J. P. Díaz Varela
B. F. López Martinolich

Resolution of Algebraic Systems of Equations in the Variety of Cyclic Post Algebras

Abstract. There is a constructive method to define a structure of simple k-cyclic Post algebra of order p, $L_{p,k}$, on a given finite field $F(p^k)$, and conversely. There exists an interpretation Φ_1 of the variety $\mathcal{V}(L_{p,k})$ generated by $L_{p,k}$ into the variety $\mathcal{V}(F(p^k))$ generated by $F(p^k)$ and an interpretation Φ_2 of $\mathcal{V}(F(p^k))$ into $\mathcal{V}(L_{p,k})$ such that $\Phi_2\Phi_1(B) = B$ for every $B \in \mathcal{V}(L_{p,k})$ and $\Phi_1\Phi_2(R) = R$ for every $R \in \mathcal{V}(F(p^k))$.

In this paper we show how we can solve an algebraic system of equations over an arbitrary cyclic Post algebra of order p, p prime, using the above interpretation, Gröbner bases and algorithms programmed in Maple.

Keywords: Varieties, equivalence, finite fields, Post algebras, Gröbner bases.

1. Introduction

M. Serfati studies in [23] the resolution of an algebraic equation in n unknowns over an arbitrary r-Post algebra. He gives first a general parametric solution for the algebraic equation in one unknown

$$f(x) = 0.$$

For algebraic equations in n unknowns, he gives a consistency condition and proposes two alternative methods for its solution.

In [1] we proved that there exists an interpretation Φ_1 of the variety $\mathcal{V}(L_{p,k})$ generated by the $k-$cyclic simple Post algebra of order p, $L_{p,k}$, in the variety $\mathcal{V}(F(p^k))$ generated by the field $\langle F(p^k); +, \cdot, F(p)\rangle$ and an interpretation Φ_2 of $\mathcal{V}(F(p^k))$ in $\mathcal{V}(L_{p,k})$ such that $\Phi_2\Phi_1(B) = B$ for every $B \in \mathcal{V}(L_{p,k})$ and $\Phi_1\Phi_2(R) = R$ for every $R \in \mathcal{V}(F(p^k))$.

In this paper we first analyze if the postian polynomial in one variable over a Post algebra of order p,

$$f(x) = 0$$

Special Issue: Algebras Related to Non-classical Logic
Edited by **Manuel Abad and Alejandro Petrovich**

Studia Logica (2011) 98: 307–330
DOI: 10.1007/s11225-011-9330-6

is consistent. We show how we can solve this equation using the interpretation described in [1] with the help of some algorithms programmed in Maple, and we also propose a solution when the polynomial does not satisfy the consistency condition. In that case we translate the equation $f(x) = 0$ and we obtain the postian polynomial f in the language of $F(p^k)$; using a well known result of Galois theory, we consider it in an extension $F(p^t)$ of $F(p^k)$ where it is solvable. Finally, using again the interpretation mentioned above, we obtain the solutions of the postian polynomial f in the cyclic Post algebra of order p, $L_{p,t}$.

We also use the procedure described above for an algebraic equation in n unknowns. We check first if it satisfies the consistency condition given by Serfati, and once we know that the equation has a solution, we use the interpretation Φ_1 to see the postian polynomial in $F(p^k)$ where it is easier to find the roots. We solve the equation using as a central tool the Gröbner bases, and proceed as above to obtain the solution of the postian equation in the postian language.

Section 2 describes the necessary facts about varieties, cyclic Post algebras, finite fields and Gröbner bases. In Section 3 we describe the constructive method to transform a field $\langle F(p^k); +, \cdot, F(p)\rangle$ into a k-cyclic Post algebra of order p, p prime, $k \geq 1$, and conversely the field operations as terms in the language of cyclic Post algebras, and give the interpretations stated above and proved in [1]. Finally in Section 4 we explain how we can solve an algebraic system of equations over a cyclic Post algebra of order p, p prime and illustrate the whole process with some examples.

2. Post Algebras, Galois Fields and Gröbner Bases

We give in this section some definitions, properties and proofs about varieties, finite fields, cyclic Post algebras and Gröbner bases which can be found in the literature.

For background material on varieties, the reader is referred to [8].

Given a class K of similar algebras, we denote the class of all subalgebras, homomorphic images and direct products respectively by $S(K)$, $H(K)$ and $P(K)$. We know that K is a *variety* if $H(K) \cup S(K) \cup P(K) \subseteq K$. We denote by $\mathcal{V}$ the variety generated by K (the least variety containing K). We denote in general, $\mathcal{V} = \mathrm{HSP}(K)$. If K is finite, say $K = \{A_1, \ldots, A_n\}$, then $\mathcal{V}$ will be denoted $\mathcal{V}(A_1, \ldots, A_n)$.

Epstein gave in [11] a definition equivalent to the following one.

DEFINITION 2.1. A Post algebra of order r, r an integer ≥ 2, is a system $\langle A; \wedge, \vee, \mathbf{0}, \mathbf{1}, \sim, \{C_i\}_{i=0}^{r-1}, \{e_i\}_{i=1}^{r-2}\rangle$, such that $\langle A; \wedge, \vee, \mathbf{0}, \mathbf{1}\rangle$ is a distributive lattice with $\mathbf{0}$ and $\mathbf{1}$; $\sim$, C_i are unary operations and e_i are nullary operations satisfying:

(1) $\sim\sim x = x$,
(2) $\sim (x \wedge y) = \sim x \vee \sim y, \quad \sim (x \vee y) = \sim x \wedge \sim y$,
(3) $C_i(x) \wedge C_j(x) = 0$ for $i \neq j$, and $\bigvee_{i=0}^{r-1} C_i(x) = \mathbf{1}$,
(4) $\mathbf{0} = e_0 \leq e_1 \leq \ldots \leq e_{r-1} = \mathbf{1}$,
(5) if $x \wedge e_1 = 0$ then $x = 0$,
(6) if $x \vee e_{i-1} = e_i$ then $x = e_i$,
(7) for every $x \in A$, $x = \bigvee_{i=0}^{r-1} C_i(x) \wedge e_i$.

It is known that if $B(A)$ is the Boolean algebra of complemented elements of A, then $x \in B$ if and only if $x = C_i(y)$ for some i and some $y \in A$.

The unary operations $C_i(x)$ are unique. This means that for any given $x \in A$ there is only one sequence of elements $C_0(x), C_1(x), \ldots, C_{r-1}(x)$ satisfying (3) and (7) of Definition 2.1.

The following example plays an important role. Let L_r be the set of all fractions $j/(r-1)$, with $j = 0, 1, \ldots, r-1$, considered as a sublattice of the real numbers, with $\sim (j/(r-1)) = 1 - j/(r-1)$ and $C_i(j/(r-1)) = 1$ if $j = i$ and $C_i(j/(r-1)) = 0$ otherwise. Then L_r is a Post algebra of order r, where $e_j = j/(r-1)$, $0 \leq j \leq r-1$.

The variety of Post algebras of order r is a discriminator variety (see [8]), generated by the chain of r elements. In particular, any finite Post algebra of order r is isomorphic to a direct product of copies of chains with r elements.

DEFINITION 2.2. A $k-$cyclic Post algebra of order r ($r \geq 2$, $k \geq 1$, r, k fixed) is a pair $\langle A; T\rangle$, where A is a Post algebra of order r and T is a Postian automorphism of A such that $T^k(x) = x$ for every $x \in A$.

Observe that the class of $k-$cyclic Post algebras of order r is equationally definable.

The set $(L_r)^k$ of all sequences $x = (x_1, x_2, \ldots, x_k)$, with $x_i \in L_r$ and with the pointwise defined operations, is also a Post algebra of order r. Defining $T(x_1, x_2, \ldots, x_k) = (x_k, x_1, x_2, \ldots, x_{k-1})$, we have that T is an automorphism of $(L_r)^k$ such that $T^k(x) = x$ for every $x \in (L_r)^k$. Then $\langle (L_r)^k; T\rangle$ is a $k-$cyclic Post algebra of order r. We will denote by $L_{r,k}$ the algebra $\langle (L_r)^k; T\rangle$, where T is the automorphism described above.

The simple algebras of the variety of all $k-$cyclic Post algebras of order r are isomorphic to the algebras $L_{r,d}$, with d a divisor of k [2].

Definition 2.3. Let F be an extension of a field K. An automorphism $\sigma : F \longrightarrow F$ is said to be a $K-$automorphism if $\sigma \mid_K = Id_K$. The group of all $K-$automorphisms of F is called the *Galois group* of F over K and it is denoted by $Aut_K F$.

If H is a subgroup of $Aut_K F$, the set $\{x \in F : \sigma(x) = x, \sigma \in H\}$ is called the *fixed field* of H.

If F is an extension of a field K such that the fixed field of the Galois group $Aut_K F$ is K, then F is called a *Galois extension* of K.

Theorem 2.4. **(The Normal Basis Theorem)** *Let F be a finite Galois extension of the field K, of degree n. Let $G = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ be the Galois group of F. Then there exists an element $w \in F$ such that $\{\sigma_1(w), \sigma_2(w), \ldots, \sigma_n(w)\}$ forms a basis of the $K-$ vector space F.*

For every prime p and every positive integer n, there exits a field having exactly p^n elements. Moreover any two fields of order p^n are isomorphic. The intersection F' of all subfields of F is called the *prime field* of F. If F has characteristic p, then $F' \cong Z_p$.

If $F = F(p^n)$ is a finite field with p^n elements, the multiplicative group $F \setminus \{0\} = \{\varepsilon, \varepsilon^2, \ldots, \varepsilon^{p^n-1} = 1\}$ is cyclic.

Definition 2.5. The mapping $\sigma : F(p^n) \longrightarrow F(p^n)$ defined by $\sigma(x) = x^p$ is a field automorphism, which is called the *Frobenius automorphism*. The group of automorphisms of $F(p^n)$ is cyclic of order n and σ is a generator.

We introduce now some concepts of Commutative Algebra. For background material on Gröbner bases, the reader is referred to [6, 10].

Given a system of polynomials in n variables over a field K,

$$f_1(x_1, \ldots, x_n) = 0$$

$$\vdots$$

$$f_m(x_1, \ldots, x_n) = 0$$

we are concerned with finding the common zeros of the f_i over some algebraically closed field $\bar{K}$ containing K.

Solving such systems of algebraic equations is one of the most challenging problems in Computer Algebra. The computational complexity of the problem is quite difficult to solve in practice. There is no hope to solve problems with more than 10 unknowns.

The *ideal generated by the f_i*, denoted by $(f_1, \ldots f_m)$, is the set of all linear combinations $f_1 g_1 + \ldots + f_m g_m$ where the g_i are arbitrary polynomials.

The *radical of the ideal* I is the ideal of all polynomial having a power in I. A *radical ideal* is an ideal which is its own radical.

If two sets of polynomials generate the same ideal, or generate ideals having the same radical, they have the same set of solutions. *Hilbert's Nullstellensatz*, an important result of the nineteenth century, asserts that the converse is true.

THEOREM 2.6. **(Hilbert's Nullstellensatz)** *Two systems of equations have the same set of solutions in an algebraic closed field if and only if the ideal generated by each of them have the same radical.*

Buchberger's algorithm for computing Gröbner bases is the first efficient one for solving algebraic systems. We begin recalling the notion of multivariate polynomial.

A polynomial is a sum of *terms*. Each term is the product of a *coefficient* and a *monomial* which is a product of powers of the variables. The *exponent* of a monomial (or of a term) is the vector of the exponents of each variable. Thus, the exponent of $x_1^{\alpha_1} \dots x_n^{\alpha_n}$ is $(\alpha_1, \dots \alpha_n)$, and the exponent of a constant monomial 1 is $(0, \dots, 0)$.

The *degree* of a monomial (or of a term) is the sum of the exponents of the variables. The degree of a polynomial is the biggest degree of its terms.

The terms are ordered by some total ordering on the coefficients. The first term for this ordering (the biggest one) is called the *leading term* and the corresponding monomial, exponent and coefficient are the *leading monomial*, the *leading exponent* and the *leading coefficient*. We will denote for a polynomial p, lmon(p), lterm(p), lexp(p) and lcoef(p).

The ordering on the monomials has to satisfy the following two axioms for any monomials m, n and p:

(a) $1 < m$ and

(b) $m < n \Leftrightarrow mp < np$.

These conditions imply that infinite decreasing sequences of monomials do not exist.

The most commonly orderings used are the following:

The *lexicographical ordering* (denoted by lex) for which the monomials are ordered by lexicographical ordering on the exponents, i.e.

$$(a_1, \dots, a_n) <_{lex} (b_1, \dots, b_n) \Leftrightarrow a_i < b_i \text{ for some } i, \text{ and } a_j = b_j \text{ for } j < i.$$

The *degree-lexicographical ordering* (denoted by glex) for which the degrees are compared first, and, lex is used in case of equality of degrees:

$$(a_1, \dots, a_n) <_{glex} (b_1, \dots, b_n) \Leftrightarrow a_1 + \dots + a_n < b_1 + \dots + b_n$$

$$or\ a_1 + \ldots + a_n = b_1 + \ldots + b_n\ and\ (a_1, \ldots, a_n) <_{lex} (b_1, \ldots, b_n).$$

The *degree reverse-lexicographical ordering* (denoted by rlex) for which the degrees are compared first, and then, in case of equality, the opposite of lex is used after reverting the ordering on the variables:

$$(a_1, \ldots, a_n) <_{rlex} (b_1, \ldots, b_n) \Leftrightarrow a_1 + \ldots + a_n < b_1 + \ldots + b_n$$

$$or\ a_1 + \ldots + a_n = b_1 + \ldots + b_n\ and\ (a_n, \ldots, a_1) >_{lex} (b_n, \ldots, b_1).$$

The latter of these orderings is generally the most efficient for the computation of Gröbner bases.

Definition 2.7. A *Gröbner basis* G of an ideal I for a fixed order on the monomials is a (finite) set of generators of I such that the leading monomials of the elements of I are exactly the multiples of the leading monomials of the members of G.

If G is a Gröbner basis, the monomials which are not multiple of a leading term in G are called *irreducible*.

A Gröbner basis is said *minimal* if none of its leading monomials is a multiple of another of them.

A Gröbner basis is said *reduced* if each polynomial in it is irreducible by the other ones, i.e. if the basis is minimal and if all not leading monomials in it are irreducible.

The Gröbner basis of an ideal for a fixed order is not unique, but the reduced Gröbner basis, which always exists, is unique.

As Gröbner bases are computable, many facts concerning polynomial systems are easily deduced from them.

The next theorem called *Weak Nullstellensatz* was the basis (and is equivalent to) the Hilbert Nullstellensatz.

Theorem 2.8. **(The Weak Nullstellensatz)** *A system of polynomial equations has an empty set of solutions if and only if the Gröbner bases of an ideal generated by the equations contains a constant polynomial, i.e. if* $\{1\}$ *is a reduced Gröbner basis for any ordering.*

The main algorithm for computing Gröbner bases is due to *Buchberger*, and was introduced in 1965 in his PhD. thesis. The reduction process and the definition of $S - polynomials$ are the main tools in the development.

Reducing a monomial m by a polynomial p consists in replacing m by $m - \frac{m}{lmon(p)} \frac{p}{lcoef(p)}$ if m is a multiple of the leading monomial $\mathrm{lmon}(p)$ of p,

or in doing nothing if it is not a multiple. *Reducing* a polynomial p by a set of polynomials S consists in reducing the monomials in p by the polynomials of S while it is possible. In the general case, the reduction depends on some choices, and, thus, the reduction has not uniquely defined result.

A polynomial lies in an ideal if and only if it is reduced to 0 by a Gröbner basis of an ideal.

Given two polynomials p and q, let m be the LCM of their leading monomials. Then, their *S-polynomial* is

$$lcoef(q)\frac{m}{lmon(p)}p - lcoef(p)\frac{m}{lmon(q)}q.$$

In other words it is the polynomial obtained by simplifying together the leading terms of p and q.

The Buchberger's algorithm consists in:
Start with a set S of polynomials
While this modify S,
compute the S-polynomial of two elements of S,
reduce it by S,
and, if the result of the reduction is not 0, add it to S
Remove the polynomials in S which have a leading monomial which is a multiple of
another leading monomial in S
Reduce the polynomials in S by the other elements of S
Return S

The algorithm described above has several improvements for an efficient implementation [6, 10]. However, the research in this field is active and many improvements are implemented in some systems without being published. In spite of these improvements, Gröbner bases computations need often very long computations and a lot of memory space. Thus further improvements are yet needed.

3. Interpretations

In this section we give the interpretation Φ_1 of the variety $\mathcal{V}(L_{p,k})$ generated by $L_{p,k}$ into the variety $\mathcal{V}(F(p^k))$ generated by $F(p^k)$ and an interpretation Φ_2 of $\mathcal{V}(F(p^k))$ into $\mathcal{V}(L_{p,k})$.

We obtain first an effective representation of any function on a finite field F as a polynomial with coefficients in F, and an effective representation of

any function on a finite cyclic Post algebra A as a (Post) polynomial with coefficients in A.

Given a structure of field $F = F(p^k)$ defined on a set with p^k elements, let $\langle F^{F^m}; +, \cdot\rangle$ be the ring of functions $f : F^m \to F$ where the operations $+$ and $\cdot$ are defined by

$(f+g)(x_1, x_2, \ldots, x_m) = f(x_1, x_2, \ldots, x_m) + g(x_1, x_2, \ldots, x_m)$,
$(f \cdot g)(x_1, x_2, \ldots, x_m) = f(x_1, x_2, \ldots, x_m) \cdot g(x_1, x_2, \ldots, x_m)$.

Let $\langle F[x_1, x_2, \ldots, x_m]; +, \cdot\rangle$ be the ring of all polynomials in m variables over the field F.

The proof of the following results can be seen in [1].

LEMMA 3.1. *Every function $f \in F^{F^m}$ can be uniquely represented as a polynomial of the form $\sum_i \lambda_i \cdot M_i$, with $i = (r_{i_1}, r_{i_2}, \ldots, r_{i_m}) \in ([0, p^k))^m$, $\lambda_i \in F$ and $M_i = x_1^{r_{i_1}} \cdot x_2^{r_{i_2}} \cdot \ldots \cdot x_m^{r_{i_m}}$.*

We can get an effective representation for each function as a polynomial by considering the following Lagrange polynomials in
$F(p^k) = \{0, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{p^k-1}\}$,

$$L_0(x) = (p-1)x^{p^k-1} + 1,$$

$$L_{\varepsilon^i}(x) = L_0(x + (p-1)\varepsilon^i).$$

As $x^{p^k} + (p-1)x = 0$, it follows that

$$L_0(x) = \begin{cases} 1 & \text{if } x = 0 \\ 0 & \text{if } x \neq 0 \end{cases} \quad \text{and} \quad L_{\varepsilon^i}(x) = \begin{cases} 1 & \text{if } x = \varepsilon^i \\ 0 & \text{if } x \neq \varepsilon^i \end{cases}.$$

So, for $f \in F^{F^m}$,

$$f(x_1, \ldots, x_m) = \sum_{(\alpha_1, \ldots, \alpha_m) \in F^m} f(\alpha_1, \cdots, \alpha_m) \cdot L_{\alpha_1}(x_1) \cdot \ldots \cdot L_{\alpha_m}(x_m). \qquad \text{(I)}$$

We consider now the simple $k-$cyclic Post algebra of order p, $L_{p,k} = \langle (L_p)^k; T\rangle$ and define the operations $\triangle$ and $\odot$ on $(L_p)^k$ as follows

$$C_i(x \triangle y) = \bigvee_{s+t \equiv i \ mod \ (p)} (C_s(x) \wedge C_t(y)),$$

$$C_i(x \odot y) = \bigvee_{s \cdot t \equiv -i \ mod \ (p)} (C_s(x) \wedge C_t(y)).$$

So, from (5) of Definition 2.1 we obtain

$$x \triangle y = \bigvee_{i=0}^{p-1} C_i(x \triangle y) \wedge e_i \quad \text{and} \quad x \odot y = \bigvee_{i=0}^{p-1} C_i(x \odot y) \wedge e_i.$$

PROPOSITION 3.2. *$\langle (L_p)^k; \triangle, \odot \rangle$ is a commutative ring with unit $e_{p-1} = \mathbf{1}$.*

LEMMA 3.3. *For $x \in (L_p)^k$, $px = \mathbf{0}$, $x^p = x$, $\sim x = \mathbf{1} \triangle (p-1)x$ and, over the chains of constants,*

$$e_i^{p-1} = \begin{cases} \mathbf{0} & \text{if } i = 0 \\ e_{p-1} = \mathbf{1} & \text{if } i \neq 0 \end{cases}.$$

On the set $\mathcal{F}_m((L_p)^k)$ of all functions $f : [(L_p)^k]^m \to (L_p)^k$ we can define a structure of ring by means of the following operations:

$$(f \triangle g)(x_1, x_2, \ldots, x_m) = f(x_1, x_2, \ldots, x_m) \triangle g(x_1, x_2, \ldots, x_m),$$
$$(f \odot g)(x_1, x_2, \ldots, x_m) = f(x_1, x_2, \ldots, x_m) \odot g(x_1, x_2, \ldots, x_m).$$

Let $\langle (L_p)^k[x_1, x_2, \ldots, x_m]; \triangle, \odot \rangle$ be the ring of all polynomials in m variables over the algebra $(L_p)^k$, that is, expressions of the form

$$\triangle_i \, \mu_i \odot N_i(x_1, x_2, \ldots, x_m),$$

where $\mu_i \in (L_p)^k$ and $N_i = \mathbf{1}$ or N_i is a formal expression of the form

$$(x_1)^{\alpha_{1,1}} \odot T(x_1)^{\alpha_{1,2}} \odot \ldots \odot T^{k-1}(x_1)^{\alpha_{1,k}} \odot$$
$$\odot (x_2)^{\alpha_{2,1}} \odot T(x_2)^{\alpha_{2,2}} \odot \ldots \odot T^{k-1}(x_2)^{\alpha_{2,k}} \odot \ldots$$
$$\ldots \odot (x_m)^{\alpha_{m,1}} \odot T(x_m)^{\alpha_{m,2}} \odot \ldots \odot T^{k-1}(x_m)^{\alpha_{m,k}},$$

where $\alpha_{i,j} \in \{0, 1, 2, \ldots, p-1\}$.

LEMMA 3.4. *Every function $f : [(L_p)^k]^m \to (L_p)^k$ can be uniquely represented as a polynomial of the form $\triangle_i \, \mu_i \odot N_i(x_1, x_2, \ldots, x_m)$ where $\mu_i \in (L_p)^k$ and $N_i = \mathbf{1}$ or N_i has the form*

$$(x_1)^{\alpha_{1,1}} \odot T(x_1)^{\alpha_{1,2}} \odot \ldots \odot T^{k-1}(x_1)^{\alpha_{1,k}} \odot$$
$$\odot (x_2)^{\alpha_{2,1}} \odot T(x_2)^{\alpha_{2,2}} \odot \ldots \odot T^{k-1}(x_2)^{\alpha_{2,k}} \odot \ldots$$
$$\ldots \odot (x_m)^{\alpha_{m,1}} \odot T(x_m)^{\alpha_{m,2}} \odot \ldots \odot T^{k-1}(x_m)^{\alpha_{m,k}},$$

where $\alpha_{i,j} \in \{0, 1, 2, \ldots, p-1\}$.

In the proof of the above Lemma we have the following formula [1]

$$f(x_1,\ldots,x_m) = \triangle_{(\alpha_1,\ldots,\alpha_m)\in A^m} f(\alpha_1,\ldots,\alpha_m)\odot\mathcal{L}_{\alpha_1}(x_1)\odot\cdots\odot\mathcal{L}_{\alpha_m}(x_m). \text{ (II)}$$

Thus we can obtain the field operations $+$ and $\cdot$ in terms of $\wedge$, $\vee$ and C_i.

We introduce now the definitions of interpretation and equivalence.

Definition 3.5. [15, 17] A variety $\mathcal{V}$ is *interpretable* in a variety $\mathcal{W}$ if for each $\mathcal{V}-$operation $F_t(x_1,\ldots,x_n)$ there is a $\mathcal{W}-$term $f_t(x_1,\ldots,x_n)$ such that if $\langle A; G_t\rangle$ is in $\mathcal{W}$, then $\langle A; f_t\rangle$ is in $\mathcal{V}$.

The constants in the language of $\mathcal{V}$ must be interpreted as constants in the language of $\mathcal{W}$. Intuitively, this means that each algebra in $\mathcal{W}$ can be turned into an algebra in $\mathcal{V}$ by defining the $\mathcal{V}-$operations applying a uniform procedure.

If $\langle A; G_t\rangle$ is any algebra and for each $\mathcal{V}-$operation $F_t(x_1,\ldots,x_n)$ there is a term $f_t(x_1,\ldots,x_n)$ in the language of $\langle A; G_t\rangle$ such that $\langle A; f_t\rangle$ is in $\mathcal{V}$, the terms $f_t(x_1,\ldots,x_n)$ define an interpretation of $\mathcal{V}$ in $\mathcal{V}(\langle A; G_t\rangle)$, the variety generated by the algebra $\langle A; G_t\rangle$. We have to observe that the evaluation of any term in an algebra B in $\mathcal{V}(\langle A; G_t\rangle)$, is determined by its evaluation in A and that both $\langle A; G_t\rangle$ and $\langle B; G_t\rangle$ satisfy the same equations. We have $\mathcal{V}(\langle A; G_t\rangle) \xrightarrow{\Phi} \mathcal{V}$, and we say that $\Phi(\langle A; G_t\rangle)$ is an interpretation of $\mathcal{V}$ in $\mathcal{V}(\langle A; G_t\rangle)$.

Definition 3.6. [17] An *equivalence* of the varieties $\mathcal{V}$ and $\mathcal{W}$ is a pair of interpretations Φ_1 of $\mathcal{V}$ in $\mathcal{W}$ and Φ_2 of $\mathcal{W}$ in $\mathcal{V}$ such that $\Phi_2\Phi_1 = Id_{\mathcal{V}}$ and $\Phi_1\Phi_2 = Id_{\mathcal{W}}$.

We can see that two varieties are equivalent if and only if they are term equivalent.

In the following theorem [1] we obtain a structure of k-cyclic Post algebra of order p isomorphic to $L_{p,k}$ from the field $F(p^k)$, and conversely.

Theorem 3.7. *Given a finite field $F(p^k)$ with p^k elements, there exists a structure of simple k-cyclic Post algebra of order p defined on $F(p^k)$ isomorphic to*

$L_{p,k} = \langle (L_p)^k; \wedge, \vee, \mathbf{0}, \mathbf{1}, \sim, \{C_i\}_{i=0}^{p-1}, \{e_i\}_{i=1}^{p-2}, T\rangle$, *such that*

1. *The constants e_i are the elements of the prime field $F(p)$.*
2. *The operations $\wedge$ and $\vee$ are polynomials in $F(p)[x_1, x_2]$ of the form $\sum_{i=1}^{p^{2k}} \lambda_i \cdot x_1^{r_{i_1}} \cdot x_2^{r_{i_2}}$, $\lambda_i \in F(p)$, and the operations $\sim$, C_i and T are polynomials in $F(p)[x]$ of the form $\sum_{i=1}^{p^k} \lambda_i \cdot x^{r_i}$, $\lambda_i \in F(p)$, uniquely determined under the conditions $r_{i_j} < p^k$ and $r_i < p^k$.*

3. *The operations $+$ and $\cdot$ are uniquely determined polynomials in $L_p[x_1, x_2]$ of the form $\triangle_i \ \mu_i \odot N_i(x_1, x_2)$ where $\mu_i \in \{e_0, \ldots, e_{p-1}\}$ and $N_i = \mathbf{1}$ or N_i is a product (with $\odot$ as product) of elements of the set $\{x_1, T(x_1), \ldots, T^{k-1}(x_1), x_2, T(x_2), \ldots, T^{k-1}(x_2)\}$.*

The following corollaries are consequence of Theorem 3.7 (see [17], Th. 4.140).

COROLLARY 3.8. *The varieties $\mathcal{V}(L_{p,k})$ and $\mathcal{V}(F(p^k))$ are equivalent, that is, there exists an interpretation Φ_1 of $\mathcal{V}(L_{p,k})$ in $\mathcal{V}(F(p^k))$ and an interpretation Φ_2 of $\mathcal{V}(F(p^k))$ in $\mathcal{V}(L_{p,k})$ such that $\Phi_2\Phi_1(B) = B$ for every $B \in \mathcal{V}(L_{p,k})$ and $\Phi_1\Phi_2(R) = R$ for every $R \in \mathcal{V}(F(p^k))$.*

COROLLARY 3.9. *Every function $f : [L_{p,k}]^n \to L_{p,k}$ commuting with T can be represented by a term in the language of $\mathcal{V}(L_{p,k})$. Similarly, every function $f : [F(p^k)]^n \to F(p^k)$ commuting with σ can be represented as a polynomial with coefficients in $F(p)$.*

In the proof of the previous theorem [1] we give a general procedure, using Lagrange polynomials, to obtain explicitly the cyclic Post operations as terms in the language of fields, and conversely. In particular, the algebras $L_{p,k}$ and $F(p^k)$ with constants $F(p)$ are term equivalent.

4. Systems of Algebraic Equations in n Unknowns

We introduce first the definition of postian polynomial in n variables and some useful results proved in [11, 22, 23].

DEFINITION 4.1. A postian polynomial in n variables over a Post algebra P of order r is an element f of the postian subalgebra generated in $P^{(P^n)}$ by the family of projections $(p_1, \ldots p_n)$, where $p_i(x_1, \ldots, x_n) = x_i$.

The reduction of a postian polynomial to a given form will be a powerful tool in the resolution of algebraic systems of equations.

THEOREM 4.2. **(Epstein)** *If f is a Post polynomial in n variables $x_1, \ldots, x_n$ then*

$$f(x_1, \ldots, x_n) = \bigvee_{0 \le i_j \le r-1} f(e_{i_1}, \ldots e_{i_n}) \wedge C_{i_1}(x_1) \wedge \ldots \wedge C_{i_n}(x_n).$$

The theorem mentioned above shows how the postian polynomial satisfies the normal disjunctive form theorem. Serfati proved in [22] that conversely,

every postian polynomial satisfying the normal disjunctive form belongs to the subalgebra generated by the family of the projections.

The set of all postian polynomial in n variables over a Post algebra P of order r is itself an r-Post algebra, denoted by $\Omega_n(P)$. If f is a postian polynomial, then $f(x) = 0$ is a postian algebraic equation.

The following theorem gives solutions of a postian polynomial f in one variable.

THEOREM 4.3. **(Serfati)** *A necessary and sufficient condition for the equation*

$$f(x) = \bigvee_{i=0}^{r-1} C_i(x) \wedge f(e_i) = 0 \qquad \text{(III)}$$

to be consistent is

$$\bigwedge_{i=0}^{r-1} f(e_i) = 0. \qquad \text{(C1)}$$

A solution of (III) *is then*

$$\hat{x} = \bigvee_{i=0}^{r-1} C_0(f(e_i)) \wedge e_i.$$

We call $\hat{x}$ a fundamental solution.

COROLLARY 4.4. *The postian components of the fundamental solution are:*

$$C_{r-1}(\hat{x}) = C_0(f(e_{r-1})), \qquad C_0(\hat{x}) = \bigwedge_{1 \le s \le r-1} \sim (C_0(f(e_s))$$

and, for $1 \le j \le r-2$,

$$C_j(\hat{x}) = C_0(f(e_j)) \wedge \bigwedge_{j+1 \le s \le r-1} \sim (C_0(f(e_s)).$$

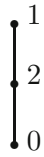
We will now be interested in the k-cyclic Post algebra of order p, $L_{p,k}$, with p prime. It is clear that applying Serfati's theorems we are able to find the solutions of a postian polynomial $f \in L_{p,k}[x]$ when the condition (C1) is satisfied. If the polynomial f doesn't verify (C1) we could find the zeros of f in an extension $L_{p,t}$ where the consistency condition is satisfied. We illustrate the process in the following example.

Let us consider the polynomial

$$f(x) = C_0(x) \vee (C_1(x) \wedge e_1) \vee (C_2(x) \wedge e_1) \in L_{3,1}.$$

As $e_2 \wedge e_1 \wedge e_1 \neq 0$ the polynomial f does not satisfy the condition (C1). Using the interpretation described in section 3 we can see it in $F(3)$.

Observe that the field $F(3) \cong Z_3 = \{0, 1, 2\}$. If we consider the order $0 < 2 < 1$, and the following unary operations C_0, C_1, C_2 we have the Post structure L_3 on the set $\{0, 1, 2\}$.



x	$C_0(x)$	$C_1(x)$	$C_2(x)$
0	1	0	0
2	0	1	0
1	0	0	1

Observe that the constants of the algebra are $e_0 = 0$, $e_1 = 2$ and $e_2 = 1$.

The Lagrange polynomials in $F(3)$ are

$$L_0(x) = 2x^2 + 1, \quad L_1(x) = 2x^2 + 2x, \quad \text{and} \quad L_2(x) = 2x^2 + x.$$

Hence we can use the formula (I) in order to express the operations $\wedge, \vee, \sim$, C_0, C_1, C_2 as terms in the language of fields, that is, in terms of the operations $+$ and $\cdot$ and the elements of the prime field $F(3)$.

The algorithms programmed in Maple have the following output:

$x \wedge y = x^2y^2 + 2x^2y + 2xy^2 + 2xy,$
$x \vee y = 2x^2y^2 + x^2y + xy^2 + xy + x + y,$
$\sim x = 2x + 1,$
$C_0(x) = 2x^2 + 1, \quad C_1(x) = 2x^2 + x, \quad C_2(x) = 2x^2 + 2x,$
$T(x) = x.$

Conversely, the Lagrange polynomials for the Post algebra $0 < 2 < 1$ are,

$\mathcal{L}_0(x) = (2 \odot x^2) \triangle 1,$
$\mathcal{L}_1(x) = (2 \odot x^2) \triangle (2 \odot x),$
$\mathcal{L}_2(x) = (2 \odot x^2) \triangle x,$

and by means of formula (II), the field operations $+$ and $\cdot$ can be expressed as

$x + y = x \triangle y$
$x \cdot y = x \odot y.$

(Recall that the operations $\triangle$ and $\odot$ are given in terms of $\wedge$, $\vee$ and the C_i).

Using another algorithm we obtain the polynomial in $F(3)$:

$$f(x) = x^2 + 1.$$

As we know it has all its zeros in the extension $F(3^2)$.

Now consider a field with 3^2 elements,

$$F(3^2) = F(3)[x]/(1 + x^2) = \{0, 1 + x, 2x, 1 + 2x, 2, 2 + 2x, x, 2 + x, 1\}.$$

Since $\varepsilon = 1 + x$ is a generator of the multiplicative group $F(3^2) \setminus \{0\}$, it follows that

$$F(3^2) = \{0, \varepsilon, \varepsilon^2, \varepsilon^3, \varepsilon^4, \varepsilon^5, \varepsilon^6, \varepsilon^7, \varepsilon^8\}.$$

Let σ be the Frobenius automorphism of $F(3^2)$, $\sigma(x) = x^3$.

By the Normal Basis Theorem, there exists $w \in F(3^2)$ such that $\{w, \sigma(w)\}$ is a basis of $F(3^2)$ as an $F(3)$-vector space. So, every $x \in F(3^2)$ can be written $x = \lambda_0(x)w + \lambda_1(x)\sigma(w)$, with $\lambda_0(x), \lambda_1(x) \in F(3)$. This element w can be any element in $F(3^2)$ that satisfies that (see [14])

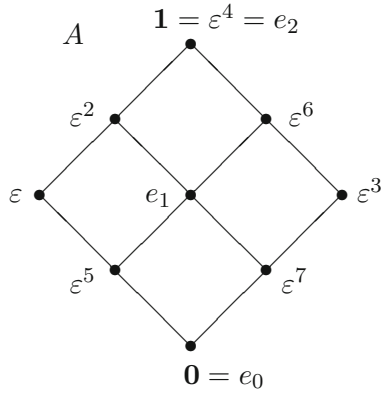
$$\begin{vmatrix} w & \varphi(w) \\ \varphi(w) & w \end{vmatrix} \neq 0.$$

Taking $w = \varepsilon$ we have the following identification.

$x \in F(3^2)$	0	ε	ε^2	ε^3	ε^4	ε^5	ε^6	ε^7	ε^8
$x =$ $\langle \lambda_0(x), \lambda_1(x) \rangle$	$\langle 0,0 \rangle$	$\langle 1,0 \rangle$	$\langle 1,2 \rangle$	$\langle 0,1 \rangle$	$\langle 1,1 \rangle$	$\langle 2,0 \rangle$	$\langle 2,1 \rangle$	$\langle 0,2 \rangle$	$\langle 2,2 \rangle$

We know that if we consider the ordering $0 < 2 < 1$ on $F(3)$ we obtain the Post algebra L_3. Now we state on $F(3^2)$ a structure of Post algebra A, where $A = L_3^2$ and $\wedge, \vee, \sim, C_0, C_1, C_2$ are defined componentwise, and the constants of A are $\mathbf{0} = e_0 = \langle 0,0 \rangle = 0$, $e_1 = \langle 2,2 \rangle = 1$ and $\mathbf{1} = e_2 = \langle 1,1 \rangle = 2$ (the constants are the elements of the prime field).

In addition, as $\sigma|_{F(3)} = id$, if we define $T = \sigma$ we obtain the following 2-cyclic Post algebra of order 3 $\langle A; T \rangle$ associated to the field $F(3^2)$.



$x \in F(3^2)$	$\sim x$	$T(x)$	$C_0(x)$	$C_1(x)$	$C_2(x)$
$0 = \langle 0,0\rangle$	$\langle 1,1\rangle$	$\langle 0,0\rangle$	$\langle 1,1\rangle$	$\langle 0,0\rangle$	$\langle 0,0\rangle$
$\varepsilon = \langle 1,0\rangle$	$\langle 0,1\rangle$	$\langle 0,1\rangle$	$\langle 0,1\rangle$	$\langle 0,0\rangle$	$\langle 1,0\rangle$
$\varepsilon^2 = \langle 1,2\rangle$	$\langle 0,2\rangle$	$\langle 2,1\rangle$	$\langle 0,0\rangle$	$\langle 0,1\rangle$	$\langle 1,0\rangle$
$\varepsilon^3 = \langle 0,1\rangle$	$\langle 1,0\rangle$	$\langle 1,0\rangle$	$\langle 1,0\rangle$	$\langle 0,0\rangle$	$\langle 0,1\rangle$
$\varepsilon^4 = \langle 1,1\rangle$	$\langle 0,0\rangle$	$\langle 1,1\rangle$	$\langle 0,0\rangle$	$\langle 0,0\rangle$	$\langle 1,1\rangle$
$\varepsilon^5 = \langle 2,0\rangle$	$\langle 2,1\rangle$	$\langle 0,2\rangle$	$\langle 0,1\rangle$	$\langle 1,0\rangle$	$\langle 0,0\rangle$
$\varepsilon^6 = \langle 2,1\rangle$	$\langle 2,0\rangle$	$\langle 1,2\rangle$	$\langle 0,0\rangle$	$\langle 1,0\rangle$	$\langle 0,1\rangle$
$\varepsilon^7 = \langle 0,2\rangle$	$\langle 1,2\rangle$	$\langle 2,0\rangle$	$\langle 1,0\rangle$	$\langle 0,1\rangle$	$\langle 0,0\rangle$
$\varepsilon^8 = \langle 2,2\rangle$	$\langle 2,2\rangle$	$\langle 2,2\rangle$	$\langle 0,0\rangle$	$\langle 1,1\rangle$	$\langle 0,0\rangle$

Now we will give the Post operations in terms of the operations of the field $F(3^2)$ and the elements of the prime field $F(3)$.

The Lagrange polynomials for $F(3^2)$ obtained with the corresponding algorithm are

$$L_0(x) = \varepsilon^4 x^8 + 1,$$
$$L_\varepsilon(x) = \varepsilon^4 x^8 + \varepsilon^5 x^7 + \varepsilon^6 x^6 + \varepsilon^7 x^5 + x^4 + \varepsilon x^3 + \varepsilon^2 x^2 + \varepsilon^3 x,$$
$$L_{\varepsilon^2}(x) = \varepsilon^4 x^8 + \varepsilon^6 x^7 + x^6 + \varepsilon^2 x^5 + \varepsilon^4 x^4 + \varepsilon^6 x^3 + x^2 + \varepsilon^2 x,$$
$$L_{\varepsilon^3}(x) = \varepsilon^4 x^8 + \varepsilon^7 x^7 + \varepsilon^2 x^6 + \varepsilon^5 x^5 + x^4 + \varepsilon^3 x^3 + \varepsilon^6 x^2 + \varepsilon x,$$
$$L_{\varepsilon^4}(x) = \varepsilon^4 x^8 + x^7 + \varepsilon^4 x^6 + x^5 + \varepsilon^4 x^4 + x^3 + \varepsilon^4 x^2 + x,$$
$$L_{\varepsilon^5}(x) = \varepsilon^4 x^8 + \varepsilon x^7 + \varepsilon^6 x^6 + \varepsilon^3 x^5 + x^4 + \varepsilon^5 x^3 + \varepsilon^2 x^2 + \varepsilon^7 x,$$
$$L_{\varepsilon^6}(x) = \varepsilon^4 x^8 + \varepsilon^2 x^7 + x^6 + \varepsilon^6 x^5 + \varepsilon^4 x^4 + \varepsilon^2 x^3 + x^2 + \varepsilon^6 x,$$
$$L_{\varepsilon^7}(x) = \varepsilon^4 x^8 + \varepsilon^3 x^7 + \varepsilon^2 x^6 + \varepsilon x^5 + x^4 + \varepsilon^7 x^3 + \varepsilon^6 x^2 + \varepsilon^5 x,$$
$$L_{\varepsilon^8}(x) = \varepsilon^4 x^8 + \varepsilon^4 x^7 + \varepsilon^4 x^6 + \varepsilon^4 x^5 + \varepsilon^4 x^4 + \varepsilon^4 x^3 + \varepsilon^4 x^2 + \varepsilon^4 x.$$

Applying formula (I) and using the necessary algorithms programmed in Maple we obtain:

$$\begin{aligned} x \wedge y &= x^6[y^6+2y^4+2y^3+2y^2]+x^4[2y^6+2y^4+y^2+2y] \\ &\quad + x^3[2y^6+y^3+y^2+2y]+x^2[2y^6+y^4+y^3+y^2] \\ &\quad + x[2y^4+2y^3+2y], \end{aligned}$$

$$\begin{aligned} x \vee y &= x^6[2y^6+y^4+y^3+y^2]+x^4[y^6+y^4+2y^2+y] \\ &\quad + x^3[y^6+2y^3+2y^2+y]+x^2[y^6+2y^4+2y^3+2y^2] \\ &\quad + x[y^4+y^3+y+1]+y, \end{aligned}$$

$$\begin{aligned} \sim x &= 2x+2, \\ C_0(x) &= x^6+x^4+2x^2+2, \\ C_1(x) &= x^6+x^4+2x^2+x, \\ C_2(x) &= x^6+x^4+2x^2+2x, \\ T(x) &= x^3. \end{aligned}$$

Similarly, the Lagrange polynomials for the 2−cyclic Post algebra A of order 3 are (we adopt the convention that in absence of parenthesis, $\odot$ is performed first, followed by $\triangle$)

$\mathcal{L}_0(x) = x^2 \odot (T(x))^2 \ \triangle \ e_1 \odot x^2 \ \triangle \ e_1 \odot (T(x))^2 \ \triangle \ \mathbf{1}$,
$\mathcal{L}_\varepsilon(x) = x^2 \odot (T(x))^2 \ \triangle \ x \odot (T(x))^2 \ \triangle \ e_1 \odot x^2 \ \triangle \ e_1 \odot x$,
$\mathcal{L}_{\varepsilon^2}(x) = x^2 \odot (T(x))^2 \ \triangle \ e_1 \odot x^2 \odot T(x) \ \triangle \ x \odot (T(x))^2 \ \triangle \ e_1 \odot x \odot T(x)$,
$\mathcal{L}_{\varepsilon^3}(x) = x^2 \odot (T(x))^2 \ \triangle \ x^2 \odot T(x) \ \triangle \ e_1 \odot (T(x))^2 \ \triangle \ e_1 \odot T(x)$,
$\mathcal{L}_{\varepsilon^4}(x) = x^2 \odot (T(x))^2 \ \triangle \ x^2 \odot T(x) \ \triangle \ x \odot (T(x))^2 \ \triangle \ x \odot T(x)$,
$\mathcal{L}_{\varepsilon^5}(x) = x^2 \odot (T(x))^2 \ \triangle \ e_1 \odot x \odot (T(x))^2 \ \triangle \ e_1 \odot x^2 \ \triangle \ x$,
$\mathcal{L}_{\varepsilon^6}(x) = x^2 \odot (T(x))^2 \ \triangle \ x^2 \odot T(x) \ \triangle \ e_1 \odot x \odot (T(x))^2 \ \triangle \ e_1 \odot x \odot T(x)$,
$\mathcal{L}_{\varepsilon^7}(x) = x^2 \odot (T(x))^2 \ \triangle \ e_1 \odot x^2 \odot T(x) \ \triangle \ e_1 \odot (T(x))^2 \ \triangle \ T(x)$,
$\mathcal{L}_{\varepsilon^8}(x) = x^2 \odot (T(x))^2 \ \triangle \ e_1 \odot x^2 \odot T(x) \ \triangle \ e_1 \odot x \odot (T(x))^2 \ \triangle \ x \odot T(x)$.

By formula (II), we have that

$$x + y = x \ \triangle \ y,$$

and

$$x \cdot y = T(x) \odot y \ \triangle \ x \odot y \ \triangle \ x \odot T(y) \ \triangle \ e_1 \odot T(x) \odot T(y).$$

Now, we are able to see the postian polynomial x^2+1 in $L_{3,2}$.

The algorithm programmed in Maple gives us the polynomial

$$f(x) = (C_0(x) \wedge C_0(Tx) \wedge e_1) \vee (C_0(x) \wedge C_1(Tx)) \vee (C_0(x) \wedge C_2(Tx)) \vee$$

$$\vee (C_1(x) \wedge C_1(Tx)) \vee (C_2(x) \wedge C_2(Tx))$$

As $f(x)$ satisfies the condition (C1) the algebraic equation is consistent and vanishes in $\langle 1, 2\rangle$ and $\langle 2, 1\rangle$, which are the roots ε^2 and ε^6 of $f(x) = x^2 + 1 \in F(3^2)$.

Let now turn our attention to algebraic systems of equations.

Serfati studies in [23] the algebraic equation in n unknowns of the form

$$f(x_1, \ldots, x_n) = 0,$$

where f is a postian polynomial over a Post algebra of order r. He first gives a consistency condition in the following theorem:

THEOREM 4.5. *A necessary and sufficient condition for the equation*

$$f(x_1, \ldots, x_n) = \bigvee_{0 \le i_j \le r-1} f(e_{i_1}, \ldots e_{i_n}) \wedge C_{i_1}(x_1) \wedge \ldots \wedge C_{i_n}(x_n) = 0$$

to be consistent is

$$\bigwedge_{0 \le i_j \le r-1} f(e_{i_1}, \ldots, e_{i_n}) = 0 \qquad \text{(C2)}$$

He proposes for the complete solution a procedure of succesive eliminations.

Assuming (C2) is fullfilled he solves the algebraic equation in n unknowns

$$f(x_1, \ldots, x_n) = 0$$

as follows.
Writing the postian polynomial as an equation relative to x_1,

$$\bigvee_{0 \le i_1 \le r-1} C_{i_1}(x_1) \wedge \bigvee_{0 \le i_j \le r-1} (C_{i_2}(x_2) \wedge \ldots \wedge C_{i_n}(x_n) \wedge f(e_{i_1}, \ldots, e_{i_n})) = 0$$

and eliminating x_1 leads to the algebraic equation in $n-1$ unknowns

$$g_1(x_2, \ldots, x_n) = 0.$$

Repeating the procedure, we get the algebraic equation in one unknown $g_{n-1}(x_n) = 0$. Each solution of the last equation must be substituted into $g_{n-2}(x_{n-1}, x_n)$. This is an effective method inspired from boolean methods.

The second method proposed by Serfati in [22] is inspired in Löwenhein style for boolean polynomials. It provides a general reproductive solution for a postian algebraic equation when some specified solution is known.

THEOREM 4.6. *Let* $f \in \Omega_n(P)$,

$$f(x) = 0$$

be the algebraic equation in one unknown and $u \in P^n$ *a specified solution of* f. *Then the general solution of* f *can be written in the following form*

$$x = \sim (C_0(f(p))) \wedge u \vee C_0(f(p)) \wedge p = \varphi(p) \qquad \text{(IV)},$$

where p *is some parameter in* P^n. *Moreover, relation* (IV) *defines a reproductive solution of* f, *that is for every* x, $\varphi(x) = x$.

The following result due to Serfati [23] describes completely the form of uniquely solvable postian equations:

THEOREM 4.7. *Let* $f \in \Omega_n(P)$, $0 \leq i \leq r-1$ *and* $x = (x_1, \ldots, x_n)$. *The following two conditions are equivalent:*

(1) *The equation* $f(x) = e_i$ *has a unique solution.*
(2) $C_i(f)$ *has the form:* $C_i(f(x)) = \bigwedge_{k=1}^{n} \bigvee_{i=0}^{r-1} (C_i(a_k) \wedge C_i(b_k))$, *for some* $a = (a_1, \ldots, a_n)$ *in* P^n.

We propose in this paper an interesting method to analyze how we could attack the resolution of an algebraic system of equations in the variety of k-cyclic Post algebras of order p, p prime, when the complexity of the problem allows us to do it.

We must see first if each algebraic equation satisfies (C2) and then decide which is the best way to find the solutions. If all of them satisfy it, using the interpretation described in section 3 and the help of some algorithms programmed in Maple, we could see all the algebraic equations in the field $F(p^k)$. In section 2 we presented some useful tools of Conmutative Algebra which let us deal with the problem of solving a system of polynomial in several variables. Looking for a Gröbner basis of the ideal I generated by all the equations of the system in a monomial order, we are able to know if the set of solutions is not empty, and if the answer is yes, find them in the easiest way. Finally the solutions could be seen in $L_{p,k}$.

In the case where an equation doesn't satisfy (C2) we have to see it in $F(p^k)$ and find an extension $F(p^t)$ of $F(p^k)$ where it is solvable. After analyzing all of them we have the biggest extension $F(p^l)$ where every equation has solution and we are able to study the solution of the system in the same way as above.

Let us illustrate the procedure with some examples.

Example 1: We saw above that in the system of equations in $L_{3,1}[x, y]$:

$f(x) = C_0(x) \vee (C_1(x) \wedge e_1) \vee (C_2(x) \wedge e_1)$
$g(x, y) = (C_1(x) \wedge C_2(y) \wedge e_1) \vee (C_2(x) \wedge C_1(y) \wedge e_1) \vee (C_1(x) \wedge C_1(y)) \vee (C_2(x) \wedge C_2(y))$,

the postian polynomial f does not satisfy the condition (C1), and found an extension of it in $L_{3,2}$ where we were able to find the zeros of f.

As the equation $g(x, y) = 0$ satisfies (C2) we could solve the problem

$f(x) = 0$
$g(x, y) = 0$ in $F(3^2)$.

The equivalent system is

$f(x) = x^2 + 1$
$g(x, y) = x \cdot y$

The Gröbner basis of the ideal $I = (x \cdot y, x^2 + 1)$, is

$$GB = \{y, x^2 + 1\},$$

and so the original system is equivalent to

$f(x) = x^2 + 1$
$h(y) = y$,

which has the same solution set in an extension $F(3^2)$ of $F(3)$,

$\{(\epsilon^2, 0), (\epsilon^6, 0)\}$.

The algorithm gives us the original polynomials in $L_{3,2}$.

$$g(x, y) = \{[(C_2(x) \wedge C_2(Tx) \wedge C_2(y)) \vee (C_1(x) \wedge C_1(Tx)) \wedge C_1(y))\vee$$
$$\vee(C_2(x) \wedge C_1(Tx) \wedge C_2(Ty)) \vee (C_1(x) \wedge C_2T(x) \wedge C_1(T(y))\vee$$
$$\vee(C_0(x) \wedge C_2T(x) \wedge C_0(y) \wedge C_2(T(y)) \vee (C_0(x) \wedge C_1T(x) \wedge C_0(y)) \wedge C_1(T(y))\vee$$
$$\vee(C_1(x) \wedge C_0T(x) \wedge C_0(y) \wedge C_2(T(y)) \vee (C_2(x) \wedge C_0T(x) \wedge C_0(y) \wedge C_1(T(y))\vee$$
$$\vee(C_0(x) \wedge C_1T(x) \wedge C_2(y) \wedge C_0(T(y)) \vee (C_1(x) \wedge C_0T(x) \wedge C_2(y) \wedge C_0(T(y))\vee$$

$$\vee(C_2(x)\wedge C_0T(x)\wedge C_1(y)\wedge C_0(T(y))\vee(C_0(x)\wedge C_2T(x)\wedge C_1(y)\wedge C_0(T(y))\vee$$
$$\vee(C_1(x)\wedge C_0T(x)\wedge C_1(y)\wedge C_1(T(y))\vee(C_2(x)\wedge C_0T(x)\wedge C_2(y)\wedge C_2(T(y))\vee$$
$$\vee(C_0(x)\wedge C_1T(x)\wedge C_1(y)\wedge C_2(T(y))\vee(C_0(x)\wedge C_2T(x)\wedge C_2(y)\wedge C_1(T(y))]\wedge e_1\}\vee$$
$$[(C_2(x)\wedge C_1(Tx)\wedge C_1(Ty))\vee(C_1(x)\wedge C_2(Tx)\wedge C_2(Ty))\vee$$
$$(C_2(x)\wedge C_2(Tx)\wedge C_1(y))\vee(C_1(x)\wedge C_1(Tx)\wedge C_2(y))\vee$$
$$(C_0(x)\wedge C_2(Tx)\wedge C_0(y))\wedge C_1(Ty))\vee(C_0(x)\wedge C_1(Tx)\wedge C_0(y))\wedge C_2(Ty))\vee$$
$$(C_0(x)\wedge C_1(Tx)\wedge C_2(y))\wedge C_1(Ty))\vee(C_0(x)\wedge C_2(Tx)\wedge C_1(y))\wedge C_2(Ty))\vee$$
$$(C_1(x)\wedge C_0(Tx)\wedge C_0(y))\wedge C_1(Ty))\vee(C_2(x)\wedge C_0(Tx)\wedge C_0(y))\wedge C_2(Ty))\vee$$
$$(C_1(x)\wedge C_0(Tx)\wedge C_2(y))\wedge C_2(Ty))\vee(C_2(x)\wedge C_0(Tx)\wedge C_1(y))\wedge C_1(Ty))\vee$$
$$(C_1(x)\wedge C_0(Tx)\wedge C_1(y))\wedge C_0(Ty))\vee(C_2(x)\wedge C_0(Tx)\wedge C_2(y))\wedge C_0(Ty))\vee$$
$$(C_0(x)\wedge C_1(Tx)\wedge C_1(y))\wedge C_0(Ty))\vee(C_0(x)\wedge C_2(Tx)\wedge C_2(y))\wedge C_0(Ty))]$$

$$f(x)=(C_0(x)\wedge C_0(Tx)\wedge e_1)\vee(C_0(x)\wedge C_1(Tx))\vee(C_0(x)\wedge C_2(Tx))\vee$$
$$\vee(C_1(x)\wedge C_1(Tx))\vee(C_2(x)\wedge C_2(Tx))$$

and the system has the same set of solutions in $L_{3,2}$ as the following one

$f(x)=(C_0(x)\wedge C_0(Tx)\wedge e_1)\vee(C_0(x)\wedge C_1(Tx))\vee(C_0(x)\wedge C_2(Tx))\vee(C_1(x)\wedge C_1(Tx))\vee$
$\vee(C_2(x)\wedge C_2(Tx))=0$
$h(y)=(C_1(y)\wedge e_1)\vee C_2(y)=0$

a much easier system to solve with solutions

$$x=(1,2),\ y=(0,0);\qquad\qquad x=(2,1),\ y=(0,0)$$

Example 2: This example is a system with an empty set of solutions.

Let f,g be polynomials in $F(3)[x,y]$ where

$f(x,y)=C_0(x)\vee C_0(y)\vee(C_1(x)\wedge C_1(y)\wedge e_1)\vee(C_2(x)\wedge C_2(y)\wedge e_1)$
$g(x,y)=(C_1(x)\wedge C_2(y)\wedge e_1)\vee(C_2(x)\wedge C_1(y)\wedge e_1)\vee(C_1(x)\wedge C_1(y))\vee(C_2(x)\wedge C_2(y))$

Both equations satisfy (C1) and the equivalent system in $F(3)[x,y]$ is

$f(x,y)=x\cdot y+1=0$
$g(x,y)=x\cdot y=0$
A Gröbner basis of the ideal $I=(x\cdot y,x\cdot y+1)$ is

$$GB=\{1\}$$

By theorem 2.8 the system has an empty set of solutions in any extension $L_{3,k}$.

Example 3: We may have a system of polynomials with complicated expressions as the following example.

$$f_1(x) = (C_1(x) \wedge C_0(T(x)) \wedge e_1) \vee (C_1(x) \wedge C_2(T(x)) \wedge e_1) \vee (C_0(x) \wedge e_1) \vee (C_2(x) \wedge e_1) \vee$$

$$(C_2(x) \wedge C_0(T(x)) \vee (C_2(x) \wedge C_1(T(x))) \vee (C_0(x) \wedge C_2(T(x))) \vee (C_0(x) \wedge C_1(T(x)))$$

$$f_2(x,y) = \{[(C_2(x) \wedge C_2(Tx) \wedge C_2(y)) \vee (C_1(x) \wedge C_1(Tx)) \wedge C_1(y)) \vee$$
$$\vee (C_2(x) \wedge C_1(Tx) \wedge C_2(Ty)) \vee (C_1(x) \wedge C_2T(x) \wedge C_1(T(y)) \vee$$
$$\vee (C_0(x) \wedge C_2T(x) \wedge C_0(y) \wedge C_2(T(y)) \vee (C_0(x) \wedge C_1T(x) \wedge C_0(y)) \wedge C_1(T(y)) \vee$$
$$\vee (C_1(x) \wedge C_0T(x) \wedge C_0(y) \wedge C_2(T(y)) \vee (C_2(x) \wedge C_0T(x) \wedge C_0(y) \wedge C_1(T(y)) \vee$$
$$\vee (C_0(x) \wedge C_1T(x) \wedge C_2(y) \wedge C_0(T(y)) \vee (C_1(x) \wedge C_0T(x) \wedge C_2(y) \wedge C_0(T(y)) \vee$$
$$\vee (C_2(x) \wedge C_0T(x) \wedge C_1(y) \wedge C_0(T(y)) \vee (C_0(x) \wedge C_2T(x) \wedge C_1(y) \wedge C_0(T(y)) \vee$$
$$\vee (C_1(x) \wedge C_0T(x) \wedge C_1(y) \wedge C_1(T(y)) \vee (C_2(x) \wedge C_0T(x) \wedge C_2(y) \wedge C_2(T(y)) \vee$$
$$\vee (C_0(x) \wedge C_1T(x) \wedge C_1(y) \wedge C_2(T(y)) \vee (C_0(x) \wedge C_2T(x) \wedge C_2(y) \wedge C_1(T(y))] \wedge e_1\} \vee$$
$$\vee [(C_2(x) \wedge C_1(Tx) \wedge C_1(Ty)) \vee (C_1(x) \wedge C_2(Tx) \wedge C_2(Ty)) \vee$$
$$\vee (C_2(x) \wedge C_2(Tx) \wedge C_1(y)) \vee (C_1(x) \wedge C_1(Tx) \wedge C_2(y)) \vee$$
$$\vee (C_0(x) \wedge C_2(Tx) \wedge C_0(y)) \wedge C_1(Ty)) \vee (C_0(x) \wedge C_1(Tx) \wedge C_0(y)) \wedge C_2(Ty)) \vee$$
$$\vee (C_0(x) \wedge C_1(Tx) \wedge C_2(y)) \wedge C_1(Ty)) \vee (C_0(x) \wedge C_2(Tx) \wedge C_1(y)) \wedge C_2(Ty)) \vee$$
$$\vee (C_1(x) \wedge C_0(Tx) \wedge C_0(y)) \wedge C_1(Ty)) \vee (C_2(x) \wedge C_0(Tx) \wedge C_0(y)) \wedge C_2(Ty)) \vee$$
$$\vee (C_1(x) \wedge C_0(Tx) \wedge C_2(y)) \wedge C_2(Ty)) \vee (C_2(x) \wedge C_0(Tx) \wedge C_1(y)) \wedge C_1(Ty)) \vee$$
$$\vee (C_1(x) \wedge C_0(Tx) \wedge C_1(y)) \wedge C_0(Ty)) \vee (C_2(x) \wedge C_0(Tx) \wedge C_2(y)) \wedge C_0(Ty)) \vee$$
$$\vee (C_0(x) \wedge C_1(Tx) \wedge C_1(y)) \wedge C_0(Ty)) \vee (C_0(x) \wedge C_2(Tx) \wedge C_2(y)) \wedge C_0(Ty))]$$

$$f_3(y) = \{[(C_0(y) \wedge C_2(T(y)) \vee (C_0(y) \wedge C_1(T(y)) \vee (C_2(y) \wedge C_1(T(y)) \vee$$
$$\vee (C_2(y) \wedge C_0(T(y))] \wedge e_1\} \vee (C_1(y) \wedge C_1(T(y))$$

$$f_4(y) = \{[(C_0(y) \wedge C_2(T(y)) \vee (C_0(y) \wedge C_1(T(y)) \vee (C_1(y) \wedge C_1(T(y)) \vee$$
$$\vee (C_2(y) \wedge C_2(T(y))] \wedge e_1\} \vee (C_1(y) \wedge C_2(T(y)) \vee (C_2(y) \wedge C_1(T(y)) \vee$$
$$\vee (C_1(y) \wedge C_0(T(y)) \vee (C_2(y) \wedge C_0(T(y))$$

We look for the solution set of the system

$$f_1(x) = 0$$
$$f_2(x, y) = 0$$
$$f_3(y) = 0$$
$$f_4(y) = 0.$$

All equations satisfy conditions (C1) or (C2), and the equivalent system in $F(3^2)[x, y]$ is

$f_1(x) = x^2 + x + 1$
$f_2(x, y) = x \cdot y$
$f_3(y) = y^2 + y$
$f_4(y) = y^2.$

A Gröbner basis of the ideal $I = (x^2 + x + 1, x \cdot y, y^2 + y, y^2)$ is

$$GB = \{y, x^2 + x + 1\}$$

so the system has the same solutions as the following one

$f(x) = x^2 + x + 1$
$g(y) = y,$

and we obtain applying Theorem 3.7 the equivalent one in $L_{3,2}$

$f(x) = (C_1(x) \wedge C_0(T(x)) \wedge e_1) \vee (C_1(x) \wedge C_2(T(x)) \wedge e_1) \vee (C_0(x) \wedge e_1) \vee (C_2(x) \wedge e_1) \vee$
$\vee (C_2(x) \wedge C_0(T(x)) \vee (C_2(x) \wedge C_1(T(x))) \vee (C_0(x) \wedge C_2(T(x))) \vee (C_0(x) \wedge C_1(T(x)))$
$g(y) = (C_1(x) \wedge e_1) \vee C_2(y)$

a very simple system with a double solution

$$x = (2, 2),\ y = (0, 0).$$

Acknowledgement. We would like to thank Walter Reartes for introducing us to Maple programming.

References

[1] Abad, M., J. P. Díaz Varela, B. F. López Martinolich, M. C. Vannicola, and M. Zander, 'An Equivalence between Varieties of Cyclic Post Algebras and Varieties generated by a Finite Field', *Central European Journal of Mathematics* 4:547–561, 2006.

[2] Abad, M., 'Cyclic Post algebras of order n', *An. Acad. Brasil. Ciênc.* 53(2):243–246, 1981.

[3] Adams, W., and P. Loustaunau, *An Introduction to Gröbner Bases*, Graduate Studies in Mathematics, 3, AMS, Providence, 1994.

[4] Allgower, E. L., and K. Georg, *Computational Solution of Nonlinear Systems of Equations*, Lectures in Applied Mathematics, 26, AMS, 1990.

[5] Balbes, R., and P. Dwinger, *Distributive Lattices*, University of Missouri Press, Columbia, MO., 1974.

[6] Becker, T., and V. Weispfenning, *Gröbner Bases*, Graduate Texts in Mathematics 141, Springer-Verlag, 1993.

[7] Boicescu, V., A. Filipoiu, G. Georgescu and S. Rudeanu, *Lukasiewicz-Moisil Algebras*, Annals of Discrete Mathematics, 49, North-Holland, Amsterdam, 1991.

[8] Burris, S., and H. Sankappanavar, *A Course in Universal Algebra*, Graduate Texts in Mathematics, 78, Springer, Berlin, 1981.

[9] Cendra, H., 'Cyclic Boolean algebras and Galois fields $F(2^k)$', *Portugal. Math.* 39, 1-4:435–440, 1980.

[10] Cox, D., J. Little, and D. O'Shea, *Ideals, Varieties and Algorithms*, Undergraduate Texts in Mathematics, Springer-Verlag, 1992, 1997.

[11] Epstein, G., 'The lattice theory of Post algebras', *Trans. Amer. Math. Soc.* 95:300–317, 1960.

[12] Kaarly, K., and A. F. Pixley, *Polynomial Completeness in Algebraic Systems*, Chapman and Hall, Boca Raton, 2001.

[13] Kunz, E., *Introduction to Commutative Algebra and Algebraic Geometry*, Birkhäuser, Boston, 1985.

[14] Lang, S., *Algebra*, Addison-Wesley Publishing Company, CA., 1984.

[15] Lewin, R., 'Interpretability into Łukasiewicz algebras', *Rev. Un. Mat. Argentina* 41(3):81–98, 1999.

[16] López Martinolich, B. F., *Resolución de Sistemas de Ecuaciones Polinomiales*, Tesis de magister, Universidad Nacional del Sur, 1998.

[17] McKenzie, R., G. McNulty, and W. Taylor, *Algebras, Lattices, Varieties, Vol. I*, Wadsworth and Brooks, Monterey, CA, 1987.

[18] Monteiro, A., 'Algèbres de Boole cycliques', *Rev. Roumaine de Mathématiques Pures Appl.* 23(1):71–76, 1978.

[19] Moisil, G., 'Algebra schemelor cu elemente ventil', *Revista Universitatii C.I. Parhon*, Bucharest, Seria St. nat. 4-5:9–15, 1954.

[20] Moisil, G., 'Algèbres universelles et automates', in *Essais sur les Logiques non Chrysippiennes*, Editions de L'Academie de la Republique Socialiste de Roumanie, Bucharest, 1972.

[21] Rudeanu, S., *Boolean functions and equations*. North-Holland Publishing Co., Amsterdam-London; American Elsevier Publishing Co., Inc., New York, 1974.
[22] Serfati, M., *Introduction aux Algèbres de Post et à leurs applications (logiques à r valeurs-équations postiennes-graphoïdes orientés)*, Cahiers du Bureau Universitaire de Recherche Opérationnelle Université Paris VI. Série Recherche, 21:35–42, 1973.
[23] Serfati, M., 'On Postian Algebraic Equations', *Discrete Math.* 152:269–285, 1996.

José Patricio Díaz Varela
Departamento de Matemática
Universidad Nacional del Sur
Alem 1253
Bahía Blanca (8000), Argentina
usdiavar@criba.edu.ar

Blanca Fernanda López Martinolich
Departamento de Matemática
Universidad Nacional del Comahue
Buenos Aires 1400
Neuquén (8300), Argentina
martinol@uncoma.edu.ar