ANNALI DELLA
SCUOLA NORMALE SUPERIORE DI PISA
Classe di Scienze

ADIL YAQUB

Primal clusters and local binary algebras

Annali della Scuola Normale Superiore di Pisa, Classe di Scienze 3^e série, tome 21, n^o 2 (1967), p. 111-119

<http://www.numdam.org/item?id=ASNSP_1967_3_21_2_111_0>

PRIMAL CLUSTERS AND LOCAL BINARY ALGEBRAS (*)

ADIL YAQUB

The theory of a primal (= strictly functionally complete) algebra subsumes and substantially generalizes the classical Boolean theory as well as that of p-rings and Post algebras. Here a primal algebra is a finite algebra in which each map is expressible in terms of the primitive operations of the algebra. The concept of independence is essentially a generalization to universal algebras of the Chinese remainder theorem in number theory. A primal cluster is a class $\{U_i\}$ of universal algebras U_i of the same species in which each U_i is primal and such that every finite subset of $\{U_i\}$ is independent.

Our present object is to show that the class $\{(B_n, \times)\}$ of all « local » binary algebras of distinct orders, endowed with a suitably chosen permutation $\frown$ of B_i, forms a primal cluster $\{(B_n, \times, \frown)\}$ (of species (2, 1)). Here a local binary algebra is a finite associative binary algebra $(B, \times)$ such that every element in B is either nilpotent or has an inverse (in B). In Theorem 5, which is our main result, we show that a much more comprehensive class K of algebras of rather *diverse* nature nevertheless forms a primal cluster. Here K is the union of all algebras in $\{(B_n, \times, \frown)\}$ and $\{(P_m, \times, \frown)\}$, where $(P_m, \times, \frown)$ is the basic Post algebra of order m (species (2,1)). This theorem subsumes Foster's results on prime fields, « n-fields », groups with null, basic Post algebras, and, in addition, yields new results especially in regard to local rings (viewed as binary algebras). Our methods for obtaining the permutation $\frown$, as well as for establishing independence, are *constructive*. Indeed, the permutation $\frown$ turns out to be of rather general (but not entirely arbitrary) nature.

1. **Fundamental concepts.** We begin this section by recalling the following results of [3]. Let $U = (U, \theta_1, \theta_2, \ldots)$ be an algebra and let

Pervenuto alla Redazione il 5 Aprile 1966.

(*) This work was supported in part by National Science Foundation Grant GP-4163.

$S = (n_1, n_2, \ldots)$ be its species, where θ_i is a primitive operation of finite rank n_i. An *S-expression* is a primitive composition of indeterminate symbols $\zeta_1, \zeta_2, \ldots$ via the primitive operations θ_i. A map $f(\zeta_1, \ldots, \zeta_n)$ from $U \times \ldots \times U$ to U is *expressible* if there exists an S-expression $\varphi(\zeta_1, \ldots, \zeta_n)$ such that $f = \varphi$ for all $\zeta_1, \ldots, \zeta_n$ in U. An algebra U is *primal*, or *strictly functionally complete* if it is finite, with at least two elements, and if every map $f(\zeta_1, \ldots, \zeta_n)$ in U is expressible. Now, let $\{U_i\} = \{U_1, \ldots, U_t\}$ be a finite set of algebras of species S. We say that $\{U_i\}$ satisfies the *Chinese remainder condition,* or is *independent* if, corresponding to each set of S-expressions $\varphi_1, \ldots, \varphi_t$, there exists a single expression ψ such that $\psi = \varphi_i$ is an identity of $U_i (i = 1, \ldots, t)$. A *primal cluster* of species S is a class $\widetilde{U} = \{\ldots, U_i, \ldots\}$ of primal algebras U_i of species S any finite subset of which is independent. We now have the following (compare Definition 2 below with Definition 3 and Theorem 6).

Definition 1. A *binary algebra* is an algebra $(B, \times)$, possessing two distinguished elements $0, 1$ $(0 \neq 1)$ such that

$$0 \times \zeta = \zeta \times 0 = 0, \quad 1 \times \zeta = \zeta \times 1 = \zeta \quad (\zeta \in B).$$

Definition 2. A *local binary algebra* is a finite binary algebra $(B, \times)$ which is associative and such that ζ in B implies ζ is nilpotent or ζ has an inverse (in B).

Examples of local binary algebras are wide-spread. Thus, the multiplicative structure of any (finite) Galois field, $(GF(p^k), \times)$, and more generally any (not necessarily cyclic) finite group with null $(G \cup \{0\}, \times)$ is a local binary algebra. Other examples include the multiplicative structure of each of the following rings: the integers $(\mathrm{mod}\, p^k$, p prime), the hypercomplex ring $GF(p^k)[\eta_1, \ldots, \eta_t]$ obtained by adjoining any finite number $\eta_1, \ldots, \eta_t$ of commuting nilpotent elements to any Galois field, and more generally, any local finite commutative ring with identity (see Definition 3).

2. **The main theorems.** Let $(B, \times)$ be any local binary algebra. Then, for some $r \geq 1$ and some $s \geq 0$, we may denote:

(1) $$B = \{0, 1, \zeta_2, \zeta_3, \ldots, \zeta_r, \eta_1, \eta_2, \ldots, \eta_s\}, \quad \zeta_i \textit{ unit}, \quad \eta_i \textit{ nilpotent}.$$

For every element α in B, define the *characteristic function* $\delta_\alpha(\zeta)$ as follows:

(2) $$\delta_\alpha(\zeta) = 1 \quad \text{if} \quad \zeta = \alpha, \quad \delta_\alpha(\zeta) = 0 \quad \text{if} \quad \zeta \neq \alpha \quad (\zeta \in B).$$

Now, define a permutation $\widehat{\ }$ of B by the ordering (1) above, i. e.,

$$(3) \qquad \widehat{\ }: \text{def: } 0\widehat{\ } = 1,\ 1\widehat{\ } = \zeta_2,\ \zeta_2\widehat{\ } = \zeta_3, \dots, \zeta_r\widehat{\ } = \eta_1, \dots, \eta_s\widehat{\ } = 0.$$

Clearly, $\widehat{\ }$ is a cyclic $0 \to 1$ permutation of B. Following [1], we define:

$$(4) \qquad a \times_{\frown} b = \text{def} = (a\widehat{\ } \times b\widehat{\ })\breve{\ }, \quad \zeta\breve{\ } = \text{def} = \text{inverse of } \zeta\widehat{\ }.$$

It is readily verified that

$$(5) \qquad a \times_{\frown} 0 = 0 \times_{\frown} a = a.$$

Moreover, for any function f on B, we have (compare with [1])

$$(6) \qquad f(x_1, \dots, x_k) = \overset{\times\frown}{\sum_{\alpha_1, \dots, \alpha_k}} f(\alpha_1, \dots, \alpha_k)\, \delta_{\alpha_1}(x_1)\, \delta_{\alpha_2}(x_2) \dots \delta_{\alpha_k}(x_k).$$

In (6), $\alpha_1, \dots, \alpha_k$ range independently over all the elements of B. Furtermore, te notation $\overset{\times\frown}{\sum_{\beta_i \in B}} \beta_i$ means $\beta_1 \times_{\frown} \beta_2 \times_{\frown} \beta_3 \times_{\frown} \dots$ where $\beta_1, \beta_2, \beta_3, \dots$ are all the elements of B. The verification of (6) is immediate upon using (2) and (5).

We also need the following easily proved

LEMMA 1. *Let $(B, \times)$ be any local binary algebra, and let η be any nilpotent element in B. Then ηx and $x\eta$ are nilpotent for all x in B.*

PROOF. Suppose η is a nilpotent element of B and x is in B. Suppose $\eta x = y =$ unit. We show that this leads to a contradiction. Indeed, if x were a unit, then $\eta = yx^{-1} =$ unit, contradiction. Moreover, if x were not a unit, then, since B is local, x would be nilpotent. Now, let k be the least positive integer such that $x^k = 0$. Clearly, $k > 1$. Then $\eta x^k = yx^{k-1}$, $0 = yx^{k-1}$, $y^{-1}0 = x^{k-1}$, $0 = x^{k-1}$, which contradicts the minimality of k. Hence $\eta x (= y)$ is *not* a unit. Again, since B is local, therefore, ηx is nilpotent. The proof for $x\eta$ is similar, and the lemma is proved.

Next, we prove the following

THEOREM 1. *Let $(B, \times)$ be any local binary algebra, and let $B = \{0, 1, \zeta_2, \zeta_3, \dots, \zeta_r, \eta_1, \dots, \eta_s\}$, each ζ_i is a unit, each η_i is nilpotent. Suppose $\widehat{\ }$ is any $0 \to 1$ cyclic permutation of B such that $1\widehat{\ } = \zeta_2$, $\zeta_2\widehat{\ } = \zeta_3, \dots, \zeta_{r-1}\widehat{\ } = \zeta_r$, but otherwise $\widehat{\ }$ is entirely arbitrary. Then the algebra $(B, \times, \widehat{\ })$ (species (2,1)) is primal.*

PROOF. Let $\zeta^{\frown n}$ denote $(\ldots((\zeta^{\frown})^{\frown})^{\frown}\ldots)^{\frown}$ (n iterations). Since $\zeta^{\frown}$ is a *cyclic* permutation of B, therefore

$$\zeta\,\zeta^{\frown}\,\zeta^{\frown 2}\ldots\zeta^{\frown r+s}=0.$$

Hence 0 (and with it $0^{\frown}, 0^{\frown 2}, \ldots, 0^{\frown r+s}$) is expressible in terms of the primitive operations $\times, ^{\frown}$. Therefore all the elements (= constant functions) of B are expressible in terms of $\times, ^{\frown}$. Next, we show that the characteristic function $\delta_a(x)$ is so expressible. Thus, let a be any element of B. Choose N so large that $\eta^N=0$ for all nilpotent elements of B. Now, since $\zeta^{\frown}$ is a *cyclic* permutation of B, there therefore exists an integer m such that $a^{\frown m}=0$. Recalling that $^{\frown}$ is defined by the ordering (3), it is readily verified that

$$\delta_a(x)=(x^{\frown m+1}\,x^{\frown m+2}\ldots x^{\frown m+r})^{rN}. \tag{7}$$

In verifying (7) we make use of Lagrange's Theorem and Lemma 1. Now, to prove the theorem, let $f: B\times\ldots\times B\to B$ be any mapping from B^k to B. By what we have just proved, and using (6) and (4), it readily follows that the right-side of (6) is expressible in terms of the operations $\times, ^{\frown}, ^{\smile}$, and hence $f(x_1,\ldots,x_k)$ is expressible in terms of $\times, ^{\frown}, ^{\smile}$. Since, however, $\zeta^{\smile}$ is the inverse of the *cyclic* permutation $\zeta^{\frown}$, therefore, $\zeta^{\smile}=\zeta^{\frown r+s}$ (see (3)). Hence $f(x_1,\ldots,x_k)$ is expressible in terms of the primitive operations $\times, ^{\frown}$, only and the theorem is proved.

Next, we investigate the independence of local binary algebras. To this end, let $B_i=(B_i,\times)$ be a local binary algebra, and let the order (= number of elements) of B_i be $n_i (i=1,\ldots,t)$. For each B_i, define a permutation $^{\frown}$ of B_i as in theorem 1 (i.e., $^{\frown}$ is as in (3)). We now have the following

THEOREM 2. *Suppose $B_1,\ldots,B_t$ are local binary algebras of distinct orders, and suppose that $^{\frown}$ is a permutation of B_i as prescribed in Theorem* 1. *Then the algebras $\{(B_1,\times,^{\frown}),\ldots,(B_t,\times,^{\frown})\}$ are independent.*

PROOF. Let us first consider the algebras $(B_1,\times,^{\frown})$ and $(B_2,\times,^{\frown})$. Let

$$|_{12}(\zeta)=\begin{cases}1\ (\text{in } B_1)\\ 0\ (\text{in } B_2)\end{cases};\qquad |_{21}(\zeta)=\begin{cases}0\ (\text{in } B_1)\\ 1\ (\text{in } B_2)\end{cases}. \tag{8}$$

We shall now construct *expressions* (built up from $\times, ^{\frown}$) $|_{12}(\zeta), |_{21}(\zeta)$ satisfying (8) above. To this end, let N be chosen so that

$$\eta^N=0 \text{ for all nilpotent elements } \eta \text{ in } B_1 \text{ or } B_2. \tag{9}$$

Now, define

(10) $E = \zeta\zeta^{\frown}\zeta^{\frown 2}\ldots\zeta^{\frown n-1}$, $n =$ larger of the orders of B_1, B_2,

(11) $r_i =$ number of units in B_i $(i = 1, 2)$.

We now distinguish three cases.

Case 1 : $r_1 > r_2$.

Recalling that $^{\frown}$ is defined for each B_i as in (3), (1), it is easily seen, using (10), (11), (9), Lagrange's Theorem, and Lemma 1, that

$$|_{12}(\zeta) = (E^{\frown} E^{\frown 2} E^{\frown 3}\ldots E^{\frown r_1})^{r_1 N} = \begin{cases} 1 \text{ (in } B_1) \\ 0 \text{ (in } B_2) \end{cases}.$$

Case 2 : $r_1 < r_2$.

As in *Case* 1, we now have

$$|_{21}(\zeta) = (E^{\frown} E^{\frown 2}\ldots E^{\frown r_2})^{r_2 N} = \begin{cases} 0 \text{ (in } B_1) \\ 1 \text{ (in } B_2) \end{cases}.$$

Case 3 : $r_1 = r_2$.

Let $n_1 =$ order of $B_1 <$ order of $B_2 = n_2$. This is possible since B_1 and B_2 have distinct orders. Again, using Lemma 1, it is easily seen that

$$|_{12}(\zeta) = (E^{\frown n_1+1} E^{\frown n_1+2}\ldots E^{\frown n_1+r_1})^{r_1 N} = \begin{cases} 1 \text{ (in } B_1) \\ 0 \text{ (in } B_2) \end{cases}.$$

Furthermore, since $0^{\frown} = 1$ (in both B_1 and B_2), therefore

(12) $$|_{ij}(\zeta) = \{(|_{ji}(\zeta))\,(|_{ij}(\zeta))^{\smile 2}\}^{\frown}; \quad i, j = 1, 2; \quad i \neq j,$$

holds in *both* B_1 and B_2. Hence, both $|_{12}(\zeta)$ and $|_{21}(\zeta)$ are *expressions.* Clearly, this holds for any pair of distinct algebras B_i, B_j in our set, and we have thus proved that if

(13) $$|_{ij}(\zeta) = \text{def} = \begin{cases} 1 \text{ (in } B_i) \\ 0 \text{ (in } B_j) \end{cases}, \quad 1 \leq i, j \leq t, \quad i \neq j,$$

then every $|_{ij}(\zeta)$ is an expression built up from $\times, \frown, \smile$. And since $\zeta^{\smile} = \zeta^{\frown n_i n_j - 1}$, therefore

(14) $\quad |_{ij}(\zeta)$ is an *expression* (built up from $\times, \frown$), $i \neq j$.

Now, let

(15) $$|_i(\zeta) = |_{i1}(\zeta)\, |_{i2}(\zeta) \ldots |_{it}(\zeta) \text{ (no } |_{ii}(\zeta)), \quad i = 1, \ldots, t.$$

Then

(16) $$|_i(\zeta) = \begin{cases} 1 \text{ (in } B_i) \\ 0 \text{ (in } B_j) \end{cases}, \quad 1 \leq i, j \leq t, \ i \neq j.$$

To prove the independence of $\{(B_1, \times, \frown), \ldots, (B_t, \times, \frown)\}$, let $\varphi_1, \ldots, \varphi_t$ be any set of expressions, and define:

$$\psi = \{\varphi_1\, |_1(\zeta)\} \times_{\frown} \ldots \times_{\frown} \{\varphi_t\, |_t(\zeta)\}.$$

Now, by (14), (15), (4), it follows that ψ is an expression built up from $\times, \frown, \smile$, and since $\zeta^{\smile} = \zeta^{\frown m}$ ($m = n_1 \ldots n_t - 1$, $n_i =$ order of B_i), therefore, ψ is an expression built up from $\times, \frown$. Furthermore, using (16) and (5), we have, $\psi = \varphi_i$ (in *each* B_i). Hence the algebras $\{B_1, \ldots, B_t\}$ are independent, and the theorem is proved.

An easy combination of Theorems 1, 2, and the definition of a primal cluster yields the following

THEOREM 3. *The class* $\{\ldots, (B_n, \times, \frown), \ldots\}$ *of all local binary algebras of pairwise distinct orders, where* $\frown$ *is as in Theorem* 2, *forms a primal cluster* (species (2, 1)).

Now, let i be any positive integer, and let $(P_i, \times, \frown)$ be the basic Post algebra of order i. Here, $P_i = \{0, \varrho_{i-2}, \varrho_{i-3}, \ldots, \varrho_1, 1\}$, $\zeta \times \eta = \min(\zeta, \eta)$, where « min » refers to the above ordering, and where $\frown$ is given by

(17) $$0^{\frown} = 1, \ 1^{\frown} = \varrho_1, \ \varrho_1^{\frown} = \varrho_2, \ldots, \varrho_{i-2}^{\frown} = 0.$$

In [2], the following theorem was proved.

THEOREM 4. *The class* $\{\ldots, (P_m, \times, \frown), \ldots\}$ *of all basic Post algebras of distinct orders forms a primal cluster* (*of species* (2,1)), *where* $\times, \frown$ *are as above.*

Now, suppose m and n are positive integers. Let $(B_n, \times, \frown)$ and $(P_m, \times, \frown)$ be as in Theorems 3, 4, and let the orders of B_n and P_m be n and m. We now have the following (compare with [4 ; 5]).

THEOREM 5. (Principal Theorem). *The class* $\{(B_n, \times, \frown)\}_{n\geq 2} \cup \{(P_m, \times, \frown)\}_{m\geq 3}$ *forms a primal cluster (species* (2,1)*), where* $\{(B_n, \times, \frown)\}$ *and* $\{(P_m, \times, \frown)\}$ *are as in Theorems* 3, 4, *(order of* B_n *is* n*, order of* P_m *is* m*).*

PROOF. First, observe that $(B_n, \times, \frown) \cong (P_m, \times, \frown)$ if and only if $n = m = 2$, and hence no two element-algebras above are isomorphic. This follows since in a local binary algebra, $x^2 = x$ holds if and only if $x = 0$ or $x = 1$. Furthermore, a careful examination of the proof of Theorem 2 shows that, in view of Theorems 3, 4, and the definition of a primal cluster, we will be through if we can show that there exist *expressions* (built up from $\times, \frown$) $|_{ij}(\zeta)$ such that

$$|_{ij}(\zeta) = \begin{cases} 1 \text{ (in } B_i) \\ 0 \text{ (in } P_j) \end{cases}, \qquad |_{ji}(\zeta) = \begin{cases} 0 \text{ (in } B_i) \\ 1 \text{ (in } P_j) \end{cases}. \tag{18}$$

Now, let $E = \zeta\zeta^{\frown} \zeta^{\frown 2} \ldots \zeta^{\frown k}$, where $k = \max\{i, j\}$. Let r be the order of the group of units in B_i, and let N be such that $\eta^N = 0$ for all nilpotent elements in B_i. By (3), (17), we have

$$|_{ij}(\zeta) = (((E^{\frown 2} E^{\smile})^{rN})^{\frown})^r = \begin{cases} 1 \text{ (in } B_i) \\ 0 \text{ (in } P_j), \end{cases}$$

$|_{ji}(\zeta)$ as in (12).

Since $\zeta^{\smile} = \zeta^{\frown ij-1}$, both $|_{ij}(\zeta)$, $|_{ji}(\zeta)$ are expressions (built up from $\times, \frown$) and the theorem is proved.

3. **Applications.** In this section, we consider certain classes of binary algebras to which the above theorems apply. First, we have the following [6 ; p. 228].

Definition 3. Let R be any associative and commutative ring with identity 1. R is called a *local ring* if and only if R is Noetherian and the nonunits of R form an ideal.

We now have the following (compare with Definition 2).

THEOREM 6. *Let* R *be any finite commutative (associative) ring with identity* $1\ (1 \neq 0)$. R *is a local ring if and only if every element in* R *is either nilpotent or is a unit.*

PROOF. Let R be a local ring, and let J be the radical of R. Let N be the set of nonunits of R. We claim that $J = N$. Clearly, $J \subseteq N$. Now, suppose $z \in N$. Since N is an ideal and $1 \notin N$, therefore $1 - z \notin N$. Hence, for any x in R, $z \in N$ implies $1 - zx$ is a unit and thus zx is quasi-regular. Therefore, $N \subseteq J$. Hence $N = J =$ set of nilpotent elements in R. The converse is immediate.

COROLLARY 1. *The multiplicative structure* $(R, \times)$ *of any finite commutative (associative) local ring with identity is a local binary algebra. In particular, the multiplicative structure of any of the following rings is a local binary algebra:*

(a) $GF(p^k)$; (b) $I_{/(p^k)}$ (= *ring of integers, mod* p^k (p *prime*));

(c) $GF(p^k)[\eta_1, \ldots, \eta_t]$ *where each* η_i *is nilpotent,* $\eta_i \eta_j = \eta_j \eta_i$, $a\eta_i = \eta_i a$, *all* i, j, *and all* a *in* $GF(p^k)$.

Thus, Theorem 5 applies to all the algebras stated in Corollary 1.

We shall conclude with reference to Foster's results [1; 2]. Indeed, let $(G, \times)$ be any finite group, and let $G' = G \cup \{0\}$, where $y \times 0 = 0 \times y = 0$ $(y \in G')$. As usual, we call the algebra $(G', \times)$ a *group with null.* If, in addition, the above group $(G, \times)$ is *cyclic* of order n, we call $(G', \times)$ an «n-field» [1]. Theorem 1 now has the following corollary which contains Foster's results [1; Theorems 29 and 32].

COROLLARY 2. *Let* $(G', \times)$ *be any finite group with null, and let* $\widehat{\ }$ *be any cyclic* $0 \to 1$ *permutation of* G'. *Then the algebra* $(G', \times, \widehat{\ })$ *is primal (species* (2,1)). *In particular,* $(F_n, \times, \widehat{\ })$ *is primal for any «*n*-field»* $(F_n, \times)$.

Similarly, by taking $B_n = F_n =$ «n-field» in Theorem 3 and Theorem 5, we obtain the following corollary which contains Foster's results [2; Theorems 4.1 and 4.3].

COROLLARY 3. (a) *The set* $\{(F_2, \times, \widehat{\ }), (F_3, \times, \widehat{\ }), \ldots\}$ *of all «*n*-fields» endowed with any cyclic* $0 \to 1$ *permutation* $\widehat{\ }$ *of each* F_n, *forms a primal cluster (species* (2,1)). *More generally,* (b) *if* $(P_m, \times, \widehat{\ })$ *is as in Theorem* 5, *then*

$$\{(F_2, \times, \widehat{\ }), (F_3, \times, \widehat{\ }), \ldots\} \cup \{(P_3, \times, \widehat{\ }), (P_4, \times, \widehat{\ }), \ldots\}$$

forms a primal cluster.

REFERENCES

1. A. L. FOSTER, *Generalized « Boolean » theory of universal algebras*, Part I, Math. Z., 58 (1953), 306-336.

2. A. L. FOSTER, *The identities of — and unique subdirect factorization within — classes of universal algebras*, Math. Z., (1955), 171-188.

3. A. L. FOSTER, *The generalized Chinese ramainder theorem for universal algebras ; subdirect factorization*, Math. Z., 66 (1957), 452-469.

4. A. YAQUB, *Primal clusters*, Pacific J. Math., 16 (1966), 379-388.

5. A. YAQUB, *On certain classes of — and an existence theorem for — primal clusters*, Ann. Sc. Norm. Pisa, 20 (1966), 1-13.

6. O. ZARISKI and P. SAMUEL, *Commutative Algebra*, Univ. Series in Higher Math., Van Nostrand Co., Princeton, New Jersey, 1 (1958).

University of California

Santa Barbara, California