Math. Z. 143, 165–174 (1975)

Polynomial Interpolation and the Chinese Remainder Theorem for Algebraic Systems

Kirby A. Baker and Alden F. Pixley

§ 1. Lattices and the Number 2

There are several intriguing instances of theorems that apply to lattices and involve the integer 2. Here are their statements; their relationships and proofs will be considered in § 2.

1.1. *First Illustration: Bergman's Double-projection Theorem.* Can a sublattice of a direct product $L_1 \times \cdots \times L_n$ of lattices be uniquely identified from its images in $L_1, \ldots, L_n$ under the projection maps on the factors L_i? No, clearly: even in a product $L \times L$, the diagonal and the full product have the same images when projected. The following fact is therefore striking:

1.2. **Theorem** (Bergman [1]). *A sublattice M of a direct product $P = L_1 \times \cdots \times L_n$ of lattices can be uniquely determined from its images under the projections π_{ij} of P onto all* ***pairs*** *of factors $L_i \times L_j$, $(i<j)$.*

In other words, two sublattices with the same "2-fold projections on factors" must coincide. Bergman's theorem will be derived in § 2 as a consequence of Theorem 2.1.

As an example, let $L_1 = \cdots = L_n = \mathbf{2}$, the two element chain $\{0, 1\}$. Then P can be regarded as the Boolean lattice of all subsets of an n-element set S, with M as a sublattice. Bergman's theorem asserts that M can be uniquely identified from its restrictions to the various two-element subsets of S. In contrast, Bergman's property fails for abelian groups: Let $\mathbb{Z}_2$ denote the group of integers modulo 2, and consider the product $P' = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ and its subgroup $M' = \{(0,0,0), (1,1,0), (1,0,1), (0,1,1)\}$. P' and M' are different subgroups of P', and yet have the same images under projections on pairs of factors.

1.3. *Second Illustration: The Pairwise Chinese Remainder Theorem.* Recall the Chinese Remainder Theorem for integers: For any integer moduli $m_1, \ldots, m_n$ and integers $a_1, \ldots, a_n$, the congruences $x \equiv a_i \pmod{m_i}$ have a simultaneous solution x, provided only that the congruences are pairwise compatible, in the sense that $a_i \equiv a_j \pmod{\gcd(m_i, m_j)}$. An equivalent but formally stronger compatibility condition is simply to require that any two congruences have a simultaneous solution. In fact the following theorem is due to Wille:

1.4. **Theorem** (Wille [19]). *For any congruence relations $\theta_1, \ldots, \theta_n$ on a lattice L and elements $a_1, \ldots, a_n$ of L, if the congruences $x \equiv a_i \pmod{\theta_i}$ are solvable any two at a time, then they are simultaneously solvable.*

Actually, Wille's theorem applies to a more general class of algebraic systems, and Huhn has generalized the theory still further [10]. For further discussion of congruence relations and corresponding variants of the Chinese Remainder Theorem, see [5], [7, pp. 221, 264-265], [14]. For a ring-theoretic version see [20, p. 279].

1.5. *Third Illustration: A Sublattice-of-the-square Criterion for Polynomial Functions.* Let L be a finite lattice, let n be a positive integer, and let f be an "n-ary function on L," i.e., a function f: $L^n \to L$.What is a necessary and sufficient condition for f to be a *polynomial* function – a function built by compositions using the lattice operations $\vee$ and $\wedge$? As a first attempt, observe that each sublattice S of L must be closed under f, in the sense that $f(S^n) \subseteq S$; if $n > 1$, though, this necessary condition is not sufficient.

In this paper, however, it will be shown that it is enough to consider sublattices of $L \times L$, no matter how large n is:

1.6. **Theorem.** *For any finite lattice L and function f*: $L^n \to L$, *f is a polynomial function if and only if every sublattice of* $L \times L$ *is closed under f.*

This fact is a corollary of 1.8 below.

Again, a sublattice S of $L \times L$ is said to be closed under f when S is closed under the n-ary operation on $L \times L$ obtained by coordinatewise application of f – the usual method of extending an operation to a direct product.

As an example, for any lattice L consider the particular sublattice S of $L \times L$ given by $S = \{(x, y) \in L \times L: x \leqq y\}$, the graph of the inequality relation. For any n, the n-ary functions f under which S is closed are simply those functions that are isotone. In effect, the closure condition for this particular S has produced a particular attribute of polynomial functions. Other choices of S correspond to the assertions that such an n-ary function preserves congruence relations on L or given isomorphisms between sublattices of L.

Theorem 1.6 does not generalize to all infinite lattices (Example 5.3). However, it does generalize to some special classes of infinite lattices, such as infinite distributive lattices (Theorem 5.2).

1.7. *Fourth Illustration: Multivariate Lagrange Interpolation for Lattices.* The familiar Lagrange Interpolation Theorem asserts that for any $m \geqq 0$, any distinct real numbers $a_0, \ldots, a_m$, and any real numbers $b_0, \ldots, b_m$ there exists a real polynomial function p of degree at most m such that $p(a_i) = b_i$ $(i = 0, \ldots, m)$. The function p can be constructed explicitly; the theorem generalizes to arbitrary fields, and even to polynomials in several variables, although the question of degrees becomes more complicated.

Observe that the pairs (a_i, b_i) constitute a function defined on a finite subset of the real field $\mathbb{R}$. More generally, by a *finite partial function in* $\mathbb{R}^n$ *to* $\mathbb{R}$ let us mean a function whose domain is a finite subset of $\mathbb{R}^n$. In this terminology, then, Lagrange's Interpolation Theorem for n real variables asserts that every finite partial function f in $\mathbb{R}^n$ to $\mathbb{R}$ has an interpolating polynomial – a polynomial function p: $\mathbb{R}^n \to \mathbb{R}$ of which f is a restriction.

Is there an analogous interpolation theorem for lattices? Clearly, there must be conditions imposed on the finite partial functions f considered: At the very least, they must be isotone, as lattice polynomials are. Moreover, "polynomials" in the sense of lattices are more special than "polynomials" as used in Lagrange's Theorem: The latter involve real constants as coefficients and so are really "algebraic functions" in the terminology of universal algebra [7, p. 45]. (Such functions will be considered in § 6.)

Here, then, is such a lattice analogue of Lagrange's Theorem – an analogue that is simultaneously a generalization of Theorem 1.6 and an additional instance of the appearance of the number 2:

1.8. Theorem. *For any lattice L and integer $n \geqq 1$, a finite partial function f in L^n to L has an interpolating polynomial if and only if all sublattices of $L \times L$ are closed under f.*

The proof will be given in § 2. For such a partial function, to say that a sublattice S of $L \times L$ is closed under f means that if $(c_1, d_1), \ldots, (c_n, d_n) \in S$, then $(f(c_1, \ldots, c_n), f(d_1, \ldots, d_n)) \in S$, provided only that both these values of f are defined.

§ 2. The Equivalence Theorem

What is behind the theorems of § 1? Why is the number 2 associated with lattices?

A clue is given by a result of Wille [19] (see also Huhn [10, Theorem 3.3]): For any variety (equational class, primitive class) V of algebras, the "pairwise Chinese Remainder Theorem" is valid in all algebras of V if and only if V has a "majority polynomial" in three variables, i.e., a polynomial expression $m(x, y, z)$ such that all algebras of V obey the identities $m(x, x, y) = x$, $m(x, y, x) = x$, $m(y, x, x) = x$. For lattices, such a polynomial is the "median polynomial"

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

In this and subsequent sections, then, the first, second, and fourth theorems of § 1 will be proved by showing that the truth of each for a variety V (in place of the variety of lattices) is *equivalent* to the existence of such a majority polynomial. The third theorem, Theorem 1.6, was already observed to be an immediate corollary of the fourth.

Moreover, at no extra cost, the integer 2 of § 1 can be generalized to an arbitrary dimension-like integer $d \geqq 2$, as Huhn does in his theory of d-distributivity [10]. Huhn's generalized $m(x, y, z)$ is a $(d+1)$-variable polynomial expression obeying the "near unanimity" identities

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

for any position of the "lone dissenter' y.

The full theorem of equivalence is as follows. (An extra condition, (4), has been included for later convenience.)

2.1. Theorem. *For a variety V and integer $d \geqq 2$, the following conditions are equivalent:*

(1) *V has a $(d+1)$-variable polynomial expression $m(x_0, \ldots, x_d)$ satisfying the "near unanimity" identities in each algebra of V.*

(2) *In V, if A is a subalgebra of a direct product $P = C_1 \times \cdots \times C_r$ $(r \geqq d)$, then A can be uniquely determined from a knowledge of its d-fold coordinate projections – its images under the projections of P on all products $C_{i(1)} \times \cdots \times C_{i(d)}$, $i(1) < \cdots < i(d)$.*

(3) *In any algebra $A \in V$, if r congruences $x \equiv a_i \bmod \theta_i$, $1 \leqq i \leqq r$, $r \geqq d$, are solvable d at a time, then they are solvable simultaneously.*

(4) *For any algebra $A \in V$, integer $n \geqq 1$, and finite partial function f in A^n to A, if the restriction of f to each subset of its domain with d or fewer elements has an interpolating polynomial, then so does f itself.*

(5) *For any algebra $A \in V$, integer $n \geqq 1$, and finite partial function f in A^n to A, f has an interpolating polynomial if and only if all subalgebras of A^d are closed under f (where defined).*

The proof will be given in § 4.

2.2. *Notes.* (i) As remarked above, this theorem has as corollaries all four lattice theorems of § 1.

(ii) It is a simple observation (e.g. [14]) that for any algebra A, a function $f\colon A^n \to A$ $(n \geqq 1)$ is a polynomial function if all subalgebras of A^{A^n} are closed under f. In contrast, if the equivalent conditions of the theorem do hold for A, then according to condition (5) the test requires only subalgebras of A^d, rather than A^{A^n} – a substantial simplification.

(iii) Condition (5) of the theorem applies in particular to the case where f is defined on $F^n \to A$ for some finite subset F of A. In this case, (5) can be rephrased as (5′): If f takes $S \cap F^d$ to S for each subalgebra S of A^d, then f coincides on F^d with some polynomial p.

(iv) The near unanimity identities of (1) constitude a (strong) Mal'cev-type characterization ([8, 15]) of the equivalent conditions (2)–(5). For the case $d = 2$, the near unanimity identities coincide with the case $n = 2$ of Jónsson's Δ_n characterizing congruence-distributivity [11].

§ 3. Characterization of Closure

In condition (5) of Theorem 2.1, the "closure" of subalgebras of A^d under f has the meaning noted above: If S is a subalgebra of A^d and n d-tuples from S are given, then the coordinatewise application of f to these d-tuples yields a d-tuple in S, provided that the application of f is defined for each coordinate.

The condition is most easily visualized by forming a matrix with the given d-tuples as rows. In these terms, the subalgebra S is closed under f when, for any $n \times d$ matrix M whose *rows* are d-tuples in S and whose *columns* are n-tuples in the domain of f, S contains the row vector "$f(M)$" of length d obtained by applying f to each column of M.

This test suggests examining the case where M is a given $n \times d$ matrix over A and S is the subalgebra of A^d *generated* by the rows of M. For convenience, let us call this subalgebra the "row space of M".

The following lemma clarifies the relationship between closure, the row space of M, and interpolation. (Because the parameter d has a specific role in the preceding theorem, the letter k will be substituted, for future flexibility.)

3.1. Lemma. *For an algebra A, positive integers n and k, and partial function f in A^n to A, the following conditions are equivalent:*

(a) *All subalgebras of A^k are closed under f;*

(b) *for any $n \times k$ matrix M with entries in A and columns in the domain of f, the row vector $f(M)$ is in the row space of M;*

(c) *f, restricted to any k or fewer elements of its domain, can be interpolated.*

Proof, cyclically. (a) $\Rightarrow$ (b): As remarked above, (b) is an instance of (a). (b) $\Rightarrow$ (c): Let M be an $n\times k$ matrix whose columns are k (or fewer) given elements of the domain of f (if fewer than k, then with repeated columns). By (b), $f(M)$ is in the row space of M. But the elements of a generated subalgebra are polynomial expressions in the generators. Thus $f(M)=p(M)$ for some n-ary polynomial $p\colon A^n\to A$. In other words, p and f agree on the k given domain elements of f. (c) $\Rightarrow$ (a): Let S be a subalgebra of A^k being tested for closure under f and let any n elements of S be given, in the form of rows of an $n\times k$ matrix M. Then either (i) not all columns are in the domain of f, in which case the test is vacuously met, or else (ii) the columns *are* in the domain of f, in which case f coincides with a polynomial p on these columns. Since all subalgebras are closed under polynomials, the test is then met.

§ 4. Proof of the Equivalence Theorem

Although a proof of Theorem 2.1 by cyclic implications is possible, it is more instructive to verify the pairwise equivalences (2) $\Leftrightarrow$ (3) $\Leftrightarrow$ (1) $\Leftrightarrow$ (4) $\Leftrightarrow$ (5).

Of these, (3) $\Leftrightarrow$ (1) is due to Huhn [10, Theorem 3.3], and (4) $\Leftrightarrow$ (5) is an immediate consequence of Lemma 3.1 with $k=d$.

4.1. *Balance of the Proof.* (2) $\Rightarrow$ (3): Let $\phi\colon A\to A/\theta_1\times\cdots\times A/\theta_r$ be the composition of the diagonal inclusion $A\to A\times\cdots\times A=A^r$ and the product map $A\times\cdots\times A\to A/\theta_1\times\cdots\times A/\theta_r$ of the individual natural projections $\pi_i\colon A\to A/\theta_i$. For the r congruences $x\equiv a_i \bmod \theta_i$, an element $a\in A$ is a simultaneous solution when $\phi(a)=\langle\bar a_1,\dots,\bar a_r\rangle$, where $\bar a_i$ is the congruence class of a_i in A/θ_i. Thus we must show $\langle\bar a_1,\dots,\bar a_r\rangle\in\phi(A)$. Since the r congruences are assumed to be solvable d at a time, we know, at least, that any d-fold projection of $\langle\bar a_1,\dots,\bar a_r\rangle$ is in the corresponding d-fold projection of $\phi(A)$. But then $\langle\bar a_1,\dots,\bar a_r\rangle$ *is* in $\phi(A)$, for otherwise, the subalgebra generated by $\langle\bar a_1,\dots,\bar a_r\rangle$ and $\phi(A)$ together would be distinct from $\phi(A)$ and so by condition (2) would have at least one distinct d-fold projection.

(3) $\Rightarrow$ (2): Suppose that A and B are subalgebras of $C_1\times\cdots\times C_r$ with the same d-fold projections. It is enough to prove that $A\subseteq B$, as the opposite inclusion follows by a symmetrical argument. Let $a\in A$ be given. We can choose for each i some $b_i\in B$ with $\pi_i(b_i)=\pi_i(a)$, since the d-fold-projection hypothesis implies that A and B certainly have the same projections on individual factors. Consider the r congruences $x\equiv b_i \bmod \ker\pi_i$ in B. Under any d-fold projection, the d corresponding b_i merge into a "d-fold image" of a, which by hypothesis equals the "d-fold image" of an element of B. This element of B solves the d corresponding congruences. Thus the congruences $x\equiv b_i \bmod \ker\pi_i$ are solvable d at a time in B. By (3), these congruences have a simultaneous solution b. Then $\pi_i(b)=\pi_i(b_i)=\pi_i(a)$ for each i. In other words, $b=a$, so that $a\in B$, as desired.

(1) $\Rightarrow$ (4): The proof is by induction on $|\mathrm{dom} f|$, the cardinality of the domain of f. The cases $|\mathrm{dom} f|=0,\dots,d$ are trivial. Suppose the assertion holds for $|\mathrm{dom} f|<r$ $(r>d)$, and consider the case $|\mathrm{dom} f|=r$. By the inductive hypothesis, for each $i=1,\dots,r$ there exists an n-ary polynomial p_i that agrees with f on the $(r-1)$ domain elements *other than* the i-th one (in some previously chosen enumeration). Let $p=m(p_1,\dots,p_{d+1})$, a composition of the near unanimity polynomial

and the first few of the p_i. By the near unanimity property of m, p must agree with f on *every* domain element, as desired. (The polynomials $p_{d+1}, \dots, p_r$ are not needed.)

(4) $\Rightarrow$ (1): Let A be the free algebra on two generators x, y in V and let f be the partial $(d+1)$-ary function whose only defined values are $f(y, x, \dots, x) = x$, $f(x, y, x, \dots, x) = x, \dots, f(x, \dots, x, y) = x$, so that f has $(d+1)$ domain elements in all. A claim: f can be interpolated on any d domain elements. By symmetry we can, without loss of generality, consider the restriction of f to just the *first* d domain elements. But these d elements all have x as their last coordinate, so that on these domain elements f can be interpolated simply by the $(d+1)$-ary function "projection on the last coordinate", which is indeed a polynomial. Thus the claim is valid. By (4), f agrees with some polynomial m on all $(d+1)$ domain elements. For this m, the near unanimity identities hold, because any relation on the generators of a free algebra in V yields a corresponding identity on all algebras in V.

4.2. *Remarks.* (i) The above proof can be short-circuited into a cyclic proof by verifying (2) $\Rightarrow$ (5). To do so, one can consider the row spaces of the $n \times d$ submatrices of a given $n \times r$ matrix.

(ii) For almost any pair of conditions (1), ..., (5), it is interesting to try to find a direct proof of their equivalence.

(iii) The critical part of the interpolation process is given in the proof of (1) $\Rightarrow$ (4). The final interpolating polynomial is a composition whose innermost polynomials are interpolating polynomials for d out of the r domain elements at a time, encased in $(r-d)$ layers of the $(d+1)$-ary polynomial m. A count shows $[(d+1)^{r-d} - 1]/d$ uses of m in producing the final interpolation.

§ 5. Finite Algebras and Locally Finite Varieties

Theorem 2.1 yields immediately:

5.1. Corollary. *Let A be a* **finite** *algebra with a polynomial $m(x_1, \dots, x_{d+1})$ that satisfies the "near unanimity" identities. Then, for any positive integer n, a function $f: A^n \to A$ is a polynomial function if and only if every subalgebra of A^d is closed under f.*

Indeed, it suffices merely to regard f as a finite partial function.

It is interesting to note the potential complexity of f as a polynomial. For example, let L be a 10-element lattice, and let f be a ternary function on L. Then $|\mathrm{dom}\, f| = 1000$, and by Remark 4.2-(iii), the construction 4.1: (1) $\Rightarrow$ (4) represents f as a 998-layered composition involving $(3^{998} - 1)/2$ uses of the majority polynomial for lattices.

Does the criterion of Corollary 5.1 for expressibility as a polynomial extend to infinite algebras? From the analogous case of Lagrange's Theorem for real numbers, one would suspect that the answer is certainly "no", and that is in fact correct: A counterexample is given below for the case of infinite lattices (5.3). However, the answer is *yes* for the variety of distributive lattices and for some other interesting varieties, as shown by the next theorem, 5.2.

An algebra is said to be *locally finite* if it is a directed union of finite subalgebras, or equivalently, if every finitely generated subalgebra is finite [4, p. 101]. A variety is said to be locally finite if all its members are. A criterion is that all finitely generated free algebras in the variety be finite. Examples include the variety of distributive lattices, the variety of tournaments [6], the variety of pseudo-complemented distributive lattices [9], and any variety generated by a single finite algebra.

5.2. Theorem. *Let V be a locally finite variety with a polynomial expression $m(x_1, \ldots, x_{d+1})$ that satisfies the "near unanimity" identities, and let $A \in V$. Then, for any positive integer n, a function f: $A^n \to A$ is a polynomial function if and only if every subalgebra of A^d is closed under f.*

Proof. If f is a polynomial, closure of subalgebras is automatic. Suppose, conversely, that all subalgebras of A^d are closed under f. By Theorem 2.1, for any finite subset F of A, the restriction of f to F^n has an interpolating n-ary polynomial p_F. Since the free algebra on n generators in V is finite, there are only finitely many n-ary polynomials on A in all. Partition the collection $\mathscr{F}$ of all finite subsets of A into pieces, one for each n-ary polynomial p on A, by letting the class corresponding to a given p consist of all F with $p_F = p$. $\mathscr{F}$ is directed under inclusion, and it is a well-known simple lemma that if a directed set is partitioned into finitely many classes, then one class, at least, must be cofinal. The union of the members of such a cofinal class is all of A. If p is the n-ary polynomial corresponding to that class, then f and p therefore agree on all of A.

5.3. *Example* of an infinite lattice L and ternary function f: $L^3 \to L$, such that f is not a lattice polynomial and yet (i) on each finite subset of its domain, f does agree with a polynomial, and (ii) each sublattice of $L \times L$ is closed under f.

First, observe that (i) implies (ii): If (ii) is tested in matrix notation as in Lemma 3.1 (b), each computation of $f(M)$ involves only the two columns of the 3×2 matrix M, for which f agrees with a polynomial, by (i).

Next, let $p_0, p_1, \ldots$ be the sequence of lattice polynomials in three variables x, y, z defined recursively by $p_0(x, y, z) = x$, $p_{k+1}(x, y, z) = (((((p_k \wedge y) \vee z) \wedge x) \vee y) \wedge z) \vee x$. As elements of the free lattice on generators x, y, z, they satisfy $p_0 < p_1 < p_2 < \cdots$, as observed by Birkhoff [2] and used by Whitman [18, § 4]; the weaker inequalities $p_k \leqq p_{k+1}$, at least, are evident by induction from the obvious relation $p_0 \leqq p_1$ and the monotonicity of the expression $(((((t \wedge y) \vee z) \wedge x) \vee y) \wedge z) \vee x$ as a function of t. In contrast to the free lattice, a *finite* lattice with n elements satisfies the lattice identities $p_{n-1} = p_n = p_{n+1} = \cdots$. Indeed, for any elements a, b, c of the lattice, the absence of an $(n+1)$-element chain forces $p_i(a, b, c) = p_{i+1}(a, b, c)$ for some i among $0, 1, \ldots, n-1$, and so for all higher i by an induction using the definition of the p_k.

Finally, let L be a locally finite lattice that satisfies no nontrivial lattice identities, for example, a linear sum (vertical sum, ordinal sum [3, p. 198]) of all finite lattices, or rather, of one finite lattice of each isomorphism type. Because L is locally finite, each sequence of values $p_0(a, b, c)$, $p_1(a, b, c)$, $p_2(a, b, c), \ldots$ is contained in a finite sublattice and so is eventually constant, for any fixed $a, b, c \in L$. Therefore, it makes sense to define f: $L^3 \to L$ by $f(a, b, c) = \lim_{n \to \infty} p_n(a, b, c)$. On any finite subset of L^3, the domain of f, we can choose n large enough that p_n agrees with f at all triples in the subset simultaneously. Thus (i) holds. As already noted, (ii) follows. However, f is not itself a polynomial, because f has the property

$(\forall x, y, z) f = (((((f \wedge y) \vee z) \wedge x) \vee y) \wedge z) \vee x$, which would be a nontrivial polynomial identity in L if f were a polynomial [18, proof of Lemma 4.3].

§ 6. Algebraic Functions

Theorem 2.1 can also be applied to obtain – in certain circumstances – an interesting characterization of algebraic functions, that is, functions which are obtained from polynomials by inserting constants in certain of their argument places [7].

By a *diagonal subalgebra* of A^d we mean any subalgebra S of A^d which contains the subalgebra $\{(a, \ldots, a)\colon a \in A\}$ of A^d. Note that any n-ary algebraic function on A extends to an n-ary algebraic function on any diagonal subalgebra of A^d.

Using this terminology Corollary 5.1 gives the following result:

6.1. Theorem. *Let A be any finite algebra having a $(d+1)$-variable algebraic function $m(x_0, \ldots, x_d)$ satisfying the near unanimity identities. For any function $f\colon A^n \to A$, f is an algebraic function if and only if every diagonal subalgebra of A^d is closed under f.*

Proof. Obviously every diagonal subalgebra of A^d is closed under each algebraic function. To prove the converse let A^* be the algebra obtained from A by adjoining all elements of A as new nullary operations. Then f is an algebraic function of A if and only if f is a polynomial of A^*. Also $m(x_0, \ldots, x_d)$ becomes a polynomial of A^* so, by Corollary 5.1, f is a polynomial of A^* if and only if all subalgebras of A^{*d} are closed under f. Since the subuniverses of A^{*d} are exactly the universes of the diagonal subalgebras of A^d, we have the desired conclusion.

Again, in the special case of lattices, where the median polynomial is certainly algebraic, we have the following companion to Theorem 1.6.

6.2. Corollary. *For any finite lattice L and function $f\colon L^n \to L$, f is an algebraic function if and only if every diagonal sublattice of $L \times L$ is closed under f.*

6.3. *Remark.* The device of adding algebra elements as new opperations can be applied to only one algebra at a time, and not to a variety. Thus, there is no evident analogue of the full Theorem 2.1 for algebraic functions. However the implications (1) ⇒ (3) and (1) ⇒ (5) of Theorem 2.1 and the assertion of Theorem 5.2 do have analogues similar to the Theorem and Corollary of this section.

§ 7. Functional Completeness and Affine Completeness

Let us say that an algebra A satisfies the *subalgebra-of-the-square condition* (or, more briefly, the *square condition*) if the polynomials of A are just those functions on A which preserve all subalgebras of $A \times A$ (i.e.: those functions f for which all subalgebras of $A \times A$ are closed under f). Further, we will say that A satisfies the *diagonal-subalgebra-of-the-square condition* (or, briefly, the *diagonal condition*) if the algebraic functions of A are exactly those functions which preserve all diagonal subalgebras of $A \times A$. Theorem 1.6 and Corollary 6.2 assert that finite lattices satisfy each of these conditions.

In this section we note some easy connections between these conditions and the concepts of functional and affine completeness. The relevant definitions are as follows ([14, 16]): An algebra A is *affine complete* if each function $f\colon A^n \to A$ which preserves all congruences of A is an algebraic function. A is said to be *functionally complete* if *all* functions $f\colon A^n \to A$ are algebraic, or equivalently, if A is affine complete and simple.

Now the subalgebras of $A \times A$ are just those binary relations on A which have the substitution property for all operations of A. In particular, each congruence relation of A is a diagonal subalgebra of $A \times A$. Hence if A is affine complete it necessarily satisfies the diagonal condition. Furthermore, Werner [17] has shown that a variety V is congruence permutable (i.e.: for all pairs θ_1, θ_2 of congruences of any algebra $A \in V$, $\theta_1\theta_2 = \theta_2\theta_1$) if and only if for each $A \in V$ the diagonal subalgebras of $A \times A$ are exactly the congruence relations if A. From this observation we have

7.1. Theorem. *If A is an algebra in a congruence-permutable variety then A is affine complete if and only if A satisfies the diagonal-subalgebra-of-the-square condition. If A is simple then A is functionally complete if and only if A satisfies the diagonal-subalgebra-of-the-square condition.*

In problem 6 of [7] Grätzer asks for a description of all affine complete algebras. Theorem 7.1 gives an answer for algebras in congruence permutable varieties.

An algebra A is *quasi-primal* [14] if each function A which preserves all subalgebras of A and all internal isomorphisms (that is, all isomorphisms among subalgebras) of A is a polynomial of A. Finite quasi-primal algebras are rather natural universal-algebra counterparts of finite fields; indeed a finite ring is quasi-primal just in case it is a field. A quasi-primal algebra is necessarily simple and generates a congruence-permutable variety. Finite (but not all infinite) quasi-primal algebras are also functionally complete. (See [12, 14] for these facts.)

Suppose A is quasi-primal, and suppose f is an n-ary function on A which preserves all subalgebras of $A \times A$. Then f clearly preserves all subalgebras of A. Moreover, if S is a subalgebra of A and ϕ is an internal isomorphism then the set S_1 of pairs $(s, \phi(s))$, $s \in S$, is a subalgebra of $A \times A$. Since f preserves S_1, we have, for $s_i \in S$, that $(f(s_1, \dots, s_n), f(\phi(s_1), \dots, \phi(s_n))) \in S_1$, which means $\phi[f(s_1, \dots, s_n)] = f(\phi(s_1), \dots, \phi(s_n))$. Thus f preserves ϕ, so that by quasi-primality f is a polynomial of A. Hence each quasi-primal algebra satisfies the square condition. Similar considerations show that all other variants of primality [14] are special cases of algebras satisfying the square condition. For quasi-primal algebras, parallel to Theorem 7.1 we even have the following characterization:

7.2. Theorem. *If the algebra A is in a congruence-permutable variety and all subalgebras of A are simple, then A is quasi-primal if and only if A satisfies the subalgebra-of-the-square condition.*

Proof. We have just shown that each quasi-primal algebra satisfies the square condition. Now suppose A is in a congruence permutable variety, has only simple subalgebras, and satisfies the square condition. Each subalgebra S of $A \times A$ is a subdirect product of subalgebras S_1, S_2 of A. However, it is well known that if an algebra is congruence-permutable and is a subdirect product of finitely many simple algebras, then it is isomorphic to the direct product of some subset of the subdirect factors. In the present context this means that a subalgebra S of $A \times A$

has one of the following two forms:

$$S = S_1 \times S_2,$$

or

$$S = \{(s, \phi(s)\colon s \in S_1\},$$

where ϕ is an isomorphism of S_1 onto S_2. Hence if f is a function on A which preserves all subalgebras and internal isomorphisms of A, it evidently preserves subalgebras of $A \times A$ of the above types, and hence all subalgebras of $A \times A$. Since A satisfies the square condition f is a polynomial. Thus A is quasi-primal.

The work of the first author was supported in part by a National Science Foundation grant.

References

1. Bergman, G.M., (unpublished)
2. Birkhoff, G.: On the combination of subalgebras. Proc. Cambridge philos. Soc. **29**, 441–464 (1933)
3. Birkhoff, G.: Lattice Theory, 3rd ed. Colloquium Publications Vol. 25. Providence: American Mathematical Society 1967
4. Cohn, P.M.: Universal Algebra. New York: Harper and Row, 1965
5. Foster, A.L.: The generalized Chinese Remainder Theorem for universal algebras; subdirect factorization. Math. Z. **66**, 171–188 (1955)
6. Fried, E., Grätzer, G.: A non-associative extension of the class of distributive lattices. Pacific J. Math. **49**, 59–78 (1973)
7. Grätzer, G.: Universal Algebra, Princeton: Van Nostrand, 1968.
8. Grätzer, G.: Two Mal'cev type theorems in universal algebra. J. combinat. Theory **8**, 334–342 (1970)
9. Grätzer, G.: Lattice theory, first concepts and distributive lattices. San Francisco: W.H.Freeman, 1971
10. Huhn, A.P.: Weakly distributive lattices, (preprint)
11. Jónsson, B.: Algebras whose congruence lattices are distributive. Math. Scandinav. **21**, 110–121 (1967)
12. Michler, G., Wille, R.: Die primitiven Klassen arithmetischer Ringe, Math. Z. **113**, 369–372 (1970)
13. Pixley, A.F.: Distributivity and permutability of congruence relations in equational classes of algebras. Proc. Amer. math. Soc. **14**, 105–109 (1963)
14. Pixley, A.F.: Completeness in arithmetical algebras. Algebra universalis **2**, 179–196 (1972)
15. Taylor, W.: Characterizing Mal'cev Conditions. Algebra universalis **3**, 351–397 (1973)
16. Werner, H.: Produkte von Kongruenzklassengeometrien universeller Algebren. Math. Z. **121**, 11–140 (1971)
17. Werner, H.: A Mal'cev condition for admissible relations. Algebra universalis **3**, 263 (1973)
18. Whitman, P.: Free lattices II. Ann. of Math, II. Ser. **43**, 104–115 (1942)
19. Wille, R.: Kongruenzklassengeometrien. Lecture Notes in Mathematics **113**, Berlin-Heidelberg-New York: Springer 1970
20. Zariski, O., Samuel, P.: Commutative algebra, vol. I. Princeton: Van Nostrand 1958

K.A. Baker
Department of Mathematics
University of California
Los Angeles, California 90024
USA

A.F. Pixley
Harvey Mudd College
The Claremont Colleges
Claremont, California 91711
USA

(Received September 2, 1974)