MANY-VALUED GENERALIZATIONS OF TWO FINITE INTERVALS IN POST'S LATTICE

By

Graham Campbell Denham

B.Sc., University of Alberta, 1992

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE

in

THE FACULTY OF GRADUATE STUDIES
Department of
COMPUTER SCIENCE

We accept this thesis as conforming
to the required standard

THE UNIVERSITY OF BRITISH COLUMBIA

June 1994

© Graham Campbell Denham, 1994

In presenting this thesis in partial fulfillment of the requirements for an advanced degree at the University of British Columbia, I agree that the Library shall make it freely available for reference and study. I further agree that permission for extensive copying of this thesis for scholarly purposes may be granted by the head of my department or by his or her representatives. It is understood that copying or publication of this thesis for financial gain shall not be allowed without my written permission.

Computer Science

The University of British Columbia

2366 Main Mall

Vancouver, Canada

V6T 1Z4

Date:

31 May 1994

abstract

A study due to Emil Post shows that, although the lattice of clones in two-valued algebraic logic is countably infinite, there exist only finitely many clones that contain both constants, and only finitely many that contain the negation function. There are, however, uncountably many k -valued clones for all $k > 2$; in fact, it is known that uncountably many clones contain all constants.

The constants of two-valued logic can also be regarded as the set of noninvertible, unary functions on a two element domain. It is shown here that, for values of k greater than two, there remain only finitely many k -valued clones containing all such functions. Similarly, one can generalize the set of clones in Post's lattice that contain the negation function to those k -valued clones that contain all invertible, unary functions. Once again, there are only finitely many such clones, and they can be described explicitly.

These two generalizations of sets of two-valued clones are presented with an introduction to the study of the lattice of clones, and a survey of relevant results. We also note and discuss the fact that the latter result serves to give a description of all homogeneous relation algebras over a finite underlying set.

Table of Contents

Abstract	ii
List of Figures	iv
1 Preliminaries	1
1.1 Introduction	1
1.2 Terminology for clone theory	3
1.2.1 The algebra of functions	9
1.2.2 The algebra of relations	11
1.3 Functions with relations	15
2 Properties of the Lattice of Clones	20
2.1 The Structure of $\mathcal{L}(\mathcal{P}_2)$	20
2.2 Coatoms and completeness criteria	23
2.3 Counting clones	26
2.4 Finitely generated clones and coclones	28
3 Two Intervals in $\mathcal{L}(\mathcal{P}_k)$	34
3.1 Clones over Ω_k	34
3.2 Clones over S_k	41
4 The Intervals in Context	54
4.1 Homogeneous algebras	54
4.2 Homogeneous relation algebras	56
4.3 Ω_k as endomorphisms	57
4.4 Concluding remarks	59
Bibliography	61

List of Figures

1.1	$f(x, y) = \text{et}(\text{vel}(x, y), \text{neg}(\text{et}(x, y))) = x + y$	1
2.2	The lattice of clones of $\mathcal{P}_2$	21
3.3	$[\Omega_2, \mathbf{P}_2]$	34
3.4	$[\Omega_3, \mathbf{P}_3]$	40
3.5	$[S_2, \mathbf{P}_2]$	41
3.6	$[S_3, \mathbf{P}_3]$	50
3.7	$[S_4, \mathbf{P}_4]$	52

Chapter 1

Preliminaries

1.1 Introduction

Clone theory is an algebraic study of the composition of functions that provides a common abstraction of two disciplines: multiple-valued propositional logic, and universal algebra. The matter under study is that of what functions of several variables, over a fixed universe, can be formed from other, given functions using composition operations. A set of functions that is closed under composition is called a clone.

The problem is natural to state in the context of digital circuitry. A function of n variables models a logic gate with n inputs and one output. An expression formed by composition of functions represents a circuit without feedback. A clone, then, corresponds to the set of all circuits that can be constructed solely from particular types of gates.

Figure 1.1: $f(x, y) = et(vel(x, y), neg(et(x, y))) = x + y$

Algebraic operations, from the point of view of universal algebra, are simply functions of several variables, and terms are the formal composition of operations. The terms of an algebra can themselves be interpreted as functions of several variables, by evaluation. The set of all functions

that can be expressed as terms of a given algebra form a clone, and, conversely, every clone is the set of term functions for some algebra. The study of clones is thus also intimately related to the study of universal algebras.

The remainder of this first chapter establishes notation and provides a collection of definitions relevant to clone theory, with the intent of keeping the presentation as self-contained as possible. The last section states and proves a fundamental correspondence theorem.

Clones over a given domain form a lattice under set inclusion. The second chapter offers a selective introduction and survey of the known properties of this lattice when the domain is finite. Clones over a two-valued domain are completely understood, and their description is summarized in Section 2.1. When the size of the domain exceeds two, the structure of the lattice is inherently far more complex, and it is impossible to give a description of the same sort.

The third chapter presents two parallel results. Both are a determination of all clones over a finite domain containing a given set of unary functions. The first generalizes a result due to Jablonskiĭ in order to find the clones containing the non-invertible unary functions, Ω_k . The second begins with an analogous result due to Salomaa and expands upon a paper by Haddad and Rosenberg in order to treat those clones containing all invertible unary functions, S_k . In both cases, the argument proceeds by proving and then combining a series of technical lemmata, most of which are based on the results and methods of Salomaa and Jablonskiĭ. The unary clones that contain Ω_k and S_k are respectively characterized, and the results are then extended to nonunary clones. In both cases, there are only finitely many clones over a domain of finite cardinality that contain the given unary functions.

We conclude by considering how these results generalize their two-valued instances. We indicate that they also serve to characterize two classes of highly symmetric relation algebras, and leave the reader with some thoughts on further research.

1.2 Terminology for clone theory

The definitions and notation used here are, for the most part, drawn from Chapter 1 of Pöschel and Kalužnin [33] and the universal algebra references of Grätzer [16] or Burris and Sankappanavar [6].

We begin with some definitions related to the fundamental objects of clone theory; that is, functions of one or more variables with domain and codomain equal to a fixed set. Let $\mathbf{N} = \{1, 2, 3, \dots\}$ denote the natural numbers. For a given set A and $n \in \mathbf{N}$, let $\mathbf{P}_A^{(n)}$ denote the set of all functions $f : A^n \rightarrow A$. Let

$$\mathbf{P}_A = \bigcup_{n \in \mathbf{N}} \mathbf{P}_A^{(n)} \quad (1.1)$$

For any $F \subseteq \mathbf{P}_A$ and $n \in \mathbf{N}$, we define $F^{(n)} = F \cap \mathbf{P}_A^{(n)}$. A function f is said to be of *arity* n if $f \in \mathbf{P}_A^{(n)}$. Since (1.1) is clearly a disjoint union, we may also define the *arity* or *order* function $o : \mathbf{P}_A \rightarrow \mathbf{N}$ by $o(f) = n$ if $f \in \mathbf{P}_A^{(n)}$. Furthermore, suppose $f \in \mathbf{P}_A^{(n)}$. Then the i th variable of f , x_i , for $0 < i \leq n$, is said to be *essential* if there exist $a_j \in A$, for $0 < j \leq n$, $j \neq i$, and $u, v \in A$, for which

$$f(a_1, a_2, \dots, u, \dots, a_n) \neq f(a_1, a_2, \dots, v, \dots, a_n),$$

where the u and v are in the i th position. In alternate phrasing, f *depends* on the i th variable. If this is not the case, the i th variable is said to be *fictitious*. The *essential arity* of a function $f \in \mathbf{P}_A$, denoted by $o_e(f)$, shall then be defined to be the number of variables on which f depends. If f depends on all of its variables, that is $o(f) = o_e(f)$, f itself is said to be *essential*. If $o(f) = 1$ or $o_e(f) = 1$, f will be called a *unary* or *essentially unary* function, respectively.

We also write the *range* of a function $f \in \mathbf{P}_A^{(n)}$ as

$$\text{rng}(f) = \{a : \exists \mathbf{x} \in A^n \text{ such that } a = f(\mathbf{x})\}.$$

By way of illustrating these definitions, let $A = \{0, 1\}$, and let

(x_1, x_2, x_3)	$f(x_1, x_2, x_3)$
000	0
001	0
010	1
011	1
100	1
101	1
110	1
111	1

Then $f \in \mathbf{P}_A^{(3)}$ and $o(f) = 3$, but $o_e(f) = 2$, since f does not depend on its third argument.

It will often be desirable to apply a function f to the rows of an $m \times n$ matrix. If $a_{ij} \in A$ for $0 \leq i < m$ and $0 \leq j < n$ and $f \in \mathbf{P}_A^{(n)}$, we shall write $f((a_{ij}))$ to abbreviate the m -tuple which has components $f(a_{i0}, a_{i1}, \dots, a_{i,n-1})$, for $0 \leq i < m$.

There are several ways to write a function explicitly. In the example above, we made use of a table of values. In order to be somewhat more succinct and descriptive, one may use a generalization of the familiar conjunctive and disjunctive normal forms from the two-element domain up to a finite domain of arbitrary size. Suppose $A = \{0, 1, \dots, k-1\}$ and, using the usual ordering of the natural numbers, define $x \wedge y = \min\{x, y\}$, and abbreviate $x \wedge y$ simply by xy , since the operation is associative. Also let $x \vee y = \max\{x, y\}$, and define $d_i \in \mathbf{P}_A^{(1)}$ for $i \in A$ by

$$d_i(x) = \begin{cases} k-1 & \text{if } x = i \\ 0 & \text{otherwise.} \end{cases}$$

Write $d_i(x)$ also as x^i . Then it is a simple matter to verify that, if $f \in \mathbf{P}_A^{(n)}$,

$$f(x_0, x_1, \dots, x_{n-1}) = \bigvee_{\sigma_0, \sigma_1, \dots, \sigma_{n-1} \in A} x_0^{\sigma_0} x_1^{\sigma_1} \cdots x_{n-1}^{\sigma_{n-1}} f(\sigma_0, \sigma_1, \dots, \sigma_{n-1}).$$

We can also represent a function $f \in \mathbf{P}_A^{(n)}$ as a polynomial over a field, if the cardinality of the underlying set is a prime power: one identifies A with the field $GF(|A|)$, then writes f as a

polynomial $p \in GF(|A|)[x_0, x_1, \dots, x_{n-1}]$. This is sometimes called the representation by *Žegalkin polynomials*. It will be of use in this document when $|A|$ is one of 2, 3, and 4.

We shall regard the composition of any two functions in $\mathbf{P}_A$ as an algebraic operation, in a way which the following definitions are intended to make precise. The language and basic concepts of universal algebra provide a natural framework for discussing the composition of logic functions. The fundamental objects of the discipline of universal algebra itself include the functions $\mathbf{P}_A$, and here, as in other areas of mathematics, we find that the objects comprising the theory's tools are also admissible as objects which the theory describes. Therefore, we shall now outline some concepts from universal algebra, using the text by Burris and Sankappanavar [6] as a reference. The material that follows is not intended as an introduction, but rather as a compendium of definitions included to minimize ambiguity in the chapters that follow, and to indicate explicitly some of the underlying mathematical notions found in clone theory.

We begin by defining partial orders and lattices. Let A be a set together with a binary relation $\leq$ possessing the following properties for all $x, y, z \in A$:

1. $x \leq x$ (reflexive property)
2. $x \leq y$ and $y \leq z \Rightarrow x \leq z$ (transitive property)
3. $x \leq y$ and $y \leq x \Rightarrow x = y$ (antisymmetric property)

Then the pair $(A, \leq)$ is called a *partial order* on A . If, in addition, $(A, \leq)$ has the further properties:

1. There exists an element $0 \in A$ for which $\forall x \in A, 0 \leq x$,
2. There is also an element $1 \in A$ for which $\forall x \in A, x \leq 1$,
3. For every two elements $x, y \in A$, there exists a unique element, denoted by $x \wedge y \in A$ and called the *meet* of x and y , for which $x \wedge y \leq x$, $x \wedge y \leq y$, and $\forall z \in A$ if $z \leq x$ and $z \leq y$, then $z \leq x \wedge y$.
4. Similarly, there exists a unique element $x \vee y \in A$, called the *join* of x and y , for which: $x \leq x \vee y$, $y \leq x \vee y$, and $\forall z \in A$ if $x \leq z$ and $y \leq z$, then $x \vee y \leq z$.

$(A, \leq, \wedge, \vee)$ is called a *lattice*. If it is also the case that, for any subset $X \subseteq A$, there exists a unique element $\bigwedge X$ for which $\bigwedge X \leq x$, $\forall x \in X$, and if $\exists z \in A$ for which $z \leq x$, $\forall x \in X$, then $z \leq \bigwedge X$, and the element $\bigvee X$ exists correspondingly, then the lattice is said to be *complete*. $\bigwedge X$ is the join of the set X , called also the *infimum* of X . $\bigvee X$ is the meet, or the *supremum*, of X . An element $x \in A$ is *compact* if

$$\forall X \subseteq A : x \leq \bigvee X \Rightarrow \exists \text{ finite } Y \subseteq X, \text{ for which } x \leq \bigvee Y.$$

A complete lattice in which every element is the supremum of compact elements is termed *algebraic*.

If a pair of distinct poset elements x and y satisfy $x \geq y$, and $x \geq z \geq y$ implies that $z = x$ or $z = y$, we say that x *covers* y . A *chain* in a poset from x_1 to x_n is a finite subset $\{x_1, x_2, \dots, x_n\}$ for which x_i covers x_{i-1} , for $2 \leq i \leq n$. The *height* of y over x , denoted by $h(x, y)$, is the length of the shortest chain from x to y , or ∞ if there is no chain from x to y .

In a lattice, an element x which covers 0 is called a minimal element, or *atom*. If every element not equal to 0 contains an atom, then the lattice is said to be *atomic*. Analogously, an element covered by 1 is called maximal, or a *coatom*. A lattice is *coatomic* if every element not equal to 1 is contained in a coatom.

A subset of a lattice which satisfies the lattice properties (1) through (4) itself is termed a *sublattice*. One frequently-encountered instance of a sublattice of a lattice A is, for some elements $x, y \in A$, $x \leq y$, the *interval*

$$[x, y] = \{z \in A : x \leq z \leq y\}.$$

The cartesian product of two lattices $(A_1, \leq_1, \wedge_1, \vee_1)$ and $(A_2, \leq_2, \wedge_2, \vee_2)$ is also a lattice, if we define

$$(x_1, x_2) \leq (y_1, y_2) \Leftrightarrow x_1 \leq_1 y_1 \text{ and } x_2 \leq_2 y_2.$$

Another natural way to create a new lattice is to put the 0 element of one above the 1 element of the other: assume that A_1 and A_2 are disjoint sets, and let $(A_1 \cdot A_2, \leq, \wedge, \vee)$ be given by $A_1 \cdot A_2 = A_1 \cup A_2$, and $\leq = \leq_1 \cup \leq_2 \cup (A_1 \times A_2)$. The lattice $A_1 \cdot A_2$ is called the *ordinal sum* of A_1 and A_2 .

We conclude our list of lattice-related definitions with another pair of important objects. Suppose $B \subseteq A$ has the property that, for all $x \in B$ and $y \in A$, $y \leq x \Rightarrow y \in B$. Then B is termed an *ideal* of A . Similarly, if for all $x \in B$ and $y \in A$, $x \leq y \Rightarrow y \in B$, then B is a *filter* of A . Let us denote the set of ideals and filters of A , respectively, by $\mathcal{I}(A)$ and $\mathcal{F}(A)$.

We now introduce the notion of a universal algebra. Let A be a set, and F a subset of $\mathbf{P}_A$. That is, F is a set of functions for which

$$\phi \in F \Rightarrow \phi : A^n \rightarrow A \text{ for some } n \in \mathbf{N}.$$

Then the pair $\langle A; F \rangle$ is called a (universal) *algebra* with *universe* or *underlying set* A and *fundamental operations* F . In particular, if $F = \{\phi_1, \phi_2, \dots, \phi_m\}$, for a finite collection of functions $\{\phi_i\}$, then $\langle A; F \rangle$ is said to be of *finite type*, and is also written $\langle A; \phi_1, \phi_2, \dots, \phi_m \rangle$.

For example, any group G is a universal algebra $\langle G; \circ, ^{-1}, 1 \rangle$, where $\circ : G \times G \rightarrow G$ is the binary operation in the group, $^{-1} : G \rightarrow G$ is the inverse operation, and $1 : G \rightarrow G$ is a constant operation distinguishing the identity element. Similarly, a lattice $(A, \leq, \wedge, \vee)$ is an algebra $\langle A; \wedge, \vee \rangle$, since the partial order $\leq$ can be recovered from the operations $\wedge$ or $\vee$ using the observation that

$$x \leq y \quad \Leftrightarrow \quad x \wedge y = x \quad \Leftrightarrow \quad x \vee y = y.$$

It should be mentioned that it is sometimes convenient to use the word ‘algebra’ for the underlying set A of $\langle A; F \rangle$, when the set of operations F intended is understood from context.

Let an algebra $\mathcal{A} = \langle A; F \rangle$ be given. A *congruence* of $\mathcal{A}$ is an equivalence relation $\equiv$ in the underlying set A that each fundamental operation preserves, in the sense that for every $f \in F^{(n)}$, if $a_i \equiv b_i$ for $1 \leq i \leq n$, then $f(a_1, \dots, a_n) \equiv f(b_1, \dots, b_n)$. An *endomorphism* of $\mathcal{A}$ is a function $\mu : A \rightarrow A$ for which

$$\mu f = f(\mu x_1, \dots, \mu x_n),$$

for all $f \in F^{(n)}$. An *automorphism* is an invertible endomorphism. We note that the endomorphisms of an algebra form a monoid under composition, as the automorphisms form a group. To continue the first example above, a congruence of a group is the equivalence relation induced by the partition of G into the cosets of a normal subgroup of G . An automorphism matches its conventional definition for groups.

A set $S \subseteq A$ is said to be (*algebraically*) *closed* if, for every $\phi \in F$, we have $\phi(x) \in A$ for all $x \in S^n$, where $n = o(\phi)$. Suppose that some collection of sets $S_\lambda \subseteq A$ for $\lambda \in \Lambda$ are closed; then one can see that the intersection $\bigcap_{\lambda \in \Lambda} S_\lambda$ is also closed. It is a consequence that, for any $S \subseteq A$, the set $[S]$ defined by

$$[S] = \bigcap \{X \subseteq A : X \supseteq S \text{ and } X \text{ is algebraically closed}\}$$

is itself a closed set. $[S]$ is called the *algebraic closure* of S , and we call the function $[\cdot] : 2^A \rightarrow 2^A$ the *algebraic closure operator* for the algebra A .

The essential properties of the closure operator are worth stating explicitly. If $X, Y \subseteq A$, it is easy to verify that

1. $X \subseteq [X]$ (extensive property)
2. $[X] = [[X]]$ (idempotent property)
3. $X \subseteq Y \Rightarrow [X] \subseteq [Y]$ (isotone property)

(Interestingly enough, these properties are in fact equivalent to the single property

$$X \subseteq [Y] \Leftrightarrow [X] \subseteq [Y],$$

for all $X, Y \subseteq A$ — see De Witte [45].)

If $X \subseteq A$ and X is algebraically closed in A , then X is the underlying set of another algebra $\langle X; F|_X \rangle$, where $F|_X$ is defined to equal $\{\phi|_X : \phi \in F\}$, the restriction of the members of F to the domain X . The restriction is usually implicit: one writes $\langle X; F \rangle$ in place of $\langle X; F|_X \rangle$. Such an algebra is called a *subalgebra* of A . If, for some set Y , one has $[Y] = X$, the set Y is said to *generate* X , and the elements of Y are called *generators*. If Y is also minimal in the sense that $[Y \setminus \{y\}] \subset X$ for all $y \in Y$, it is called an *independent* set, and a *basis* for X . X is said to be *finitely generated* if there exists a finite set Y which generates X . Let us also write $Y \vdash y \Leftrightarrow y \in [Y]$, and $x \cong y \Leftrightarrow \{x\} \vdash y$ and $\{y\} \vdash x$. It is worth noting that $\cong$ is an equivalence relation on $\mathbf{P}_A$. The expression “ $Y \vdash y$ ” is easiest read as “ y is derivable from Y .”

$[\cdot]$ imposes a lattice structure on the algebraically closed subsets of A :

1.2.1 Proposition *Let $\mathcal{A} = \langle A; X \rangle$ be given. Then the algebraically closed subsets of A form an algebraic lattice $\mathcal{L}(A)$, ordered by inclusion, where $\wedge$ is set intersection, and $\vee$ is defined by $X \vee Y = [X \cup Y]$.*

1.2.1 The algebra of functions

The next series of definitions is concerned with describing a universal algebra whose universe is the set of functions $\mathbf{P}_A$. The operations are chosen to formalize the composition of functions and the rearrangement of a function's arguments. The subalgebras are thus closed under the intuitive rules for forming one function in $\mathbf{P}_A$ out of others; that is, by composing functions and renaming variables.

1.2.2 Definition We define the operations $\zeta, \tau, \Delta, \nabla$, and $*$ on the set $\mathbf{P}_A$ as follows. Let $f \in \mathbf{P}_A^{(n)}$ and $g \in \mathbf{P}_A^{(m)}$, where $n, m \in \mathbb{N}$. If $n = 1$, define $\zeta f = \tau f = \Delta f = f$. For $n > 1$, let

$$(\zeta f)(x_0, x_1, \dots, x_{n-1}) = f(x_1, x_2, \dots, x_{n-1}, x_0),$$

$$(\tau f)(x_0, x_1, \dots, x_{n-1}) = f(x_1, x_0, x_2, \dots, x_{n-1}),$$

$$(\Delta f)(x_0, x_1, \dots, x_{n-1}) = f(x_0, x_0, x_1, \dots, x_{n-2}).$$

Then both ζf and τf are also functions of n variables, while Δf is a function of $n - 1$ variables. Let $(\nabla f)(x_0, x_1, \dots, x_n) = f(x_1, x_2, \dots, x_n)$. Let

$$(* (f, g))(x_0, x_1, \dots, x_{n+m-2}) = f(g(x_0, x_1, \dots, x_{m-1}), x_m, x_{m+1}, \dots, x_{n+m-2}).$$

We shall call ζ and τ the *permutation* operations, and Δ, ∇ , and $*$ the *identification*, *cylindrification*, and *composition* operations, respectively.

We also define the *projection* functions $e_i^n : A^n \rightarrow A$ by $e_i^n(x_0, x_1, \dots, x_{n-1}) = x_{i-1}$, and then let $\mathbf{e}$ be a unary operation on $\mathbf{P}_A$ defined by $\mathbf{e} : \mathbf{P}_A \rightarrow \{e_1^1\}$. Then the universal algebra $\mathcal{P}_A = \langle \mathbf{P}_A; \mathbf{e}, \zeta, \tau, \Delta, \nabla, * \rangle$ obtained using these operations on $\mathbf{P}_A$ is known variously as the *full iterative algebra over A* , or the *algebra of functions of A -valued logic*.

The algebraically closed sets of $\mathcal{P}_A$ are known historically as *iteratively closed classes of functions*; here they shall be called *clones*, in accordance with modern terminology. Their importance

within universal algebra stems from the observation that, if F is a subset of $\mathbf{P}_A$, then $\mathcal{A} = \langle A; F \rangle$ is an algebra, and $[F]$ consists of exactly those functions on A which can be realized using only the operations F . Here, the set $[F]$ is called the *term functions* of $\mathcal{A}$, or the set of *polynomials* of $\mathcal{A}$. (The latter term generalizes the conventional definition of a polynomial over a ring $\langle R; +, *, -, 0 \rangle$.) If $F, G \subseteq \mathbf{P}_A$ and $[F] = [G]$, then the algebras $\mathcal{A}_F = \langle A; F \rangle$ and $\mathcal{A}_G = \langle A; G \rangle$ are equivalent, in the sense that all of the operations F can be expressed in terms of the operations G , and vice versa. In particular, $S \subseteq A$ is a closed subset of $\mathcal{A}_F$ iff it is a closed subset of $\mathcal{A}_G$, which means that $\mathcal{L}(\mathcal{A}_F) = \mathcal{L}(\mathcal{A}_G)$. Such algebras $\mathcal{A}_F$ and $\mathcal{A}_G$ are said to be *polynomially equivalent*. Thus we see that there is a bijective correspondence between the clones of $\mathcal{P}_A$, and the equivalence classes, under polynomial equivalence, of algebras with universe A . Furthermore, finitely generated clones correspond to algebras of finite type.

1.2.3 Proposition *Let $F \subseteq \mathbf{P}_A$ be a clone. Then the following statements hold:*

- (a) *If $f(x_0, x_1, \dots, x_{n-1}) \in F$, and σ is a permutation of $\llbracket n \rrbracket$, then $f(x_{\sigma 0}, x_{\sigma 1}, \dots, x_{\sigma(n-1)}) \in F$ as well.*
- (b) *$e_i^n \in F$ for all $1 \leq i \leq n$.*

The proof of both parts is a matter of inspection.

It is often of interest to consider the set of functions derivable from another set using only a particular subset of the rules of formation listed above. For example, we may wish to consider a set of functions which we obtain only by reordering or identifying arguments. Formally, this amounts to considering the closed sets of algebras on $\mathbf{P}_A$ whose fundamental operations are a subset of those of the algebra $\mathcal{P}_A$. The closure of a set X in the algebra $\langle \mathbf{P}_A; \Delta, \mathbf{e}, \zeta, \tau \rangle$ is just the set of functions obtainable from X by any identification or permutation of variables. Let us write $X \vdash_{\Delta} f$ if f is a member of $[X]$ in this algebra. Similarly, we shall consider the set of operations $\nabla, \mathbf{e}, \zeta$, and τ . The closure of X here is the set of functions obtained only by adding fictitious arguments and reordering. We shall write $X \vdash_{\nabla} f$ in this case. Note that the removal of some of an algebra's fundamental operations decreases the size of its closed sets. In particular, then, if $X \vdash_{\Delta} f$ or $X \vdash_{\nabla} f$, it follows that $X \vdash f$.

1.2.2 The algebra of relations

We shall now give an analogous definition of the algebra $\mathcal{R}_A$, which will play an important role in the upcoming discussion of $\mathcal{P}_A$. We begin with its underlying set.

For any $m \in \mathbb{N}$, we call a set $\rho \subseteq A^m$ an *m-ary relation* on the set A . The elements of a relation ρ are called *points*. An n -tuple of points of ρ will frequently be written as an $m \times n$ matrix (a_{ij}) , the columns of which are $(a_{1j}, a_{2j}, \dots, a_{mj}) \in \rho$: for short, we will write $(a_{ij}) \prec \rho$. Let $\mathbf{R}_A^{(m)} = \{\rho : \rho \subseteq A^m\}$, and let

$$\mathbf{R}_A = \bigcup_{m \in \mathbb{N}} \mathbf{R}_A^{(m)}, \quad (1.2)$$

the set of all relations on A . As we did for sets of functions, if $Q \subseteq \mathbf{R}_A$, define $Q^{(m)} = Q \cap \mathbf{R}_A^{(m)}$. Once again, the equality (1.2) is a disjoint union, the arity function $\tilde{o} : \mathbf{R}_A \rightarrow \mathbb{N}$ given by

$$\tilde{o}(\rho) = \begin{cases} m & \text{if } \rho \in \mathbf{R}_A^{(m)} \text{ and } \rho \neq \emptyset, \\ 0 & \text{otherwise} \end{cases}$$

is well defined. In practice, we will use the symbol o for this arity function as well, where there is no danger of ambiguity. The i th component of a relation $\rho \in \mathbf{R}_A^{(m)}$ is *essential* if there exist $a_j \in A$, for $0 < j \leq n$, and $a'_i \in A$, for which $(a_1, a_2, \dots, a_n) \in \rho$ and $(a_1, a_2, \dots, a'_i, \dots, a_m) \notin \rho$. A component of ρ which is not essential is said to be *fictitious*. By *identical* components $i \neq j$ in ρ , we mean that $a_i = a_j$ for all $a \in \rho$. A relation ρ will be called *essential* if all of its components are essential, and it will be called *simple* if, in addition, no two of them are identical.

If $Q \subseteq \mathbf{R}_A$, the pair $\langle A; Q \rangle$ is called a *relational algebra*. A relation can be viewed as a predicate over the set A ; thus, a relational algebra is a set of predicates, together with their domain. In the same way $\mathcal{P}_A$ formalizes the composition of functions, the algebra $\mathcal{R}_A$ shall formalize the logical conjunction of predicates.

There are several equivalent ways to select a set of fundamental operations for $\mathcal{R}_A$. Let $\rho \in \mathbf{R}_A^{(m)}$ and $\sigma \in \mathbf{R}_A^{(m')}$ for $m, m' \in \mathbb{N}$. The definitions of the operations ζ, τ, Δ , and ∇ are analogous to those for the function algebra. If $m > 1$, let

$$\begin{aligned} \zeta \rho &= \{(x_1, x_2, \dots, x_{m-1}, x_0) : (x_0, x_1, \dots, x_{m-1}) \in \rho\}, \\ \tau \rho &= \{(x_1, x_0, x_2, \dots, x_{m-1}) : (x_0, x_1, \dots, x_{m-1}) \in \rho\}, \end{aligned}$$

$$\begin{aligned}\Delta\rho &= \{(x_1, x_1, x_2, \dots, x_{m-1}) : (x_0, x_1, \dots, x_{m-1}) \in \rho\}, \\ \pi\rho &= \{(x_0, x_1, \dots, x_{m-2}) : (x_0, x_1, \dots, x_{m-1}) \in \rho\}.\end{aligned}$$

For $m \leq 1$, define $\zeta\rho = \tau\rho = \Delta\rho = \rho$, and $\pi\rho = \emptyset$. Let

$$\nabla\rho = \{(x_0, x_1, \dots, x_m) : (x_0, x_1, \dots, x_{m-1}) \in \rho\}.$$

Let $\mathbf{c}$ be the constant operation $\mathbf{c} : \mathbf{R}_A \rightarrow \{A\}$. We also define the intersection of two relations: assume, without loss of generality, that $m \geq m'$. Let $\tilde{\sigma}$ be the m -ary relation obtained by applying ∇ to σ $m - m'$ times, let $\rho \cap \sigma$ denote the set-theoretic intersection of ρ and $\tilde{\sigma}$, and let $\sigma \cap \rho = \rho \cap \sigma$. Finally, let the cartesian product of relations $\rho \times \sigma$ be given by

$$\rho \times \sigma = \{(x_0, x_1, \dots, x_{m+m'-1}) : (x_0, x_1, \dots, x_{m-1}) \in \rho \text{ and } (x_m, x_{m+1}, \dots, x_{m+m'-1}) \in \sigma\}.$$

Then the algebra $\mathcal{R}_A = \langle \mathbf{R}_A; \mathbf{c}, \zeta, \tau, \Delta, \nabla, \pi, \cap \rangle$ is called the *complete relational algebra* on A . In accordance with the observations in the previous section, we may replace our choice of fundamental operations for $\mathcal{R}_A$ with any other set of generators for the clone $\{\{\mathbf{c}, \zeta, \tau, \Delta, \nabla, \pi, \cap\}\}$ in $\mathcal{P}_{\mathbf{R}_A}$ and obtain a polynomially equivalent algebra. The following proposition thus gives two alternatives for the set of fundamental operations.

1.2.4 Lemma *The following are true in the algebra $\mathcal{P}_{\mathbf{R}_A}$:*

- (a) $\{\zeta, \nabla, \cap\} \vdash \times$,
- (b) $\{\zeta, \tau, \times, \pi, \Delta\} \vdash \cap$,
- (c) $\{\mathbf{c}, \times\} \vdash \nabla$,
- (d) $\{\zeta, \tau, \nabla, \pi, \cap\} \vdash \Delta$.

1.2.5 Proposition $\mathcal{R}_A = \langle \mathbf{R}_A; \mathbf{c}, \zeta, \tau, \Delta, \pi, \times \rangle$, and $\mathcal{R}_A = \langle \mathbf{R}_A; \mathbf{c}, \zeta, \tau, \nabla, \pi, \cap \rangle$.

Proof: The first equivalence is established using items (b) and (c) from the lemma. The second is obtained from (d). ■

The algebraically closed classes of the relational algebra are called *coclones*. They too form an algebraic lattice under inclusion: we shall denote the lattice operations and partial ordering

by $\vee_R, \wedge_R, \leq_R$, respectively. Similarly, let those operations in the lattice of function classes be written $\vee_P, \wedge_P$, and $\leq_P$, although the subscripts will be freely dropped when the lattice to which we refer is indicated clearly by context. The greatest element in the lattice of clones and coclones is, respectively, $\mathbf{P}_A$ and $\mathbf{R}_A$. Let us denote their least element by $\mathbf{J}_A$ and $\mathbf{D}_A$, respectively. The latter shall be called the coclone of *diagonal* relations.

Although a significant portion of the theory discussed here generalizes to infinite underlying sets, the results of this investigation depend essentially on finiteness; we shall be hereafter restricting our attention, then, to the case where $|A| < \infty$. Since no properties are assumed of the actual elements of the underlying set, we shall usually set $A = \{0, 1, \dots, k-1\}$ for some $k \in \mathbf{N}$, in the interests of uniformity. We shall adopt the notation $\llbracket k \rrbracket = \{0, 1, \dots, k-1\}$, for $k \in \mathbf{N}$. It is conventional to abbreviate $\mathcal{P}_{\llbracket k \rrbracket}, \mathbf{P}_{\llbracket k \rrbracket}, \mathcal{R}_{\llbracket k \rrbracket}$, and $\mathbf{R}_{\llbracket k \rrbracket}$ by $\mathcal{P}_k, \mathbf{P}_k, \mathcal{R}_k$, and $\mathbf{R}_k$, respectively.

Let us now consider some additional operations that may be derived from the fundamental operations, in the interests of convenience. First, if $\rho \in \mathbf{R}_A^{(n)}$ and g is a permutation of $\llbracket n \rrbracket$, one can see that the relation ρ' obtained from ρ by permuting its components with g is equivalent to ρ , since the operations ζ and τ generate all permutations of the components of ρ . More generally, if $g : \llbracket n \rrbracket \rightarrow \llbracket l \rrbracket$ is an injection, it is also true that if we let

$$\Sigma_g(\rho) = \left\{ \mathbf{b} \in A^l : b_i = a_{g(i)}, 1 \leq i \leq n, \mathbf{a} \in \rho \right\},$$

then $\rho \cong \Sigma_g(\rho)$, since one can derive $\Sigma_g(\rho)$ from ρ by some sequence of ζ , τ , and ∇ , and one can also obtain ρ from $\Sigma_g(\rho)$ using ζ , τ , and π .

If ϵ is an equivalence relation on the set $\llbracket n \rrbracket$, for some $n \in \mathbf{N}$, define the n -ary relation

$$\delta_\epsilon = \{(x_0, x_1, \dots, x_{n-1}) \in A^n : x_i = x_j \text{ if } (i, j) \in \epsilon\},$$

and define for $\rho \in \mathbf{R}_A^{(n)}$

$$\Delta_\epsilon \rho = \rho \cap \delta_\epsilon.$$

The latter is the relation obtained by identifying those components of ρ which are equivalent in ϵ .

We shall abbreviate $\Delta_{\{(i,j)\}}$ by Δ_{ij} .

By analogy with our definition for functions, we shall define $Q \vdash_\Delta \rho$ to mean that ρ is contained

in the closure of the set of relations Q under the operations Δ , ζ , τ , and $\mathbf{c}$. For example, if ϵ is an equivalence relation on $\llbracket n \rrbracket$, then $\rho \vdash_{\Delta} \Delta_{\epsilon} \rho$.

Let us define $K_n = \llbracket k \rrbracket^n$, called the *full relation*. It is easy to see that $K_n \in \mathbf{D}_k$ for all $n \in \mathbf{N}$. More generally, define the relation $\delta_{\epsilon} = \Delta_{\epsilon} K_n$ for an equivalence relation ϵ on $\llbracket n \rrbracket$. Then we have the following:

1.2.6 Proposition

- (a) $\mathbf{J}_k$ is the set $\{e_i^n : n \in \mathbf{N} \text{ and } 1 \leq i \leq n\}$.
- (b) $\mathbf{D}_k$ consists of the empty relation $\emptyset$ and all relations δ_{ϵ} , where ϵ is an equivalence relation on the set $\{1, 2, \dots, m\}$, for some $m \in \mathbf{N}$.

Proof: For both, one verifies that the set given is indeed closed, and then observes that it is contained in every closed subset of $\mathbf{P}_k$ or $\mathbf{R}_k$, respectively. See Proposition 1.2.3. ■

Several more special clones and coclones will now be named. Let $\text{Con}_R(k)$ denote the coclone generated by the constant relations $\{\{0\}, \dots, \{k-1\}\}$. Analogously, let $\text{Con}_P(k)$ be the clone generated by all the constant-valued functions in $\mathbf{P}_k$. Define $S_k = \left[\left\{ f \in \mathbf{P}_k^{(1)} : |\text{rng}(f)| = k \right\} \right]$, the clone generated by the set of permutations on $\llbracket k \rrbracket$. Let $\Omega_k = [\mathbf{P}_k^{(1)} \setminus S_k]$, the clone of noninvertible, essentially unary functions. Since a clone F of essentially unary functions consists just of unary functions and those nonunary functions obtained from them by adding fictitious variables, we shall identify such a clone with its unary subset. F is most naturally viewed as a monoid whose operation is composition, $\langle F; *, e_1^1 \rangle$. If the members of F all happen to be invertible, $\langle F; *, {}^{-1}, e_1^1 \rangle$ is a group; for example, we shall regard S_k as the symmetric group on $\llbracket k \rrbracket$. Finally, let $U = [\mathbf{P}_k^{(1)}]$, the clone of all essentially unary functions.

We conclude this section with a pair of schemes for obtaining relations from functions. First, for a function $f : D \rightarrow \llbracket k \rrbracket$ with $D \subseteq \llbracket k \rrbracket^n$, define $f^{\bullet} \in \mathbf{R}_k^{(n)}$ by

$$f^{\bullet} = \{(x_0, \dots, x_n) \in \llbracket k \rrbracket^n : f(x_0, \dots, x_{n-1}) = x_n\}.$$

$f^{\bullet}$ is called the *graph* of f . One defines the graph of a set $X \subseteq \mathbf{P}_k$ to be $X^{\bullet} = [\{f^{\bullet} : f \in X\}]$. For example, $\text{Con}_P(k)^{\bullet} = \text{Con}_R(k)$.

1.2.7 Proposition *Let $X \subseteq \mathbf{P}_k$. If $X \vdash f$, then $f^\bullet \in X^\bullet$.*

Proof: Omitted. ■

The second construction adds new points to a given relation. For $\rho \in \mathbf{R}_k^{(m)}$ and A an $n \times m$ matrix over $\llbracket k \rrbracket$, we write $A \prec \rho$ if every column of A is an element of ρ . Put $\rho_0 = \rho$, and for $i \geq 0$ let

$$\rho_{i+1} = \rho_i \cup \{f(A) : A \prec \rho_i\}. \quad (1.3)$$

Then we define $\Gamma_f(\rho) = \bigcup_{i \in \mathbb{N}} \rho_i$. The definition can be extended a set of functions F as well, by replacing (1.3) with

$$\rho_{i+1} = \rho_i \cup \{f(A) : A \prec \rho_i \text{ and } f \in F\}.$$

The two definitions relate conveniently:

1.2.8 Proposition *Let $F \leq \mathbf{P}_k$ be a clone, $f \in \mathbf{P}_k$, and $\rho \in \mathbf{R}_k$. Then*

$$(a) \Gamma_f(\rho) = \{g(A) : f \vdash g \text{ and } A \prec \rho\}, \quad \text{and}$$

$$(b) \Gamma_F(\rho) = \{g(A) : F \vdash g \text{ and } A \prec \rho\}.$$

Our use of this construction will be restricted to a specific relation, χ_n . Let A be the $k^n \times k$ matrix whose rows are the elements of $\llbracket k \rrbracket^n$, in ascending lexicographic order. Then we define χ_n to be the relation whose points are the columns of A . We call χ_n the *n-ary ordinate* relation on $\llbracket k \rrbracket$, and $\Gamma_f(\chi_n)$ the *n-ary orbit* of f .

1.3 Functions with relations

Since clones are infinite sets, it is desirable to be able to specify them more succinctly than by simply enumerating their elements. We have already seen that one can designate a clone by listing its generators, which is a particularly satisfying representation if the clone is finitely generated. Following a quite different approach, one can also specify a clone by stating a condition which its members must satisfy.

For example, let $F \subset \mathbf{P}_2$ be the set of *monotone* functions, defined to be those functions $f \in \mathbf{P}_2^{(n)}$, for some n , for which $f(x_0, x_1, \dots, x_{n-1}) \leq f(y_0, y_1, \dots, y_{n-1})$ if $x_i \leq y_i$ for each $0 \leq i < n$.

We can restate this definition in the language of the last section by letting σ denote the relation

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix},$$

then observing that $F = \{f \in \mathbf{P}_2 : A \prec \sigma \Rightarrow f(A) \in \sigma\}$. F is also a clone, since the property of monotonicity is preserved under composition and the other clone operations. Properties of functions or sets of functions that are preserved under the clone operations are of particular interest, and we shall distinguish them with the adjective *relational*. While it is not hard to show that F is generated by $\{\text{et}, \text{vel}, \mathbf{0}, \mathbf{1}\}$, our characterization of F by a relational property is, from some perspective, the more natural one.

In order to elucidate the notion of a relational description of a clone, we require some definitions. Let $f \in \mathbf{P}_k^{(n)}$ and $\rho \in \mathbf{R}_k^{(m)}$. Then f is said to *preserve* ρ if, for all $A \prec \rho$, $f(A) \in \rho$. We define the maps

$$\text{Inv} : 2^{\mathbf{P}_k} \rightarrow 2^{\mathbf{R}_k} : \text{Inv } X = \{\rho \in \mathbf{R}_k : \forall f \in X, f \text{ preserves } \rho\},$$

$$\text{Pol} : 2^{\mathbf{R}_k} \rightarrow 2^{\mathbf{P}_k} : \text{Pol } Y = \{f \in \mathbf{P}_k : \forall \rho \in Y, f \text{ preserves } \rho\}.$$

Inv and Pol are called the *invariant* operator and *polymorph* operator, respectively. Inv gives the set of relations which are preserved by (that is, invariant under) a set of functions, while Pol is the set of all functions preserving each member of a set of relations. In the example above, $\sigma \in \text{Inv } F$, and $F \subseteq \text{Pol } \{\sigma\}$.

The next proposition shows a connection between functions and coclones, and between relations and clones. We saw that the functions F preserving σ were closed under the clone operations. More generally, it is the case that the property of “preserving” is hereditary under both the operations of $\mathcal{P}_k$, and the operations of $\mathcal{R}_k$:

1.3.1 Proposition *If $X \subseteq \mathbf{P}_k$ and $Y \subseteq \mathbf{R}_k$, $\text{Inv } X$ is closed in $\mathcal{R}_k$, and $\text{Pol } Y$ is closed in $\mathcal{P}_k$.*

Proof: First, we would like to show that $\text{Inv } X$ is closed under the fundamental operations of $\mathcal{R}_k$; let us make use of the second characterization of $\mathcal{R}_k$ given in Proposition 1.2.5. Suppose $\rho \in \text{Inv } X$: then every $f \in X$ preserves ρ . That f also preserves $\zeta\rho$, $\tau\rho$, $\pi\rho$, and $\nabla\rho$ is immediate. If f preserves ρ_1 and ρ_2 , where $h_i = o(\rho_i)$ for $i = 1, 2$ and $h_1 > h_2$, then for any $A \prec \rho_1 \cap \rho_2$, $X \prec \rho_1$,

so $f(X) \in \rho_1$, and $X \prec \nabla^{h_1-h_2} \rho_2$, so $f(X) \in \nabla^{h_1-h_2} \rho_2$, whence $f(X) \in \rho_1 \cap \rho_2$. Finally, every function preserves the relation $\mathbf{c} = \{\llbracket k \rrbracket\}$.

The argument that $\text{Pol } Y$ is closed in $\mathcal{P}_k$ is similar. The projection function e_1^2 preserves all relations. If a function f preserves a relation $\rho \in \text{Pol } Y$, then clearly ζf , τf , and δf do as well. Similarly, $(\nabla f)(A) \in \rho$ if and only if the first $o(f)$ columns of A are in ρ , which is certainly true when $A \prec \rho$, so ∇f preserves ρ . If f and g preserve ρ , then so does $f * g$: Let $n = o(f)$ and $l = o(g)$. Then if $(A|A') \prec \rho$ for submatrices A and A' with n and l columns, respectively, $g(A) \in \rho$, so $(g(A)|A') \prec \rho$, which implies in turn that $(f * g)(A|A') = f(g(A)|A') \in \rho$. ■

Note that the functions Inv and Pol both reverse the direction of the inclusion of sets: that is, if $X_1 \subseteq X_2 \subseteq \mathbf{P}_k$, then $\text{Inv } X_1 \supseteq \text{Inv } X_2$, and the analogous statement is true for Pol . Functions with this property are said to be *antiisotone*.

The proposition shows that the range of Pol is contained in the set of clones, and the range of Inv is contained in the set of coclones. In fact, a much stronger result holds: Pol and Inv realize a bijection between the clones of $\mathcal{P}_k$ and the coclones of $\mathcal{R}_k$. This fundamental observation is due to Geiger [15] and Bodnarčuk, Kalužnin, Kotov, and Romov [4]. Formally, we have

1.3.2 Theorem *If $X \subseteq \mathbf{P}_k$, $\text{Pol } \text{Inv } X = [X]$. If $Y \subseteq \mathbf{R}_k$, $\text{Inv } \text{Pol } Y = [Y]$.*

A lemma is required before proving the theorem. If for some $D \subseteq \llbracket k \rrbracket^n$, g is a function $g : D \rightarrow \llbracket k \rrbracket$, g is said to be a *partial function* on $\llbracket k \rrbracket$. Let $\text{dom } g \subseteq \llbracket k \rrbracket^n$ denote the domain of g . The definition of functions preserving relations is extended to partial functions as follows: g preserves a relation ρ if, for every $m \times n$ matrix $A \prec \rho$ for which each row of A is a member of $\text{dom } g$, we have $g(A) \in \rho$.

1.3.3 Lemma *If a partial function g preserves a coclone Y in $\mathcal{R}_k$, then there exists a function $f \in \mathbf{P}_k$ with $f^\bullet \supseteq g^\bullet$ that also preserves Y .*

Proof: Since the domain of a given function is finite, it is sufficient to prove that if g is a partial function preserving Y , then there exists a function f with $f^\bullet \supset g^\bullet$ with $|\text{dom } f| = |\text{dom } g| + 1$ which also preserves Y . For some $x \notin \text{dom } g$, then, let us define $g_i(x) = i$ for $i \in \llbracket k \rrbracket$, and agreeing with g elsewhere. To show that at least one of the functions g_i preserves Y , suppose the contrary. Then

there is a relation $\sigma_i \in Y$ for which $g_i(A_i) \notin \sigma_i$ for some $A_i \prec \sigma_i$, for each i . Since g preserves Y , it must be the case that x is a row of each matrix A_i . Since a coclone is closed under the operations of row permutations, we may assume that x is the first row of each. Form the relation $\sigma \in Y$, then, by

- (a) taking the product of the relations σ_i ,
- (b) identifying the first component of each factor σ_i ,
- (c) projecting out the first component of the factors $\sigma_1, \sigma_2, \dots, \sigma_{k-1}$.

Let $\sigma' \in Y$ denote the relation obtained by projecting out the first component of σ_0 as well.

For a $m \times n$ matrix A , let $\overline{A}$ denote the $m-1 \times n$ matrix obtained from A by deleting the first row. Let

$$A = \begin{pmatrix} x \\ \overline{A_0} \\ \overline{A_1} \\ \vdots \\ \overline{A_{k-1}} \end{pmatrix}.$$

By construction, $A \prec \sigma$ and $\overline{A} \prec \sigma'$. We have assumed that $g_i(A) \notin \sigma$ for any $i \in \llbracket k \rrbracket$. It follows by the definition of projection that $g(\overline{A}) \notin \sigma'$. Since $\sigma_i \in Y$ for each i , though, we have $\pi_0 \sigma_i \in Y$ and thus $\sigma' \in Y$, by the closure properties of coclones. However, g does not preserve σ' , a contradiction.

■

We may now prove the theorem.

Proof: One shows first that for clones X_1 and X_2 , $\text{Inv } X_1 = \text{Inv } X_2 \Rightarrow X_1 = X_2$: Suppose that $X_1 \neq X_2$ and assume, without loss of generality, that $X_1 \not\subseteq X_2$. Choose a function $f \in X_1 \setminus X_2$, and let $n = o(f)$. Then we claim that the relation $\Gamma_{X_2}(\chi_n)$ is in $\text{Inv } X_2 \setminus \text{Inv } X_1$: first, that every function in X_2 preserves $\Gamma_{X_2}(\chi_n)$ follows directly from the construction of $\Gamma_{X_2}(\cdot)$. If it were true that f preserved $\Gamma_{X_2}(\chi_n)$, we would have, in particular, $f(\chi_n) \in \Gamma_{X_2}(\chi_n)$; however, Proposition 1.2.8 indicates that there would exist an n -ary function $g \in X_2$ for which $f(\chi_n) = g(\chi_n)$. By the definition of χ_n , though, this would imply that $f = g$, contradicting $f \notin X_2$. We conclude that $\Gamma_{X_2}(\chi_n) \notin \text{Inv } X_1$.

Similarly, if Y_1 and Y_2 are coclones, then $\text{Pol } Y_1 = \text{Pol } Y_2 \Rightarrow Y_1 = Y_2$. The argument is analogous: suppose that there is a relation $\rho \in Y_1 \setminus Y_2$. Then we construct a function $f \in \text{Pol } Y_2 \setminus \text{Pol } Y_1$: that is, a function f which does not preserve ρ . To do so, we first produce a partial function g preserving Y_2 and not ρ , and then appeal to Lemma 1.3.3. Note that we may assume that ρ is simple. Now let

$$\sigma = \bigcap_{\xi \in Y_2, \xi \supseteq \rho} \xi.$$

Since Y_2 is closed under intersection, $\sigma \in Y_2$. By assumption, then, $\rho \subset \sigma$. For an arbitrary point $\mathbf{c} \in \sigma \setminus \rho$ and matrix $A = \rho$, let $f(A) = \mathbf{c}$. Our assumption that ρ is simple implies that f is well-defined, since A then contains no repeated rows. By construction, f does not preserve ρ . To see that f preserves Y_2 , however, suppose the contrary instead. Then $\exists \xi \in Y_2$ and $S \prec \xi$ for which $f(S) \notin \xi$. Assume again, without loss of generality, that the rows of S are distinct. Then the rows of S are also rows of A , so there is an injection $g : \llbracket o(\xi) \rrbracket \rightarrow \llbracket o(\sigma) \rrbracket$ mapping rows of S to matching rows of A . From the discussion on page 13, $\xi \cong \Sigma_g(\xi)$ where $\Sigma_g(\xi) \supseteq \rho$ and $f(A) = \mathbf{c} \notin \Sigma_g(\xi)$. But $\Sigma_g(\xi) \in Y_2 \Rightarrow \sigma \subseteq \Sigma_g(\xi)$, so $\mathbf{c} \notin \sigma$, yielding a contradiction. ■

Lemma 1.3.3 can be viewed as an analogue of Lagrange's Theorem for clones. We may rephrase it to state that if a given set of values of a function on a subset of its domain preserve $\text{Inv } K$ for clone K , then there exists an interpolating polynomial in K for those values; the classical theorem of Lagrange states that, given $n + 1$ values of a function from a field into itself, there exists a polynomial of degree no more than n interpolating those values. For insight of this nature, see the 1975 paper by Baker and Pixley [2].

Chapter 2

Properties of the Lattice of Clones

2.1 The Structure of $\mathcal{L}(\mathcal{P}_2)$

The only clone of the algebra $\mathcal{P}_1$ is $\mathbf{P}_1$, the set of all functions.

The structure of the lattice of clones of the algebra $\mathcal{P}_2$ was completely determined by 1941 by Post [34]. The proof he gave is lengthy, and uses an independent argument to establish each covering relation in the lattice. In [20], Jablonskiĭ, Gavrilov, and Kudrjavcev give a somewhat more modern presentation of Post's result. A substantially refined argument can be found in a recent paper by Ugol'nikov [43].

The lattice $\mathcal{L}(\mathcal{P}_2)$ is as shown in Figure 2.2. Before describing what functions make up the elements of the lattice, the reader should be warned that our definition of a clone is somewhat different from that used by Post, since he did not require the presence of the projection functions in each clone, and he did not assume closure under the addition of fictitious variables. His classification, then, is of the subalgebras of $\langle \mathbf{P}_2; \zeta, \tau, \Delta, * \rangle$, rather than $\mathcal{P}_2$. A consequence is that the names he gives to the clones are somewhat unnatural in our context. Since the clones that have analogues in $\mathcal{P}_k$ for $k > 2$ do not have names which are easily extended, we shall employ Post's nomenclature only for clones peculiar to $\mathcal{P}_2$, and within the description below of $\mathcal{L}(\mathcal{P}_2)$.

The bilateral symmetry evident in Figure 2.2 has an immediate explanation. Every Boolean function has a *dual* obtained by completely exchanging the roles of 0 and 1 in its definition. Duality is a relational property of pairs of functions, in the sense of Section 1.3; thus each Boolean clone has a dual clone consisting of the duals of its elements. The clones on the axis of symmetry of $\mathcal{L}(\mathcal{P}_2)$ are their own duals.

At the top, we have $C_1 = \mathbf{P}_2$. $C_3 = \text{Pol } \{0\} = \{f : f(0, 0, \dots, 0) = 0\}$. By duality, $C_2 = \text{Pol } \{1\}$, and $C_4 = C_2 \cap C_3$. C_2 and C_3 are the classes of functions preserving 1 and 0, respectively.

Next, $M_1 = \text{Pol} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$, equal to the set of monotone functions introduced in Section 1.3.

Once again, $M_2 = M_1 \cap C_2$, $M_3 = M_1 \cap C_3$, and $M_4 = M_1 \cap C_4$. Then $D_3 = \text{Pol} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, which is also equal to

$$\left\{ f : f(x_0, x_1, \dots, x_{n-1}) = \overline{f(\overline{x_0}, \dots, \overline{x_{n-1}})} \right\}.$$

The functions of D_3 are called *self-dual*. $D_1 = D_3 \cap C_4$, and $D_2 = D_3 \cap M_1$.

Figure 2.2: The lattice of clones of $\mathcal{P}_2$

The classes L_i consist of the *linear* functions:

$$L_1 = \left\{ f : f(x_0, x_1, \dots, x_{n-1}) = c_n + \sum_{i \in [n]} c_i x_i, \text{ for some } \mathbf{c} \in \llbracket 2 \rrbracket^{n+1} \right\}.$$

Equivalently,

$$L_1 = \text{Pol} \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

L_2, L_3 and L_4 are L_1 intersected with C_2, C_3 and C_4 , respectively: they are the linear functions preserving 1, preserving 0, and both, respectively. In addition, $L_5 = L_1 \cap D_3$.

$P_1 = [\{\text{et}(x, y)\}]$, the functions which are a conjunction of a subset of their variables. $P_3 = [\{\text{et}(x, y), \mathbf{0}\}]$, $P_5 = [\{\text{et}(x, y), \mathbf{1}\}]$, and $P_6 = P_3 \vee P_5$. The clones S_1, S_3, S_5 , and S_6 are their duals, obtainable by replacing et by vel, the disjunction operation.

The sets O_i contain the essentially unary functions. $O_1 = \mathbf{J}_2$: the clone of projections. O_5 and O_6 are $[\{\mathbf{1}\}]$ and $[\{\mathbf{0}\}]$, respectively, while $O_8 = O_5 \vee O_6$. $O_4 = [\{\bar{x}\}]$, and O_9 consists of all the unary functions.

Finally, the lattice contains eight infinite chains of clones $F_j^2 > F_j^3 > \dots$ for $1 \leq j \leq 8$, and their infima $F_j^\infty = \bigwedge_i F_j^i$. We define

$$F_8^i = \left\{ f : \text{if } \forall j, 1 \leq j \leq i, \exists \mathbf{y}^j : f(\mathbf{y}^j) = 1, \text{ then } \exists l : \mathbf{y}_l^j = 1, \text{ for all } 1 \leq l \leq i \right\}.$$

In the interests of easier visualization, one may associate a function $f \in \mathbf{P}_k^{(n)}$ with a family of n -sets

$$\{S_f \subseteq \llbracket n \rrbracket : f(x_0, x_1, \dots, x_{n-1}) = 1, \text{ where } x_i = 1 \Leftrightarrow i \in S\};$$

in this framework, $f \in F_8^i$ if and only if S_f is a family of sets in which any i members have non-empty intersection.

It is also the case that $F_8^i = \text{Pol}(K_i \setminus (1, 1, \dots, 1))$. F_8^∞ consists of those functions which assume the value 1 only if a given variable is 1. Equivalently, $\bigcap S_f \neq \emptyset$.

The other chains are similar, with $F_5^i = F_8^i \cap C_4$, $F_6^i = F_8^i \cap M_4$, and $F_7^i = F_8^i \cap M_1$. The clones F_j^i for $j = 1, 2, 3, 4$ are obtained by the duality principle.

Post's description of the lattice $\mathcal{L}(\mathcal{P}_2)$ afforded a complete answer to most questions about two-valued clones. As interest grew both in propositional logic of more than two values, and in clones with more general underlying sets, comparable results were sought for the clones of $\mathcal{P}_k$, for $k > 2$. Here we outline some of the work in that direction.

2.2 Coatoms and completeness criteria

One of the first questions that arises in clone theory is known as the completeness problem, and asks sets of functions in $\mathbf{P}_k$ are complete (that is, generate the clone $\mathbf{P}_k$.) Its solution is closely related to knowledge about the coatoms (maximal, proper subclones) of $\mathbf{P}_k$: one may check to see if a given collection of functions $S = \{f_1, f_2, \dots, f_n\}$ is complete by testing the membership of each f_i in each of the coatoms of $\mathbf{P}_k$. S is complete exactly when no coatom contains all of S 's members, in view of the isotone property of the closure operator (page 8.) Conversely, a clone K is a coatom iff the set $K \cup \{f\}$ is complete for any $f \notin K$.

In $\mathcal{P}_2$, the determination of $\mathcal{L}(\mathcal{P}_2)$ provides a solution to the completeness problem: $\mathbf{P}_2$ has five coatoms, each with an easily verified defining property. A set S is complete if not all of its members are monotone, not all are linear, *et cetera*.

Long before much progress was made towards a solution of the completeness problem in $\mathcal{P}_k$ for $k > 2$, a solution to an important special case appeared. The result is known as the Šlupecki Criterion, and was presented by Šlupecki [44] in 1939, then later rediscovered by Butler [7]. It gives necessary and sufficient conditions for the completeness of a set of functions that includes all unary functions:

2.2.1 Theorem (Šlupecki Criterion) *Suppose $k \geq 3$. Then for $f \in \mathbf{P}_k$, one has $[\{f\} \cup \mathbf{P}_k^{(1)}] = \mathbf{P}_k$ if and only if $|\text{rng}(f)| = k$ and $o_e(f) > 1$.*

(An equivalent statement is that, if a set of functions contains the set of unary functions, $\mathbf{P}_k^{(1)}$, then it is complete if and only if it also contains some surjective function that depends on more than one variable.)

A natural weakening of the theorem's conditions is to consider the clone $[\{f\} \cup \mathbf{P}_k^{(1)}]$ when $|\text{rng}(f)| < k$. Such clones have been studied by A. I. Mal'cev [26], Burle [5], and I. A. Mal'cev [25]. It happens that all clones containing $\mathbf{P}_k^{(1)}$ arise in this way, and that they are finite in number. Let us digress briefly in order to give them names. First let $V_i = \{f \in \mathbf{P}_k : |\text{rng}(f)| \leq i\} \cup \mathbf{J}_k$, for $1 \leq i \leq k$. It is not hard to see that each set V_i is, in fact, a clone; they are referred to as *basic cells*. For each $1 \leq i \leq k$, let $U_i = V_i \cup U$. Recall that U is the clone of essentially unary functions. We

define the *quasilinear* clone, L_2 , to be those functions that add their arguments modulo 2, subject to an independent interpretation of each argument as a value mod 2. Specifically, L_2 consists of all $f \in \mathbf{P}_k^{(n)}$, for some $n \in \mathbf{N}$, for which there exist functions $\phi_i : \llbracket k \rrbracket \rightarrow \mathbf{Z}_2$, for $1 \leq i \leq n$, and some $\psi : \mathbf{Z}_2 \rightarrow \llbracket k \rrbracket$, such that

$$f(x_1, x_2, \dots, x_n) = \psi\left(\sum_{i=1}^n \phi_i(x_i)\right). \quad (2.4)$$

The addition takes place in $\mathbf{Z}_2$, the ring of integers modulo 2. Let us also take this opportunity to define L_2^ε as the largest clone contained in L_2 for which all of the maps ϕ_i have the additional property that

$$|\{j : \phi_i(j) = a\}|$$

is even, for $a = 0$ and 1 . When k is odd, of course, we have $L_2^\varepsilon = \mathbf{J}_k$: just the projections.

2.2.2 Theorem (Burle) *Suppose $k \geq 3$. Then the interval $[U, \mathbf{P}_k]$ consists of only the chain*

$$U = U_1 < L_2 \vee U_1 < U_2 < \dots < U_{k-1} < U_k = \mathbf{P}_k.$$

While it was known quite early that the number of coatoms of $\mathbf{P}_k$ is finite for each k , it was also observed that their number grew very rapidly with k , and several years passed before their complete classification (and its attendant solution to the completeness problem) appeared in print. Before discussing this classification, though, let us refer to Kuznecov [23] and Butler [7] for the following:

2.2.3 Proposition (Kuznecov) *For $k > 2$, $\mathbf{P}_k$ has at most one coatom for each submonoid of U .*

Proof: For any clone $K \leq \mathbf{P}_k$, we define $\text{Tr } K = K \wedge U$, called the *trace* of K . It is routine to verify that if $\text{Tr } K = \text{Tr } K' = M$ for some $M \leq U$, then $\text{Tr } (K \vee K') = M$ as well. Denote the coatoms of $\mathbf{P}_k$ by $\{K_i\}$ for $i \in I$, and suppose that $\text{Tr } K_i = \text{Tr } K_j = M$ for some M and $K_i \neq K_j$. Then we have $M = \text{Tr } (K_i \vee K_j) = \text{Tr } \mathbf{P}_k = U$. Burle's Theorem (2.2.2) shows, however, that U is contained in at most one coatom. By contradiction, we conclude that no two coatoms have the same trace. ■

Since U contains no more submonoids than subsets, $\mathbf{P}_k$ can have no more than 2^{k^*} coatoms. In fact, their classification proceeded by characterizing those submonoids which corresponded with coatoms. This was completed by Rosenberg around 1970 [37], using partial results due to Kuznecov [23], [24], Schofield [42], Jablonskiĭ [21], and others. If K is a coatom of $\mathbf{P}_k$, then the Galois Correspondence (Theorem 1.3.2) implies that $\text{Inv } K$ is an atom of $\mathbf{D}_k$: that is, a minimal, nontrivial coclone in $\mathcal{R}_k$. A minimal coclone is generated by any of its nondiagonal elements: $\text{Inv } K = [\rho]$ for any $\rho \in \text{Inv } K \setminus \mathbf{D}_k$. Therefore, the coatoms of $\mathbf{P}_k$ can all be expressed in the form $K = \text{Pol } \rho$, for some relations ρ .

Preparatory to stating Rosenberg's Theorem, we need to introduce the defining properties for some classes of such relations. First, an abelian group G is said to be *p-elementary* if it has exponent p . If G is finite and *p-elementary*, clearly $|G|$ is a power of p .

Next, a relation $\rho \in \mathbf{R}_k^{(h)}$ is called *central* if

- (a) there is some nonempty set $C \subseteq \llbracket k \rrbracket$ such that

$$x_j \in C \Rightarrow (x_0, \dots, x_{h-1}) \in \rho$$

for every $0 \leq j \leq h-1$,

- (b) $(x_0, \dots, x_{h-1}) \in \rho \Rightarrow (x_{\sigma 0}, \dots, x_{\sigma(h-1)}) \in \rho$, for all permutations $\sigma \in S_h$, and

- (c) $x_i = x_j \Rightarrow (x_0, \dots, x_{h-1}) \in \rho$, for every $0 \leq i < j \leq h-1$.

By definition, then, all unary relations are central. The last two conditions can be regarded as generalizations of the symmetric and reflexive properties, respectively, of a binary relation.

Last, for a fixed value of $k > 2$ and $2 \leq h \leq k$, we define the relation

$$\iota_h = \left\{ (x_0, \dots, x_{h-1}) \in \llbracket k \rrbracket^h : |\{x_0, \dots, x_{h-1}\}| < h \right\}.$$

A relation $\rho \in \mathbf{R}_k^{(h)}$ is said to be *h-universal* if there is a value $m \geq 1$ and a surjective map $\lambda : \llbracket k \rrbracket \rightarrow \llbracket h \rrbracket^m$ such that for all $\mathbf{x} = (x_0, \dots, x_{h-1}) \in \llbracket k \rrbracket^h$, $\mathbf{x} \in \rho$ if and only if

$$(\lambda(x_0)_i, \dots, \lambda(x_{h-1})_i) \in \iota_h \quad (\forall i : 0 \leq i < m).$$

A trivial example of an h -universal relation is ι_h itself. Alternatively, let λ map $\llbracket 4 \rrbracket$ onto $\llbracket 2 \rrbracket \times \llbracket 2 \rrbracket$ via

x	$\lambda(x)$
0	(0, 0)
1	(0, 1)
2	(1, 0)
3	(1, 1)

from which we get the 2-universal relation

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 & 3 & 3 & 3 \\ 0 & 1 & 3 & 0 & 1 & 2 & 1 & 2 & 3 & 2 & 3 & 0 \end{pmatrix}.$$

2.2.4 Theorem (Rosenberg [37], [39]) *The coatoms of $\mathbf{P}_k$ are exactly those clones of the form $\text{Pol } \rho$, where ρ is a member of one of $R_1, \dots, R_6$:*

R_1 : *Partial orders on $\llbracket k \rrbracket$ with a least and greatest element.*

R_2 : *Relations $\{(x, \sigma x) : x \in \llbracket k \rrbracket\}$ where $\sigma \in S_k$ is a product of cycles of equal, prime length.*

R_3 : *Relations $\{(x_0, \dots, x_3) \in \llbracket k \rrbracket^4 : a_0 + a_1 = a_2 + a_3\}$, where $\langle \llbracket k \rrbracket; + \rangle$ is a p -elementary abelian group.*

R_4 : *Non-trivial equivalence relations on $\llbracket k \rrbracket$.*

R_5 : *Non-diagonal central relations on $\llbracket k \rrbracket$.*

R_6 : *Non-diagonal h -universal relations on $\llbracket k \rrbracket$.*

Consequently, a set of functions S is complete in $\mathcal{P}_k$ if, for every $\rho \in R_1, \dots, R_6$, there exists an $f \in S$ not preserving ρ . While there exist some relations ρ and ρ' in the list above for which $\rho \cong \rho'$, one can account for all such duplications to obtain a list of relations in one-to-one correspondence with the coatoms of $\mathbf{P}_k$. [36]

2.3 Counting clones

In the previous chapter, we saw that $\mathcal{L}(\mathcal{P}_2)$ is countable, and that its elements can be described explicitly. However, Janov and Mučnik [22] laid to rest any hopes that a similar analysis could be

carried out for $\mathcal{L}(\mathcal{P}_k)$ for $k > 2$ by showing that $|\mathcal{L}(\mathcal{P}_k)| = 2^{\aleph_0}$. That is, $\mathbf{P}_k$ contains as many clones as it does subsets. It thus became apparent that qualitative differences distinguished $\mathcal{L}(\mathcal{P}_2)$ from the lattices $\mathcal{L}(\mathcal{P}_k)$ for $k > 2$. Subsequent work has looked for properties shared by the lattices for $k > 2$, and has more fully shown the extent to which those lattices differ from $\mathcal{L}(\mathcal{P}_2)$.

Let us begin with an example of an uncountable family of clones. Let $k \geq 4$, and for $n \geq 1$, define the function $f_n \in \mathbf{P}_k^{(n)}$ by

$$f_n(\mathbf{x}) = \begin{cases} 1 & \text{if } (x_0, x_1, \dots, x_{n-1}) \text{ contains } n-1 \text{ 2's and one 3,} \\ 0 & \text{otherwise.} \end{cases}$$

These functions have the property that the composition of any two of them is the constant $\mathbf{0}$, which makes it easy to establish that:

2.3.1 Proposition *For a set $S \subseteq \{f_1, f_2, \dots\}$, we have*

$$[S] \cap \{f_1, f_2, \dots\} = S.$$

Consequently, each subset of $\{f_1, f_2, \dots\}$ generates a distinct clone. Therefore there are $2^{\aleph_0}$ clones contained in $[\{f_1, f_2, \dots\}]$. We note in passing that this also shows that the Boolean lattice $\langle \llbracket 2 \rrbracket^{\mathbf{N}}; \vee, \wedge \rangle$, the lattice of subsets of a countable set, can be (order) embedded in the lattice $\mathcal{L}(\mathcal{P}_k)$ when $k \geq 4$: another tribute to its structural complexity.

We have seen that some regions of the lattice remain similar in character for $k = 2$ and $k > 2$. Recall from Section 2.1 that the interval $[U, \mathbf{P}_2]$ is the three-element chain $U < L_1 < \mathbf{P}_2$, and that Burle's Theorem (2.2.2) shows that the interval $[U, \mathbf{P}_k]$ is a finite chain as well for $k \geq 3$. It is natural to wonder if this analogy extends any further. For example, note that the interval $[O_8, \mathbf{P}_2]$ has seven elements. Since $O_8 = \text{Con}_P(2)$, one might ask whether or not $[\text{Con}_P(k), \mathbf{P}_k]$ is finite in general: one asks, that is, how many clones contain all constant functions. The answer is negative, though; an argument of Ágoston, Demetrovics, and Hannák [1] shows that $[\text{Con}_P(k), \mathbf{P}_k]$ is uncountable for values $k > 2$. In fact, one may readily construct a (countably) infinite family of clones containing $\llbracket k \rrbracket$ as follows. (I. A. Mal'cev, [27])

We define the function $\phi : \llbracket k \rrbracket \rightarrow \mathbf{Z}_2$ by

$$\phi(x) = \begin{cases} 0 & \text{if } x \in \{0, 1\}; \\ 1 & \text{otherwise,} \end{cases}$$

and define $\psi : \mathbf{Z}_2 \rightarrow \llbracket k \rrbracket$ by $\psi(0) = 0$, $\psi(1) = 1$. Then for each $n \in \mathbf{N}$, let

$$f_n(x_0, x_1, \dots, x_{n-1}) = \psi\left(\sum_{i \in \llbracket n \rrbracket} \phi(x_i)\right).$$

Let $F_n = [\{f_n\} \cup \llbracket k \rrbracket]$. It is not hard to see that $o_e(f) \leq n$ for all $f \in F_n$; consequently, the containment $F_i \subset F_{i+1}$ is proper for each $i \in \mathbf{N}$. I. A. Mal'cev [27] established that $|\llbracket \mathbf{J}_k, L_2 \rrbracket| = \aleph_0$, ($k \geq 3$), where L_2 is the quasilinear clone. He also showed that one encounters an uncountable interval by increasing L_2 to U_2 : $|\llbracket \mathbf{J}_k, U_2 \rrbracket| = 2^{\aleph_0}$. (See Proposition 2.3.1)

If $\{f_1, f_2, \dots\}$ is an independent subset of $\mathbf{P}_k$, then the $2^{\aleph_0}$ clones generated by each of its subsets are distinct, as in the example at the beginning of this section. Furthermore, a set of functions is independent iff there exist relations $\delta_1, \delta_2, \dots$ for which $f_i \in \text{Pol } \delta_j \Leftrightarrow i \neq j$. Demetrovics and Hannák [12] used this observation in the construction of several independent sets in order to prove

2.3.2 Theorem *Let K be a coatom of $\mathbf{P}_k$ for some $k \geq 3$. Then*

$$|\llbracket \mathbf{J}_k, K \rrbracket| = \begin{cases} \text{finite} & \text{if } \text{Inv } K \text{ is of type } R_3 \text{ in Th. 2.2.4 and } k \text{ is prime,} \\ \aleph_0 & \text{if } \text{Inv } K \text{ is of type } R_3 \text{ and } k \text{ is not prime,} \\ 2^{\aleph_0} & \text{otherwise.} \end{cases}$$

Finally, we say that $F \subseteq \mathbf{P}_k$ is *complete with constants* if $[F \cup \text{Con}_P(k)] = \mathbf{P}_k$.¹ Demetrovics and Hannák [12] have also shown that when $k > 2$, there are uncountably many clones $K \leq \mathbf{P}_k$ that are complete with constants. These and other results seem to indicate that uncountable structures are ubiquitous when $k > 2$, rather than confined to some easily delimited region of the lattice.

2.4 Finitely generated clones and coclones

A noteworthy consequence of Post's analysis [34] is that one can give an explicit, finite set of generators for each two-valued clone; we saw using Proposition 2.3.1 that not all clones are finitely generated when $k \geq 3$. [14], [29]. While the finite generation property is certainly valuable in studying any clone that possesses it, it is also closely related to the question of lattice cardinality. From the knowledge that all clones of $\mathcal{P}_2$ are finitely generated, we note that the countable set $\mathbf{P}_2$

¹This is sometimes a more natural notion of completeness, within a purely algebraic context. For such a set F , the algebra $\langle \llbracket k \rrbracket; F \rangle$ is also called *functionally complete*; however, we shall avoid the use of this term.

has only countably many finite subsets, and it follows directly that $|\mathcal{L}(\mathcal{P}_2)| \leq \aleph_0$. On the other hand, a clone with an infinite basis has uncountably many subclones. In general, we have:

2.4.1 Proposition *Let $\mathcal{A}$ be an algebra, $|\mathcal{A}| \leq \aleph_0$. Then*

- (a) *If S is a sublattice of $\mathcal{L}(\mathcal{A})$ for which all subalgebras $X \in S$ are finitely generated, then $|S| \leq \aleph_0$.*
- (b) *If $[X, Y]$ is an interval, X is finitely generated, and there exists a $Z \in [X, Y]$ with an infinite basis, then $|[X, Y]| = 2^{\aleph_0}$.*
- (c) *If $[X, Y]$ is an interval for which X is finitely generated and all $Z \in [X, Y]$ have finite height over X (see page 6), then all $Z \in [X, Y]$ are finitely generated.*

Proof: We have already given some justification for the first claim. In order to prove (b), suppose that $S = \{x_1, x_2, \dots\}$ is an infinite basis. By hypothesis, there is a finite subset T of S for which $X \leq [T]$. Then for any sets U and V contained in S , if $[U] = [V]$ then $U = V$; otherwise, $[S \setminus (U \setminus V)] = [S \setminus (U \setminus V)] = [S]$ would contradict the basis property. Since there are uncountably many subsets of S containing T , $|[X, Y]| \geq |[X, [S]]| = 2^{\aleph_0}$.

To establish the last claim, we observe that if $Z \in [X, Y]$ has generators $\{x_1, \dots, x_n\}$ and Z' covers Z , then Z' is generated by $\{x_1, \dots, x_n, x_{n+1}\}$, for any element $x_{n+1} \in Z' \setminus Z$. Thus Z' too is finitely generated. When the height of any $Z \in [X, Y]$ is finite, one can proceed upwards inductively from X to show that Z is finitely generated.

In particular, the conditions of (c) are met if X is finitely generated, and $|[X, Y]| < \infty$. ■

The algebras $\mathcal{A}$ of interest here are, of course, $\mathcal{P}_k$ and $\mathcal{R}_k$. For economy of expression, a clone whose image under Inv is finitely generated in $\mathcal{R}_k$ will be called *relationally finitely generated (rfg)*, in contrast to a *functionally finitely generated (ffg)* clone. Applied to $\mathcal{P}_k$, the third claim above states that all members of a finite interval are ffg (rfg) if the bottom (top) of the interval is also ffg (or rfg, respectively). By taking the unions of the appropriate bases, one may also observe that if $K, K' \leq \mathcal{P}_k$ are ffg, so is $K \vee K'$. If K, K' are rfg, then so is $K \wedge K'$. Unfortunately, though, the finitely generated subalgebras do not, in general, form a sublattice: for example, Haddad [17] has shown there exist ffg clones $K, K' \leq \mathcal{P}_3$ for which $K \wedge K'$ is not ffg.

The finite generation property is equivalent to a lattice condition. It is well known that

2.4.2 Proposition *A subalgebra X of $\mathcal{A}$ is finitely generated if and only if it is coatomic in $\mathcal{L}(\mathcal{A})$.*

That is, X is finitely generated if and only if, for every $Z < X$, there exists a coatom Y of X such that $Z \leq Y < X$. Another equivalent condition is given by noting that X is coatomic iff the union of any ascending chain in X is properly contained in X . For example, the structure of the lattice $\mathcal{L}(\mathcal{R}_2)$ (Figure 2.2) reveals that the coclones $\text{Inv } F_i^\infty$, $1 \leq i \leq 8$, are not finitely generated, since they are each the limit of an infinite, ascending chain, and hence are not contained in any coatom. $\mathcal{P}_2$, then, provides clones which are simultaneously ffg and rfg, or ffg and not rfg. One can also account for the remaining two combinations: Demetrovics and A. I. Mal'cev [13] have exhibited a clone which is rfg but not ffg for $k \geq 3$, and the cardinality properties of Proposition 2.4.1 guarantee the existence of uncountably many clones of the fourth type; Pöschel and Kalužnin [33] construct an example.

2.4.3 Definition For any $F \leq \mathbf{P}_k$, let the *order* of F be

$$o(F) = \min_{[S]=F} \max_{f \in S} \{o(f)\},$$

setting $o(F) = \infty$ if none of the maxima exist. Define $o(Q)$ for any $Q \leq \mathbf{R}_k$ analogously. For $F \leq \mathbf{P}_k$, also let

$$d(F) = o(\text{Inv } F),$$

called the *degree* of F . We note that $o(F) < \infty$ iff F is ffg, and $d(F) < \infty$ iff F is rfg.

An elegant use of the Galois Correspondence furnishes a refinement of Proposition 2.4.2 for the algebras $\mathcal{P}_k$ and $\mathcal{R}_k$.

2.4.4 Lemma *Let $f \in \mathbf{P}_k$ and $\rho \in \mathbf{R}_k$ be given with $f \notin \text{Pol } \rho$.*

- (a) *There exists a relation σ for which $f \notin \text{Pol } \sigma$, $\rho \vdash_\Delta \sigma$, and $o(\sigma) \leq k^{o(f)}$.*
- (b) *There exists a function g for which $g \notin \text{Pol } \rho$, $f \vdash_\Delta g$, and $o(g) \leq k^{o(\rho)} - 1$.*

Proof: We prove (b). Set $h = o(\rho)$; if $o(f) \leq k^h - 1$, we are done. Otherwise, observe that ρ is not trivial, since $f \notin \text{Pol } \rho$; therefore, $|\rho| \leq k^h - 1$. Let $A \prec \rho$ be such that $f(A) \notin \rho$. Clearly A contains at most $|\rho|$ distinct columns: let A' consist of those columns in order of appearance. Let ϵ be the equivalence relation on $\llbracket o(f) \rrbracket$ induced by equality amongst the columns of A , and let $g = \Delta_\epsilon f$. Since ϵ has at most $|\rho|$ equivalence classes,

$$\begin{aligned} o(g) &\leq |\rho| \\ &\leq k^h - 1, \end{aligned}$$

and $g(A') = f(A) \notin \rho$. Therefore $g \notin \text{Pol } \rho$. ■

The following consequence refines the generic observation made in Proposition 2.4.2: we refer to Jablonskiĭ [21] or Pöschel and Kalužnin [33].

2.4.5 Proposition *$K \leq \mathbf{P}_k$ is ffg if and only if K is coatomic and has finitely many coatoms. K is rfg if and only if K is atomic and has finitely many atoms.*

Proof: Omitted. ■

Another interesting consequence is noted by Salomaa [40] and others. A basis $S \subseteq \mathbf{P}_k$ for a clone K is said to be *simple* if, for every $f \in S$ and $0 \leq i < j < o(f)$,

$$[S \cup \{\Delta_{ij} f\} \setminus \{f\}] \subset K.$$

That is, a simple basis is one which is minimal with respect to diagonalization. It is clear that one can obtain a simple basis from any basis for K by diagonalizing its elements appropriately.

2.4.6 Proposition *If $K \leq \mathbf{P}_k$ is ffg, there exist only finitely many simple bases for K .*

Proof: Let K be finitely generated; then K has coatoms $K_1, \dots, K_n$ for some finite n , by Proposition 2.4.5. For each $1 \leq i \leq n$, choose a relation $\rho_i \in \text{Inv } K_i \setminus \text{Inv } K$. Now let S be a simple basis for K . By virtue of generating K , it contains a function $f_i \in S \setminus K_i$, for each $i \leq n$; that is, $f_i \notin \text{Pol } \rho_i$. Since S is a basis, $S = \{f_i\}_{i=1}^n$, although the functions f_i need not all be distinct.

By Lemma 2.4.4(b), there exist functions $g_i \notin \text{Pol } \rho_i$ for which $f_i \vdash_\Delta g_i$ and $o(g_i) \leq k^{o(\rho_i)} - 1$. Since $g_i \in K \setminus K_i$, the set $\{g_i\}_{i=1}^n$ also generates K . Because S is simple, we must have $g_i = f_i$ for each i .

Now let $h = \max\{o(\rho_i) : 1 \leq i \leq n\}$. We have $o(f_i) = o(g_i) \leq k^h - 1$ for each i . Since h depends only on K , we have shown that the arities of functions comprising a simple basis are bounded; therefore, there are finitely many simple bases. ■

The complementary theorem for $\mathcal{R}_k$ is also true. As a final application of Lemma 2.4.4, we include a result from Pöschel and Kalužnin [33]. A clone $K \leq \mathbf{P}_k$ is said to have the *expansion property* Δh if

$$f \in K \quad \Leftrightarrow \quad \forall g : f \vdash_{\Delta} g, \text{ and } o(g) \leq h \Rightarrow g \in K. \quad (2.5)$$

2.4.7 Proposition *Let $K \leq \mathbf{P}_k$. Then for $h \in \mathbf{N}$,*

(a) *If K has the expansion property Δh , then $d(K) \leq k^h$.*

(b) *If $d(K) \leq h$, K has the expansion property $\Delta(k^h - 1)$.*

By way of illustration, consider the clone $F = \bigcup_{i=1}^{\infty} F_i$ when $k = 3$, from the example on page 28. If a function $f \in \mathbf{P}_3^{(n)}$ is not a member of F , then it is not difficult to see that there must be three vectors $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \llbracket 3 \rrbracket^n$ for which $f(\mathbf{x}), f(\mathbf{y})$, and $f(\mathbf{z})$ bear witness to this fact. Since there are at most 3^3 distinct triples (x_i, y_i, z_i) , there must be some function g also for which $g \notin F$, and $f \vdash_{\Delta} g$, and $o(g) \leq 3^3$, by identifying any components with repeated triples. This means that F has the expansion property $\Delta 27$, so $d(F) \leq 3^{27}$. We saw, though, that $o(F) = \infty$; therefore, F is rfg, but not ffg.

To provide another example, we recall the comment on page 22 that a function was in the clone F_8^{∞} if and only if the family of sets S_f had $\bigcap S_f \neq \emptyset$. For any h -ary function $f \in F_8^{\infty}$, if $A \in S_f$, we have $A \subseteq \llbracket h \rrbracket$. Let $T = S_f \cup \{\{h\}\}$, adding on a singleton subset of $\llbracket h+1 \rrbracket$ so that $\bigcap T = \emptyset$. Let f_h be the $h+1$ -ary function associated with T . Now $f_h \notin F_8^{\infty}$, but for any $g \neq f_h$ for which $f_h \vdash_{\Delta} g$, we have $S_g \subseteq S_f$, whence $\bigcap S_g \neq \emptyset$, and so $g \in F_8^{\infty}$. Therefore F_8^{∞} does not have the property Δh , for any h . By the proposition above, F_8^{∞} is not rfg.

The corresponding proposition for $\mathcal{R}_k$ also holds if we define the expansion property for coclones in the same way, replacing functions and clones with relations and coclones in expression (2.5).

2.4.8 Proposition *Let $Q \leq \mathbf{R}_k$. Then for $h \in \mathbf{N}$,*

- (a) *If Q is Δh , then $o(\text{Pol } Q) \leq (k^h - 1)$.*
- (b) *If $o(\text{Pol } Q) \leq h$, then Q is Δk^h .*

Proof: We prove only (a). Let $Q \leq \mathbf{R}_k$ be given with the property Δh . In order to show that $o(\text{Pol } Q) \leq k^h - 1$, we show $Q = \text{Inv } (\text{Pol } Q)^{(k^h-1)}$. The containment “ $\subseteq$ ” is clear by the antiisotone property of Inv . To establish the other inclusion, pick $\rho \notin Q$. We assume that $o(\rho) \geq h$. By the contrapositive of the expansion property, there exists a relation $\sigma \notin Q$ for which $o(\sigma) = h$ and $\rho \vdash_{\Delta} \sigma$. Let $f \in \text{Pol } Q$ be a function not preserving σ . By Lemma 2.4.4, there also exists a g for which $f \vdash_{\Delta} g$ and $g \notin \text{Pol } \sigma$ with $g \in (\text{Pol } Q)^{(k^h-1)}$. Since $g \notin \text{Pol } \sigma$, it does not preserve ρ either, from which it follows that $\rho \notin \text{Inv } (\text{Pol } Q)^{(k^h-1)}$. ■

Chapter 3

Two Intervals in $\mathcal{L}(\mathcal{P}_k)$

Figure 3.3: $[\Omega_2, \mathbf{P}_2]$

3.1 Clones over Ω_k

From Post's catalog [34], we see that the interval $[\Omega_2, \mathbf{P}_2]$ consists of seven classes, arranged as shown in Figure 3.3. (Recall that S_6 is the clone generated by vel and the constants, and P_6 is its dual. M_1 is the class of all monotone functions.)

This section gives a description of the interval $[\Omega_k, \mathbf{P}_k]$ for $k \geq 3$, which is equivalent to the task of determining all clones containing Ω_k . The description reveals that the interval shares the finiteness of $[\Omega_2, \mathbf{P}_2]$ for all (finite) values of k .

A result due to Jablonskiĭ [21] gives from the outset some evidence of similarity between $[U, \mathbf{P}_k]$ and $[\Omega_k, \mathbf{P}_k]$. He shows that Ω_2 shares with U the Słupecki Criterion property, in that $[\Omega_k \cup \{f\}] = \mathbf{P}_k$ when $f \notin U$ is surjective or, equivalently, that the only coatom above Ω_k is U_{k-1} . Although the interval $[\mathbf{J}_k, U_{k-1}]$ is uncountable (see Section 2.3), this condition considerably simplifies the search for members of $[\Omega_k, \mathbf{P}_k]$.

Our theorem states that the interval is lattice-isomorphic to the product of a chain of length k and lattice of subgroups of the symmetric group, S_k . For a fixed value of $k \geq 3$, let us define the clone $W_i = V_i \vee \Omega_k$ for $1 \leq i \leq k$. Note that $W_1 = \Omega_k$, and $W_k = \mathbf{P}_k$. We find that the interval $[W_1, W_{k-1}]$ has the same structure as $[U, \mathbf{P}_k]$ (as given in Burle's Theorem, 2.2.2).

3.1.1 Theorem

(a) $[\Omega_k, \mathbf{P}_k] \cong ([W_1, W_{k-1}] \times [\mathbf{J}_k, S_k]) \cdot \{W_k\}$, and

(b) $[W_1, W_{k-1}] = \{W_1, L_2 \vee W_1, W_2, \dots, W_{k-1}\}$.

Part (b) is a special case of a result due to I. A. Mal'cev [25]; however, we shall include a complete proof here in an attempt to illuminate the mechanism of not only this theorem, but also those of Burle and Shupecki. The proof depends upon the following series of lemmata.

3.1.2 Lemma *If $f, g \in \Omega_k$, so that $|\text{rng}(f)| \leq i$ and $|\text{rng}(g)| = i$ for some $i < k$, then there exist functions $\sigma, \tau \in \Omega_k$ for which $f = \sigma g \tau$.*

More specifically, if $\text{rng}(f) \subseteq \text{rng}(g)$, then $f = g\tau$ for some $\tau \in \Omega_k$.

Proof: Let $A_i = \{j : f(j) = i\}$, for $i \in \llbracket k \rrbracket$, and choose b_i such that $g(b_i) = i$, for $i \in \text{rng}(g)$. Assume that $\text{rng}(f) \subseteq \text{rng}(g)$. The sets A_i partition $\llbracket k \rrbracket$, and if $|A_i| = 1$ for all $i \in \llbracket k \rrbracket$, it follows that f is a permutation. Therefore there must be some l for which $|A_l| > 1$. Define $\tau(x) = b_i$ for $x \in A_i$, $i \in \llbracket k \rrbracket$. Then $\tau \in \Omega_k$, since τ maps at least two elements of its domain to the value b_l . By construction, $f = g\tau$.

Now consider the case when $\text{rng}(f) \not\subseteq \text{rng}(g)$. Since $|\text{rng}(f)| \leq |\text{rng}(g)| < k$, it is possible to choose a function $\sigma \in \Omega_k$ which maps $\text{rng}(g)$ onto $\text{rng}(f)$. We apply the argument in the paragraph above to the pair of functions f and σg to find a τ for which $f = \sigma g \tau$. ■

The following three lemmata are due to Jablonskiĭ [21]; see also [19].

3.1.3 Lemma Suppose $|\text{rng}(f)| \geq 3$, f is not essentially unary, and f depends on its first argument. Let $n = o(f)$. Then there exist $x, y \in \llbracket k \rrbracket$ and $\mathbf{u}, \mathbf{v} \in \llbracket k \rrbracket^{n-1}$ for which

$$f(x, u_1, u_2, \dots, u_{n-1}) = a,$$

$$f(y, u_1, u_2, \dots, u_{n-1}) = b,$$

$$f(x, v_1, v_2, \dots, v_{n-1}) = c,$$

for some three distinct values a, b , and c .

3.1.4 Definition For $n \geq 2$, four n -tuples in $\llbracket k \rrbracket^n$ of the form

$$(u_1, \dots, u_{i-1}, u_i, u_{i+1}, \dots, u_{j-1}, u_j, u_{j+1}, \dots, u_n),$$

$$(u_1, \dots, u_{i-1}, v_i, u_{i+1}, \dots, u_{j-1}, u_j, u_{j+1}, \dots, u_n),$$

$$(u_1, \dots, u_{i-1}, u_i, u_{i+1}, \dots, u_{j-1}, v_j, u_{j+1}, \dots, u_n),$$

$$(u_1, \dots, u_{i-1}, v_i, u_{i+1}, \dots, u_{j-1}, v_j, u_{j+1}, \dots, u_n),$$

for which $i < j$, $u_i \neq v_i$, and $u_j \neq v_j$, shall be called a *quadrate*.

3.1.5 Lemma Suppose $|\text{rng}(f)| \geq 3$, and $o_e(f) > 1$. Let $n = o(f)$. Then there exists a value in the range of f which f assumes on exactly one member of some quadrate in $\llbracket k \rrbracket^n$.

3.1.6 Lemma (Jablonskiĭ's Climbing Lemma) For a given function f , let $n = o(f)$. For any value l , $3 \leq l \leq |\text{rng}(f)|$, if f is not essentially unary, there exist subsets $G_1, G_2, \dots, G_n \subseteq \llbracket k \rrbracket$ having the properties that $|G_i| < l$ for $1 \leq i \leq n$ and

$$|\{f(\mathbf{x}) : x_i \in G_i, 1 \leq i \leq n\}| = l. \quad (3.6)$$

Proof: Without loss of generality, suppose that f depends on its first argument. By Lemma 3.1.3, there exist $x, y \in \llbracket k \rrbracket$ and $\mathbf{u}, \mathbf{v} \in \llbracket k \rrbracket^{n-1}$ for which f assumes three distinct values on the n -tuples $(x, u_1, \dots, u_{n-1})$, $(y, u_1, \dots, u_{n-1})$, and $(x, v_1, \dots, v_{n-1})$. Let $\mathbf{w}^i \in \llbracket k \rrbracket^n$, for $1 \leq i \leq l-3$, be arbitrary n -tuples on which f assumes some remaining $l-3$ values of its range.

Then we let

$$\begin{aligned} G_1 &= \{x, y, w_1^1, w_1^2, \dots, w_1^{l-3}\}, \\ G_2 &= \{u_1, v_1, w_2^1, w_2^2, \dots, w_2^{l-3}\}, \\ G_3 &= \{u_2, v_2, w_3^1, w_3^2, \dots, w_3^{l-3}\}, \\ &\vdots \\ G_n &= \{u_{n-1}, v_{n-1}, w_n^1, w_n^2, \dots, w_n^{l-3}\} \end{aligned}$$

By construction, the requirement 3.6 is satisfied. We see also that $|G_i| \leq l - 1$ for each $1 \leq i \leq n$, which completes the proof. ■

We may now prove Theorem 3.1.1.

Proof: Let us begin with part (b). It is clear that $W_1 \subset L_2 \vee W_1 \subset W_2 \subset \dots \subset W_{k-1}$. To show that each containment is, in fact, a covering relation, suppose that $W_1 \subset K \subseteq W_k$ for some clone K . First, suppose $K \subseteq L_2 \vee W_1$. For any $f \in K \setminus W_1$, then, f is quasilinear, so there exist $\phi_i : \llbracket k \rrbracket \rightarrow \mathbf{Z}_2$ for $i \in \llbracket n \rrbracket$, and $\psi : \mathbf{Z}_2 \rightarrow \llbracket k \rrbracket$ for which

$$f(x_0, x_1, \dots, x_{n-1}) = \psi\left(\sum_{i \in \llbracket n \rrbracket} \phi_i(x_i)\right).$$

Since $f \notin W_1$, f depends on at least two variables, so at least two of the functions $\{\phi_i\}$ are onto. Without loss of generality, assume that ϕ_0 and ϕ_1 are onto. Since the constant functions are contained in W_1 , $W_1 \cup \{f\} \vdash f'(x, y)$, where $f'(x, y) = f(x, y, 0, 0, \dots, 0)$. Then $f'(x, y) = \psi'(\phi_0(x) + \phi_1(y))$, for some map ψ' . Using Lemma 3.1.2, we see that $W_1 \cup \{f'\} \vdash g(x, y)$, where $g(x, y) = \iota(\phi(x) + \phi(y))$, $\iota(0) = 0$, $\iota(1) = 1$, and

$$\phi(x) = \begin{cases} 0 & x = 0 \\ 1 & x > 0. \end{cases}$$

By composing g with itself $m - 2$ times, one obtains the m -ary function

$$g_m(x_0, x_1, \dots, x_{m-1}) = \iota(\phi(x_0) + \phi(x_1) + \dots + \phi(x_{m-1})).$$

We then make use of Lemma 3.1.2 once again: for any function $h \in L_2^{(m)}$, there exist functions $\sigma \in \Omega_k$ and $\tau_i \in \Omega_k$ for $i \in \llbracket m \rrbracket$ for which

$$h(x_0, x_1, \dots, x_{m-1}) = \sigma g_m(\tau_0 x_0, \tau_1 x_1, \dots, \tau_{m-1} x_{m-1}).$$

Then $W_1 \cup \{g\} \vdash h$ for any $h \in L_2$, which means that $K = K \vee W_1 = L_2 \vee W_1$.

To establish the next covering relation, suppose $K \subseteq W_2$ and $K \not\subseteq L_2 \vee W_1$. For a function $f \in K \setminus (L_2 \vee W_1)$, assume without loss of generality that $\text{rng}(f) = \llbracket 2 \rrbracket$. Let n be the arity of f , and for $\mathbf{u} = (u_1, \dots, u_{n-1})$, set

$$A_{i,\mathbf{u}} = \{x : f(u_1, \dots, u_{i-1}, x, u_i, u_{i+1}, \dots, u_{n-1}) = 0\}.$$

We observe that $f \in L_2$ if, for any $0 < i \leq n$ and $\mathbf{u}, \mathbf{v} \in \llbracket k \rrbracket^{n-1}$, either $A_{i,\mathbf{u}} = A_{i,\mathbf{v}}$ or $A_{i,\mathbf{u}} = \llbracket k \rrbracket \setminus A_{i,\mathbf{v}}$.

Since $f \notin L_2$, there must be some i , $\mathbf{u}$, and $\mathbf{v}$ for which this property does not hold. That is, $A_{i,\mathbf{u}} \triangle A_{i,\mathbf{v}} \notin \{\emptyset, \llbracket k \rrbracket\}$. Either $A_{i,\mathbf{u}} \not\subseteq A_{i,\mathbf{v}}$ or $A_{i,\mathbf{v}} \not\subseteq A_{i,\mathbf{u}}$; fix the notation so that $A_{i,\mathbf{u}} \not\subseteq A_{i,\mathbf{v}}$. Then there exist elements $a \in \llbracket k \rrbracket \setminus (A_{i,\mathbf{u}} \triangle A_{i,\mathbf{v}})$ and $b \in A_{i,\mathbf{u}} \setminus A_{i,\mathbf{v}}$. Define the functions $\phi_j \in \Omega_k$, for $0 < j \leq n-1$, by

$$\phi_j(x) = \begin{cases} u_j & \text{if } x = 0, \\ v_j & \text{otherwise.} \end{cases}$$

Let $\phi \in \Omega_k$ be the analogous function mapping $0 \mapsto a$ and $\{1, 2, \dots, k-1\} \mapsto b$; then we may form the binary function

$$f'(x, y) = f(\phi_1(y), \dots, \phi_{i-1}(y), \phi(x), \phi_i(y), \dots, \phi_{n-1}(y)).$$

Now if $a \in A_{i,\mathbf{u}} \cap A_{i,\mathbf{v}}$, we see that $f'(x, y) = 1$ when $x \geq 1$ and $y \geq 1$, and $f'(x, y) = 0$ otherwise; f' restricted to the domain $\llbracket 2 \rrbracket$ realizes the Boolean conjunction (et). The other case to consider is $a \in \llbracket k \rrbracket \setminus (A_{i,\mathbf{u}} \cup A_{i,\mathbf{v}})$. Here, $f'(x, y) = 0$ only if $x = 1$ and $y = 0$; otherwise, $f'(x, y) = 1$. In this case, f' realizes the Boolean “implication” ($\rightarrow$). Choose a function $\sigma \in \Omega_k$ that transposes the elements $\{0, 1\}$, and thereby realizes the neg function on the domain $\llbracket 2 \rrbracket$. Either pair of functions $\{\text{et}, \text{neg}\}$ or $\{\rightarrow, \text{neg}\}$ is complete in $\mathcal{P}_2$; therefore $W_1 \cup \{f'\} \vdash \text{et}$, vel. It follows that $W_1 \cup \{f'\} \vdash g$ for any g with $\text{rng}(g) = \llbracket 2 \rrbracket$, by expressing g in the generalized disjunctive normal form (see page 4). Consequently,

$$W_2 \subseteq [W_1 \cup \{f'\}] \subseteq W_1 \vee K,$$

and $K = W_2$.

Finally, we show that if $l > 2$ and $W_{l-1} \subset K \subseteq W_l$, then $K = W_l$, again by selecting any function $f \in K \setminus W_{l-1}$. The cardinality of the range of f is exactly l , and f is not unary; therefore Lemma 3.1.6 shows the existence of sets G_i for $1 \leq i \leq n$ that satisfy the equation (3.6), and for which

$$|G_i| \leq l - 1 \quad (3.7)$$

We assume once again, without loss of generality, that $\text{rng}(f) = \llbracket l \rrbracket$, and we let g be any other function for which $\text{rng}(g) = \llbracket l \rrbracket$ as well. For each i , $1 \leq i \leq l$, choose an n -tuple $\mathbf{u}^i$ for which $\mathbf{u}_j^i \in G_j$ and $f(\mathbf{u}^i) = i$. For each $1 \leq j \leq n$, let $g_j \in \mathbf{P}_k^{(n)}$ be the function defined by $g_j(\mathbf{x}) = \mathbf{u}_j^i$ if $g(\mathbf{x}) = i$. In fact, $g_j \in W_{l-1}$, by (3.7), so $W_{l-1} \cup \{f\} \vdash f(g_1, g_2, \dots, g_n)$. However, that composition is exactly the function g , so $g \in [W_{l-1} \cup \{f\}]$. By virtue of Lemma 3.1.2, for any $h \in W_l$, there exists $\sigma \in W_1$ such that $h = \sigma g$. Therefore $W_l \subseteq [W_{l-1} \cup \{f\}] \subseteq K$, from which it follows that $K = W_l$.

The proof of part (a) is now straightforward. Define the function $\Psi : [W_1, W_{k-1}] \times [E, S_k] \rightarrow [W_1, U_{k-1}]$ by $\Psi(X, Y) = X \vee Y$. To establish that Ψ is an injection, suppose that $\Psi(X, Y) = \Psi(X', Y')$. Observe that $(X \vee Y) \wedge S_k = Y$, since $X \wedge S_k = [\emptyset] = \mathbf{J}_k$, and a composition of functions $f * g$ is in S_k iff both f and g are in S_k . It follows that

$$\begin{aligned} (X \vee Y) \wedge S_k &= (X \cup Y) \wedge S_k \\ &= (X \wedge S_k) \cup (Y \wedge S_k) \\ &= \mathbf{J}_k \cup Y \\ &= Y. \end{aligned}$$

Thus $\Psi(X, Y) = \Psi(X', Y')$ implies

$$\Psi(X, Y) \wedge S_k = \Psi(X', Y') \wedge S_k,$$

from which $Y = Y'$. Now recall that $U_i = W_i \vee S_k$. It is easy to see that the set inclusions $U_1 \subset L_2 \vee U_1 \subset U_2 \subset \dots \subset U_{k-1}$ are all strict. It follows that the inclusions

$$W_1 \vee Y \subset L_2 \vee W_1 \vee Y \subset W_2 \vee Y \subset \dots \subset W_{k-1} \vee Y$$

are also strict, and $\Psi(X, Y) = \Psi(X', Y) \Rightarrow X = X'$, as required.

One establishes that Ψ is surjective by projecting any clone in $[W_1, W_k)$ onto the interval's factors. Given a clone F for which $W_1 \leq F < W_k$, let $Y = F \wedge S_k$, and let $X = F \wedge W_{k-1}$. Then clearly $F = X \vee Y$, and Ψ is an isomorphism. Furthermore, it follows from the Stupecki Criterion (Theorem 2.2.1) that W_k covers $W_{k-1} \vee S_k$. ■

Figure 3.4: $[\Omega_3, \mathbf{P}_3]$

The statement of Theorem 3.1.1 is illustrated for $[\Omega_3, \mathbf{P}_3]$ in Figure 3.4. The symmetric group S_3 has four proper, nontrivial subgroups. The subgroups of order two are all indicated by C_2 for the sake of simplicity. The interval contains nineteen clones in all. A corollary of the theorem is that the number of clones containing Ω_k equals $k|[\mathbf{J}_k, S_k]| + 1$, where $|[\mathbf{J}_k, S_k]|$ is the number of subgroups of the symmetric group S_k .

Figure 3.5: $[S_2, \mathbf{P}_2]$

3.2 Clones over S_k

The unary functions are partitioned into permutations and non-permutations: that is, $U = \Omega_k \cup S_k$, and $\Omega_k \cap S_k = \mathbf{J}_k$. We now turn our attention to the interval of clones containing S_k . When $k = 2$, they consist of the six shown in Figure 3.5 (Post [34]). When $k > 2$, one can determine the structure of $[S_k, \mathbf{P}_k]$ using a method similar to that of the previous section, although the outcome here is a somewhat more involved description. One begins by characterizing the unary clones in the interval, then extending the characterization to the entire interval. The result depends on whether k is even or odd, and the cases in which $k = 3$ and $k = 4$ will need to be treated separately.

During the preparation of this thesis, it was observed that Haddad and Rosenberg [18] have shown that $[S_k, \mathbf{P}_k]$ is finite by determining its elements, for $k \geq 5$, using an argument similar to the one presented here. We differ, however, by determining the explicit structure of the interval, and resolving the special cases encountered when $k = 3$ or 4 .

Recall from the previous section that, when $k \geq 3$, the only coatom containing Ω_k is U_{k-1} . Salomaa [41] has shown that the same is true of S_k when k is large enough ($k \geq 5$). Once again, one is led to expect some similarity with the interval $[U, \mathbf{P}_k]$.

3.2.1 Theorem (Salomaa [41]) *If $k \geq 5$, $|\text{rng}(f)| = k$, and $o_e(f) > 1$, then $\{\{f\} \cup S_k\} = \mathbf{P}_k$.*

3.2.2 Definition Denote the set of all partitions of k by Π_k :

$$\Pi_k = \left\{ \{a_1, a_2, \dots, a_n\} : a_i \in \mathbb{N}, \sum_{i=1}^n a_i = k, \text{ for some } n \in \mathbb{N} \right\}.$$

Each partition is regarded as a multiset: elements may occur more than once, and order is neglected. Given a function $f \in \mathbf{P}_k^{(1)}$, let $B_i = \{j : f(j) = i\}$, for $i \in \llbracket k \rrbracket$. Let $I = \{i : B_i \neq \emptyset\}$. Define $\Pi(f) = \{|B_i|\}_{i \in I}$, and observe that $\Pi(f)$ is a partition of k . In order to name to the set of functions that give rise to a particular partition $A \in \Pi_k$, define

$$\Omega_{k,A} = \left\{ f \in \mathbf{P}_k^{(1)} : \Pi(f) = A \right\}.$$

Furthermore, for all $F \subseteq \Pi_k$, define the clone

$$O_F = [\{\Omega_{k,A} : A \in F\}] \vee S_k.$$

The set Π_k admits a partial ordering in the usual fashion: if $A, B \in \Pi_k$, write $A \leq B$ if and only if A is a refinement of B . That is, suppose $B = \{b_1, b_2, \dots, b_n\}$. Then A is said to be a *refinement* of B if there exist sets $B_1, B_2, \dots, B_m$ which partition B , and $A = \left\{ \sum_{i \in B_j} b_i : 1 \leq j \leq m \right\}$. The minimum element of this poset is $A_0 = \{1, 1, \dots, 1\}$, while the maximum is $A_1 = \{k\}$. The set of filters $\mathcal{F}(\Pi_k)$ form a lattice whose minimum and maximum elements are $F_0 = \emptyset$, and $F_1 = \Pi_k$, respectively.

For filters $F, G \in \mathcal{F}(\Pi_k)$ and for each $1 \leq i \leq k$, define the relation $F \equiv_i G$ to hold if and only if, for all $A \in \Pi_k$ with $|A| > i$, $A \in F \Leftrightarrow A \in G$. It can be seen that $\equiv_i$ is an equivalence relation and, in fact, a congruence on the lattice $\mathcal{F}(\Pi_k)$. The intuition here is that two filters are related if they are equal on all but partitions of small cardinality. In particular, note that $F \equiv_1 G$ iff $F = G$.

We shall introduce another congruence, $\equiv_L$, which has special properties when k is even. A partition $A \in \Pi_k$ is said to be *even* if all of its elements are divisible by 2, and *odd* otherwise. A set of partitions F is called even if A is even for all $A \in F$. We define $\equiv_L$ as follows: if $F, G \in \mathcal{F}(\Pi_k)$ and either F or G is even, let $F \equiv_L G$ hold if and only if, for all partitions A for which either $|A| > 2$ or A is odd, $A \in F \Leftrightarrow A \in G$. Otherwise, let $F \equiv_L G \Leftrightarrow F \equiv_2 G$.

3.2.3 Lemma *If $f \in \Omega_{k,A}$ for some $A \in \Pi_k$, then $S_k \cup \{f\} \vdash \Omega_{k,A}$.*

Proof: For any $g \in \Omega_{k,A}$, one can find permutations $\sigma, \tau \in S_k$ for which $g = \sigma f \tau$. ■

3.2.4 Lemma *For a set $F \subseteq \Pi_k$, let $\overline{F}$ be the smallest filter in Π_k for which $F \subseteq \overline{F}$. Then if $F \neq \{A_0\}$, it is the case that $O_F = O_{\overline{F}}$.*

Proof: Suppose that $F \neq \{A_0\}$, and let $A \in \Pi_k$ be any partition for which there exists some $B \in F$, $B \neq A_0$, with $B \trianglelefteq A$. We shall prove the claim by showing that, for any $f \in \Omega_{k,A}$, $O_F \vdash f$.

It is sufficient to consider the case when A covers B . Begin by choosing any function $g \in \Omega_{k,B}$, and let $B_i = \{j : g(j) = i\}$, and $b_i = |B_i|$. Then $B = \{b_i : b_i \neq 0\}$, and $A = (B \setminus \{b_i, b_j\}) \cup \{b_i + b_j\}$, for some $i \neq j$, since A covers B . In fact, the argument shall not depend on the values of i and j , so we shall assume that they are 0 and 1, in the interests of simplicity.

Let $m = |B|$. For some $l \in \llbracket k \rrbracket$, we must have $b_l > 1$, since $B \neq A_0$. Let c_0 and c_1 be distinct members of B_l , and let $c_2, c_3, \dots, c_{m-1}$ be members of some $m-2$ of the remaining $m-1$ sets $\{B_i\}$. Now define a permutation $\sigma \in S_k$ by setting $\sigma(i) = c_i$ for $0 \leq i < m$, and choosing $\sigma(i)$ in an arbitrary, bijective manner on the remaining $k-m$ elements of its domain and range.

Defining $f' = f\sigma f$, one sees that $f'(i) = f(i)$ for $i \notin B_1$, and $f'(i) = 0$ for $i \in B_0 \cup B_1$. Therefore $\Pi(f') = A$. With the help of Lemma 3.2.3, one obtains $S_k \cup \{f'\} \vdash g$, which completes the proof. ■

3.2.5 Lemma *Let $2 \leq i \leq k$. If $F \in \mathcal{F}(\Pi_k)$ is a filter which contains all partitions A with $|A| \leq i$, then $O_F \vee V_i = O_F \cup V_i$.*

Proof: Let f be any member of $O_F \vee V_i$. If f is essentially unary, it is clear that $O_F \cup V_i^{(1)} \vdash f$. Since our choice of F implies that $V_i^{(1)} \subseteq O_F$, it follows that $f \in O_F$. Otherwise, $o_e(f) > 1$. In this case, we make use of the observation that for *any* clone $K \leq U_1$, if $g \in K \vee V_i$ and g is not essentially unary, then $|\text{rng}(g)| \leq i$. Consequently, $f \in V_i$, so $O_F \vee V_i \subseteq O_F \cup V_i$, as required. ■

The preceding three arguments shall serve to classify the unary functions found in clones containing S_k . The remaining clones — that is, those which include functions that depend on more than one variable — are determined for the most part by the cardinality of the range of each function, very much as were their analogues in the interval over Ω_k , in the previous section. The following three lemmata will provide the necessary tools to elaborate this notion precisely.

3.2.6 Lemma *Let $f \in L_2 \setminus U$. Then*

$$[S_k \cup \{f\}] = \begin{cases} L_2^e \vee S_k & \text{if } f \in L_2^e, \\ L_2 \vee S_k & \text{otherwise.} \end{cases}$$

Proof: Since $f \in L_2$, it can be written in the form of equation (2.4). It is easily determined that all of the constant functions are in $[S_k \cup \{f\}]$. By substituting constants for the variables of f , we find that the functions ϕ_i , are as well, for all i , $1 \leq i \leq n$. f is not essentially unary; assume, without loss of generality, that f depends on its first two variables. That is, ϕ_0 and ϕ_1 are not constant, and ψ is an injection. With the help of the permutations, we may assume that ψ is the inclusion map, and ignore it henceforth. Substituting constants again, one sees that $S_k \cup \{f\} \vdash f'$, where

$$f'(x, y) = \phi_0(x) + \phi_1(y).$$

Since ϕ_0 is not constant, there exist $a, b \in \llbracket k \rrbracket$ for which $\phi_0(a) = 0$ and $\phi_0(b) = 1$. For any function $\phi : \llbracket k \rrbracket \rightarrow \mathbf{Z}_2$, let $\sigma \in S_k$ be some permutation mapping $0 \mapsto a$ and $1 \mapsto b$. Then

$$f'(\sigma(\phi(x)), y) = \phi(x) + \phi_1(y),$$

which is to say that

$$S_k \cup \{f, \phi, \phi'\} \vdash \phi(x) + \phi'(y)$$

for arbitrary ϕ and ϕ' mapping $\llbracket k \rrbracket$ into $\mathbf{Z}_2$. So let $\sigma \in S_k$ be a transposition of a and b , and consider the function $\phi_0(x) + \phi_0(\sigma(y))$. Since ϕ_0 and $\phi_0\sigma$ agree on all values except $\{a, b\}$, the function $\xi(x)$ defined by identifying x and y assumes the value 1 on $\{a, b\}$, and 0 elsewhere. Therefore $\Pi(\xi) = \{2, k-2\}$.

Using a similar argument, one can use ξ to show that, for any function $\phi \in [S_k \cup f]$ with $\Pi(\phi) = \{l, k-l\}$, for $l \geq 2$, there is also a ϕ' with $\Pi(\phi') = \{l-2, k-l+2\}$. If at least one of l and $k-l$ is odd, it is not hard to see that one may obtain any function ϕ' that induces a partition of size 2, using two-place addition and permutations. If instead both are even, one generates only those functions with even partitions of size 2. The consequence is that, if $f \in L_2 \setminus L_2^e$, then $\Omega_{k,A} \subseteq [S_k \cup f]$ for all $A \in \Pi_k$, $|A| = 2$. If $f \in L_2^e$ instead, we add the restriction that A be even.

To prove the claim, let us first consider the case $f \notin L_2^e$. We show that $L_2 \subseteq [S_k \cup \{f\}]$ in the same manner as in the proof of Theorem 3.1.1: one constructs $\phi(x) + \phi(y)$, where

$$\phi(x) = \begin{cases} 0 & \text{if } x = 0 \\ 1 & \text{otherwise,} \end{cases}$$

then composes this function with itself to form a quasilinear function of arbitrary arity. One then constructs an arbitrary function in L_2 by further composition with appropriate functions $\{\phi_i\}$ and ψ , since the argument above concludes that all $S_k \cup \{f\} \vdash \phi_i$ for all $\phi_i : \llbracket k \rrbracket \rightarrow \mathbf{Z}_2$.

When $f \in L_2^e$, the argument is directly analogous. ■

The next two lemmata are drawn from the proof given by Jablonskiĭ [19] of Salomaa's theorem (3.2.1).

3.2.7 Lemma *Suppose $k > 3$, and $f \in \mathbf{P}_k \setminus U$ is a function for which $|\text{rng}(f)| = m$, for some $m \geq 3$. Then there exists a unary function $\phi \in [S_k \cup \{f\}]$ for which $2 \leq |\text{rng}(\phi)| < k$.*

Proof: Let $n = o(f)$. We shall prove the claim first for $m \geq 4$.

Lemma 3.1.6 provides sets $G_1, G_2, \dots, G_n$ for which each $|G_i| < m$ and for which also the range of f is unchanged when its domain is restricted to $\prod_{i=1}^n G_i$. If necessary, add elements to the sets $\{G_i\}$ so that $|G_i| = m - 1$ for all i . Since we are free to compose f with the permutations S_k , we shall assume that each set G_i equals $\llbracket m - 1 \rrbracket$.

Set $\mathbf{s}_0 = (m - 1, m - 1, \dots, m - 1)$, and $c = f(\mathbf{s}_0)$. We claim that there exist n -tuples $\mathbf{s}_1$ and $\mathbf{s}_2$ in $\llbracket m - 1 \rrbracket^n$ which do not equal each other in any component, and for which $f(\mathbf{s}_2) \neq f(\mathbf{s}_1) = c$:

For any $\mathbf{t} \in \llbracket m - 1 \rrbracket^n$ for which $f(\mathbf{t}) = c$, let

$$I_{\mathbf{t}} = \{\mathbf{x} \in \llbracket m - 1 \rrbracket^n : \exists i : x_i = t_i\}.$$

There are two cases to consider. First, suppose that there exists some $\mathbf{u} \in \llbracket m - 1 \rrbracket^n \setminus I_{\mathbf{t}}$ for which $f(\mathbf{u}) \neq c$. In this case, set $\mathbf{s}_1 = \mathbf{t}$, and $\mathbf{s}_2 = \mathbf{u}$.

Otherwise, for each $\mathbf{u} \in \llbracket m - 1 \rrbracket^n \setminus I_{\mathbf{t}}$, $f(\mathbf{u}) = c$. Then there must exist a $\mathbf{v} \in I_{\mathbf{t}}$ for which $f(\mathbf{v}) \neq c$. It is not hard to see, given our hypothesis $m - 1 \geq 3$, that the set $\llbracket m - 1 \rrbracket^n \setminus (I_{\mathbf{t}} \cup I_{\mathbf{v}})$ cannot be empty; let $\mathbf{w}$ be a member of it. By assumption, $f(\mathbf{w}) = c$; therefore we may set $\mathbf{s}_1 = \mathbf{w}$ and $\mathbf{s}_2 = \mathbf{v}$.

Now choose s_i arbitrarily, for $3 \leq i < k$, subject to the restriction that for each i, j and l with $0 \leq i < j < k$ and $1 \leq l \leq n$, the components s_{il} and s_{jl} are distinct. For each $1 \leq l \leq n$, define the permutation $\phi_l(i) = s_{il}$, and let

$$\phi(x) = f(\phi_1(x), \phi_2(x), \dots, \phi_n(x)). \quad (3.8)$$

Since $\phi(0) = \phi(1) = c$ and $\phi(2) \neq c$, ϕ has the desired properties.

We complete the argument by considering what happens when $m = 3$. Suppose that no ϕ in the clone has $2 \leq |\text{rng}(\phi)| < k$. m is strictly less than k ; hence every composition of the form (3.8) is a constant function. This means that, for any $s \in \llbracket k \rrbracket^n$, we have $f(t) = f(s)$ for all $t \in \llbracket k \rrbracket^n \setminus I_s$. Consider the following consequence of the definition of the sets I_x : for every $u \in \llbracket k \rrbracket^n$, either $u \notin I_s$, or there exists a $t \notin I_s$ for which $u \notin I_t$. We see that $f(u) = f(s)$ for all $u \in I_s$ as well, which makes f a constant function. However, this contradicts our hypothesis concerning the range of f . ■

3.2.8 Lemma *Suppose $k > 3$, $f \in V_m \setminus V_{m-1}$, for $3 \leq m \leq k$, excluding $m = k = 4$, and $o_e(f) > 1$. Then $S_k \cup \{f\} \vdash V_m$.*

Proof: The proof is by induction. We begin by showing that $S_k \cup \{f\} \vdash V_2$. First, we claim that $S_k \cup \{f\} \vdash \{\text{et}, \text{vel}\}$, where *et* and *vel* are the minimum and maximum functions, respectively, on the domain $\llbracket 2 \rrbracket^2$:

$[S_k \cup \{f\}]$ contains a unary function which is not a permutation; therefore it contains all constant functions, by Lemma 3.2.4. Using Lemma 3.1.5, we find a quadrate on which f assumes some value exactly once. Construct a binary function $f'(x, y)$ from f with the same property through the substitution of constants. By composing f' appropriately with permutations, we may obtain another function $g(x, y)$ for which $g(0, 0) = 0$, and $g(x, y) \neq 0$ on the remaining values in $\llbracket 2 \rrbracket^2$.

Let ϕ be the singular function constructed in the previous lemma (3.2.7). From Lemmas 3.2.3 and 3.2.4, we see that we can construct from it a function ϕ' whose range is of cardinality two. If one of the elements of $\Pi(\phi')$ equals 1, then we can construct a function ϕ'' for which $\phi''(0) = 0$ and $\phi''(x) = 1$ for $x \neq 0$. Then clearly $\phi''g$ equals the function *vel* on $\llbracket 2 \rrbracket^2$. Otherwise, both elements of $\Pi(\phi')$ are at least two. We assumed that $k - \min\{4, m\} > 0$; consequently, some value $c \in \llbracket k \rrbracket$ does

not appear in $g(\llbracket 2 \rrbracket^2)$. From ϕ' we can construct a function $\phi''(x)$ that is 0 for $x = 0$ and c , and 1 on the nonzero values of $g(\llbracket 2 \rrbracket^2)$. Then $\phi''g(0,0) = 0$, and $\phi g(x,y) = 1$ for $(x,y) \in \llbracket 2 \rrbracket^2 \setminus (0,0)$. That is, $\text{vel} = \phi''g$ once again. Since the function neg on $\llbracket 2 \rrbracket$ is simply a permutation, we can also form et by de Morgan's law.

It is clear that, from ϕ' , vel , and the permutations, one can construct any unary function on $\llbracket k \rrbracket$ of range 2. In particular, we may form the functions $d_i(x)$ defined by

$$d_i(x) = \begin{cases} k-1 & x = i \\ 0 & \text{otherwise,} \end{cases}$$

for each $i \in \llbracket k \rrbracket$. Then any function $g \in V_2$ can be expressed in terms of et , vel , and the functions d_i , by writing g in generalized disjunctive normal form (page 4).

It remains to show that if $3 \leq l \leq m$, then

$$S_k \cup V_{l-1} \cup \{f\} \vdash V_l,$$

from which our claim follows by induction. Let g be any member of V_l . By Lemma 3.1.6, there exist sets G_i for $1 \leq i \leq n$ for which $|G_i| \leq l-1$ and

$$|\{f(\mathbf{x}) : x_i \in G_i, 1 \leq i \leq n\}| = l.$$

Without loss of generality, assume that f assumes the values $\llbracket l \rrbracket$ on $\prod_{i=1}^n G_i$, and that $\text{rng}(g) = \llbracket l \rrbracket$ as well. For each i , $1 \leq i \leq l$, choose an element $\mathbf{u}^i \in \prod_{i=1}^n G_i$ for which $f(\mathbf{u}^i) = i$. For each $1 \leq j \leq n$, let g_j be the function defined by $g_j(\mathbf{x}) = u_j^i$ if $g(\mathbf{x}) = i$. The range of each g_j is contained in the set G_i , so $g_j \in V_{l-1}$. Since $f(g_1, g_2, \dots, g_n) = g$, we have shown that $S_k \cup V_{l-1} \cup \{f\} \vdash g$. ■

We are now sufficiently prepared to state and prove the results at the heart of this section.

3.2.9 Proposition *Suppose $k > 2$. The interval $[S_k, U] = [O_{F_0}, O_{F_1}] = \{O_F : F \in \mathcal{F}(\Pi_k)\}$, ordered by inclusion.*

Proof: By definition, $S_k = O_\emptyset = O_{F_0}$, and $U = O_{F_1}$. The claim follows easily from Lemmas 3.2.3 and 3.2.4: Suppose $K \in [O_{F_0}, O_{F_1}]$. For any function $f \in K \setminus S_k$, we have $S_k \cup \{f\} \vdash \Omega_{k, \Pi(f)}$. Let $F = \{\Pi(f) : f \in K \setminus S_k\}$, from which we see $K \vee S_k = O_F = O_{\overline{F}}$, where $\overline{F} \in \mathcal{F}(\Pi_k)$. That is, the

only clones in the interval $[S_k, U]$ are of the form O_F for some $F \in \mathcal{F}(\Pi_k)$. Since clearly $O_F = O_G$ if and only if $F = G$, there is, in fact, a distinct clone for each filter F . ■

The main result depends on the parity of k . To keep its statement concise, let L be the class L_2^e if k is odd, and L_2 otherwise.

3.2.10 Theorem *If $k \geq 5$, then*

$$[S_k, \mathbf{P}_k] \cong [O_{F_0}, U] \times (V_1, L, V_2, \dots, V_k) / \simeq,$$

where $(O_F, K) \simeq (O_G, K')$ if and only if

- (a) either $K = K' = V_i$ for some i , and $F \equiv_i G$, or
- (b) $K = K' = L$, and $F \equiv_L G$.

Proof: We prove the claim by defining the map

$$\Phi : [O_{F_0}, U] \times (V_1, L, V_2, \dots, V_k) \rightarrow [O_{F_0}, \mathbf{P}_k],$$

as $\Phi(X, Y) = X \vee Y$, then showing that it is surjective and has kernel exactly $\simeq$.

First, we suppose a clone K is in the interval $[O_{F_0}, \mathbf{P}_k]$, and prove that K is in the image of Φ . For each $f \in K$, if $f \in U$, then $[O_{F_0} \cup \{f\}] = O_F$, for some filter F , by the preceding proposition. Otherwise, f is not essentially unary. If $f \in L$, then $[S_k \cup \{f\}] = L$, by Lemma 3.2.6, and L is in the image of Φ . Otherwise $f \in V_i \setminus V_{i-1}$ for $i > 2$ or $f \in V_2 \setminus L$, and so by the lemma to Salomaa's theorem (3.2.8), it is the case that $[S_k \cup \{f\}] = V_i$. Since the image of Φ is closed under the join operation, it follows that K itself is in the image.

It remains to show that

$$O_F \vee Y = O_G \vee Z \tag{3.9}$$

holds if and only if $(O_F, Y) \simeq (O_G, Z)$. First, equation (3.9) implies that $Y = Z$:

Suppose $Y = L$. Then $O_F \vee Y = O_G \vee Z \subseteq L \vee U \subset U_i$, for $i > 1$. Therefore $Z \neq V_i$ for $i > 1$, and clearly $Z \neq V_1$, which leaves $Z=L$ as well.

Otherwise, $Y = V_i$ and $Z = V_j$ for some i and j . Let F' and G' be the filters obtained by augmenting F and G by all partitions of size no greater than i and j , respectively. Then $O_F \vee V_i = O_{F'} \vee V_i$, and $O_G \vee V_j = O_{G'} \vee V_j$, so $i = j$ (Lemma 3.2.5), and again $Y = Z$.

Given $Y = Z$, we show that (3.9) is equivalent to the conditions (a) and (b). First suppose that $Y = Z = V_i$, for some i , $1 \leq i \leq k$. Let F' be the smallest filter containing F and all $A \in \Pi_k$ for which $|A| \leq i$. Then

$$\begin{aligned} O_F \vee V_i &= O_{F'} \vee V_i \\ &= O_{F'} \cup V_i, \text{ (by Lemma 3.2.5)} \end{aligned}$$

and similarly for G' containing G . Therefore

$$\begin{aligned} (3.9) &\Leftrightarrow O_{F'} \cup V_i = O_{G'} \cup V_i \\ &\Leftrightarrow F' \equiv_i G'. \end{aligned}$$

Since $F \equiv_i F'$ and $G \equiv_i G'$ as well, the condition is equivalent to $F \equiv_i G$, as required.

Finally, suppose that $Y = Z = L$. It is clear that if $F \equiv_L G$, then (3.9) must hold. To show the converse, suppose first that F is not even. A filter which contains odd elements must contain odd elements of size 2. Therefore the set

$$\{\Pi(f) : f \in (O_F \vee L) \cap \Omega_k\} \quad (3.10)$$

contains all partitions of size 2, and so must the corresponding set for G . For any f with $|\Pi(f)| > 2$, certainly $f \in O_F \vee L \Leftrightarrow f \in O_F$, using Lemma 3.2.5 again, and $F \equiv_L G$.

If F is instead even, the set (3.10) contains only even partitions, and the same argument applies to show that $F \equiv_L G$.

Consequently, the kernel of Φ is $\simeq$, and the theorem is proven. ■

It remains to consider the special case of $k = 3$ or $k = 4$. For small values of k , we shall give names to specific clones O_F by listing partitions which generate F : for example, let $O_{13,22}$ denote the clone in Ω_4 for which $F = \overline{\{\{1, 3\}, \{2, 2\}\}}$.

We also need to describe two clones peculiar to $k = 3, 4$. Identify $\llbracket 3 \rrbracket$ with $GF(3)$ in some manner, and then define L_3 as those functions $f \in \mathbf{P}_3^{(n)}$ for which there exist constants $a_i \in \llbracket 3 \rrbracket$ and $c \in \llbracket 3 \rrbracket$, for $1 \leq i \leq n$, such that

$$f(x_1, \dots, x_n) = c + \sum_{i=1}^n a_i x_i.$$

Similarly, identify $\llbracket 4 \rrbracket$ with $GF(4)$, and let L_{2+2} consist of $f \in \mathbf{P}_4^{(n)}$ for which there exist $a_i, b_i \in \llbracket 4 \rrbracket$ and $c \in \llbracket 4 \rrbracket$, for $1 \leq i \leq n$, such that

$$f(x_1, \dots, x_n) = c + \sum_{i=1}^n a_i x_i + \sum_{i=1}^n b_i x_i^2.$$

It is implicit in these two definitions that one obtains the same clone no matter how one identifies the elements of $\llbracket 3 \rrbracket$ or $\llbracket 4 \rrbracket$ with those of the corresponding field. Indeed, this is equivalent to the observation that $S_3 \leq L_3$, and $S_4 \leq L_{2+2}$.

Figure 3.6: $[S_3, \mathbf{P}_3]$

3.2.11 Theorem $[S_3, \mathbf{P}_3]$ consists of the interval described for $k = 3$ in Theorem 3.2.10, with the addition of the class L_3 situated by $O_3 < L_3 < U_3$.

Proof: Let $\rho \subseteq \llbracket 3 \rrbracket^3$ be the relation consisting of all triples (a, b, c) for which either $\{a, b, c\}$ are all distinct, or all the same: it is easily shown that $\text{Pol } \rho = L_3$.

For any function $f \in U_3 \setminus U_2$, then, either there exists a unary function g in both $U \setminus O_3$ and $[S_3 \cup \{f\}]$, or there does not. If there does, then $[S_3 \cup \{g\}] = U$ (3.2.4). By the Słupecki Criterion (2.2.1), we have $[S_3 \cup \{f\}] = \mathbf{P}_3$.

Otherwise, we claim that f preserves ρ . If not, for some $A \prec \rho$ and $a \neq b \in \llbracket 3 \rrbracket$, $f(A) = (a, a, b)^t$. Clearly $[S_3 \cup \{f\}]$ contains all permutations and constant functions. Each column of A is the image of a permutation or constant function on the triple $(0, 1, 2)$; therefore, by composing f with the

appropriate permutation or constant for each column, we obtain a unary function $f' \in [S_k \cup \{f\}]$ for which $f'(0) = f'(1) = a$ and $f'(2) = b$. This is a contradiction, since $f' \in U \setminus O_3$. Consequently, $f \in L_3$. This reasoning shows that the only two coatoms of $\mathbf{P}_3$ in the interval $[S_3, \mathbf{P}_3]$ are U_2 and L_3 .

Suppose next that K is a clone in the interval $[S_3, U_2]$. If there exists a function $f \in K \setminus L_2$, then Lemma 3.2.6 implies that $K = U_2$. If not, but there exists $f \in K \setminus U$, previous arguments show that $K \supseteq L_2$, and hence $K = L_2$. Otherwise, $K \subseteq U$, and Proposition 3.2.9 shows that it must be one of $S_3 < O_3 < U$.

Finally, we observe that if $f \in L_3 \setminus U$, then the set $f \cup S_k$ generates L_3 in the same manner as for L_2 . Since L_3 contains O_3 but not U , the lattice is as shown in Figure 3.6. ■

Figure 3.7: $[S_4, \mathbf{P}_4]$

3.2.12 Theorem $[S_4, \mathbf{P}_4]$ consists of the lattice described in Theorem 3.2.10, with the addition of the clone L_{2+2} , situated between L_2^e and $\mathbf{P}_4$.

Proof: Let $\epsilon_1, \dots, \epsilon_6$ be the six equivalence relations on $\llbracket 4 \rrbracket$ with two equivalence classes of size two, and let $\sigma \in \mathbf{R}_4^{(4)}$ be the relation $\delta_{\epsilon_1} \cup \dots \cup \delta_{\epsilon_6}$. It is not hard to verify that $L_{2+2} = \text{Pol } \sigma$.

We observe that the theorem above excludes the case where $k = 4$ because of a restriction of the hypotheses of Lemma 3.2.8; specifically, it does not follow when $k = 4$ that $S_4 \cup \{f\} \vdash V_4$ whenever $f \in V_4 \setminus V_3$. Instead, we show that, for such an f , either $S_4 \cup \{f\} \vdash V_4$, or f preserves the relation σ .

Suppose that $f \in V_4 \setminus (V_3 \cup U)$ does not preserve σ . We claim, then, that $S_4 \cup \{f\} \vdash V_4$. By hypothesis, there exists $A \prec \sigma$ for which $f(A) = (a, b, c, d)^t$, where $a \notin \{b, c, d\}$, and $|\{b, c, d\}| < 3$. (σ is row-symmetric, so we may reorder the rows of A according to taste.) In fact, it is sufficient to consider the case where $b = c = d$ (Lemma 3.2.4). Since σ is symmetric in $\llbracket 4 \rrbracket$, we shall also assume that $a = 1$ and $b = c = d = 0$.

Now each column of A contains either 1, 2, or 4 distinct elements. Let A_1, A_2 , and A_4 be submatrices of A consisting of the columns of each respective number of elements. We permute the components of f to obtain a function f' for which $f'(A_1|A_2|A_4) = f(A) = (1, 0, 0, 0)^t$. $[S_4 \cup \{f\}]$ contains the constant functions: see Lemma 3.2.7. Construct a function f'' by substitution for which $f''(A_2|A_4) = f(A)$.

f is not essentially unary, and its range is $\llbracket 4 \rrbracket$, so Lemma 3.1.5 asserts that there exists a quadrate on which f assumes some value exactly once. In fact, f assumes each value of its range on this quadrate: otherwise the argument used to prove Lemma 3.2.8 would hold for f as well, and $S_4 \cup \{f\} \vdash V_4$. Composing f with the appropriate permutations and identifying variables yields the following function g :

$\mathbf{x}$	$g(\mathbf{x})$
00	0
01	1
10	2
11	3

Using such a g , we can parameterize f'' in such a way as to replace the columns A_4 by columns that consist each of only two distinct values. We shall also use permutations to replace the columns A_2 by columns consisting only of $\{0, 1\}$. We obtain some function $h \in [S_4 \cup \{f''\}]$ for which

$h(B) = f''(A_2|A_4) = f(A) = (1, 0, 0, 0)^t$, where

$$B = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}.$$

From this it is clear that h , restricted to the domain $\llbracket 2 \rrbracket$, is not linear. That is, $h|_{\llbracket 2 \rrbracket} \notin L_2 \leq \mathbf{P}_2$. The $\mathbf{P}_2$ functions $\mathbf{0}, 1$, and neg are also in the restriction of $[S_4 \cup \{f\}]$ to $\llbracket 2 \rrbracket$. Together with h , they constitute a complete set in $\mathbf{P}_2$: refer to Figure 3.5. It follows that $S_4 \cup \{f\} \vdash V_2$, and the argument of Lemma 3.2.8 gives $S_4 \cup \{f\} \vdash V_4$, as claimed.

Consequently, the coatoms of $\mathbf{P}_4$ are U_3 and L_{2+2} . To establish that L_{2+2} covers L_2^e , suppose $f \in L_{2+2} \setminus L_2^e$. The observation of importance is that f is surjective and depends on more than one variable; our familiar constructive technique then shows $S_4 \cup \{f\} \vdash +_{GF(4)}$, and $+_{GF(4)}$, together with S_4 , generates L_{2+2} .

The proof is completed by remarking that the only exception in the proof of the general theorem when $k = 4$ involved the functions in $V_4 \setminus V_3$. The structure of the interval $[S_4, U_3]$ follows the general result. ■

Chapter 4

The Intervals in Context

4.1 Homogeneous algebras

The objective of this section is to set Theorem 3.2.10 within the context of universal algebra. An algebra that admits all permutations of its underlying set as automorphisms is said to be *homogeneous*. Homogeneous algebras are of interest because of their high degree of internal symmetry; in fact, no finite algebra on five or more elements has an endomorphism monoid that properly contains the set of all permutations. (See Birkenhead [3].) The homogeneous algebras have been analyzed completely within the last fifteen years. It will be shown here how Theorem 3.2.10 can be applied to describe the finite, relation algebras with an analogous automorphism condition.

A function $f \in \mathbf{P}_k$ is called homogeneous if it admits all $\sigma \in S_k$ as automorphisms, and a set of functions F is homogeneous if all of its members are or, equivalently, if the algebra $\langle \llbracket k \rrbracket; F \rangle$ is. We remark that homogeneity is a relational property: if F is homogeneous, so is $[F]$.

As before, the simplest case to consider is that of $\mathcal{P}_2$, in which the property coincides with self-duality, and hence the homogeneous clones are just those of the interval $[\mathbf{J}_2, D_3]$ (v. Figure 2.2). Homogeneity can thus be regarded as a generalization of the self-dual property of Boolean functions and clones.

Marczewski has characterized homogeneous functions in the following way.

4.1.1 Definition (Quackenbush [35]) $\mathbf{a}, \mathbf{b} \in \llbracket k \rrbracket^n$ are said to be of the same *pattern* if, for $1 \leq i, j \leq n$,

$$a_i = a_j \quad \Leftrightarrow \quad b_i = b_j$$

A function $f \in \mathbf{P}_k^{(n)}$ is a *pattern function* if there exists a function $s : \llbracket k \rrbracket^n \rightarrow 2^{\llbracket n \rrbracket} \setminus \{\emptyset\}$ for which,

$\forall \mathbf{a} \in \llbracket k \rrbracket^n$ and $\forall i \in s(\mathbf{a})$,

$$f(\mathbf{a}) = a_i,$$

and $s(\mathbf{a}) = s(\mathbf{b})$ when $\mathbf{a}$ and $\mathbf{b}$ are of the same pattern.

That is, f is a projection when its domain is restricted to any subset of $\llbracket k \rrbracket^n$ of the same pattern. It turns out that the homogeneous functions exhibit only slightly more diversity:

4.1.2 Proposition (Marczewski [28]) *A function $f \in \mathbf{P}_k^{(n)}$ is homogeneous if and only if there exists a function $s : \llbracket k \rrbracket^n \rightarrow 2^{\llbracket n \rrbracket}$ for which*

(a) $s(\mathbf{a}) = s(\mathbf{b})$ when $\mathbf{a}$ and $\mathbf{b}$ are of the same pattern,

(b) $s(\mathbf{a}) = \emptyset$ only if $|\{a_1, \dots, a_n\}| = k - 1$, and

(c) $f(\mathbf{a}) = a_i$ iff $i \in s(\mathbf{a})$.

A moment's reflection shows that, if clones K and K' are homogeneous, then so are $K \wedge K'$ and $K \vee K'$; hence, the homogeneous clones form a sublattice of $\mathcal{L}(\mathcal{P}_k)$. In order to be more precise, let A be a $k! \times k$ matrix whose rows are the $k!$ permutations of $\llbracket k \rrbracket$. Regard the columns of A as a relation in $\mathbf{R}_k$. It is immediate from the definition that $f \in \mathbf{P}_k$ is homogeneous if and only if f preserves A and, in fact, it is not hard to see that A is equivalent to the relation

$$\rho_k = \begin{pmatrix} 0 & 1 & 2 & \cdots & k-1 \\ 1 & 0 & 2 & \cdots & k-1 \\ 1 & 2 & 3 & \cdots & 0 \end{pmatrix}$$

since the permutations in the second and third rows of ρ together generate the group S_k . Consequently, a clone K is homogeneous if and only if it is a member of the interval $[\mathbf{J}_k, \text{Pol } \rho_k]$.

Csákány has shown in [8] and [9] that when $k \geq 5$, all nontrivial homogeneous clones in $\mathbf{P}_k$ are complete with constants. That is, if $K \in (\mathbf{J}_k, \text{Pol } \rho_k]$, then $K \vee \text{Con}_P(k) = \mathbf{P}_k$. He has also determined the only six such clones that are not complete with constants, which are as follows:

$$\left. \begin{array}{l} K_1 = [1 + x] = O_4, \\ K_2 = L_4, \\ K_3 = L_5, \\ K_4 = D_2, \end{array} \right\} \text{ in } \mathcal{P}_2. \text{ See Figure 2.2.}$$

$K_5 = [2x +_3 2y]$ in $\mathcal{P}_3$, and

$K_6 \cong K_2 \times K_2$ in $\mathbf{P}_4$, the four-element Świerczkowski algebra.

Subsequent investigations completely revealed the structure of the interval of homogeneous algebras for each $k \geq 2$. Csákány and Gavalcová [10] first described its minimal elements. Marčenkov [31] and [30] then gave a description of the remaining structure showing that there are finitely many homogeneous algebras for each $k \geq 2$. Their lattices are easily drawn for $k \geq 3$, with the exceptional clones K_5 and K_6 added to a general pattern when $k = 3$ and 4, respectively.

4.2 Homogeneous relation algebras

It is also possible to formulate the notion of a homogeneous relation: we refer to Pöschel [32]. Let a permutation $\sigma \in S_k$ act on an m -tuple by the application of σ to each component. Then a relation $\rho \in \mathbf{R}_k$ is defined to be homogeneous if and only if, for each point $\mathbf{r} \in \rho$ and $\sigma \in S_k$, it is the case that $\sigma \mathbf{r} \in \rho$. Correspondingly, a coclone $R \leq \mathbf{R}_k$ is homogeneous if every $\rho \in R$ is a homogeneous relation. This definition is equivalent to writing that R is homogeneous if and only if the clone S_k preserves R ; thus we see that the homogeneous coclones are exactly those comprising the interval $[\mathbf{D}_k, \text{Inv } S_k]$.

If $K \in \mathbf{P}_k$ is a homogeneous clone, clearly $K^\bullet \leq \mathbf{R}_k$ (the graph of K) is a homogeneous coclone. Furthering the analogy with the case of functions, we say that R is complete with constants if $R \vee \text{Con}_R(k) = \mathbf{R}_k$. Pöschel [32] has proven that the only nontrivial, homogeneous coclones that are not complete with constants are $K_1^\bullet, K_2^\bullet, \dots, K_6^\bullet$. This is surprising in that there is no *a priori* reason to expect such a degree of correspondence.

We remark that the interval of homogeneous coclones, $[\mathbf{D}_k, \text{Inv } S_k]$, is the image of $[S_k, \mathbf{P}_k]$ under Inv operator. Application of the Galois Correspondence to the description of the interval $[S_k, \mathbf{P}_k]$ given for $k \geq 3$ in Theorems 3.2.10–3.2.12, then, yields the relational analogue to Marčenkov’s characterization of the homogeneous clones. In particular, we see that there are also only finitely many homogeneous coclones. At this point, one might make the reasonable objection that this correspondence gives no explicit description of the homogeneous coclones themselves, but only of their polymorphs. It is not difficult, though, to find generators for the invariants of each clone discussed in Section 3.2; one might begin with Rosenberg’s observation [38] that $\text{Inv } U_i = [\iota_i]$ in $\mathcal{R}_k$ for $2 \leq i < k$. (ι_i is defined on page 25.)

To illustrate the sort of information provided by this correspondence, we use it to rederive Pöschel’s result that all homogeneous coclones except $K_5^\bullet$ and $K_6^\bullet$ are complete with constants when $k \geq 3$. Suppose $R \leq \mathbf{R}_k$ is not complete with constants. That is, $R \vee \text{Con}_R(k) < \mathbf{R}_k$, which is equivalent to $\mathbf{J}_k < \text{Pol } R \wedge \text{Pol } \text{Con}_R(k)$. Clearly $f \in \text{Pol } \text{Con}_R(k)$ if and only if $\text{Tr } f = e_1^1$; consequently, if $f \in \text{Pol } R \wedge \text{Pol } \text{Con}_R(k)$ and $f \notin \mathbf{J}_k$, then f is surjective and not essentially unary. When $k \geq 5$, Theorem 3.2.10 indicates that the only member of $[S_k, \mathbf{P}_k]$ containing such a function f is $\mathbf{P}_k$, whence $R = \text{Inv } \mathbf{P}_k = \mathbf{D}_k$, the trivial coclone. If $k = 3$ or 4 , there remain the additional possibilities that $\text{Pol } R = L_3$, or $\text{Pol } R = L_{2+2}$. Thus the only nontrivial choices of R are $\text{Inv } L_3$ and $\text{Inv } L_{2+2}$. By definition, $K_5 = [2x +_3 2y]$. From Proposition 1.2.7, $K_5^\bullet = [(2x +_3 2y)^\bullet]$, and

$$(2x +_3 2y)^\bullet = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \\ 0 & 2 & 1 & 2 & 1 & 0 & 1 & 0 & 2 \end{pmatrix},$$

which we noted in the proof of Theorem 3.2.11 was a generator of $\text{Inv } L_3$. In the same way, K_6 is generated by $g(x, y, z) = x + y + z$ over $GF(4)$, and we saw that $g^\bullet$ generates $\text{Inv } L_{2+2}$; hence $K_6^\bullet = \text{Inv } L_{2+2}$.

4.3 Ω_k as endomorphisms

Enquiries about homogeneous clones and coclones are part of a more general study of endomorphism monoids. The interval of clones with given endomorphisms has been considered for monoids other

than S_k . For example, Marčenkov [31] has determined the clones with automorphism group A_k , the alternating group, and Demetrovics and Hannák [11] have shown that uncountably many clones have a cyclic automorphism group, for $k \geq 5$.

Let us briefly reconsider Theorem 3.1.1 in this spirit. A coclone $Q \leq \mathbf{R}_k$ admits the endomorphisms Ω_k if $\Omega_k \leq \text{Pol } Q$. We have shown that $|\llbracket \Omega_k, \mathbf{P}_k \rrbracket| < \infty$, so there are only finitely many such coclones. One might be motivated to seek an analogy with the case of S_k and ask if there are also finitely many clones admitting this monoid of endomorphisms.

The answer is affirmative for $k \geq 3$ and somewhat trivial; it turns out that the only functions with the endomorphisms Ω_k are projection functions. Suppose $f \in \mathbf{P}_k^{(n)}$ is such a function. It is immediate that $f(\mathbf{a}) \in \{a_0, \dots, a_{n-1}\}$, for any $\mathbf{a} \in \llbracket k \rrbracket^n$. One can also show that f must be a pattern function. The elements of $\llbracket k \rrbracket^n$ of a given pattern induce an equivalence relation on $\llbracket n \rrbracket$ in natural way, and equivalence relations form a lattice under the partial ordering of refinement: write $\epsilon \trianglelefteq \epsilon'$ if ϵ is a refinement of ϵ' . For $\mathbf{a} \in \llbracket k \rrbracket^n$, define $s(\mathbf{a}) = \{i : f(\mathbf{a}) = a_i\}$, and let $p(\mathbf{a})$ denote the equivalence relation on $\llbracket n \rrbracket$ induced by equality amongst the components of $\mathbf{a}$. Suppose $p(\mathbf{a}) = p(\mathbf{b})$. We wish to show that $s(\mathbf{a}) = s(\mathbf{b})$. If not, choose $\mathbf{c} \in \llbracket k \rrbracket^n$ equal to 1 on $s(\mathbf{a})$, and 0 elsewhere. Since $p(\mathbf{a}) \trianglelefteq p(\mathbf{c})$ and $p(\mathbf{b}) \trianglelefteq p(\mathbf{c})$, there exist functions τ and σ in Ω_k , when $k > 2$, for which $\mathbf{c} = \tau\mathbf{a}$, and $\mathbf{c} = \sigma\mathbf{b}$. Since τ and σ are endomorphisms of f ,

$$\begin{aligned} f(\mathbf{c}) &= f(\tau\mathbf{a}) \\ &= \tau f(\mathbf{a}) \\ &= \tau a_i = 1. \end{aligned}$$

On the other hand,

$$\begin{aligned} f(\mathbf{c}) &= f(\sigma\mathbf{b}) \\ &= \sigma f(\mathbf{b}) \\ &= \sigma b_j = 0, \end{aligned}$$

a contradiction. The argument above shows, more generally, that if $p(\mathbf{a}) \trianglelefteq p(\mathbf{b})$, then $s(\mathbf{a}) \subseteq s(\mathbf{b})$, which we may interpret as stating that f is a projection when it is restricted to any subset of $\llbracket k \rrbracket^n$ constituting an ideal of patterns.

Now we continue to show that f must be a projection. Since f is a pattern function, there is a function s as above. Let $\mathcal{S} = \{s(\mathbf{a}) : \mathbf{a} \in \llbracket k \rrbracket^n\}$. If some two sets $s(\mathbf{a})$ and $s(\mathbf{b})$ are disjoint, then one mimics the argument in the previous paragraph by choosing a $\mathbf{c}$ to show that f is not well defined. For any two sets $s(\mathbf{a})$ and $s(\mathbf{b})$ in $\mathcal{S}$, then, it is possible to choose some $\mathbf{c}$ for which

$$p(\mathbf{c}) = \{s(\mathbf{a}) \setminus s(\mathbf{b}), s(\mathbf{a}) \cap s(\mathbf{b}), \llbracket n \rrbracket \setminus s(\mathbf{a})\},$$

since $k \geq 3$. Also choose $\mathbf{a}'$ so that $p(\mathbf{a}') = \{s(\mathbf{a}), \llbracket n \rrbracket \setminus s(\mathbf{a})\}$; then $s(\mathbf{a}') = s(\mathbf{a})$, since $p(\mathbf{a}) \trianglelefteq p(\mathbf{a}')$. Do the same for $\mathbf{b}$ to obtain a $\mathbf{b}'$ for which $s(\mathbf{b}') = s(\mathbf{b})$. Then

$$p(\mathbf{c}) \trianglelefteq p(\mathbf{a}') \Rightarrow s(\mathbf{c}) \subseteq s(\mathbf{a}') = s(\mathbf{a}),$$

and, similarly, $s(\mathbf{c}) \subseteq s(\mathbf{b})$. It follows that $s(\mathbf{c}) = s(\mathbf{a}) \cap s(\mathbf{b})$, from which $s(\mathbf{a}) \cap s(\mathbf{b}) \in \mathcal{S}$. Then $\mathcal{S}$ is closed under intersection, and no two members of $\mathcal{S}$ are disjoint; therefore $\bigcap \mathcal{S}$ is nonempty. However, this is equivalent to the statement that f is a projection.

The arguments above exclude the two-valued case. When $k = 2$, the only constraint is that $f(0, \dots, 0) = 0$ and $f(1, \dots, 1) = 1$. Clones of this form make up the interval $[\mathbf{J}_2, C_4]$, as we saw in Section 2.1, and there are countably many of them.

4.4 Concluding remarks

This investigation was prompted, in part, by the lack of a satisfying explanation for the substantial difference between $\mathcal{L}(\mathcal{P}_2)$ and its higher-valued analogues. While the work here does not at all attempt such an explanation, one might hope that it contributes a mote of insight in that direction. We have extended existing results to show that specific regions of the lattice are finite and easy to describe for all finite underlying sets. The intervals' structure is regular for sufficiently large underlying sets, while the special properties of sets of fewer than five elements give rise to irregularities. In the two-valued case, almost nothing is left of the regular structure.

Both intervals considered are expressed in terms of the product of an interval of unary clones and Burle's chain. While the description of $[S_k, \mathbf{P}_k]$ is subject to the added detail that not all elements of the product are distinct, one should note that $[S_k, \mathbf{P}_k]$ remains the simpler interval in a descriptive sense. Its structure reflects that of the lattice of filters of a well-known poset, whereas

$[\Omega_k, \mathbf{P}_k]$ contains the subgroup lattice of the symmetric group, which itself has a structure rich enough to remain incompletely understood.

The reader might observe that the arguments used to establish the structure of $[S_k, \mathbf{P}_k]$ do not, in most cases, require the presence of the entire symmetric group. Instead, it seems likely that the methods of Section 3.2 could be adapted to establish a similar result describing those clones containing a proper subgroup of S_k ; a natural candidate would be A_k , the alternating group.

The theorems of Chapter 3 indicate the structure of the intervals, and their finiteness. If one is willing to relinquish the quest to describe the structure, it seems probable that one could determine whether or not other, related intervals are finite. In their book, Pöschel and Kalužnin pose the problem of finding general criteria for $[\mathbf{J}_k, K]$ or $[K, \mathbf{P}_k]$ to be of finite cardinality. A reasonable restriction might be to consider first the interval $[K, \mathbf{P}_k]$ for clones K that share with U , Ω_k , and S_k the property that they are contained in U_{k-1} and no other coatom of $\mathbf{P}_k$.

Bibliography

- [1] I. Ágoston, J. Demetrovics, and L. Hannák. On the number of clones containing all constants. In *Lectures in Universal Algebra*, pages 21–25. Colloq. Math. Soc. János Bolyai, 43, North-Holland, 1983.
- [2] K. A. Baker and A. F. Pixley. Polynomial interpolation and the Chinese Remainder Theorem for algebraic systems. *Mathematische Zeitschrift*, 143:165–174, 1975.
- [3] R. Birkenhead. Endomorphism monoids containing all permutations. *Algebra Universalis*, 13(1):268–269, 1981.
- [4] V. G. Bodnarčuk, L. A. Kalužnin, B. N. Kotov, and B. A. Romov. Galois theory for Post algebras I-II. *Cybernetics*, pages 243–252, 531–539, 1969. English trans. of В. Г. Боднарчук, Л. А. Калужнин, Б. Н. Котов и Б. А. Ромов, Теория Галуа для алгебр Поста И, ИИ. Кибернетика 3 (1969), 1–10; 5 (1969), 1–9.
- [5] G. A. Burle (Г. А. Бурле). Классы k -значной логики, содержащие все функции одной переменной. *Дискретный анализ*, 10:3–7, 1967.
- [6] S. Burris and H. P. Sankappanavar. *A Course in Universal Algebra*. Springer-Verlag, New York, 1981.
- [7] J. W. Butler. On complete and independent sets of operations in finite algebras. *Pacific Journal of Mathematics*, 10:1169–1179, 1960.
- [8] B. Csákány. Homogeneous algebras. In H. Kautschitsch, W. Müller, and W. Nöbauer, editors, *Contributions to General Algebra*, pages 77–81, Klagenfurt, 1978. Johannes Heyn.
- [9] B. Csákány. Homogeneous algebras are functionally complete. *Algebra Universalis*, 11:149–158, 1980.
- [10] B. Csákány and T. Gavalcová. Finite homogeneous algebras I. *Acta. Sci. Math.*, 42:57–65, 1980.
- [11] J. Demetrovics and L. Hannák. The number of reducts of a preprimal algebra. *Algebra Universalis*, 16:178–185, 1983.
- [12] J. Demetrovics and L. Hannák. Construction of large sets of clones. *Z. Logik und Grundlagen Math.*, 33:127–133, 1987.
- [13] J. Demetrovics and I. A. Mal'cev. On the depth of infinitely generated subalgebras of Post's iterative algebra $\mathbf{P}_3$. In *Lectures in Universal Algebra*, pages 85–96. Colloq. Math. Soc. János Bolyai, 43, North-Holland, 1983.

- [14] G. P. Gavrilov. Inductive representations of Boolean functions and the finite generation of Post classes. *Algebra and Logic*, 23(1):1–19, 1984. English trans. of Г. П. Гаврилов. Индуктивные представления булевых функций и конечная порождаемость классов Поста. *Алгебра и Логика*, 23(1):3–26, 1984.
- [15] D. Geiger. Closed systems of functions and predicates. *Pacific Journal of Mathematics*, 27(1):95–100, 1968.
- [16] G. Grätzer. *Universal Algebra*. Springer-Verlag, New York, 1979.
- [17] L. Haddad. Intersections of finitely generated clones. *Algebra Universalis*, 27(2), 1990.
- [18] L. Haddad and I. Rosenberg. A note on finite clones containing all permutations. In *Proceedings of the ISMVL*, pages 34–41, Washington D.C., 1990. IEEE Computer Society Press.
- [19] S. V. Jablonskiĭ. Einführung in die Theorie der Funktionen der k -wertigend Logik. In S. V. Jablonskiĭ and O. B. Lupanov, editors, *Diskrete Mathematik und Mathematische Fragen der Kybernetik*, pages 13–70. Birkhäuser Verlag, Basel, Stuttgart, 1980.
- [20] S. V. Jablonskiĭ, G. P. Gavrilov, and V. B. Kudrjavcev. *Boolesche Funktionen und Postsche Klassen*. Akademie-Verlag, Berlin, 1970. trans. R. Lindner of С. В. Яблонский, Г. П. Гаврилов, и В. Б. Кудрявцев. *Функции алгебры логики и классы Поста*. Наука, Москва, 1966.
- [21] S. V. Jablonskiĭ (С. В. Яблонский). Функциональные построения в k -значной логике. *Труды Матем. инст. им. В. А. Стеклова*, 51:5–142, 1958.
- [22] Ju. Janov and A. Mučnik (Ю. Янов и А. Мучник). О существовании k -значных замкнутых классов не имеющих конечного базиса. *Докл. Акад. Наук СССР*, 127:44–46, 1959.
- [23] A. V. Kuznesov (А. В. Кузнецов). Алгебра логики и ее обобщения. In *Математика в СССР за 40 лет. т. II*, pages 102–115. Москва, 1959.
- [24] A. V. Kuznesov (А. В. Кузнецов). Структуры с замыканием и критерии функциональной полноты. *Усп. Мат. Наук*, 16(98):201–202, 1961.
- [25] I. A. Mal'cev. Some properties of cellular subalgebras of a Post algebra and their basic cells. *Algebra and Logic*, 11(5):315–325, 1972. English trans. of И. А. Мальцев. Некоторые свойства клеточных подалгебр алгебр Поста и их основных клеток. *Алгебра и Логика*, 11(5):571–587, 1972.
- [26] A. I. Mal'cev (А. И. Мальцев). Об одном усилении теорем Слупецкого и Яблонского. *Алгебра и Логика*, 6(3):61–75, 1967.
- [27] I. A. Mal'cev (И. А. Мальцев). Некоторые свойства клеток алгебр Поста. *Дискретный анализ*, 20:24–31, 1973.
- [28] E. Marczewski. Homogeneous algebras and homogeneous operations. *Fund. Math.*, 56:81–103, 1964.

- [29] S. S. Marčenkov. Existence of finite bases in closed classes of Boolean functions. *Algebra and Logic*, 23(1):66–74, 1984. English trans. of С. С. Марченков. К существованию конечных базисов в замкнутых классах булевых функций. *Алгебра и Логика*, 23(1):88–99, 1984.
- [30] S. S. Marčenkov (С. С. Марченков). О замкнутых классах самодвойственных функций многозначной логики. *Проблемы Кибернетики*, 36:5–22, 1979.
- [31] S. S. Marčenkov (С. С. Марченков). Однородные алгебры. *Проблемы Кибернетики*, 39:85–106, 1982.
- [32] R. Pöschel. Homogeneous relational algebras are relationally complete. In *Finite Algebra and Multiple-Valued Logic*, pages 587–601. Colloq. Math. Soc. János Bolyai, 28, North-Holland, 1979.
- [33] R. Pöschel and L. Kalužnin. *Funktionen- und Relationenalgebren: Ein Kapitel der Diskreten Mathematik*. Birkhäuser Verlag, Basel, Stuttgart, 1979.
- [34] E. L. Post. The two-valued iterative systems of mathematical logic. *Annals of Math. Studies* 5, Princeton University Press, Princeton, 1941.
- [35] R. W. Quackenbush. Some classes of idempotent functions and their compositions. *Colloq. Math.*, 29:71–81, 1974.
- [36] I. G. Rosenberg. Über die Verschiedenheit maximaler Klassen in $\mathbf{P}_k$. *Rev. Roumaine Math. Pures Appl.*, 14:431–483, 1969.
- [37] I. G. Rosenberg. Über die functionale Vollständigkeit in den mehrwertigen Logiken. *Rozprawy Československé Akademie Věd. Řada Mat. Přír. Věd.*, 80(4):3–93, 1970.
- [38] I. G. Rosenberg. Universal algebras with all operations of bounded range. *Colloq. Math.*, 30:77–85, 1974.
- [39] I. G. Rosenberg. Completeness properties of multiple-valued logic algebras. In D. C. Rine, editor, *Computer Science and Multiple-Valued Logic: Theory and Applications*, pages 150–192. North-Holland, Amsterdam, 1984. revised ed.
- [40] A. Salomaa. On the number of simple bases of the set of functions over a finite domain. *Ann. Univ. Turkuensis, Ser. A I*, 52, 1962.
- [41] A. Salomaa. On basic groups for the set of functions over a finite domain. *Ann. Acad. Sci. Fenn., Series A I Math.*, 339:3–11, 1963.
- [42] P. Schofield. Complete subsets of mappings over a finite domain. *Proc. Camb. Phil. Soc.*, 63:597–611, 1966.
- [43] A. B. Ugol'nikov. Closed Post classes. *Soviet Mathematics (Izvestiya VUZ)*, 32:131–142, 1988.
- [44] J. Ślupecki. Kriterion pełności wielowartościowych systemów logiki zdań. *C. R. Seanc. Soc. Sci. Varsovie*, 32:102–109, 1939.
- [45] P. De Witte. A single axiom for closure operations. *Algebra Universalis*, 12:268–269, 1981.