SÉMINAIRE DE MATHÉMATIQUES SUPÉRIEURES
SÉMINAIRE SCIENTIFIQUE OTAN (NATO ADVANCED STUDY INSTITUTE)
DÉPARTEMENT DE MATHÉMATIQUES ET DE STATISTIQUE — UNIVERSITÉ DE MONTRÉAL

CLONES IN UNIVERSAL ALGEBRA

ÁGNES SZENDREI
József Attila University
Szeged

1986
LES PRESSES DE L'UNIVERSITÉ DE MONTRÉAL
C.P. 6128, succ. «A», Montréal (Québec), Canada H3C 3J7

Notes du cours de Madame Ágnes Szendrei à la vingt-troisième session du Séminaire de mathématiques supérieures / Séminaire scientifique OTAN (ASI 697/83), tenue au Département de mathématiques et de statistique de l'Université de Montréal du 23 juillet au 10 août 1984. Cette session avait pour titre général « Algèbre universelle et relations » et était placée sous les auspices de l'Organisation du Traité de l'Atlantique Nord, du ministère de l'Éducation du Québec, du Conseil de recherches en sciences naturelles et en génie du Canada et de l'Université de Montréal.

FOREWORD

The investigation of clones originates partly in logic, namely in the study of composition of truth functions, and partly in universal algebra, from the observation that most properties of algebras depend on their term operations rather than on the choice of their basic operations. During the last fifteen years or so the combination of these two aspects and the application of new algebraic methods produced a rapid development, and by now the theory of clones has become an integral part of universal algebra.

The aim of these lecture notes is to introduce the reader to some results showing how clones can contribute to the understanding of the structure of algebras, and not less importantly, to present several techniques in clone theory. To keep the length within reasonable limits I had to select a few topics. The choice is certainly rather subjective. I took this opportunity to reconsider a number of results I was interested in, and to point out some connections between them, a part of which may not have been known before.

The book is self-contained, the reader is assumed to be familiar only with the rudiments of universal algebra and lattice theory, and some basic facts in other fields of abstract algebra (e.g. groups, permutation groups, rings, modules). Four textbooks, three on universal algebra and one on clones, are listed

on p. 159. Throughout, they are referred to by an abbreviation. To all other books and papers reference is made by the author's name and year of publication.

This volume is an extended version of my lectures delivered at the 23rd Session of the Séminaire de mathématiques supérieures on "Universal Algebra and Relations", held at the Université de Montréal in 1984. I wish to express my thanks to the organizers, Professors P. Berthiaume and I.G. Rosenberg, for the invitation. I am greatly indebted to P.P. Pálfy who read most of the manuscript and made a lot of valuable suggestions and corrections. I am grateful also for the helpful remarks by B. Csákány and L. Szabó.

CONTENTS

Chapter 1

ALGEBRAS AND CLONES

The notion of a clone, which will be fundamental throughout these notes, was introduced by P. Hall. In 2-valued as well as in multiple-valued logic a related concept, called closed class, or iterative class of truth functions was used already by E.L. Post [1921], [1941]. However, the importance of clones in universal algebra was not recognized until the early seventies.

By an operation we will always mean a finitary, nonnullary operation. (The exclusion of nullary operations does not cause any essential restriction in generality.) Let A be a set. For integers $n \geq 1$ and $1 \leq i \leq n$, the *i-th n-ary projection* on A is the operation defined by

$$e_{n,i}(a_1,\ldots,a_n) = a_i \quad \text{for all} \quad a_1,\ldots,a_n \in A.$$

If f is an n-ary and $g_1,\ldots,g_n$ are k-ary operations on A, then we define a k-ary operation $f(g_1,\ldots,g_n)$ on A, called the *superposition* of $f,g_1,\ldots,g_n$, as follows:

$$f(g_1,\ldots,g_n)(a_1,\ldots,a_k) = f(g_1(a_1,\ldots,a_k),\ldots,g_n(a_1,\ldots,a_k))$$

for all $a_1,\ldots,a_k \in A$.

DEFINITION. A set of operations on a fixed set A is said to be a *clone* on A iff it contains the projections and is closed under superposition.

Clearly, the set O_A of all operations on A, and the set J_A of all projections on A are clones. Furthermore, the intersection of arbitrary set of clones on A is again a clone. Thus it follows that the clones on A form a complete lattice Lat(A) with least element J_A and greatest element O_A. Furthermore, for arbitrary set F of operations on A there exists a least clone containing F. As usual, this clone will be called the *clone generated by* F, and will be denoted by [F]. Instead of [{f}] we write simply [f]. For a clone C and $n \geq 1$ we let $C^{(n)}$ denote the set of n-ary operations from C.

An n-ary operation f on A is said to *depend* on its i-th variable ($1 \leq i \leq n$) iff there exist elements $a_1,\ldots,a_{i-1},a_{i+1},\ldots,a_n,b,c \in A$ such that

$$f(a_1,\ldots,a_{i-1},b,a_{i+1},\ldots,a_n) \neq f(a_1,\ldots,a_{i-1},c,a_{i+1},\ldots,a_n).$$

Otherwise the i-th variable of f is called *fictitious*. In that case f can be regarded to arise from an (n-1)-ary operation by adding a new, fictitious variable in the i-th place. Using the projections it is easy to see that for every clone C and every operation $g \in C$, C contains all operations arising from g by identifying variables, or by permuting variables, or by adding fictitious variables.

Two clones are naturally attached to every algebra $\mathcal{A} = (A;F)$: the clone $T(\mathcal{A})$ of term operations (or term functions [BS], polynomials [G]) of $\mathcal{A}$, which is the clone generated by F, and is called the *clone of* $\mathcal{A}$; and the clone $P(\mathcal{A})$ of polynomial operations (polynomials [BS], algebraic functions [G]) of $\mathcal{A}$, which is the clone generated by F and all the unary constant operations on A.

EXAMPLES. 1. If $\underline{A} = (A;+,-,0)$ is an Abelian group, then

$$T(\underline{A}) = \{\sum_{i=1}^{n} c_i x_i : n \geq 1,\ c_1,\ldots,c_n \in \mathbf{Z}\},$$

$$P(\underline{A}) = \{\sum_{i=1}^{n} c_i x_i + a: n \geq 1,\ c_1,\ldots,c_n \in \mathbf{Z},\ a \in A\}$$

($\mathbf{Z}$ denotes the set of integers).

2. For a ring R with 1 and a unitary R-module ${}_R\underline{A} = (A;+,-,0,R)$ we have

$$T({}_R\underline{A}) = \{\sum_{i=1}^{n} r_i x_i: n \geq 1,\ r_1,\ldots,r_n \in R\},$$

$$P({}_R\underline{A}) = \{\sum_{i=1}^{n} r_i x_i + a: n \geq 1,\ r_1,\ldots,r_n \in R,\ a \in A\}.$$

3. For a commutative ring R with 1, the clone $P(R)$ consists of all polynomial functions of several variables (in the classical sense) on R.

4. Lagrange's interpolation theorem for functions of several variables implies that $P(K) = O_K$ for every finite field K.

5. Let $\mathfrak{B}_2 = (\{0,1\};\wedge,\vee,r,0,1)$ be the 2-element Boolean algebra (r stands for complementation). It is known from elementary logic that $T(\mathfrak{B}_2) = O_{\{0,1\}}$.

DEFINITION. Two algebras with a common universe are called *term equivalent* [*polynomially equivalent*] iff they have the same term [polynomial] operations. We say that two algebras $\mathfrak{A}_i = (A_i;F_i)$ $(i = 1,2)$ are *equivalent* iff $\mathfrak{A}_1$ is isomorphic to an algebra term equivalent to $\mathfrak{A}_2$.

It is easy to see that all three relations defined above are indeed equivalence relations. Equivalence of algebras is just the abstract version of term equivalence. Term equivalence is important because term equivalent algebras behave very similarly: they have the same subalgebras, endomorphisms, congruences, etc., moreover, they have finite bases for their identities simultaneously provided both are of finite type. In fact, most properties of an algebra depend on its clone rather than the choice of its basic operations. Several well-known

instances of term equivalence are listed below to illustrate that term equivalent algebras are indeed "essentially the same".

EXAMPLES. 1. A $\mathbf{Z}$-module and its additive group;

2. a Boolean algebra and the corresponding Boolean ring with 1;

3. a zero ring and its additive group are term equivalent.

Recall that an operation f on A is *idempotent* iff it satisfies the identity $f(x,\ldots,x) = x$. A clone on A is called idempotent iff it consists of idempotent operations, while an algebra $(A;F)$ is idempotent iff its basic operations (or equivalently, its term operations) are idempotent.

DEFINITION. Let $\mathcal{A}_1 = (A;F_1)$ be an algebra. An algebra $\mathcal{A}_2 = (A;F_2)$ is said to be a *reduct* [*polynomial reduct*] of $\mathcal{A}_1$ iff $T(\mathcal{A}_2) \subseteq T(\mathcal{A}_1)$ [$P(\mathcal{A}_2) \subseteq P(\mathcal{A}_1)$, respectively]. The *full idempotent reduct* of $\mathcal{A}_1$ is the algebra on A whose operations are the idempotent term operations of $\mathcal{A}_1$.

EXAMPLE. The full idempotent reduct of a unitary R-module ${}_R\underline{A} = (A;+,-,0,R)$ is the algebra

$$(A;\{\sum_{i=1}^{n} r_i x_i : n \geq 1,\ r_1,\ldots,r_n \in R,\ \sum_{i=1}^{n} r_i = 1\}),$$

which is term equivalent to the affine R-module

$$(A;x-y+z,\{rx + (1-r)y : r \in R\})$$

corresponding to ${}_R\underline{A}$ (cf. Proposition 2.6).

It is easy to see that a clone C on A is the clone of a unary algebra with universe A if and only if every operation in C depends on at most one of its variables. These clones will be termed *unary clones*. Occasionally it will be convenient to call J_A the *trivial clone* on A. Accordingly, by a *trivial algebra* we mean an algebra whose basic operations (or equivalently, term operations) are projections.

For an algebra $\mathcal{A} = (A;F)$ a subset B of A is said to be a *subuniverse* of $\mathcal{A}$ iff B is empty or is the universe of a subalgebra of $\mathcal{A}$.

The fundamental notions of universal algebra and lattice theory, which are not defined here, can be found in any textbook on universal algebra, say [BS], [G], or [MMPT]. The 1-element algebras are considered simple. For a set A, the equality relation $\Delta_A = \{(a,a): a \in A\}$ and the total relation $\nabla_A = A^2$ are called *trivial equivalence relations* on A. The identity mapping $A \to A$ will be denoted by id_A. (The subscripts A can be omitted if there is no danger of confusion.) For an Abelian group $\underline{A} = (A;+,-,0)$ the *exponent* of $\underline{A}$ is the least positive integer n such that $\underline{A}$ satisfies the identity $nx = 0$, if such an n exists; otherwise the exponent of $\underline{A}$ is 0.

Term operations and subalgebras

The most fundamental observation in clone theory is that the clone $T(\mathcal{A})$ of an algebra $\mathcal{A} = (A;F)$ can also be described by "invariants" rather than its generating set F. Namely, these invariants are the subuniverses of powers of $\mathcal{A}$. This connection between the term operations and the subuniverses of powers of $\mathcal{A}$ is especially nice if $\mathcal{A}$ is finite, for then the subuniverses of finite powers of $\mathcal{A}$ already determine $T(\mathcal{A})$. Although in a completely different terminology, these ideas go back to the investigations of A. V. Kuznetsov and his school, and M. Krasner in the forties and fifties. However, a systematic treatment was not available until the late sixties and early seventies.

The aim of this section is to record those facts from the general theory which will be needed later on. A more complete discussion can be found in the books [PK] and [MMPT; Chapter VII].

DEFINITION. Let A be a set and B a subset of a power A^I of A. An operation f on A is said to *preserve* B iff B is a subuniverse of the algebra $(A;f)^I$.

For example, if $B \subseteq A^2$ is an equivalence relation on A, then f preserves B means that B is a congruence of the algebra $(A;f)$, while if $B \subseteq A^2$ is a partial order on A, then f preserves B is equivalent to saying that f is monotone with respect to B.

The set of those operations on A which preserve a subset B of a power of A will be denoted by $\mathrm{Pol}_A\{B\}$ (as these operations are sometimes called polymorphisms). More generally, for arbitrary set S of subsets of powers of A we define the set $\mathrm{Pol}_A S$ of operations by

$$\mathrm{Pol}_A S = \bigcap_{B \in S} \mathrm{Pol}_A\{B\}.$$

(The subscript A may be omitted if it is understood from the context.)

To every function $f: A_1 \times \ldots \times A_n \to A_o$ $(n \geq 1,\ A_o, A_1, \ldots, A_n \subseteq A)$ we can assign in a natural way a subset of A^{n+1} as follows:

$$f^{\square} = \{(a_1, \ldots, a_n, f(a_1, \ldots, a_n)) : a_1 \in A_1, \ldots, a_n \in A_n\}.$$

Sometimes it will be more convenient to write the values of f in the first component, that is, to associate with f the set

$$f_{\square} = \{(f(a_1, \ldots, a_n), a_1, \ldots, a_n) : a_1 \in A_1, \ldots, a_n \in A_n\}$$

instead of $f^{\square}$. In most cases these notations will be used for operations.

DEFINITION. For two operations f, g on A we say that f *commutes* with g iff f preserves $g^{\square}$ (or equivalently, $g_{\square}$).

In particular, if g is unary, this means that g is an endomorphism of the algebra $(A;f)$. As we shall see below (Proposition 1.1(b)), the

commutativity of two operations is a symmetric relation.

The following simple facts are immediate consequences of the definitions, therefore the proofs are left to the reader.

PROPOSITION 1.1. *Let* A *be a set.*

(a) $\mathrm{Pol}_A S$ *is a clone for arbitrary set* S *of subsets of powers of* A.

(b) *An operation* $f \in O_A^{(k)}$ *commutes with an operation* $g \in O_A^{(n)}$ *if and only if* f *and* g *satisfy the identity*

$$f(g(x_{11},\ldots,x_{1n}),\ldots,g(x_{k1},\ldots,x_{kn})) = g(f(x_{11},\ldots,x_{k1}),\ldots,f(x_{1n},\ldots,x_{kn})).$$

(c) *For a subset* B *of* A *and for arbitrary operations* $f \in O_A$, $h \in O_B$, *we have* $f \in \mathrm{Pol}_A\{h^{\square}\}$ *if and only if* B *is closed under* f *and the restriction* $f|_B$ *of* f *commutes with* h.

Let us consider a set T of n-ary operations on A. Each member of T is a mapping $A^n \to A$, and hence is an element of A^{A^n}. Thus T corresponds to a subset X_T of A^{A^n}. The proof of the following lemma is again straightforward.

LEMMA 1.2. *Let* T *be a set of* n*-ary operations on* A. *A* k*-ary operation* g *on* A *preserves* X_T *if and only if for all operations* $f_1,\ldots,f_k \in T$ *we have* $g(f_1,\ldots,f_k) \in T$.

Now we can state more precisely the connection between the term operations and the subuniverses of powers of an algebra.

PROPOSITION 1.3. *Let* $\mathcal{A} = (A;F)$ *be an algebra. For every integer* $n \geq 1$, $X_{T^{(n)}(\mathcal{A})}$ *is a subuniverse of* $\mathcal{A}^{A^n}$, *and an operation* f *on* A *is a term operation of* $\mathcal{A}$ *if and only if it preserves all subuniverses* $X_{T^{(n)}(\mathcal{A})}$ $(n \geq 1)$.

PROOF. Let $C = \mathrm{Pol}_A\{X_{T^{(n)}(\mathcal{A})} : n \geq 1\}$. By Lemma 1.2 we have $T(\mathcal{A}) \subseteq C$, implying also that $X_{T^{(n)}(\mathcal{A})}$ is a subuniverse of $\mathcal{A}^{A^n}$ for every $n \geq 1$. To prove

the reverse inclusion $T(\mathcal{A}) \supseteq C$, let $g \in C$, say g is n-ary. Then g preserves $X_{T^{(n)}(\mathcal{A})}$, so applying Lemma 1.2 for the n-ary projections $e_{n,1},\ldots,e_{n,n} \in T^{(n)}(\mathcal{A})$ we get that $g = g(e_{n,1},\ldots,e_{n,n}) \in T^{(n)}(\mathcal{A})$. This completes the proof.

COROLLARY 1.4. *For a finite algebra* $\mathcal{A} = (A;F)$, *an operation* g *on* A *is a term operation of* $\mathcal{A}$ *if and only if it preserves the subuniverses of finite powers of* $\mathcal{A}$.

PROOF. Let S denote the set of subuniverses of finite powers of $\mathcal{A}$. Since $\{X_{T^{(n)}(\mathcal{A})} : n \geq 1\} \subseteq S$, we have

$$\mathrm{Pol}_A\{X_{T^{(n)}(\mathcal{A})} : n \geq 1\} \supseteq \mathrm{Pol}_A S.$$

The left hand side equals $T(\mathcal{A})$ by Proposition 1.3. The right hand side contains F by definition, so it contains $T(\mathcal{A})$ as well by Proposition 1.1(a). Thus $T(\mathcal{A}) = \mathrm{Pol}_A S$, as claimed.

If $\mathcal{A}$ is infinite, then $|A^n| = |A|$ for all $n \geq 1$, so the same argument as above yields

COROLLARY 1.5. *For an infinite algebra* $\mathcal{A} = (A;F)$, *an operation* g *on* A *is a term operation of* $\mathcal{A}$ *if and only if it preserves the subuniverses of* $\mathcal{A}^A$.

Proposition 1.3 for A finite and Corollary 1.4 were proved independently by D. Geiger [1968] and V. G. Bodnarchuk, L. A. Kaluzhnin, V. N. Kotov, B. A. Romov [1969], and they were generalized to the infinite case by I. G. Rosenberg [1972].

For comparison, it is worth mentioning how those operations g on A can be characterized which preserve the subuniverses of finite powers of an infinite algebra $\mathcal{A} = (A;F)$.

DEFINITION. Let C be a clone on A. We say that an operation $g \in O_A^{(n)}$ can be interpolated by operations from C iff for every finite subset B of A^n there exists an operation $f \in C$ such that $f|_B = g|_B$. The clone C is called *locally closed* iff it contains every operation that can be interpolated by operations from C. For an algebra $\mathcal{A} = (A;F)$, the operations that can be interpolated by operations from $T(\mathcal{A})$ [$P(\mathcal{A})$] are called *local term operations* of $\mathcal{A}$ [*local polynomial operations* of $\mathcal{A}$, respectively].

The definitions immediately imply

PROPOSITION 1.6. *Let* A *be a set.*

(a) *The local term operations of any algebra* $\mathcal{A} = (A;F)$ *form a locally closed clone on* A.

(b) $\mathrm{Pol}_A S$ *is a locally closed clone for arbitrary set* S *of subsets of finite powers of* A.

For arbitrary set T of n-ary operations on A, and for arbitrary finite subset B of A^n, we let $X_{T,B}$ denote the subset of A^B consisting of the functions $g|_B$ with $g \in T$, considered as elements of A^B. Similarly to Lemma 1.2 we have

LEMMA 1.7. *Let* T *be a set of* n*-ary operations on* A *and let* B *be a finite subset of* A^n. *A* k*-ary operation* g *on* A *preserves* $X_{T,B}$ *if and only if for all operations* $f_1,\ldots,f_k \in T$, *there exists* $f \in T$ *such that* $g(f_1,\ldots,f_k)|_B = f|_B$.

Thus we get the following analogue of Proposition 1.3 for local term operations.

PROPOSITION 1.8. *Let* $\mathcal{A} = (A;F)$ *be an algebra. For every integer* $n \geq 1$ *and for arbitrary finite subset* B *of* A^n, $X_{T^{(n)}(\mathcal{A}),B}$ *is a subuniverse of* $\mathcal{A}^B$, *and an operation* f *on* A *is a local term operation of* $\mathcal{A}$ *if and only*

if it preserves all these subuniverses $X_{T^{(n)}(\mathcal{A}),B}$.

PROOF. Let $C = \mathrm{Pol}_A\{X_{T^{(n)}(\mathcal{A}),B} : n \geq 1,\ B \subseteq A^n,\ B \text{ is finite}\}$. In the same way as in Proposition 1.3, making use of Lemma 1.7 in place of Lemma 1.2, we can conclude that C is the clone of local term operations of $\mathcal{A}$. The details are left to the reader.

As before, we get the required characterization, which is due to B. A. Romov [1977].

COROLLARY 1.9. *For an algebra* $\mathcal{A} = (A;F)$, *an operation* g *on* A *is a local term operation of* $\mathcal{A}$ *if and only if it preserves the subuniverses of finite powers of* $\mathcal{A}$.

Clearly, if $\mathcal{A}$ is finite, then the local term operations of $\mathcal{A}$ are term operations as well, so Corollary 1.4 is a special case of Corollary 1.9.

For a set F of operations on a fixed set A, let $\mathrm{Inv}_A F$ denote the family of subuniverses of finite powers of the algebra $(A;F)$.

EXERCISE 1.10. For every set A, the mappings

$$F \mapsto \mathrm{Inv}\ F$$

$$\mathrm{Pol}\ S \leftarrow S$$

between the power sets of $\mathcal{O}_A$ and $\{B: B \subseteq A^n \text{ for some } n \geq 1\}$ define a Galois connection (or polarity), that is, the following two conditions hold for arbitrary subsets F, F' of $\mathcal{O}_A$ and for arbitrary sets S, S' of subsets of finite powers of A:

(1) if $F \subseteq F'$ then $\mathrm{Inv}\ F \supseteq \mathrm{Inv}\ F'$, and similarly, if $S \subseteq S'$ then $\mathrm{Pol}\ S \supseteq \mathrm{Pol}\ S'$;

(2) $F \subseteq \mathrm{Pol}\ \mathrm{Inv}\ F$ and $S \subseteq \mathrm{Inv}\ \mathrm{Pol}\ S$.

This implies also that for F, S as above we have

(3) $\mathrm{Inv}\, F = \mathrm{Inv}\, \mathrm{Pol}\, \mathrm{Inv}\, F$ and $\mathrm{Pol}\, S = \mathrm{Pol}\, \mathrm{Inv}\, \mathrm{Pol}\, S$.

Consequently

(4) the mappings Pol Inv and Inv Pol are closure operators, hence the respective closed sets (that is the sets of the form Pol S and those of the form Inv F, respectively) constitute complete lattices; moreover, Pol and Inv, when restricted to these lattices, yield mutually inverse dual isomorphisms.

Propositions 1.6 and 1.8 (or Corollary 1.9) show that the sets of the form $\mathrm{Pol}_A\, S$ are exactly the locally closed clones on A, or for A finite, they are exactly the clones on A. We note that the sets of the form $\mathrm{Inv}_A\, F$ can also be described as sets of subsets of finite powers of A that are closed under certain constructions. (For A finite this was discovered independently by V. G. Bodnarchuk, et al [1969] and D. Geiger [1968]. Later these results were generalized to the infinite case independently by R. Pöschel [1979] and L. Szabó [1978].) However, as we will not need this fact later on, we do not go into the details. Nevertheless, some constructions will be used quite often, so we introduce the notations here.

Let B be a subset of A^k $(k \geq 1)$. We will write $\underline{k}$ for the set $\{1,\ldots,k\}$ indexing the components of B. For an ℓ-tuple $(i_1,\ldots,i_\ell) \in \underline{k}^\ell$ we define the projection of B onto its components $i_1,\ldots,i_\ell$ by

$$\mathrm{pr}_{i_1,\ldots,i_\ell} B = \{(x_{i_1},\ldots,x_{i_\ell}) : (x_1,\ldots,x_k) \in B\}.$$

In particular, if $\ell = k$ and $i_1,\ldots,i_k$ is a permutation of $1,\ldots,k$, then $\mathrm{pr}_{i_1,\ldots,i_k} B$ arises from B by rearranging the components. The property that, up to the order of their components, the subsets B and B' of A^k coincide, will be denoted by $B \approx B'$. For example, if $k = 2$, then $\mathrm{pr}_{2,1} B$ is the inverse of B, which will be denoted by $B^\cup$. For a nonvoid subset I of $\underline{k}$ with $I = \{i_1,\ldots,i_\ell\}$, $i_1 < \ldots < i_\ell$, we write $\mathrm{pr}_I B$ for $\mathrm{pr}_{i_1,\ldots,i_\ell} B$. The symbol

$B \preccurlyeq B_1 \times \ldots \times B_k$ will be used to designate that $\mathrm{pr}_i B = B_i$ for all $1 \leq i \leq k$. The sign $\prec$ stands for "$\preccurlyeq$ and $\neq$". For $B \preccurlyeq B_1 \times \ldots \times B_k$ and for arbitrary bijections $\pi_i\colon B_i \to C_i$ $(C_i \subseteq A,\ 1 \leq i \leq k)$ we set

$$B[\pi_1,\ldots,\pi_k] = \{(x_1\pi_1,\ldots,x_k\pi_k)\colon (x_1,\ldots,x_k) \in B\}.$$

If $1 \leq \ell < k$ and $a = (a_{\ell+1},\ldots,a_k) \in A^{k-\ell}$, then we define the subset of A^ℓ arising from B by "substituting the constants $a_{\ell+1},\ldots,a_k$ for the $(\ell+1)$-st up to the k-th components" as follows:

$$\begin{aligned} B(x_1,\ldots,x_\ell,a) &= B(x_1,\ldots,x_\ell,a_{\ell+1},\ldots,a_k) \\ &= \{(x_1,\ldots,x_\ell) \in A^\ell\colon (x_1,\ldots,x_\ell,a_{\ell+1},\ldots,a_k) \in B\}. \end{aligned}$$

As usual, for $C,C' \subseteq A^2$ we set

$$C \circ C' = \{(x,y) \in A^2\colon (x,z) \in C \text{ and } (z,y) \in C' \text{ for some } z \in A\}.$$

Let now $\mathcal{A} = (A;F)$ be an arbitrary algebra. It is easy to check that $C \circ C'$ is a subuniverse of $\mathcal{A}^2$ if C and C' are such. Similarly, $\mathrm{pr}_{i_1,\ldots,i_\ell} B$ is a subuniverse of $\mathcal{A}^\ell$ whenever B is a subuniverse of $\mathcal{A}^k$ and $(i_1,\ldots,i_\ell) \in \underline{k}^\ell$. Furthermore, if $B \preccurlyeq B_1 \times \ldots \times B_k$ is a subuniverse of $\mathcal{A}^k$ and for each bijection $\pi_i\colon B_i \to C_i$ $(C_i \subseteq A,\ 1 \leq i \leq k)$, $\pi_i^\square$ is a subuniverse of $\mathcal{A}^2$, then $B[\pi_1,\ldots,\pi_k]$ is also a subuniverse of $\mathcal{A}^k$. In general, the remaining construction fails to have the analogous property. However, if $\mathcal{A}$ is idempotent, then $B(x_1,\ldots,x_\ell,a_{\ell+1},\ldots,a_k)$ is a subuniverse of $\mathcal{A}^\ell$ whenever B is a subuniverse of $\mathcal{A}^k$ and $a_{\ell+1},\ldots,a_k$ are arbitrary elements from A.

For later use and to illustrate the power of the above tools we finally prove a result establishing a relation between the subuniverses of finite powers of a finite algebra and its full idempotent reduct. We will call a subset B of A^k *irredundant* iff $\mathrm{pr}_{i,j} B \nsubseteq \Delta_A$ for all $1 \leq i < j \leq k$ and $|\mathrm{pr}_i B| > 1$ for all $1 \leq i \leq k$.

PROPOSITION 1.11. *Let* $\mathcal{A} = (A;F)$ *be a finite algebra and* $\mathcal{A}_o$ *its full idempotent reduct. Every set of the form* $\mathrm{pr}_{\underline{n}} B(x_1,\ldots,x_\ell,a)$, *where* B *is a subuniverse of* $\mathcal{A}^k$, $1 \le n \le \ell \le k$ *and* $a \in A^{k-\ell}$, *is a subuniverse of* $\mathcal{A}_o^n$. *Conversely, all irredundant subuniverses of finite powers of* $\mathcal{A}_o$ *are of this form.*

PROOF. The first claim is easy to check. To prove the second one, consider an irredundant subuniverse S of $\mathcal{A}_o^n$ $(n \ge 1)$, and let $|S| = m$, $S = \{(s_{i1},\ldots,s_{in}): 1 \le i \le m\}$. Since S is irredundant, the elements $(s_{1j},\ldots,s_{mj}) \in A^m$ $(1 \le j \le n)$ are pairwise distinct, and none of them equals $(a,\ldots,a) \in A^m$ for any $a \in A$. Thus, if in the subuniverse $X_{T^{(m)}(\mathcal{A})}$ of $\mathcal{A}^{A^m}$ (cf. Proposition 1.3) we first substitute a in the component corresponding to $(a,\ldots,a) \in A^m$ for every $a \in A$, and then project the resulting set onto its components $(s_{1j},\ldots,s_{mj}) \in A^m$ $(1 \le j \le n)$, then we get the set

$$S' = \{(g(s_{11},\ldots,s_{m1}),\ldots,g(s_{1n},\ldots,s_{mn})): g \in T^{(m)}(\mathcal{A}_o)\}.$$

Because of the projections we have $S \subseteq S'$. On the other hand, $S' \subseteq S$, since S is a subuniverse of $\mathcal{A}_o^n$. Thus $S = S'$, concluding the proof.

Minimal clones and maximal clones

It is easy to see that for every set A, the lattice $\mathrm{Lat}(A)$ of subclones of $\mathcal{O}_A$ is an algebraic lattice. The atoms [dual atoms] of $\mathrm{Lat}(A)$ are called *minimal* [*maximal*] *clones*; that is, a subclone C of $\mathcal{O}_A$ is minimal iff $C \neq \mathcal{J}_A$ and C, $\mathcal{J}_A$ are the only subclones of C, while C is maximal iff $C \neq \mathcal{O}_A$ and C, $\mathcal{O}_A$ are the only clones containing C. We prove that for a finite set A, the lattice $\mathrm{Lat}(A)$ is atomic and dually atomic with finitely many atoms and dual atoms.

Clearly, every minimal clone is 1-generated. To describe what kind of operations may define minimal clones, we introduce several names.

DEFINITION. Let A be a fixed set. A ternary operation f on A is called a *majority operation* iff it satisfies the identities

$$f(x,x,y) = f(x,y,x) = f(y,x,x) = x,$$

a *minority operation* iff it satisfies the identities

$$f(x,x,y) = f(x,y,x) = f(y,x,x) = y,$$

and a *2/3-minority operation* iff it satisfies the identities

$$f(x,x,y) = f(y,x,y) = f(y,x,x) = y.$$

For $k \geq 3$ and $1 \leq i \leq k$, a k-ary operation g on A is called a *k-ary semiprojection onto* the *i-th variable*, or an *i-th k-ary semiprojection*, iff it satisfies all identities

$$g(x_{j_1},\ldots,x_{j_k}) = x_{j_i}$$

such that $j_1,\ldots,j_k \in \{1,\ldots,k-1\}$.

PROPOSITION 1.12. *Every nontrivial algebra* $\mathcal{A} = (A;F)$ *has a term operation of one of the following types:*

(I) *a nonidentical unary operation,*

(II) *a binary idempotent operation distinct from the projections,*

(III) *a ternary majority operation,*

(IV) *a ternary minority operation, or*

(V) *for some* $k \geq 3$, *a* k*-ary semiprojection which is not a projection.*

PROOF. Select a term operation f of $\mathcal{A}$ so that f is not a projection, and the arity k of f is the least possible. If $k = 1$, then we have case (I). If $k \geq 2$, then by the choice of f

(1.1) every operation arising from f by identification of some variables is a projection.

Thus, in case $k = 2$, f is of type (II). Assume now $k = 3$. By (1.1), f satisfies one of the identities $f(x,x,y) = x$ or $f(x,x,y) = y$, and similarly for $f(x,y,x)$ and $f(y,x,x)$. This leads to eight possible systems of identities describing the behaviour of f under identification of variables. One of them means that f is a majority operation, another one that f is a minority operation, and three others that f is a first, second or third semiprojection, respectively The remaining three sets of identities yield that f itself, or an operation arising from f by permuting its variables is a 2/3-minority operation. In this case, it is easy to produce a majority term operation. Indeed, if f is a 2/3-minority operation, then $f(x,f(x,y,z),z)$ is a majority operation. Therefore we are done if $k = 3$. Finally, the case $k \geq 4$ is settled by the following result often referred to as Świerczkowski's Lemma (cf. S. Świerczkowski [1960-61]).

LEMMA 1.13. *Every at least quaternary operation with property* (1.1) *is a semiprojection.*

PROOF. Let f be a k-ary ($k \geq 4$) operation on A satisfying (1.1). We may assume without loss of generality that $|A| > 1$. Since both of the $(k-1)$-ary operations $f(x,x,x_3,\ldots,x_k)$ and $f(x_1,x_2,x,x,x_5,\ldots,x_k)$ are projections, looking at the operation $f(y,y,z,z,x_5,\ldots,x_k)$ we can see that one of them is a projection onto a variable distinct from x. So, permuting the variables of f we can suppose that f satisfies the identity $f(x_1,x,x,x_4,\ldots,x_k) = x_1$. Taking into account property (1.1) we conclude that the identity

$$f(x_1,x_2,\ldots,x_{i-1},x,x_{i+1},\ldots,x_{j-1},x,x_{j+1},\ldots,x_k) = x_1 \tag{1.2}$$

holds for all $2 \leq i < j \leq k$, as in view of $f(x_1,y,\ldots,y) = x_1$ the operation on the left hand side of (1.2) can be no other projection. Similarly, making use of

(1.2) and $k \geq 4$, we also get that the identity

$$f(x,x_2,\ldots,x_{i-1},x,x_{i+1},\ldots,x_k) = x$$

holds for all $2 \leq i \leq k$. Thus f is a first semiprojection.

Proposition 1.12 yields the result mentioned above on the minimal clones.

COROLLARY 1.14. *Every nontrivial clone on a finite base set* A *contains a minimal clone. Furthermore, there are only a finite number of minimal clones on* A, *and each of them is generated by an operation of one of the types* (I)-(V).

PROOF. Observe that on the finite set A, every k-ary semiprojection with $k > |A|$ is a projection. Therefore the operations (I)-(V) on A are finite in number. Proposition 1.12 implies that every minimal clone is generated by one of these operations, and hence there are only finitely many of them. On the other hand, since by Proposition 1.12 every nontrivial clone on A contains a clone generated by one of the operations (I)-(V), the finiteness ensures that every nontrivial clone contains a minimal one, as well.

We note that all the five types do indeed occur among the minimal clones.

EXAMPLES. Let A be an arbitrary set, $|A| \geq 2$.

(I) If $f \neq id_A$ is a unary operation on A such that $f^2 = f$ or $f^q = id_A$ for some prime q, then $[f]$ is a minimal clone. In fact, it is easy to see that every minimal clone of type (I) on a finite set A is of one of these forms.

(II) If $(A;\cdot)$ is a semilattice (that is a commutative, idempotent semigroup), then its clone is minimal.

(III) The *dual discriminator* d on A is the operation defined by

$$d(a,b,c) = \begin{cases} a & \text{if } a = b \\ c & \text{otherwise} \end{cases} \qquad (a,b,c \in A).$$

It is not hard to show that $[d]$ is a minimal clone. (For $|A| \geq 5$ this follows also from the results of Chapter 5.)

(IV) If $(A;+,0)$ is an Abelian group of exponent 2, then $[x + y + z]$ is a minimal clone.

(V) Let A be finite, $|A| = n \geq 3$, and define an n-ary operation ℓ_n on A as follows:

$$\ell_n(a_1,\ldots,a_n) = \begin{cases} a_n & \text{if } \{a_1,\ldots,a_n\} = A \\ a_1 & \text{otherwise} \end{cases} \qquad (a_1,\ldots,a_n \in A).$$

It can be proved that $[\ell_n]$ is a minimal clone. (Again, for $n \geq 5$ this follows also from the results of Chapter 5.)

The results summarized in Proposition 1.12 and Corollary 1.14 have been around for some time, and were used implicitly in a number of papers, perhaps for the first time in B. Csákány [1980]. An improved version of Corollary 1.14, to be discussed in Chapter 2, which states that every minimal clone of type (IV) is of the form mentioned in the example above was discovered recently by I. G. Rosenberg [a]. So the minimal clones that need further investigation are those of types (II), (III) and (V). All minimal clones are explicitly described only for $|A| = 2$ (an easy exercise, using Corollary 1.14) and for $|A| = 3$ (B. Csákány [1983a],[1983b]).

Let us turn now to the maximal clones. More generally, we discuss the maximal subclones of arbitrary clones on finite sets. The main result is the following characterization of finitely generated clones (S. V. Yablonskiĭ [1958]).

PROPOSITION 1.15. *For a clone C on a finite set, the following conditions are equivalent:*

(i) *C is finitely generated;*

(ii) *every proper subclone of C is contained in a maximal subclone of*

C, and the maximal subclones of C are finite in number.

The proof is based on a lemma.

LEMMA 1.16. *Let C be a clone on a finite set, and let $T \subset C^{(n)}$ for some $n \geq 1$. Then C has at most one maximal subclone $\mathcal{D}$ such that $\mathcal{D}^{(n)} = T$.*

PROOF. Let $\mathcal{D}$ be a maximal subclone of C with $\mathcal{D}^{(n)} = T$. Applying Proposition 1.3 for the algebra $(A;\mathcal{D})$ and Lemma 1.2 for $\mathcal{D}^{(n)}$, respectively, we get that

$$\mathcal{D} \subseteq \mathrm{Pol}_A X_{\mathcal{D}^{(n)}} \quad \text{and} \quad \mathrm{Pol}_A^{(n)} X_{\mathcal{D}^{(n)}} = \mathcal{D}^{(n)}.$$

Thus, since $\mathcal{D}^{(n)} = T \subset C^{(n)}$ and $\mathcal{D} \subseteq C$, we have

$$\mathcal{D} \subseteq C \cap \mathrm{Pol}_A X_T \subset C.$$

The maximality of $\mathcal{D}$ implies then that $\mathcal{D} = C \cap \mathrm{Pol}_A X_T$, hence $\mathcal{D}$ is uniquely determined by T.

PROOF of Proposition 1.15. The implication (ii) $\Rightarrow$ (i) is trivial, as every subset of C containing for each maximal subclone $\mathcal{D}$ of C an operation outside $\mathcal{D}$, generates C. Conversely, suppose (i) holds. Then the first part of (ii) is an immediate consequence of Zorn's Lemma. Furthermore, there exists a natural number $n \geq 1$ such that $[C^{(n)}] = C$. Clearly, $\mathcal{D}^{(n)} \subset C^{(n)}$ holds for every maximal subclone $\mathcal{D}$ of C. By Lemma 1.16, $\mathcal{D}$ is uniquely determined by $\mathcal{D}^{(n)}$, so the number of maximal subclones of C does not exceed $2^{|C^{(n)}|}$. However, $C^{(n)}$ is finite, as the base set is finite.

To get the required results for the maximal clones on a finite set A it suffices by Proposition 1.15 to show that $\mathcal{O}_A$ is finitely generated. This can be done, for example, by considering finite algebras which mimic the 2-element Boolean algebra.

DEFINITION. The *Post algebra* of order n is the algebra

$\mathfrak{P}_n = (\{0,\ldots,n-1\}; \wedge,\vee,r,0,1)$ where $\wedge$, $\vee$ denote meet and join with respect to the order $0 \le n-1 \le n-2 \le \ldots \le 2 \le 1$ and r is the cyclic permutation $(0\ 1\ \ldots\ n-1)$.

Obviously, $\mathfrak{P}_2$ is the 2-element Boolean algebra.

EXERCISE 1.17. $T(\mathfrak{P}_n) = C_{\{0,\ldots,n-1\}}$ holds for every integer $n \ge 1$. (Hint: Represent every operation in a form similar to the disjunctive normal form for the term operations of the 2-element Boolean algebra, or apply Corollary 1.25 to be proved in the next section.)

Thus we have

COROLLARY 1.18. *Let* A *be a finite set. Every proper subclone of* C_A *is contained in a maximal clone on* A, *and the maximal clones on* A *are finite in number.*

Contrary to the minimal clones, the maximal clones are known on every finite set A. The deep theorem explicitly describing all maximal clones on A is due to I. G. Rosenberg [1965], [1970]. The special cases $|A| = 2$, 3 and 4 were settled earlier by E. L. Post [1941], S. V. Yablonskiĭ [1958], and A. I. Mal'tsev [unpublished], respectively. A new proof for Rosenberg's Theorem was found by R. W. Quackenbush [1981] (see also the book [MMPT]). Here we include the theorem without proof.

It is clear that every maximal clone on a finite set A is of the form $\mathrm{Pol}_A\{B\}$ for some subset B of a finite power of A. So the description of the maximal clones amounts to the determination of the corresponding sets B. We need some definitions. A subset B of A^k is called *totally reflexive* (in case $k = 2$ *reflexive*) iff it contains every k-tuple $(a_1,\ldots,a_k) \in A^k$ with $|\{a_1,\ldots,a_k\}| < k$, and *totally symmetric* iff $(a_{1\pi},\ldots,a_{k\pi}) \in B$ for every k-tuple $(a_1,\ldots,a_k) \in B$ and every permutation π of $\{1,\ldots,k\}$. A totally reflexive,

totally symmetric subset B of A^k is termed *central* iff $B \neq A^k$ and there is an element $c \in A$ such that $\{c\} \times A^{k-1} \subseteq B$. (Note that every nonempty proper subset of A is central.) For $3 \leq k \leq |A|$, a set $T = \{\theta_1,\ldots,\theta_\ell\}$ $(\ell \geq 1)$ of equivalence relations on A is called k-*regular* iff each θ_i $(1 \leq i \leq \ell)$ has exactly k equivalence classes and the intersection $\bigcap_{i=1}^{\ell} \varepsilon_i$ of arbitrary equivalence classes ε_i of θ_i is nonempty. The *subset of* A^k *determined by* T consists of all k-tuples $(a_1,\ldots,a_k) \in A^k$ having the property that for each $1 \leq j \leq \ell$ at least two of the elements $a_1,\ldots,a_k$ are equivalent modulo θ_j. A partial order on A is said to be *bounded* iff there are a least element and a greatest element as well.

Now we can formulate Rosenberg's Theorem.

THEOREM 1.19. *The maximal clones on a finite set* A *are exactly the clones of the form* $\mathrm{Pol}_A\{B\}$ *where*

(α) $B \subseteq A^2$ *is a bounded partial order on* A; *or*

(β) $B = \pi^{\square}$ *where* π *is a fixed point free permutation of* A *with* $\pi^q = \mathrm{id}_A$ *for some prime* q; *or*

(γ) $B = (x-y+z)^{\square}$ *with* $(A;+,-,0)$ *an Abelian group of exponent* q *for some prime* q; *or*

(δ) $B \subseteq A^2$ *is a nontrivial equivalence relation on* A; *or*

(ε) B *is a central subset of* A^k $(1 \leq k < |A|)$; *or*

(ζ) B *is the subset of* A^k *determined by a* k-*regular family of equivalence relations on* A $(3 \leq k \leq |A|)$.

DEFINITION. An algebra $\mathcal{A} = (A;F)$ is called *primal* iff $\mathcal{A}$ is finite and every operation on A is a term operation of $\mathcal{A}$.

Corollary 1.18 and Theorem 1.19 immediately imply

COROLLARY 1.20. *A finite algebra* $\mathcal{A} = (A;F)$ *is primal if and only if*

no set of types (α)-(ζ) *is among the subuniverses of finite powers of* $\mathcal{A}$.

If we want to generalize the concept of primality to infinite algebras $\mathcal{A} = (A;F)$, we have two possibilities: we may require either the clone of term operations or the clone of local term operations of $\mathcal{A}$ to be equal to O_A. However, as $|O_A| > \aleph_0$ if A is infinite, no infinite algebra of finite (or countable) type can satisfy the first condition. Therefore we consider local term operations, and call an algebra $\mathcal{A} = (A;F)$ *locally primal* iff every operation on A is a local term operation of $\mathcal{A}$. Interestingly, in spite of the fact that the lattice of locally closed clones on an infinite set A is not dually atomic, a characterization similar to (but weaker than) Corollary 1.20 can be proved for locally primal algebras as well (I. G. Rosenberg, L. Szabó [1984]).

Clones containing special operations

Although varieties of algebras will not be considered in these notes, it should be mentioned that the existence of certain operations among the term operations of an algebra $\mathcal{A}$ is closely related to properties of the variety $V(\mathcal{A})$ generated by $\mathcal{A}$.

DEFINITION. A ternary operation p satisfying the identities

$$p(x,y,y) = p(y,y,x) = x$$

is called a *Mal'tsev operation*.

In particular, minority and 2/3-minority operations introduced earlier are special Mal'tsev operations. The name refers to a theorem of A. I. Mal'tsev [1954] (see also [BS], [G], [MMPT]) stating that an algebra $\mathcal{A}$ has a Mal'tsev operation among its term operations if and only if the variety $V(\mathcal{A})$ is congruence permutable (that is, every algebra $\mathcal{B} \in V(\mathcal{A})$ has permutable congruences). Mal'tsev's Theorem was the first result of this nature, characterizing some

property of varieties by the existence of terms satisfying certain identities. Since then an abundance of such theorems, called Mal'tsev conditions, were discovered, of which we mention only those playing a role here. A. F. Pixley [1963] proved that an algebra $\mathcal{A}$ has a Mal'tsev operation as well as a majority operation among its term operations if and only if the variety $V(\mathcal{A})$ generated by $\mathcal{A}$ is arithmetical (that is, for every algebra $\mathcal{B} \in V(\mathcal{A})$ the congruence lattice of $\mathcal{B}$ is distributive and $\mathcal{B}$ has permutable congruences). For a majority operation alone, a similar theorem does not hold. In fact, it follows that the existence of a majority operation among the term operations of $\mathcal{A}$ implies that the congruence lattice of every algebra $\mathcal{B} \in V(\mathcal{A})$ is distributive, however, the converse is not true. The Mal'tsev condition characterizing congruence distributivity was found by B. Jónsson [1967] (see [BS] or [G; p. 221]).

DEFINITION. An algebra will be called a *Mal'tsev algebra* [*majority algebra, arithmetical algebra*] iff it has a Mal'tsev operation [majority operation, or both, respectively] among its term operations.

EXAMPLES. 1. Groups, rings and modules are Mal'tsev algebras.

2. Every lattice is a majority algebra.

3. Boolean algebras, finite fields, and the Post algebras $\mathcal{P}_n$ $(n \geq 1)$ are arithmetical.

Note that an algebra $\mathcal{A}$ is arithmetical if and only if it has a 2/3-minority term operation. Indeed, if p is a Mal'tsev operation and f is a majority operation, then $f(x,p(x,y,z),z)$ is a 2/3-minority operation; and conversely, if g is a 2/3-minority operation, then it is also a Mal'tsev operation and $g(x,g(x,y,z),z)$ is a majority operation.

Quasigroups provide an important and wide class of examples of Mal'tsev algebras. Let A be a set. A groupoid $(A;\cdot)$ is called a *quasigroup*, or $\cdot$ is

called a *quasigroup operation*, iff the unary operations ax and xa are permutations of A for all $a \in A$. It is easy to see that this condition on $\cdot$ is equivalent to requiring that there exist binary operations $\backslash$ and $/$ on A such that the identities

$$x\backslash(xy) = y, \quad x(x\backslash y) = y, \quad (xy)/y = x, \quad (x/y)y = x$$

are satisfied. Clearly, $\backslash$ and $/$ are uniquely determined. They are called the *left* and *right divisions*, respectively, corresponding to $\cdot$. The above identities immediately imply that the term operation

$$p(x,y,z) = (x/x)\backslash((x/y)z)$$

of $(A;\cdot,\backslash,/)$ is a Mal'tsev operation, and hence $(A;\cdot,\backslash,/)$ is a Mal'tsev algebra. Indeed, the identity $p(x,x,z) = z$ is obvious, while the other one can be proved as follows:

$$p(x,y,y) = (x/x)\backslash((x/y)y) = (x/x)\backslash x = (x/x)\backslash((x/x)x) = x.$$

A stronger claim is true if A is finite.

PROPOSITION 1.21. *If $(A;\cdot)$ is a finite quasigroup, then the left and right divisions corresponding to $\cdot$ are term operations of $(A;\cdot)$. Consequently every finite quasigroup is a Mal'tsev algebra.*

PROOF. For every integer $k \geq 1$ define a binary term operation $f^{(k)}$ of $(A;\cdot)$ as follows:

$$f^{(k)}(x,y) = \underbrace{x(x(\ldots(xy)\ldots))}_{k \text{ times}}.$$

Since ay is a permutation of A for all $a \in A$, we get the identity $f^{(|A|!)}(x,y) = y$. Hence $x\backslash y = f^{(|A|!-1)}(x,y)$ is the left division corresponding to $\cdot$. The argument for the right division is symmetric.

Next we discuss an important theorem of K. A. Baker and A. F. Pixley [1975] on a class of algebras including majority algebras.

DEFINITION. For $m \geq 3$, an m-ary operation f satisfying the identities

$$f(y,x,\ldots,x) = f(x,y,x,\ldots,x) = \ldots = f(x,\ldots,x,y) = x$$

is called an m-ary *near-unanimity operation*.

Clearly, the ternary near-unanimity operations are exactly the majority operations.

THEOREM 1.22. *Let* $\mathcal{A} = (A;F)$ *be an algebra having an* m*-ary near-unanimity operation among its term operations* $(m \geq 3)$. *Then an operation on* A *is a local term operation of* $\mathcal{A}$ *if and only if it preserves all subuniverses of* $\mathcal{A}^{m-1}$.

PROOF. In view of Corollary 1.9 we are done if we show that every operation preserving the subuniverses of $\mathcal{A}^{m-1}$ preserves all subuniverses of finite powers of $\mathcal{A}$. Let g be an n-ary operation preserving all subuniverses of $\mathcal{A}^{m-1}$, and let B be a subuniverse of $\mathcal{A}^k$ $(k \geq 1)$. If $k \leq m-1$, then $B \times A^{m-k-1}$ is a subuniverse of $\mathcal{A}^{m-1}$, and hence is preserved by g. Therefore g preserves B, too. From now on we proceed by induction on k. Assume that $k \geq m$ and g preserves all subuniverses of $\mathcal{A}^{k-1}$. Consider arbitrary elements $b_i = (b_{i1},\ldots,b_{ik})$ $(1 \leq i \leq n)$ of B, and set $c = g(b_1,\ldots,b_n)$, that is, $c = (c_1,\ldots,c_k)$ with $c_j = g(b_{1j},\ldots,b_{nj})$ $(1 \leq j \leq k)$. We have to prove that $c \in B$. Since g preserves the subuniverse $B^{(1)} = \mathrm{pr}_{2,\ldots,k} B$ of $\mathcal{A}^{k-1}$, we have

$$(c_2,\ldots,c_k) = g((b_{12},\ldots,b_{1k}),\ldots,(b_{n2},\ldots,b_{nk})) \in B^{(1)}.$$

Hence there is an element $a_1 \in A$ such that the k-tuple $c^{(1)} = (a_1,c_2,\ldots,c_k)$ belongs to B. Repeating the same argument for the i-th component $(1 \leq i \leq m)$

we get that there exists an element $a_i \in A$ such that the k-tuple $c^{(i)} = (c_1,\ldots,c_{i-1},a_i,c_{i+1},\ldots,c_k)$ belongs to B. Now, taking into account that there is an m-ary near-unanimity operation f among the term operations of $\mathcal{A}$, we conclude that $c = f(c^{(1)},c^{(2)},\ldots,c^{(m)}) \in B$, as required.

COROLLARY 1.23. *Let $\mathcal{A} = (A;F)$ be a finite algebra having an m-ary near-unanimity operation among its term operations* $(m \geq 3)$. *Then an operation on A is a term operation of $\mathcal{A}$ if and only if it preserves all subuniverses of $\mathcal{A}^{m-1}$.*

In the most important special case, when $m = 3$, we have

COROLLARY 1.24. *For a majority algebra $\mathcal{A} = (A;F)$, an operation on A is a local term operation of $\mathcal{A}$ if and only if it preserves all subuniverses of $\mathcal{A}^2$.*

COROLLARY 1.25. *For a finite majority algebra $\mathcal{A} = (A;F)$, an operation on A is a term operation of $\mathcal{A}$ if and only if it preserves all subuniverses of $\mathcal{A}^2$.*

Besides providing an easy test for the term operations of a finite near-unanimity algebra, Corollary 1.23 has another interesting consequence.

COROLLARY 1.26. *On a finite base set, every clone containing a near-unanimity operation is finitely generated.*

PROOF. Let C be a clone on a finite set A, and let f be a near-unanimity operation in C, say f is m-ary $(m \geq 3)$. By Corollary 1.23 every clone $\mathcal{D}$ with $[f] \subseteq \mathcal{D} \subseteq C$ is determined by a set of subsets of A^{m-1}. Hence these clones are finite in number, implying that C is finitely generated.

Finally, we mention a simple fact concerning the subuniverses of $\mathcal{A}^2$ of a Mal'tsev algebra $\mathcal{A}$.

EXERCISE 1.27. For every Mal'tsev algebra $\mathcal{A}$, the reflexive subuniverses of $\mathcal{A}^2$ are exactly the congruences of $\mathcal{A}$. (Cf. the proof of Theorem 4.2.)

The lattice of clones on a 2-element set

Operations on a 2-element set, say $A = \{0,1\}$, are truth functions. In propositional logic it is important to decide whether a truth function is expressible via other given truth functions. This problem was the motivation for E. L. Post's investigations which led him to the full description of the lattice of clones on $\{0,1\}$, announced in E. L. Post [1921] and published in [1941]. Later, the applications in computer science, for example in the synthesis of switching circuits, have increased the significance of these investigations.

E. L. Post's original proof is rather complicated, and involves a lot of computations. Making use of some recent developments in universal algebra, such as for example Corollary 1.23 or the theory of para-primal algebras discussed in Chapter 4, J. Berman [1980] deviced a fairly short proof. However, even this one is too long to be included here. The interested reader can find it in the book [MMPT].

The diagram of the lattice of clones on $A = \{0,1\}$, often called *Post's lattice*, is shown in Figure 1. The dotted lines indicate 8 descending ω-chains, each one followed at the bottom by the meet (= intersection) of the chain.

To describe the clones corresponding to the vertices of the diagram, we have two possibilities. Every clone C on $A = \{0,1\}$ can be described either by a generating set, that is a set $F \subseteq C$ with $C = [F]$, or in view of Corollary 1.4 by a set of invariants, that is a set S of subuniverses of finite powers of $(A;C)$ with $C = \mathrm{Pol}\, S$. Since $[F] = \bigvee_{f \in F} [f]$, it follows that the join irreducible clones are 1-generated, furthermore, it suffices to present a generating

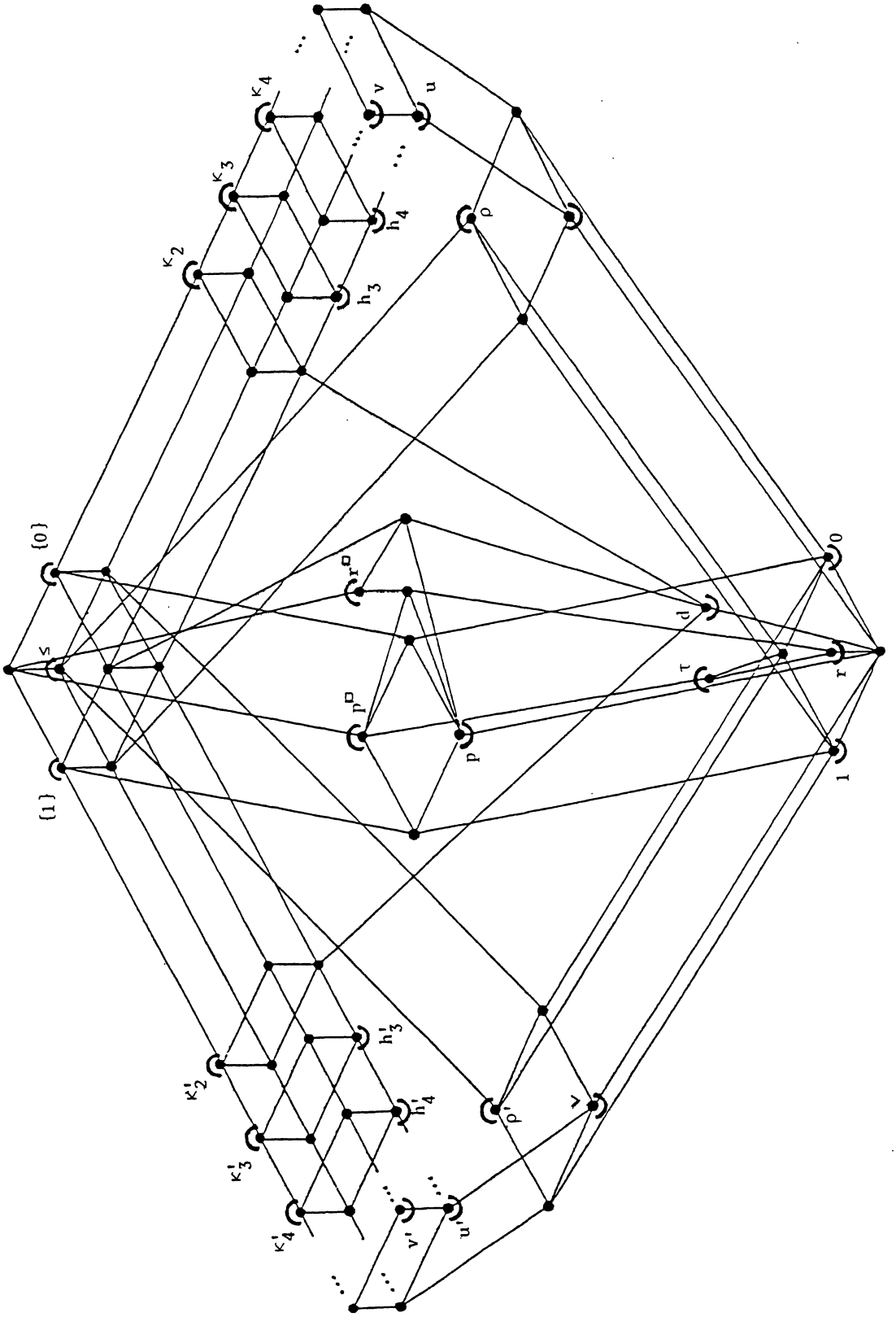


Figure 1. Post's lattice Lat({0,1})

operation for each join irreducible element of Post's lattice. Similarly, as $\mathrm{Pol}\ S = \bigcap_{B \in S} \mathrm{Pol}\ \{B\}$, the meet irreducible clones are determined by a single subuniverse B, and it is enough to present such a subuniverse for each meet irreducible element of the lattice.

Accordingly, in Figure 1, the join irreducible elements of the diagram, denoted by $\cup$, are labelled with the generating operation of the corresponding clone, while the meet irreducible elements, denoted by $\cap$, are labelled with the subuniverse determining the corresponding clone. The notations are as follows: $\cdot$ stands for multiplication modulo 2 (or conjunction), $+$ for addition modulo 2, $\vee$ for disjunction, r for negation, and 0, 1 for the two constants; furthermore,

$$p(x,y,z) = x + y + z,$$

$$d(x,y,z) = xy \vee yz \vee zx \quad \text{(the dual discriminator on } \{0,1\}),$$

$$u(x,y,z) = x(y \vee z), \qquad u'(x,y,z) = x \vee yz,$$

$$v(x,y,z) = u(x,y,r(z)), \qquad v'(x,y,z) = u'(x,y,r(z)),$$

$$h_i(x_1,\ldots,x_{i+1}) = \bigvee_{j=1}^{i+1} x_1 \ldots x_{j-1} x_{j+1} \ldots x_{i+1} \quad (i \geq 3),$$

$$h_i'(x_1,\ldots,x_{i+1}) = \bigvee_{j=1}^{i+1} (x_1 \vee \ldots \vee x_{j-1} \vee x_{j+1} \vee \ldots \vee x_{i+1}) \quad (i \geq 3);$$

$\leq$ denotes the natural order $0 \leq 1$, and

$$\kappa_i = \{0,1\}^i - \{(1,\ldots,1)\}, \quad \kappa_i' = \{0,1\}^i - \{(0,\ldots,0)\} \quad (i \geq 2),$$

$$\rho = \{(0,0,0),(0,0,1),(0,1,0),(1,0,0),(1,1,1)\},$$

$$\rho' = \{(0,0,0),(0,1,1),(1,0,1),(1,1,0),(1,1,1)\},$$

$$\tau = \{a \in \{0,1\}^8 : \text{ exactly } 0, 4, \text{ or } 8 \text{ components of } a \text{ equal } 1\}.$$

In universal algebra, Post's result has the effect that for many considerations, 2-element algebras can be regarded as known. For example, R. C. Lyndon [1951] made essential use of it when he proved that every 2-element algebra has

a finite basis for its identities. The description of the clones on $\{0,1\}$ in terms of invariants provides a quick and easy algorithm to decide whether two given algebras on $\{0,1\}$ are term equivalent, or one is a reduct of the other, etc.

Finally, it should be pointed out that Post's result is unique in that nothing similar can be expected for any of the clone lattices $\mathrm{Lat}(A)$ with $|A| > 2$. Yu. I. Yanov and A. A. Muchnik [1959] proved that $|\mathrm{Lat}(A)| = 2^{\aleph_0}$ if A is finite, $|A| > 2$, while a result of I. G. Rosenberg [1976] shows that $|\mathrm{Lat}(A)| = 2^{2^{|A|}}$ if A is infinite. (Moreover, in the latter case even the maximal clones are $2^{2^{|A|}}$ in number.) Compared to $\mathrm{Lat}(\{0,1\})$, rather little is known about the lattices $\mathrm{Lat}(A)$ when A is finite, $|A| > 2$, and even less when A is infinite. Nevertheless, most results to be discussed here yield a piece of information on $\mathrm{Lat}(A)$.

Chapter 2

AFFINE AND SEMI-AFFINE ALGEBRAS

Affine algebras are a special kind of Mal'tsev algebras which, during the last decade, turned out to play an important role in universal algebra. Before the definition we state a simple proposition.

PROPOSITION 2.1. *For an arbitrary Abelian group* $\underline{A} = (A;+,-,0)$ *and for every operation* f *on* A *the following conditions are equivalent:*

(i) $(x-y+z)^{\square}$ *is a subuniverse of* $(A;f)^4$;

(ii) f *commutes with the ternary operation* $x - y + z$;

(iii) $f(u+v) + f(\underline{0}) = f(u) + f(v)$ *holds for all* $u,v \in A^n$, *where* n *is the arity of* f *and* $\underline{0} = (0,\ldots,0)$;

(iv) f *is a polynomial operation of the unitary* (End $\underline{A}$)*-module* (End $\underline{A}$)$\underline{A}$ = $(A;+,-,0,\text{End }\underline{A})$, *where* End $\underline{A}$ *is the endomorphism ring of* $\underline{A}$.

PROOF. (i) $\Leftrightarrow$ (ii) holds by definition. The implications (ii) $\Rightarrow$ (iii), (iv) $\Rightarrow$ (i) are straightforward, the reader can verify them without difficulty. To establish (iii) $\Rightarrow$ (iv) consider the operation $f^{\circ}(x_1,\ldots,x_n) = f(x_1,\ldots,x_n) - f(\underline{0})$. Then

$$f^{\circ}(u+v) = f^{\circ}(u) + f^{\circ}(v) \quad \text{for all} \quad u,v \in A^n,$$

implying that

$$f^{\circ}(x_1,\ldots,x_n) = \sum_{i=1}^{n} f^{\circ}(0,\ldots,0,\overset{i}{\check{x}}_i,0,\ldots,0) \quad \text{for all} \quad x_1,\ldots,x_n \in A,$$

where each summand, considered as a function of x_i, is an endomorphism of $\underline{A}$.

DEFINITION. Let $\underline{A} = (A;+,-,0)$ be an Abelian group. The operations satisfying the equivalent conditions of the preceding proposition are said to be *affine with respect to* $\underline{A}$. The set of these operations will be denoted by $A(\underline{A})$.

It is clear from (iv) that $A(\underline{A})$ is a clone, namely $A(\underline{A}) = P_{(\text{End } \underline{A})}\underline{A}$. In accordance with the notation commonly used for modules, the members of $A(\underline{A})$ will be written in the form

$$\sum_{i=1}^{n} r_i x_i + a \quad \text{with} \quad a \in A \quad \text{and} \quad r_1,\ldots,r_n \in \text{End } \underline{A}.$$

DEFINITION. An algebra $\mathcal{A} = (A;F)$ is called *affine* iff there exists an Abelian group $\underline{A} = (A;+,-,0)$ such that

(a) $x - y + z$ is a term operation of $\mathcal{A}$, and

(b) every basic operation (and hence every polynomial operation) of $\mathcal{A}$ is affine with respect to $\underline{A}$.

Since $x - y + z$ is a Mal'tsev operation, every affine algebra is indeed a Mal'tsev algebra. Furthermore, as $x - y + z$ is easily seen to be the only Mal'tsev operation in $A(\underline{A})$, it follows that every affine algebra has a unique Mal'tsev operation among its term operations.

EXAMPLES. 1. Abelian groups and, more generally, modules are affine algebras.

2. If C is a maximal clone of type (γ) on a finite set A (cf. Theorem 1.19), then $(A;C)$ is an affine algebra.

3. A group is an affine algebra if and only if it is Abelian.

4. A ring is an affine algebra if and only if it is a zero ring.

The concept of affine algebras was introduced by R. McKenzie [1976] in connection with his investigations on locally finite, minimal, congruence permutable varieties. The so-called term condition (TC), which later turned out to play a significant role in the representation problem for congruence lattices (see R. McKenzie [1983] and the references there) as well as in commutator theory (see R. Freese and R. McKenzie [a]), was defined in the same paper, although it appeared also in H. Werner [1974].

DEFINITION. An algebra $\mathcal{A} = (A;F)$ is said to be a TC-*algebra* iff for every $n \geq 1$, for every n-ary term operation f of $\mathcal{A}$ and for arbitrary elements $u,v \in A$ and $(n-1)$-tuples $a,b \in A^{n-1}$,

(TC) $\quad f(u,a) = f(u,b)$ holds if and only if $f(v,a) = f(v,b)$ does.

Notice that the requirement (TC) for all $f \in T(\mathcal{A})$ implies that the same holds for all $f \in P(\mathcal{A})$ as well. It is easy to see that $\mathcal{A}$ is a TC-algebra if and only if Δ_A is a congruence class of a congruence of $\mathcal{A}^2$.

EXAMPLE. Affine algebras and unary algebras are TC-algebras.

Affine algebras

As we mentioned earlier, affine algebras have a unique Mal'tsev operation among their term operations, namely the term operation $x - y + z$ of the corresponding Abelian group. Since this operation is crucial in establishing the affineness of an algebra, it is useful to find necessary and sufficient conditions ensuring that a Mal'tsev operation be of this form.

PROPOSITION 2.2. *For a Mal'tsev operation* p *on a set* A *the following conditions are equivalent:*

(i) *there exists an Abelian group* $(A;+,-,0)$ *such that* $p(x,y,z) = x - y + z$;

(ii) p *commutes with itself;*

(iii) p *satisfies the identities*

(2.1) $$p(x,y,z) = p(z,y,x),$$

(2.2) $$p(p(x,y,z),z,u) = p(x,y,u).$$

PROOF. (i) $\Rightarrow$ (ii) is trivial.

(ii) $\Rightarrow$ (iii). A direct application of Mal'tsev's identities and the commutativity yields that

$$\begin{aligned} p(x,y,z) &= p(p(y,y,x),p(y,y,y),p(z,y,y)) \\ &= p(p(y,y,z),p(y,y,y),p(x,y,y)) = p(z,y,x), \end{aligned}$$

$$\begin{aligned} p(p(x,y,z),z,u) &= p(p(x,y,z),p(z,z,z),p(z,z,u)) \\ &= p(p(x,z,z),p(y,z,z),p(z,z,u)) = p(x,y,u). \end{aligned}$$

(iii) $\Rightarrow$ (i). Choose an element $0 \in A$ arbitrarily, and define operations $+$ and $-$ on A by

$$x + y = p(x,0,y) \quad \text{and} \quad -x = p(0,x,0).$$

Then $+$ is commutative by (2.1), and 0 is a neutral element for $+$. Now using (2.1) and (2.2) we get that

(2.3) $$x + (-y) = (-y) + x = p(p(0,y,0),0,x) = p(0,y,x) = p(x,y,0),$$

in particular, $x + (-x) = p(x,x,0) = 0$, whence also

$$-(-x) = p(0,-x,0) = p(x+(-x),-x,0) = p(p(x,0,-x),-x,0) = x.$$

Furthermore, (2.3) implies that

$$(x + (-y)) + z = p(p(x,y,0),0,z) = p(x,y,z),$$

thus

$$(x + (-y)) + z = p(x,y,z) = p(z,y,x) = (z + (-y)) + x = x + ((-y) + z).$$

Since we have $-(-y) = y$, it follows that $+$ is associative. Hence $(A;+,-,0)$

is an Abelian group and $p(x,y,z) = x - y + z$.

Clearly, minority operations are special Mal'tsev operations, and a Mal'tsev operation arising from an Abelian group is a minority operation if and only if the group is of exponent 2.

COROLLARY 2.3. *Let* p *be a minority operation on a set* A $(|A| \geq 2)$ *such that every semiprojection in the clone* $[p]$ *is a projection. Then there exists an Abelian group* $(A;+,0)$ *of exponent* 2 *such that* $p(x,y,z) = x + y + z$.

PROOF. First we show that p is the unique minority operation in $[p]$. For arbitrary minority operations $p_1, p_2 \in [p]$ the ternary operation

$$p_1(p_2(x,y,z),z,y) \tag{2.4}$$

is a semiprojection onto x, hence by assumption it is a projection onto x, that is the identity

$$p_1(p_2(x,y,z),z,y) = x \tag{2.5}$$

holds. Thus, applying (2.5) for the pairs p_1,p_2 and p_1,p_1, respectively, we get

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

This immediately implies that (2.1) as well as the identity $p(x,y,z) = p(y,x,z)$ hold for p. To prove (2.2) we consider the quaternary operation

$$p(p(p(x,y,z),z,u),u,y), \tag{2.6}$$

and check, using (2.5), that it is a semiprojection onto x. Consequently, we have the identity

$$p(p(p(x,y,z),z,u),u,y) = x.$$

Substituting both sides for x in $p(x,y,u)$ and applying (2.5) we get (2.2). Therefore, Proposition 2.2 implies the existence of an Abelian group $(A;+,-,0)$

with $p(x,y,z) = x - y + z$, which is necessarily of exponent 2 as $2x = p(x,0,x) = 0$.

Notice that a clone generated by a semiprojection can never contain a minority operation if the base set A has at least two elements, as every semiprojection preserves the sets $\{(a,a),(a,b),(b,b)\} \subseteq A^2$ $(a \neq b)$, whereas no minority operation does. So Corollary 2.3 implies the result of I. G. Rosenberg [a] mentioned in Chapter 1, which states that a minority operation p on a set A generates a minimal clone only if $p(x,y,z) = x + y + z$ for some Abelian group $(A;+,0)$ of exponent 2.

Applying Proposition 2.2 we can prove several useful characterizations for affine algebras.

THEOREM 2.4. *For every Mal'tsev algebra* $\mathcal{A} = (A;F)$ *the following conditions are equivalent:*

(i) $\mathcal{A}$ *is an affine algebra;*

(ii) $\mathcal{A}$ *has a Mal'tsev term operation* p *commuting with the basic operations (hence with all term operations) of* $\mathcal{A}$*;*

(iii) $\mathcal{A}$ *is a* TC*-algebra;*

(iv) *the first projection is the only polynomial operation* s *of* $\mathcal{A}$ *which satisfies the identities*

$$s(x,y,y) = s(x,x,y) = x; \tag{2.7}$$

(v) *for every natural number* $n \geq 3$, *the first projection is the only* n*-ary term operation* s *of* $\mathcal{A}$ *which satisfies the identities*

$$s(x,y,y,x_4,\ldots,x_n) = s(x,x,y,x_4,\ldots,x_n) = x; \tag{2.8}$$

(vi) $\mathcal{A}$ *has a Mal'tsev term operation* p *satisfying the identity*

$$p(p(x,y,z),z,y) = x, \tag{2.9}$$

and p *is the unique Mal'tsev operation among the polynomial operations of* $\mathcal{A}$*;*

(vii) $\mathcal{A}$ *has a Mal'tsev term operation* p *satisfying the identity* (2.9), *and for every natural number* $n \geq 3$, p *with* $n - 3$ *fictitious variables added is the unique* n*-ary term operation* q *of* $\mathcal{A}$ *satisfying the identities*

$$q(x,x,y,x_4,\ldots,x_n) = q(y,x,x,x_4,\ldots,x_n) = y. \tag{2.10}$$

PROOF. The implication (i) $\Rightarrow$ (ii) is obvious, while (ii) $\Rightarrow$ (i) follows easily from Propositions 2.1, 2.2 and 1.1(a). The implication (i) $\Rightarrow$ (iii), which was mentioned earlier, can also be verified without difficulty.

We now show that (iii) $\Rightarrow$ (iv). Assume $\mathcal{A}$ is a TC-algebra and (2.7) holds for some $s \in P(\mathcal{A})$. Since

$$s(a,b,b) = a = s(a,a,b) \quad \text{for every} \quad a,b \in A,$$

the condition (TC) implies

$$s(a,b,c) = s(a,a,c) = a \quad \text{for every} \quad a,b,c \in A,$$

that is, s is the first projection.

The implication (iv) $\Rightarrow$ (v) is straightforward, noticing that for arbitrary $s \in T(\mathcal{A})$ satisfying (2.8), all operations $s(x,y,z,a_4,\ldots,a_n) \in P(\mathcal{A})$ $(a_4,\ldots,a_n \in A)$ satisfy (2.7). Similarly, (vi) $\Rightarrow$ (vii). It is an easy consequence of Proposition 2.1 that the algebra $(A;P(\mathcal{A}))$ is affine with respect to $\underline{A}$ provided $\mathcal{A}$ is such. Therefore (i) $\Rightarrow$ (vi). So the proof will be complete if we show that (v) $\Rightarrow$ (vii) $\Rightarrow$ (i).

Assume (v). For every $n \geq 3$ and for arbitrary n-ary operations $q_1,q_2 \in T(\mathcal{A})$ satisfying (2.10) the n-ary operation

$$q_1(q_2(x,y,z,x_4,\ldots,x_n),z,y,x_4,\ldots,x_n)$$

satisfies (2.8), and hence the identity

$$q_1(q_2(x,y,z,x_4,\ldots,x_n),z,y,x_4,\ldots,x_n) = x$$

holds. Applying it for the pairs q_1,q_2 and q_1,q_1, respectively, we get

$$q_1(x,y,z,x_4,\ldots,x_n) = q_1(q_1(q_2(x,y,z,x_4,\ldots,x_n),z,y,x_4,\ldots,x_n),y,z,x_4,\ldots,x_n)$$
$$= q_2(x,y,z,x_4,\ldots,x_n).$$

The ternary operation on the left hand side of (2.9) also satisfies the identities (2.8), whence (2.9) follows. Thus (v) $\Rightarrow$ (vii).

The most difficult part of the proof is to establish (vii) $\Rightarrow$ (i). First we show that (vii) implies the following property stronger than (v):

(v)' *for every natural number* $n \geq 3$, *the first projection is the only* n-*ary term operation* s *of* $\mathcal{A}$ *which satisfies the identities* (2.8), *or*

(2.8)' $$s(x,y,x,x_4,\ldots,x_n) = s(x,x,y,x_4,\ldots,x_n) = x.$$

Observe that for arbitrary, say k-ary, operations $f,g,h \in T(\mathcal{A})$,

(2.11) $$p(f,g,h) = h \text{ implies } f = g,$$

since by (2.9), $g = p(h,h,g) = p(p(f,g,h),h,g) = f$. Let now $s \in T(\mathcal{A})$ satisfy (2.8) or (2.8)', and consider the operation

$$q(x,y,z,x_4,\ldots,x_n) = p(s(x,y,z,x_4,\ldots,x_n),x,p(x,y,z))$$

or

$$q(x,y,z,x_4,\ldots,x_n) = p(s(y,x,z,x_4,\ldots,x_n),y,p(x,y,z)),$$

respectively. It is easy to check that q satisfies (2.10), whence by assumption we get the identity $q(x,y,z,x_4,\ldots,x_n) = p(x,y,z)$. Thus (2.11) yields that s is the first projection.

It is easy to see that (2.1)-(2.2) hold for p. (2.1) is an immediate consequence of the uniqueness of Mal'tsev operations. In view of (2.9) the operation (2.6) satisfies the identities (2.8), so it follows, like in the proof of Corollary 2.3, that (2.2) holds for p. Thus, by Proposition 2.2, there exists an Abelian group $\underline{A} = (A;+,-,0)$ such that $p(x,y,z) = x - y + z$. We are done if we

prove the sufficiency part of the following claim, since the identities required below include (2.8)'.

Claim 1. Let $\mathcal{A} = (A;F)$ be an algebra and $\underline{A} = (A;+,-,0)$ an Abelian group such that $x - y + z$ is a term operation of $\mathcal{A}$. Then $\mathcal{A}$ is affine with respect to $\underline{A}$ if and only if for every natural number $n \geq 3$, the first projection is the only n-ary term operation s of $\mathcal{A}$ which satisfies the identities

$$s(z,x_2,\ldots,x_{i-1},z,x_{i+1},\ldots,x_n) = z \quad \text{for all} \quad 2 \leq i \leq n.$$

The necessity is straightforward to check. Conversely, assume that the conditions of Claim 1 hold for the term operations of $\mathcal{A}$. We show that for every natural number $k \geq 3$, the first projection is the only k-ary term operation $u(z,x_2,\ldots,x_k)$ of $\mathcal{A}$ which satisfies the identities

$$u(z,z,\ldots,z,\overset{i}{\breve{x}},z,\ldots,z) = z \quad \text{for all} \quad 2 \leq i \leq k. \tag{2.12}$$

Suppose not, and consider an operation $u \in T(\mathcal{A})$ satisfying (2.12) which is not the first projection. Clearly, u cannot be any other projection, either. Select a minimal subset X of $\{x_2,\ldots,x_k\}$ such that the operation arising from u by substituting z for all variables outside X is not a projection. Let, say, $X = \{x_2,\ldots,x_n\}$, and put

$$s(z,x_2,\ldots,x_n) = u(z,x_2,\ldots,x_n,z,\ldots,z).$$

By construction, s is not a projection, while by our assumption on u we have

$$s(z,z,\ldots,z,\overset{i}{\breve{x}},z,\ldots,z) = z \quad \text{for all} \quad 2 \leq i \leq n. \tag{2.13}$$

Hence, in particular, $n \geq 3$. On the other hand, by the minimality of X, all operations

$$s(z,x_2,\ldots,x_{j-1},z,x_{j+1},\ldots,x_n), \quad 2 \leq j \leq n,$$

are projections. In view of (2.13) they must be projections onto z. However, this contradicts our assumption on $\mathcal{A}$.

Now it is easy to prove that $\mathcal{A}$ is affine with respect to $\underline{A}$. For arbitrary, say m-ary, operation $f \in F$ the (2m+1)-ary term operation

$$z - f(x_1-z+y_1,\ldots,x_m-z+y_m) + f(x_1,\ldots,x_m) - f(z,\ldots,z) + f(y_1,\ldots,y_m)$$

of $\mathcal{A}$ has the property that it turns into a projection onto z whenever we identify with z all but one of the variables $x_1,\ldots,x_m,y_1,\ldots,y_m$. Therefore, by the preceding paragraph, the identity

$$z - f(x_1-z+y_1,\ldots,x_m-z+y_m) + f(x_1,\ldots,x_m) - f(z,\ldots,z) + f(y_1,\ldots,y_m) = z$$

holds in $\mathcal{A}$. Substituting 0 for z we get that f is affine with respect to $\underline{A}$.

The equivalence (i) $\Longleftrightarrow$ (iii) in Theorem 2.4 was noticed independently by J. D. H. Smith [1976] and R. McKenzie [1976], while (i) $\Longleftrightarrow$ (vii) is a result of G. Czédli and J. D. H. Smith [1981].

All characterizations of affine algebras $\mathcal{A}$ in Theorem 2.4 are based on the assumption that $\mathcal{A}$ is a Mal'tsev algebra, which is equivalent to requiring that $\mathcal{A}$ generates a congruence permutable variety. C. Herrmann [1979] proved that (iii) characterizes affine algebras $\mathcal{A}$ even under the much weaker assumption that $\mathcal{A}$ generates a congruence modular variety. (New proofs were found by H. P. Gumm [1980] and W. Taylor [1982].)

It is clear from the proof of Theorem 2.4 and Proposition 2.2 that for every affine algebra $\mathcal{A}$, the corresponding Abelian group is determined only up to the selection of the neutral element 0. Let p denote the (unique) Mal'tsev operation of $\mathcal{A}$. If $\mathcal{A}$ is affine with respect to the Abelian groups $\underline{A} = (A;+,-,0)$ and $\underline{A}' = (A;+',-',0')$ as well, then $x - y + z = p(x,y,z) = x -' y +' z$, so

$$x +' y = x - 0' + y \quad \text{and} \quad -'y = 0' - y + 0'.$$

Conversely, given an Abelian group $\underline{A} = (A;+,-,0)$, these operations $+'$, $-'$ define an Abelian group $\underline{A}' = (A;+',-',0')$ for arbitrary $0' \in A$; furthermore, since $x - y + z = x -' y +' z$, an algebra $\mathcal{A} = (A;F)$ is affine with respect to $\underline{A}$ if and only if it is affine with respect to $\underline{A}'$. If so, then the operations of $\mathcal{A}$ are polynomial operations of the modules $(\text{End } \underline{A})^{\underline{A}}$ and $(\text{End } \underline{A}')^{\underline{A}'}$ as well. There is an easy rule "translating" one representation into the other. The details are left as an exercise to the reader.

EXERCISE 2.5. For the Abelian groups $\underline{A}$ and $\underline{A}'$ as above we have that

(a) $\underline{A} \to \underline{A}'$, $x \mapsto x + 0'$ is an isomorphism;

(b) $r'x = rx + (1-r)0'$ is an endomorphism of $\underline{A}'$ for every $r \in \text{End } \underline{A}$;

(c) $\text{End } \underline{A} \to \text{End } \underline{A}'$, $r \mapsto r'$ is a ring isomorphism;

(d) $\sum_{i=1}^{n}{}' r_i'x_i +' a = \sum_{i=1}^{n} r_ix_i - (\sum_{i=1}^{n} r_i)0' + a$ for all $r_1,\dots,r_n \in \text{End } \underline{A}$ and $a \in A$.

By definition, the operations of every affine algebra are polynomial operations of a module. In the rest of this section we look more closely at the question how affine algebras are related to modules. The following useful, though very simple, proposition describes affine algebras up to term equivalence (see Á. Szendrei [1980]).

PROPOSITION 2.6. *Given an algebra* $\mathcal{A} = (A;F)$ *which is affine with respect to an Abelian group* $\underline{A} = (A;+,-,0)$, *there exists a unique unitary subring* R *of* $\text{End } \underline{A}$ *and a unique submodule* M *of the* R*-module* $R \times {}_R\underline{A}$ *such that* $T(\mathcal{A})$ *coincides with the clone*

$$K({}_R\underline{A},M) = \{\sum_{i=1}^{n} r_ix_i + a: n \geq 1,\ r_1,\dots,r_n \in R,\ (1 - \sum_{i=1}^{n} r_i,\ a) \in M\}.$$

PROOF. If $T(\mathcal{A}) = K({}_R\underline{A},M)$ for some R and M as claimed, then

$$R = \{r \in \operatorname{End} \underline{A}\colon rx+(1-r)y \in T(\mathcal{A})\},$$

$$M = \{(r,a) \in (\operatorname{End} \underline{A}) \times \underline{A}\colon (1-r)x+a \in T(\mathcal{A})\},$$

implying the uniqueness of R and M. Suppose now that $\mathcal{A}$ is affine with respect to $\underline{A}$, and define the sets R and M as above. For arbitrary elements $r,r' \in R$, $(r_i,a_i) \in M$ $(i = 1,2)$ we have

$$1x + 0y \in T(\mathcal{A}),$$

$$(r-r')x + (1-r+r')y = (rx+(1-r)y) - (r'x+(1-r')y) + y \in T(\mathcal{A}),$$

$$rr'x + (1-rr')y = r(r'x+(1-r')y) + (1-r)y \in T(\mathcal{A}),$$

yielding that R is a unitary subring of $\operatorname{End} \underline{A}$, furthermore,

$$r_1x + (1-r_1)y = ((1-r_1)y+a_1) - ((1-r_1)x+a_1) + x \in T(\mathcal{A}),$$

$$(1-r_1+r_2)x + (a_1-a_2) = ((1-r_1)x+a_1) - ((1-r_2)x+a_2) + x \in T(\mathcal{A}),$$

$$(1-rr_1)x + ra_1 = r((1-r_1)x+a_1) + (1-r)x \in T(\mathcal{A}),$$

showing that $M \leqq R \times \underline{A}$ and M is a submodule of $R \times {}_R\underline{A}$.

To prove the equality $T(\mathcal{A}) = K({}_R\underline{A},M)$ assume first $\sum_{i=1}^{n} r_ix_i + a \in T(\mathcal{A})$. Then $(\sum_{i=1}^{n} r_i)x + a \in T(\mathcal{A})$, and for any $1 \le j \le n$,

$$r_jx + (1-r_j)y = (\sum_{i=1}^{n} r_ix+a) - (\sum_{\substack{i=1\\ i\neq j}}^{n} r_ix+r_jy+a) + y \in T(\mathcal{A}),$$

that is, $(1 - \sum_{i=1}^{n} r_i,a) \in M$ and $r_1,\ldots,r_n \in R$. Hence the inclusion $\leqq$ holds. Conversely, let $\sum_{i=1}^{n} r_ix_i + a \in K({}_R\underline{A},M)$. Then, by definition,

$$(2.14) \qquad (\sum_{i=1}^{n} r_i)x + a \in T(\mathcal{A}), \quad r_jx + (1-r_j)y \in T(\mathcal{A}) \quad (j = 1,\ldots,n).$$

Since $x - y + z \in T(\mathcal{A})$, it follows by induction on k that the $(k+2)$-ary operation $p_k = x_1 + \ldots + x_{k+1} - kx_{k+2}$ belongs to $T(\mathcal{A})$ $(k = 1,2,\ldots)$. Thus, substituting the operations (2.14) into p_n we get that

$$\sum_{i=1}^{n} r_i x_i + a = \sum_{i=1}^{n} (r_i x_i + (1-r_i)x_1) + ((\sum_{i=1}^{n} r_i)x_1 + a) - nx_1 \in T(\mathcal{A}),$$

concluding the proof.

Proposition 2.6 immediately implies that for every affine algebra $\mathcal{A}$ there is a unique subring R of the endomorphism ring of the corresponding Abelian group $\underline{A}$ such that the clone $K({}_R\underline{A},M)$ of $\mathcal{A}$ lies between $K({}_R\underline{A},\{(0,0)\})$, the clone of the affine R-module corresponding to ${}_R\underline{A}$ (that is, the clone of the full idempotent reduct of ${}_R\underline{A}$), and $K({}_R\underline{A},R\times\underline{A})$, the clone of polynomial operations of ${}_R\underline{A}$. In particular, it follows for instance that every subalgebra of $\mathcal{A}$ is a coset of a submodule of ${}_R\underline{A}$, or that $\mathcal{A}$ has the same congruences as ${}_R\underline{A}$. We get also

COROLLARY 2.7. *Every affine algebra is polynomially equivalent to a faithful unitary module.*

Interestingly, the converse of this statement is also true:

EXERCISE 2.8. Let $\mathcal{A} = (A;F)$ be an algebra. If there exists an R-module ${}_R\underline{A} = (A;+,-,0,R)$ such that $x - y + z \in P(\mathcal{A}) \subseteq P({}_R\underline{A})$, then $x - y + z \in T(\mathcal{A})$. Consequently, every algebra which is polynomially equivalent to a module, is affine.

Polynomial reducts of vector spaces and simple affine algebras

We now apply Proposition 2.6 to determine, up to term equivalence, all finite algebras in the title. They will turn out to be related in the same way as vector spaces and simple modules are by Schur's Lemma and Jacobson's Density Theorem (see N. Jacobson [1956]).

Let ${}_K\underline{A} = (A;+,-,0,K)$ be a vector space over a field. For a coset S of a subspace of ${}_K\underline{A}$ and for a subspace U of ${}_K\underline{A}$ define two subsets of $P({}_K\underline{A})$ as follows:

$$X(_K\underline{A},S) = \{\sum_{i=1}^{n} r_i x_i + a: n \geq 1,\ r_1,\ldots,r_n \in K,\ a = s - (\sum_{i=1}^{n} r_i)s' \text{ for some } s,s' \in S\},$$

$$Y(_K\underline{A},U) = \{\sum_{i=1}^{n} r_i x_i + a: n \geq 1,\ r_1,\ldots,r_n \in K,\ \sum_{i=1}^{n} r_i = 1,\ a \in U\}.$$

It is easy to see that $X(_K\underline{A},S)$ as well as $Y(_K\underline{A},U)$ are subclones in $P(_K\underline{A})$.

PROPOSITION 2.9. *Let* $_K\underline{A}$ *be a vector space over a finite field* K. *The nonunary subclones of* $P(_K\underline{A})$ *are exactly the clones* $X(_L\underline{A},S)$ *and* $Y(_L\underline{A},U)$ *where* L *is a subfield of* K, *and* S *is a coset of a subspace and* U *is a subspace of the vector space* $_L\underline{A}$ *over* L.

REMARK. The clones listes in the proposition are pairwise distinct. Moreover, for any subfields L_i of K, for any cosets S_i of subspaces of $_{L_i}\underline{A}$, and for any subspaces U_i of $_{L_i}\underline{A}$ $(i = 1,2)$ we have

$$X(_{L_1}\underline{A},S_1) \subseteq X(_{L_2}\underline{A},S_2) \text{ iff } L_1 \subseteq L_2 \text{ and } S_1 \subseteq S_2,$$

$$Y(_{L_1}\underline{A},U_1) \subseteq Y(_{L_2}\underline{A},U_2) \text{ iff } L_1 \subseteq L_2 \text{ and } U_1 \subseteq U_2,$$

$$Y(_{L_1}\underline{A},U_1) \subseteq X(_{L_2}\underline{A},S_2) \text{ iff } L_1 \subseteq L_2 \text{ and } U_1 \subseteq \{s-s': s,s' \in S_2\},$$

$$X(_{L_1}\underline{A},S_1) \nsubseteq Y(_{L_2}\underline{A},U_2).$$

PROOF of Proposition 2.9. We have to show that every nonunary subclone C of $P(_K\underline{A})$ coincides with $X(_L\underline{A},S)$ or $Y(_L\underline{A},U)$ for some L, S or L, U, respectively, as above. Using that C is nonunary, select $f = \sum_{i=1}^{n} s_i x_i + b \in C$ so that $n \geq 2$, $s_i \neq 0$ for $i = 1,\ldots,n$ $(s_1,\ldots,s_n \in K,\ b \in A)$. First we show that $x - y + z \in C$. If $\sum_{i=1,\, i\neq j}^{n} s_i \neq 0$ for some $1 \leq j \leq n$, then the operation $s_j x + (\sum_{i=1,\, i\neq j}^{n} s_i)y + b \in C$ is a quasigroup operation. Since K is finite, the same argument as in the proof of Proposition 1.21 yields that the left and right divisions corresponding to this operation also belong to C. Hence C contains a

Mal'tsev operation, which must be $x - y + z$. Suppose now that $\sum_{\substack{i=1 \\ i\neq j}}^{n} s_i = 0$ for all $1 \le j \le n$. Then $s_1 = \ldots = s_n = \sum_{i=1}^{n} s_i$, whence $s_1 x \in C$ and $s_1^2 x_1 + \sum_{i=2}^{n} s_i x_i + b \in C$. The former case applies for this operation unless $s_1^2 = s_1$, that is $s_1 = 1$ (as $s_1 \neq 0$). So let $1 = s_1 = \ldots = s_n = \sum_{i=1}^{n} s_i$. If the characteristic of K is not 2, then $2x + (-1)y = (s_1+s_2)x + (s_3+\ldots+s_n)y \in C$ is again a quasigroup operation, and we may repeat the above reasoning. Finally, if K is of characteristic 2, then $x - y + z = s_1 x + s_2 y + (s_3+\ldots+s_n)z \in C$.

Thus $(A;C)$ is an affine algebra. Taking into account Proposition 2.6 and the fact that every unitary subring of a finite field is a subfield, we get that there exist a subfield L of K and a subspace W of the vector space $L \times {}_L\underline{A}$ (over L) such that $C = K({}_L\underline{A},W)$. Set

$$W_1 = \{r \in L: (r,a) \in W \text{ for some } a \in A\},$$
$$W_2(r) = \{a \in A: (r,a) \in W\} \quad (r \in L).$$

Since W is a subspace of $L \times {}_L\underline{A}$, it follows that $W_1 = \{0\}$ or L, and $W_2(r)$ is a coset of a subspace of ${}_L\underline{A}$ for every $r \in L$.

If $W_1 = \{0\}$, then $W = \{0\} \times W_2(0)$ and, as $0 \in W_2(0)$, $W_2(0)$ is a subspace of ${}_L\underline{A}$. Furthermore, it is clear from the definitions that $K({}_L\underline{A},W) = Y({}_L\underline{A},W_2(0))$. In the opposite case, if $W_1 = L$, then we have $K({}_L\underline{A},W) = X({}_L\underline{A},W_2(1))$. Indeed, $\sum_{i=1}^{n} r_i x_i + a \in K({}_L\underline{A},W)$ if and only if $r_1,\ldots,r_n \in L$ and $(1 - \sum_{i=1}^{n} r_i, a) \in W$. On the other hand, $\sum_{i=1}^{n} r_i x_i + a \in X({}_L\underline{A},W_2(1))$ if and only if $r_1,\ldots,r_n \in L$ and $a = s - (\sum_{i=1}^{n} r_i)s'$ for some $s,s' \in W_2(1)$. However,

$$(1 - \sum_{i=1}^{n} r_i, a) = (1, a + (\sum_{i=1}^{n} r_i)s') - \sum_{i=1}^{n} r_i(1,s')$$

belongs to W for some $s' \in W_2(1)$ if and only if $s = a + (\sum_{i=1}^{n} r_i)s' \in W_2(1)$, concluding the proof.

To prove the remark after the proposition, observe that the constant operation with value $a \in A$ belongs to $X({}_L\underline{A},S)$ if and only if $a \in S$, while a translation $x + a$ $(a \in A)$ belongs to $Y({}_L\underline{A},U)$ if and only if $a \in U$.

Note that in Proposition 2.9 the finiteness of the base set A is not assumed, however the finiteness of the field K is crucial. The proof presented here is essentially the same as in Á. Szendrei [1980], although there the claim is formulated for 1-dimensional vector spaces only. In the special case when $|A| = q$ (q prime), that is, we have a 1-dimensional vector space over the prime field $\mathbf{Z}_q$, this result is due to A. A. Salomaa [1964]. (It was later rediscovered by J. Bagyinszki and J. Demetrovics [1982].)

The unary subclones of $P({}_K\underline{A})$, which are not covered by Proposition 2.9, are in one-to-one correspondence with the submonoids of $P^{(1)}({}_K\underline{A})$. These clones will not play any role in the sequel.

We now turn to the discussion of finite simple affine algebras. Consider a vector space ${}_K\underline{A}$ over a field K, and let $\mathrm{End}\ {}_K\underline{A}$ denote the endomorphism ring of ${}_K\underline{A}$. Clearly, $\underline{A}$ can be considered as an $(\mathrm{End}\ {}_K\underline{A})$-module ${}_{(\mathrm{End}\ {}_K\underline{A})}\underline{A}$. For a coset S of a subspace of ${}_K\underline{A}$ and for a subspace U of ${}_K\underline{A}$ define two subsets of $P({}_{(\mathrm{End}\ {}_K\underline{A})}\underline{A})$ as follows:

$$X^*({}_K\underline{A},S) = \{\sum_{i=1}^{n} r_i x_i + a: n \geq 1,\ r_1,\dots,r_n \in \mathrm{End}\ {}_K\underline{A},\ (1 - \sum_{i=1}^{n} r_i)s = a \text{ for all } s \in S\},$$

$$Y^*({}_K\underline{A},U) = \{\sum_{i=1}^{n} r_i x_i + a: n \geq 1,\ r_1,\dots,r_n \in \mathrm{End}\ {}_K\underline{A},\ (1 - \sum_{i=1}^{n} r_i)u = 0 \text{ for all } u \in U\}.$$

It is easy to see that $X^*({}_K\underline{A},S)$ and $Y^*({}_K\underline{A},U)$ are subclones in $P({}_{(\mathrm{End}\ {}_K\underline{A})}\underline{A})$.

PROPOSITION 2.10. *Let $\mathcal{A} = (A;F)$ $(|A| > 1)$ be a finite algebra which is affine with respect to an Abelian group $\underline{A} = (A;+,-,0)$. Then $\mathcal{A}$ is simple*

if and only if there exist a finite field K *and a vector space* ${}_K\underline{A}$ *such that* $T(\mathcal{A})$ *coincides with* $X^*({}_K\underline{A},S)$ *or* $Y^*({}_K\underline{A},U)$ *for some coset* S *of a subspace of* ${}_K\underline{A}$ *or for some subspace* U *of* ${}_K\underline{A}$, *respectively.*

PROOF. Let R denote the subring of End $\underline{A}$ corresponding to $\mathcal{A}$ (cf. Proposition 2.6). Since $\mathcal{A}$ is polynomially equivalent to the R-module ${}_R\underline{A}$, therefore $\mathcal{A}$ is simple if and only if ${}_R\underline{A}$ is simple. Now we can apply a well-known result from ring theory: if ${}_R\underline{A}$ is simple, then Schur's Lemma together with Wedderburn's Theorem on the commutativity of finite division rings yields that $K = \text{End}\ {}_R\underline{A}$ is a finite field; moreover, by Jacobson's Density Theorem and by the finiteness of A it follows that $R = \text{End}\ {}_K\underline{A}$. Conversely, if R is of this form for some vector space ${}_K\underline{A}$, then ${}_R\underline{A}$ is simple.

Assume that $\mathcal{A}$ is simple. According to Proposition 2.6 we have $T(\mathcal{A}) = K({}_R\underline{A},M)$ for some submodule M of $R \times {}_R\underline{A}$. As in the proof of the preceding proposition, set

$$M_1 = \{r \in R: (r,a) \in M \text{ for some } a \in A\},$$
$$M_2(r) = \{a \in A: (r,a) \in M\} \quad (r \in R).$$

Clearly, M_1 is a left ideal of R, so there is a subspace U of ${}_K\underline{A}$ such that $M_1 = \{r \in R: ru = 0 \text{ for all } u \in U\}$. On the other hand, $M_2(0)$ is a submodule of ${}_R\underline{A}$, whence $M_2(0) = \{0\}$ or $M_2(0) = A$. In the latter case $M = M_1 \times A$, so we have $T(\mathcal{A}) = K({}_R\underline{A},M) = Y^*({}_K\underline{A},U)$. In the first case $|M_2(r)| = 1$ for all $r \in M_1$. However, M_1 being a left ideal of R, there exists an element $e = e^2 \in R$ with $M_1 = Re$. Therefore, if a_o is the unique element of $M_2(e)$, then $(r,ra_o) = r(e,a_o) \in M$ for all $r \in Re$ $(= M_1)$. Hence $ea_o = a_o$ and

$$M = \{(r,ra_o): r \in M_1\}.$$

We claim that for the coset $S = U + a_o$ we have $K({}_R\underline{A},M) = X^*({}_K\underline{A},S)$. Indeed, operation $\sum_{i=1}^{n} r_i x_i + a$ with $r_1,\ldots,r_n \in R$ belongs to $K({}_R\underline{A},M)$ if and only

$(1 - \sum_{i=1}^{n} r_i, a) \in M$, that is $(1 - \sum_{i=1}^{n} r_i)u = 0$ for all $u \in U$ and $(1 - \sum_{i=1}^{n} r_i)a_o = a$. However, this is equivalent to requiring that $(1 - \sum_{i=1}^{n} r_i)s = a$ for all $s \in S$, which is exactly the condition defining the elements of $X^*({}_K\underline{A},S)$. Hence $T(\mathcal{A}) = X^*({}_K\underline{A},S)$.

Conversely, if $T(\mathcal{A})$ is one of the clones $X^*({}_K\underline{A},S)$ or $Y^*({}_K\underline{A},U)$ with K, S, U as described in the proposition, then $\mathcal{A}$ is polynomially equivalent to the module $(\text{End }{}_K\underline{A})\underline{A}$, therefore $\mathcal{A}$ is simple.

There is an intimate connection between the polynomial reducts of finite vector spaces and the finite simple affine algebras.

EXERCISE 2.11. Let ${}_K\underline{A}$ be a vector space over a field K. For arbitrary coset S of a subspace of ${}_K\underline{A}$, each of the clones $X({}_K\underline{A},S)$ and $X^*({}_K\underline{A},S)$ consists exactly of those operations on A which commute with every operation in the other clone. Similarly, for arbitrary subspace U of ${}_K\underline{A}$, each of the clones $Y({}_K\underline{A},U)$ and $Y^*({}_K\underline{A},U)$ consists exactly of those operations on A which commute with every operation in the other clone.

This fact together with Propositions 2.9 and 2.10 shows that finite simple affine algebras come in pairs with certain polynomial reducts of vector spaces on their universes. In particular, the companion of a finite simple R-module ${}_R\underline{A}$ ($R \subseteq \text{End } \underline{A}$) is the corresponding vector space ${}_K\underline{A}$ with $K = \text{End }{}_R\underline{A}$, $R = \text{End }{}_K\underline{A}$, as $T({}_K\underline{A}) = X({}_K\underline{A},\{0\})$ and $T({}_R\underline{A}) = X^*({}_K\underline{A},\{0\})$. In fact, the claim of Exercise 2.11 for the clones $T({}_K\underline{A})$ and $T({}_R\underline{A})$ is a way of rephrasing Jacobson's Dentity Theorem. This interesting phenomenon will be discussed more generally, and with a different approach, in the theory of para-primal algebras in Chapter 4.

If we are interested in some abstract properties of affine algebras rather than their clones, then it is sufficient to know them up to equivalence.

Using Proposition 2.10 the finite simple affine algebras can be described, up to equivalence, as follows:

COROLLARY 2.12. *Every finite simple affine algebra with at least two elements is equivalent to one of the algebras*

(a) $(K^n;\ x-y+z,\ \{rx + (1-r)y:\ r \in K_{n\times n}\},\ e_k x)$, *or*

(b) $(K^n;\ x-y+z,\ \{rx + (1-r)y:\ r \in K_{n\times n}\},\ e_k x,\ \{x + a:\ a \in K^n\})$,

where $n \geq 1$, $0 \leq k \leq n$, K *is a finite field,* $K_{n\times n}$ *is the* $n \times n$ *matrix ring over* K, *and* $e_k \in K_{n\times n}$ *is the diagonal matrix*

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

with k *entries equal to* 1.

PROOF. Let $\mathcal{A}$ be a finite simple affine algebra. If, in the notation of Proposition 2.10, $T(\mathcal{A}) = X^*({}_K\underline{A},S)$, then $\mathcal{A}$ has 1-element subalgebras, so by changing the neutral element of the Abelian group corresponding to $\mathcal{A}$ we may assume that $0 \in S$, that is S is a subspace of ${}_K\underline{A}$. If ${}_K\underline{A}$ is n-dimensional and S is k-dimensional, then ${}_K\underline{A}$ and K^n can be identified via a vector space isomorphism ${}_K\underline{A} \to K^n$ sending S into $K^k \times \{0\}^{n-k}$. This identification carries the algebra $(A;X^*({}_K\underline{A},S))$ into $(K^n;X^*({}_K(K^n),K^k\times\{0\}^{n-k}))$, and the latter is easily seen to be term equivalent to the algebra (a). The other case, when $T(\mathcal{A}) = Y^*({}_K\underline{A},U)$, can be treated similarly (except that the Abelian group corresponding to $\mathcal{A}$ need not be changed), to conclude that $\mathcal{A}$ is equivalent to the algebra (b) provided ${}_K\underline{A}$ is n-dimensional and U is k-dimensional.

This result was first proved by D. M. Clark and P. H. Krauss [1980] in a roundabout manner, using a property of the universal Horn class generated by a finite simple affine algebra.

Semi-affine algebras

If we drop condition (a) from the definition of affine algebras, we get the class of reducts of affine algebras, or equivalently, the class of polynomial reducts of modules (cf. Proposition 2.1).

DEFINITION. An algebra $\mathcal{A} = (A;F)$ is called *semi-affine* iff there exists an Abelian group $\underline{A} = (A;+,-,0)$ such that every basic operation (and hence every polynomial operation) of $\mathcal{A}$ is affine with respect to $\underline{A}$.

In this section we deal mostly with finite algebras. Let A be a finite set. The number of Abelian groups on A being finite, it is easily seen from Proposition 2.6 that, up to term equivalence, there are only finitely many affine algebras on A. If we consider semi-affine algebras instead of affine algebras, this claim is no longer true in general. However, we still have

PROPOSITION 2.13. *For every finite set* A, *up to term equivalence, there are only countably many semi-affine algebras on* A.

PROOF. Let $\underline{A} = (A;+,-,0)$ be an Abelian group. We have to show that $A(\underline{A})$ has only countably many subclones. The proof will be reduced to the following well-known result on the ordered set $(\mathbf{N}_0;\leq)$ of the natural numbers (with the natural order): For every integer $k \geq 1$, $(\mathbf{N}_0;\leq)^k$ has only countably many order ideals.

Let $E = \operatorname{End} \underline{A}$, and let m denote the exponent of $\underline{A}$. For arbitrary $f \in A(\underline{A})$ and $r \in E - \{0\}$ denote by $\nu_f(r)$ the number of occurrences of r as a coefficient in f. Furthermore, for $f,g \in A(\underline{A})$ let

$$f \equiv g \text{ iff } f(\underline{0}) = g(\underline{0}) \text{ and } \nu_f(r) \equiv \nu_g(r) \pmod{m} \text{ for all } r \in E - \{0\}$$

and

$$f \leq g \text{ iff } f \equiv g \text{ and } \nu_f(r) \leq \nu_g(r) \text{ for all } r \in E - \{0\}.$$

It is clear that the number of $\equiv$-blocks is finite, and every subclone of $A(\underline{A})$ is an order ideal with respect to $\leq$. In fact, for the latter we need only

identification of variables. So, in order to prove that $A(\underline{A})$ has only countably many subclones, it suffices to show that every $\equiv$-block contains only countably many $\leq$-ideals. However, within a fixed block we have a bijective mapping $f \mapsto n_f \in \mathbf{N}_o^{E-\{0\}}$, where $\nu_f(r) = mn_f(r) + u$ $(0 \leq u < m)$ for all $r \in E - \{0\}$. Since this is an order isomorphism as well, an application of the claim stated at the beginning concludes the proof.

This result is due to D. Lau [1978] although she proved a weaker statement, but she credits the idea to I. A. Mal'tsev [1973].

Now it is natural to ask: When is the number of semi-affine algebras finite; more precisely, for which finite Abelian groups $\underline{A} = (A;+,-,0)$ has the clone $A(\underline{A})$ only finitely many subclones? If $|A|$ is not square free, then End $\underline{A}$ is easily seen to contain an element $r \neq 0$ such that $r^2 = 0$. Now the 1-generated clones

$$[rx_1 + \ldots + rx_k], \quad k = 1,2,3,\ldots,$$

form an ω-chain, hence $A(\underline{A})$ has infinitely many subclones. Assume now that $n = |A|$ is square free. Then $\underline{A}$ is a cyclic group and End $\underline{A}$ is isomorphic to the ring $\mathbf{Z}_n$ of integers modulo n. A. A. Salomaa [1964] conjectured that in this case $A(\underline{A})$ has only finitely many subclones, and he proved the conjecture for n prime (see the previous section).

The problem can be raised more generally as follows: Determine those finite faithful unitary R-modules ${}_R\underline{A}$ for which $P({}_R\underline{A})$ has only finitely many subclones. By the above argument a necessary condition is that R contain no element $r \neq 0$ with $r^2 = 0$. Since R is necessarily finite (R is isomorphic to a subring of End $\underline{A}$), the Wedderburn-Artin Theorems (see N. Jacobson [1956]) and Wedderburn's Theorem on the commutativity of finite division rings imply that R is isomorphic to a direct product of finitely many finite fields. It can be

proved that this condition is already sufficient (Á. Szendrei [1981b]). Clearly, this result includes Salomaa's conjecture as a special case. Therefore Proposition 2.13 can be supplemented with the following statement:

The number of semi-affine algebras on a finite set A is finite if and only if $|A|$ is square free.

In general, one cannot expect to get a "nice" explicit description for all subclones of $A(\underline{A})$ or $P(_R\underline{A})$, therefore most attention was devoted to some special subclones. Such are, for example, the idempotent subclones, which will be discussed in the next section. Some other results of this nature can be found in D. Lau [a] and L. Szabó and Á. Szendrei [1981].

Let us close this section with some remarks on the relation between TC-algebras and semi-affine algebras. Clearly, every semi-affine algebra, moreover, every subalgebra of a semi-affine algebra, is a TC-algebra. Interestingly, Proposition 2.13 carries over to TC-algebras. J. Berman and R. McKenzie [1984] proved that for every finite set A, up to term equivalence, there are only countably many TC-algebras on A. The question how close TC-algebras are to semi-affine algebras, which is motivated also by tame congruence theory (see the remarks following the proof of Theorem 3.5), was not investigated until quite recently. R. Quackenbush [a] proved that, in general, TC-algebras are very far from semi-affine algebras. More precisely, he constructed an infinite list of more and more complicated conditions, the simplest one among them being (TC), such that an algebra is isomorphic to a subalgebra of a semi-affine algebra if and only if it satisfies all these conditions. On the positive side, the most important result is the following theorem of R. McKenzie [a] (see also D. Hobby and R. McKenzie [a]): Every finite simple TC-algebra is isomorphic to a subalgebra of a semi-affine algebra. It is easy to see that every 2-element TC-algebra is semi-affine.

Detailed information is available also on the 3-element TC-algebras (see J. Berman, R. McKenzie [1984] and J. Demetrovics, I. A. Mal'tsev [a]).

Idempotent semi-affine algebras

Let $\underline{A} = (A;+,-,0)$ be an Abelian group. Clearly, an operation $\sum_{i=1}^{n} r_i x_i + a \in A(\underline{A})$ is idempotent if and only if $a = 0$ and $\sum_{i=1}^{n} r_i = 1$. These operations form a subclone in $A(\underline{A})$, which will be denoted by $A_i(\underline{A})$. To every subclone C of $A_i(\underline{A})$ we make correspond the subring R_C of End $\underline{A}$ generated by the coefficients of operations in C (R_C is necessarily unitary). Put differently, R_C is the least subring R of End $\underline{A}$ such that $C \subseteq P({}_R\underline{A})$. In particular, if $x - y + z \in C$, then R_C is exactly the ring R for which we have $C = K({}_R\underline{A},\{(0,0)\})$ (cf. Proposition 2.6).

We now define some subclones of $A_i(\underline{A})$ which will play an important role in this section. From now on, a subring of End $\underline{A}$ will always mean a not necessarily unitary subring. For a subring S of End $\underline{A}$ let

$$I(\underline{A},S) = \{\sum_{i=1}^{n} r_i x_i : n \geq 1,\ r_1,\ldots,r_n \in \text{End } \underline{A},\ \sum_{i=1}^{n} r_i = 1, \text{ and } r_i \notin S \text{ for at most one } i\ (1 \leq i \leq n)\}.$$

It is straightforward to check that $I(\underline{A},S)$ is a subclone of $A_i(\underline{A})$. If S is a unitary subring, then $I(\underline{A},S) = K({}_S\underline{A},\{(0,0)\})$. The following lemma shows that every clone $C \subseteq A_i(\underline{A})$ has a largest subclone of the form $I(\underline{A},S)$.

LEMMA 2.14. *For arbitrary subclone C of $A_i(\underline{A})$,*

$$H_C = \{r \in \text{End } \underline{A} : x - ry + rz \in C\}$$

is an ideal of R_C, and $I(\underline{A},H_C) \subseteq C$. Furthermore, if $r_i, r_i' \in R_C$ are such that $h_i = r_i - r_i' \in H_C$ for all $1 \leq i \leq n$ and $\sum_{i=1}^{n} h_i = 0$, then the operation $\sum_{i=1}^{n} r_i x_i$ belongs to C if and only if $\sum_{i=1}^{n} r_i' x_i$ does.

PROOF. The last statement follows from the equality $\sum_{i=1}^{n} r_i x_i = (\sum_{i=1}^{n} r_i' x_i) + \sum_{i=1}^{n} h_i x_i$, since $\sum_{i=1}^{n} h_i = 0$ implies that

$$x_o + \sum_{i=1}^{n} h_i x_i = (\ldots((x_o - h_1 x_o + h_1 x_1) - h_2 x_o + h_2 x_2)\ldots) - h_n x_o + h_n x_n \in C.$$

The inclusion $I(\underline{A},H_C) \subseteq C$ is an immediate consequence of this. Finally, for arbitrary $h,h' \in H_C$ and $r \in R_C$ with $rx + (1-r)y \in C$ we have

$$x - (h-h')y + (h-h')z = (x-hy+hz) - h'z + h'y \in C,$$

$$x - hry + hrz = x - h(ry+(1-r)x) + h(rz+(1-r)x) \in C,$$

$$x - rhy + rhz = r(x-hy+hz) + (1-r)x \in C,$$

showing that $h - h'$, hr, $rh \in H_C$. This implies that $H_C \lhd R_C$, since the elements r with $rx + (1-r)y \in C$ form a generating set in the ring R_C.

It follows from Lemma 2.14 that the join of clones of the form $I(\underline{A},S)$ (in the lattice of subclones of $A_i(\underline{A})$) is also of this form. The same for meet is not true.

DEFINITION. A subclone C of $A_i(\underline{A})$ will be called *saturated* iff $C = \bigcap_{\gamma\in\Gamma} I(\underline{A},S_\gamma)$ for some subrings S_γ of R_C. An idempotent semi-affine algebra is saturated iff its clone is such.

Heuristically, the saturated clones are those subclones C of $A_i(\underline{A})$, for which H_C is "large". This is made more precise in

THEOREM 2.15. *Let* $\underline{A} = (A;+,-,0)$ *be an Abelian group, and let* $F \subseteq A_i(\underline{A})$. *The following conditions are equivalent:*

(i) $[F]$ *is saturated;*

(ii) $[F] = \bigcap(I(\underline{A},J)\colon J \lhd R_{[F]},\ F \subseteq I(\underline{A},J))$;

(iii) $r(1-r) \in H_{[F]}$ *for every coefficient* r *of each operation from* F.

PROOF. Let $C = [F]$. The implication (ii) $\Rightarrow$ (i) is trivial. Assume now (i),

say, $C = \bigcap_{\gamma\in\Gamma} I(\underline{A},S_\gamma)$ for some subrings S_γ of R_C, and let us consider an element $r \in R_C$ occurring as a coefficient of some operation in F. Then $rx + (1-r)y \in C$, hence for every $\gamma \in \Gamma$ we have $r \in S_\gamma$ or $1 - r \in S_\gamma$. Thus

$$r(1-r) = r - r^2 = (1-r) - (1-r)^2 \in \bigcap_{\gamma\in\Gamma} S_\gamma \subseteq H_C,$$

proving that (i) $\Rightarrow$ (iii). The implication (iii) $\Rightarrow$ (ii) is the most essential claim of the theorem. For simplicity, it will be proved for finite F only.

Assume that $F \subseteq A_i(\underline{A})$ is a finite set of operations satisfying (iii). We start the proof of the equality with a few observations.

Claim 1. If $\sum_{i=1}^{n} r_i x_i$ is an operation in C such that $r_i(1-r_i) \in H_C$ for all $1 \le i \le n$, then $r_i r r_j \in H_C$ for all $r \in R_C$ and $1 \le i,j \le n$, $i \neq j$.

It is easy to see that the set D_C of coefficients of operations in C is closed under multiplication, and hence is a generating set of the additive group of R_C. Therefore, since $H_C \lhd R_C$, it suffices to prove Claim 1 for $r \in D_C$. So let $r \in D_C$ and $1 \le i,j \le n$, $i \neq j$. Then $rx + (1-r)y \in C$ and

$$x - r_i r_j y + r_i r_j z = (r_i(r_i x + r_j z + (1-r_i-r_j)y) + (1-r_i)x) - r_i(1-r_i)y + r_i(1-r_i)x \in C,$$

whence

$$x - r_i r r_j y + r_i r r_j z = (r_i(r(r_j z + (1-r_j)x) + (1-r)(r_j y + (1-r_j)x)) + (1-r_i)x) - r_i r_j y + r_i r_j x \in C.$$

By a repeated application of Claim 1 we immediately get

Claim 2. For every operation $\sum_{i=1}^{k} s_i x_i \in C$ and for all indices $1 \le i,j \le k$, $i \neq j$, we have $s_i s_j \in H_C$.

Since any two idempotent operations $\sum_{i=1}^{n} r_i x_i$, $\sum_{j=1}^{n} s_j x_j$ generate the same clone as the single operation $\sum_{i=1}^{n}\sum_{j=1}^{k} r_i s_j x_{ij}$, it follows that C is

1-generated. Therefore, in view of Claim 2, we may assume that $|F| = 1$, say, $F = \{\sum_{i=1}^{n} r_i x_i\}$. Then, clearly, R_C is the subring of End $\underline{A}$ generated by $\{r_1,\ldots,r_n\}$, and

(2.15) $$r_i r_j \in H_C \quad \text{for all} \quad 1 \le i,j \le n, \quad i \ne j.$$

For $1 \le i \le n$ denote by J_i the ideal of R_C generated by $\{r_j: 1 \le j \le n, j \ne i\}$, and let $J = \bigcap_{i=1}^{n} J_i$.

We show that $J \subseteq H_C$. Let J' denote the ideal of R_C generated by $\{r_i r_j: 1 \le i,j \le n, i \ne j\}$. By (2.15) we have $J' \subseteq H_C$, so it is enough to show that $J \subseteq J'$ (the inclusion $J' \subseteq J$ obviously holds). Since J_i is the additive subgroup of R_C generated by all products of elements from $\{r_1,\ldots,r_n\}$ with at least one factor distinct from r_i, we have $r_i J_i \subseteq J'$ for all $1 \le i \le n$. To prove $J \subseteq J'$ let $s \in J$ be arbitrary. Then $s = \sum_{i=1}^{n} r_i s$ where, for every $1 \le i \le n$,

$$r_i s \in r_i J \subseteq r_i J_i \subseteq J'.$$

Hence $s \in J'$.

The proof of (ii) will be complete if we show that

$$C = \bigcap_{i=1}^{n} I(\underline{A},J_i).$$

The inclusion $\subseteq$ is obvious, since $\sum_{j=1}^{n} r_j x_j \in I(\underline{A},J_i)$ for every $1 \le i \le n$. Conversely, consider an operation $\sum_{j=1}^{m} s_j x_j \in \bigcap_{i=1}^{n} I(\underline{A},J_i)$. If $J_1 = \ldots = J_n = R_C$, then $R_C = J \subseteq H_C$, implying $C = I(\underline{A},R_C)$ and $\sum_{j=1}^{m} s_j x_j \in C$. In the opposite case let, for example, $J_1,\ldots,J_k \ne R_C$ and $J_{k+1} = \ldots = J_n = R_C$ $(1 \le k \le n)$. Then

$J = \bigcap_{i=1}^{k} J_i$ and $r_{k+1},\dots,r_n \in J$. Furthermore, for each i with $1 \le i \le k$ there exists exactly one coefficient s_j $(1 \le j \le m)$ such that $s_j \notin J_i$. Assume that, say, $s_1,\dots,s_\ell \notin J$ and $s_{\ell+1},\dots,s_m \in J$. Setting

$$\delta_j = \{i: 1 \le i \le k,\ s_j \notin J_i\} \quad \text{for} \quad 1 \le j \le \ell,$$

we get that $\delta_1,\dots,\delta_\ell$ is a partition of $\{1,\dots,k\}$. Consider the elements $\bar{r}_j = \sum_{i\in\delta_j} r_i$ and $h_j = \bar{r}_j - s_j$ $(1 \le j \le \ell)$. Then

$$h_j = \bar{r}_j - s_j \in \bigcap_{\substack{i=1 \\ i\notin\delta_j}}^{k} J_i \quad (1 \le j \le \ell),$$

$$\sum_{j=1}^{\ell} h_j = (1 - \sum_{j=1}^{\ell} s_j) - (1 - \sum_{j=1}^{\ell} \bar{r}_j) = \sum_{j=\ell+1}^{m} s_j - \sum_{j=k+1}^{n} r_j \in J,$$

whence also

$$h_j = (\sum_{j=1}^{\ell} h_u) - \sum_{\substack{u=1 \\ u\neq j}}^{\ell} h_u \in \bigcap_{i\in\delta_j} J_i \quad (1 \le j \le \ell).$$

(In all three cases above, every term of the rightmost expression belongs to the ideal indicated.) Consequently, $h_j \in J \subseteq H_C$ for every $1 \le j \le \ell$. Therefore Lemma 2.14 can be applied for the operations

$$\sum_{j=1}^{\ell} \bar{r}_j x_j + (\sum_{j=k+1}^{n} r_j) x_{\ell+1} \quad \text{and} \quad \sum_{j=1}^{m} s_j x_j,$$

of which the first one belongs to C, since it arises from $\sum_{i=1}^{n} r_i x_i \in F$ by identification of variables. Hence $\sum_{j=1}^{m} s_j x_j \in C$.

The saturated clones are relatively easy to handle, and have some nice properties, too, for example

EXERCISE 2.16. Every saturated subclone of $A_i(\underline{A})$ is generated by at most ternary operations.

Next we want to exhibit large families of saturated idempotent semi-affine algebras. To this end we first give a necessary and sufficient condition for an idempotent semi-affine groupoid to be saturated.

PROPOSITION 2.17. *Let* $\underline{A} = (A;+,-,0)$ *be an Abelian group. For* $r \in \operatorname{End} \underline{A}$ *the following conditions are equivalent:*

(i) *the groupoid* $\mathcal{A} = (A;rx+(1-r)y)$ *is saturated;*

(ii) *there exist natural numbers* $k \geq 2$ *and* $a_1,\dots,a_{k-1}$ *with* $a_1 \neq 0$, $a_{k-1} \neq 0$ *such that* $\sum_{i=1}^{k-1} a_i r^i (1-r)^{k-i} = 0$.

PROOF. Let $C = T(\mathcal{A})$. Assume C is saturated, that is, the operation $x - r(1-r)y + r(1-r)z$ belongs to C. It is easy to see that every member of C arises, for some $n \geq 2$, from the 2^n-ary operation

$$\sum_{i_1,\dots,i_n \in \{0,1\}} r^{i_1+\dots+i_n}(1-r)^{n-i_1-\dots-i_n} x_{i_1,\dots,i_n}$$

by identification of variables. Thus there exist $n \geq 2$ and natural numbers b_i, c_i $(0 \leq i \leq n)$ such that $b_i + c_i \leq \binom{n}{i}$ for all $0 \leq i \leq n$ and

$$\sum_{i=0}^{n} b_i r^i (1-r)^{n-i} = 1, \quad \sum_{i=0}^{n} c_i r^i (1-r)^{n-i} = -r(1-r). \tag{2.16}$$

If $c_o = c_n = 0$, then the second equation yields the required property:

$$\sum_{i=1}^{n-1} (c_i + \tbinom{n-2}{i-1}) r^i (1-r)^{n-i} = \sum_{i=1}^{n-1} c_i r^i (1-r)^{n-i} + r(1-r) = 0.$$

Otherwise, let us multiply the two equalities in (2.16). Then we get an equality of the form

$$\sum_{i=0}^{2n} c'_i r^i (1-r)^{2n-i} = -r(1-r)$$

with $c'_o = b_o c_o = 0$ and $c'_{2n} = b_n c_n = 0$, as $b_o + c_o \leq 1$, $b_n + c_n \leq 1$. Therefore the previous argument can be repeated.

Conversely, assume (ii) holds. Then for every $n \geq k$,

$$\sum_{i=1}^{k-2} a_i r^{n-k+i}(1-r)^{k-i} + (a_{k-1}-1)r^{n-1}(1-r) = -r^{n-1}(1-r),$$

$$(a_1-1)r(1-r)^{n-1} + \sum_{i=2}^{k-1} a_i r^i (1-r)^{n-i} = -r(1-r)^{n-1}.$$

If we let $n = \max\{k, a_1, \ldots, a_{k-1}\} + 1$, then $\binom{n}{j} \geq a_1, \ldots, a_{k-1}$ for every $1 \leq j \leq n-1$, therefore by the remark at the beginning of the proof we get that

$$x - r^{n-1}(1-r)y + r^{n-1}(1-r)z, \quad x - r(1-r)^{n-1}y + r(1-r)^{n-1}z \in C,$$

that is, $r^{n-1}(1-r)$, $r(1-r)^{n-1} \in H_C$. If $n = 2$, we are done, so suppose $n \geq 3$. Then, using the fact $H_C \lhd R_C$ we infer that

$$r(1-r)^{n-2} = r(1-r)^{n-1}(1+r+\ldots+r^{n-3}) + r^{n-1}(1-r)(1-r)^{n-3} \in H_C,$$

and similarly $r^{n-2}(1-r) \in H_C$. Repeating this argument we get finally that $r(1-r) \in H_C$.

EXERCISE 2.18. Let $\mathbf{R}$ denote the set of real numbers, and let $r \in \mathbf{R}$. The idempotent groupoid $\mathcal{A}_r = (\mathbf{R}; rx+(1-r)y)$ is saturated if and only if r is an algebraic number which is conjugate over the field $\mathbf{Q}$ of rationals to no $r' \in \mathbf{R}$ with $0 < r' < 1$.

As we shall soon see, there are a lot of rings in which condition (ii) of Proposition 2.17 holds for every element r. Denote the class of these rings by C. In view of Theorem 2.15 and Proposition 2.17 a ring R belongs to C if and only if for arbitrary faithful unitary R-module $_R\underline{A}$, all idempotent subclones of $T(_R\underline{A})$ are saturated. Using condition (ii) of Proposition 2.17 it is easy to check that, for instance, the ring of integers, the ring of Gaussian integers, and all rings of finite characteristic belong to C.

EXERCISE 2.19. C is a local variety, that is, it is closed under taking homomorphic images, (unitary) subrings, direct products of finite families,

and direct limits. A ring belongs to C if and only if its 1-generated subrings do.

Finite idempotent semi-affine algebras are worth mentioning explicitly. From the foregoing we immediately get

COROLLARY 2.20. *Every finite idempotent semi-affine algebra is saturated. Up to term equivalence, there are only finitely many idempotent semi-affine algebras on a fixed universe, and their clones are finitely generated.*

An interesting application is the following.

COROLLARY 2.21. *Let* $\mathcal{A}$ = (A;F) *be a finite, simple, idempotent semi-affine algebra. Then either* $\mathcal{A}$ *is a 2-element trivial algebra, or* $\mathcal{A}$ *is affine.*

PROOF. Let $\mathcal{A}$ = (A;F) be semi-affine with respect to an Abelian group $\underline{A}$ = (A;+,-,0). Assume $|A| > 1$ and $\mathcal{A}$ is not a 2-element trivial algebra. Then $\mathcal{A}$ is nontrivial. Furthermore, the algebra $\mathcal{A}^+$ = (A;FU{x-y+z}) is also finite, simple and idempotent, moreover it is affine with respect to $\underline{A}$. By Proposition 2.10 there exist a finite field K and a vector space ${}_K\underline{A}$ such that the clones $T(\mathcal{A}^+)$ and $X^*({}_K\underline{A},A) = I(\underline{A},\mathrm{End}\ {}_K\underline{A})$ coincide. Clearly, $R_{T(\mathcal{A})} = R_{T(\mathcal{A}^+)} = \mathrm{End}\ {}_K\underline{A}$. By Corollary 2.20 $\mathcal{A}$ is saturated, hence by Theorem 2.15

$$T(\mathcal{A}) = \cap(I(\underline{A},J) : J \lhd \mathrm{End}\ {}_K\underline{A},\ T(\mathcal{A}) \subseteq I(\underline{A},J)).$$

However, since the ring $\mathrm{End}\ {}_K\underline{A}$ is simple, we get that $T(\mathcal{A}) = I(\underline{A},\{0\})$ or $T(\mathcal{A}) = I(\underline{A},\mathrm{End}\ {}_K\underline{A})$. The first possibility would imply that is trivial, which is not the case. So we have the second possibility, that is, $T(\mathcal{A}) = T(\mathcal{A}^+)$.

Most parts of the material of this section are based on Á. Szendrei [1982a], although some results are stated there in a weaker form.

We remark that the nice properties of saturated clones can also be used to construct a basis for the identities of saturated idempotent semi-affine algebras (see Á. Szendrei [1981a]). Consider, for instance, the groupoids $\mathcal{A}_r$ ($r \in \mathbf{R}$) defined in Exercise 2.18. The problem whether they have finite bases for their identities whenever r is algebraic was raised by S. Fajtlowicz and J. Mycielski [1974]. If $\mathcal{A}_r$ is saturated, it follows that the answer is affirmative. However, as far as I know, the problem for the nonsaturated groupoids $\mathcal{A}_r$ is still unsolved in general.

Chapter 3

UNARY TERM OPERATIONS IN ALGEBRAS

The question we discuss in this section is how far the unary term operations determine an algebra. More precisely, given a transformation monoid (that is a monoid of unary operations) M on a set A, the problem is to describe all clones C with $C^{(1)} = M$. In general, this task is rather hopeless even if the base set A is finite, as for $|A| \geq 3$ there are $2^{\aleph_0}$ clones on A and only finitely many transformation monoids. However, in quite a few interesting special cases the number of clones with unary part M turns out to be finite.

PROPOSITION 3.1. *For arbitrary transformation monoid* M *on a set* A, *the clones* C *on* A *with* $C^{(1)} = M$ *form an interval in the clone lattice.*

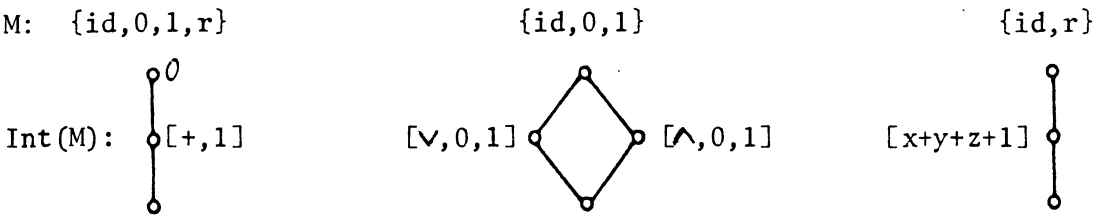
PROOF. By Lemma 1.2 we have

$$C^{(1)} = M \text{ if and only if } [M] \subseteq C \subseteq \mathrm{Pol}_A \{X_M\}.$$

This interval will be denoted by $\mathrm{Int}(M)$. Let us mention now some examples of M for which $\mathrm{Int}(M)$ is known. We assume throughout that the base set A is finite.

EXAMPLES. 1. If $|A| = 2$, say $A = \{0,1\}$, then there are 6 transformation monoids and $\aleph_0$ clones on A. As the clone lattice $\mathrm{Lat}(A)$ is fully known in this case (see Chapter 1), the intervals $\mathrm{Int}(M)$ are easy to determine. Three

of them turn out to be finite, their diagrams are given below:



From now on we assume that $|A| \geq 3$.

2. For $M = O_A^{(1)}$ the interval $\mathrm{Int}(M)$ was shown by G. A. Burle [1967] to be the $(|A|+1)$-element chain

$$[M] \subset \mathcal{B}_1 \subset \mathcal{B}_2 \subset \ldots \subset \mathcal{B}_{|A|-1} \subset \mathcal{B}_{|A|} = O_A$$

where $\mathcal{B}_1$ consists of the operations depending on at most one variable and the operations having the form $h(h_1(x_1)+\ldots+h_k(x_k))$ with $h_1,\ldots,h_k: A \to \{0,1\}$, $h: \{0,1\} \to A$ arbitrary mappings and $+$ denoting addition modulo 2, while for $2 \leq j \leq |A|$, $\mathcal{B}_j$ consists of the operations depending on at most one variable and the operations taking on at most j values.

3. A slight extension of this result, observed by L. Szabó [unpublished], is that for every transformation monoid $M \subset O_A^{(1)}$ containing all non-permutations, the interval $\mathrm{Int}(M)$ is the $|A|$-element chain

$$[M] \subset \mathcal{B}_1(M) \subset \mathcal{B}_2(M) \subset \ldots \subset \mathcal{B}_{|A|-1}(M)$$

where each $\mathcal{B}_i(M)$, $1 \leq i < |A|$, arises from $\mathcal{B}_i$ by omitting all operations depending on at most one variable which are outside $[M]$.

4. Let now M be the monoid of affine transformations of a finite vector space, that is, $M = P^{(1)}(_{(\mathrm{End}\ _K\underline{A})}\underline{A})$ where $_K\underline{A}$ is a k-dimensional $(k \geq 1)$ vector space over a finite field K. It is not hard to see that in this case we have $\mathrm{Pol}_A\{X_M\} = P(_{(\mathrm{End}\ _K\underline{A})}\underline{A})$, so by a result of L. Szabó and Á. Szendrei [1981] the interval $\mathrm{Int}(M)$ is the chain

$$[M] = \underset{\sim}{Q}_0 \subset \underset{\sim}{Q}_1 \subset \ldots \subset \underset{\sim}{Q}_{k-1} \subset \underset{\sim}{Q}_k = P(_{(\mathrm{End}\ _K\underline{A})}\underline{A})$$

where for each $0 \le j \le k$, $\underset{\sim}{Q}_j$ consists of all operations $\sum_{i=1}^{n} r_i x_i + a$ ($r_1,\ldots,r_n \in \mathrm{End}\ _K\underline{A}$, $a \in A$) such that either at most one of the endomorphisms $r_1,\ldots,r_n$ differs from 0 or the sum of the ranges of the endomorphisms $r_1,\ldots,r_n$ is an at most j-dimensional subspace of $_K\underline{A}$.

5. We get a similar chain for $\mathrm{Int}(M)$ if M is the monoid of linear transformations of a k-dimensional vector space $_K\underline{A}$ over a finite field K, that is $M = T^{(1)}(_{(\mathrm{End}\ _K\underline{A})}\underline{A})$, provided $k \ge 2$. Namely, the chain is

$$[M] = \underset{\sim}{Q}'_0 \subset \underset{\sim}{Q}'_1 \subset \ldots \subset \underset{\sim}{Q}'_{k-1} \subset \underset{\sim}{Q}'_k = T(_{(\mathrm{End}\ _K\underline{A})}\underline{A})$$

where $\underset{\sim}{Q}'_j = \underset{\sim}{Q}_j \cap T(_{(\mathrm{End}\ _K\underline{A})}\underline{A})$ for every $0 \le j \le k$. (The assumption $k \ge 2$ is needed to ensure that $\mathrm{Pol}_A\{X_M\} = T(_{(\mathrm{End}\ _K\underline{A})}\underline{A})$.)

6. Let M be the monoid consisting of all the constants and the identity operation on A. It is well known, and easy to verify, that for $|A| \ge 3$ every nonunary clone on A containing the constants contains a unary operation outside M. Hence $\mathrm{Int}(M)$ is a 1-element interval with $[M]$ as its unique member.

7. If $(A;+)$ is a cyclic group of prime order, $a \in A - \{0\}$ and M is the regular permutation group on A generated by $x + a$, then $\mathrm{Int}(M)$ is a 3-element chain:

$$[M] = [x+a] \subset [x-y+z, x+a] \subset \mathrm{Pol}_A\{(x+a)^{\square}\} = \mathrm{Pol}_A\{X_M\}$$

(see Á. Szendrei [1982b]).

8. There are a lot of permutation groups M for which $\mathrm{Int}(M)$ is a 1-element interval. Such are, for example, the dihedral groups of odd degree, the general linear groups $GL(k,K)$ ($k \ge 2$) acting on the nonzero vectors of a k-dimensional vector space over a finite field K, moreover, every nonregular

transitive permutation group in which all nontrivial normal subgroups are transitive (P. P. Pálfy and Á. Szendrei [1983]).

The investigation of the intervals $\mathrm{Int}(M)$ is, as yet, a quite unexplored area, although the special case to be discussed in detail in the next section has already found important applications in other fields of universal algebra.

The topic, in general, deserves some more attention for the following reason. As was mentioned earlier, for a finite set A with $|A| \geq 3$ the clone lattice $\mathrm{Lat}(A)$ has $2^{\aleph_0}$ elements. It is thought that $\mathrm{Lat}(A)$ is nice at the top and at the bottom in the sense that the clones belonging to those two parts can be explicitly described, while the middle of the lattice, which contains the families of cardinality $2^{\aleph_0}$ is hopeless. Contrasted to this "horizontal" division, the intervals $\mathrm{Int}(M)$ provide a natural "vertical" division of $\mathrm{Lat}(A)$. Therefore the solution of the following problem would contribute to a better understanding of the structure of $\mathrm{Lat}(A)$.

PROBLEM. Let A be a finite set with $|A| \geq 3$. For which transformation monoids M on A is

(a) $\mathrm{Int}(M)$ finite,

(b) $|\mathrm{Int}(M)| = 2^{\aleph_0}$?

A characterization of finite vector spaces

In this section the interval $\mathrm{Int}(M)$ is determined for those monoids M on finite sets A ($|A| \geq 3$) which contain all the constants and have the property that every nonconstant operation in M is a permutation. The main result, which was proved by P. P. Pálfy [1984], shows that $|\mathrm{Int}(M)| \leq 2$ for all such M, moreover, equality holds if and only if M is the monoid of all unary polynomial operations of a vector space.

THEOREM 3.2. *A finite algebra* $\mathcal{A} = (A;F)$ *with* $|A| \geq 3$ *is polynomially equivalent to a vector space if and only if every nonconstant unary polynomial operation of* $\mathcal{A}$ *is a permutation, and at least one operation in* F *depends on at least two of its variables.*

A similar, but slightly weaker statement was proved by Th. Ihringer [1984a]. New proofs were found by B. Jónsson [unpublished] and D. Hobby [1984]. The proof presented here combines some ideas from P. P. Pálfy's and B. Jónsson's approach. The theorem will immediately follow from Lemma 3.3 (with $C = P(\mathcal{A})$) and Proposition 3.4 below.

LEMMA 3.3. *Let* C *be a clone on a finite set* A *with* $|A| \geq 3$ *such that* C *contains all the constants, and every nonconstant unary operation in* C *is a permutation. If an* n*-ary* $(n \geq 1)$ *operation* $f \in C$ *depends on its first variable, then* $f(x,a_2,\ldots,a_n)$ *is a permutation for arbitrary elements* $a_2,\ldots,a_n \in A$.

PROOF. Since $f(x,a_2,\ldots,a_n) \in C$ for every $a_2,\ldots,a_n \in A$, it is a permutation or a constant. However, not all of them are constants, as f depends on its first variable. Assume that, contrary to our claim, there exist $a_2,\ldots,a_n$, $b_2,\ldots,b_n \in A$ such that $f(x,a_2,\ldots,a_n)$ is a permutation while $f(x,b_2,\ldots,b_n)$ is constant. Substituting $b_2,b_3,\ldots$ one-by-one for the corresponding a's we get an i $(2 \leq i \leq n)$ such that

$$f(x,b_2,\ldots,b_{i-1},a_i,a_{i+1},\ldots,a_n) \text{ is a permutation,}$$
$$f(x,b_2,\ldots,b_{i-1},b_i,a_{i+1},\ldots,a_n) \text{ is constant.}$$

Denote the binary operation $f(x,b_2,\ldots,b_{i-1},y,a_{i+1},\ldots,a_n) \in C$ by multiplication, and let $a = a_i$, $b = b_i$. Then xa is a permutation and xb is constant, say $xb = c$. For the (unique) element $b' \in A$ with $b'a = c$, the unary operation $b'y$ takes on the value c at least twice (namely for $y = a$ and

$y = b$), hence $b'y$ is the constant c. This means that in the multiplication table one row and one column are constant c.

	a	b
		c
	⋮	⋮
		c
b'	c ... ccc ...	ccc ...
		c
	⋮	⋮

Since there also exists a column which is a permutation, it follows that the unary operations xu and vy are permutations for all $u,v \in A$, $u \neq b$, $v \neq b'$.

Now define a new binary operation in C by

$$x * y = (\ldots((\underbrace{xy)y)\ldots)y}_{|A|!\text{ times}}.$$

Since for arbitrary element $u \in A$, $x * u$ is the $|A|!$-th power of xu, we have that

$$x * y = \begin{cases} x & \text{if } y \neq b, \\ c & \text{if } y = b. \end{cases}$$

Thus, for $c' \in A - \{c\}$ the unary operation $c' * y \in C$ takes on exactly two values (c and c'), a contradiction.

DEFINITION. We will say that an n-ary operation f on A has the *constant substitution property* (CSP) iff $f(a_1,\ldots,a_{i-1},x,a_{i+1},\ldots,a_n)$ is a permutation for every $1 \leq i \leq n$ and for arbitrary elements $a_j \in A$ $(1 \leq j \leq n,\ j \neq i)$.

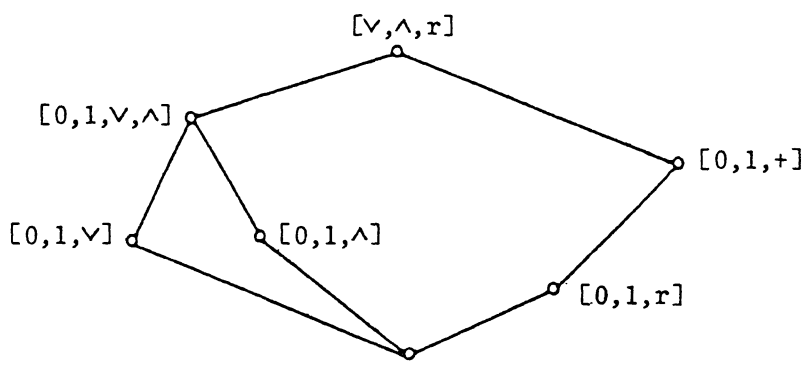
PROPOSITION 3.4. *A finite algebra* $\mathcal{A} = (A;F)$ $(|A| \geq 2)$ *is polynomially equivalent to a vector space if and only if* F *contains an operation depending on at least two of its variables, and every polynomial operation of* $\mathcal{A}$ *which depends on all of its variables has the* CSP.

PROOF. The necessity of the conditions is obvious. To prove the sufficiency, let $\overline{\mathcal{A}}$ denote the algebra arising from $\mathcal{A}$ by adding the constants as new basic operations. Clearly, $T(\overline{\mathcal{A}}) = P(\overline{\mathcal{A}}) = P(\mathcal{A})$. By our assumption on F, $T(\overline{\mathcal{A}})$ is a nonunary clone. Let $g \in T(\overline{\mathcal{A}})$ be an n-ary operation depending on all of its variables $(n \geq 2)$. Since g has the CSP, every binary operation $g(x,y,a_3,\ldots,a_n) \in T(\overline{\mathcal{A}})$ $(a_3,\ldots,a_n \in A)$ is a quasigroup operation. Hence by Proposition 1.21, $T(\overline{\mathcal{A}})$ contains a Mal'tsev operation.

Applying Theorem 2.4(iv) we show that $\overline{\mathcal{A}}$ is an affine algebra. Suppose not, and let s be a ternary operation in $P(\overline{\mathcal{A}})$ $(= P(\mathcal{A}))$, distinct from the first projection and satisfying the identities (2.7). It is easy to see that s depends on all the three variables. Hence s has the CSP. On the other hand, by (2.7), the unary operation $s(a,y,b) \in P(\overline{\mathcal{A}})$ $(a,b \in A,\ a \neq b)$ sends both a and b to a, a contradiction.

Corollary 2.7 implies now that there exists a faithful unitary R-module ${}_R\underline{A}$ $(R \subseteq \mathrm{End}\ \underline{A})$ such that $P(\overline{\mathcal{A}}) = P({}_R\underline{A})$. The CSP ensures that every element of $R - \{0\}$ is a permutation. Hence, by the finiteness, R is a field.

The claim of Theorem 3.2 is obviously not true for 2-element algebras; for instance, the 2-element Boolean algebra is a counter-example. It is easy to see from Post's lattice (see Chapter 1) that on the 2-element set $\{0,1\}$ there are exactly 7 clones containing both constants, namely the following:



Congruence lattices of finite algebras

The so-called *abstract representation problem for congruence lattices*, in its most general form, is the following: For which lattices L does there exist an algebra $\mathcal{A}$ such that the congruence lattice $\mathrm{Con}\mathcal{A}$ of $\mathcal{A}$ is isomorphic to L? G. Grätzer and E. T. Schmidt [1963] solved the problem by proving that every algebraic lattice is isomorphic to the congruence lattice of some algebra. In particular, it follows that for every finite lattice L there is an algebra $\mathcal{A}$ with $L \cong \mathrm{Con}\mathcal{A}$, however, the proof always yields an infinite algebra $\mathcal{A}$. The simpler proof for the Grätzer-Schmidt Theorem found by P. Pudlák [1976] yields, for certain finite lattices L, a finite algebra $\mathcal{A}$, however, the answer to the following question is still unknown.

PROBLEM. Is it true that every finite lattice is isomorphic to the congruence lattice of a finite algebra?

The results presented in this section seem to support the conjecture that the answer is negative, but they have independent interest as well. First we show that there are a lot of finite lattices L such that L can be represented as the congruence lattice of a finite algebra if and only if there are a finite set A and a permutation group G acting on A with $L \cong \mathrm{Con}(A;G)$.

DEFINITION. Let L be a lattice. A mapping $\varphi: L \to L$ is called *decreasing* [*increasing*] iff $x\varphi \leq x$ [$x\varphi \geq x$] for all $x \in L$. A decreasing [increasing] mapping $\varphi: L \to L$ is said to be *strictly decreasing* [*strictly increasing*] iff $x\varphi = x$ holds only if $x = 0$ [resp. $x = 1$].

THEOREM 3.5. *Let L be a finite simple lattice with $|L| > 2$ such that*

(a) *the constant 0 is the only strictly decreasing join endomorphism of L, or*

(b) *the constant 1 is the only strictly increasing meet endomorphism*

of L.

If $\mathcal{A} = (A;F)$ *is a finite algebra of minimum cardinality such that* $\mathrm{Con}\,\mathcal{A} \cong L$, *then* $\mathcal{A}$ *is polynomially equivalent to a vector space or to a unary algebra* $(A;G)$ *where* G *is a permutation group acting on* A.

REMARK. We will prove in Chapter 6 that conditions (a) and (b) are equivalent for every finite simple lattice L. Some other characterizations for these lattices will also be given there. (See Corollary 6.22.)

It is easy to see that every finite lattice in which the join of atoms is 1 satisfies condition (a), and dually, every finite lattice in which the meet of coatoms is 0 satisfies condition (b). Thus we get

COROLLARY 3.6. *Let* L *be a finite simple lattice with* $|L| > 2$ *in which*

(a)' *the join of atoms is* 1, *or*

(b)' *the meet of coatoms is* 0.

If $\mathcal{A} = (A;F)$ *is a finite algebra of minimum cardinality such that* $\mathrm{Con}\,\mathcal{A} \cong L$, *then* $\mathcal{A}$ *is polynomially equivalent to a vector space or to a unary algebra* $(A;G)$ *where* G *is a permutation group acting on* A.

PROOF of Theorem 3.5. Let $\mathcal{A} = (A;F)$ be an arbitrary finite algebra such that $\mathrm{Con}\,\mathcal{A} \cong L$, and let $U = P^{(1)}(\mathcal{A})$. It is well known that the algebra $\tilde{\mathcal{A}} = (A;U)$ has the same congruences as $\mathcal{A}$, so $\mathrm{Con}\,\tilde{\mathcal{A}} \cong L$. Consider the family of nonsingleton subsets of A of the form h(A) with $h \in U$. This family being finite and nonempty (it contains A) we can select from it a set B which is minimal with respect to inclusion. Now put

$$U_B = \{f \in U: f(A) \subseteq B\}, \quad U|_B = \{f|_B: f \in U_B\}$$

where $f|_B$ denotes the restriction of f to B, and let $\tilde{\mathcal{A}}|_B = (B;U|_B)$. The following two claims are straightforward to verify.

Claim 1. For arbitrary congruence δ of $\tilde{\mathcal{A}}|_B$ the binary relation $\hat{\delta}$ defined by

$$\hat{\delta} = \{(x,y) \in A^2 : (f(x),f(y)) \in \delta \text{ for all } f \in U_B\}$$

is a congruence of $\tilde{\mathcal{A}}$.

Moreover, we have

Claim 2. $\hat{\delta}$ contains every congruence ε of $\tilde{\mathcal{A}}$ with the property $\varepsilon|_B \subseteq \delta$.

Here $\varepsilon|_B$ denotes the restriction of ε to B, that is, $\varepsilon|_B = \varepsilon \cap B^2$. Obviously, $\varepsilon|_B \in \operatorname{Con} \tilde{\mathcal{A}}|_B$ whenever $\varepsilon \in \operatorname{Con}\tilde{\mathcal{A}}$. Now we want to prove

Claim 3. There exists an operation $e \in U$ such that $e = e^2$ and $B = e(A)$.

Suppose first that (b) holds for L, and consider the mapping

$$\Phi: \operatorname{Con}\tilde{\mathcal{A}} \to \operatorname{Con}\tilde{\mathcal{A}}, \quad \alpha \mapsto \widehat{\alpha|_B}.$$

It follows easily from the definition of $\widehat{\ }$ and from Claim 2 that Φ is an increasing meet endomorphism. Since not all operations $f \in U_B$ are constant, we have $\Delta_A\Phi \neq \nabla_A$. Thus, by (b), Φ is not strictly increasing, therefore there exists a congruence $\gamma \in \operatorname{Con}\tilde{\mathcal{A}}$ such that $\gamma \neq \nabla_A$ and $\gamma\Phi = \gamma$. Consequently $\Delta_A\Phi^2 \subseteq \gamma\Phi^2 = \gamma \neq \nabla_A$, implying $\Delta_A\Phi^2 \subset \nabla_A$. By the definition of Φ this is equivalent to the existence of elements $a,b \in A$ and operations $f,g \in U_B$ such that $fg(a) \neq fg(b)$. Then $fg(A)$ is not a singleton and $fg(A) \subseteq B$, whence by the minimality of B it follows that $fg(A) = B$. Since $f,g \in U_B$ and B is finite, this implies that $f(B) = B$. So by the finiteness we also get that some power e of f satisfies the requirements of the claim.

Assume now that (a) holds for L. Let Ψ denote the mapping $\operatorname{Con}\tilde{\mathcal{A}} \to \operatorname{Con}\tilde{\mathcal{A}}$ assigning to each $\alpha \in \operatorname{Con}\tilde{\mathcal{A}}$ the congruence of $\tilde{\mathcal{A}}$ generated by

$$\{(f(x),f(y)): (x,y) \in \alpha, \quad f \in U_B\}.$$

Clearly, Ψ is a decreasing join endomorphism. Again, since not all operations $f \in U_B$ are constant, we have $\nabla_A\Psi \neq \Delta_A$. Thus, by (a), Ψ is not strictly decreasing, therefore there exists $\beta \in \mathrm{Con}\,\mathcal{A}$ such that $\beta \neq \Delta_A$ and $\beta\Psi = \beta$. Hence $\nabla_A\Psi^2 \supseteq \beta\Psi^2 = \beta \neq \Delta_A$, implying $\nabla_A\Psi^2 \supset \Delta_A$. The latter is again equivalent to the existence of elements $a,b \in A$ and operations $f,g \in U_B$ such that $fg(a) \neq fg(b)$. So we can repeat the argument at the end of the preceding paragraph to conclude the proof of Claim 3.

Let us fix an operation $e \in U$ satisfying the requirements of Claim 3. We want to show that $\mathrm{Con}\,\mathcal{A} \cong \mathrm{Con}\,\mathcal{A}|_B$. Since $\mathrm{Con}\,\mathcal{A}$ ($\cong L$) is a simple lattice, it suffices to prove

Claim 4. The restriction of congruences to B is a surjective lattice homomorphism $|_B: \mathrm{Con}\,\mathcal{A} \to \mathrm{Con}\,\mathcal{A}|_B$.

First we show that for every $\delta \in \mathrm{Con}\,\mathcal{A}|_B$ the congruence $\hat{\delta}$ of $\mathcal{A}$ defined in Claim 1 has the property $\hat{\delta}|_B = \delta$. Since the operations of $\mathcal{A}|_B$ are of the form $f|_B$ with $f \in U_B$, the inclusion $\hat{\delta}|_B \supseteq \delta$ follows easily from the definition of $\hat{\delta}$. Conversely, if $(a,b) \in \hat{\delta}|_B$, then $(e(a),e(b)) \in \delta$. However, as $e = e^2$ and $a,b \in B = e(A)$, therefore $e(a) = a$ and $e(b) = b$, so that $(a,b) \in \delta$. Thus $\hat{\delta}|_B \subseteq \delta$ holds as well. This proves the surjectivity of $|_B$. Moreover, we get that Claim 2 can be strengthened as follows: for arbitrary congruences $\delta \in \mathrm{Con}\,\mathcal{A}|_B$ and $\varepsilon \in \mathrm{Con}\,\mathcal{A}$ we have $\varepsilon \subseteq \hat{\delta}$ if and only if $\varepsilon|_B \subseteq \delta$. Applying this statement we prove that $|_B$ is a join homomorphism. Let $\alpha,\beta \in \mathrm{Con}\,\mathcal{A}$ be arbitrary. Since $\alpha|_B \subseteq \widehat{\alpha|_B \vee \beta|_B}$, it follows that $\alpha \subseteq \widehat{\alpha|_B \vee \beta|_B}$. By symmetry this implies that $\alpha \vee \beta \subseteq \alpha|_B \vee \beta|_B$, which is equivalent to $(\alpha\vee\beta)|_B \subseteq \alpha|_B \vee \beta|_B$. The reverse inclusion trivially holds. Thus $|_B$ is a join homomorphism. Clearly, it is also a meet homomorphism, completing the proof of Claim 4.

In the same way as we defined $\tilde{\mathcal{A}}|_B$ from $\tilde{\mathcal{A}}$, we can construct an algebra $\mathcal{A}|_B$ from $\mathcal{A}$ where $\mathcal{A}$ is considered up to polynomial equivalence only. Namely, let $\mathcal{A}|_B = (B;P|_B)$ where

$$P|_B = \{f|_B : n \geq 1,\ f \in P^{(n)}(\mathcal{A}),\ f(A^n) \subseteq B\}. \tag{3.1}$$

Alternatively, $P|_B$ can be described as follows:

$$P|_B = \{g|_B : n \geq 1,\ g \in P^{(n)}(\mathcal{A}),\ g(B^n) \subseteq B\}. \tag{3.2}$$

Indeed, the first set is trivially included in the second one, while if $g \in P(\mathcal{A})$ is an n-ary operation with $g(B^n) \subseteq B$, then for the operation $f(x_1,\ldots,x_n) = g(e(x_1),\ldots,e(x_n)) \in P(\mathcal{A})$ we have $f(A^n) \subseteq B$ and $f|_B = g|_B$, so the reverse inclusion also holds. Thus (3.2) shows that $P|_B = P(\mathcal{A}|_B)$, and by (3.1), $U|_B = P^{(1)}(\mathcal{A}|_B)$.

Using the well-known fact that $\mathcal{A}|_B$ and $\tilde{\mathcal{A}}|_B = (B;P^{(1)}(\mathcal{A}|_B))$ have the same congruences, we get the isomorphisms

$$\operatorname{Con}\mathcal{A}|_B = \operatorname{Con}\tilde{\mathcal{A}}|_B \cong \operatorname{Con}\tilde{\mathcal{A}} = \operatorname{Con}\mathcal{A} \cong L.$$

On the other hand, if $f|_B \in U|_B$ $(f \in U_B)$ is not constant, then $f(B) = fe(A)$ $(\subseteq B)$ is not a singleton, hence by the minimality of B we have $f(B) = B$, that is, $f|_B$ is a permutation. This means that every unary polynomial operation of $\mathcal{A}|_B$ is either constant or a permutation. The assumption $|L| > 2$ implies that $|B| > 2$. Thus, by Theorem 3.2, $\mathcal{A}|_B$ is polynomially equivalent to a vector space provided $P|_B$ contains an operation depending on at least two of its variables. In the opposite case $\mathcal{A}|_B$ is polynomially equivalent to the algebra $(B;G)$ where G is the set of permutations from $U|_B$. Since $U|_B$ is closed under composition and B is finite, G is a permutation group.

Clearly, if $\mathcal{A}$ is assumed to be of minimum cardinality such that $\operatorname{Con}\mathcal{A} \cong L$, then we must have $B = A$, and the conclusion of the theorem holds for $\mathcal{A}$.

Notice that we proved more than what was actually stated in Theorem 3.5, namely the following: If L satisfies the assumptions of the theorem, then every algebra $\mathcal{A}$ with $\mathrm{Con}\,\mathcal{A} \cong L$ contains a subset B such that the so-called *induced algebra* $\mathcal{A}|_B$ is polynomially equivalent to a vector space or to a unary algebra $(B;G)$ with G a permutation group acting on B, and $\mathrm{Con}\,\mathcal{A}|_B \cong L$. This result was first observed by R. McKenzie [1983] (in fact, he drew the same conclusion under weaker assumptions on L), although some ideas go back to P. P. Pálfy and P. Pudlák [1980]. Since then a far-reaching theory on the structure of finite algebras and locally finite varieties has been developed from these ideas, see D. Hobby and R. McKenzie [a].

We sketch the starting point of the theory. Observe that in the proof of Theorem 3.5 the assumption $|L| > 2$ was used only to ensure $|B| > 2$. Therefore the same argument as in the proof of Theorem 3.5, combined with Theorem 3.2 and the remark at the end of the preceding section, yields that for arbitrary finite simple algebra $\mathcal{A}$, the induced algebras $\mathcal{A}|_B$ are polynomially equivalent to

I. a unary algebra $(B;G)$ with G a permutation group on B, or

II. a vector space, or

III. a 2-element Boolean algebra, or

IV. a 2-element lattice, or

V. a 2-element semilattice.

Moreover, it can be shown that all these induced algebras $\mathcal{A}|_B$ of $\mathcal{A}$ are of the same type. So this type characterizes the simple algebra $\mathcal{A}$. In a similar fashion, for arbitrary finite algebra $\mathcal{A}$ one of the types I - V can be assigned to each prime interval of the congruence lattice of $\mathcal{A}$. It turns out that the type of a finite simple algebra $\mathcal{A}$ (or the type set of a finite algebra $\mathcal{A}$) has strong implications on the structure of $\mathcal{A}$. For example, a finite simple algebra is of type I or II if and only if it is a TC-algebra, and every finite

simple algebra of type IV or V has a compatible ordering (see R. McKenzie [a], D. Hobby and R. McKenzie [a]).

Returning to the representation problem of finite lattices we next prove the theorem of P. P. Pálfy and P. Pudlák [1980] relating this problem to the characterization of principal filters of subgroup lattices of finite groups.

THEOREM 3.7. *The following statements are equivalent:*

(i) *Every finite lattice is isomorphic to the congruence lattice of a finite algebra.*

(ii) *Every finite lattice is isomorphic to a principal filter of the subgroup lattice of a finite group.*

The proof is based on a consequence of Corollary 3.6(a)'.

PROPOSITION 3.8. *Let* ($|L| > 2$) *be a finite simple lattice in which the join of atoms is* 1, *and for every element* $a \in L - \{0\}$ *such that* a *is not an atom* L *contains at least* 4 *atoms less than* a. *Then the following conditions are equivalent:*

(i) *there exists a finite algebra* $\mathcal{A}$ *with* $\mathrm{Con}\,\mathcal{A} \cong L$;

(ii) *there exists a transitive permutation group* G *acting on some finite set* A *such that* $\mathrm{Con}(A;G) \cong L$;

(iii) *there exist a finite group* G *and a subgroup* H *of* G *such that the principal filter* [H,G] *of the subgroup lattice of* G *is isomorphic to* L.

PROOF. Assuming (i) consider a finite algebra $\mathcal{A} = (A;F)$ of minimum cardinality with $\mathrm{Con}\,\mathcal{A} \cong L$. Since the congruences of $\mathcal{A}$ and $(A;P^{(1)}(\mathcal{A}))$ coincide, we may assume that $\mathcal{A}$ is a unary algebra. Hence, by Corollary 3.6(a)', it is polynomially equivalent to $\mathcal{A}' = (A;G)$ for some permutation group G acting on A. Clearly, $\mathrm{Con}\,\mathcal{A}' = \mathrm{Con}\,\mathcal{A} \cong L$. So it remains to show that G is transitive, that is, $\mathcal{A}'$ has no proper subalgebras.

It is easy to see that A can be decomposed into a disjoint union of minimal subuniverses A_i $(1 \le i \le k)$ of $\mathcal{A}'$ (the orbits of G), and every subuniverse is a union of some of them. Suppose $\mathcal{A}'$ has two disjoint subalgebras $\mathcal{B}_1$, $\mathcal{B}_2$ with universes B_1, B_2 such that $B_1 \cup B_2 = A$ and $|B_i| \ge 2$ $(i = 1,2)$. Then select an atom α_i from $\operatorname{Con} \mathcal{B}_i$ $(i = 1,2)$. The smallest extension $\bar{\alpha}_i \in \operatorname{Con} \mathcal{A}'$ of α_i is $\bar{\alpha}_i = \alpha_i \cup \Delta_A$ $(i = 1,2)$, so it is easily seen that $\bar{\alpha}_1 \vee \bar{\alpha}_2$ contains only two atoms (namely $\bar{\alpha}_1$ and $\bar{\alpha}_2$), contradicting our assumption on L. Thus we can have only the following possibilities:

(1) $k = 3$, $|A_1| = |A_2| = |A_3| = 1$,

(2) $k = 2$, $|A_1| = |A_2| = 1$,

(3) $k = 2$, $|A_1| = 1$, $|A_2| > 1$,

(4) $k = 1$.

In the first two cases $|G| = 1$, hence $\operatorname{Con} \mathcal{A}'$ is the partition lattice on a 3-element or a 2-element set, but these lattices do not satisfy the assumptions. In case (3) the greatest congruence $\nabla_A \in \operatorname{Con} \mathcal{A}'$ is join irreducible, which is again impossible. Thus (4) holds, that is, $\mathcal{A}'$ has no proper subalgebras. This completes the proof of (ii).

The implication (ii) $\Rightarrow$ (iii) follows from

Claim 1. Let $\mathcal{A} = (A;G)$ be a unary algebra with G a transitive permutation group on A, and let $a \in A$, $G_a = \{g \in G: g(a) = a\}$. Then $\operatorname{Con} \mathcal{A}$ is isomorphic to the principal filter $[G_a,G]$ of the subgroup lattice of G.

The mappings

$$\Phi: \operatorname{Con} \mathcal{A} \rightleftarrows [G_a,G]: \Psi$$

$$\Phi: \rho \mapsto \rho\Phi = \{g \in G: (g(a),a) \in \rho\},$$

$$H\Psi = \{(gh(a),g(a)): g \in G, \ h \in H\} \mapsfrom H: \Psi$$

are mutually inverse lattice isomorphisms. Indeed, it is straightforward to check that for H and ρ as above, $H\Psi \in \operatorname{Con} \mathcal{A}$, $\rho\Phi$ is a subgroup of G with

$\rho\Phi \supseteq G_a$, and $H\Psi\Phi = H$. Furthermore, we have $(b,c) \in \rho\Phi\Psi$ if and only if there exist $g,h \in G$ such that $b = gh(a)$, $c = g(a)$ and $(h(a),a) \in \rho$. Since G is transitive, this is equivalent to $(b,c) \in \rho$. Therefore $\rho\Phi\Psi = \rho$. Finally, for $\rho,\sigma \in \mathrm{Con}\,\mathcal{A}$ we have $\rho\Phi \subseteq \sigma\Phi$ if and only if $\rho \subseteq \sigma$.

Suppose now that (iii) holds. If G has a normal subgroup N with $N \subseteq H$, then $[H/N,G/N] \cong [H,G]$. So we may assume that H contains no nontrivial normal subgroup of G. Every element $g \in G$ defines a permutation g' on the set $A = \{xH: x \in G\}$ of left cosets of H by multiplication: $g'(xH) = gxH$. It is easy to see that the mapping $g \mapsto g'$ is an isomorphism between G and the permutation group $G' = \{g': g \in G\}$. Furthermore, G' is transitive, and G'_H coincides with the subgroup $H' = \{h': h \in H\}$ of G'. Hence, by Claim 1, $L \cong [H,G] \cong [H',G'] \cong \mathrm{Con}(A;G')$, proving (i).

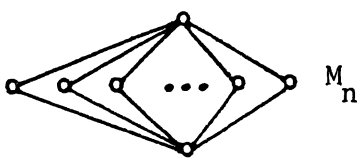
PROOF of Theorem 3.7. In view of Proposition 3.8 it suffices to show that every finite lattice can be embedded as a principal filter into a lattice L satisfying the assumptions of the proposition. Given a finite lattice L_o we construct a new lattice L consisting of the elements of L_o, pairwise distinct elements $z_i \notin L_o$ $(i = 1,2,3,4)$ for every $z \in L_o$, and another element o. For $x,y \in L$ let

$$x \leq y \text{ iff } \begin{cases} x = y, \text{ or} \\ x = o, \ y \text{ arbitrary, or} \\ x = z_i \text{ for some } z \in L_o, \ 1 \leq i \leq 4, \ y \in L_o \\ \qquad \text{and } z \leq y \text{ in } L_o, \text{ or} \\ x,y \in L_o \text{ and } x \leq y \text{ in } L_o. \end{cases}$$

It is not hard to verify that L is a lattice. The atoms of L are exactly the elements z_i $(z \in L_o, \ i = 1,2,3,4)$, and the least element is o, while the greatest element is 1 $(\in L_o)$. Thus the condition that every element which is

neither an atom nor the least element is greater than at least 4 atoms is clearly satisfied in L. Furthermore, we have $1_1 \vee 1_2 = 1$, hence the join of atoms is 1. The simplicity of L can be checked by routine computations. Obviously, the identity mapping embeds L_o into L as a principal filter.

In trying to solve the representation problem for particular finite lattices, most investigations were concentrated on the lattices of height 2. Let M_n denote the lattice of height 2 with n atoms:



If n-1 is a prime power, then the congruence lattice of the 2-dimensional vector space over the field of order n-1 is isomorphic to M_n, therefore M_n is representable. So the question is whether M_n is representable for $n = 7,11,13, \ldots$. It is clear that for $n \geq 4$ the lattice M_n satisfies the assumptions of Proposition 3.8, therefore it is representable as a congruence lattice of a finite algebra if and only if it is isomorphic to a principal filter of the subgroup lattice of a finite group. Recently, W. Feit [1983] [unpublished], found a principal filter isomorphic to M_7, and one isomorphic to M_{11} in the subgroup lattice of the alternating group A_{31} of degree 31. However, these examples seem to be quite accidental. It can be shown (P. P. Pálfy [a]) that A_{31} is the only alternating group of prime degree whose subgroup lattice contains a principal filter isomorphic to some M_n with $n \geq 7$. So, at present, the smallest lattice of height 2 for which the problem of representability is open is M_{13}.

By a result of P. Köhler [1983], if a finite group G has a subgroup H not containing a nontrivial normal subgroup of G and such that $[H,G] \cong M_n$ for

some n with $n-1$ not a prime power, then G must be subdirectly irreducible; as was shown by P. P. Pálfy and P. Pudlák [1980], G has to be nonsolvable, too. Attacking the representation problem from another direction, Th. Ihringer [1984b] investigated some properties of the (possibly nonexisting) finite algebras $\mathcal{A}$ with $\mathrm{Con}\,\mathcal{A} \cong M_n$, $n-1$ not a prime power. R. McKenzie [1983] proved that many lattices, including all M_n with $n-1$ not a prime power, cannot be isomorphic to the congruence lattice of a finite algebra with a single basic operation.

Chapter 4

QUASI-PRIMAL AND PARA-PRIMAL ALGEBRAS

Recall from Chapter 1 that an algebra $\mathcal{A} = (A;F)$ is called *primal* iff it is finite and every operation on A is a term operation of $\mathcal{A}$. A. L. Foster [1953] introduced primal algebras as a natural generalization of the 2-element Boolean algebra, and studied first of all the structure of algebras in the variety generated by a primal algebra.

EXAMPLES. Some of the most well-known primal algebras are the following:

1. the 2-element Boolean algebra,
2. every finite field of prime order (1 is considered as an operation),
3. the Post algebras $\mathfrak{P}_n$ $(n \geq 1)$ defined in Chapter 1,
4. the reduct $\mathfrak{M}_n = (\{0,1,\ldots,n-1\};r(x \vee y))$ of $\mathfrak{P}_n$ for every $n \geq 1$ (D. Webb [1935]).

We have seen in Chapter 1 that the description of all maximal clones on a finite set yields a necessary and sufficient condition for a finite algebra to be primal (Corollary 1.20). For our purposes here some older and easier characterizations of primal algebras will be more useful.

THEOREM 4.1. *For a finite algebra* $\mathcal{A} = (A;F)$ *the following conditions are equivalent:*

(i) $\mathcal{A}$ *is primal;*

(ii) *for each natural number* k, *each subuniverse* B *of* $\mathcal{A}^k$, *and each set* I *containing exactly one element from each block of the equivalence* ~ *defined on* {1,...,k} *by*

$$i \sim j \quad \text{iff} \quad \mathrm{pr}_{i,j} B \subseteq \Delta_A \qquad (1 \le i,j \le k),$$

we have $\mathrm{pr}_I B = A^I$;

(iii) $\mathcal{A}$ *is a simple arithmetical algebra having no proper subalgebras and no nontrivial automorphisms.*

Condition (iii) characterizing primal algebras is due to A. L. Foster and A. F. Pixley [1964], while (ii) seems to have been discovered independently by several authors, e.g. I. G. Rosenberg [1970], P. H. Krauss [1972]. The proof of Theorem 4.1 is delayed until Theorem 4.2 from which it will immediately follow.

A number of generalizations of primal algebras were defined by weakening one or another of the conditions in Theorem 4.1. Here we deal only with the two most important among them. A different kind of generalization will be discussed in Chapter 6.

Quasi-primal algebras

How far is a finite field of order q^k (q prime, $k > 1$) from being primal? By all means, it has proper subfields, and every subfield of order greater than q has nontrivial automorphisms. We want to generalize primal algebras so as to admit subalgebras and isomorphisms between subalgebras.

DEFINITION. An isomorphism between two subalgebras of an algebra $\mathcal{A}$ is called an *internal isomorphism* of $\mathcal{A}$.

Note that a bijection $\pi: B \to C$ with $B,C \subseteq A$ is an internal isomorphism of $\mathcal{A} = (A;F)$ if and only if $\pi^\square$ is a subuniverse of $\mathcal{A}^2$. The set of these subuniverses $\pi^\square$ will be denoted by $\mathrm{Iso}\,\mathcal{A}$.

DEFINITION. An algebra $\mathcal{A} = (A;F)$ is called *quasi-primal* iff it is finite and every operation on A preserving the internal isomorphisms of $\mathcal{A}$ is a term operation of $\mathcal{A}$.

Note that every operation preserving the internal isomorphisms of $\mathcal{A}$ preserves the identity automorphism of each subalgebra, and hence preserves each subalgebra as well. Quasi-primal algebras were introduced by A. F. Pixley [1970], [1971]. We mention several examples of quasi-primal algebras.

EXAMPLES. 1. Every primal algebra is quasi-primal.

2. Finite fields are quasi-primal.

3. For a set A, the *discriminator* t on A is defined by

$$t(a,b,c) = \begin{cases} c & \text{if } a = b \\ a & \text{otherwise} \end{cases} \qquad (a,b,c \in A).$$

The algebra $(A;t)$ is quasi-primal for every finite set A.

The characterizations of primal algebras in Theorem 4.1 carry over nicely to quasi-primal algebras.

THEOREM 4.2. *For a finite algebra $\mathcal{A} = (A;F)$ the following conditions are equivalent:*

(i) *$\mathcal{A}$ is quasi-primal;*

(ii) *for each natural number k, each subuniverse B of $\mathcal{A}^k$, and each set I containing exactly one element from each block of the equivalence $\sim$ on $\{1,\ldots,k\}$ defined by*

$$i \sim j \quad \text{iff} \quad \mathrm{pr}_{i,j} B \in \mathrm{Iso}\,\mathcal{A} \qquad (1 \le i,j \le k),$$

we have $\mathrm{pr}_I B = \prod_{i \in I} \mathrm{pr}_i B$;

(iii) *t is a term operation of $\mathcal{A}$;*

(iv) *$\mathcal{A}$ is arithmetical and every subalgebra of $\mathcal{A}$ is simple.*

PROOF. To verify (i) $\Rightarrow$ (ii) assume $\mathcal{A}$ is quasi-primal, and consider a subuniverse $B \leqslant B_1 \times \ldots \times B_k$ of $\mathcal{A}^k$. It is straightforward to check that $\sim$ is indeed an equivalence relation. Assume for simplicity that $I = \{1,\ldots,m\}$ contains exactly one element from each block of $\sim$. Clearly, $\mathrm{pr}_I B \subseteq B_1 \times \ldots \times B_m$. We have to show that equality holds. Let $n = |\mathrm{pr}_I B|$ and

$$\mathrm{pr}_I B = \{(b_{\ell 1},\ldots,b_{\ell m}): 1 \leq \ell \leq n\}.$$

Since $\mathrm{pr}_{i,j} B = \{(b_{\ell i},b_{\ell j}): 1 \leq \ell \leq n\}$ $(1 \leq i,j \leq m)$, our assumption on I implies that for $i \neq j$ there exists no internal isomorphism $\pi: B_i \to B_j$ of $\mathcal{A}$ with $b_{\ell i}\pi = b_{\ell j}$ for all $1 \leq \ell \leq n$. Hence, for arbitrary m-tuple $(a_1,\ldots,a_m) \in B_1 \times \ldots \times B_m$ there is an n-ary operation f preserving the internal isomorphisms of $\mathcal{A}$ such that

$$f(b_{1i},\ldots,b_{ni}) = a_i \quad \text{for} \quad i = 1,\ldots,m.$$

However, $\mathcal{A}$ being quasi-primal, f is a term operation of $\mathcal{A}$. Therefore the subuniverse $\mathrm{pr}_I B$ of $\mathcal{A}^m$ contains $(a_1,\ldots,a_m)$, proving that $\mathrm{pr}_I B = B_1 \times \ldots \times B_m$.

By Corollary 1.4 the implication (ii) $\Rightarrow$ (iii) is clear, since t preserves every set B of the form described in (ii). Clearly, t is a 2/3-minority operation. So, to show (iii) $\Rightarrow$ (iv), it suffices to verify that the term operation t forces the subalgebras of $\mathcal{A}$ be simple. The easy details are left to the reader.

Finally, we prove (iv) $\Rightarrow$ (i). Suppose $\mathcal{A}$ has properties (iv), and let p be a Mal'tsev operation among the term operations of $\mathcal{A}$. Since $\mathcal{A}$ has a majority term operation as well, in view of Corollary 1.25 the term operations of

are determined by the subuniverses of $\mathcal{A}^2$. Now let $B \leqslant B_1 \times B_2$ be a subuniverse of $\mathcal{A}^2$. Clearly, B_1 and B_2 are subuniverses of $\mathcal{A}$. Moreover, we have $B \circ B^{\smile} \circ B \subseteq B$, since $(b_1,b_2),(b_1',b_2),(b_1',b_2') \in B$ imply that

$$(b_1,b_2') = p((b_1,b_2),(b_1',b_2),(b_1',b_2')) \in B.$$

Hence $B \circ B^{\smile}$ and $B^{\smile} \circ B$ are congruences of the subalgebras $\mathfrak{B}_1 = (B_1;F)$ and $\mathfrak{B}_2 = (B_2;F)$ of $\mathcal{A}$, respectively. Since $\mathfrak{B}_1$ and $\mathfrak{B}_2$ are simple, there are two possibilities. If both $B \circ B^{\smile}$ and $B^{\smile} \circ B$ are the equality relation, then $B = \pi^{\square}$ for an isomorphism $\pi: \mathfrak{B}_1 \to \mathfrak{B}_2$. If $B \circ B^{\smile} = \nabla_{B_1}$ or $B^{\smile} \circ B = \nabla_{B_2}$, then $B_1 \times B_2 \subseteq B \circ B^{\smile} \circ B$, yielding that $B = B_1 \times B_2$. In either case, every operation on A preserving the internal isomorphisms of $\mathcal{A}$ preserves B. Thus $\mathcal{A}$ is quasi-primal, completing the proof.

Except for characterization (ii) which is due to P. H. Krauss [1973], Theorem 4.2 was found by A. F. Pixley [1970], [1971]. Observe that Theorem 4.1 is an easy consequence of Theorem 4.2.

Condition (iii) shows an interesting feature of quasi-primal algebras: up to term equivalence, there is a least quasi-primal algebra on every finite set A, namely $(A;t)$. In other words, the clones of quasi-primal algebras on a finite set A form a principal filter in the clone lattice, the least element of the filter being $[t]$.

Idempotent non-quasi-primal algebras

The main result of this section, Theorem 4.3, prepares the study of paraprimal algebras as well as the description of homogeneous algebras to be discussed in the next chapter.

Let A be a finite set, and let $B \leqslant B_1 \times \ldots \times B_k$ $(k \geq 1)$ be a subset of A^k. The number $\max\{|B_i|: 1 \leq i \leq k\}$ will be called the *size* of B and will be denoted by $\|B\|$. The subset B of A^k will be termed *directly indecomposable* iff $B \not\cong (\mathrm{pr}_I B) \times (\mathrm{pr}_{\overline{I}} B)$ holds for all partitions $\{I,\overline{I}\}$ of $\underline{k} = \{1,\ldots,k\}$. Furthermore, B is said to be *reduced* iff B is directly indecomposable and no

projection $pr_{i,j}\ B$ $(1 \le i < j \le k)$ of B is of the form $\pi^{\square}$ for a bijection $\pi: B_i \to B_j$. (For brevity, these sets $\pi^{\square}$ will also be called bijections.)

It is clear from Theorem 4.2 that a finite algebra $\mathcal{A} = (A;F)$ is quasi-primal if and only if $\mathcal{A}^k$ has no reduced subuniverses for $k \ge 2$.

THEOREM 4.3. *Let $\mathcal{A} = (A;F)$ be a finite idempotent algebra. Suppose is not quasi-primal, and let $B \prec B_1 \times \ldots \times B_n$ be a reduced subuniverse of $\mathcal{A}^n$ for some $n \ge 2$. Then either*

(a) *$\mathcal{A}^2$ has a reduced subuniverse of the same size as B, or*

(b) *$\mathcal{B}_i = (B_i;F)$ $(1 \le i \le n)$ are isomorphic affine subalgebras of $\mathcal{A}$, and there exist a finite field K and a vector space ${}_K\underline{B}_1 = (B_1;+,K)$ such that $\mathcal{B}_1$ is term equivalent to the full idempotent reduct of the $(\mathrm{End}\ {}_K\underline{B}_1)$-module $(\mathrm{End}\ {}_K\underline{B}_1)^{\underline{B}_1}$.*

First we prove a weaker statement.

LEMMA 4.4. *Let $\mathcal{A} = (A;F)$ be a finite idempotent algebra with $|A| > 1$, and assume $\mathcal{A}^2$ has no reduced subuniverse of size m for some integer $1 < m \le |A|$. If $B \prec B_1 \times \ldots \times B_n$ is a directly indecomposable subuniverse of $\mathcal{A}^n$ $(n \ge 2)$ of size m, then*

(b_1) *$\mathcal{B}_i = (B_i;F)$ $(1 \le i \le n)$ are isomorphic subalgebras of $\mathcal{A}$, and*

(b_2) *for arbitrary isomorphisms $\pi_i: \mathcal{B}_i \to \mathcal{B}_1$ $(1 \le i \le n)$ we have*

$$B[\pi_1,\ldots,\pi_n] \approx \{(y_1,\ldots,y_{u-1},g_u(y_1,\ldots,y_{u-1}),\ldots,g_n(y_1,\ldots,y_{u-1})): y_1,\ldots,y_{u-1} \in B_1\} \tag{4.1}$$

for some $2 \le u \le n$ and some operations $g_j \in O_{B_1}^{(u-1)}$ $(u \le j \le n)$.

PROOF. We start with an auxiliary observation.

Claim 1. Under the assumptions of the lemma, B has a projection $\overline{B} = pr_{i_1,\ldots,i_k} B \leqslant B_{i_1} \times \ldots \times B_{i_k}$ $(\{i_1,\ldots,i_k\} \subseteq \underline{n})$ with $k \ge 2$ such that

(α) $|B_{i_\ell}| = m$ for all $1 \le \ell \le k$,

(β) $\mathrm{pr}_{\underline{\underline{k}}-\{j\}}\, \overline{B} = \prod_{\ell \in \underline{\underline{k}}-\{j\}} B_{i_\ell}$ for all $1 \le j \le k$, and

(γ) $\overline{B}(x_1, b_2, \ldots, b_{j-1}, x_2, b_{j+1}, \ldots, b_k)$ is a bijection $B_{i_1} \to B_{i_j}$ for all $2 \le j \le k$ and for all elements $b_\ell \in B_{i_\ell}$ $(2 \le \ell \le k,\ \ell \ne j)$.

Since B is directly indecomposable, $B \not\approx B_i \times (\mathrm{pr}_{\underline{\underline{n}}-\{i\}} B)$ for all $i \in \underline{\underline{n}}$ (consequently $|B_i| > 1$ for all $i \in \underline{\underline{n}}$). Let, say, $I = \underline{\underline{k}}$ $(k \le n)$ be a minimal subset of $\underline{\underline{n}}$ such that for $\overline{B} = \mathrm{pr}_{\underline{\underline{k}}} B$ we have $\|\overline{B}\| = m$ and

(4.2) $\overline{B} \not\approx B_i \times (\mathrm{pr}_{\underline{\underline{k}}-\{i\}} \overline{B})$ for some $i \in \underline{\underline{k}}$ with $|B_i| = m$; say $i = 1$.

Clearly, $k \ge 2$ and by the minimality

(4.3) $\mathrm{pr}_{\underline{\underline{k}}-\{j\}} \overline{B} \approx B_i \times \mathrm{pr}_{\underline{\underline{k}}-\{i,j\}} \overline{B}$ for all $i,j \in \underline{\underline{k}}$, $i \ne j$, with $|B_i| = m$.

We may assume that $|B_1| \ge |B_2| \ge \ldots \ge |B_k|$.

For arbitrary $(k-2)$-tuple $c = (c_3, \ldots, c_k) \in \mathrm{pr}_{\underline{\underline{k}}-\underline{\underline{2}}} \overline{B}$, the nonempty set $\overline{B}(x_1, x_2, c)$ is a subuniverse of $\mathcal{A}^2$. Property (4.3) for $i = 1$, $j = 2$ ensures that $\mathrm{pr}_1 \overline{B}(x_1, x_2, c) = B_1$, hence $\|\overline{B}(x_1, x_2, c)\| = m$. Therefore, by assumption,

$$\overline{B}(x_1, x_2, c) = B_1 \times (\mathrm{pr}_2 \overline{B}(x_1, x_2, c)) \quad \text{or} \quad \overline{B}(x_1, x_2, c) \text{ is a bijection.}$$

However, in view of (4.2) $(i = 1)$, the former cannot hold for all c, hence

$$\overline{B}(x_1, x_2, a) \text{ is a bijection for some } a = (a_3, \ldots, a_k) \in \mathrm{pr}_{\underline{\underline{k}}-\underline{\underline{2}}} \overline{B}.$$

So $|B_1| = |B_2| = m$, and similarly, $|B_1| = |B_\ell| = m$ for all $2 \le \ell \le k$. This proves (α), whence (4.3) yields (β), too. It follows also that

$$\mathrm{pr}_i \overline{B}(x_1, x_2, c) = B_i \quad \text{for} \quad i = 1,2 \quad \text{and for all} \quad c \in B_3 \times \ldots \times B_k.$$

By symmetry, it suffices to show (γ) for $j = 2$. Supposing it fails we get that

$$\overline{B}(x_1, x_2, b) = B_1 \times B_2 \quad \text{for some} \quad b = (b_3, \ldots, b_k) \in B_3 \times \ldots \times B_k.$$

Then the sequence $\overline{B}(x_1,x_2,b_3,\ldots,b_i,a_{i+1},\ldots,a_k)$ $(i = 2,3,\ldots,k)$ contains two consecutive members such that the first one is a bijection, while the second one equals $B_1 \times B_2$. Permuting the last $k-2$ components of $\overline{B}$ we may assume that $a_j = b_j$ for $4 \le j \le k$. Now, for arbitrary element $d_1 \in B_1$ the subuniverse $D = \overline{B}(d_1,x_1,x_2,a_4,\ldots,a_k)$ of $\mathcal{A}^2$ is of size m, as $pr_1 D = B_2$ and $pr_2 D = B_3$. Furthermore, $|D(x_1,a_3)| = 1$ and $D(x_1,b_3) = B_2$, so that D is reduced. This contradiction completes the proof of Claim 1.

For simplicity of notation we assume in the sequel that the projection $\overline{B}$ of B in Claim 1 is $\overline{B} = pr_{\underline{\underline{k}}} B$ $(2 \le k \le n)$. Property (γ) shows that there exists a function $g: B_2 \times \ldots \times B_k \to B_1$ such that $\overline{B} = g_{\square}$. Moreover, for the projection $B' = pr_{\underline{\underline{n}}-\underline{\underline{1}}} B$ of B we have

$$B = \{(g(x_2,\ldots,x_k),x_2,\ldots,x_n) \in A^n : (x_2,\ldots,x_n) \in B'\}. \tag{4.4}$$

The subuniverse B' of $\mathcal{A}^{n-1}$ is a direct product of directly indecomposable projections of B', say $B' \approx (pr_{I_1} B') \times \ldots \times (pr_{I_h} B')$ where $\{I_1,\ldots,I_h\}$ is a partition of $\underline{\underline{n}}-\underline{\underline{1}}$. Since B is directly indecomposable, (4.4) implies that

$$I_j \cap \underline{\underline{k}} \neq \emptyset \quad \text{for all} \quad 1 \le j \le h. \tag{4.5}$$

In particular, every indecomposable direct factor of B' is of size m. Hence each factor $pr_{I_j} B'$ of B' with $|I_j| = 1$ is one of the sets $B_2,\ldots,B_k$, and by induction on n we may suppose that for each factor $pr_{I_j} B'$ with $|I_j| \ge 2$ the conclusions (b_1)-(b_2) of the lemma hold.

This implies on the one hand that for every $1 \le j \le h$, the subalgebras $\mathcal{L}_i = (B_i;F)$ $(i \in I_j)$ of $\mathcal{A}$ are pairwise isomorphic. However, the bijections occurring in (γ) of Claim 1 are subuniverses of $\mathcal{A}^2$, hence they are isomorphisms between the corresponding subalgebras. Therefore $\mathcal{L}_1 \cong \ldots \cong \mathcal{L}_k$, which, together with (4.5), concludes the proof of (b_1).

On the other hand, it follows that for arbitrary isomorphisms $\pi_i: \mathscr{L}_i \to \mathscr{L}_1$ $(1 \le i \le n)$, the subuniverse $B'[\pi_2,\ldots,\pi_n]$ of $\mathcal{A}^{n-1}$ has the form (4.1) (with $n-1$ in place of n). In fact, we get this form for the indecomposable direct factors of B' first, and then observe that by adding fictitious variables to the functions occurring we can get a similar form for their direct product. Now, by (4.4), the first component of $B[\pi_1,\pi_2,\ldots,\pi_n]$ is a function of the first $k-1$ components of $B'[\pi_2,\ldots,\pi_n]$, whence it follows that (b_2) holds.

PROOF of Theorem 4.3. Let B be of size m, and assume (a) fails for $\mathcal{A}$. Then $n > 2$ and the conclusions of Lemma 4.4 hold for B. Therefore it remains to prove the claims for $\mathscr{L}_1$.

In what follows, all operations occurring are defined on B_1. Let G denote the set of operations commuting with the basic operations of $\mathscr{L}_1$ (and hence with every term operation of $\mathscr{L}_1$). Equivalently, a k-ary operation g belongs to G if and only if $g_\square$ is a subuniverse of $\mathscr{L}_1^{k+1}$. By Proposition 1.1 G is a clone on B_1. Since $\mathscr{L}_1$ is idempotent, G contains all the constants. Moreover, every operation g_j $(u \le j \le n)$ occurring in the representation (4.1) of $B[\pi_1,\ldots,\pi_n]$ belongs to G, as $(g_j)_\square$ is a projection of $B[\pi_1,\ldots,\pi_n]$. Since (a) fails and B is reduced, therefore each g_j $(u \le j \le n)$ depends on at least two variables. We show that every operation $g \in G$ depending on all of its variables has the CSP. If, say, g is k-ary, then $g_\square$ is a directly indecomposable subuniverse of $\mathcal{A}^{k+1}$ of size m. Furthermore, no proper projection of $g_\square$ can satisfy condition (γ) from Claim 1 in the proof of Lemma 4.4. Hence (γ) holds for $g_\square$, which means that g has the CSP.

Thus Proposition 3.4 applies for the algebra $(B_1;G)$ whose clone of polynomial operations is G. Thus there exists a vector space $\underset{K}{B_1} = (B_1;+,K)$ over some finite field K such that $G = P(\underset{K}{B_1})$. It is easy to see that the clone of the full idempotent reduct of the $(\mathrm{End}\ \underset{K}{B_1})$-module $(\mathrm{End}\ \underset{K}{B_1})\underset{K}{B_1}$ coincides with

the clone G^* of all operations commuting with each member of G (cf. Exercise 2.11). We have to prove that $T(\mathscr{L}_1) = G^*$. By the definition of G the inclusion $\subseteq$ is trivial.

Before verifying the reverse inclusion observe that the singletons are the only proper subuniverses of $\mathscr{L}_1$. Indeed, if $S \subset B_1$ $(S \neq \emptyset)$ is a proper subuniverse of $\mathscr{L}_1$, then $x_1 - x_2 \in G$ implies that

$$U = \{(x_1, x_2) \in B_1^2 : x_1 - x_2 \in S\}$$

is a subuniverse of $\mathscr{L}_1^2$. Since $\mathrm{pr}_1 U = \mathrm{pr}_2 U = B_1$, $U \neq B_1^2$, and by assumption U is not reduced, therefore it follows that U is a bijection. Hence $|S| = 1$.

Now let $f \in G^*$, and let C be an arbitrary directly indecomposable subuniverse of $\mathscr{L}_1^q$ for some $q \geq 1$. Since $\mathscr{L}_1$ has no nonsingleton proper subalgebras, we have either $C \leqslant B_1^q$, so that C is of size m or $|C| = q = 1$. If $q = 1$, then f obviously preserves C. Suppose $q \geq 2$. Lemma 4.4 implies then that C has the form

$$C \approx \{(y_1, \ldots, y_{v-1}, f_v(y_1, \ldots, y_{v-1}), \ldots, f_q(y_1, \ldots, y_{v-1})) : y_1, \ldots, y_{v-1} \in B_1\}$$

for some $2 \leq v \leq q$ and some operations $f_j \in O_{B_1}^{(v-1)}$ $(v \leq j \leq q)$. The sets $(f_j)^{\square}$ $(v \leq j \leq q)$ are projections of C, yielding that $f_v, \ldots, f_q \in G$. Thus f commutes with $f_v, \ldots, f_q$, implying that f preserves C as well. This means that f preserves every directly indecomposable subuniverse of each finite power of $\mathscr{L}_1$. Hence it preserves all subuniverses of finite powers of $\mathscr{L}_1$, that is, $f \in T(\mathscr{L}_1)$. Therefore $G^* = T(\mathscr{L}_1)$, which was to be proved.

For later use, let us state explicitly the following fact established during the proof of Theorem 4.3.

REMARK. If, under the assumptions of Theorem 4.3, condition (a) fails, then in (b) for arbitrary isomorphisms $\pi_i : \mathscr{L}_i \to \mathscr{L}_1$ $(1 \leq i \leq n)$ the subuniverse $B[\pi_1, \ldots, \pi_n]$ of $\mathscr{L}_1^n$ has the form (4.1) with $g_u, \ldots, g_n \in P(_{K}B_1)$.

Theorem 4.3 provides an easy test for the quasi-primality of idempotent algebras. For a set A, the subsets of A^2 of the form

$$(A_1 \times B_2) \cup (B_1 \times A_2) \quad \text{with} \quad \emptyset \neq B_i \subset A_i \quad (i = 1,2)$$

will be called *thick crosses*.

COROLLARY 4.5. *A finite idempotent algebra $\mathcal{A} = (A;F)$ is quasi-primal if and only if every subalgebra of $\mathcal{A}$ is simple, $\mathcal{A}$ has no nonsingleton affine subalgebras, and there are no thick crosses among the subuniverses of $\mathcal{A}^2$.*

PROOF. The necessity of the conditions is obvious. Conversely, suppose that $\mathcal{A}$ is not quasi-primal. Then by Theorem 4.3 either $\mathcal{A}^2$ has a reduced subuniverse or $\mathcal{A}$ has a nonsingleton affine subalgebra. In the latter case we are done. The former case can be settled by verifying the following claim.

EXERCISE 4.6. Let $\mathcal{A} = (A;F)$ be a finite idempotent algebra. If $D \prec D_1 \times D_2$ $(|D_1| \geq |D_2|)$ is a reduced subuniverse of $\mathcal{A}^2$ which is minimal with respect to inclusion, then either D is a thick cross, or $D \circ D^{\smile}$ is a nontrivial congruence of the subalgebra $(D_1;F)$ of $\mathcal{A}$.

Para-primal algebras

Para-primal algebras were introduced by D. M. Clark and P. H. Krauss [1976]. Their aim was to weaken condition (ii) in the characterization of quasi-primal algebras (Theorem 4.2) so as to include also groups of prime order.

DEFINITION. Let A be a finite set and $B \subseteq A^k$ $(k \geq 1)$. A nonvoid subset I of $\underline{k} = \{1,\ldots,k\}$ is said to be B-*minimal* iff it is minimal with respect to the property that the projection $B \to \mathrm{pr}_I B$ is one-to-one.

DEFINITION. An algebra $\mathcal{A} = (A;F)$ is called *para-primal* iff it is finite and for every natural number k, every subuniverse B of $\mathcal{A}^k$, and every

B-minimal set I, we have $\mathrm{pr}_I B = \prod_{i \in I} \mathrm{pr}_i B$.

The definition immediately yields two natural classes of examples.

EXAMPLES. 1. Every quasi-primal algebra is para-primal.

2. Groups of prime order are para-primal.

More generally, we will see that every finite Mal'tsev algebra in which all subalgebras are simple is para-primal. The most remarkable fact concerning para-primal algebras is that this quite easy sufficient condition is necessary, too. This yields a nice characterization for para-primal algebras, closely paralleling Theorem 4.2(iv) for quasi-primal algebras.

THEOREM 4.7. *For a finite algebra* $\mathcal{A} = (A;F)$ *the following conditions are equivalent:*

(i) $\mathcal{A}$ *is para-primal;*

(ii) $\mathcal{A}$ *is a Mal'tsev algebra and every subalgebra of* $\mathcal{A}$ *is simple.*

The difficulty in the proof is to show that every para-primal algebra has a Mal'tsev operation among its term operations. The original proof found by D. M. Clark and P. H. Krauss [1976] is rather complicated. A more elegant way is provided by a nice theorem of R. McKenzie [1982] (see also IV. §13 in [BS]). Here we use another approach which gives more insight into the clones of para-primal algebras. Our main tool is Theorem 4.3; however, to be able to apply it we need several lemmas on the full idempotent reduct of para-primal algebras.

LEMMA 4.8. *A finite algebra is para-primal if and only if its full idempotent reduct is para-primal.*

PROOF. It is clear from the definition that an algebra is para-primal whenever a reduct of it is para-primal. This implies the "if" part of the lemma. For the "only if" part we first prove

Claim 1. Let $\mathcal{A}$ be a para-primal algebra. For every integer $k \geq 2$ and for arbitrary subuniverse $B \prec B_1 \times \ldots \times B_k$ of $\mathcal{A}^k$ there exists a subset J of $\underline{\underline{k}}$ such that $|J| \geq 2$ and $J - \{i\}$ is $(\mathrm{pr}_J B)$-minimal for every $i \in J$.

As $B \neq B_1 \times \ldots \times B_k$, there exists a subset J of $\underline{\underline{k}}$ which is minimal with respect to the property $\mathrm{pr}_J B \neq \prod_{i \in J} B_i$. Clearly, $|J| \geq 2$. Let, say, $J = \underline{\underline{n}}$ $(n \leq k)$, and put $B' = \mathrm{pr}_{\underline{\underline{n}}} B$. Obviously, the set $\underline{\underline{n}}$ is not B'-minimal. On the other hand, by the choice of $J = \underline{\underline{n}}$ we have

$$\mathrm{pr}_{\underline{\underline{n}}-\{j\}} B' = \prod_{\substack{i=1 \\ i \neq j}}^{n} B_i \quad \text{for all } j \in \underline{\underline{n}}. \tag{4.6}$$

Thus $|B_1|, \ldots, |B_n| > 1$, and the B'-minimal sets have $n-1$ elements.

Assume that, contrary to our claim, not all $(n-1)$-element subsets of $\underline{\underline{n}}$ are B'-minimal. Suppose for instance that $\underline{\underline{n}} - \{n\}$ is B'-minimal, while $\underline{\underline{n}} - \{1\}$ is not. For every integer $m \geq 2$ let

$$C_m = \{(x_1, \ldots, x_m) \in B_1^m : \text{there exist } b_2 \in B_2, \ldots, b_n \in B_n \text{ such that } (x_i, b_2, \ldots, b_n) \in B' \text{ for all } 1 \leq i \leq m\}.$$

It is easy to check that C_m is a subuniverse of $\mathcal{A}^m$ for every $m \geq 2$. Clearly, $\Delta_{B_1} \subseteq C_2$. Moreover, since $\underline{\underline{n}} - \{1\}$ is not B'-minimal, therefore the projection $B' \to \mathrm{pr}_{\underline{\underline{n}}-\{1\}} B' = B_2 \times \ldots \times B_n$ is not one-to-one. Hence B' contains two n-tuples $(b_1, b_2, \ldots, b_n)$, $(b_1', b_2, \ldots, b_n)$ with $b_1 \neq b_1'$, implying that $(b_1, b_1') \in C_2$. Thus $\Delta_{B_1} \subset C_2$. We show that $C_{|B_1|} \neq B_1^{|B_1|}$. Otherwise there would exist $b_2 \in B_2, \ldots, b_n \in B_n$ such that $(x, b_2, \ldots, b_n) \in B'$ for all $x \in B_1$. Taking into account that $\underline{\underline{n}} - \{n\}$ is B'-minimal, we would get that $(b_2, \ldots, b_{n-1}, a) \notin \mathrm{pr}_{\underline{\underline{n}}-\{1\}} B'$ for all $a \in B_n - \{b_n\}$, which contradicts (4.6).

Let m (≥ 2) be the least natural number such that $C_m \neq B_1^m$. If $m = 2$, then by the foregoing remark $\Delta_{B_1} \subset C_2$. If $m > 2$, then $C_{m-1} = B_1^{m-1}$, so

that $C_m \prec B_1^m$ is totally reflexive (on B_1). Therefore, in either case, none of the projections $C_m \to B_1^{m-1}$ is one-to-one. Hence $\underline{\underline{m}}$ is C_m-minimal. This contradicts the para-primality of $\mathcal{A}$, concluding the proof of Claim 1.

Now let $\mathcal{A} = (A;F)$ be a para-primal algebra and $\mathcal{A}_o = (A;F_o)$ its full idempotent reduct. To show that $\mathcal{A}_o$ is para-primal, we apply Proposition 1.11. Clearly, we are done if we prove

Claim 2. Let $B \leqslant B_1 \times \ldots \times B_k$ be a subuniverse of $\mathcal{A}^k$ $(k \geq 1)$, $1 \leq n \leq \ell \leq k$, $a \in A^{k-\ell}$, and $C = \mathrm{pr}_{\underline{\underline{n}}} B(x_1,\ldots,x_\ell,a)$, $|C| > 1$. Every C-minimal set I $(\subseteq \underline{\underline{n}})$ is contained in a B-minimal set and $\mathrm{pr}_I C = \prod_{i\in I} B_i$.

We proceed by induction on k. The claim is trivial if $B = B_1 \times \ldots \times B_k$ (in particular, if $k = 1$). So assume that $B \prec B_1 \times \ldots \times B_k$, $k \geq 2$, and the claim is true for all subuniverses of $\mathcal{A}^{k-1}$. Choose a set J $(\subseteq \underline{\underline{k}})$ according to Claim 1. For every $i \in J$, the $(\mathrm{pr}_J B)$-minimality of the set $J - \{i\}$ ensures the existence of a function $g_i: \prod_{j\in J-\{i\}} B_j \to B_i$ such that $\mathrm{pr}_J B \approx (g_i)^{\square}$. This implies that if $i \in J \cap (\underline{\underline{\ell}}-\underline{\underline{n}})$, then for the subuniverse $\tilde{B} = \mathrm{pr}_{\underline{\underline{k}}-\{i\}} B$ of $\mathcal{A}^{k-1}$ we have

$$C = \mathrm{pr}_{\underline{\underline{n}}} \tilde{B}(x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_\ell,a).$$

Thus, by the induction hypothesis, I is contained in a $\tilde{B}$-minimal set and $\mathrm{pr}_I C = \prod_{j\in I} B_j$. Obviously, this $\tilde{B}$-minimal set is B-minimal as well. Similar argument applies also if $J \subseteq \underline{\underline{k}}-\underline{\underline{\ell}}$, $i \in J$. Finally, suppose that $J \cap (\underline{\underline{\ell}}-\underline{\underline{n}}) = \emptyset$, $J \cap \underline{\underline{n}} \neq \emptyset$. Then for every $i \in J \cap \underline{\underline{n}}$ we have

$$\mathrm{pr}_{J\cap\underline{\underline{n}}} C = \mathrm{pr}_{J\cap\underline{\underline{n}}} B(x_1,\ldots,x_\ell,a) \subseteq (f_i)^{\square}$$

for the function f_i arising from g_i by substituting the components a_j $(j \in J \cap (\underline{\underline{k}}-\underline{\underline{\ell}}))$ of a for the corresponding variables of g_i. Therefore $J \cap \underline{\underline{n}} \not\subseteq I$. Fixing an $i \in J \cap \underline{\underline{n}}$ with $i \notin I$ and putting $\tilde{C} = \mathrm{pr}_{\underline{\underline{n}}-\{i\}} C$ we get that I is $\tilde{C}$-minimal; furthermore, $|\tilde{C}| = |C| > 1$, and for $\tilde{B}$ as above we have

$$\tilde{C} = \mathrm{pr}_{\underline{n}-\{i\}}\, \tilde{B}(x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_\ell,a).$$

As $\mathrm{pr}_I\, C = \mathrm{pr}_I\, \tilde{C}$, the claim follows again from the induction hypothesis. This concludes the proof of Lemma 4.8.

Note the following important consequence of Claim 1 above, which will be used without further reference: For a para-primal algebra $\mathcal{A}$, $\mathcal{A}^2$ has no reduced subuniverses.

LEMMA 4.9. *Let $\mathcal{A} = (A;F)$ be an idempotent para-primal algebra, and let $\mathcal{L} = (C;F)$ be a nonsingleton affine subalgebra of $\mathcal{A}$. Then there exist a finite field K and a vector space ${}_K\underline{C} = (C;+,K)$ such that $\mathcal{L}$ is term equivalent to the full idempotent reduct of the $(\mathrm{End}\ {}_K\underline{C})$-module $(\mathrm{End}\ {}_K\underline{C})\underline{C}$ (that is, an operation on C is a term operation of $\mathcal{L}$ if and only if it commutes with every polynomial operation of ${}_K\underline{C}$).*

PROOF. By the para-primality, $\mathcal{A}^2$ has no reduced subuniverses. Since $(x-y+z)^{\square} \prec C^4$ is a reduced subuniverse of $\mathcal{A}^4$, the claim follows from Theorem 4.3.

Now we look at the relation between the affine subalgebras of a para-primal algebra and its full idempotent reduct.

LEMMA 4.10. *Let $\mathcal{A} = (A;F)$ be a para-primal algebra and $\mathcal{A}_o = (A;F_o)$ its full idempotent reduct. For a nonsingleton set $C \subseteq A$, $(C;F)$ is an affine subalgebra of $\mathcal{A}$ if and only if $(C;F_o)$ is an affine subalgebra of $\mathcal{A}_o$.*

PROOF. The necessity being obvious suppose $(C;F_o)$ is an affine subalgebra of $\mathcal{A}_o$, say $(C;F_o)$ is affine with respect to the Abelian group $\underline{C} = (C;+)$, and let $P = (x-y+z)^{\square}$. Since P is an irredundant subuniverse of $\mathcal{A}_o^4$, by Proposition 1.11 we have

$$P = \mathrm{pr}_{\underline{4}}\, B(x_1,\ldots,x_h,a_{h+1},\ldots,a_n)$$

for some $4 \leq h \leq n$ and some subuniverse $B \leqslant B_1 \times \ldots \times B_n$ of $\mathcal{A}^n$. However, B is a subuniverse of $\mathcal{A}_o^n$ as well. We may assume without loss of generality that B is reduced. Hence, by Theorem 4.3 and the remark following its proof, $(B_i;F_o)$ $(1 \leq i \leq n)$ are isomorphic affine subalgebras of $\mathcal{A}_o$ and for arbitrary isomorphisms $\pi_i: (B_i;F_o) \to (B_1;F_o)$ $(1 \leq i \leq n)$ the subuniverse $B[\pi_1,\ldots,\pi_n]$ has the form (4.1) with $g_u,\ldots,g_n \in P(_K\underline{B}_1)$ where $n \geq u \geq 2$ and $_K\underline{B}_1$ is the vector space corresponding to $(B_1;F_o)$ (see Lemma 4.9). Since B is reduced, $g_u,\ldots,g_n$ depend on at least two variables. It is easy to see that $B_1 = B_2 = B_3 = B_4 = C$. Furthermore, at least one of the projections $pr_{I_j} B$ $(u \leq j \leq n)$ of B with

$$pr_{I_j} B[\pi_1,\ldots,\pi_n] \approx (g_j)^{\square}$$

has the property that there exists an index $k \in I_j \cap \underline{4}$ such that the k-th component of B corresponds either to the values of g_j or to a nonfictitious variable of g_j. Hence, omitting the fictitious variables we get that for some subuniverses $C_1 = C, C_2,\ldots,C_m$ $(\in \{B_1,\ldots,B_n\})$ of $\mathcal{A}$ and for some (hence for all) internal isomorphisms $\sigma_i: C_i \to C$ $(1 \leq i \leq m)$ of $\mathcal{A}_o$, the vector space $_K\underline{C}$ $(= {}_K\underline{B}_1)$ has a polynomial operation $\sum_{i=1}^{m-1} r_i x_i + c$ $(m \geq 3,\ r_1,\ldots,r_{m-1} \in K - \{0\},\ c \in C)$ such that the set

$$((\sum_{i=1}^{m-1} r_i(y_i\sigma_i)+c)\sigma_m^{-1})^{\square} \leqslant C_1 \times \ldots \times C_m$$

is a subuniverse of $\mathcal{A}^m$. Up to the order of its components, the same subuniverse is

$$((r_2^{-1}(y_m\sigma_m) - \sum_{\substack{i=1 \\ i\neq 2}}^{m-1} r_2^{-1}r_i(y_i\sigma_i) - r_2^{-1}c)\sigma_2^{-1})^{\square} \leqslant C_m \times C_1 \times C_3 \times \ldots \times C_{m-1} \times C_2.$$

Consider the function $g: C \times C \times C_2 \to C_2$ defined by

$$g(y_1,y_1',y_2) = (r_2^{-1}r_1(y_1\sigma_1) - r_2^{-1}r_1(y_1'\sigma_1) + (y_2\sigma_2))\sigma_2^{-1}$$

$$= (r_2^{-1}(\sum_{i=1}^{m-1} r_i(y_i\sigma_i)+c) - r_2^{-1}r_1(y_1'\sigma_1) - \sum_{i=3}^{m-1} r_2^{-1}r_i(y_i\sigma_i) - r_2^{-1}c)\sigma_2^{-1}$$

(the fictitious variables $y_3,\ldots,y_{m-1}$ are omitted). Since it arises from the previous ones by superposition, therefore the set $g^{\square} \preccurlyeq C \times C \times C_2 \times C_2$ is a subuniverse of $\mathcal{A}^4$ as well. Repeating this construction once more, we get that

$$((-(z\sigma_1) + (z'\sigma_1) + (z''\sigma_1))\sigma_1^{-1})^{\square} \preccurlyeq C^4$$

is also a subuniverse of $\mathcal{A}^4$. As $\sigma_1\colon C = C_1 \to C$ can be chosen to be the identity, it follows that P is a subuniverse of $\mathcal{A}^4$, that is the subalgebra $(C;F)$ of $\mathcal{A}$ is affine.

We now derive from Theorem 4.3 a nice description for the term operations of idempotent para-primal algebras.

THEOREM 4.11. *Let $\mathcal{A} = (A;F)$ be an idempotent para-primal algebra, and let $\mathcal{A}_i = (A_i;F)$ $(1 \le i \le k)$ be the nonsingleton affine subalgebras of $\mathcal{A}$, say $\mathcal{A}_i$ is affine with respect to $\underline{A}_i = (A_i;+_i)$. Then an operation on A is a term operation of $\mathcal{A}$ if and only if it preserves*

(a) *all internal isomorphisms of $\mathcal{A}$, and*

(b) *the subuniverse $P_i = (x -_i y +_i z)^{\square}$ of $\mathcal{A}_i^4$ for all $1 \le i \le k$.*

PROOF. Let ${}_{K_i}\underline{A}_i = (A_i;+_i,K_i)$ be the vector space corresponding to $\mathcal{A}_i$ $(1 \le i \le k)$ (see Lemma 4.9). For an operation $f \in O_A^{(n)}$ $(n \ge 1)$ to be a term operation of $\mathcal{A}$ the preservation of the subuniverses (a)-(b) is clearly necessary. Conversely, assume now that f preserves all subuniverses (a)-(b). Then f preserves all subuniverses of $\mathcal{A}$ as well, in particular, f is idempotent. We show that for each $1 \le i \le k$ the restriction $f|_{A_i}$ of f commutes with all polynomial operations of ${}_{K_i}\underline{A}_i$. Indeed, $f|_{A_i}$ commutes with the constants as it is idempotent. It commutes with $x -_i y +_i z$, since f preserves P_i.

Furthermore, $f|_{A_i}$ commutes with each unary operation cx ($c \in K_i$, $c \neq 0$) of $_{K_i}\underline{A_i}$, because the mapping $A_i \to A_i$, $x \mapsto cx$ is an internal isomorphism of $\mathcal{A}$. Thus $f|_{A_i}$ commutes with each member of a generating set of the clone $P(_{K_i}\underline{A_i})$, implying that it commutes with every operation in $P(_{K_i}\underline{A_i})$.

Let $B \leq B_1 \times \ldots \times B_n$ be a reduced subuniverse of $\mathcal{A}^n$ ($n \geq 1$). We claim that f preserves B. This is trivial for $n = 1$. If $n \geq 2$, then by Theorem 4.3 and by the remark after its proof, the subalgebras $\mathcal{L}_j = (B_j;F)$ ($1 \leq j \leq n$) of $\mathcal{A}$ are affine and pairwise isomorphic, moreover, for arbitrary isomorphisms $\pi_j: \mathcal{L}_j \to \mathcal{L}_1$ ($1 \leq j \leq n$) the subuniverse $B[\pi_1,\ldots,\pi_n]$ of $\mathcal{A}^n$ has the form (4.1) with $g_u,\ldots,g_n$ polynomial operations of the vector space corresponding to $\mathcal{L}_1$. Since $f|_{B_1}$ commutes with $g_u,\ldots,g_n$, therefore f preserves $B[\pi_1,\ldots,\pi_n]$, and hence B, too. Thus f preserves all reduced subuniverses of finite powers of $\mathcal{A}$. As it preserves the internal isomorphisms of $\mathcal{A}$ as well, it follows that f preserves all subuniverses of finite powers of $\mathcal{A}$. Hence f is a term operation of $\mathcal{A}$.

COROLLARY 4.12. *A para-primal algebra is quasi-primal if and only if it has no nonsingleton affine subalgebras.*

PROOF. Let $\mathcal{A} = (A;F)$ be a para-primal algebra. If it has a subalgebra $\mathcal{L} = (B;F)$ ($|B| > 1$) which is affine with respect to $\underline{B} = (B;+)$, then $(x-y+z)^{\square}$ is a subuniverse of $\mathcal{A}^4$, whence by Theorem 4.2 $\mathcal{A}$ is not quasi-primal. Conversely, if $\mathcal{A}$ has no nonsingleton affine subalgebra, then by Lemma 4.10 its full idempotent reduct $\mathcal{A}_o$ has none, either. However, by Lemma 4.8 $\mathcal{A}_o$ is para-primal, therefore Theorem 4.11 implies that $\mathcal{A}_o$ is quasi-primal. Consequently, $\mathcal{A}$ is also quasi-primal.

Applying Theorem 4.3 we can get a characterization for idempotent para-primal algebras, similar to Corollary 4.5.

COROLLARY 4.13. *A finite idempotent algebra* $\mathcal{A} = (A;F)$ *is para-primal if and only if every subalgebra of* $\mathcal{A}$ *is simple and there are no thick crosses among the subuniverses of* $\mathcal{A}^2$.

PROOF. The necessity is obvious. Conversely, if $\mathcal{A}$ satisfies the conditions, then by Exercise 4.6 $\mathcal{A}^2$ has no reduced subuniverses. Hence the description of the reduced subuniverses of finite powers of $\mathcal{A}$ in the remark following the proof of Theorem 4.3 yields that $\mathcal{A}$ is para-primal.

Using Lemma 4.8 and Theorem 4.11 from these preparations we can prove Theorem 4.7.

PROOF of Theorem 4.7. In view of Lemma 4.8, in proving (i) $\Rightarrow$ (ii) we may confine ourselves to idempotent algebras. So let $\mathcal{A}$ be an idempotent para-primal algebra. Since $\mathcal{A}^2$ has no reduced subuniverses, it follows that the subalgebras of $\mathcal{A}$ are simple. With the notations of Theorem 4.11 define a Mal'tsev operation p on A as follows:

$$(4.7)\quad p(a,b,c) = \begin{cases} a -_i b +_i c & \text{if } a,b,c \in A_i \text{ for some } 1 \le i \le k \\ t(a,b,c) & \text{otherwise} \end{cases} \qquad (a,b,c \in A).$$

We have $|A_i \cap A_j| \le 1$ for $1 \le i < j \le k$, since $\mathcal{A}_1, \ldots, \mathcal{A}_k$ have no proper nonsingleton subalgebras. Thus p is well defined. Making use of the fact that for $1 \le i \le k$, $x -_i y +_i z$ is the unique Mal'tsev operation among the term operations of $\mathcal{A}_i$, one can easily see that p preserves the internal isomorphisms of $\mathcal{A}$ as well as the subuniverse P_i of $\mathcal{A}_i^4$ for every $1 \le i \le k$. Hence by Theorem 4.11, p is a term operation of $\mathcal{A}$.

To verify the easy direction (ii) $\Rightarrow$ (i) of Theorem 4.7, consider an algebra $\mathcal{A} = (A;F)$ satisfying (ii) and a subuniverse $B \leqslant B_1 \times \ldots \times B_h$ of $\mathcal{A}^h$ $(h \ge 1)$. Denote by Θ_i the kernel of the projection $B \to B_i$ $(1 \le i \le h)$. Clearly, $\mathcal{L} = (B;F)$ is a Mal'tsev algebra, hence it has permutable congruences.

Furthermore, since the algebras $\mathscr{A}_i = (B_i;F)$ are simple, Θ_i $(1 \le i \le h)$ are maximal congruences of $\mathscr{A}$. It is well known (see, e.g. [BS]) that, under these conditions, for arbitrary subset I of $\underline{h}$ which is minimal with respect to the property $\bigcap_{i\in I} \Theta_i = \Delta_B$, the natural mapping $B \to \prod_{i\in I} B/\Theta_i \cong \prod_{i\in I} B_i$, $(b_1,\dots,b_h) \mapsto (b_i)_{i\in I}$ is an isomorphism $\mathscr{A} \to \prod_{i\in I} \mathscr{A}_i$. Observing now that the kernel of the projection $B \to \mathrm{pr}_I B$ $(I \subseteq \underline{h})$ is $\bigcap_{i\in I} \Theta_i$, we get that I is B-minimal if and only if I is minimal with respect to the property $\bigcap_{i\in I} \Theta_i = \Delta_B$. Hence, if I is B-minimal, then the projections $B \to \mathrm{pr}_I B$ and $B \to \prod_{i\in I} B_i$ are both bijective, implying that $\mathrm{pr}_I B = \prod_{i\in I} B_i$. Thus $\mathcal{A}$ is para-primal, as claimed.

The question naturally arises whether there exists a characterization of para-primal algebras in terms of "preservation properties of term operations", analogous to the property defining quasi-primal algebras, which can be restated as follows: For a finite set A, let S denote the family of bijections between the subsets of A; an algebra $\mathcal{A} = (A;F)$ is quasi-primal if and only if

(*) the term operations of $\mathcal{A}$ are exactly the operations on A preserving those subuniverses of finite powers of $\mathcal{A}$ which belong to S.

Theorem 4.11 describes the term operations of idempotent para-primal algebras via preservation properties, however, these properties *do not characterize* idempotent para-primal algebras, because a finite idempotent algebra whose term operations are defined by such preservation properties is not necessarily para-primal. In fact, as was noticed by E. W. Kiss [1984], if A is a finite set with $|A| \ge 3$, then there exists no family S of subsets of finite powers of A such that an algebra $\mathcal{A} = (A;F)$ is para-primal if and only if (*) holds. Otherwise it would follow that the intersection of clones of para-primal algebras on A is the clone of a para-primal algebra, however, the reader can easily prove

EXERCISE 4.14. For any group $(A;+)$ of odd prime order, the intersection of the clones of $(A;t)$ and $(A;x-y+z)$ is the clone of projections.

This shows also that, unlike with quasi-primal algebras, there is no least para-primal algebra, up to term equivalence, on a finite set A, unless $|A| \leq 2$. However, clearly, the clones of para-primal algebras on A form an order filter in the clone lattice. We now derive the result of R. W. Quackenbush [1983] showing that on every finite set A, up to term equivalence, there are only finitely many minimal para-primal algebras, and that every para-primal algebra has a minimal para-primal reduct.

Let A be a finite set, and $A_1,\ldots,A_k$ a family of subsets of A with $|A_i \cap A_j| \leq 1$ for all $1 \leq i < j \leq k$ and $|A_i| = q_i$, a prime power, for all $1 \leq i \leq k$. Let us fix a generating element c_i of the multiplicative group of each finite field $GF(q_i)$ so that $c_i = c_j$ whenever $q_i = q_j$ $(1 \leq i,j \leq k)$. Consider a vector space $GF(q_i)^{\underline{A_i}} = (A_i;+_i,-_i,GF(q_i))$ for every $1 \leq i \leq k$, and define a ternary operation p on A by (4.7), and a binary operation g on A by

$$(4.8)\quad g(a,b) = \begin{cases} c_i a +_i (1-c_i)b & \text{if } a,b \in A_i \text{ for some } 1 \leq i \leq k \\ a & \text{otherwise} \end{cases} \qquad (a,b \in A).$$

Note that g is well defined. Making use of Theorem 4.11 we show that the algebras $(A;p,g)$ are exactly the minimal para-primal algebras with nonsingleton affine subuniverses $A_1,\ldots,A_k$.

THEOREM 4.15. *The algebra $(A;p,g)$ constructed above is para-primal, and has no proper para-primal reduct in which the nonsingleton affine subuniverses are exactly $A_1,\ldots,A_k$. Moreover, every para-primal algebra $(A;F)$ with nonsingleton affine subuniverses $A_1,\ldots,A_k$ has a reduct of the form $(A;p,g)$.*

PROOF. The operation g ensures that the subalgebras $(A_i;p,g)$ $(1 \leq i \leq k)$ of $(A;p,g)$ are simple. Since elsewhere p behaves like the discriminator, it is easy to see that the other subalgebras are also simple. Thus, by Theorem 4.7,

$(A;p,g)$ is para-primal. Let $\mathcal{A} = (A;F)$ be a para-primal reduct of $(A;p,g)$ such that the nonsingleton affine subalgebras of $\mathcal{A}$ are exactly the algebras $\mathcal{A}_i = (A_i;F)$ $(1 \le i \le k)$. Clearly, $\mathcal{A}$ is idempotent and for every $1 \le i \le k$, $\mathcal{A}_i$ is a reduct of $(A_i;p,g)$. Since $(A_i;p,g)$ is term equivalent to the full idempotent reduct of $_{GF(q_i)}\underline{A_i}$, which has no proper para-primal reduct, therefore $\mathcal{A}_i$ is term equivalent to $(A_i;p,g)$.

In view of Theorem 4.11 the first claim will follow if we show that every internal isomorphism of $\mathcal{A}$ is an internal isomorphism of $(A;p,g)$ as well. Let $\varphi: B \to C$ be an internal isomorphism of $\mathcal{A}$. Then B and C are subuniverses of $\mathcal{A}$, hence for each $1 \le i \le k$ we have $A_i \subseteq B$ or $|A_i \cap B| \le 1$, and similarly for C. Thus B and C are subuniverses of $(A;p,g)$. Since φ carries affine subuniverses into affine subuniverses, the restriction of φ to each $A_i \subseteq B$ $(1 \le i \le k)$ is an isomorphism $\mathcal{A}_i \to \mathcal{A}_{i\varphi}$, and hence also an isomorphism $(A_i;p,g) \to (A_i\varphi;p,g)$. Now it follows easily that φ is an isomorphism $(B;p,g) \to (C;p,g)$.

In view of Lemmas 4.8 and 4.10, it suffices to prove the second statement for idempotent para-primal algebras $\mathcal{A} = (A;F)$. Let $\mathcal{A}_i = (A_i;F)$ $(1 \le i \le k)$ be the nonsingleton affine subalgebras of $\mathcal{A}$, and $_{K_i}\underline{A_i} = (A_i;+_i,K_i)$ $(1 \le i \le k)$ the corresponding vector spaces (see Lemma 4.9). Since $\mathcal{A}_1,\dots,\mathcal{A}_k$ have no nonsingleton proper subalgebras, we have $|A_i \cap A_j| \le 1$ for all $1 \le i < j \le k$. Moreover, clearly, $q_i = |A_i|$ is a prime power for every $1 \le i \le k$. Now we construct the vector spaces $_{GF(q_i)}\underline{A_i}$. Let $\sim$ denote the equivalence on $\underline{k}$ such that $i \sim j$ $(i,j \in \underline{k})$ if and only if $\mathcal{A}_i \cong \mathcal{A}_j$. Pick an element i from each $\sim$-block, and fix an isomorphism $\chi_j: \mathcal{A}_i \to \mathcal{A}_j$ for every $j \sim i$ so that $\chi_i = \mathrm{id}$. We define $_{GF(q_i)}\underline{A_i}$ so that $_{K_i}\underline{A_i}$ be a reduct of it, otherwise arbitrarily (this is possible, since $q_i = |A_i|$ is a power of $|K_i|$), and let $\mathcal{A}_i'$ denote the full

idempotent reduct of $GF(q_i)^{\underline{A}_i}$. An easy application of Lemma 4.9 shows that $\mathcal{A}_i'$ is a reduct of $\mathcal{A}_i$. For $j \sim i$, $j \neq i$, let $\mathcal{A}_j'$ denote the isomorphic copy of $\mathcal{A}_i'$ under χ_j. Clearly, $\mathcal{A}_j'$ is a reduct of $\mathcal{A}_j$. Furthermore, Lemma 4.9 yields that $\mathcal{A}_j'$ is the full idempotent reduct of an appropriately defined vector space $GF(q_j)^{\underline{A}_j}$ such that $K_j^{\underline{A}_j}$ is a reduct of $GF(q_j)^{\underline{A}_j}$.

Observe that every isomorphism $\varphi: \mathcal{A}_\ell \to \mathcal{A}_m$ $(\ell, m \in \underline{k})$ is an isomorphism $\mathcal{A}_\ell' \to \mathcal{A}_m'$ as well. Indeed, if $\varphi: \mathcal{A}_\ell \to \mathcal{A}_m$ is an isomorphism, then $\ell \sim m$, hence $\varphi = \pi\chi_\ell^{-1}\chi_m$ for some automorphism π of $\mathcal{A}_\ell$. Since π, χ_ℓ, χ_m are isomorphisms between the corresponding algebras $\mathcal{A}_\ell'$, $\mathcal{A}_m'$, $\mathcal{A}_i'$ (i is the fixed element of the $\sim$-block of ℓ, m) as well, the claim follows. Now it can be verified without difficulty that the operations p and g defined by (4.7) and (4.8), respectively, preserve the subuniverses (a) and (b) in Theorem 4.11. Hence p and g are term operations of $\mathcal{A}$, that is, $(A;p,g)$ is a reduct of $\mathcal{A}$.

It is clear from Theorem 4.7 that finite simple modules and, more generally, finite simple affine algebras are para-primal.

EXERCISE 4.16. Derive Proposition 2.10 as well as Jacobson's Density Theorem (see N. Jacobson [1956]) for finite simple modules directly from the theory of para-primal algebras.

Chapter 5

HOMOGENEOUS ALGEBRAS

The least quasi-primal algebra $(A;t)$ where t is the discriminator on A is as "symmetric" as an algebra can be in the sense that every permutation of A is an automorphism of $(A;t)$.

DEFINITION. An algebra $\mathcal{A} = (A;F)$ is called *homogeneous* iff every permutation of A is an automorphism of $\mathcal{A}$. An operation f on A is said to be homogeneous iff the algebra $(A;f)$ is homogeneous.

Homogeneous algebras were first investigated by E. Marczewski [1964]. Here we study the clones of homogeneous algebras. They will turn out to be easy to handle because homogeneous algebras have a lot of internal isomorphisms.

PROPOSITION 5.1. *For a finite homogeneous algebra* $\mathcal{A} = (A;F)$, *every bijection* $B \to C$ *with* $\emptyset \neq B, C \subseteq A$, $|B| = |C| \neq |A| - 1$ *is an internal isomorphism of* $\mathcal{A}$. *Moreover, if* $\mathcal{A}$ *has an* $(|A|-1)$*-element subuniverse, then every bijection* $B \to C$ *with* $\emptyset \neq B, C \subseteq A$ *is an internal isomorphism of* $\mathcal{A}$.

PROOF. Since the set of fixed points of any automorphism of $\mathcal{A}$ is a subuniverse of $\mathcal{A}$, we get that every subset B of A with $|B| \neq |A| - 1$ is a subuniverse of $\mathcal{A}$. Furthermore, if $\mathcal{A}$ has an $(|A|-1)$-element subuniverse, then by the homogenity every subset B of A with $|B| = |A| - 1$ is also a subuniverse of

$\mathcal{A}$. Finally, for arbitrary subuniverses B, C of $\mathcal{A}$ and for every bijection $\pi: B \to C$, we have $\pi^{\square} = \varphi^{\square} \cap (B \times C)$ for some automorphism φ of $\mathcal{A}$, hence π is an internal isomorphism.

In particular, it follows that every finite homogeneous algebra $\mathcal{A} = (A;F)$ is idempotent, unless $|A| = 2$.

DEFINITION. A homogeneous operation f on a set A is called a *pattern operation* iff every subset of A is a subuniverse of $(A;f)$.

By the preceding proposition, if A is finite, then a homogeneous operation f on A is a pattern operation if and only if $(A;f)$ has $(|A|-1)$-element subuniverses. A similar argument shows that if A is infinite, then every homogeneous operation is a pattern operation. Homogeneous operations can be described as follows (E. Marczewski [1964]).

EXERCISE 5.2. Let f be a k-ary operation on a set A. For arbitrary k-tuples $(a_1,\ldots,a_k)$, $(b_1,\ldots,b_k) \in A^k$ we write $(a_1,\ldots,a_k) \sim (b_1,\ldots,b_k)$ to denote that for all $1 \le i,j \le k$ we have $a_i = a_j$ if and only if $b_i = b_j$ (that is, the two k-tuples have the same "pattern" of equalities among their components). The operation f is homogeneous if and only if it satisfies the following conditions:

(A) if $|A - \{a_1,\ldots,a_k\}| \neq 1$, then $f(a_1,\ldots,a_k) \in \{a_1,\ldots,a_k\}$;

(B) if $f(a_1,\ldots,a_k) = a_i$ $(1 \le i \le k)$ and $(b_1,\ldots,b_k) \sim (a_1,\ldots,a_k)$, then $f(b_1,\ldots,b_k) = b_i$;

(C) if $A - \{a_1,\ldots,a_k\} = \{f(a_1,\ldots,a_k)\}$ and $(b_1,\ldots,b_k) \sim (a_1,\ldots,a_k)$, then $A - \{b_1,\ldots,b_k\} = \{f(b_1,\ldots,b_k)\}$.

Clearly, f is a pattern operation if and only if case (C) does not occur, that is, for every $a_1,\ldots,a_k \in A$ there is an index $1 \le i \le k$ such that $f(a_1,\ldots,a_k) = a_i$, and i depends only on the "pattern" of the k-tuple $(a_1,\ldots,a_k)$.

We list a few homogeneous operations which will play an important role in the sequel.

EXAMPLES. Let A be a finite set, $|A| = n$. The following operations on A are homogeneous:

1. the discriminator t (see Chapter 4);

2. the dual discriminator d (see Chapter 1);

3. the so-called *switching operation* s defined by

$$s(a,b,c) = \begin{cases} c & \text{if } a = b \\ b & \text{if } a = c \\ a & \text{otherwise} \end{cases} \qquad (a,b,c \in A);$$

in particular, on a 2-element set A, $s(x,y,z) = x + y + z$ for any group $(A;+)$;

4. the k-ary *near-projection* ℓ_k $(3 \le k \le n)$ defined by

$$\ell_k(a_1,\ldots,a_k) = \begin{cases} a_1 & \text{if } |\{a_1,\ldots,a_k\}| < k \\ a_k & \text{otherwise} \end{cases} \qquad (a_1,\ldots,a_k \in A);$$

5. the $(n-1)$-ary operation r_n defined by

$$r_n(a_1,\ldots,a_{n-1}) = \begin{cases} a_1 & \text{if } |\{a_1,\ldots,a_{n-1}\}| < n-1 \\ a_n \text{ with } \{a_n\} = A-\{a_1,\ldots,a_{n-1}\} & \text{otherwise} \end{cases} \qquad (a_1,\ldots,a_{n-1} \in A);$$

for $n = 2$, r_2 is the unique nonidentity permutation on A, while for $n = 3$, $r_3(x,y) = 2x + 2y$ for arbitrary group $(A;+)$;

6. the $(n-1)$-ary operation d_n defined by

$$d_n(a_1,\ldots,a_{n-1}) = \begin{cases} d(a_1,a_2,a_3) & \text{if } |\{a_1,\ldots,a_{n-1}\}| < n-1 \\ a_n \text{ with } \{a_n\} = A-\{a_1,\ldots,a_{n-1}\} & \text{otherwise} \end{cases} \qquad (a_1,\ldots,a_{n-1} \in A)$$

provided $n \ge 4$;

7. the operation $x + y + z$ if $(A;+)$ is a 4-element group of exponent 2.

In this chapter we determine, up to term equivalence, all finite homogeneous algebras $\mathcal{A} = (A;F)$ with $|A| \geq 5$. Two types will be distinguished. First we consider the *dual discriminator algebras*, that is, those algebras in which d is a term operation, and then the remaining ones.

Homogeneous dual discriminator algebras

The homogeneous dual discriminator algebras were described by B. Csákány and T. Gavalcová [1980] (although one algebra is missing by mistake). The presentation here closely follows their ideas.

Let A be a set and $k,\ell \geq 2$ arbitrary integers. A $k \times \ell$ *cross* on A is a subset of A^2 of the form

$$(B \times \{c\}) \cup (\{b\} \times C) \quad \text{with} \quad B,C \subseteq A, \quad b \in B, \quad c \in C$$

such that $|B| = k$, $|C| = \ell$. Clearly, the size of a $k \times \ell$ cross is $\max\{k,\ell\}$. Crosses are significant in the study of discriminator algebras for the following reason.

PROPOSITION 5.3. *For a finite set* A, *the reduced subuniverses of* $(A;d)^2$ *are exactly the crosses.*

PROOF. It is easy to check that every cross on A is indeed a subuniverse of $(A;d)^2$. Conversely, let $B \leq B_1 \times B_2$ be a subuniverse of $(A;d)^2$. Then B has the following properties:

if $(a,b),(a',b),(a'',c) \in B$ with $a \neq a'$, then $(a'',b) \in B$,

as $(a'',b) = d((a,b),(a',b),(a'',c))$; similarly,

if $(b,a),(b,a'),(c,a'') \in B$ with $a \neq a'$, then $(b,a'') \in B$.

Now it can be verified without difficulty that either $B = \pi^{\square}$ for a bijection $\pi: B_1 \to B_2$, or B is a cross, or $B = B_1 \times B_2$.

PROPOSITION 5.4. *Let* $\mathcal{A} = (A;F)$ *be a finite homogeneous algebra such that there is a cross of size* m $(2 \le m \le |A|)$ *among the subuniverses of* $\mathcal{A}^2$.

(a) *If* $m < |A|$, *or* $m = |A|$ *and* $\mathcal{A}$ *has* $(|A|-1)$*-element subuniverses, then every cross of size at most* m *is a subuniverse of* $\mathcal{A}^2$.

(b) *If* $m = |A|$ *and* $\mathcal{A}$ *has no* $(|A|-1)$*-element subuniverses, then every* $k \times \ell$ *cross with* $k,\ell \neq |A| - 1$ *is a subuniverse of* $\mathcal{A}^2$.

PROOF. Assume first $|A| \neq 3$. Let $B = (B_1 \times \{u_2\}) \cup (\{u_1\} \times B_2)$ $(u_1 \in B_1, u_2 \in B_2)$ be an $m \times n$ cross $(m \ge n)$ among the subuniverses of $\mathcal{A}^2$. What we have to show is that every $k \times \ell$ cross with $k,\ell \le m$ such that $\mathcal{A}$ has both k-element and ℓ-element subuniverses is a subuniverse of $\mathcal{A}^2$. A $k \times 2$ cross C can be constructed from B as follows: $C = B \cap (C_1 \times C_2)$ where C_1 is a k-element subset of B_1 with $u_1 \in C_1$ while C_2 is a 2-element subset of B_2 with $u_2 \in C_2$. Furthermore, every $k \times 2$ cross is of the form $C[\pi_1,\pi_2]$ for appropriate bijections π_1, π_2 between k-element, resp. 2-element subsets of A. Hence, by Proposition 5.1, we get that every $k \times 2$ cross is a subuniverse of $\mathcal{A}^2$. The same holds for $\ell \times 2$ crosses, too. Finally, for arbitrary $k \times \ell$ cross

$$D = \{(a_k,b_1),\ldots,(a_2,b_1),(a_1,b_1),(a_1,b_2),\ldots,(a_1,b_\ell)\}$$

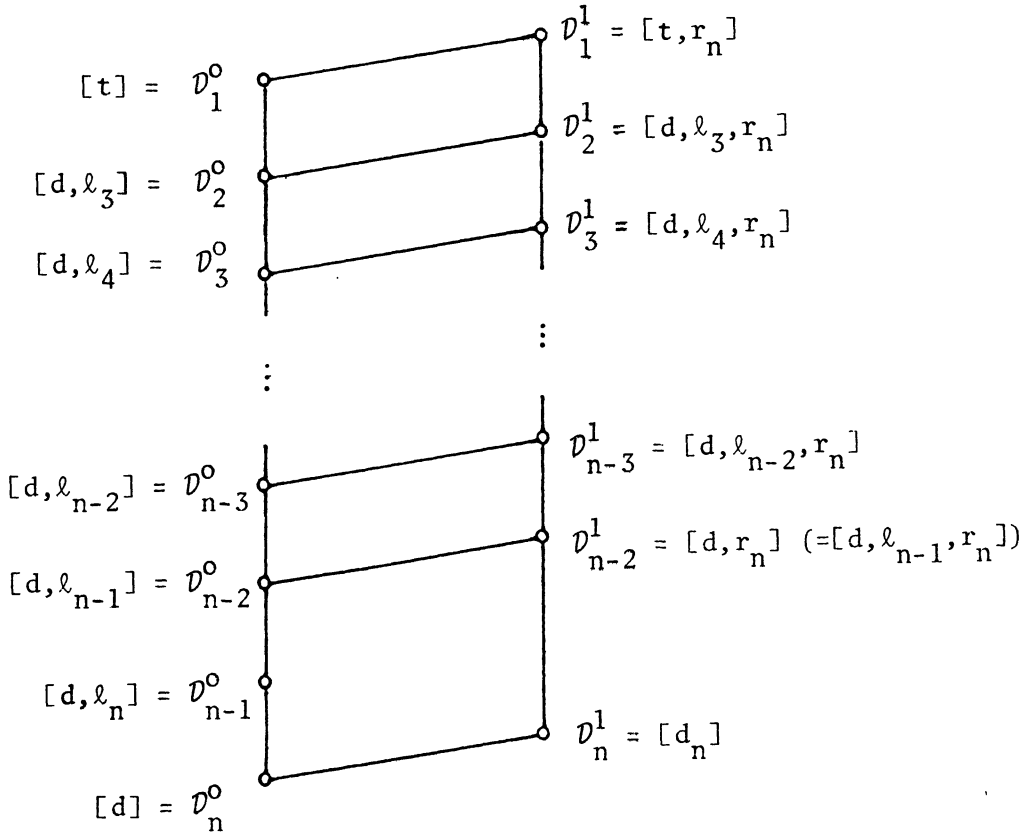
we have $D = \tilde{D} \circ \tilde{\tilde{D}}^{\smile}$, where $\tilde{D} = \{(a_k,c),\ldots,(a_2,c),(a_1,c),(a_1,c')\}$ is a $k \times 2$ cross and $\tilde{\tilde{D}} = \{(b_\ell,c'),\ldots,(b_2,c'),(b_1,c'),(b_1,c)\}$ is an $\ell \times 2$ cross (c, c' are arbitrary distinct elements of A). Hence D is a subuniverse of $\mathcal{A}^2$ as well.

Now let $|A| = 3$. If B is a 3×3 cross, then every 3×3 cross is of the form $B[\pi_1,\pi_2]$ for some permutations π_1, π_2 of A. If in turn, B is a 3×2 or 2×2 cross, then $\mathcal{A}$ has 2-element subuniverses, and the same argument applies as in the preceding paragraph.

REMARK. It is easy to see that for a 3-element homogeneous algebra $\mathcal{A} = (A;F)$ the existence of a 3×3 cross among the subuniverses of $\mathcal{A}^2$ implies that $\mathcal{A}$ has 2-element subuniverses.

We can now describe the homogeneous dual discriminator algebras. Let $\mathcal{D}_i^0$ [resp. $\mathcal{D}_i^1$] denote the clone of all pattern [resp. homogeneous] operations on A which preserve all crosses of size i $(1 \leq i \leq |A|)$.

THEOREM 5.5. *Every finite homogeneous dual discriminator algebra* $\mathcal{A} = (A;F)$ *with* $|A| \geq 4$ *is term equivalent to one of the algebras* $(A;\mathcal{D}_i^j)$ *with* $j \in \{0,1\}$, $1 \leq i \leq |A|$ *and* $(i,j) \neq (|A|-1,1)$. *These clones* $\mathcal{D}_i^j$ *are pairwise distinct. The lattice they form, together with a generating set of each clone is shown in Figure 2.*



$(n = |A| \geq 4)$

Figure 2

PROOF. Let $\mathcal{A} = (A;F)$ be a finite homogeneous algebra, $n = |A| \geq 4$, and let $C = T(\mathcal{A})$, $d \in C$. Since d is a majority operation, Corollary 1.25 shows that C is determined by the subuniverses of $\mathcal{A}^2$. Hence Proposition 5.3 implies that C consists exactly of those operations which preserve the internal isomorphisms of $\mathcal{A}$ and the crosses among the subuniverses of $\mathcal{A}^2$. Taking into account Propositions 5.1 and 5.4 we get that if i denotes the maximum of the sizes of crosses among the subuniverses of $\mathcal{A}^2$, then $C = \mathcal{D}_i^j$ with $j = 0$ or 1 according to whether $\mathcal{A}$ has $(n-1)$-element subuniverses or not. Obviously, $i \neq n-1$ if $j = 1$.

Clearly, t, d, ℓ_k $(3 \leq k \leq n)$ are pattern operations, while r_n and d_n are not. Furthermore, it is easy to see that d_n preserves the $n \times n$ crosses, r_n preserves the $(n-2) \times (n-2)$ crosses, and ℓ_k $(3 \leq k \leq n)$ preserves the $(k-1) \times (k-1)$ crosses, but does not preserve the crosses of size k. Therefore for each pair $(i,j) \in \underline{n} \times \{0,1\}$, $(i,j) \neq (n-1,1)$, the set claimed to be a generating set of $\mathcal{D}_i^j$ is contained in $\mathcal{D}_k^\ell$ $((k,\ell) \in \underline{n} \times \{0,1\}$, $(k,\ell) \neq (n-1,1))$ if and only if $k \leq i$ and $\ell \geq j$. This shows that the clones $\mathcal{D}_i^j$ are pairwise distinct, and the sets indicated are indeed generating sets.

The remaining homogeneous algebras

The description of finite homogeneous algebras was completed by S. S. Marchenkov [1982a]. The proof presented here is different from his; it makes use of Theorem 4.3, and is similar in spirit to the above discussion of homogeneous dual discriminator algebras, in spite of the essential difference that Corollary 1.25 cannot be applied.

First we give a necessary and sufficient condition for a homogeneous algebra not to be a dual discriminator algebra.

LEMMA 5.6. *For a finite homogeneous algebra* $\mathcal{A} = (A;F)$ *with* $|A| \geq 5$, *the following conditions are equivalent:*

(i) d *is not a term operation of* $\mathcal{A}$;

(ii) *for arbitrary distinct elements* $a,b \in A$, *the set*

$$L_{a,b} = \{(a,a,a),(a,b,b),(b,a,b),(b,b,a)\}$$

is a subuniverse of $\mathcal{A}^3$.

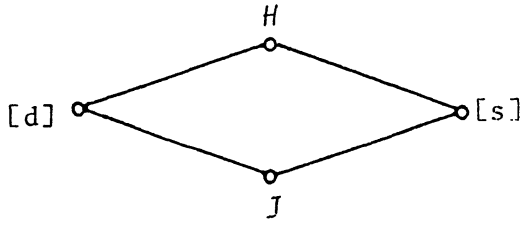
PROOF. Since $d((a,b,b),(b,a,b),(b,b,a)) = (b,b,b)$, the operation d does not preserve $L_{a,b}$ if $a \neq b$ $(a,b \in A)$. Thus (ii) $\Rightarrow$ (i). We start the proof of the reverse implication with

Claim 1. If $d \notin T(\mathcal{A})$, then for arbitrary distinct elements $a,b \in A$, and for every operation $f \in T^{(3)}(\mathcal{A})$, the restriction $f|_{\{a,b\}}$ of f is not a majority operation.

Suppose that $\mathcal{A}$ has a term operation f with $f|_{\{a,b\}}$ a majority operation for some $a,b \in A$, $a \neq b$. Then by the homogeneity of f, $f|_B$ is a majority operation for every 2-element subset B of A. Thus f itself is a majority operation. However, since $|A| \geq 5$, f is a pattern operation. Hence, up to a permutation of its variables, f coincides with d.

We will need a fact concerning clones of homogeneous operations on a 2-element set.

Claim 2. The clone H of all idempotent homogeneous operations on a 2-element set A has exactly 4 subclones, namely



Indeed, making use of Proposition 1.12 it is easy to see that every non-trivial subclone C of H contains either d, the unique majority operation on A, or s, the unique minority operation on A. If $d \in C$, then a simple application of Corollary 1.25 yields that $C = [d]$ or $C = H$, while if $s \in C$, then $(A;C)$ is an idempotent para-primal algebra and $C = [s]$ or $C = H$ follows from Theorem 4.11. Since $[d]$ and $[s]$ are incomparable, the proof is complete. (Of course, the claim can also be checked by referring to Post's lattice, see Chapter 1. Recall that on $\{0,1\}$ the operation s coincides with p.)

Now the implication (i) $\Rightarrow$ (ii) follows quite easily. If $d \notin T(\mathcal{A})$, then by Claim 1 the restriction $T(\mathcal{A})|_{\{a,b\}}$ of $T(\mathcal{A})$ to each 2-element subuniverse $\{a,b\}$ of $\mathcal{A}$ contains no majority operation. On the other hand, clearly, $T(\mathcal{A})|_{\{a,b\}}$ is a clone of idempotent homogeneous operations on $\{a,b\}$. Hence by Claim 2 it is contained in the clone generated by the minority operation s on $\{a,b\}$. Since s preserves $L_{a,b}$, it follows that $L_{a,b}$ is a subuniverse of $\mathcal{A}^3$.

The preceding lemma shows that on every finite set A with $|A| \geq 5$, there is, up to term equivalence, a largest homogeneous algebra $\mathcal{A} = (A;F)$ such that $d \notin T(\mathcal{A})$. Surprisingly, crosses turn out to play an important role in the description of homogeneous non-dual-discriminator algebras as well.

LEMMA 5.7. *Let $\mathcal{A} = (A;F)$ be a finite homogeneous algebra with $|A| \geq 5$. If $\mathcal{A}^2$ has a reduced subuniverse of size m $(2 \leq m \leq |A|)$, then there is an $m \times 2$ cross among the subuniverses of $\mathcal{A}^2$.*

PROOF. Let $B \prec B_1 \times B_2$ be a reduced subuniverse of $\mathcal{A}^2$ such that $m = |B_1| \geq |B_2|$ (≥ 2). First we show that there is a 2×2 cross among the subuniverses of $\mathcal{A}^2$. Since B is reduced and $|B_1| \geq |B_2|$, the subuniverses $B(x,b)$ $(b \in B_2)$ of $\mathcal{A}$ are neither all equal, nor all singletons. If there are two distinct sets

$B(x,b)$ and $B(x,b')$ $(b,b' \in B_2)$ which are not disjoint, say $a \in B(x,b) \cap B(x,b')$ and $a' \in B(x,b) - B(x,b')$, then the subuniverse

$$B \cap (\{a,a'\} \times \{b,b'\})$$

of $\mathcal{A}^2$ is a 2×2 cross. Otherwise, that is, if any two distinct sets of the form $B(x,b)$ $(b \in B_2)$ are disjoint, then select $b',b'' \in B_2$ so that $B(x,b') \cap B(x,b'') = \emptyset$ and $|B(x,b')| \geq 2$. Let, say, $a,a' \in B(x,b')$ with $a \neq a'$, $a'' \in B(x,b'')$, and consider the subuniverse

$$C = B \cap (\{a,a',a''\} \times \{b',b''\})$$

of $\mathcal{A}^2$. Clearly, $C = \{(a,b'),(a',b'),(a'',b'')\}$, so $E = C \circ C^{\cup}$ is the equivalence relation with blocks $\{a,a'\}$, $\{a''\}$ on $\{a,a',a''\}$. Using the cycle $\pi = (a\ a'\ a'')$, which is an internal isomorphism of $\mathcal{A}$, we get the subuniverse

$$E[\pi,\pi] \circ E = \{a,a',a''\}^2 - \{(a,a'')\}$$

of $\mathcal{A}^2$. The first case settled above applies for this subuniverse, so we again conclude that there is a 2×2 cross among the subuniverses of $\mathcal{A}^2$.

From now on we proceed by induction. Suppose $2 \leq k < m$ and there is a $k \times 2$ cross among the subuniverses of $\mathcal{A}^2$. We prove that for some n, $k < n \leq m$, there is also an $n \times 2$ cross among the subuniverses of $\mathcal{A}^2$. Since B is not a bijection and $|B_1| = m > k$, therefore there exist pairwise distinct elements $a_1,\ldots,a_k \in B_2$ such that

$$\Big|\bigcup_{i=1}^{k} B(x,a_i)\Big| > k.$$

Moreover, since $B \neq B_1 \times B_2$, we can select $a_1,\ldots,a_k$ so that not all sets $B(x,a_i)$ $(1 \leq i \leq k)$ are equal, say

$$\bigcup_{i=1}^{k} B(x,a_i) \supset B(x,a_1). \tag{5.1}$$

Let C_1 [resp. C_0] denote the left [resp. right] hand side of (5.1), and let

$n = |C_1|$. Then we have $n > k$, furthermore, by assumption and by Proposition 5.4, the cross

$$K = \{(a_1,v'),(a_1,v),(a_2,v),\ldots,(a_k,v)\}$$

is a subuniverse of $\mathcal{A}^2$ for arbitrary elements $v,v' \in A$, $v \neq v'$. In particular, it follows that $\{a_1,\ldots,a_k\}$ is a subuniverse of $\mathcal{A}$. Thus

$$C = B \cap (B_1 \times \{a_1,\ldots,a_k\}) \quad \text{and} \quad D = C \circ K$$

are subuniverses of $\mathcal{A}^2$. It is easy to see that

$$D = (C_o \times \{v'\}) \cup (C_1 \times \{v\}),$$

so for arbitrary cyclic permutation $\sigma = (c_1\ c_2\ \ldots\ c_n)$ of C_1 with $C_o = \{c_1,\ldots,c_\ell\}$ $(\ell = |C_o|)$, the subuniverse

$$\bigcap_{j=1}^{\ell-1} D[\sigma^j,\mathrm{id}]$$

of $\mathcal{A}^2$ is an $n \times 2$ cross.

LEMMA 5.8. *Let $\mathcal{L} = (B;F)$ be a finite idempotent homogeneous algebra. If a set of the form $L_{a,b}$ $(a,b \in B,\ a \neq b)$ as well as a $|B| \times 2$ cross is among the subuniverses of $\mathcal{L}^3$ and $\mathcal{L}^2$, respectively, then $\mathcal{L}$ is trivial.*

PROOF. By proposition 1.12 it suffices to prove that no operation listed there is a term operation of $\mathcal{L}$. Idempotency immediately excludes unary operations. Assume $f \in T(\mathcal{L})$ is binary. Since $L_{a,b}$ is a subuniverse of $\mathcal{L}^3$, $\{a,b\}$ is a subuniverse of $\mathcal{L}$. Hence $f(a,b) \in \{a,b\}$, say $f(a,b) = a$. Thus homogeneity and idempotency yield that f is the first projection. Majority operations do not preserve $L_{a,b}$, therefore $T(\mathcal{L})$ contains no majority operation. Suppose now that $f \in T(\mathcal{L})$ is a k-ary, say first, semiprojection. By assumption and by Proposition 5.4 every $|B| \times 2$ cross

$$K = (B \times \{b\}) \cup \{(a,b')\} \qquad (a,b,b' \in B,\ b \neq b')$$

is a subuniverse of $\mathcal{A}^2$. Hence for arbitrary elements $a_2,\dots,a_k \in B$,

$$(f(a,a_2,\dots,a_k),b') = f((a,b'),(a_2,b),\dots,(a_k,b)) \in K,$$

implying that $f(a,a_2,\dots,a_k) = a$. Thus f is a projection. Finally, if f were a minority operation, then for the cross K above and for arbitrary element $c \in B$, $c \neq a$, we would get that

$$(c,b') = f((c,b),(a,b),(a,b')) \in K,$$

a contradiction. The proof of the lemma is complete.

After these preparations we can describe those homogeneous algebras in which d is not a term operation. Let E_1^0 [resp. E_1^1] denote the clone of all pattern [resp. homogeneous] operations on A which preserve $L_{a,b}$ for all $a,b \in A$, $a \neq b$. For $2 \leq i \leq |A|$, let E_i^0 [resp. E_i^1] denote the clone of all pattern [resp. homogeneous] operations f such that $f|_B$ is a projection for every i-element subset B of A. It is easy to see that $E_i^j \subseteq E_1^j$ $(2 \leq i \leq |A|$, $j \in \{0,1\})$.

THEOREM 5.9. *Every nontrivial finite homogeneous algebra* $\mathcal{A} = (A;F)$ *with* $|A| \geq 5$ *such that* d *is not a term operation of* $\mathcal{A}$ *is term equivalent to one of the algebras* $(A;E_i^j)$ *with* $j \in \{0,1\}$ *and* $1 \leq i \leq |A| - j - 1$. *These clones* E_i^j *are nontrivial and pairwise distinct. The lattice they form, together with a generating set of each clone is shown in Figure* 3.

PROOF. Let $\mathcal{A} = (A;F)$ be a finite homogeneous algebra such that $n = |A| \geq 5$ and $d \notin T(\mathcal{A})$. Set $C = T(\mathcal{A})$. Let $j = 0$ if $\mathcal{A}$ has $(n-1)$-element subalgebras and $j = 1$ otherwise. By Lemma 5.6 we have $C \subseteq E_1^j$. Assume first that $\mathcal{A}^2$ has no reduced subuniverses. Since $\mathcal{A}$ is idempotent, Corollary 4.13 shows that $\mathcal{A}$ is para-primal. Each subuniverse $L_{a,b}$ $(a,b \in A,\ a \neq b)$ of $\mathcal{A}^3$ is $+^{\square}$ for a group operation $+$ on $\{a,b\}$. Therefore it follows that for every

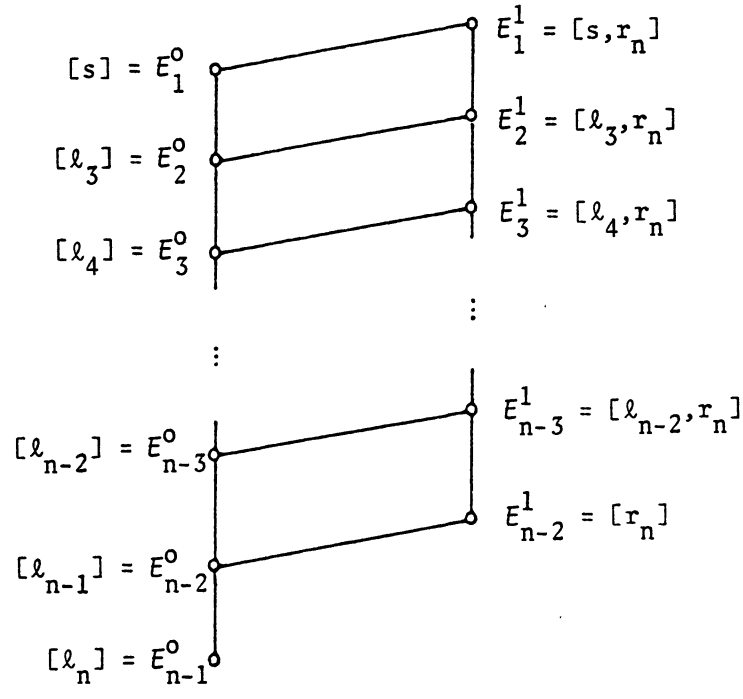


Figure 3

$a,b \in A$, $a \neq b$,

$P_{a,b} = (x+y+z)^{\square} = \{w \in \{a,b\}^4$: an even number of components of w equal $b\}$

is a subuniverse of $\mathcal{A}^4$. This implies that each 2-element subset of A is an affine subuniverse of $\mathcal{A}$. Moreover, $\mathcal{A}$ has no other affine subuniverses, as an affine subalgebra of a para-primal algebra has no nonsingleton proper subalgebras. Hence Theorem 4.11 can be applied to conclude that $E_1^j \subseteq C$. Thus in this case $C = E_1^j$.

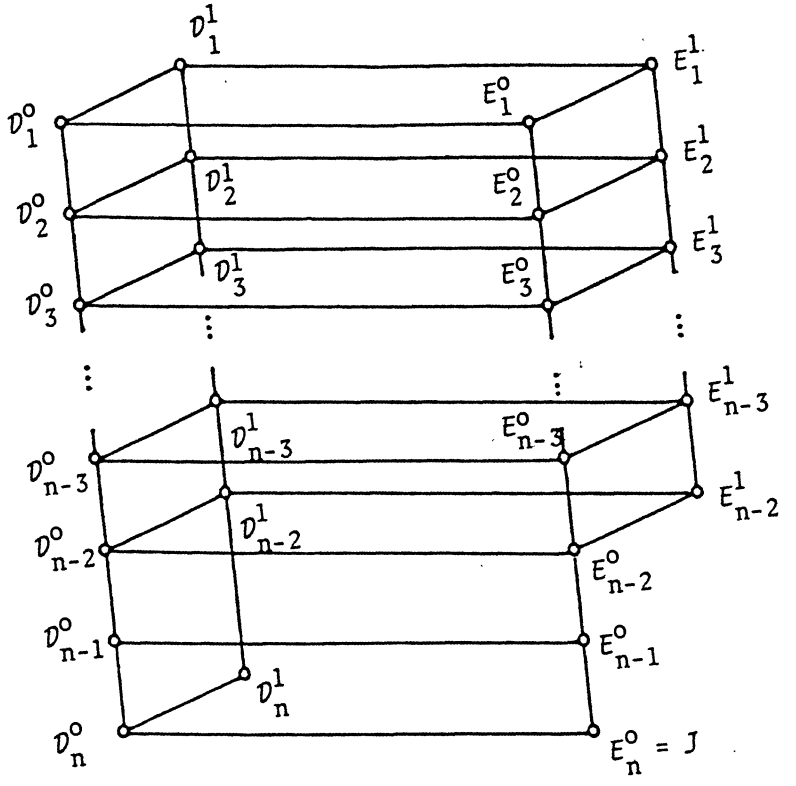
Assume now that $\mathcal{A}^2$ has reduced subuniverses, and let i denote the maximum of the sizes of reduced subuniverses of $\mathcal{A}^2$. Obviously, $2 \leq i \leq n$. By Lemma 5.7 and by Proposition 5.4, every $i \times 2$ cross is a subuniverse of $\mathcal{A}^2$. Thus, for every i-element subset B of A, the subalgebra $(B;F)$ of $\mathcal{A}$ satisfies the assumptions of Lemma 5.8. Hence its clone, the restriction of C to B, contains projections only, implying that $C \subseteq E_i^j$. As $\mathcal{A}$ was assumed to be

nontrivial, we have $i < n$. We prove that $C = E_i^j$. The algebras $\mathcal{A}$ and $(A;E_i^j)$ are easily seen to have the same internal isomorphisms. Therefore it remains to show that every operation $f \in E_i^j$ preserves the reduced subuniverses of finite powers of $\mathcal{A}$.

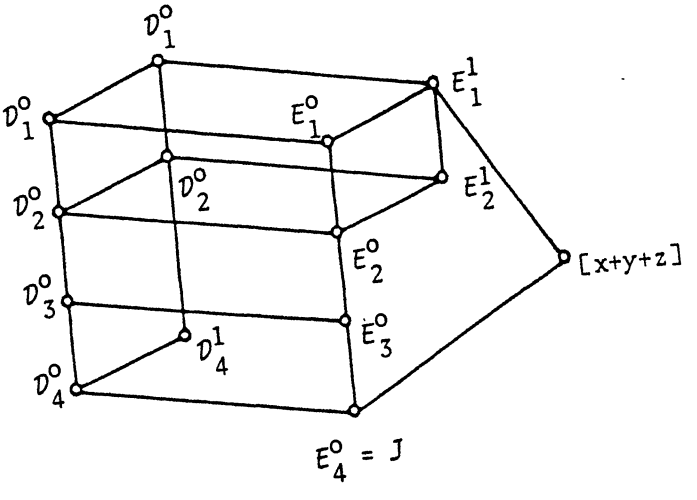
Let $C \prec C_1 \times \ldots \times C_k$ be a reduced subuniverse of $\mathcal{A}^k$ $(k \geq 2)$. Observe that C is of size at most i. Indeed, otherwise Theorem 4.3 and the maximality of i would imply that $|C_1| = \ldots = |C_k|$ $(> i \geq 2)$ and $(C_1;F)$ is an affine subalgebra of $\mathcal{A}$ without nonsingleton proper subalgebras. However, this is impossible, because by Proposition 5.1 every 2-element subset of A is a subuniverse of $\mathcal{A}$. Hence $|C_\ell| \leq i$ for all $1 \leq \ell \leq k$. Select a fixed i-element subset B of A and arbitrary bijections $\pi_\ell: C_\ell \to B_\ell$ with $B_\ell \subseteq B$ $(1 \leq \ell \leq k)$. Since $f|_B$ is a projection, f clearly preserves $C[\pi_1,\ldots,\pi_k]$. However, $\pi_1,\ldots,\pi_k$ are internal isomorphisms of $\mathcal{A}$, therefore f preserves C, too. Thus $C = E_i^j$, as stated. Obviously, $j = 0$ if $i = n-1$.

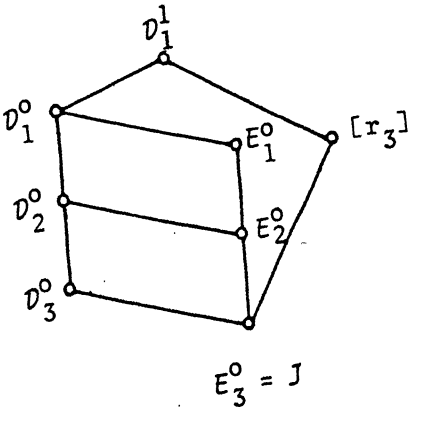
The rest of the proof can be finished as in Theorem 5.5. The details are left to the reader.

Summarizing Theorems 5.5 and 5.9 we get the lattice of clones of homogeneous algebras on a finite set A of n (≥ 5) elements:

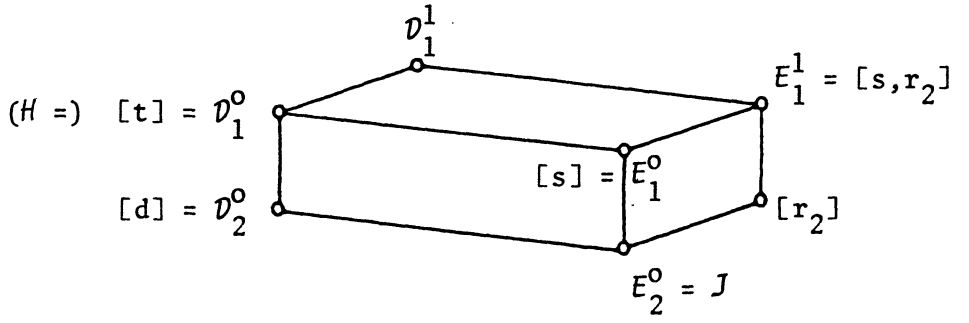


The assumption $|A| = n \geq 4$ or 5 was made throughout the discussion only to avoid some technical details which are mainly due to the existence of "exceptional" homogeneous algebras on small sets. The lattices of clones of homogeneous algebras on a 4-element, resp. 3-element set A are the following (S. S. Marchenkov [1982a], [1979]):





The clones $\mathcal{D}_3^1$ and E_1^1 do not exist on a 3-element set because every 3-element homogeneous algebra $\mathcal{A} = (A;F)$ which is not term equivalent to $(A;\mathcal{D}_1^1)$ or $(A;r_3)$ has 2-element subuniverses. This can be proved by making use of Theorem 4.3 and the remark after Proposition 5.4. The lattice of clones of homogeneous algebras on a 2-element set A is

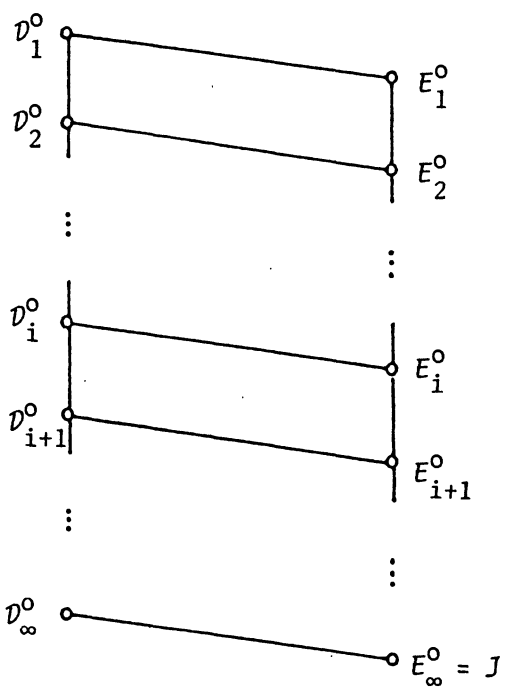


This follows from Claim 2 in the proof of Lemma 5.6 and from the fact that every nonidempotent clone C of homogeneous operations on A is generated by r_2 and the idempotent operations from C. (Cf. also Figure 1 where $r_2 = r$, $s = p$, and $\mathcal{D}_1^1$ is the clone determined by $r^{\square}$.)

A way to understand the structure of the lattice of clones of finite homogeneous algebras is as follows. For each homogeneous quasi-primal algebra $\mathcal{A}^*$ on A (up to term equivalence, there are only two of them), the reducts $\mathcal{A}$ of $\mathcal{A}^*$ having the same internal isomorphisms as $\mathcal{A}^*$ form a "ladder" (some vertices at the bottom may be missing); the two sides of the ladder consist of those $\mathcal{A}$ with $d \in T(\mathcal{A})$ and of those with $d \notin T(\mathcal{A})$, respectively; furthermore, the rungs of the ladder correspond to the maximal size of crosses among the subuniverses of $\mathcal{A}^2$. The approach presented here yields that this holds also under weaker symmetry conditions than homogeneity. A special case is, for instance, the result announced by S. S. Marchenkov [1982b] on the finite algebras $\mathcal{A} = (A;F)$ with $|A| \geq 4$ such that every even permutation of A is an automorphism of $\mathcal{A}$.

Interestingly, the infinite homogeneous algebras $\mathcal{A} = (A;F)$ are less complicated than the finite ones. As we mentioned earlier, all operations of $\mathcal{A}$ are pattern operations. On the other hand, it can be seen that $\mathcal{A}$ is determined by its finite subalgebras. So, making use of the above results on finite homogeneous algebras, the reader can easily verify

EXERCISE 5.10. For arbitrary infinite set A, the lattice of clones of homogeneous algebras on A is



where the clones $\mathcal{D}_i^o$ and E_i^o $(i = 1,2,\ldots)$ are defined as in the finite case, and $\mathcal{D}_\infty^o = \bigcap_{i=1}^{\infty} \mathcal{D}_i^o$, $E_\infty^o = \bigcap_{i=1}^{\infty} E_i^o$.

Chapter 6

FUNCTIONALLY COMPLETE ALGEBRAS

We now consider a property which parallels primality in other respects than the concepts introduced in Chapter 4.

DEFINITION. A finite algebra $\mathcal{A} = (A;F)$ is called *functionally complete* iff every operation on A is a polynomial operation of $\mathcal{A}$. Otherwise $\mathcal{A}$ is called *functionally incomplete*.

EXAMPLES. The following algebras are functionally complete:

1. finite fields;

2. every finite algebra $(A;\oplus,\circ,\{\chi_a: a \in A\})$ containing two elements $0, 1$ such that $a \oplus 0 = a = 0 \oplus a$, $a \circ 0 = 0$, $a \circ 1 = a$, and

$$\chi_a(b) = \begin{cases} 1 & \text{if } b = a \\ 0 & \text{otherwise} \end{cases} \qquad (b \in A)$$

for all $a \in A$;

3. $(A;t)$ with A an arbitrary finite set and t the discriminator on A (H. Werner [1970]);

4. $(A;d)$ where A is a finite set with $|A| \neq 2$, and d is the dual discriminator on A (E. Fried and A. F. Pixley [1979]).

Clearly, a finite algebra $\mathcal{A}$ is functionally complete if and only if the algebra $\overline{\mathcal{A}}$ arising from $\mathcal{A}$ by adding all constants as basic operations is primal. This simple observation, combined with some earlier results, yields the following criteria for the functional completeness of majority algebras and Mal'tsev algebras.

EXERCISE 6.1. A finite majority algebra $\mathcal{A} = (A;F)$ is functionally complete if and only if Δ_A and ∇_A are the only reflexive subuniverses of $\mathcal{A}^2$. (Hint: use Corollary 1.25.)

EXERCISE 6.2. A finite arithmetical algebra is functionally complete if and only if it is simple. (Apply Exercises 6.1 and 1.27.)

EXERCISE 6.3. A finite Mal'tsev algebra containing at least two elements is functionally complete if and only if it is simple and non-affine. (Make use of Theorem 4.7 and Corollary 4.12.)

The latter result is due to R. McKenzie [1976], and generalizes the corresponding theorems for groups (A. V. Kuznetsov [unpublished][1], W. D. Maurer and J. L. Rhodes [1965]) and rings (L. Rédei and T. Szele [1947] in the commutative case, A. V. Kuznetsov [unpublished][1] in general).

The most general criterion for functional completeness can be derived from Corollary 1.20.

We want to extend the concept of functional completeness to infinite algebras as well. For cardinality reasons, like in the case of primality, it seems natural to consider local polynomial operations instead of polynomial operations.

DEFINITION. An algebra $\mathcal{A} = (A;F)$ is called *locally functionally complete* iff every operation on A is a local polynomial operation of $\mathcal{A}$.

---

[1] See p. 106 in: Mathematics in the USSR during the forty years 1917-1957, vol. I, Fizmatgiz, Moscow, 1959.

Obviously, for finite algebras local functional completeness is equivalent to functional completeness. Interestingly, all results mentioned so far carry over to infinite algebras, we have only to replace functional completeness with local functional completeness. This is straightforward for the examples, for Exercise 6.1 (use Corollary 1.24 in the proof) and for Exercise 6.2. More difficult is the generalization of Exercise 6.3, which was done by H. P. Gumm [1979]. In the next section we prove a general theorem from which all these results can be derived.

An elementary interpolation theorem

Given a finite algebra $\mathcal{A} = (A;F)$, how can we decide whether $\mathcal{A}$ is functionally complete if we do not know much about the structure of $\mathcal{A}$? For every operation g on A, we can try to construct, step by step, polynomial operations of $\mathcal{A}$ agreeing with g on two, three, etc., elements of its domain. The same idea may work also in establishing local functional completeness.

DEFINITION. Let $\mathcal{A} = (A;F)$ be an algebra and $n \geq 2$ a natural number. We say that $\mathcal{A}$ has the *n-interpolation property* iff for every integer $k \geq 1$, for arbitrary pairwise distinct k-tuples $a_1,\ldots,a_n \in A^k$, and for arbitrary elements $b_1,\ldots,b_n \in A$ there exists a k-ary polynomial operation f of $\mathcal{A}$ such that $f(a_i) = b_i$ for all $1 \leq i \leq n$. The algebra $\mathcal{A}$ is said to have the *$1\frac{1}{2}$-interpolation property* iff for arbitrary elements $a,b,c \in A$ with $a \neq c$ there exists a unary polynomial operation f of $\mathcal{A}$ such that $f(a) = b$ and $f(c) = c$.

Clearly, an algebra $\mathcal{A} = (A;F)$ is locally functionally complete, or a finite algebra $\mathcal{A} = (A;F)$ is functionally complete, if and only if it has the n-interpolation property for all $n \geq 2$. The $1\frac{1}{2}$-interpolation property is easier to handle than the 2-interpolation property, and, though apparently weaker, is equivalent to it if $|A| > 2$.

LEMMA 6.4. *An algebra* $\mathcal{A} = (A;F)$ *with* $|A| > 2$ *has the 2-interpolation property if and only if it has the* $1\frac{1}{2}$*-interpolation property.*

PROOF. The necessity being trivial, suppose that $\mathcal{A}$ has the $1\frac{1}{2}$-interpolation property. First we show that $\mathcal{A}$ has the 2-interpolation property for unary operations, that is, for arbitrary elements $a,b,c,d \in A$ with $a \neq c$ there exists an $f \in P^{(1)}(\mathcal{A})$ such that $f(a) = b$ and $f(c) = d$. If $b \neq c$, then by the $1\frac{1}{2}$-interpolation property there are $f_1,f_2 \in P^{(1)}(\mathcal{A})$ such that $f_1(a) = b$, $f_1(c) = c$, $f_2(b) = b$, $f_2(c) = d$. Hence $f = f_2f_1 \in P^{(1)}(\mathcal{A})$ is as required. The case $a \neq d$ is symmetric. Assume finally that $b = c$, $a = d$. Since $|A| > 2$, there exists an element $u \in A - \{a,b\}$. Now the $1\frac{1}{2}$-interpolation property yields the existence of $f_1,f_2,f_3 \in P^{(1)}(\mathcal{A})$ such that $f_1(a) = a$, $f_1(b) = u$, $f_2(a) = b$, $f_2(u) = u$, $f_3(b) = b$, $f_3(u) = a$. Thus $f = f_3f_2f_1 \in P^{(1)}(\mathcal{A})$ is the operation we were after.

To prove the 2-interpolation property in general, consider for $k \geq 1$ arbitrary distinct k-tuples $a_i = (a_{i1},\ldots,a_{ik}) \in A^k$ $(i = 1,2)$ and arbitrary elements $b_1,b_2 \in A$. Since $a_1 \neq a_2$, we have $a_{1j} \neq a_{2j}$ for some $1 \leq j \leq k$. Furthermore, by the preceding paragraph, there is an operation $f_o \in P^{(1)}(\mathcal{A})$ such that $f_o(a_{ij}) = b_i$ for $i = 1,2$. Let f be the k-ary operation arising from f_o by adding k-1 fictitious variables so that the original variable be the j-th one. Then obviously $f(a_i) = b_i$ for $i = 1,2$, completing the proof.

The main result of this section is a general interpolation theorem establishing some fairly mild conditions under which the step-by-step interpolation can be carried out. The idea goes back to E. Fried, H. K. Kaiser and L. Márki [1982].

THEOREM 6.5. *An algebra* $\mathcal{A} = (A;F)$ *is locally functionally complete if and only if it has the 2-interpolation property and has a family* $\{f_\lambda : \lambda \in \Lambda\}$

(f_λ is n_λ-ary) of local polynomial operations such that

(a) *the identity* $f_\lambda(x,x,x_3,\dots,x_{n_\lambda}) = x$ *holds for all* $\lambda \in \Lambda$;

(b) *for every* $\lambda \in \Lambda$, *there is a mapping* $\iota_\lambda : \{x_3,\dots,x_n\} \to \{x,y\}$ *such that the identity* $f_\lambda(x,y,x_3\iota_\lambda,\dots,x_{n_\lambda}\iota_\lambda) = x$ *is satisfied;*

(c) *for arbitrary distinct elements* $a,b \in A$, *there exist* $\lambda \in \Lambda$ *and* $c_2,\dots,c_{n_\lambda} \in A$ *such that* $f_\lambda(a,c_2,\dots,c_{n_\lambda}) = b$.

REMARK. Notice that if $n_\lambda \le 2$ for some $\lambda \in \Lambda$, then by (b) f_λ is the first projection, so it cannot play a role in (c). Therefore there is no loss of generality in assuming that every f_λ ($\lambda \in \Lambda$) is at least ternary.

PROOF of Theorem 6.5. The necessity of the conditions follows easily. For example, any majority operation f alone forms a family satisfying (a)-(c), as the identities $f(x,x,y) = x$ and $f(x,y,x) = x$ hold for f and $f(a,b,b) = b$ for arbitrary elements $a,b \in A$.

Conversely, assume now that $\mathcal{A} = (A;F)$ has the 2-interpolation property, and has a family $\{f_\lambda : \lambda \in \Lambda\}$ of local polynomial operations satisfying (a)-(c). We prove by induction on n that $\mathcal{A}$ has the n-interpolation property for all $n > 2$, too. Suppose that $\mathcal{A}$ has the n-interpolation property for some $n \ge 2$, and consider for arbitrary $k \ge 1$ pairwise distinct k-tuples $a_0,a_1,\dots,a_n \in A^k$ and arbitrary elements $b_0,b_1,\dots,b_n \in A$. We are done if we find a k-ary local polynomial operation g of $\mathcal{A}$ such that $g(a_i) = b_i$ for all $0 \le i \le n$. The table below helps to follow the construction. By the n-interpolation property $\mathcal{A}$ has a k-ary polynomial operation g_1 with $g_1(a_i) = b_i$ for all $1 \le i \le n$. If $g_1(a_0) = b_0$, then g_1 is the operation we wanted to find. Otherwise, by condition (c), there exist $\lambda \in \Lambda$ and $c_2,\dots,c_{n_\lambda} \in A$ such that $f_\lambda(g_1(a_0),c_2,\dots,c_{n_\lambda}) = b_0$. As it was remarked, $n_\lambda \ge 3$. Using again the n-interpolation property we get that $\mathcal{A}$ has a k-ary polynomial operation g_2 such that $g_2(a_0) = c_2$ and $g_2(a_i) = b_i$ for all $1 \le i \le n-1$. Now condition

	a_o	a_1	a_2	...	a_{n-1}	a_n
g_1	$g_1(a_o)$	b_1	b_2		b_{n-1}	b_n
g_2	c_2	b_1	b_2		b_{n-1}	$g_2(a_n)$
g_3	c_3					u_3
$\vdots$	$\vdots$					$\vdots$
g_{n_λ}	c_{n_λ}					u_{n_λ}
f_λ	b_o	b_1	b_2		b_{n-1}	b_n

(b) ensures that there exist elements $u_3,\dots,u_{n_\lambda} \in \{b_n, g_2(a_n)\}$ such that $f_\lambda(b_n, g_2(a_n), u_3, \dots, u_{n_\lambda}) = b_n$. Using the 2-interpolation property, select for every $3 \le j \le n_\lambda$ a polynomial operation g_j of $\mathcal{A}$ so that $g_j(a_o) = c_j$ and $g_j(a_n) = u_j$. In view of (a) it follows that for the operation $g = f_\lambda(g_1,\dots,g_{n_\lambda})$ we have $g(a_i) = b_i$ for all $0 \le i \le n$. Clearly, g is a local polynomial operation of $\mathcal{A}$. Thus $\mathcal{A}$ is locally functionally complete.

Condition (c) in Theorem 6.5 can be replaced by a stronger condition which implies the $1\frac{1}{2}$-interpolation property. Thus we get a variant of the interpolation theorem of E. Fried, H. K. Kaiser and L. Márki [1982].

COROLLARY 6.6. *An algebra* $\mathcal{A} = (A;F)$ *with* $|A| > 2$ *is locally functionally complete if and only if it has a family* $\{f_\lambda : \lambda \in \Lambda\}$ (f_λ *is* n_λ*-ary*) *of local polynomial operations such that* (a) *and* (b) *of Theorem* 6.5 *hold, moreover,*

(c') *for arbitrary distinct elements* $a_1, a_2, b \in A$, *there exist* $\lambda \in \Lambda$ *and* $c_3,\dots,c_{n_\lambda} \in A$ *such that* $f_\lambda(a_1, a_2, c_3, \dots, c_{n_\lambda}) = b$.

PROOF. The necessity is again easy, as the dual discriminator on A alone forms a family satisfying (a), (b) and (c'). Conversely, suppose $\mathcal{A}$ has a family

$\{f_\lambda : \lambda \in \Lambda\}$ of local polynomial operations such that (a), (b) and (c') hold. Since $|A| > 2$, (c') implies (c), therefore by Theorem 6.5 and Lemma 6.4 it remains to show that $\mathcal{A}$ has the $1\frac{1}{2}$-interpolation property. Let $a_1, a_2, b \in A$, $a_1 \neq a_2$. If we find a local polynomial operation f of $\mathcal{A}$ with $f(a_1) = a_1$ and $f(a_2) = b$, we are done. Assume first $b \neq a_1, a_2$. Then selecting f_λ and $c_3, \ldots, c_{n_\lambda} \in A$ by (c') and putting $f(x) = f_\lambda(a_1, x, c_3, \ldots, c_{n_\lambda})$, we get the required operation. Otherwise, if $b = a_1$ or $b = a_2$, then f can be chosen to be the constant operation with value b or the identity, respectively.

As an application we derive the infinite versions of Exercises 6.1-6.3 from Theorem 6.5. Observe first how the 2-interpolation property is related to the subuniverses of the square of the algebra.

LEMMA 6.7. *An algebra* $\mathcal{A} = (A;F)$ *has the 2-interpolation property if and only if* Δ_A *and* ∇_A *are the only reflexive subuniverses of* $\mathcal{A}^2$.

PROOF. For every pair $(a,b) \in A^2$, the reflexive subuniverse of $\mathcal{A}^2$ generated by (a,b) is the set

$$\{(g(a),g(b)) : g \in P^{(1)}(\mathcal{A})\}.$$

Therefore $\mathcal{A}$ has the 2-interpolation property for unary operations if and only if Δ_A and $\nabla_A = A^2$ are the only reflexive subuniverses of $\mathcal{A}^2$. However, as we have seen in the proof of Lemma 6.4, the 2-interpolation property for unary operations implies the 2-interpolation property for operations of arbitrary arity.

As was observed in the proof of Theorem 6.5, a majority operation alone satisfies conditions (a)-(c). Combined with the preceding lemma this immediately yields

PROPOSITION 6.8. *A majority algebra* $\mathcal{A} = (A;F)$ *is locally functionally complete if and only if* Δ_A *and* ∇_A *are the only reflexive subuniverses of* $\mathcal{A}^2$.

Taking into account Exercise 1.27 we get

COROLLARY 6.9. *An arithmetical algebra is locally functionally complete if and only if it is simple.*

The same is almost true for the more general class of Mal'tsev algebras as well, only the affine algebras have to be excluded.

THEOREM 6.10. *A Mal'tsev algebra containing at least two elements is locally functionally complete if and only if it is simple and nonaffine.*

PROOF. The necessity of the conditions is obvious. Conversely, assume $\mathcal{A} = (A;F)$ is a simple Mal'tsev algebra which is not affine. In view of Lemma 6.7 and Exercise 1.27, the simplicity implies that $\mathcal{A}$ has the 2-interpolation property. We construct a family of polynomial operations of $\mathcal{A}$ so that they satisfy conditions (a)-(c) of Theorem 6.5.

Let us fix a Mal'tsev operation $p \in T(\mathcal{A})$, and consider the family of ternary polynomial operations of $\mathcal{A}$ of the form

$$p(x_1,a,g(p(s(g'(x_i),g'(x_2),g'(x_j)),g'(x_i),a'))) \tag{6.1}$$

where $a,a' \in A$, $\{i,j\} = \{1,3\}$, $g,g' \in P^{(1)}(\mathcal{A})$ with $g(a') = a$, and $s \in P^{(3)}(\mathcal{A})$ satisfies the identities

$$s(x,x,y) = s(x,y,y) = x. \tag{6.2}$$

It is easy to check that for every such operation $f \in P^{(3)}(\mathcal{A})$ the identities $f(x,x,y) = f(x,y,y) = x$ hold. Hence (a) and (b) of Theorem 6.5 are satisfied. It remains to show that (c) also holds.

Let $a,b \in A$, $a \neq b$. Since $\mathcal{A}$ is not affine, Theorem 2.4 yields that $\mathcal{A}$ has a ternary polynomial operation s satisfying the identities (6.2), and distinct from the first projection. If there exists such an s with the stronger property that $s(x,y,a)$ is not the first projection, say $s(c_1,c_2,a) \neq c_1$ $(c_1,c_2 \in A)$, then let f be the polynomial operation (6.1) where $a' = c_1$,

$(i,j) = (3,1)$, g' is the identity, and g is a unary polynomial operation with $g(c_1) = a$, $g(s(c_1,c_2,a)) = b$. (Such a g exists by the 2-interpolation property.) Thus

$$f(a,c_2,c_1) = g(p(s(c_1,c_2,a),c_1,c_1)) = g(s(c_1,c_2,a)) = b.$$

In the opposite case we have

$$p(p(x,y,a),a,y) = x \quad \text{for all} \quad x,y \in A,$$

as the ternary polynomial operation $p(p(x,y,z),z,y)$ of $\mathcal{A}$ satisfies the identities (6.2). Now select arbitrary operation $s \in P^{(3)}(\mathcal{A})$ satisfying (6.2) so that s is not the first projection; say $s(c_1,c_2,c_3) \neq c_1$ $(c_1,c_2,c_3 \in A)$. Let f be the operation of the form (6.1) with $a' = c_1$, $(i,j) = (1,3)$, $g'(x) = p(x,a,c_1)$, and g a unary polynomial operation with $g(c_1) = a$, $g(s(c_1,c_2,c_3)) = b$. Then $g'(a) = c_1$ and $g'(c_k') = c_k$ for the elements $c_k' = p(c_k,c_1,a)$ $(k = 2,3)$. Hence

$$\begin{aligned} f(a,c_2',c_3') &= g(p(s(g'(a),g'(c_2'),g'(c_3')),g'(a),c_1)) \\ &= g(s(c_1,c_2,c_3)) = b, \end{aligned}$$

completing the proof.

COROLLARY 6.11. *The locally functionally complete groups are exactly the nonabelian simple groups and the 1-element group. The locally functionally complete rings are exactly the simple nonzero rings and the 1-element ring.*

As we mentioned earlier, Theorem 6.10 is a result of H. P. Gumm [1979]. The special cases in Corollary 6.11 were proved in H. K. Kaiser [1975a], [1975b], respectively. The idea of the proof presented here comes from the paper by E. Fried, H. K. Kaiser and L. Márki [1982], where Corollary 6.11 is derived from their version of Corollary 6.6.

Further applications of Theorem 6.5 will be given in the next section.

Symmetric algebras and functional completeness

As we mentioned at the beginning of this chapter, the finite homogeneous algebras $(A;t)$ and $(A;d)$, the latter provided $|A| \neq 2$, are functionally complete. B. Csákány [1980] proved that functional completeness is a property shared by almost all finite homogeneous algebras; in fact, up to equivalence, there are only six finite homogeneous algebras which are not functionally complete, four of which are 2-element, one 3-element and one 4-element. The same remains true with local functional completeness for arbitrary homogeneous algebras. Loosely speaking, we may say that with a "few" exceptions, highly symmetric algebras are locally functionally complete. We show that this statement remains true even if "highly symmetric" means a much weaker symmetry than homogeneity.

Recall that a permutation group G on A is said to be *k-transitive* (*doubly transitive* for $k = 2$, *triply transitive* for $k = 3$) iff for any k-tuples $(a_1,\ldots,a_k)$, $(b_1,\ldots,b_k) \in A^k$ with pairwise distinct components there exists a permutation $\pi \in G$ such that $a_i\pi = b_i$ for all $1 \leq i \leq k$. The automorphism group of an algebra $\mathcal{A}$ will be denoted by $\mathrm{Aut}\,\mathcal{A}$.

Let $_K\underline{A} = (A;+,K)$ be a vector space over a field K. The *affine space* corresponding to $_K\underline{A}$ (cf. p. 14) is the algebra

$$(A;x-y+z,\{rx + (1-r)y: r \in K\}),$$

which is term equivalent to the full idempotent reduct of $_K\underline{A}$. Its automorphism group,

$$G(_K\underline{A}) = \{ux + a: u \in \mathrm{Aut}\ {}_K\underline{A},\ a \in A\},$$

is doubly transitive. Moreover, for $|A| \geq 4$, $G(_K\underline{A})$ is triply transitive if and only if $|K| = 2$, that is, $_K\underline{A}$ is term equivalent to an Abelian group of exponent 2. On the other hand, clearly, affine spaces are not functionally complete.

The following theorem shows that among the algebras with triply transitive automorphism groups the affine spaces over the 2-element field are essentially the only ones which are not locally functionally complete.

THEOREM 6.12. *An at least 4-element nontrivial algebra with triply transitive automorphism group is either locally functionally complete, or is term equivalent to an affine space over the 2-element field.*

PROOF. Let $\mathcal{A} = (A;F)$ be a nontrivial algebra such that $|A| \geq 4$ and $\mathrm{Aut}\,\mathcal{A}$ is triply transitive. Observe that every binary term operation f of $\mathcal{A}$ is a projection. Indeed, for arbitrary elements $a,b \in A$ and for every automorphism π of $\mathcal{A}$ fixing a and b we have $f(a,b)\pi = f(a\pi,b\pi) = f(a,b)$, that is π fixes $f(a,b)$. Since $|A| \geq 4$ and $\mathrm{Aut}\,\mathcal{A}$ is triply transitive, this implies that $f(a,b) \in \{a,b\}$. In particular, it follows that f is idempotent. Furthermore, if, say, $f(a,b) = a$ for some $a,b \in A$, $a \neq b$, then the double transitivity of $\mathrm{Aut}\,\mathcal{A}$ yields that $f(x,y) = x$ for all distinct $x,y \in A$. Hence f is the first projection.

As $\mathcal{A}$ is nontrivial, we get from Proposition 1.12 and Corollary 2.3 that either $\mathcal{A}$ has a term operation f which is a majority operation or a k-ary ($k \geq 3$) first semiprojection distinct from the first projection, or there exists an Abelian group $\underline{A} = (A;+,0)$ of exponent 2 such that $x + y + z$ is a term operation of $\mathcal{A}$. Moreover, in the latter case, if $\mathcal{A}$ is not affine with respect to $\underline{A}$, then Claim 1 in the proof of Theorem 2.4 shows that $\mathcal{A}$ has, for some $n \geq 3$, an n-ary term operation g distinct from the first projection and satisfying the identities

$$g(z,x_2,\ldots,x_{i-1},z,x_{i+1},\ldots,x_n) = z \quad \text{for all} \quad 2 \leq i \leq n. \tag{6.3}$$

Clearly, every majority operation and every first semiprojection distinct from the first projection also has these properties.

We prove that the algebra $(A;g)$ with g as above is locally functionally complete. Suppose first that there exist elements $a_1,a_2,\ldots,a_n \in A$ such that not all of $a_2,\ldots,a_n$ are equal and $g(a_1,a_2,\ldots,a_n) \neq a_1$. By (6.3) we have $a_1 \neq a_2$. Clearly, $g(a_1,a_2,\ldots,a_n) \neq a_i$ for some $2 \leq i \leq n$. Since the identities (6.3) are symmetric in the second up to the n-th variables, interchanging those variables of g we may assume that $g(a_1,a_2,\ldots,a_n) \neq a_2$. Thus a_1, a_2 and $g(a_1,a_2,\ldots,a_n)$ are pairwise distinct. Since Aut $\mathcal{A}$ is triply transitive, these elements can be sent into any three distinct elements $a,b,c \in A$, respectively, by an automorphism. This implies that condition (c') in Corollary 6.6 holds for the 1-element family $\{g\}$. The other two conditions (a), (b) ensuring the local functional completeness of $(A;g)$ are immediate consequences of (6.3).

Suppose now that $g(a_1,a_2,\ldots,a_n) = a_1$ whenever $a_1,a_2,\ldots,a_n \in A$ are such that $|\{a_2,\ldots,a_n\}| \geq 2$. As g is not the first projection, we have $g(a,b,\ldots,b) \neq a$ for some $a,b \in A$, $a \neq b$. However, then the binary term operation $g(x_1,x_2,\ldots,x_2)$ of $\mathcal{A}$ must be the second projection. Thus $g(x_3,x_2,x_1,\ldots,x_1)$ is the dual discriminator on A, for which the foregoing argument applies.

So far we established that either $\mathcal{A}$ is locally functionally complete or $\mathcal{A}$ is affine with respect to an Abelian group $\underline{A}$ of exponent 2. Taking into account Proposition 2.6 and the fact that $\mathcal{A}$ is idempotent, in the latter case we get $T(\mathcal{A}) = K({}_R\underline{A},\{(0,0)\})$ for a subring R of End $\underline{A}$. Then every binary operation $rx + (1-r)y$ $(r \in R)$ is a term operation of $\mathcal{A}$. Since every binary term operation of $\mathcal{A}$ is a projection, it follows that $R = \{0,1\}$. Hence $\mathcal{A}$ is term equivalent to the affine space corresponding to ${}_R\underline{A}$.

The result in Theorem 6.12 was proved, somewhat differently, by H. K. Kaiser and L. Márki [1980], following the finite version of the theorem in L. Szabó and Á. Szendrei [1979]. However, for finite algebras this result can be

considerably improved. The following theorem of P. P. Pálfy, L. Szabó and Á. Szendrei [1981] is an analogue of Theorem 6.12 for finite algebras with doubly transitive automorphism groups.

THEOREM 6.13. *An at least 3-element nontrivial finite algebra with doubly transitive automorphism group is either functionally complete, or is term equivalent to an affine space over a finite field.*

PROOF. Let $\mathcal{A} = (A;F)$ be a nontrivial finite algebra such that $|A| \geq 3$ and $\mathrm{Aut}\mathcal{A}$ is doubly transitive. For arbitrary operation $f \in F$ and element $a \in A$, every automorphism of $\mathcal{A}$ fixing a must fix $f(a,\ldots,a)$, too. Since $\mathrm{Aut}\mathcal{A}$ is doubly transitive and $|A| \geq 3$, it follows that $f(a,\ldots,a) = a$. Hence the algebra $\mathcal{A}$ idempotent. As $\mathcal{A}$ is nontrivial, Proposition 1.12 yields that $\mathcal{A}$ has a term operation of one of the types (II)-(V).

Claim 1. Every binary term operation of $\mathcal{A}$ is a projection or a quasigroup operation.

Let $\cdot$ be a binary term operation of $\mathcal{A}$, which is not a projection. Fix an element $a \in A$ arbitrarily and consider the unary operation ax. Since $\cdot$ is not the first projection, therefore there exist elements $a_0,b_0,c_0 \in A$ such that $a_0 \neq c_0$ and $a_0b_0 = c_0$. The double transitivity implies that for arbitrary element $c \in A$, $c \neq a$, there exists a $\pi \in \mathrm{Aut}\mathcal{A}$ such that $a_0\pi = a$ and $c_0\pi = c$. Hence $a(b_0\pi) = c$. This, together with the idempotency of $\mathcal{A}$, shows that the unary operation ax is surjective. As A is finite, it is a permutation. Similarly, xa is also a permutation for every $a \in A$. Thus $\cdot$ is a quasigroup operation.

By Proposition 1.21 and Claim 1 we get that $\mathcal{A}$ is a Mal'tsev algebra whenever it has a binary term operation distinct from the projections. Accordingly, we will distinguish three cases:

(1) $\mathcal{A}$ is a Mal'tsev algebra (this includes types (II) and (IV)),

(2) $\mathcal{A}$ is a majority algebra (type (III)), and

(3) for some $k \geq 3$, $\mathcal{A}$ has a k-ary semiprojection among its term operations, which is not a projection (type (V)).

(1) Suppose $\mathcal{A}$ is a Mal'tsev algebra, and let Θ be a maximal congruence of $\mathcal{A}$. For any $\pi \in \mathrm{Aut}\mathcal{A}$ let $\Theta_\pi = \Theta[\pi,\pi]$. It is easy to see that Θ_π is again a maximal congruence of $\mathcal{A}$. We show that $\bigcap(\Theta_\pi : \pi \in \mathrm{Aut}\mathcal{A}) = \Delta_A$. Indeed, select $c,d \in A$ so that $(c,d) \notin \Theta$, and consider arbitrary distinct elements $a,b \in A$. Then there exists a $\pi \in \mathrm{Aut}\mathcal{A}$ such that $c\pi = a$ and $d\pi = b$, whence $(a,b) \notin \Theta_\pi$, proving the claim. This implies that $\mathcal{A}$ is isomorphic to a subdirect product of the algebras $\mathcal{A}/\Theta_\pi$ ($\pi \in \mathrm{Aut}\mathcal{A}$). These algebras are all isomorphic to $\mathcal{L} = \mathcal{A}/\Theta$ which, by the maximality of Θ, is simple. We can now apply the following well-known theorem (see e.g. [BS]): Every algebra with permuting congruence relations, which is a subdirect product of finitely many simple algebras, is isomorphic to the direct product of some of those factors. Hence we immediately get that $\mathcal{A}$ is isomorphic to $\mathcal{L}^n$ for a natural number $n \geq 1$.

Next we prove that $\mathcal{A}$ is either functionally complete or affine. This holds true for $\mathcal{L}$ by Theorem 6.10 (or Exercise 6.3), establishing the claim if $n = 1$. Assume now that $n \geq 2$. We show that $\mathcal{L}$ is not functionally complete. Let Θ denote the kernel of the projection of $\mathcal{L}^n$ onto its first factor. Since $n \geq 2$, we can select elements $a,a' \in B^n$ so that $a \neq a'$ and $(a,a') \in \Theta$. Furthermore, let $b,b' \in B$, $b \neq b'$, and set $\underline{b} = (b,\ldots,b)$, $\underline{b}' = (b',\ldots,b') \in B^n$. As $\mathcal{A}$ is isomorphic to $\mathcal{L}^n$ and $\mathrm{Aut}\mathcal{A}$ is doubly transitive, $\mathrm{Aut}\,\mathcal{L}^n$ is also doubly transitive. Therefore there exists a $\pi \in \mathrm{Aut}\,\mathcal{L}^n$ such that $a\pi = \underline{b}$ and $a'\pi = \underline{b}'$. Consequently $(\underline{b},\underline{b}') \in \Theta_\pi$. Viewing Θ_π as a subset of $B^n \times B^n$ we have that

$$(b_1,\dots,b_n,b_1,\dots,b_n) \in \Theta_\pi \quad \text{for all} \quad b_1,\dots,b_n \in B$$

(6.4) (reflexivity of Θ_π),

$$(b,\dots,b,b',\dots,b') \in \Theta_\pi, \text{ and } \Theta_\pi \neq B^n \times B^n.$$

On the other hand, Θ_π is a subuniverse of $\overline{\mathscr{L}}^{2n}$ where $\overline{\mathscr{L}}$ is the algebra arising from $\mathscr{L}$ by adding the constants as basic operations. Since by (6.4) Θ_π fails to satisfy the condition required in Theorem 4.1(ii), we conclude that $\overline{\mathscr{L}}$ is not primal, that is, $\mathscr{L}$ is not functionally complete. Theorem 6.10 (or Exercise 6.3) implies then that $\mathscr{L}$ is affine with respect to an Abelian group $\underline{B}$. Hence $\mathscr{L}^n$ is affine with respect to $\underline{B}^n$. However, affineness is preserved by isomorphisms, so we get that $\mathcal{A}$ is also affine.

What remains to show is that if $\mathcal{A}$ is affine with respect to an Abelian group $\underline{A}$, then $\mathcal{A}$ is term equivalent to an affine space. Since $\mathcal{A}$ is idempotent, Proposition 2.6 yields that there is a subring R of End $\underline{A}$ such that $T(\mathcal{A}) = K({}_R\underline{A},\{(0,0)\})$, that is, $\mathcal{A}$ is term equivalent to the full idempotent reduct of ${}_R\underline{A}$. If $r \in R$, $r \neq 0,1$, then by Claim 1 the binary term operation $rx + (1-r)y$ of $\mathcal{A}$ is a quasigroup operation. Thus every element of $R - \{0\}$ is a permutation, that is an automorphism of $\underline{A}$. Since R is finite, it must be a field. Hence $\mathcal{A}$ is term equivalent to the affine space corresponding to ${}_R\underline{A}$.

(2) Suppose now that $\mathcal{A}$ is a majority algebra, and let f be a majority term operation of $\mathcal{A}$. Making use of Theorem 6.5 we prove that $\mathcal{A}$ is functionally complete. As was mentioned earlier, a majority operation alone satisfies conditions (a)-(c) in Theorem 6.5. Therefore, in view of Lemma 6.4, the only thing to be verified is the $1\frac{1}{2}$-interpolation property. For arbitrary distinct elements $a,b \in A$ put

$$C(a,b) = \{c \in A: \text{ there exists } g \in P^{(1)}(\mathcal{A}) \text{ such that } g(a) = a \text{ and } g(b) = c\}.$$

Clearly, $\mathcal{A}$ has the $1\frac{1}{2}$-interpolation property if and only if $C(a,b) = A$ for all $a,b \in A$, $a \neq b$. Let us call a nonvoid subset I of A an *ideal* of $\mathcal{A}$ iff $f(u_1,u_2,u_3) \in I$ whenever at least two of the elements $u_1,u_2,u_3 \in A$ belong to I. Obviously, the intersection of ideals of $\mathcal{A}$ is again an ideal provided it is not empty. Thus, for arbitrary elements $a,b \in A$ there exists a least ideal in $\mathcal{A}$ containing $\{a,b\}$, called the ideal generated by $\{a,b\}$. It will be denoted by $I(a,b)$. Observe that $C(a,b)$ is an ideal of $\mathcal{A}$ for all $a,b \in A$, $a \neq b$. Indeed, if, say, $u_1,u_2 \in C(a,b)$, that is $g_i(b) = u_i$ for some $g_i \in P^{(1)}(\mathcal{A})$ with $g_i(a) = a$ $(i = 1,2)$, then for $g(x) = f(g_1(x),g_2(x),u_3) \in P^{(1)}(\mathcal{A})$ we have $g(a) = a$ and $g(b) = f(u_1,u_2,u_3)$, implying that $f(u_1,u_2,u_3) \in C(a,b)$. Furthermore, choosing g the constant with value a or the identity, respectively, we get that $a,b \in C(a,b)$. Hence $I(a,b) \subseteq C(a,b)$.

The $1\frac{1}{2}$-interpolation property follows if we show that $I(a,b) = A$ for arbitrary distinct elements $a,b \in A$. Assume there exists an element $c \in A - I(a,b)$. Then $I(a,c) \neq I(a,b)$. However, since $\mathrm{Aut}\,\mathcal{A}$ is doubly transitive, the 2-generated ideals of $\mathcal{A}$ are of the same cardinality. Hence the ideal $I(a,b) \cap I(a,c)$ of $\mathcal{A}$ has at most one element, so that $I(a,b) \cap I(a,c) = \{a\}$. Similarly, $I(a,b) \cap I(b,c) = \{b\}$. Consequently

$$I(a,b) \cap I(a,c) \cap I(b,c) = \emptyset.$$

On the other hand, by definition,

$$f(a,b,c) \in I(a,b) \cap I(a,c) \cap I(b,c).$$

This contradiction proves that $I(a,b) = A$.

(3) Suppose finally that $\mathcal{A}$ has a k-ary $(k \geq 3)$, say first, semi-projection f among its term operations, which is not the first projection. Again we apply Theorem 6.5 to prove that $\mathcal{A}$ is functionally complete. Observe first that f alone forms a family satisfying conditions (a)-(c) in Theorem 6.5.

In fact, (a) and (b) are obvious. To verify (c) let $a,b \in A$, $a \neq b$. Since f is not the first projection, there exist elements $a_1,\ldots,a_k \in A$ such that $f(a_1,\ldots,a_k) \neq a_1$. Choosing now $\pi \in \mathrm{Aut}\,\mathcal{A}$ so that $a_1\pi = a$ and $f(a_1,\ldots,a_k)\pi = b$, we get that $f(a,a_2\pi,\ldots,a_k\pi) = b$.

By Theorem 6.5 and Lemma 6.4 it remains to show that $\mathcal{A}$ has the $1\frac{1}{2}$-interpolation property. For arbitrary distinct elements $a,b \in A$ define the sets $C(a,b)$ as in the previous case. In this context we introduce the concept of an ideal as follows: a nonvoid subset I of A is an *ideal* of $\mathcal{A}$ iff $f(u_1,u_2,\ldots,u_k) \in I$ holds for the elements $u_1,u_2,\ldots,u_k \in A$ whenever there exists an index $1 < i \leq k$ such that $u_1,u_i \in I$. Again, we denote by $I(a,b)$ the ideal of $\mathcal{A}$ generated by $\{a,b\}$ $(a,b \in A)$. Since $\mathrm{Aut}\,\mathcal{A}$ is doubly transitive, the 2-generated ideals of $\mathcal{A}$ have the same cardinality. Hence, if $a',b' \in I(a,b)$ and $a' \neq b'$, then $I(a',b') = I(a,b)$. Furthermore, for arbitrary elements $a,b,a',b' \in A$, if $I(a,b) \neq I(a',b')$, then $|I(a,b) \cap I(a',b')| \leq 1$.

Claim 2. For arbitrary elements $a_1,\ldots,a_k \in A$ we have $f(a_1,\ldots,a_k) = a_1$ unless $I(a_1,a_2) = \ldots = I(a_1,a_k)$.

Indeed, suppose that $I(a_1,a_2) \neq I(a_1,a_i)$ for some $2 < i \leq k$. Then $|I(a_1,a_2) \cap I(a_1,a_i)| \leq 1$, implying that $I(a_1,a_2) \cap I(a_1,a_i) = \{a_1\}$. However, by definition, $f(a_1,\ldots,a_k) \in I(a_1,a_2) \cap I(a_1,a_i)$.

As in the previous case, it follows that for arbitrary distinct elements $a,b \in A$ we have $a,b \in C(a,b)$. Furthermore, $C(a,b)$ is an ideal of $\mathcal{A}$, for if $u_1,u_2,\ldots,u_k \in A$ are such that $u_1,u_i \in C(a,b)$ $(1 < i \leq k)$, that is $g_1(b) = u_1$ and $g_2(b) = u_i$ for appropriate operations $g_1,g_2 \in P^{(1)}(\mathcal{A})$ with $g_1(a) = a$, $g_2(a) = a$, then for

$$g(x) = f(g_1(x),u_2,\ldots,u_{i-1},g_2(x),u_{i+1},\ldots,u_k) \in P^{(1)}(\mathcal{A})$$

we have $g(a) = a$ and $g(b) = f(u_1,u_2,\ldots,u_k)$, implying $f(u_1,u_2,\ldots,u_k) \in C(a,b)$.

Thus $I(a,b) \subseteq C(a,b)$.

To establish the $1\frac{1}{2}$-interpolation property, we have to show that $A - I(a,b) \subseteq C(a,b)$ also holds for arbitrary distinct elements $a,b \in A$. Let $c \in A - I(a,b)$. Clearly, a, b, c are pairwise distinct. As we proved above, condition (c) from Theorem 6.5 holds for the 1-element family $\{f\}$. Therefore there exist elements $v_2,\ldots,v_k \in A$ such that $f(b,v_2,\ldots,v_k) = c$. Since f is a semiprojection, the elements $v_2,\ldots,v_k$ are pairwise distinct. By Claim 2 we have $I(b,v_2) = \ldots = I(b,v_k)$. Thus any two of the elements $b,v_2,\ldots,v_k$ generate the same ideal of $\mathcal{A}$, which, by definition, contains $c = f(b,v_2,\ldots,v_k)$. In particular, it follows that $I(b,c) = I(v_2,v_3)$. We show that $I(a,v_2) \neq I(a,v_3)$. Suppose the contrary. Then $a \neq v_2,v_3$ and any two elements of the ideal $I(a,v_2) = I(a,v_3)$, in particular, any two of the elements a, v_2, v_3, b, generate the same ideal. This implies that $c \in I(a,b)$, contradicting our assumption on c. Thus $I(a,v_2) \neq I(a,v_3)$, which yields by Claim 2 that $f(a,v_2,\ldots,v_k) = a$. Hence for $g(x) = f(x,v_2,\ldots,v_k)$ we have $g(b) = c$ and $g(a) = a$, so that $c \in C(a,b)$. This completes the proof.

REMARK. The infinite version of Theorem 6.13 is not true. For example, if $0 < r < 1$ $(r \in \mathbf{R})$, then the (nontrivial) algebra $\mathcal{A}_r$ defined in Exercise 2.18 is a nonaffine idempotent reduct of the vector space ${}_{\mathbf{R}}\mathbf{R}$, hence Aut $\mathcal{A}_r$ $(\supseteq G({}_{\mathbf{R}}\mathbf{R}))$ is doubly transitive while $\mathcal{A}_r$ is neither locally functionally complete nor term equivalent to an affine space.

The question arises how far the transitivity degree of Aut $\mathcal{A}$ can be weakened so that we still have only a "few" functionally incomplete finite algebras with such automorphism groups. To make more precise what "few" should mean, it is natural to require that not all permutation groups of that degree of transitivity occur as automorphism groups of functionally incomplete algebras. Recall

that a permutation group G on A is said to be *primitive* iff the unary algebra $(A;G)$ is simple and $|G| > 1$ provided $|A| = 2$. One can easily see that primitivity is stronger than transitivity and weaker than double transitivity. It is not difficult to show that, if a permutation group G on a finite set A is not primitive, then there always exists a functionally incomplete algebra $\mathcal{A} = (A;F)$ with $\mathrm{Aut}\,\mathcal{A} = G$. Thus the widest class of finite symmetric algebras to be considered from the point of view of functional completeness is the class of finite algebras with primitive automorphism groups. The functionally incomplete members of this class are described in P. P. Pálfy, L. Szabó and Á. Szendrei [1982]. The proof makes use of Corollary 1.20. (A special case was settled earlier by J. Demetrovics, L. Hannák and L. Rónyai [1981].) Concerning infinite algebras, a slight improvement of Theorem 6.12 was found by L. Szabó [1983a].

Order functionally complete algebras

A finite lattice can never be functionally complete, as its polynomial operations preserve the natural order of the lattice. However, it may be "as complete as possible" in the sense that every operation on its base set preserving the natural order is a polynomial operation of the lattice. The infinite case, with local polynomial operations instead of polynomial operations, is similar. More generally, the same holds for arbitrary partially ordered algebras. For an algebra $\mathcal{A} = (A;F)$ and for a partial order $\leq$ on A we say that $\leq$ is a *compatible partial order* of $\mathcal{A}$, or $(A;F;\leq)$ is a *partially ordered algebra*, iff the basic operations (and hence all local polynomial operations) of $\mathcal{A}$ preserve $\leq$.

DEFINITION. Let $(A;F;\leq)$ be a partially ordered algebra. The algebra $(A;F)$ is called *order functionally complete* [*locally order functionally complete*] with respect to $\leq$, or the partially ordered algebra $(A;F;\leq)$ is called order functionally complete [resp. locally order functionally complete], iff every

operation on A preserving $\leq$ is a polynomial operation [resp. local polynomial operation] of $(A;F)$.

Clearly, for finite algebras order functional completeness is the same as local order functional completeness. However, let us mention in passing that, unlike with functional completeness, there is no obvious reason preventing an infinite, partially ordered algebra of finite type from being order functionally complete. For example, the following problem is still open.

PROBLEM. Does there exist an infinite, order functionally complete lattice?

E. Fried [a] proved that no countably infinite modular lattice can be order functionally complete.

Corollaries 1.24 and 1.25 can be applied to find some interesting examples of (locally) order functionally complete lattices.

EXAMPLES. 1. The 2-element lattice is order functionally complete;

2. for every natural number $n > 2$ the lattice M_n of height 2 with n atoms is order functionally complete;

3. for every infinite cardinal α the lattice M_α of height 2 with α atoms is locally order functionally complete.

Most investigations on (local) order functional completeness were done for majority algebras, in particular for lattices. As regards the partial orders to be considered, if we want a finite, order functionally complete algebra to have a large clone of polynomial operations, then it is natural to confine ourselves to bounded partial orders, because they are those determining maximal clones. The infinite counterpart of finite bounded partial order is the so-called locally bounded partial order: a partial order on a set A is termed *locally bounded* iff any two elements of A have an upper bound as well as a lower bound in A (that

is the partial order is directed and down directed simultaneously). The following proposition shows that with these restrictions we do not get very far from lattices.

PROPOSITION 6.14. *If* $(A;F;\leq)$ *is a partially ordered majority algebra such that* $\leq$ *is locally bounded, then* $\leq$ *is a lattice order, moreover, meet and join with respect to* $\leq$ *are local polynomial operations of* $(A;F)$.

PROOF. Let f be a majority term operation of $(A;F)$. Since $\leq$ is locally bounded, every nonvoid finite subset B of A has a lower bound a and an upper bound b $(a,b \in A,\ a \leq b)$. Thus B is contained in the interval $[a,b]$. We show that the polynomial operations $f(x,y,a)$, $f(x,y,b)$ of $(A;F)$ yield the greatest lower bound, resp. least upper bound of x, y for every $x,y \in [a,b]$. Indeed, $f(x,y,a)$ is a lower bound of $x,y \in [a,b]$, as $f(x,y,a) \leq f(x,y,x) = x$ and $f(x,y,a) \leq f(x,y,y) = y$. Furthermore, if $z \leq x,y$ $(z \in A)$, then $z = f(z,z,a) \leq f(x,y,a)$, therefore $f(x,y,a)$ is the greatest lower bound of $x,y \in [a,b]$. The proof for the least upper bound is similar. This fact implies on the one hand that $\leq$ is a lattice order (the special case $|B| = 2$ is enough for this purpose) and on the other hand that meet and join are local polynomial operations of $(A;F)$.

Thus, in the sequel, we consider lattice ordered majority algebras. In fact, Proposition 6.14 also shows that if we do not distinguish algebras with the same clone of local polynomial operations, as it is natural in studying local order functional completeness, then lattice ordered majority algebras are essentially lattices with some additional monotone operations.

In view of Corollary 1.24 the local polynomial operations of a lattice ordered majority algebra are determined by the reflexive subuniverses of the square of the algebra. A considerable improvement was found by H. J. Bandelt [1981a]

(cf. also D. Schweigert [1975] in the finite case), in which tolerances play an important role. For a set A, a reflexive, symmetric subset of A^2 is called a *tolerance* on A. In particular, Δ_A and ∇_A are tolerances on A; they are called *trivial tolerances*. Let $\mathcal{A} = (A;F)$ be an algebra. A tolerance B on A is said to be a *tolerance of the algebra* $\mathcal{A}$ iff the basic operations of $\mathcal{A}$ preserve B. Obviously, the congruences of $\mathcal{A}$ are tolerances of $\mathcal{A}$ as well.

PROPOSITION 6.15. *For a lattice ordered majority algebra* $\mathcal{A} = (A;F;\leq)$, *an operation on* A *is a local polynomial operation of* $\mathcal{A}$ *if and only if it preserves* $\leq$ *and the tolerances of* $\mathcal{A}$.

PROOF. Take an arbitrary reflexive subuniverse C of $\mathcal{A}^2$, and put

$$D_1 = C \cap \leq, \quad D_2 = C \cap \geq, \quad B_1 = D_1 \circ D_1^{\cup}, \quad B_2 = D_2 \circ D_2^{\cup}.$$

Clearly, D_i is reflexive, B_i is a tolerance of $\mathcal{A}$, and $D_i \subseteq B_i$ $(i = 1,2)$. We show that

$$C = (B_1 \cap \leq) \circ (B_2 \cap \geq). \tag{6.5}$$

We will make use of the fact that by Proposition 6.14, meet and join of the lattice $(A;\leq)$, denoted by $\wedge$, $\vee$, are local polynomial operations of $\mathcal{A}$, therefore they preserve C, $\leq$, D_i, B_i $(i = 1,2)$. Let $(x,y) \in C$. Then $(x,x\vee y) \in B_1 \cap \leq$, since $x \leq x \vee y$, $(x,x\vee y) = (x,x) \vee (x,y) \in C$, and hence $(x,x\vee y) \in D_1 \subseteq B_1 \cap \leq$. Similarly, $(x\vee y,y) \in B_2 \cap \geq$. Thus $(x,y) \in (B_1 \cap \leq) \circ (B_2 \cap \geq)$. Assume now that $(x,y) \in (B_1 \cap \leq) \circ (B_2 \cap \geq)$, that is there exist $u,v_1,v_2 \in A$ such that $x \leq u \leq v_1$, $(x,v_1) \in C$, $(u,v_1) \in C$ and $u \geq y \geq v_2$, $(u,v_2) \in C$, $(y,v_2) \in C$. Then $(x,u) = (x,v_1) \wedge (u,u) \in C$, $(u,y) = (u,v_2) \vee (y,y) \in C$, whence $(x,y) = (x,u) \wedge (u,y) \in C$. This concludes the proof of (6.5).

Clearly, if an operation on A preserves B_1, B_2 and $\leq$, then it preserves C. Thus every operation f on A preserving $\leq$ and the tolerances of

$\mathcal{A}$ preserves all reflexive subuniverses of $\mathcal{A}^2$, hence by Corollary 1.24 f is a local polynomial operation of $\mathcal{A}$. The converse is trivial.

This result immediately yields a criterion for the local order functional completeness of lattice ordered majority algebras. Let us call an algebra *tolerance free* iff it has no nontrivial tolerances.

COROLLARY 6.16. *A lattice ordered majority algebra is locally order functionally complete if and only if it is tolerance free.*

PROOF. The sufficiency of the condition follows from Proposition 6.15. To prove the necessity we have to verify that for arbitrary lattice $(A;\leq)$, the algebra $\mathcal{A} = (A;\mathrm{Pol}\{\leq\})$ is tolerance free. In fact, this is true also for every locally bounded partial order $\leq$. Consider a tolerance B of $\mathcal{A}$ such that $B \neq \Delta_A$, and let $(a,b) \in B$, $a \neq b$. It is easy to check that for arbitrary elements $u_1,u_2 \in A$ and for any upper bound v and lower bound w of u_1, u_2 the operation

$$f(x,y) = \begin{cases} v & \text{if } x \geq a,\ y \geq b,\ (x,y) \neq (a,b) \\ & \text{or } x \geq b,\ y \geq a,\ (x,y) \neq (b,a) \\ u_1 & \text{if } (x,y) = (a,b) \\ u_2 & \text{if } (x,y) = (b,a) \\ w & \text{otherwise} \end{cases} \qquad (x,y \in A)$$

belongs to $\mathrm{Pol}\{\leq\}$. Since $(a,b),(b,a) \in B$, we get that $(u_1,u_2) = f((a,b),(b,a)) \in B$. Thus $B = \nabla_A$, completing the proof.

For finite lattices this result was found by M. Kindermann [1979]. The infinite version is due to H. J. Bandelt [1981a]. D. Schweigert [a] (cf. also D. Schweigert, M. Szymańska [1983]) observed that tolerance freeness has strong implications on finite majority algebras even if they are not assumed to be lattice ordered. The corresponding result for infinite algebras was proved by

L. Szabó [1983].

PROPOSITION 6.17. *Every tolerance free majority algebra is either locally functionally complete, or locally order functionally complete with respect to a lattice order.*

PROOF. Let $\mathcal{A} = (A;F)$ be a tolerance free majority algebra and f a majority term operation of $\mathcal{A}$. Suppose $\mathcal{A}$ is not locally functionally complete. Then by Proposition 6.8 $\mathcal{A}^2$ has a reflexive subuniverse B such that $B \neq \Delta_A, \nabla_A$. Since $B \cap B^\smile$ $(\subset \nabla_A)$ and $B \circ B^\smile$, $B^\smile \circ B$ $(\supset \Delta_A)$ are tolerances of $\mathcal{A}$, we have $B \cap B^\smile = \Delta_A$ and $B \circ B^\smile = B^\smile \circ B = \nabla_A$. The first equality means that B is antisymmetric. We prove that B is transitive, too. Let $(a,b),(b,c) \in B$. Using $(a,c) \in \nabla_A = B \circ B^\smile$ select an element $u \in A$ so that $(a,u),(c,u) \in B$. Then

$$(c,f(u,b,c)) = f((c,u),(b,b),(c,c)) \in B$$

and

$$(f(u,b,c),c) = f((u,u),(b,c),(c,c)) \in B,$$

implying by the antisymmetry that $f(u,b,c) = c$. Hence

$$(a,c) = f((a,u),(a,b),(b,c)) \in B.$$

Thus B is a partial order on A. Now $B \circ B^\smile = B^\smile \circ B = \nabla_A$ implies that any two elements have an upper bound and a lower bound, hence B is locally bounded. In view of Proposition 6.14, B is a lattice order, and by Corollary 6.16 $\mathcal{A}$ is locally order functionally complete with respect to B.

It is not hard to see that for two lattice orders $\leq_1$ and $\leq_2$ on A the clones $\mathrm{Pol}\{\leq_1\}$ and $\mathrm{Pol}\{\leq_2\}$ coincide if and only if $\leq_1 = \leq_2$ or $\leq_1 = \geq_2$. Therefore in Proposition 6.17 the lattice order is uniquely determined up to dualization. This proposition also provides an improvement of the local functional completeness criterion in Proposition 6.8.

COROLLARY 6.18. *A majority algebra is locally functionally complete if and only if it is tolerance free and has no compatible lattice order.*

After this small detour we return to order functional completeness. R. Wille [1977] characterized finite, order functionally complete lattices in terms of certain join homomorphisms. His theorem was extended by B. A. Davey and I. Rival [1982] to finite lattices with additional monotone operations. As we remarked after Proposition 6.14, up to polynomial equivalence, the latter class of algebras is the same as the class of finite, lattice ordered majority algebras. We now look at how the join homomorphisms occurring in these characterizations are related to the tolerances of the algebra.

Let $\mathcal{A} = (A;F;\leq)$ be a finite, lattice ordered majority algebra. Meet, join, the greatest element, and the least element with respect to $\leq$ will be denoted by $\wedge$, $\vee$, 1 and 0, respectively. We know that $\wedge$ and $\vee$ are polynomial operations of $\mathcal{A}$. As in Chapter 3, a mapping $\varphi: A \to A$ is called *decreasing* [*increasing*] iff $x\varphi \leq x$ [$x\varphi \geq x$] for all $x \in A$. A decreasing [increasing] mapping $\varphi: A \to A$ is said to be *strictly decreasing* [*strictly increasing*] iff $x\varphi = x$ holds only if $x = 0$ [resp. $x = 1$].

For a set $B \subseteq A^2$ let φ_B denote the mapping

$$\varphi_B: A \to A, \quad x \mapsto \wedge\{y: (x,y) \in B\},$$

and for a mapping $\varphi: A \to A$ set

$$B_\varphi = \{(x,y) \in A^2: x\varphi \leq y \text{ and } y\varphi \leq x\}.$$

LEMMA 6.19. *For every finite, lattice ordered majority algebra* $\mathcal{A} = (A;F;\leq)$ *the mappings* $B \mapsto \varphi_B$ *and* $\varphi \mapsto B_\varphi$ *define mutually inverse bijections between the tolerances of* $\mathcal{A}$ *and the decreasing mappings* $\varphi: A \to A$ *such that for every basic operation* g *of* $\mathcal{A}$ *(say* g *is* n*-ary)*

(6.6) $\quad g(x_1,\ldots,x_n)\varphi \le g(x_1\varphi,\ldots,x_n\varphi)$ for all $x_1,\ldots,x_n \in A$.

REMARK. Let $\varphi\colon A \to A$ be a decreasing mapping. It is easy to check that if (6.6) holds for all basic operations of $\mathcal{A}$, then it holds for all polynomial operations as well. In particular, (6.6) for $\wedge$ shows that φ is monotone with respect to $\le$, and hence (6.6) for $\vee$ implies that φ is a join homomorphism.

PROOF of Lemma 6.19. Let B be a tolerance of $\mathcal{A}$. As B is closed under $\wedge$, φ_B assigns to every element x the least element y in A with $(x,y) \in B$. Thus φ_B is clearly decreasing, as $(x,x) \in B$. Furthermore, if g is an n-ary basic operation of $\mathcal{A}$ and $x_1,\ldots,x_n \in A$, then $(x_i, x_i\varphi_B) \in B$ for all $1 \le i \le n$, hence $(g(x_1,\ldots,x_n), g(x_1\varphi_B,\ldots,x_n\varphi_B)) \in B$, implying (6.6) for $\varphi = \varphi_B$. Now let φ be a decreasing mapping satisfying (6.6). Then B_φ is obviously reflexive and symmetric. If g is an n-ary basic operation of $\mathcal{A}$ and $(x_i,y_i) \in B_\varphi$ for all $1 \le i \le n$, then $x_i\varphi \le y_i$ and $y_i\varphi \le x_i$ for all $1 \le i \le n$. Hence

$$g(x_1,\ldots,x_n)\varphi \le g(x_1\varphi,\ldots,x_n\varphi) \le g(y_1,\ldots,y_n),$$

and symmetrically $g(y_1,\ldots,y_n)\varphi \le g(x_1,\ldots,x_n)$, which means that $(g(x_1,\ldots,x_n), g(y_1,\ldots,y_n)) \in B_\varphi$. Thus B_φ is a tolerance of $\mathcal{A}$.

To show that the mappings $B \mapsto \varphi_B$ and $\varphi \mapsto B_\varphi$ are inverse of each other, let first B be a tolerance of $\mathcal{A}$, and put $B' = B_{\varphi_B}$. The inclusion $B \subseteq B'$ is clear. If $(x,y) \in B'$, then $x\varphi_B \le y$ and $y\varphi_B \le x$, whence $(x,y) = (x,x\varphi_B) \vee (y\varphi_B,y) \in B$. Thus $B = B'$. Secondly, let $\varphi\colon A \to A$ be a decreasing mapping satisfying (6.6), and put $\varphi' = \varphi_{B_\varphi}$. Then for every $x \in A$ we have $x\varphi' = \wedge\{y\colon x\varphi \le y$ and $y\varphi \le x\}$. Obviously, $x\varphi \le x\varphi'$ for all $x \in A$. On the other hand, since $x\varphi$ is among the y's occurring on the right hand side, we get that $x\varphi' \le x\varphi$ also holds for every $x \in A$. Therefore $\varphi = \varphi'$, concluding the proof.

LEMMA 6.20. *Let* $\mathcal{A} = (A;F;\leq)$ *be a finite, lattice ordered majority algebra. For a tolerance* B *of* $\mathcal{A}$ *the following conditions are equivalent:*

(i) *the transitive closure of* B *is* ∇_A;

(ii) *there exist elements* $0 = a_0 \leq a_1 \leq \ldots \leq a_k = 1$ *in* A *such that* $(a_i,a_{i+1}) \in B$ *for all* $0 \leq i < k$;

(iii) φ_B *is strictly decreasing.*

PROOF. If (i) holds, then there exist elements $0 = b_0,b_1,\ldots,b_k = 1$ in A such that $(b_j,b_{j+1}) \in B$ for all $0 \leq j < k$. Then

$$(b_0 \vee \ldots \vee b_j, b_0 \vee \ldots \vee b_j \vee b_{j+1}) = (b_0 \vee \ldots \vee b_j, b_0 \vee \ldots \vee b_j) \vee (b_j,b_{j+1}) \in B$$

for all $0 \leq j < k$, therefore

$$0 = b_0 \leq b_0 \vee b_1 \leq \ldots \leq b_0 \vee \ldots \vee b_{k-1} \leq b_0 \vee \ldots \vee b_k = 1$$

is a sequence required in (ii). Assume now that (ii) holds, and consider arbitrary element $x \in A - \{0\}$. Again, in the sequence

$$0 = a_0 \wedge x \leq a_1 \wedge x \leq \ldots \leq a_k \wedge x = x$$

every pair of consecutive members belongs to B. Hence for the greatest index $0 \leq i \leq k$ such that $a_i \wedge x \neq x$ we have $(x,a_i \wedge x) \in B$ and $x > a_i \wedge x$. Thus $x\varphi_B \leq a_i \wedge x < x$, implying (iii). Finally, if (iii) holds, then the sequence

$$1 > 1\varphi_B > 1\varphi_B^2 > \ldots$$

reaches 0 in a finite number of steps. Furthermore, $(1\varphi_B^i, 1\varphi_B^{i+1}) \in B_{\varphi_B} = B$ for all $i \geq 0$. Thus the pair (0,1) belongs to the transitive closure of B. However, the latter is a congruence of $\mathcal{A}$, therefore equals ∇_A, as stated in (i).

Lemmas 6.19 and 6.20, combined with Corollary 6.16, yield some nice characterizations of finite, order functionally complete majority algebras.

THEOREM 6.21. *For a finite, lattice ordered majority algebra*

$\mathcal{A} = (A;F;\leq)$ *the following conditions are equivalent:*

(i) $\mathcal{A}$ *is order functionally complete;*

(ii) $\mathcal{A}$ *is tolerance free;*

(iii) *the identity and the constant* 0 *are the only decreasing mappings* $\varphi: A \to A$ *satisfying* (6.6) *for all basic operations* g *of* $\mathcal{A}$*;*

(iii)' *the identity and the constant* 1 *are the only increasing mappings* $\psi: A \to A$ *such that for every basic operation* g *of* $\mathcal{A}$ *(say* g *is* n*-ary)*

$$(6.6)' \qquad g(x_1,\ldots,x_n)\psi \geq g(x_1\psi,\ldots,x_n\psi) \quad \text{for all } x_1,\ldots,x_n \in A;$$

(iv) $\mathcal{A}$ *is simple and the constant* 0 *is the only strictly decreasing mapping* $\varphi: A \to A$ *satisfying* (6.6) *for all basic operations* g *of* $\mathcal{A}$*;*

(iv)' $\mathcal{A}$ *is simple and the constant* 1 *is the only strictly increasing mapping* $\psi: A \to A$ *satisfying* (6.6)' *for all basic operations* g *of* $\mathcal{A}$.

PROOF. The equivalence of (i) and (ii) is established in Corollary 6.16. The equivalence of (ii) and (iii) follows from Lemma 6.19, as the mappings φ_B corresponding to $B = \Delta_A, \nabla_A$ are exactly the identity and the constant 0, respectively. Clearly, (ii) and (iii) imply (iv). Suppose now that (iv) holds, and let $B \neq \Delta_A$ be a tolerance of $\mathcal{A}$. The transitive closure of B equals ∇_A, as it is a congruence of $\mathcal{A}$ and $\mathcal{A}$ is simple. Therefore, by Lemmas 6.19 and 6.20, φ_B is a strictly decreasing mapping satisfying (6.6). Our assumption implies that φ_B is the constant 0, that is, $B = \nabla_A$. Hence (ii) holds. Thus (i) $\Longleftrightarrow$ (ii) $\Longleftrightarrow$ (iii) $\Longleftrightarrow$ (iv).

The conditions (iii)' and (iv)' are dual to (iii) and (iv), respectively, that is, (iii)' for $(A;F;\leq)$ is the same as condition (iii) for the algebra $(A;F;\geq)$, and similarly with (iv)' and (iv). Since (i) and (ii) are self-dual, that is, $(A;F;\leq)$ satisfies (i), resp. (ii), if and only if $(A;F;\geq)$ does, therefore the equivalences (i) $\Longleftrightarrow$ (ii) $\Longleftrightarrow$ (iii)' $\Longleftrightarrow$ (iv)' also follow.

The characterization (iii) above is the result of B. A. Davey and I. Rival [1982] mentioned earlier. By the remark after Lemma 6.19, Theorem 6.21 specializes for lattices as follows.

COROLLARY 6.22. *For a finite lattice* L *the following conditions are equivalent:*

(i) L *is order functionally complete;*

(ii) L *is tolerance free;*

(iii) *the identity and the constant* 0 *are the only decreasing join endomorphisms of* L*;*

(iii)' *the identity and the constant* 1 *are the only increasing meet endomorphisms of* L*;*

(iv) L *is simple and the constant* 0 *is the only strictly decreasing join endomorphism of* L*;*

(iv)' L *is simple and the constant* 1 *is the only strictly increasing meet endomorphism of* L.

Characterization (iii) and the corollary below, which is an immediate consequence of (iv) and (iv)', are due to R. Wille [1977].

COROLLARY 6.23. *Every finite simple lattice* L *in which*

(a) *the join of atoms is* 1, *or*

(b) *the meet of coatoms is* 0

is order functionally complete.

Recall that precisely those lattices satisfying the equivalent conditions of Corollary 6.22 occurred in Theorem 3.5. For more details on the connection between the tolerances of L and Theorem 3.5 the reader is referred to D. Hobby and R. McKenzie [a]. Lemma 6.20, which paves the way to characterization (iv) for finite, order functionally complete lattices, also comes from this paper.

It follows from Corollary 6.23 that every finite, simple, complemented lattice is order functionally complete. R. Wille [1977] proved that for finite modular lattices the converse also holds. We state his result without proof.

COROLLARY 6.24. *A finite modular lattice is order functionally complete if and only if it is simple and complemented.*

A part of the above results on finite algebras can be extended to infinite algebras. For example, infinite versions of Corollary 6.24 can be found in D. Schweigert [1981] and E. Fried [a]. Various extensions of Lemma 6.19 to infinite lattices are discussed by H. J. Bandelt [1981b] and I. G. Rosenberg, D. Schweigert [1984]. The latter is a survey paper containing an extensive bibliography on the topic.

Further characterizations of (local) order functional completeness, including some improvements of Corollary 6.16, can be found in the papers H. J. Bandelt [1981a], B. A. Davey and I. Rival [1982], I. G. Rosenberg, D. Schweigert [1984]. Recently, K. Denecke and L. Szabó [a] considered order primality for finite majority algebras without proper subalgebras, and proved a generalization of Proposition 6.17, which was extended by L. Szabó [1985] to infinite algebras as well.

REFERENCES

[BS] S. Burris, H.P. Sankappanavar

A Course in Universal Algebra, Graduate Texts in Mathematics, vol. 78, Springer-Verlag, Berlin - Heidelberg - New York, 1981.

[G] G. Grätzer

Universal Algebra, 2nd ed., Springer-Verlag, Berlin - Heidelberg - New York, 1979.

[MMPT] R. McKenzie, G.F. McNulty, D. Pigozzi, W. Taylor

Universal Algebra, in print.

[PK] R. Pöschel, L.A. Kalužnin

Funktionen- und Relationenalgebren. Ein Kapitel der diskreten Mathematik, VEB Deutscher Verlag der Wissenschaften, Berlin, 1979.

J. Bagyinszki, J. Demetrovics

[1982] The lattice of linear classes in prime valued logics, in: *Discrete Mathematics, Banach Center Publ.*, vol. 7, Warsaw; pp. 105-123.

K.A. Baker, A.F. Pixley

[1975] Polynomial interpolation and the chinese remainder theorem for algebraic systems, *Math. Z.* 143, 165-174.

H.J. Bandelt

[1981a] Local polynomial functions on lattices, *Houston J. Math.* 7, 317-325.

[1981b] Tolerance relations on lattices, *Bull. Austral. Math. Soc.* 23, 367-381.

J. Berman

[1980] A proof of Lyndon's finite basis theorem, *Discrete Math.* 29, 229-233.

J. Berman, R. McKenzie

[1984] Clones satisfying the term condition, *Discrete Math.* 52, 7-29.

V.G. Bodnarchuk, L.A. Kaluzhnin, V.N. Kotov, B.A. Romov

[1969] Galois theory for Post algebras I-II(Russian), *Kibernetika* 3, 1-10; 5, 1-9.

G.A. Burle

[1967] The classes of k-valued logics containing all one-variable functions (Russian), *Diskret. Analiz* 10, 3-7.

D.M. Clark, P.H. Krauss

[1976] Para primal algebras, *Algebra Universalis* 6, 165-192.

[1980] Plain para primal algebras, *Algebra Universalis* 11, 365-388.

B. Csákány

[1980] Homogeneous algebras are functionally complete, *Algebra Universalis* 11, 149-158.

[1983a] Three-element groupoids with minimal clones, *Acta Sci. Math. (Szeged)* 45, 111-117.

[1983b] All minimal clones on the three-element set, *Acta Cybernet.* 6, 227-238.

B. Csákány, T. Gavalcová

[1980] Finite homogeneous algebras. I, *Acta Sci. Math. (Szeged)* 42, 57-65.

G. Czédli, J.D.H. Smith

[1981] On the uniqueness of Mal'cev polynomials, in: *Finite Algebra and Multiple-Valued Logic* (Proc. Conf. Szeged, 1979), Colloq. Math. Soc. J. Bolyai, vol. 28, North-Holland, Amsterdam; pp. 127-145.

B.A. Davey, I. Rival

[1982] Exponents of lattice-ordered algebras, *Algebra Universalis* 14, 87-98.

J. Demetrovics, L. Hannák, L. Rónyai

[1981] Almost all prime-element algebras with transitive automorphism groups are functionally complete, in: *Finite Algebra and Multiple-Valued Logic* (Proc. Conf. Szeged, 1979), Colloq. Math. Soc. J. Bolyai, vol. 28, North-Holland, Amsterdam; pp. 191-201.

J. Demetrovics, I.A. Mal'tsev

[a] Essentially minimal TC-clones on three-element base set, preprint, 1985.

K. Denecke, L. Szabó

[a] Characterization of tolerance-free algebras having majority term functions and admitting no proper subalgebras, in: *Lectures in Universal Algebra* (Proc. Conf. Szeged, 1983), Colloq. Math. Soc. J. Bolyai, vol. 43, North-Holland, Amsterdam; to appear.

S. Fajtlowicz, J. Mycielski

[1974] On convex linear forms, *Algebra Universalis* 4, 244-249.

W. Feit

[1983] An interval in the subgroup lattice of a finite group which is isomorphic to M_7, *Algebra Universalis* 17, 220-221.

A.L. Foster

[1953] Generalized "Boolean" theory of universal algebras. II: Identities and subdirect sums in functionally complete algebras, *Math. Z.* 59, 191-199.

A.L. Foster, A.F. Pixley

[1964] Semi-categorical algebras. I. Semi-primal algebras, *Math. Z.* 83, 147-169.

R.S. Freese, R.N. McKenzie

[a] The commutator, an overview, preprint.

E. Fried

[a] Interpolation in modular lattices, preprint, 1985.

E. Fried, H.K. Kaiser, L. Márki

[1982] An elementary approach to polynomial interpolation in universal algebras, *Algebra Universalis* 15, 40-57.

E. Fried, A.F. Pixley

[1979] The dual discriminator function in universal algebra, *Acta Sci. Math. (Szeged)* 41, 83-100.

D. Geiger

[1968] Closed systems of functions and predicates, *Pacific J. Math.* 27, 95-100.

G. Grätzer, E.T. Schmidt

[1963] Characterizations of congruence lattices of abstract algebras, *Acta Sci. Math. (Szeged)* 24, 34-59.

H.P. Gumm

[1979] Algebras in congruence permutable varieties: Geometrical properties of affine algebras, *Algebra Universalis* 9, 8-34.

[1980] An easy way to the commutator in modular varieties, *Arch. Math. (Basel)* 34, 220-228.

C. Herrmann

[1979] Affine algebras in congruence modular varieties, *Acta Sci. Math. (Szeged)* 41, 119-125.

D. Hobby

[1984] *Algebras Derived From Minimal Congruences*, Ph.D. Thesis, University of California, Berkeley.

D. Hobby, R. McKenzie

[a] The structure of finite algebras, in preparation.

Th. Ihringer

[1984a] On finite algebras having a linear congruence class geometry, *Algebra Universalis* 19, 1-10.

[1984b] A property of finite algebras having M_n's as congruence lattices, *Algebra Universalis* 19, 269-271.

N. Jacobson

[1956] *Structure of Rings*, Coll. Publ., vol. 37, Amer. Math. Soc., Providence, R.I.

B. Jónsson

[1967] Algebras whose congruence lattices are distributive, *Math. Scand.* 21, 110-121.

H.K. Kaiser

[1975a] Über lokal polynomvollständige universale Algebren, *Abh. Math. Sem. Univ. Hamburg* 43, 158-165.

[1975b] A class of locally complete universal algebras, *J. London Math. Soc.* 9, 5-8.

H.K. Kaiser, L. Márki

[1980] Remarks on a paper of L. Szabó and Á. Szendrei, *Acta Sci. Math. (Szeged)* 42, 95-98.

M. Kindermann

[1979] Über die Äquivalenz von Ordnungspolynomvollständigkeit und Toleranzeinfachheit endlicher Verbände, in: *Contributions to General Algebra* (Proc. Conf. Klagenfurt, 1978), Verlag J. Heyn; pp. 145-149.

E.W. Kiss

[1984] Term functions and subalgebras, *Acta Sci. Math. (Szeged)* 47, 303-306.

P. Köhler

[1983] M_7 as an interval in a subgroup lattice, *Algebra Universalis* 17, 263-266.

P.H. Krauss

[1972] On primal algebras, *Algebra Universalis* 2, 62-67.

[1973] On quasi primal algebras, *Math. Z.* 134, 85-89.

D. Lau

[1978] Über die Anzahl von abgeschlossenen Mengen linearer Funktionen der n-wertigen Logik, *Elektron. Informationsverarb. Kybernet.* 14, 567-569.

[a] Über abgeschlossene Mengen linearer Funktionen von P_k, I, preprint, WPU Rostock, 1983.

R.C. Lyndon

[1951] Identities in two-valued calculi, *Trans. Amer. Math. Soc.* 71, 457-465.

A.I. Mal'tsev

[1954] On the general theory of algebraic systems (Russian), *Mat. Sb.* (77) 35, 3-20.

I.A. Mal'tsev

[1973] Certain properties of the cells of Post algebras (Russian), *Diskret. Analiz* 23, 24-31.

S.S. Marchenkov

[1979] On closed classes of selfdual functions of multiple-valued logic (Russian), *Problemy Kibernetiki* 36, 5-22.

[1982a] Homogeneous algebras (Russian), *Problemy Kibernetiki* 39, 85-106.

[1982b] On the classification of algebras whose automorphism group is the alternating group (Russian), *Dokl. Akad. Nauk SSSR* 265, 533-536.

E. Marczewski

[1964] Homogeneous algebras and homogeneous operations, *Fund. Math.* 56, 81-103.

W.D. Maurer, J.L. Rhodes

[1965] A property of finite simple nonabelian groups, *Proc. Amer. Math. Soc.* 16, 552-554.

R. McKenzie

[1976] On minimal, locally finite varieties with permuting congruence relations, preprint.

[1982] Narrowness implies uniformity, *Algebra Universalis* 15, 67-85.

[1983] Finite forbidden lattices, in: *Universal Algebra and Lattice Theory* (Proc. Conf. Puebla, 1982), Lecture Notes in Math. 1004, Springer-Verlag; pp. 176-205.

[a] Tame congruences, in: *Lectures in Universal Algebra* (Proc. Conf. Szeged, 1983), Colloq. Math. Soc. J. Bolyai, vol. 43, North-Holland, Amsterdam; to appear.

P.P. Pálfy

[1984] Unary polynomials in algebras. I, *Algebra Universalis* 18, 262-273.

[a] On Feit's examples of intervals in subgroup lattices, preprint, 1985.

P.P. Pálfy, P. Pudlák

[1980] Congruence lattices of finite algebras and intervals in subgroup lattices of finite groups, *Algebra Universalis* 11, 22-27.

P.P. Pálfy, L. Szabó, Á. Szendrei

[1981] Algebras with doubly transitive automorphism groups, in: *Finite Algebra and Multiple-Valued Logic* (Proc. Conf. Szeged, 1979), Colloq. Math. Soc. J. Bolyai, vol. 28, North-Holland, Amsterdam; pp. 521-535.

[1982] Automorphism groups and functional completeness, *Algebra Universalis* 15, 385-400.

P.P. Pálfy, Á. Szendrei

[1983] Unary polynomials in algebras. II, in: *Contributions to General Algebra 2* (Proc. Conf. Klagenfurt, 1982), Verlag Hölder-Pichler-Tempsky, Wien, Verlag Teubner, Stuttgart; pp. 273-290.

A.F. Pixley

[1963] Distributivity and permutability of congruence relations in equational classes of algebras, *Proc. Amer. Math. Soc.* 14, 105-109.

[1970] Functionally complete algebras generating distributive and permutable classes, *Math. Z.* 114, 361-372.

[1971] The ternary discriminator function in universal algebra, *Math. Ann.* 191, 167-180.

R. Pöschel

[1979] Concrete representation of algebraic structures and general Galois theory, in: *Contributions to General Algebra* (Proc. Conf. Klagenfurt, 1978), Verlag J. Heyn, Klagenfurt; pp. 249-272.

E.L. Post

[1921] Introduction to a general theory of elementary propositions, *Amer. J. Math.* 43, 163-185.

[1941] *The Two-Valued Iterative Systems of Mathematical Logic*, Ann. Math. Studies 5, Princeton University Press, Princeton, N.J.

P. Pudlák

[1976] A new proof of the congruence lattice representation theorem, *Algebra Universalis* 6, 269-275.

R.W. Quackenbush

[1981] A new proof of Rosenberg's primal algebra characterization theorem, in: *Finite Algebra and Multiple-Valued Logic* (Proc. Conf. Szeged, 1979), Colloq. Math. Soc. J. Bolyai, vol. 28, North-Holland, Amsterdam; pp. 603-634.

[1983] Minimal para primal algebras, in: *Contributions to General Algebra 2* (Proc. Conf. Klagenfurt, 1982), Verlag Hölder-Pichler-Tempsky, Wien, Verlag Teubner, Stuttgart; pp. 291-304.

[a] Quasi-affine algebras, preprint, 1984.

L. Rédei, T. Szele

[1947] Algebraisch-zahlentheoretische Betrachtungen über Ringe. I, *Acta Math.* 79, 291-320.

B.A. Romov

[1977] The Galois connection between the iterative Post algebras and relations on an infinite set, *Kibernetika (Kiev)* 3, 62-64.

I.G. Rosenberg

[1965] La structure des fonctions de plusieurs variables sur un ensemble fini, *C.R. Acad. Sci. Paris, Ser. A.B.* 260, 3817-3819.

[1970] Über die funktionale Vollständigkeit in den mehrwertigen Logiken (Struktur der Funktionen von mehreren Veränderlichen auf endlichen Mengen), *Rozpravy Československe Akad. Věd. Řada Mat. Přírod. Věd.* 80, 3-93.

[1972] Classification of universal algebras by infinitary relations, *Algebra Universalis* 1, 350-354.

[1976] The set of maximal closed classes of operations on an infinite set A has cardinality $2^{2^{|A|}}$, *Arch. Math. (Basel)* 27, 561-568.

[a] Minimal clones I: The five types, in: *Lectures in Universal Algebra* (Proc. Conf. Szeged, 1983), Colloq. Math. Soc. J. Bolyai, vol. 43, North-Holland, Amsterdam; to appear.

I.G. Rosenberg, D. Schweigert

[1982] Compatible orderings and tolerances of lattices, in: *Orders: Description and Roles* (Proc. Conf. Ordered Sets and Their Applications, Château de la Tourette, 1982), Annals of Discrete Math., vol. 23, North-Holland, Amsterdam; pp. 119-150.

I.G. Rosenberg, L. Szabó

[1984] Local completeness I, *Algebra Universalis* 18, 308-326.

A.A. Salomaa

[1964] On infinitely generated sets of operations in finite algebras, *Ann. Univ. Turku., Ser. A I* 74, 1-12.

D. Schweigert

[1975] Some remarks on polarity lattices and on ortholattices, in: *Proceedings of the Lattice Theory Conference* (Ulm, 1975); pp. 254-256.

[1978] On order-polynomially complete algebras, *Notices Amer. Math. Soc.* 25, p. A-582, Abstract 78T-206.

[1981] Compatible relations of modular and orthomodular lattices, *Proc. Amer. Math. Soc.* 81, 462-464.

D. Schweigert, M. Szymańska

[1983] Polynomial functions of correlation lattices, *Algebra Universalis* 16, 355-359.

J.D.H. Smith

[1976] *Mal'cev Varieties*, Lecture Notes in Math. 554, Springer-Verlag, Berlin.

S. Swierczkowski

[1960-1961] Algebras which are independently generated by every n elements, *Fund. Math.* 49, 93-104.

L. Szabó

[1978] Concrete representation of related structures of universal algebras. I, *Acta Sci. Math. (Szeged)* 40, 175-184.

[1983a] Interpolation in algebras with doubly primitive automorphism groups, *Elektron. Informationsverarb. Kybernet.* 19, 603-610.

[1983b] Tolerance-free algebras with a majority function, in: *Contributions to General Algebra 2* (Proc. Conf. Klagenfurt, 1982), Verlag Hölder-Pichler-Tempsky, Wien, Verlag Teubner, Stuttgart; pp. 359-364.

[1985] Tolerance-free infinite algebras having majority term functions and no proper subalgebras, in: *Contributions to General Algebra 3* (Proc. Conf. Vienna, 1984), Verlag Hölder-Pichler-Tempsky, Wien, Verlag Teubner, Stuttgart; pp. 355-363.

L. Szabó, Á. Szendrei

[1979] Almost all algebras with triply transitive automorphism groups are functionally complete, *Acta Sci. Math. (Szeged)* 41, 391-402.

[1981] Słupecki-type criteria for quasilinear functions over a finite dimensional vector space, *Elektron. Informationsverarb. Kybernet.* 17, 601-611.

Á. Szendrei

[1980] On closed classes of quasilinear functions, *Czechoslovak Math. J.* 30 (105), 498-509.

[1981a] Identities in idempotent affine algebras, *Algebra Universalis* 12, 172-199.

[1981b] Clones of linear operations on finite sets, in: *Finite Algebra and Multiple-Valued Logic* (Proc. Conf. Szeged, 1979), Colloq. Math. Soc. J. Bolyai, vol. 28, North-Holland, Amsterdam; pp. 693-738.

[1982a] On the idempotent reducts of modules. I-II, in: *Universal Algebra* (Proc. Conf. Esztergom, 1977), Colloq. Math. Soc. J. Bolyai, vol. 29, North-Holland, Amsterdam; pp. 753-780.

[1982b] Algebras of prime cardinality with a cyclic automorphism, *Arch. Math. (Basel)* 39, 417-427.

W. Taylor

[1982] Some applications of the term condition, *Algebra Universalis* 14, 11-25.

D. Webb

[1935] Generation of an n-valued logic by one binary operator, *Proc. Nat. Acad. Sci.* 21, 252-254.

H. Werner

[1970] Eine Charakterisierung funktional vollständiger Algebren, *Arch. Math. (Basel)* 21, 381-385.

[1974] Congruences on products of algebras, *Algebra Universalis* 4, 99-105.

R. Wille

[1977] Eine Charakterisierung endlicher, ordnungspolynomvollständiger Verbände, *Arch. Math. (Basel)* 28, 557-560.

S.V. Yablonskiĭ

[1958] Functional constructions in k-valued logic (Russian), *Trudy Mat. Inst. Steklov* 51, 5-142.

Yu. I. Yanov, A.A. Muchnik

[1959] On the existence of k-valued closed classes without a finite basis (Russian), *Dokl. Akad. Nauk SSSR* 127, 44-46.

LES PRESSES DE L'UNIVERSITÉ DE MONTRÉAL
C.P. 6128, succ. «A», Qué., Canada H3C 3J7

EXTRAIT DU CATALOGUE

Mathématiques

COLLECTION «SÉMINAIRE DE MATHÉMATIQUES SUPÉRIEURES»

1. **Problèmes aux limites dans les équations aux dérivées partielles.** Jacques L. LIONS
2. **Théorie des algèbres de Banach et des algèbres localement convexes.** Lucien WAELBROECK
3. **Introduction à l'algèbre homologique.** Jean-Marie MARANDA
4. **Séries de Fourier aléatoires.** Jean-Pierre KAHANE
5. **Quelques aspects de la théorie des entiers algébriques.** Charles PISOT
6. **Théorie des modèles en logique mathématique.** Aubert DAIGNEAULT
7. **Promenades aléatoires et mouvements brownien.** Anatole JOFFE
8. **Fondements de la géométrie algébrique moderne.** Jean DIEUDONNÉ
9. **Théorie des valuations.** Paulo RIBENBOIM
10. **Catégories non abéliennes.** Peter HILTON, Tudor GANEA, Heinrich KLEISLI, Jean-Marie MARANDA, Howard OSBORN
11. **Homotopie et cohomologie.** Beno ECKMANN
12. **Intégration dans les groupes topologiques.** Geoffrey FOX
13. **Unicité et convexité dans les problèmes différentiels.** Shmuel AGMON
14. **Axiomatique des fonctions harmoniques.** Marcel BRELOT
15. **Problèmes non linéaires.** Félix E. BROWDER
16. **Équations elliptiques du second ordre à coefficients discontinus.** Guido STAMPACCHIA
17. **Problèmes aux limites non homogènes.** José BARROS-NETO
18. **Équations différentielles abstraites.** Samuel ZAIDMAN
19. **Équations aux dérivées partielles.** Robert CARROL, George F.D. DUFF, Jöran FRIBERG, Jules GOBERT, Pierre GRISVARD, Jindrich NECAS et Robert SEELEY
20. **L'Algèbre logique et ses rapports avec la théorie des relations.** Roland FRAÏSSÉ
21. **Logical Systems Containing Only a Finite Number of Symbols.** Leon HENKIN
24. **Représentabilité et définissabilité dans les algèbres transformationnelles et dans les algèbres polyadiques.** Léon LEBLANC
25. **Modèles transitifs de la théorie des ensembles de Zermelo-Fraenkel.** Andrzej MOSTOWSKI
26. **Théorie de l'approximation des fonctions d'une variable complexe.** Wolfgang H.J. FUCHS
27. **Les Fonctions multivalentes.** Walter K. HAYMAN
28. **Fonctionnelles analytiques et fonctions entières (n variables).** Pierre LELONG
29. **Applications of Functional Analysis to Extremal Problems for Polynomials.** Qazi Ibadur RAHMAN
30. **Topics in Complex Manifolds.** Hugo ROSSI
31. **Théorie de l'inférence statistique robuste.** Peter J. HUBER
32. **Aspects probabilistes de la théorie du potentiel.** Mark KAC
33. **Théorie asymptotique de la décision statistique.** Lucien M. LECAM
34. **Processus aléatoires gaussiens.** Jacques NEVEU
35. **Nonparametric Estimation.** Constance van EEDEN
36. **K-Théorie.** Max KAROUBI
37. **Differential Complexes.** Joseph J. KOHN
38. **Variétés hilbertiennes : aspects géométriques.** Nicolaas H. KUIPER
39. **Deformations of Compact Complex Manifold.** Masatake KURANISHI
40. **Grauert's Theorem of Direct Images of Coherent Sheaves.** Raghavan NARASIMHAN
41. **Systems of Linear Partial Differential Equations and Deformation of Pseudogroup Structures.** A. KUMPERA et D.C. SPENCER
42. **Analyse globale.** P. LIBERMANN, K.D. ELWORTHY, N. MOULIS, K.K. MUKHERJEA, N. PRAKASH, G. LUSZTIC et W. SHIH
43. **Algebraic Space Curves.** Sheeram S. ABHYANKAR
44. **Théorèmes de représentabilité pour les espaces algébriques.** Michael ARTIN
45. **Groupes de Barsotti-Tate et cristaux de Dieudonné.** Alexandre GROTHENDIECK
46. **On Flat Extensions of a Ring.** Massayoshi NAGATA
47. **Introduction à la théorie des sites et son application à la construction des préschémas quotients.** Masayoshi MIYANISHI
48. **Méthodes logiques en géométrie diophantienne.** Shuichi TAKAHASHI
49. **Index Theorems of Atiyah — Bott — Patodi and Curvature Invariants.** Ravindra S. KULKARNI
50. **Numerical Methods in Statistical Hydrodynamics.** Alexandre CHORIN
51. **Introduction à la théorie des hypergraphes.** Claude BERGE
52. **Automath, a Language for Mathematics.** Nicolaas G. DE BRUIJN
53. **Logique des topos (Introduction à la théorie des topos élémentaires).** Dana SCHLOMIUK
54. **La Série génératrice exponentielle dans les problèmes d'énumération.** Dominique FOATA
55. **Feuilletages : résultats anciens et nouveaux (Painlevé, Hector et Martinet).** Georges H. REEB

56. **Finite Embedding Theorems for Partial Designs and Algebras.** Charles C. LINDNER et Trevor EVANS
57. **Minimal Varieties in Real and Complex Geometry.** H. Blaine LAWSON, Jr
58. **La Théorie des points fixes et ses applications à l'analyse.** Kazimierz GEBA, Karol BORSUK, Andrzej JANKOWSKI et Edward ZHENDER
59. **Numerical Analysis of the Finite Element Method,** Philippe G. CIARLET
60. **Méthodes numériques en mathématiques appliquées.** J.F. Giles AUCHMUTY, Michel CROUZEIX, Pierre JAMET, Colette LEBAUD, Pierre LESAINT et Bertrand MERCIER
61. **Analyse numérique matricielle.** Paul ARMINJON
62. **Problèmes d'optimisation en calcul des probabilités.** Serge DUBUC
63. **Chaînes de Markov sur les permutations.** Gérard LETAC
64. **Géométrie différentielle stochastique.** Paul MALLIAVIN
65. **Numerical Methods for Solving Time-Dependent Problems for Partial Differential Equations.** Heinz-Otto KREISS
66. **Difference Sets in Elementary Abelian Groups.** Paul CAMION
67. **Groups in Physics : Collective Model of the Nucleus; Canonical Transformation in Quantum Mechanics.** Marcos MOSHINSKY
68. **Points fixes pour les applications compactes : espaces de Lefschetz et la théorie de l'indice.** Andrzej GRANAS
69. **Set Theoretic Methods in Homological Algebra and Abelian Groups.** Paul EKLOF
70. **Abelian p-Groups and Mixed Groups.** Laszlo FUCHS
71. **Integral Representations and Structure of Finite Group Rings.** Klaus W. ROGGENKAMP
72. **Homological Invariants of Modules over Commutative Rings.** Paul ROBERTS
73. **Representations of Valued Graphs.** Vlastimil DLAB
74. **Groupes abéliens sans torsion.** Khalid BENABDALLAH
75. **Lie Groups, Lie Algebras and Representation Theory.** Hans ZASSENHAUS
76. **Birational Geometry for Open Varieties.** Shigeru IITAKA
77. **Lectures on Hilbert Modular Surfaces.** Friedrich HIRZEBRUCH, Gerard van der GEER
78. **Complex Geometry in Mathematical Physics.** R.O. WELLS, Jr.
79. **Lectures on Approximation and Value Distribution.** Tord GANELIUS, Walter K. KAYMAN, Donald J. NEWMAN
80. **Sur la topologie des surfaces complexes compactes.** Srinivasacharyulu KILAMBI, Gottfried BARTHEL, Ludger KAUP
81. **Topics in Polynomial and Rational Interpolation and Approximation.** Richard S. VARGA
82. **Approximation uniforme qualitative sur des ensembles non bornés.** Paul M. GAUTHIER, Walter HENGARTNER
83. **Convolutions in Geometric Function Theory.** Stephan RUSCHEWEYH.
84. **Characteristic Properties of Quasidisks.** Frederick W. GEHRING.
85. **Curves in Projective Space.** Joe HARRIS.
86. **Les Inégalités de Markoff et de Bernstein.** Qazi Ibadur RAHMAN, Gerhard SCHMEISSER
87. **Analyse des données.** Francis CAILLIEZ
88. **Inférence statistique et analyse des données sous des plans d'échantillonnages complexes.** Carl E. SÄRNDAL
89. **Analyse de données chronologiques.** Guy MÉLARD
90. **Schauder's Estimates and Boundary Value Problems for Quasilinear Partial Differential Equations.** Manfred KÖNIG
91. **Topological Methods in Bifurcation Theory.** Kazimierz GĘBA et Paul H. RABINOWITZ
92. **Points fixes, points critiques et problèmes aux limites.** Jean MAWHIN
93. **Problèmes aux limites non linéaires pour certaines classes d'équations différentielles ordinaires.** Ronald B. GUENTHE
94. **The Fixed Point Index and Some Applications.** Roger D. NUSSBAUM
95. **Méthodes topologiques en analyse non linéaire.** Comptes rendus colligés par Andrzej GRANAS.
96. **Analysis of Categorical Data.** Gary G. KOCH, Peter B. IMREY *et al.*
97. **Infinite Dimensional Morse Theory and its Applications.** Kung-Ching CHANG.
98. **Ordination and Classification.** P.G.N. DIGBY et J.C. GOWER.
99. **Clones in Universal Algebra.** Ágnes SZENDREI.
100. **Hamiltonian Structure and Lyapunov Stability for Ideal Continuum Dynamics.** D.D. HOLM, J.E. MARDSEN et T.S. RATIU.

COLLECTION «CHAIRE AISENSTADT»

Physical Aspects of Lie Group Theory. Robert HERMANN
Quelques problèmes mathématiques en physique statistique. Mark KAC
La Transformation de Weyl et la fonction de Wigner : une forme alternative de la mécanique quantique. Sybren DE GROOT
Sur quelques questions d'analyse, de mécanique et de contrôle optimal. Jacques Louis LIONS
Mariages stables et leurs relations avec d'autres problèmes combinatoires. Donald E. KNUTH
Symétries, jauges et variétés de groupe. Yuval NE'EMAN
La Théorie des sous-gradients et ses applications à l'optimisation. Fonctions convexes et non convexes. R. Tyrrel ROCKAFELLAR

Achevé d'imprimer
en juillet 1986 sur les presses
des Ateliers Graphiques Marc Veilleux Inc.
Cap-Saint-Ignace, Qué.