São Paulo Journal of Mathematical Sciences **3**, 1 (2009), 1–12

Characterization of Multivariate Permutation Polynomials in Positive Characteristic

Pablo A. Acosta-Solarte

Universidad Distrital Francisco José de Caldas, Bogotá, Colombia.

E-mail address: paacostas@udistrital.edu.co

Víctor S. Albis

Universidad Nacional de Colombia, Bogotá, Colombia.

E-mail address: valbis@accefyn.org.co and vsalbisg@unal.edu.co

Abstract. Multivariate permutation polynomials over the algebra of formal series over a finite field and its residual algebras are characterized. Some known properties of permutation polynomials over finite fields are also extended.
AMS Classification 2000: 13B25, 13F25, 11T55.
Keywords: Multivariate permutation polynomials.

1. Introduction

If R is a commutative ring let us consider the ring $R[t_1,\dots,t_n]$. In [10], **W. Nöbauer** introduces the following definition: For an ideal $\mathfrak{a}$ of R and $f(t_1,\dots,t_n)\in R[t_1,\dots,t_n]$ the polynomial $f(t_1,\dots,t_n)$ is called a *permutation polynomial modulo* $\mathfrak{a}$ if there are polynomials

$$f_2(t_1,\dots,t_n),\dots,\ f_n(t_1,\dots,t_n)\in R[t_1,\dots,t_n]$$

such that the mapping

$$(\boldsymbol{\alpha}_1,\dots,\boldsymbol{\alpha}_n)\to(f(\boldsymbol{\alpha}_1,\dots,\boldsymbol{\alpha}_n),f_2(\boldsymbol{\alpha}_1,\dots,\boldsymbol{\alpha}_n),\dots,f_n(\boldsymbol{\alpha}_1,\dots,\boldsymbol{\alpha}_n))$$

induces a permutation of the set $(R/\mathfrak{a})^n$ into itself. If $R/\mathfrak{a}$ is a finite set of cardinality c, a polynomial $f(t_1,\dots,t_n)\in R[t_1,\dots,t_n]$ is said to be a *regular polynomial* modulo $\mathfrak{a}$ if the equation $f(t_1,\dots,t_n)\equiv a(\bmod\mathfrak{a})$ has exactly c^{n-1} solutions for all $a \bmod \mathfrak{a}$. Let us denote by $\mathcal{P}(\mathfrak{a})$ the set of all permutation polynomials modulo $\mathfrak{a}$ and by $\mathcal{R}(\mathfrak{a})$ the set of all regular polynomials modulo $\mathfrak{a}$. In the same paper he gives conditions for the equality of these two sets. In particular, equality holds if R is a finite

field L, or the ring $\mathbb{Z}$ of the rational integers, or $\mathfrak{q}$ is a $\mathfrak{p}-$primary ideal of R, for which there is a positive integer m such that $\mathfrak{p}^m \subseteq \mathfrak{q} \subseteq \mathfrak{p}^2 \subset \mathfrak{p}$, and $R/\mathfrak{p}^m$ is finite. **N. Lausch & W. Nöbauer** have proved in [5] the following result:

Proposition A. *Let $\mathfrak{q}$ be a $\mathfrak{p}-$primary ideal of R, and $\mathfrak{q} \neq \mathfrak{p}$, $R/\mathfrak{q}$ finite. Then a polynomial $f(t_1, \ldots, t_n) \in R[t_1, \ldots, t_n]$ is a permutation polynomial modulo $\mathfrak{q}$ if, and only if, $f(t_1, \ldots, t_n)$ is a permutation polynomial mod $\mathfrak{p}$ and the system of congruences*

$$\frac{\partial f(t_1, \ldots, t_n)}{\partial t_i} \equiv 0 (mod\, \mathfrak{p}) \,, \quad i = 1, \ldots, n \,, \tag{1}$$

has no solution in R.

This always will be the case for

(1) The ring of rational integers $\mathbb{Z}$ and the ideals $\mathfrak{q}_\nu = p^\nu\mathbb{Z}$ and $\mathfrak{p} = p\mathbb{Z}$, p a prime number, $\nu \geq 2$.
(2) The ring of $p-$adic integers $\mathbb{Z}_p$ and the ideals $\mathfrak{q}_\nu = p^\nu\mathbb{Z}_p$ and $\mathfrak{p} = p\mathbb{Z}_p$, p a prime number, $\nu \geq 2$.
(3) The ring of formal power series $L[[Z]]$ where L is a finite field, and the ideals $\mathfrak{q}_\nu = (Z^\nu)$ and and $\mathfrak{p} = (Z)$, $\nu \geq 2$ (see below).

Moreover, in these examples $\mathcal{P}(\mathfrak{q}) = \mathcal{R}(\mathfrak{q})$. Actually, multivariate permutation polynomials over $\mathbb{Z}/p^\nu\mathbb{Z}$, $\nu \geq 2$ have been studied quite recently often, using a variety of methods, always trying to answer the question: when a permutation polynomial over $p\mathbb{Z}$ can be lifted to a permutation polynomial over $p^\nu\mathbb{Z}$? (see, for example, [11, 1996], [13, 1996], [14, 1993], [15, 1995]).

In this paper we will deal with case 3. Indeed, the analogous of case 1 when $\mathbb{Z}$ is replaced by $K[X]$, where K is a finite field, and the prime p is replaced by an irreducible monic polynomial $p(X) \in K[X]$ can be translated to case 3. For it has been established (see [2], or [12]) that

$$K[X]/(p(X)^\nu) = \{\lambda_0 + \lambda_1 z_\nu + \ldots + \lambda_{\nu-1} z_\nu^{\nu-1} ;\, \lambda_i \in L\} \,,$$

where L is the finite field $K[X]/(p(X))$, and $z_\nu^j = 0$ for $j \geq \nu$, and the z_ν^i, for $i < \nu$, are $\neq 0$ and linearly independent over L. From now on, $K[X]/(p(X)^\nu)$ will be denoted by L_ν, and its elements by $\boldsymbol{\lambda}(z_\nu)$. As we will see in Section 2, $L[[Z]]$ may be considered as a projective limit of the $L-$algebras L_ν, and $L[[Z]]/(Z^\nu) \approx L_\nu$, where $L_1 = L$.

This particular case has never been mentioned explicitly in the literature, as far as we know. For this reason, in Section 3, we present a proof of Proposition A for this particular case, leaning heavily on some interesting algebraic combinatorial arguments, which have proved to be useful in other problems concerning the arithmetic of polynomial rings over finite fields (e.g., see [2]). In a forthcoming paper we will apply the same arguments to

explicitly study the orthogonal systems of polynomials over $L[[Z]][t_1,\ldots,t_n]$ to prove results similar to those contained in [9] or [11]. Finally, in section 4 we extend to this case a known result on polynomials over finite fields.

2. Preliminaries

In this section, for a finite field L with q elements, we establish the properties of $L[[Z]]$ and L_ν we need for the rest of the paper. Most of what follows is found in [2]. Let

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

be the $L-$algebra of formal power series in the indeterminate Z and coefficients in L. This algebra is a local ring with maximal ideal (Z). The series $\varepsilon(Z) = \sum_{i=0}^{\infty} \varepsilon_i Z^i$ is a unit in this algebra if, and only, if $\varepsilon_0 \neq 0$. Also each formal power series $\lambda(Z)$ can be written uniquely as $\lambda(Z) = \varepsilon(Z) Z^{v(\lambda(Z))}$, where $\varepsilon(Z)$ is a unit and $v(\lambda(Z))$ is a uniquely determined integer ≥ 0. Therefore, the mapping defined by $\lambda(Z) \to v(\lambda(Z))$ if $\lambda(Z) \neq 0$ and $v(0) = \infty$ is a discrete valuation on $L[[Z]]$. The ideals

$$(0) \subset \ldots \subset (Z^\nu) \subset \ldots \subset (Z^2) \subset (Z) \tag{2}$$

are the only ideals of $L[[Z]]$, and furthermore $L[[Z]]/(Z^\nu) \approx L_\nu$, a finite ring, of cardinality q^ν, for all $\nu \geq 1$.

Now $L[[Z]]$ is the projective limit of the projective system of $L-$algebras $(L_\mu, (\pi_{\nu,\mu})_{\nu \leq \mu})$, where the epimorphisms $\pi_{\nu,\mu} : L_\mu \to L_\nu$ are defined by

$$\boldsymbol{\lambda}(z_\mu) = \lambda_0 + \lambda_1 z_\mu + \ldots + \lambda_{\mu-1} z_\mu^{\mu-1} \mapsto \boldsymbol{\lambda}(z_\nu) = \lambda_0 + \lambda_1 z_\nu + \ldots + \lambda_{\nu-1} z_\nu^{\nu-1} \,;$$

the canonical projections $\pi_\nu : L[[Z]] \to L_\nu$ are thus given by

$$\lambda(Z) = \sum_{i=0}^{\infty} \lambda_i Z^i \mapsto \boldsymbol{\lambda}(z_\nu) = \sum_{i=0}^{\nu-1} \lambda_i z_\nu^i \,,$$

and is easily seen that $L[[Z]]/(Z^\nu) \approx L_\nu$.

If $f(t_1,\ldots,t_n) \in L[[Z]][t_1,\ldots,t_n]$, 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 $\mu \geq \nu$, $\pi_{\nu,\mu}(f_\mu(t_1,\ldots,t_n)) = f_\nu(t_1,\ldots,t_n)$.

We write

$$\boldsymbol{\tau}_\nu := \left(\sum_{i=0}^{\nu-1} \tau_{1,i} z_\nu^i, \ldots, \sum_{i=0}^{\nu-1} \tau_{n,i} z_\nu^i \right) \quad (\tau_{i,j} \in L) \tag{3}$$

for an element of L_ν^n.

If $\boldsymbol{\tau}_\mu \in L_\mu^n$ is a zero of $f_\mu(t_1,\ldots,t_n)$ and $\mu \geq \nu$, 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 such is the case, $f_\nu(\boldsymbol{\tau}_\nu) = 0$, and we also say that $\boldsymbol{\tau}_\nu$ is an *ascendant* of $\boldsymbol{\tau}_\mu$. Conversely, if $\boldsymbol{\tau}_\nu \in L_\nu^n$ is a zero of $f_\nu(t_1,\ldots,t_n)$, then in L_μ^n, $\mu \geq \nu$, $\boldsymbol{\tau}_\nu$ 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.

If $\boldsymbol{\tau}_\nu$ is given by (3), let us denote by $\widehat{\boldsymbol{\tau}}_\nu$ the element in L_ν^n given by

$$\widehat{\boldsymbol{\tau}}_\nu \ := \left(\sum_{i=0}^{\nu-2} \tau_{1,i} z_\nu^i, \ldots, \sum_{i=0}^{\nu-2} \tau_{n,i} z_\nu^i\right).$$

With the above notations, in [2] the following version of Taylor's formula is proven:

Lemma 2.1. *If $f(t_1,\ldots,t_n)$ is a polynomial with coefficients in $L[[Z]]$, then for each $\nu = 2,3,\ldots$ we have*

$$f_\nu(\boldsymbol{\tau}_\nu) = f_\nu(\widehat{\boldsymbol{\tau}}_\nu) + z_\nu^{\nu-1} \sum_{j=1}^{n} \tau_{j,\nu-1} \frac{\partial f_\nu(\widehat{\boldsymbol{\tau}}_\nu)}{\partial t_j}. \quad \square \tag{4}$$

If for $j = 1,\ldots,n$, we write

$$\frac{\partial f_\nu(\widehat{\boldsymbol{\tau}}_\nu)}{\partial t_j} = \beta_{j,0} + \beta_{j,1} z_\nu + \ldots + \beta_{j,\nu-1} z_\nu^{\nu-1} \tag{5}$$

($\beta_{j,k} \in L$), then after replacing in (4) we obtain

$$f_\nu(\boldsymbol{\tau}_\nu) = f_\nu(\widehat{\boldsymbol{\tau}}_\nu) + \left[\sum_{j=1}^{n} \tau_{j,\nu-1} \beta_{j,0}\right] z_\nu^{\nu-1}. \tag{6}$$

Now, given $f(t_1,\ldots,t_n)$ with coefficients in $L[[Z]]$, and a zero $\boldsymbol{\tau}_1 = (\tau_{1,0},\ldots,\tau_{n,0})$ of $f_1(t_1,\ldots,t_n)$ in L_1^n, we will denote by $d(\nu; f; \boldsymbol{\tau}_1)$ the number of its descendants in L_ν^n $(\nu \geq 1)$. Of course, $d(1; f; \boldsymbol{\tau}_1) = 1$. With this

notation,

$$c(\nu; f) = \sum_{\{\boldsymbol{\tau}_1 \ ; \ f_1(\boldsymbol{\tau}_1)=0\}} d(\nu; f; \boldsymbol{\tau}_1) \ , \quad \nu \geq 1 \, ,$$

indicates the total number of descendants in L_ν^n of the solutions of $f_1(\boldsymbol{\tau}_1) = 0$.

Lemma 2.2. [2, Proposition 2.5, part (b) and Proposition 3.1] *Let $f(t_1, \ldots, t_n)$ be a polynomial with coefficients in $L[[Z]]$, and let $\nu > 1$. Then:*

(a) For each singular zero $\boldsymbol{\tau}_\nu$ of $f_\nu(t_1, \ldots, t_n)$ we have

$$f_\nu(\boldsymbol{\tau}_\nu) = f_\nu(\widehat{\boldsymbol{\tau}}_\nu) \tag{7}$$

Further, the zero

$$\overset{\vee}{\boldsymbol{\tau}}_{\nu-1} := \pi_{\nu-1,\nu}(\boldsymbol{\tau}_\nu) = \left(\sum_{i=0}^{\nu-2} \tau_{1,i} z_{\nu-1}^i, \ldots, \sum_{i=0}^{\nu-2} \tau_{n,i} z_{\nu-1}^i \right) \tag{8}$$

of $f_{\nu-1}((t_1, \ldots, t_n)$ has always exactly q^n descendants in L_ν^n.

(b) For each nonsingular zero $\boldsymbol{\tau}_\nu$ of $f_\nu(t_1, \ldots, t_n)$ we have that

$$\overset{\vee}{\boldsymbol{\tau}}_{\nu-1} := \pi_{\nu-1,\nu}(\boldsymbol{\tau}_\nu) = \left(\sum_{i=0}^{\nu-2} \tau_{1,i} z_{\nu-1}^i, \ldots, \sum_{i=0}^{\nu-2} \tau_{n,i} z_{\nu-1}^i \right) \tag{9}$$

has always exactly q^{n-1} descendants in L_ν^n. Moreover,

$$d(\nu; f; \boldsymbol{\tau}_1) = d(\nu - 1; f; \boldsymbol{\tau}_1) q^{n-1} \, , \tag{10}$$

for all $\nu \geq 2$.

Proof. Let us put

$$f_\nu(\widehat{\boldsymbol{\tau}}_\nu) = \gamma_0 + \gamma_1 z_\nu + \ldots + \gamma_{\nu-1} z_\nu^{\nu-1} \, .$$

If $\boldsymbol{\tau}_\nu$ is a singular zero of $f_\nu(t_1, \ldots, t_n)$, then in (5), $\beta_{j,0} = 0$ for all $j = 1, \ldots, n$. Thus we have (7). The rest of part (a) in the proposition is an inmediate consequence of (7).

It follows from (6) that $\boldsymbol{\tau}_\nu$ is a non-singular zero of $f_\nu(t_1, \ldots, t_n)$ if, and only if,

$$\gamma_0 = \gamma_1 = \ldots = \gamma_{\nu-2} = 0 \ , \tag{11}$$

and

$$\gamma_{\nu-1} + \sum_{j=1}^{n} \tau_{j,\nu-1} \beta_{j,0} = 0 \, . \tag{12}$$

Let us remark that (11) is equivalent to $f_{\nu-1}(\overset{\vee}{\boldsymbol{\tau}}_{\nu-1}) = 0$. Thus $\overset{\vee}{\boldsymbol{\tau}}_\nu$ has as many descendants in L_ν^n as solutions has the linear equation (12). But, by

hypothesis, there is an index k ($k = 1, \ldots, n$) such that $\beta_{k,0} \neq 0$; therefore, for any choice of the coefficients $\tau_{j,\nu-1}$, $j \neq k$, the equation (12) is solvable for $\tau_{k,\nu-1}$. But there are exactly q^{n-1} choices for the $\tau_{j,\nu-1}$ ($j \neq k$), hence q^{n-1} descendants of $\overset{\vee}{\boldsymbol{\tau}}_{\nu-1}$. Finally, let us notice that the foregoing argument also shows that (12) is always solvable, from which the last part of the Lemma follows. □

3. **Characterization of multivariate permutation polynomials**

Let us recall that a polynomial $f(t) \in L[t]$ is said a permutation polynomial if the mapping induced on the field L is bijective. The same definition works for $f_\nu(t) \in L_\nu[t]$, for $\nu = 1, 2, \ldots$, and $f(t) \in L[[Z]][t]$. In [1] we proved that *$f(t) \in L[[Z]][t]$ is a permutation polynomial if, and only if, $f_1(t) \in L[t]$ is a permutation polynomial with no singular zeroes.* In the this section we obtain a similar characterization for multivariate polynomials.

Using the notation established in Section 1, **W. Nöbauer** [10] proves the following:

Lemma 3.1. [10, Property 3)] *Let R be a commutative ring such that $R/\mathfrak{a}$ is a finite ring for all ideals $\mathfrak{a}$ of R, then: [(v)] If $\mathfrak{p}$ is a prime ideal of R and $\mathfrak{q}$ is a $\mathfrak{p}$–primary ideal, and $\mathfrak{p}^m \subseteq \mathfrak{q} \subseteq \mathfrak{p}^2 \subset \mathfrak{p}$, for some $m \in \mathbb{N}^*$, then $\mathcal{P}(\mathfrak{q}) = \mathcal{R}(\mathfrak{q})$.* □

The fact that the ideals of $L[[Z]]$ satisfy (2), implies that the radical of (Z^ν) is (Z), and, since this ideal is maximal, (Z^ν) is $(Z)-$primary. This said, and since $(Z^\nu) = (Z)^\nu \subseteq (Z^2) \subset (Z)$, Lemma 3.1 proves that $\mathcal{P}((Z^\nu)) = \mathcal{R}((Z^\nu))$ for all $\nu \geq 1$. Thus

Lemma 3.2. *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, the equation $f_\nu(t_1, \ldots, t_n) = \boldsymbol{\alpha}(z_\nu)$, for each $\boldsymbol{\alpha}(z_\nu) \in L_\nu$ has exactly $q^{\nu(n-1)}$ solutions.* □

Lemma 3.3. *If the polynomial $f_\nu(t_1, \ldots, t_n)$ is a permutation polynomial over L_ν, then $f_{\nu-1}(t_1, \ldots, t_n)$ is a permutation polynomial over $L_{\nu-1}$. In particular, $f_1(t_1, \ldots, t_n) \in L[t_1, \ldots, t_n]$ is a permutation polynomial.*

Proof. Let $f_\nu(t_1, \ldots, t_n) \in L_\nu[t_1, \ldots, t_n]$ be a permutation polynomial and consider the equation $f_{\nu-1}(t_1, \ldots, t_n) = \boldsymbol{\alpha}(z_{\nu-1})$, where $\boldsymbol{\alpha}(z_{\nu-1}) = \alpha_0 + \alpha_1 z_{\nu-1} + \ldots + \alpha_{\nu-2} z_{\nu-1}^{\nu-2} \in L_{\nu-1}$. Let N denote the number of solutions of this equation in $L_{\nu-1}^n$. On the other hand, there are q elements $\boldsymbol{\alpha}(z_\nu) = \alpha_0 + \alpha_1 z_\nu + \ldots + \alpha_{\nu-2} z_\nu^{\nu-2} + \lambda_{\nu-1} z_u^{\nu-1} \in L_\nu$, one for each $\lambda_{\nu-1} \in L$, such that $\pi_{\nu-1,\nu}(\boldsymbol{\alpha}(z_\nu)) = \boldsymbol{\alpha}(z_{\nu-1})$. Then, by hypothesis, for each of the above $\boldsymbol{\alpha}(z_\nu)$,

the equation $f_\nu(t_1,\dots,t_n)=\boldsymbol{\alpha}(z_\nu)$ has $q^{\nu(n-1)}$ distinct solutions in L_ν^n, all of which are descendants of the solutions of $f_{\nu-1}(t_1,\dots,t_n)=\boldsymbol{\alpha}(z_{\nu-1})$. Thus $q^{\nu(n-1)}=Nq^{n-1}$ and $N=q^{(\nu-1)(n-1)}$. □

Let $f(t_1,\dots,t_n)\in L[[Z]][t_1,\dots,t_n]$ be such that $f_1(t_1,\dots,t_n)\in L[t_1,\dots,t_n]$ is a permutation polynomial. We ask now when this polynomial can be lifted to a permutation polynomial $f_\nu(t_1,\dots,t_n)\in L_\nu[t_1,\dots,t_n]$.

Proposition 3.1. *Let $f(t_1,\dots,t_n)\in L[[Z]][t_1,\dots,t_n]$ be such that $f_1(t_1,\dots,t_n)$ is a permutation polynomial. Then*

(i) If all the zeroes of $f_1(t_1,\dots,t_n)-\alpha_0\in L[t_1,\dots,t_n]$ are nonsingular, then the polynomials $f_\nu(t_1,\dots,t_n)\in L_\nu[t_1,\dots,t_n]$ are permutation polynomials, for all $\nu\geq 1$.

(ii) Conversely, if at least one solution of the equation $f_1(t_1,\dots,t_n)-\alpha_0=0$ is singular then $f_\nu(t_1,\dots,t_n)$ is not a permutation polynomial over L_ν for $\nu\geq 2$.

Proof. (i) By hypothesis, the zeroes of the polynomial $H_1=f_1(t_1,\dots,t_n)-\alpha_0$ are nonsingular, and each one of them has exactly $q^{(\nu-1)(n-1)}$ descendants in L_ν^n for all $\nu\geq 2$, from Lemma 2.2, (b). Since there are exactly q^{n-1} zeroes of $H_1(t_1,\dots,t_n)$ in L^n, the result now follows.

(ii) Let $\boldsymbol{\tau}_1=(\tau_{1,0},\dots,\tau_{n,0})$ be a singular zero of $f_1(t_1,\dots,t_n)\in L[t_1,\dots,t_n]$, and suppose that there exists a descendant

$$\boldsymbol{\tau}_2=(\tau_{1,0}+\tau_{1,1}z_2,\dots,\tau_{n,0}+\tau_{n,1}z_2)$$

of $\boldsymbol{\tau}_1$ in L_2^n. Then by Lemma 2.2, (a), $\boldsymbol{\tau}_1$ has exactly q^n descendants in L_2^n. Since, by hypothesis, the equation $f_1(t_1,\dots,t_n)=0$ has exactly q^{n-1} solutions, the equation $f_2(t_1,\dots,t_n)=0$ has exactly $q^nq^{n-1}=q^{2n-1}>q^{2(n-1)}$ solutions, showing that $f_2(t_1,\dots,t_n)$ is not a permutation polynomial. Thus in order to $f_\nu(t_1,\dots,t_n)$ be a permutation polynomial for $\nu\geq 2$ all the zeroes of the polynomial $f_1(t_1,\dots,t_n)-\alpha_0$ must be nonsingular. □

The above result suggest the following definition: a polynomial $f(t_1,\dots,t_n)\in L[[Z]][t_1,\dots,t_n]$ is a *permutation polynomial* if $f_1(t_1,\dots,t_n)\in L[t_1,\dots,t_n]$ is a permutation polynomial and the zeroes of $f_1(t_1,\dots,t_n)-\alpha_0$ are nonsingular for all $\alpha_0\in L$.

Combining the above results we can state now the following characterization of permutation polynomials.

Proposition 3.2. *The polynomial $f(t_1,\ldots,t_n)\in L[[Z]][t_1,\ldots,t_n]$ is a permutation polynomial if, and only if, $f_\nu(t_1,\ldots,t_n)\in L_\nu[t_1,\ldots,t_n]$ is a permutation polynomial for each $\nu=1,\,2,\,\ldots$.* □

If $H_1=f_1(t_1,\ldots,t_n)-\alpha_0$, and since

$$\frac{\partial H_1(t_1,\ldots,t_n)}{\partial t_i}=\frac{\partial f_1(t_1,\ldots,t_n)}{\partial t_i}\,,$$

the above result is a rewording of the more general Proposition A in the case considered here.

Since $L[[Z]]$ is a unique factorization domain, the elements of $L[[Z]][t_1,\ldots,t_n]$ can be uniquely written as

$$f(t_1,\ldots,t_n)=\varepsilon(Z)Z^r f^*(t_1,\ldots,t_n)\,, \tag{13}$$

where $\varepsilon(Z)Z^r$, $r\geq 0$, is the content of $f(t_1,\ldots,t_n)$ and $f^*(t_1,\ldots,t_n)$ is primitive. From (13) it follows that $f_\nu(t_1,\ldots,t_n)$ is identically the null polynomial if $r\geq\nu\geq 1$, i.e., it is not a permutation polynomial. Therefore, in our context we must assume always that the polynomials considered are primitive.

4. Some consequences

In this section we generalize a result on multivariate permutation polynomials over a finite field found in [8], though remarking that this is not the only one that could be generalized.

The following result, which provides a tool to find from known ones new permutation polynomials, is proved by **W. Nöbauer** in [10, p. 338].

Proposition B. *If $m<n$ and $h(t_{m+1},\ldots,t_n)\in R[t_{m+1},\ldots,t_n]$ is a permutation polynomial modulo the ideal $\mathfrak{a}$, and $g(t_1,\ldots,t_m)\in R[t_1,\ldots,t_m]$ is an arbitrary polynomial, then the polynomial $g(t_1,\ldots,t_m)+h(t_{m+1},\ldots,t_n)$ is a permutation polynomial modulo $\mathfrak{a}$. In particular, every permutation polynomial modulo $\mathfrak{a}$ in $R[t_1,\ldots,t_m]$ is again a permutation polynomial modulo $\mathfrak{a}$ in $R[t_1,\ldots,t_n]$.*

Its translation to the case which occupies us, reads thus as follows:

Proposition 4.1. *Suppose that $f(t_1,\ldots,t_n)\in L[[Z]][t_1,\ldots,t_n]$ is of the form*

$$f(t_1,\ldots,t_n)=g(t_1\ldots,t_m)+h(t_{m+1},\ldots,t_n)\,,$$

$1\leq m<n$, where $h\in L[[Z]][t_{m+1},\ldots,t_n]$ is a permutation polynomial and $g\in L[[Z]][t_1,\ldots,t_m]$. Then f is a permutation polynomial. In particular, every permutation polynomial in $L[[Z]][t_1,\ldots,t_m]$ is a permutation polynomial in $L[[Z]][t_1,\ldots,t_n]$.

Proof. Here we provide a direct proof of this Proposition based on our previous results and techniques. Indeed, if $f(t_1,\ldots,t_n) \in L[[Z]][t_1,\ldots,t_n]$ is such that

$$f(t_1,\ldots,t_n) = g(t_1\ldots,t_m) + h(t_{m+1},\ldots,t_n)\,,$$

where $h(t_{m+1},\ldots,t_n) \in L[[Z]][t_{m+1},\ldots,t_n]$ is a permutation polynomial, let us assume that $\boldsymbol{\tau}_1 = (\tau_{1,0},\ldots,\tau_{m,0},\tau_{m+1,0},\ldots,\tau_{n,0})$ is a singular zero of

$$H_1(t_1,\ldots,t_n) = f_1(t_1,\ldots,t_n) - \alpha_0\,,$$

so that

$$\frac{\partial H_1}{\partial t_j}(\boldsymbol{\tau}_1) = \frac{\partial f_1}{\partial t_j}(\boldsymbol{\tau}_1) = \frac{\partial g_1}{\partial t_j}(\tau_{1,0},\ldots,\tau_{m,0}) + \frac{\partial h_1}{\partial t_j}(\tau_{m+1,0},\ldots,\tau_{n,0}) = 0$$

for all $j = 1,\ldots,n$. But for $j \geq m+1$, $\dfrac{\partial g_1}{\partial t_j}(\tau_{1,0},\ldots,\tau_{m,0}) = 0$ always, and consequently

$$\frac{\partial h_1}{\partial t_j}(\tau_{m+1,0},\ldots,\tau_{n,0}) = 0 \quad \text{for} \quad j \geq m+1\,.$$

But this means that $h \in L[[Z]][t_{m+1},\ldots,t_n]$ is not a permutation polynomial (Proposition 3.1). □

Let us recall now that for a commutative ring with unity R, a *nonsingular linear transformation* in R^n is defined as a system of equations

$$t_i = \sum_{j=1}^{n} a_{ij}y_j + b_i \quad (i = 1,\ldots,n)\,,$$

where $a_{ij},\ b_i \in R$ and $\det(a_{ij}) \in R^{\times}$. In particular, for a polynomial $f(t_1,\ldots,t_n) \in L[[Z]][t_1,\ldots,t_n]$, we define a *nonsingular linear transformation of its indeterminates* to be a transformation of the form

$$t_i = \sum_{j=1}^{n} \alpha_{ij}(Z)y_j + \beta_i(Z), \tag{14}$$

where $\alpha_{ij}(Z),\ \beta_i(Z) \in L[[Z]]$, and $\det(\alpha_{ij}(Z)) = \det(A) \in L[[Z]]^{\times}$. If we write

$$\det(\alpha_{ij}(Z)) = \varepsilon_0 + \sum_{k=1}^{\infty} \varepsilon_k Z^k\,,\ \varepsilon_0 \neq 0\,,$$

it is clear that $\pi_\nu(\det(A)) = \varepsilon_0 + \varepsilon_1 z_\nu + \ldots + \varepsilon_{\nu-1} z_\nu^{\nu-1} \in L_\nu^{\times}$. Therefore the projection of (14) by π_ν

$$t_i = \sum_{j=1}^{n} \boldsymbol{\alpha}_{ij}(z_\nu)y_j + \boldsymbol{\beta}(z_\nu)\,,\ i = 1,\ldots,n\,, \tag{15}$$

is a non-singular linear transformation of the indeterminates, since $\pi_\nu(\det(A)) = \det(\boldsymbol{\alpha}_{ij}(z_\nu)) \in L_\nu^\times$. In particular, $\pi_1(\det(A)) = \varepsilon_0 \neq 0$, and

$$t_i = \sum_{j=1}^{n} \alpha_{ij,0} y_j + \beta_{i,0}$$

where $\alpha_{ij,0} = \pi_1(\alpha_{ij}(Z))$ and $\beta_{i,0} = \pi_1(\beta_i(Z))$ is a nonsingular linear transformation in L^n. Conversely, the nonsingular linear transformation in L^n

$$t_i = \sum_{j=1}^{n} \alpha_{ij} y_j + \beta_i \quad \alpha_{ij}\,, \beta_i \in L \tag{16}$$

is a nonsingular linear transformation in $L[[Z]]^n$.

By abuse of language we still write $f(y_1, \ldots, y_n) \in L[[Z]][y_1, y_2, \ldots, y_n]$ (resp., $f_\nu(y_1, \ldots, y_n) \in L_\nu[y_1, y_2, \ldots, y_n]$, $\nu = 1, 2, \ldots$) for the polynomial obtained from $f(t_1, \ldots, t_n) \in L[[Z]][t_1, t_2, \ldots, t_n]$ (resp., $f_\nu(t_1, \ldots, t_n) \in L_\nu[t_1, \ldots, t_n]$, $\nu = 1, 2, \ldots$) under the nonsingular linear transformation (14) (resp., (15)).

Let now $f(t_1, \ldots, t_n) \in L[[Z]][t_1, \ldots, t_n]$ be a permutation polynomial and let $\boldsymbol{\tau}_0 = (\tau_{1,0}, \tau_{2,0}, \ldots, \tau_{n,0})$ be one of the q^{n-1} nonsingular zeroes of $f_1(t_1, \ldots, t_n) - \alpha$, for some $\alpha \in L$. Using (16) we obtain, putting $\gamma_{i,0} = \tau_{i,0} - \beta_i$,

$$\begin{aligned}
\gamma_{1,0} &= \alpha_{11} y_1 + \alpha_{12} y_2 + \ldots + \alpha_{1n} y_n \\
\gamma_{2,0} &= \alpha_{21} y_1 + \alpha_{22} y_2 + \ldots + \alpha_{2n} y_n \\
&\vdots \\
\gamma_{n,0} &= \alpha_{n1} y_1 + \alpha_{n2} y_2 + \ldots + \alpha_{nn} y_n\,,
\end{aligned}$$

Since $\det(\alpha_{ij}) \neq 0$, the above system has a unique solution $\boldsymbol{\tau}_0' = (\xi_1, \ldots, \xi_n)$ which is then a zero of $f_1(y_1, y_2, \ldots, y_n) - \alpha$. Thus we have shown that the property of being a permutation polynomial over a finite field L is invariant under singular linear transformations of the indeterminates.

Now we will prove that if for $\alpha \in L$ all the zeroes of $f_1(t_1, \ldots, t_n) - \alpha$ are nonsingular, then all the zeroes of $f_1(y_1, y_2, \ldots, y_n) - \alpha$ are nonsingular. Indeed, let $\boldsymbol{\tau}_0$ be a zero of $f_1(t_1, \ldots, t_n) - \alpha$, and $\boldsymbol{\tau}_0'$ the corresponding zero under (16). If $\boldsymbol{\tau}_0'$ were singular, then for $j = 1, 2, \ldots, n$, we would have

$$\begin{aligned}
\frac{\partial f_1(\boldsymbol{\tau}_0')}{\partial y_j} &= \frac{\partial f_1(\boldsymbol{\tau}_0)}{\partial t_1} \cdot \frac{\partial t_1}{\partial y_j} + \ldots \frac{\partial f_1(\boldsymbol{\tau}_0)}{\partial t_n} \cdot \frac{\partial t_n}{\partial y_j} \\
&= \frac{\partial f_1(\boldsymbol{\tau}_0)}{\partial t_1} \alpha_{1j} + \ldots + \frac{\partial f_1(\boldsymbol{\tau}_0)}{\partial t_n} \alpha_{nj} = 0
\end{aligned}$$

Since $\det(\alpha_{ij}) \neq 0$, the above system of linear homogeneous equations has a unique solution, the null vector. Therefore $\dfrac{\partial f_1(\boldsymbol{\tau}_0)}{\partial t_i} = 0$ for all $i = 1, \ldots, n$, which forces $\boldsymbol{\tau}_0$ to be a singular zero of $f_1(t_1, \ldots, t_n)$, contradicting our initial choice of $\boldsymbol{\tau}_0$. Thus we have proved

Proposition 4.2. *Let $f(t_1, \ldots, t_n) \in L[[Z]][t_1, \ldots, t_n]$ be a permutation polynomial. If*

$$t_i = \sum_{j=1}^{n} \alpha_{ij}(Z) y_j + \beta_i(Z), \tag{17}$$

is a nonsingular transformation of the variables of $f(t_1, \ldots, t_n)$ then $f(y_1, \ldots, y_n)$, the polynomial obtained by the transformation of the variables of $f(t_1, \ldots, t_n)$, is again a permutation polynomial. □

Two polynomials f and g in $L[[Z]][t_1, \ldots, t_n]$ *are called equivalent* if f and g can be transformed into each other by nonsingular linear transformations of its variables.

Proposition 4.3. *Let $f(t_1, \ldots, t_n) \in L[[Z]][t_1, \ldots, t_n]$ be a polynomial. If $f(t_1, \ldots, t_n)$ is equivalent to a polynomial of the form*

$$g(t_1, \ldots, t_{n-1}) + t_n \,,$$

where $g(t_1, \ldots, t_{n-1}) \in L[[Z]][t_1, \ldots, t_{n-1}]$, then f is a permutation polynomial.

Proof. Let (17) be the nonsingular linear transformation taking $f(t_1, \ldots, t_n)$ into $g(t_1, \ldots, t_{n-1}) + t_n$. Since t_n is a permutation polynomial this transformed polynomial is a permutation polynomial, by proposition 4.2. Applying the inverse nonsingular transformation, Proposition 4.2 tells us that the polynomial $f(t_1, \ldots, t_n)$ is a permutation polynomial. □

References

[1] **Acosta, 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]

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

[3] **Albis, V. S.** *Polinomios de permutación. Algunos problemas de interés*, Lecturas Matemáticas **22** (2001), 35–58. [MR: 2348568]

[4] **Dickson, L. E.** *Linear Groups with an Exposition of the Galois Field Theory.* Dover Publi.: New York, 1958.

[5] **Lausch, H. & Nöbauer, W.** *Algebra of Polynomials.*, North–Holland: Amsterdam & London: 1973.

[6] **Lidl, R. & Niederreiter, H.** *Introduction to Finite Fields and their Aplications.* Cambridge University Press.: Inglaterra, 1986.

[7] **Lidl, R. & Niederreiter, H.** *Finite Fields*, Encycl. of Math. and its Appl., Addison Wesley Pub. Comp. Reading Mass., 1983. [MR: 86c:11106].

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

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

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

[11] **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].

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

[13] **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].

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

[15] **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].