MATEMÁTICAS

ORTHOGONAL SYSTEMS AND PERMUTATION POLYNOMIAL VECTORS OVER MODULAR ALGEBRAS

Pablo A. Acosta-Solarte*, Víctor S. Albis**

Abstract

Acosta–Solarte, Pablo A. & Víctor S. Albis: Orthogonal systems and permutation polynomial vectors over modular algebras. Rev. Acad. Colomb. Cienc. **36** (139): 237–242, 2012. ISSN 0370-3908.

Known results on orthogonal systems and permutation polynomials vectors over finite fields are extended to modular algebras of the form $L_\nu = K[X]/(p(X)^\nu)$, where K is a finite field, $p(X) \in K[X]$ is an irreducible polynomial, $\nu = 1, 2, \ldots$, and to the algebra of formal power series $L[[Z]]$, where $L_1 = K[X]/(p(X)) = L$.

Key words: Permutation polynomial, orthogonal systems, permutation polynomial vectors.

Resumen

Resultados sobre sistemas ortogonales y vectores de polinomios de permutación se extienden a las álgebras modulares de la forma $L_\nu = K[X]/(p(X)^\nu)$, donde K es un cuerpo finito, $p(X) \in K[X]$ un polinomio irreducible, $\nu = 1, 2, \ldots$ y al álgebra de las series potenciales formales $L[[Z]]$, donde $L_1 = K[X]/(p(X)) = L$.

Palabras clave: Polinomio de permutación, sistemas ortogonales, vectores de polinomios de permutación.

*Universidad Distrital Francisco José de Caldas, Bogotá, Colombia. Email: paacostas@udistrital.edu.co
**Universidad Nacional de Colombia, Bogotá, Colombia. Email: valbis@accefyn.org.co
AMS Classification 2010: 13B25, 13F25, 11T55.

1. Introduction.

Let K be a finite field, $K[X]$ its ring of polynomials and $p(X) \in K[X]$ an irreducible monic polynomial. It is known that $L = K[X]/(p(X))$ is a finite field and that $L_\nu = K[X]/(p(X)^\nu)$, $\nu = 1, 2, \ldots$, are $L-$algebras (see infra for details). In previous papers ([1] and [2]) the authors obtained results about permutation polynomial over the $L-$algebras $L[[Z]]$ (formal series over L) and L_ν, analogous to some known results over finite fields, Galois rings $GR(p^m, k)$ and the rings $\mathbb{Z}/p^n\mathbb{Z}$ (see, for example, [5], [7], [8], [10], [13] and [14]). Permutation polynomial, find applications currently in cryptography and coding theory (see [4] for more references).

In this paper we deal with systems of polynomials in $L[[Z]]$ and L_ν, obtaining results than in some cases lead to construct new permutation polynomials. The systems we are interested in are know as orthogonal systems and permutation polynomial vectors. These systems has being studied by Niederreiter in [6] when the coefficients of the polynomials are in finite fields. Moreover, Wei & Zhang in [12] and Shiue, Sun & Zhang in [8] extended some of these results to certain finite rings.

2. Preliminaries.

In this section we recall some properties of L_ν and $L[[Z]]$ needed for the best understanding of what follows (see [3], [9]). Here the elements of L_ν will be denoted by

$$\boldsymbol{\alpha}(z_\nu) = \alpha_0 + \alpha_1 z_\nu + \alpha_2 z_\nu^2 + \ldots + \alpha_{\nu-1} z_\nu^{\nu-1}, \ (\nu = 2, \ldots)$$

wher z_ν is the class of equivalence $p(X)$ modulo $p(X)^\nu$. The elements of L will simply be denote by α. It is known that

$$L[[Z]] = \left\{ \alpha(Z) = \sum_{i=0}^{\infty} \alpha_i Z^i ; \alpha_i \in L \right\}$$

is a local ring with maximal ideal (Z), and

$$(0) \subset \ldots \subset (Z^\nu) \subset \ldots \subset (Z^2) \subset (Z)$$

are the only ideals of $L[[Z]]$. Also, $L[[Z]]/(Z^\nu) \approx L_\nu$, and L_ν is a finite ring with q^ν elements, $(\nu = 1, 2, \ldots,)$ when L has q elements. Thus $L[[Z]]$ is the projective limit of the projective system of $L-$algebras $(L_\mu, (\pi_{\nu,\mu})_{\nu \le \mu})$, where

$$\pi_{\nu,\mu} : L_\mu \longrightarrow L_\nu$$

$$\boldsymbol{\alpha}(z_\mu) = \sum_{i=0}^{\mu-1} \alpha_i z_\mu^i \overset{\pi_{\nu,\mu}}{\longmapsto} \boldsymbol{\alpha}(z_\nu) = \sum_{i=0}^{\nu-1} \alpha_i z_\nu^i$$

and

$$\pi_\nu : L[[Z]] \longrightarrow L_\nu$$

$$\alpha(Z) = \sum_{i=0}^{\infty} \alpha_i Z^i \overset{\pi_\nu}{\longmapsto} \boldsymbol{\alpha}(z_\nu) = \sum_{i=0}^{\nu-1} \alpha_i z_\nu^i.$$

is the canonical projection.

If $f(t_1, \ldots, t_n) \in L[[Z]]$, its *reduction* $f_\nu(t_1, \ldots, t_n)$ modulo (Z^ν) is the polynomial in $L_\nu[t_1, \ldots, t_n]$ whose coefficients are the classes modulo (Z^ν) of the coefficients of $f(t_1, \ldots, t_n)$. Clearly, if $\nu \le \mu$, $\pi_{\nu,\mu}(f_\mu(t_1, \ldots, t_n)) = f_\nu(t_1, \ldots, t_n)$.

If

$$\boldsymbol{\tau}_\mu = \left(\sum_{i=0}^{\mu-1} \tau_{1,i} z_\mu^i, \ldots, \sum_{i=0}^{\mu-1} \tau_{n,i} z_\mu^i \right) \in L_\mu^n$$

is a zero of $f_\mu(t_1, \ldots, t_n)$ and $\nu \le \mu$, we say that $\boldsymbol{\tau}_\mu$ is a *descendant* of $\boldsymbol{\tau}_\nu$ if $\pi_{\nu,\mu}(\boldsymbol{\tau}_\mu) = \boldsymbol{\tau}_\nu$; obviously, if that is the case, $f_\nu(\boldsymbol{\tau}_\nu) = 0$, and we also say that $\boldsymbol{\tau}_\nu$ is an *ascendant* of $\boldsymbol{\tau}_\mu$. Moreover, if $\boldsymbol{\tau}_\nu \in L_\nu^n$ is a zero of $f_\nu(t_1, \ldots, t_n)$, then in L_μ^n, $\nu \le \mu$, $\boldsymbol{\tau}_\nu$ has at most $q^{n(\mu-\nu)}$ descendants, if any.

A zero $\boldsymbol{\tau}_\nu \in L_\nu^n$ of $f_\nu(t_1, \ldots, t_n)$ is said to be *non-singular* if

$$\frac{\partial f_1(\pi_{1,\nu}(\boldsymbol{\tau}_\nu))}{\partial t_j} = \frac{\partial f_1(\tau_{1,0}, \ldots, \tau_{n,0})}{\partial t_j} \neq 0$$

for some $j = 1, \ldots, n$. Otherwise $\boldsymbol{\tau}_\nu$ is called a *singular zero*. It is clear that any descendant (resp. ascendant) of a non-singular zero is a non-singular zero.

3. Orthogonal systems and permutation polynomial vectors.

In this section we introduce definitions and some results on the systems we are interested in. For a given commutative ring R, and $R[t_1, \ldots, t_n]$, and $\mathfrak{a}$ an ideal of R, W. Nöbauer [7] introduces the notion of *permutation polynomial* modulo $\mathfrak{a}$ and also the notion of *regular polynomial* if $R/\mathfrak{a}$ is a finite set. In [1] we proved that a permutation polynomial modulo (Z^ν) is also a regular polynomial in $L[[Z]]/(Z^\nu)$. More precisely, we prove that *$f(t_1, \ldots, t_n) \in L[[Z]][t_1, \ldots, t_n]$ induces a permutation polynomial over L_ν if, and only if, the equation $f_\nu(t_1, \ldots, t_n) = \boldsymbol{\alpha}(z_\nu)$ has exactly $q^{\nu(n-1)}$ solutions for each $\boldsymbol{\alpha}(z_\nu) \in L_\nu$.*

Accordingly to Zhang ([11], [12]) this means that *the polynomial $f(t_1, \ldots, t_n) \in L[[Z]][t_1, \ldots, t_n]$ induces*

a permutation polynomial over L_ν if, and only if, $f_\nu(t_1,\ldots,t_n)$ is a uniform map.

The system $f_1(t_1,\ldots,t_n),\ldots,f_k(t_1,\ldots,t_n)$ of polynomials in $L[[Z]][t_1,\ldots,t_n]$, $k\leq n$, is said to be an *orthogonal system* over L_ν if the map $L_\nu^n \longrightarrow L_\nu^k$ given by $(f_{\nu,1}(\boldsymbol{\alpha}_1(z_\nu),\ldots,\boldsymbol{\alpha}_n(z_\nu)),\ldots,f_{\nu,k}(\boldsymbol{\alpha}_1(z_\nu),\ldots,\boldsymbol{\alpha}_n(z_\nu)))$ for $(\boldsymbol{\alpha}_1(z_\nu),\ldots,\boldsymbol{\alpha}_n(z_\nu))\in L_\nu^n$ is a uniform map over L_ν, i.e., if the system of equations

$$\begin{aligned} f_{\nu,1}(t_1,\ldots,t_n)&=\boldsymbol{\alpha}_1(z_\nu)\\ f_{\nu,2}(t_1,\ldots,t_n)&=\boldsymbol{\alpha}_2(z_\nu)\\ &\vdots\\ f_{\nu,k}(t_1,\ldots,t_n)&=\boldsymbol{\alpha}_k(z_\nu)\end{aligned} \tag{1}$$

has $q^{\nu(n-k)}$ solutions in L_ν^n, where $f_{\nu,j}$ is the reduction of f_j in $L_\nu[t_1,\ldots,t_n]$. If $n=k$, the system is called *permutation polynomial vector (PPV) over L_ν*.

Is clear that when $k=1$, an orthogonal system is a permutation polynomial.

Proposition 3.1. *Let $f_1,\ldots,f_k\in L[[Z]][t_1,\ldots,t_n]$. If $f_1,\ldots,f_k$ is an orthogonal system over L_ν then it is an orthogonal system over $L_{\nu-1}$. In particular, it is an orthogonal system over L.*

Proof. Let $f_1,\ldots,f_k\in L[[Z]][t_1,\ldots,t_n]$ be an orthogonal system over L_ν. Then the system

$$\begin{aligned} f_{\nu-1,1}(t_1,\ldots,t_n)&=\boldsymbol{\alpha}_1(z_{\nu-1})\\ f_{\nu-1,2}(t_1,\ldots,t_n)&=\boldsymbol{\alpha}_2(z_{\nu-1})\\ &\vdots\\ f_{\nu-1,k}(t_1,\ldots,t_n)&=\boldsymbol{\alpha}_k(z_{\nu-1}).\end{aligned} \tag{2}$$

has solutions $\boldsymbol{\beta}(z_{\nu-1})=(\boldsymbol{\beta}_1(z_{\nu-1}),\ldots,\boldsymbol{\beta}_n(z_{\nu-1}))$ in $L_{\nu-1}^n$. Let N be the number of these solutions. Each of them has q^n descendants. On the other hand, from (2) we see that there are q^k systems of the form

$$\begin{aligned} f_{\nu,1}(t_1,\ldots,t_n)&=\boldsymbol{\alpha}_1(z_\nu)\\ f_{\nu,2}(t_1,\ldots,t_n)&=\boldsymbol{\alpha}_2(z_\nu)\\ &\vdots\\ f_{\nu,k}(t_1,\ldots,t_n)&=\boldsymbol{\alpha}_k(z_\nu)\end{aligned} \tag{3}$$

each of which has, by hypothesis, $q^{\nu(n-k)}$ different solutions, i.e., taken altogether all the above q^k systems will have $q^{\nu(n-k)}q^k$ different solutions. Since each solution descends from $\boldsymbol{\beta}(z_{\nu-1})$, then

$$q^{\nu(n-k)}q^k=Nq^n$$

therefore, $N=q^{(\nu-1)(n-k)}$. So, $f_1,\ldots,f_k$ is an orthogonal system over $L_{\nu-1}$. □

Corollary 3.1. *Let $f_1,\ldots,f_n\in L[[Z]][t_1,\ldots,t_n]$ be a permutation polynomial vector over L_ν, then $f_1,\ldots,f_n$ is a permutation polynomial vector over $L_{\nu-1}$. In particular is a permutation polynomial vector over L.* □

Proposition 3.2. *Let $f_1,\ldots,f_k\in L[[Z]][t_1,\ldots,t_n]$ be an orthogonal system over $L_1=L$, and such that the zeroes of $f_{1,i}(t_1,\ldots,t_n)-\alpha_i$ are nonsingular for all $\alpha_i\in L$. Then $f_1,\ldots,f_k$ is an orthogonal system over L_ν $(\nu=1,2,\ldots)$.*

Proof. Let N be the number of solutions of (1), where $\boldsymbol{\alpha}_i(z_\nu)=\alpha_{i,0}+\alpha_{i,1}z_\nu+\ldots+\alpha_{i,\nu-1}z_\nu^{\nu-1}$. We obtain the system

$$\begin{aligned} f_{1,1}(t_1,\ldots,t_n)&=\alpha_{1,0}\\ f_{1,2}(t_1,\ldots,t_n)&=\alpha_{2,0}\\ &\vdots\\ f_{1,k}(t_1,\ldots,t_n)&=\alpha_{k,0}\end{aligned} \tag{4}$$

which has q^{n-k} solutions. Since the zeroes of $f_{1,i}(t_1,\ldots,t_n)-\alpha_{i,0}$, $i=1,2,\ldots,k$ are non singular, each of the polynomials in (3) has exactly $q^{(\nu-1)(n-1)}$ descendants in L_ν ([1, lem. 2.2]). All of them are not different, since otherwise each zero of (4) would have $kq^{n(\nu-1)}$ descendants and since each element of L can be viewed in $q^{n(\nu-1)}$ ways in L_ν, then for $k>1$, a zero of (4) would have more than $q^{n(\nu-1)}$ ways to be viewed in L_ν. On the other hand, if $k=1$ then the proposition is true by proposition 3.1 in [1]. Now, if these descendants were the same for each polynomial in (4), then (3) would have $q^{n-k}q^{(\nu-1)(n-1)}$ different solutions. Then the system would have

$$\begin{aligned} q^{k\nu}q^{(n-k)}q^{(\nu-1)(n-1)}&=q^{k\nu+n-k+n\nu-\nu-n+1}\\ &=q^{n\nu}q^{(\nu-1)(k-1)}>q^{n\nu}\end{aligned}$$

different solutions, thus for $\nu>1,\ k>1$. But this contradicts, the cardinality of L_ν^n.

Therefore, the number of descendants, let us say D, contributed, by each polynomial in the system (4) to the solutions of system (3) is such that

$$q^{(n-k)}Dq^{\nu k}=q^{n\nu}.$$

Thus, $D=q^{(\nu-1)(n-k)}$, and the total number of solutions of (3) is $q^{(n-k)}q^{(\nu-1)(n-k)}=q^{\nu(n-k)}$, i.e.,

$f_1, \ldots, f_k \in L[[Z]][t_1, \ldots, t_n]$ is an orthogonal system over L_ν. □

Corollary 3.2. *Let $f_1, \ldots, f_n \in L[[Z]][t_1, \ldots, t_n]$ be a PPV over L such that the zeroes of $f_{1,i}(t_1, \ldots, t_n) - \alpha_i$ are nonsingular for all $\alpha_i \in L$. Then $f_1, \ldots, f_n$ is a PPV over L_ν.* □

The following propositions are extensions to $L[[Z]]$ of results known in finite fields, see [6].

Proposition 3.3. *Let $\nu > 1$ be, $f \in L[[Z]][t_1, \ldots, t_n]$ and $n \geq 2$. Let $f_2, \ldots, f_n \in L[[Z]][t_1, \ldots, t_n]$ be polynomials such that $f,\ f_2, \ldots,\ f_n$ is a PPV over L_ν then, $f_{(\nu)}$, the projection of f in $L_\nu[t_1, \ldots, t_n]$, is a permutation polynomial.*

Proof. If $f,\ f_2, \ldots,\ f_n$ is a PPV over L_ν then, for all $(\boldsymbol{\alpha}_1(z_\nu), \ldots, \boldsymbol{\alpha}_n(z_\nu)) \in L_\nu^n$, the system

$$\begin{aligned} f_{(\nu)}(t_1, \ldots, t_n) &= \boldsymbol{\alpha}_1(z_\nu) \\ f_{\nu,2}(t_1, \ldots, t_n) &= \boldsymbol{\alpha}_2(z_\nu) \\ &\vdots \\ f_{\nu,n}(t_1, \ldots, t_n) &= \boldsymbol{\alpha}_n(z_\nu) \end{aligned} \tag{5}$$

has a unique solution. Therefore the equation $f_{(\nu)}(t_1, \ldots, t_n) = \boldsymbol{\alpha}_1(z_\nu)$ has at least one solution in L_ν. Let $(\boldsymbol{\alpha}_1(z_\nu), \boldsymbol{\alpha}_2'(z_\nu) \ldots, \boldsymbol{\alpha}_n'(z_\nu)) \neq (\boldsymbol{\alpha}_1(z_\nu), \ldots, \boldsymbol{\alpha}_n(z_\nu)) \in L_\nu^n$. The system

$$\begin{aligned} f_{(\nu)}(t_1, \ldots, t_n) &= \boldsymbol{\alpha}_1(z_\nu) \\ f_{\nu,2}(t_1, \ldots, t_n) &= \boldsymbol{\alpha}_2'(z_\nu) \\ &\vdots \\ f_{\nu,n}(t_1, \ldots, t_n) &= \boldsymbol{\alpha}_n'(z_\nu) \end{aligned} \tag{6}$$

has again a unique solution, different to the solution of (5), because, otherwise, $(\boldsymbol{\alpha}_1(z_\nu), \boldsymbol{\alpha}_2'(z_\nu) \ldots, \boldsymbol{\alpha}_n'(z_\nu)) = (\boldsymbol{\alpha}_1(z_\nu), \ldots, \boldsymbol{\alpha}_n(z_\nu))$. But this can be done in $q^{\nu(n-1)}$ ways, i.e., for $\boldsymbol{\alpha}_1(z_\nu) \in L_\nu$, $f_{(\nu)}(t_1, \ldots, t_n) = \boldsymbol{\alpha}_1(z_\nu)$ has at least $q^{\nu(n-1)}$ solutions. If there is one more solution, say $(\boldsymbol{\beta}_1(z_\nu), \ldots, \boldsymbol{\beta}_n(z_\nu))$, we can construct the system

$$\begin{aligned} f_{(\nu)}(t_1, \ldots, t_n) &= \boldsymbol{\alpha}_1(z_\nu) \\ f_{\nu,2}(t_1, \ldots, t_n) &= \boldsymbol{\theta}_2(z_\nu) \\ &\vdots \\ f_{\nu,n}(t_1, \ldots, t_n) &= \boldsymbol{\theta}_n(z_\nu) \end{aligned} \tag{7}$$

where

$$\begin{aligned} f_{\nu,2}(\boldsymbol{\beta}_1(z_\nu), \ldots, \boldsymbol{\beta}_n(z_\nu)) &= \boldsymbol{\theta}_2(z_\nu), \\ &\vdots \\ f_{\nu,n}(\boldsymbol{\beta}_1(z_\nu), \ldots, \boldsymbol{\beta}_n(z_\nu)) &= \boldsymbol{\theta}_n(z_\nu), \end{aligned}$$

system that necessarily is one of previous systems (6). Therefore $f_{(\nu)}(t_1, \ldots, t_n) = \boldsymbol{\alpha}_1(z_\nu)$ has exactly $q^{\nu(n-1)}$ solutions, thus $f_{(\nu)}(t_1, \ldots, t_n)$ is a permutation polynomial. □

Corollary 3.3. *Every polynomial in a PPV is a permutation polynomial.* □

Proposition 3.4. *Let $f_1, \ldots, f_k \in L[[Z]][t_1, \ldots, t_n]$, $1 \leq k \leq n$ be an orthogonal system over L_ν and $\boldsymbol{\beta}_1(z_\nu), \ldots, \boldsymbol{\beta}_k(z_\nu) \in L_\nu$ and at least one them a unit. Then the polynomial*

$$\boldsymbol{\beta}_1(z_\nu) f_{\nu,1}(t_1, \ldots, t_n) + \ldots + \boldsymbol{\beta}_k(z_\nu) f_{\nu,k}(t_1, \ldots, t_n)$$

is a permutation polynomial over L_ν.

Proof. Let be $\boldsymbol{\lambda}(z_\nu) \in L_\nu$. We see that the number of solutions of

$$\begin{aligned} \boldsymbol{\beta}_1(z_\nu) f_{\nu,1}(t_1, \ldots, t_n) + \ldots \\ + \boldsymbol{\beta}_k(z_\nu) f_{\nu,k}(t_1, \ldots, t_n) = \boldsymbol{\lambda}(z_\nu) \end{aligned}$$

is $q^{\nu(n-1)}$. By hypothesis, the system,

$$\begin{aligned} f_{\nu,1}(t_1, \ldots, t_n) &= \boldsymbol{\alpha}_1(z_\nu) \\ f_{\nu,2}(t_1, \ldots, t_n) &= \boldsymbol{\alpha}_2(z_\nu) \\ &\vdots \\ f_{\nu,k}(t_1, \ldots, t_n) &= \boldsymbol{\alpha}_k(z_\nu) \end{aligned} \tag{8}$$

has $q^{\nu(n-k)}$ solutions, thus

$$\begin{aligned} \boldsymbol{\beta}_1(z_\nu) f_{\nu,1}(t_1, \ldots, t_n) &= \boldsymbol{\beta}_1(z_\nu) \boldsymbol{\alpha}_1(z_\nu) \\ \boldsymbol{\beta}_2(z_\nu) f_{\nu,2}(t_1, \ldots, t_n) &= \boldsymbol{\beta}_2(z_\nu) \boldsymbol{\alpha}_2(z_\nu) \\ &\vdots \\ \boldsymbol{\beta}_1(z_\nu) f_{\nu,1}(t_1, \ldots, t_n) + \ldots \\ + \boldsymbol{\beta}_k(z_\nu) f_{\nu,k}(t_1, \ldots, t_n) &= \boldsymbol{\beta}_1(z_\nu) \boldsymbol{\alpha}_1(z_\nu) + \\ &\quad \ldots + \boldsymbol{\beta}_k(z_\nu) \boldsymbol{\alpha}_k(z_\nu) \end{aligned} \tag{9}$$

is equivalent to (8). Since $\boldsymbol{\beta}_i(z_\nu)$ for some $i = 1, \ldots, k$ is a unit, then (9) has $q^{\nu(n-k)}$ solutions, i.e.,

$$\begin{aligned} \boldsymbol{\beta}_1(z_\nu) f_{\nu,1}(t_1, \ldots, t_n) + \ldots + \boldsymbol{\beta}_k(z_\nu) f_{\nu,k}(t_1, \ldots, t_n) \\ = \boldsymbol{\beta}_1(z_\nu) \boldsymbol{\alpha}_1(z_\nu) + \ldots + \boldsymbol{\beta}_k(z_\nu) \boldsymbol{\alpha}_k(z_\nu) \end{aligned}$$

has at least $q^{\nu(n-k)}$ solutions. Now, the polynomial $g(t_1,\ldots,t_n) = \boldsymbol{\beta}_1(z_\nu)t_1 + \ldots + \boldsymbol{\beta}_k(z_\nu)t_k$ is a permutation polynomial, and for $\boldsymbol{\lambda}(z_\nu)$ in L_ν, the equation $\boldsymbol{\beta}_1(z_\nu)t_1 + \ldots + \boldsymbol{\beta}_k(z_\nu)t_k = \boldsymbol{\lambda}(z_\nu)$ has $q^{\nu(k-1)}$ solutions. So, the equation

$$\boldsymbol{\beta}_1(z_\nu)f_{\nu,1}(t_1,\ldots,t_n) + \ldots + \boldsymbol{\beta}_k(z_\nu)f_{\nu,k}(t_1,\ldots,t_n) = \boldsymbol{\lambda}(z_\nu)$$

has $q^{\nu(n-k)}q^{\nu(k-1)} = q^{\nu(n-1)}$ solutions. □.

Corollary 3.4. *Every polynomial in an orthogonal system is a permutation polynomial.* □

Proposition 3.5. *If*

$$\boldsymbol{\beta}_1(z_\nu)f_{\nu,1}(t_1,\ldots,t_n) + \ldots + \boldsymbol{\beta}_k(z_\nu)f_{\nu,k}(t_1,\ldots,t_n),$$

$1 \le k \le n$, *is a permutation polynomial over L_ν and the zeroes of $f_{\nu,i}(t_1,\ldots,t_n) - \boldsymbol{\alpha}(z_\nu)$, $i = 1,\ldots,k$ are non singular for all $\boldsymbol{\alpha}(z_\nu) \in L_\nu$ and $\boldsymbol{\beta}_1(z_\nu),\ldots,\boldsymbol{\beta}_k(z_\nu) \in L_\nu$, where at least one them is a unit, then $f_1,\ldots,f_k \in L[[Z]][t_1,\ldots,t_n]$ is an orthogonal system over L_ν.*

Proof. If

$$\boldsymbol{\beta}_1(z_\nu)f_{\nu,1}(t_1,\ldots,t_n) + \ldots + \boldsymbol{\beta}_k(z_\nu)f_{\nu,k}(t_1,\ldots,t_n)$$

is a permutation polynomial then $\beta_{1,0}f_{1,1}(t_1,\ldots,t_n) + \ldots + \beta_{k,0}f_{1,k}(t_1,\ldots,t_n)$ is also a permutation polynomial ([1, lem. 3.3]). By hypothesis, the zeroes of $f_{\nu,i}(t_1,\ldots,t_n) - \alpha(z_\nu)$ are non singular; then by the corollary to theorem 2 in [6], the system $f_1,\ldots,f_k$ is an orthogonal system over L and by proposition 3.2 $f_1,\ldots,f_k$ is an orthogonal system over L_ν. □

Proposition 3.6. *Let $f_1,\ldots,f_k \in L[[Z]][t_1,\ldots,t_n]$. If $f_1,\ldots,f_k$ is an orthogonal system over L_ν then for all permutation polynomial $g(y_1,\ldots,y_k) \in L[[Z]][y_1,\ldots,y_k]$ over L_ν, the polynomial*

$$g_\nu(f_{\nu,1}(t_1,\ldots,t_n),\ldots,f_{\nu,k}(t_1,\ldots,t_n))$$

is a permutation polynomial.

Proof. Let be $\boldsymbol{\alpha}(z_\nu) \in L_\nu$. Since g is a permutation polynomial, $g_\nu(y_1,\ldots,y_k) = \boldsymbol{\alpha}(z_\nu)$ has $q^{\nu(k-1)}$ solutions $(\boldsymbol{\beta}_1(z_\nu),\ldots,\boldsymbol{\beta}_k(z_\nu))$ in L_ν and the system

$$\begin{aligned} f_{\nu,1}(t_1,\ldots,t_n) &= \boldsymbol{\beta}_1(z_\nu)\\ f_{\nu,2}(t_1,\ldots,t_n) &= \boldsymbol{\beta}_2(z_\nu)\\ &\vdots\\ f_{\nu,k}(t_1,\ldots,t_n) &= \boldsymbol{\beta}_k(z_\nu) \end{aligned}$$

has $q^{\nu(n-k)}$ solutions. But $f_1,\ldots,f_k$ is an orthogonal system over L_ν and, therefore,

$$g_\nu(f_{\nu,1}(t_1,\ldots,t_n),\ldots,f_{\nu,k}(t_1,\ldots,t_n)) = \boldsymbol{\alpha}(z_\nu)$$

has $q^{\nu(k-1)}q^{\nu(n-k)} = q^{\nu(n-1)}$ solutions, i.e,

$$g_\nu(f_{\nu,1}(t_1,\ldots,t_n),\ldots,f_{\nu,k}(t_1,\ldots,t_n))$$

is a permutation polynomial over L_ν. □

Proposition 3.7. *Let $f_1,\ldots,f_k \in L[[Z]][t_1,\ldots,t_n]$. If*

$$g_\nu(f_{\nu,1}(t_1,\ldots,t_n),\ldots,f_{\nu,k}(t_1,\ldots,t_n))$$

is a permutation polynomial over L_ν for all permutation polynomial over L_ν, $g(y_1,\ldots,y_k) \in L[[Z]][y_1,\ldots,y_k]$, and the zeroes of $f_{\nu,i}(t_1,\ldots,t_n) - \boldsymbol{\alpha}_\nu(z_\nu)$ are non singular for all $\boldsymbol{\alpha}(z_\nu) \in L_\nu$ and $i = 1,\ldots,k$ then $f_1,\ldots,f_k$ is an orthogonal system over L_ν.

Proof. Since $g_\nu(f_1,\ldots,f_k)$ is a permutation polynomial, for all permutation polynomial g_ν, in particular it is a permutation polynomial for $g(y_1,\ldots,y_k) = \boldsymbol{\beta}_1(Z)y_1 + \ldots + \boldsymbol{\beta}_k(Z)y_k$, where at least one $\boldsymbol{\beta}_i(Z)$ is a unit. Then by proposition 3.5, the system $f_1,\ldots,f_k$ is an orthogonal system over L_ν. □

Proposition 3.8. *Let f_1, f_2, ... , $f_{n+1} \in L[[Z]][t_1,\ldots,t_n]$ be a polynomials system. Then there exist coefficients $\boldsymbol{\beta}_1(Z),\ldots,\boldsymbol{\beta}_{n+1}(Z) \in L[[Z]]$, where at least one of them is a unit, such that*

$$\boldsymbol{\beta}_1(Z)f_1(t_1,\ldots,t_n) + \boldsymbol{\beta}_2(Z)f_2(t_1,\ldots,t_n) + \ldots + \boldsymbol{\beta}_{n+1}(Z)f_{n+1}(t_1,\ldots,t_n)$$

is not a permutation polynomial.

Proof. Let $\boldsymbol{\beta}_1(Z),\ldots,\boldsymbol{\beta}_{n+1}(Z) \in L[[Z]]$ where at least one of them is a unit. If the polynomial

$$\boldsymbol{\beta}_1(Z)f_1(t_1,\ldots,t_n) + \boldsymbol{\beta}_2(Z)f_2(t_1,\ldots,t_n) + \ldots + \boldsymbol{\beta}_{n+1}(Z)f_{n+1}(t_1,\ldots,t_n)$$

were a permutation polynomial, then the polynomial

$$\boldsymbol{\beta}_{1,0}f_{1,1}(t_1,\ldots,t_n) + \boldsymbol{\beta}_{2,0}f_{1,2}(t_1,\ldots,t_n) + \ldots + \boldsymbol{\beta}_{n+1,0}f_{1,n+1}(t_1,\ldots,t_n)$$

is also a permutation polynomial with $(\boldsymbol{\beta}_{1,0},\ldots,\boldsymbol{\beta}_{n+1,0})$ different from $(0,\ldots,0)$. This contradicts [6, theor. 4]. □

Proposition 3.9. *If $f_1,\ldots,f_k \in L[[Z]][t_1,\ldots,t_n]$ is an orthogonal system, then any of its nonempty subsystem is again an orthogonal system.*

Proof. If $f_1, \ldots, f_k$ is an orthogonal system then

$$\begin{aligned} f_{1,1}(t_1, \ldots, t_n) &= \alpha_{1,0} \\ &\vdots \\ f_{1,k}(t_1, \ldots, t_n) &= \alpha_{k,0} \end{aligned} \tag{10}$$

has q^{n-k} solutions. The lemma is proved, without lost of generality, if the system

$$\begin{aligned} f_{1,1}(t_1, \ldots, t_n) &= \alpha_{1,0} \\ &\vdots \\ f_{1,k-1}(t_1, \ldots, t_n) &= \alpha_{k-1,0} \end{aligned} \tag{11}$$

has $q^{n-(k-1)} = q^{n-k+1}$ solutions. Then, for all $(\alpha_{1,0}, \ldots, \alpha_{k-1,0}) \in L^{k-1}$, the equation (11) has at least q^{n-k} solutions, the same as (10). If we take $(\alpha'_{1,0}, \ldots, \alpha'_{k-1,0}, \alpha_{k,0}) \neq (\alpha_{1,0}, \ldots, \alpha_{k,0})$, then again for this $k-$ple (10) has q^{n-k} solutions, which are different to the initial ones; therefore for each $\alpha_{k,0} \in L$, the equation (11) has q^{n-k} solutions more. In total (11) has $q^{n-k}q = q^{n-k+1}$ solutions. □

Corollary 3.5. *If $f_1, \ldots, f_n \in L[[Z]][t_1, \ldots, t_n]$ is a PPV, then any of its nonempty subsystems is an orthogonal system.*

Proof. It is clear from Proposition 3.9 and the definition of PPV. □

Acknowledgements

We wish to express our thanks to Yuguang Lu for his help in the reading and understanding of [8], [10] and [14].

References

[1] **Acosta, S. P. A. & Albis, V. S.** *Characterization of multivariate permutation polynomials in positive characteristic*, Sao Paulo J. Math. Sci. **3** No. 1 (2009), 1–12.

[2] **Acosta, S. P. A. & Albis, V. S.** *Permutation polynomials in one indeterminate over modular algebras*, Rev. Acad. Colomb. Cienc. **30** No. 117 (2006), 541–548. [MR:2334082].

[3] **Albis, V. S. & Chaparro, R.** *On a conjeture of Borevich and Shafarevich*, Rev. Acad. Colomb. Cienc. **21** (1997), 313–319. [MR: 98g:11130].

[4] **Laigle-Chapuy, Y.** *Permutations polynomials and applications to coding theory.*, Finite Fields Appl. **13** (2007), 58–70.

[5] **Niederreiter, H.** *Permutation polynomials in several variables over finite fields*, Proc. Japan Acad. **46** No. 9 (1970), 1001–1005. [MR: 44#5298].

[6] **Niederreiter, H.** *Orthogonal systems of polynomials in finite fields*, Proc. Amer. Math. Soc. **28** (1971), 415–422. [MR:45# 230].

[7] **Nöbauer, Wilfried**. *Zur Theorie der Polynomtransformationen und Permutations polynome*, Math. Annalen **157** (1964), 332-342.

[8] **Shiue, P. J. S; Sun, Q. & Zhang, Q.** *Multivariate permutation polynomials and orthogonal systems over residue class rings*, Chinese. Ann. Math. Ser. A. **17** No. 1 (1996), 43–46. [in Chinese] [MR: 97e:11152].

[9] **Smits, T. H. .** *On the group of units of $GF(q)[X]/(a(X))$.* Indag. Math. **44** (1982), 355-358.

[10] **Sun, Q.** *A note on permutation polynomials vectors over $\mathbb{Z}/m\mathbb{Z}$*, Adv. Math. (China) **25** No. 1 (1996), 311–314. [In Chinese] [MR: 98h:11157].

[11] **Zhang, Q.** *Polynomials functions and permutation polynomials over some finite commutatuve rings*, J. Number Theory **105** (2004), 192–202.

[12] **Wei, Q. & Zhang, Q.** *On strong orthogonal systems and weak permutation polynimials over finite commutative rings*, Finite Fields Appl. **13** (2007), 113–120.

[13] **Zhang, Q.** *On the polynomials in several indeterminates which can be extended to permutation polynomial vector over $\mathbb{Z}/p^l\mathbb{Z}$*, Adv. Math. **22** No. 5 (1993), 456–457.

[14] **Zhang, Q.** *Permutation polynomials in several indeterminates over $\mathbb{Z}/m\mathbb{Z}$*, Chinese Ann. Math. Ser. A. **16** No. 2 (1995), 168–172. [In Chinese] [MR: 96g:11143].

Recibido: 5 de marzo de 2012
Aceptado para publicación: 19 de abril de 2012