S, \cdot)$ is a Jordan-Hölder factor which is repeated k times.

Theorem 76 *Let $(G, \cdot)$ be a finite group, $|G| > 1$. Then $(G, \cdot) \prec (A_n, F_n) \circ \cdots \circ (A_1, F_1)$, where each factor is, for some $k > 0$, one of the following, up to polynomial equivalence:*

1. *$(S^k, \cdot, \alpha_1, \ldots, \alpha_m)$ where $(S, \cdot)$ is a simple nonabelian group and $a_1, \ldots, a_m \in$ Aut $(S^k, \cdot)$*
2. *a simple module whose underlying group is $(Z_p^k, +)$ for some prime p.*

Furthermore, each factor divides $(G, \text{Pol } (G, \cdot))$, and the underlying groups of the factors are the same as the Jordan-Hölder factors with some repetitions replaced by powers.

Proof. Induct on $|\mathrm{Con}\ (G,\cdot)|$. If $(G,\cdot)$ is simple, there's nothing to show. Otherwise, apply the lemmas to a minimal normal subgroup N. □

A module whose underlying group is $(Z_p^k,+)$ is a reduct of $(Z_p, \mathrm{Pol}\ (Z_p,+))^{[k]}$. Trivially, $(S^k,\cdot,a_1,\ldots,a_m)$ (notation as above) is a reduct of $(S,\mathrm{Pol}\ (S,\cdot))^{[k]}$, since $(S,\mathrm{Pol}\ (S,\cdot))$ is primal and matrix powers of primal algebras are primal. Hence, up to polynomial equivalence and matrix powers, every finite group decomposes into its Jordan-Hölder factors. By Lemma 2.13, polynomials can be obtained by taking a subreduct of a matrix power. Therefore every finite group decomposes into matrix powers of its Jordan-Hölder factors. (Of course, every finite algebra divides a sufficiently high matrix power of any finite SNAG.)

The unary operations that must be added to a normal subgroup to get a decomposition may carry some interesting information about the extension. Thus one might study classes of groups obtained by wreath products as in the theorem but with various restrictions on which constants and automorphisms may appear. It might also be interesting to look at classes of *algebras* defined in the same manner with or without such restrictions (not all divisors of these wreath products are groups!).

7.4 Aprimal semigroups

This section applies the ideas of Chapter 4 to semigroup decomposition theory.

Let $(S,\cdot)$ be a finite semigroup. The *kernel* of $(S,\cdot)$, denoted $\ker S$, is the smallest two-sided ideal of $(S,\cdot)$. Since S is finite, $\ker S$ is always nonempty.

Theorem 77 *Let $(S,\cdot)$ be a finite semigroup. Then:*

1. *$(S,\cdot)$ is aprimal iff every subgroup of $(S,\cdot)$ is solvable.*
2. *$(S,\cdot)$ is aperiodic iff every subgroup of $(S,\cdot)$ is trivial.*
3. *$(S,\cdot)$ is solvable iff $(S,\cdot)$ is aprimal and $(S/\ker S,\cdot)$ is null.*
4. *$(S,\cdot)$ is strongly solvable iff $(S,\cdot)$ is aperiodic and solvable.*

Proof. (1) If $(S,\cdot)$ has a nonsolvable subgroup, then there is a simple nonabelian group $(G,\cdot)$ such that $(G,\cdot) \prec (S,\cdot)$, so $(S,\cdot)$ is not aprimal. Conversely, if every subgroup is solvable, then, by the theorems of this chapter, $(S,\cdot)$ decomposes into factors which are, up to polynomial equivalence, either unary algebras, semilattices, or modules, all of which are aprimal. Since *Aprim* is closed under wreath product, $(S,\cdot)$ is aprimal.

(2) If $(S,\cdot)$ has a nontrivial subgroup, G, then $(S,\cdot)$ is not aperiodic. Conversely, if every subgroup of $(S,\cdot)$ is trivial, then, by Theorem 7.8, $(S,\cdot)$ decomposes into factors which are, up to polynomial equivalence, either unary algebras or semilattices, all of which are aperiodic. Since *Aper* is closed under wreath product, $(S,\cdot)$ is aperiodic.

(3) Suppose that $(S/kerS, \cdot)$ is not null. Then there is an $s \in S$ such that, for all n, $s^n \notin \ker S$. Choose n so that $(s^n)^2 = s^n$. Now consider the subsemigroup $T = \{sn\} \cup \ker S$. The Rees quotient $(T/kerS, \cdot)$ is a two-element semilattice, and so $(S, \cdot)$ is not solvable.

Conversely, suppose that $(S/\ker S, \cdot)$ is null. Since $\ker S$ has no proper ideals (no zero even, unless $\ker S = 0$), Lemma 7.7 and the subsequent remarks show that we can decompose $(S, \cdot)$ using $(S/\ker S, \cdot)$ and factors which do not involve a semilattice. Next, choose a minimal ideal of $(S/\ker S, \cdot)$, apply 7.7 to this null ideal, and repeat. All factors in the resulting decomposition are solvable.

(4) This equivalence follows directly from the definitions. □

Unfortunately, what are called here aprimal semigroups would be called "solvable" by semigroups theorists. Statement (2) shows that our definition of aperiodic agrees (for semigroups) with that of semigroup theory. In the language of Green's relations, the right-hand side of statement (3) says that $(S, \cdot)$ has exactly one regular $\mathcal{J}$-class, and the right-hand side of (4) says that $(S, \cdot)$ has exactly one regular $\mathcal{J}$-class and its $\mathcal{H}$-classes are trivial.

Bibliography

[1] G. M. Bergman. Embedding arbitrary algebras in groups. *Algebra Universalis*, 25:107–120, 1988.

[2] J. Berman, E. Kiss, P. Pröhle, and Á. Szendrei. The set of types of a finitely generated variety. *Discrete Math*, 112:1–20, 1993.

[3] J. Berman and S. Seif. An approach to tame congruence theory via subtraces. *Algebra Universalis*, 30:479–520, 1993.

[4] Stanley Burris and H. P. Sankappanavar. *A Course in Universal Algebra*. Number 78 in Graduate Texts in Mathematics. Springer-Verlag, 1981.

[5] A. H. Clifford and G. B. Preston. *Algebraic Theory of Semigroups*. American Mathematical Society, Vol. I: 1961, Vol II: 1967.

[6] Samuel Eilenberg. *Automata, Languages, and Machines, Volume B*. Number 59 in Pure and Applied Mathematics. Academic Press, 1976. Includes two chapters by Bret Tilson.

[7] D. Hobby. Finding type sets is NP hard. *International Journal of Algebra and Computation*, 1:437–444, 1991.

[8] David Hobby and Ralph McKenzie. *The Structure of Finite Algebras*. Number 76 in Contemporary Mathematics. American Mathematical Society, 1988.

[9] K. Krohn and J. Rhodes. Algebraic theory of machines. i. prime decomposition theorem for finite semigroups and machines. *Transactions of the American Mathematical Society*, 116:450–464, 1965.

[10] W. D. Maurer and J. Rhodes. A property of simple non-abelian groups. *Proceedings of the American Mathematical Society*, 16:552–554, 1965.

[11] R. McKenzie. A new product of algebras and a type reduction theorem. *Algebra Universalis*, 18:29–69, 1984.

[12] Ralph McKenzie, George McNulty, and Walter Taylor. *Algebras, Lattices, Varieties*, volume 1. Wadsworth & Brooks/Cole, 1987.

[13] J. Rhodes and B. Tilson. The kernel of monoid morphisms. *Journal of Pure and Applied Algebra*, 62:227–268, 1989.

[14] J. Rhodes and P. Weil. Decomposition techniques for finite semigroups using categories, I. *Journal of Pure and Applied Algebra*, 62:269–284, 1989.

[15] J. Rhodes and P. Weil. Decomposition techniques for finite semigroups using categories, II. *Journal of Pure and Applied Algebra*, 62:285–312, 1989.

[16] John Rhodes, editor. *Monoids and Semigroups with Applications*. World Scientific, 1991.

[17] B. Tilson. Categories as algebra: An essential ingredient in the theory of monoids. *Journal of Pure and Applied Algebra*, 48:83–198, 1987.

[18] J. VanderWerf. *Wreath Decompositions of Algebras*. PhD thesis, University of California at Berkeley, 1994.

[19] J. VanderWerf. Wreath products of algebras: Generalizing the Krohn-Rhodes Theorem to arbitrary algebras. *Semigroup Forum*, To appear.