Monografías de la Real Academia de Ciencias. Zaragoza. **43:** 119–122, (2018).
ISSN: 1132-6360

LINEARIZED MULTIVARIATE SKEW POLYNOMIALS AND HILBERT 90 THEOREMS WITH MULTIVARIATE NORMS

UMBERTO MARTÍNEZ-PEÑAS

Abstract. We linearize the concept of free multivariate skew polynomials. We give a vector space description of their sets of roots in one conjugacy class, whose univariate counterpart is crucial in applications such as network coding. As a collateral consequence, we derive new Hilbert 90 theorems for general Galois field extensions. In contrast with the homological versions, these are computational theorems based on multivariate norms that reflect the relations among generators of the corresponding Galois group.

1. Introduction

Univariate skew polynomials were introduced by Ore in [6], and evaluation and interpolation using them were studied by Lam and Leroy in [1, 2]. Their results on linearizing their sets of roots are crucial for finding optimal error-correcting codes for the rank and sum-rank metrics [4], which have applications in linear network coding, among others (see [4] and its references). Moreover, they observed in [3] that Hilbert's famous Theorem 90 can be naturally written in terms of conjugacy and evaluation of skew polynomials.

In [5], we extended the concepts of skew polynomials and their evaluation and interpolation properties to free multivariate skew polynomial rings. One of the main motivations was to construct good codes for new (or old) metrics yet to be found. In this work, we give a linearized description of (free) multivariate skew polynomials and their root sets in one conjugacy class similar to that in [2]. We then deduce a generalization of Hilbert's Theorem 90 based on multivariate norms reflecting the relations among generators of the Galois group.

Throughout this paper, we will use the definitions, results and notations from [5]. Fix a division ring $\mathbb{F}$ and variables $x_1, x_2, \ldots, x_n$ and denote by $\mathcal{M}$ the set of (free) strings on these variables, which we will simply call monomials. Inspired by Ore's work [6], we showed in [5, Th. 1] that a product in a free multivariate polynomial ring with coefficients in $\mathbb{F}$ consists in appending monomials and is additive on degrees if, and only if, there exist a ring morphism $\sigma : \mathbb{F} \longrightarrow \mathbb{F}^{n\times n}$ and a σ-derivation $\delta : \mathbb{F} \longrightarrow \mathbb{F}^n$ such that

$$\mathbf{x}\beta = \sigma(\beta)\mathbf{x} + \delta(\beta),$$

for all $\beta \in \mathbb{F}$, where $\mathbf{x}$ is the column vector whose i-th component is x_i, for $i = 1, 2, \ldots, n$. We denote by $\mathbb{F}[\mathbf{x}; \sigma, \delta]$ such a non-commutative ring.

2. Linearized multivariate skew polynomials

We start by introducing linearized multivariate skew polynomials.

Definition 2.1. Given a (ring) morphism $\sigma : \mathbb{F} \longrightarrow \mathbb{F}^{n\times n}$, a σ-derivation $\delta : \mathbb{F} \longrightarrow \mathbb{F}^n$, a point $\mathbf{a} \in \mathbb{F}^n$ and a monomial $\mathfrak{m} \in \mathcal{M}$, we define the operator

$$\mathcal{D}_{\mathbf{a}}^{\mathfrak{m}} : \mathbb{F} \longrightarrow \mathbb{F}$$

as follows. First we define $\mathcal{D}_{\mathbf{a}}^{1} = \mathrm{Id}$, then we define

$$\mathcal{D}_{\mathbf{a}}(\beta) = (\mathcal{D}_{\mathbf{a}}^{x_1}(\beta), \mathcal{D}_{\mathbf{a}}^{x_2}(\beta), \ldots, \mathcal{D}_{\mathbf{a}}^{x_n}(\beta))^T = \sigma(\beta)\mathbf{a} + \delta(\beta) \in \mathbb{F}^n,$$

for all $\beta \in \mathbb{F}$. Next, if $\mathcal{D}_{\mathbf{a}}^{\mathfrak{m}}$ is defined for $\mathfrak{m} \in \mathcal{M}$, then we define

$$\mathcal{D}_{\mathbf{a}}^{\mathbf{x}\mathfrak{m}}(\beta) = (\mathcal{D}_{\mathbf{a}}^{x_1\mathfrak{m}}(\beta), \mathcal{D}_{\mathbf{a}}^{x_2\mathfrak{m}}(\beta), \ldots, \mathcal{D}_{\mathbf{a}}^{x_n\mathfrak{m}}(\beta))^T = \sigma(\mathcal{D}_{\mathbf{a}}^{\mathfrak{m}}(\beta))\mathbf{a} + \delta(\mathcal{D}_{\mathbf{a}}^{\mathfrak{m}}(\beta)) \in \mathbb{F}^n,$$

for all $\beta \in \mathbb{F}$. Denote by $\mathbb{F}[\mathcal{D}_{\mathbf{a}}]$ the left vector space over $\mathbb{F}$ with basis $\{\mathcal{D}_{\mathbf{a}}^{\mathfrak{m}} \mid \mathfrak{m} \in \mathcal{M}\}$. We define linearized multivariate skew polynomials as the elements of $\mathbb{F}[\mathcal{D}_{\mathbf{a}}]$. Given $F \in \mathbb{F}[\mathbf{x}; \sigma, \delta]$, we may construct a $F^{\mathcal{D}} \in \mathbb{F}[\mathcal{D}_{\mathbf{a}}]$ as the image of F by the left linear map

$$\begin{array}{ccc} \mathbb{F}[\mathbf{x}; \sigma, \delta] & \longrightarrow & \mathbb{F}[\mathcal{D}_{\mathbf{a}}] \\ \sum_{\mathfrak{m}\in\mathcal{M}} F_{\mathfrak{m}}\mathfrak{m} & \mapsto & \sum_{\mathfrak{m}\in\mathcal{M}} F_{\mathfrak{m}}\mathcal{D}_{\mathbf{a}}^{\mathfrak{m}}. \end{array}$$

Linearized skew polynomials are right linear over certain division subrings of $\mathbb{F}$, called centralizers, which motivates the terminology. Centralizers for univariate skew polynomials were defined in [2, Eq. (3.1)].

Definition 2.2. Given $\mathbf{a} \in \mathbb{F}^n$, we define its (σ, δ)-centralizer, or simply centralizer, as

$$K_{\mathbf{a}} = K_{\mathbf{a}}^{\sigma,\delta} = \{\beta \in \mathbb{F} \mid \mathcal{D}_{\mathbf{a}}(\beta) = \mathbf{a}\beta\}.$$

The following lemma extends [2, Lemma 3.2] (see also [3, Sec. 3]) from the univariate to the multivariate case. The proof is straightforward.

Lemma 2.3. *For all $\mathbf{a} \in \mathbb{F}^n$, it holds that $K_{\mathbf{a}} \subseteq \mathbb{F}$ is a division subring of $\mathbb{F}$. Moreover, for $F \in \mathbb{F}[\mathcal{D}_{\mathbf{a}}]$, the map $\beta \mapsto F(\beta)$, for $\beta \in \mathbb{F}$, is right linear over $K_{\mathbf{a}}$.*

We now connect multivariate skew polynomial evaluation [5, Def. 3] and linearized skew polynomial evaluation. The following result can be proven exactly as [4, App. A].

Theorem 2.4. *Given $\mathbf{a} \in \mathbb{F}^n$, $\beta \in \mathbb{F}^*$, $F \in \mathbb{F}[\mathbf{x}; \sigma, \delta]$, and writing $\mathcal{D} = \mathcal{D}_{\mathbf{a}}$, it holds that*

$$F(\mathcal{D}(\beta)\beta^{-1}) = F^{\mathcal{D}}(\beta)\beta^{-1}.$$

3. Linearized P-closed sets in one conjugacy class

In this section, we give linearized descriptions of finitely generated P-closed sets in one conjugacy class. Here, we will need the concepts of conjugacy, P-closed sets, P-independence and P-bases from [5]. We denote by $\overline{\mathcal{A}} = Z(I(\mathcal{A})) \subseteq \mathbb{F}^n$ the P-closure of a set $\mathcal{A} \subseteq \mathbb{F}^n$. Observe that the conjugacy relation in [5, Def. 4] is $\mathbf{a} \sim \mathbf{b}$ if, and only if, there exists $\beta \in \mathbb{F}^*$ such that $\mathbf{b} = \mathbf{a}^{\beta} = \mathcal{D}_{\mathbf{a}}(\beta)\beta^{-1}$. We will denote by $C(\mathbf{a})$ the conjugacy class of $\mathbf{a} \in \mathbb{F}^n$.

Our main result is the following lemma, which extends [2, Th. 4.5] from the univariate to the multivariate case.

Lemma 3.1. *Let $\mathbf{a}, \mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_M \in \mathbb{F}^n$ and $\beta_1, \beta_2, \ldots, \beta_M \in \mathbb{F}^*$ be such that*

$$\mathbf{b}_i = \mathcal{D}_{\mathbf{a}}(\beta_i)\beta_i^{-1},$$

for $i = 1, 2, \ldots, M$. Then $\mathcal{B} = \{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_M\}$ is P-independent if, and only if, $\mathcal{B}_{\mathcal{D}} = \{\beta_1, \beta_2, \ldots, \beta_M\}$ is right linearly independent over $K_{\mathbf{a}}$.

Proof. Assume first that $\mathcal{B}$ is P-independent, but $\mathcal{B}_{\mathcal{D}}$ is not right linearly independent over $K_{\mathbf{a}}$. Let $\mathcal{B}^* = \{F_1, F_2, \dots, F_M\} \subseteq \mathbb{F}[\mathbf{x}, \sigma, \delta]$ be a dual P-basis of $\mathcal{B}$ (see [5, Def. 11]). We may assume without loss of generality that there exist $\lambda_1, \lambda_2, \dots, \lambda_{M-1} \in K_{\mathbf{a}}$ such that

$$\beta_M = \sum_{i=1}^{M-1} \beta_i \lambda_i.$$

Therefore by Lemma 2.3 and Theorem 2.4, we reach the following contradiction

$$\beta_M = F_M^{\mathcal{D}}(\beta_M) = \sum_{i=1}^{M-1} F_M^{\mathcal{D}}(\beta_i)\lambda_i = 0.$$

Assume now that $\mathcal{B}_{\mathcal{D}}$ is right linearly independent over $K_{\mathbf{a}}$. We will prove by induction on M that $\mathcal{B}$ is P-independent. The case $M = 1$ is obvious since singleton sets are always P-independent. Assume then that $\mathcal{B}' = \{\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_{M-1}\}$ is P-independent but $\mathbf{b}_M \in \overline{\mathcal{B}'}$.

First we see that we may assume without loss of generality that $\beta_M = 1$, redefining $\beta_i = \beta_i \beta_M^{-1}$ and $\mathbf{a} = \mathbf{b}_M$ ($\mathbf{b}_i$ remains unchanged), for $i = 1, 2, \dots, M$.

Now let $\mathcal{B}'^* = \{F_1, F_2, \dots, F_{M-1}\}$ be a dual P-basis of $\mathcal{B}'$. Fix $i = 1, 2, \dots, M-1$ and define $\mathbf{G}_i = (\mathbf{x} - \mathbf{b}_i)F_i \in \mathbb{F}[\mathbf{x}; \sigma, \delta]^n$. It holds that $\mathbf{G}_i(\mathbf{b}_j) = \mathbf{0}$, for $j = 1, 2, \dots, M-1$, by [5, Th. 3]. Since $\mathbf{a} = \mathbf{b}_M \in \overline{\mathcal{B}'}$, we deduce from [5, Th. 3] and [5, Th. 5] that

$$\mathbf{0} = \mathbf{G}_i(\mathbf{a}) = (\mathbf{a}^{F_i(\mathbf{a})} - \mathbf{b}_i)F_i(\mathbf{a}) = \mathcal{D}_{\mathbf{a}}(F_i(\mathbf{a})) - \mathcal{D}_{\mathbf{a}}(\beta_i)\beta_i^{-1}F_i(\mathbf{a})$$

if $F_i(\mathbf{a}) \neq 0$. Now, we have that

$$\mathcal{D}_{\mathbf{a}}(F_i(\mathbf{a}))F_i(\mathbf{a})^{-1} = \mathcal{D}_{\mathbf{a}}(\beta_i)\beta_i^{-1} \iff \mathbf{a}^{F_i(\mathbf{a})} = \mathbf{a}^{\beta_i} \iff \mathbf{a}^{\beta_i^{-1}F_i(\mathbf{a})} = \mathbf{a},$$

thus $\beta_i^{-1}F_i(\mathbf{a}) \in K_{\mathbf{a}}$. Hence in all cases ($F_i(\mathbf{a}) = 0$ or $\neq 0$) we have that $F_i(\mathbf{a}) = \beta_i\lambda_i$, for some $\lambda_i \in K_{\mathbf{a}}$. Next if $F = F_1 + F_2 + \cdots + F_{M-1}$, we have that $F(\mathbf{b}_j) = 1$, for $j = 1, 2, \dots, M-1$. Since $\mathbf{a} = \mathbf{b}_M \in \overline{\mathcal{B}'}$, we deduce from [5, Th. 5] the following contradiction

$$\beta_M = 1 = F(\mathbf{a}) = \sum_{i=1}^{M-1} F_i(\mathbf{a}) = \sum_{i=1}^{M-1} \beta_i\lambda_i.$$

□

With the same techniques, we can also prove that if $\mathcal{G} \subseteq \mathbb{F}^n$ is finite and $\mathbf{b} \in \overline{\mathcal{G}}$, then $\mathbf{b}$ is conjugate to an element in $\mathcal{G}$. Hence we can easily deduce the following result.

Theorem 3.2. *Let $\mathbf{a} \in \mathbb{F}$. The following hold:*

(1) *If $\mathcal{G} \subseteq C(\mathbf{a})$ is finite and $\Omega = \overline{\mathcal{G}} \subseteq \mathbb{F}^n$, then*

$$\Omega = \{\mathcal{D}_{\mathbf{a}}(\beta)\beta^{-1} \mid \beta \in \Omega^{\mathcal{D}} \setminus \{0\}\} \subseteq C(\mathbf{a}), \tag{1}$$

for a finite-dimensional right vector space $\Omega^{\mathcal{D}} \subseteq \mathbb{F}$ over $K_{\mathbf{a}}$.

(2) *Conversely, if $\Omega^{\mathcal{D}} \subseteq \mathbb{F}$ is a finite-dimensional right vector space over $K_{\mathbf{a}}$, then $\Omega \subseteq C(\mathbf{a})$ given as in (1) is a finitely generated P-closed set.*

Moreover if Item 1 or 2 holds, then $\mathcal{B}$ is a P-basis of Ω if, and only if, $\mathcal{B}_{\mathcal{D}} = \{\beta \in \mathbb{F}^* \mid \mathcal{D}_{\mathbf{a}}(\beta)\beta^{-1} \in \mathcal{B}\}$ is a right basis of $\Omega^{\mathcal{D}}$ over $K_{\mathbf{a}}$. In particular, we have that

$$\mathrm{Rk}(\Omega) = \dim_{K_{\mathbf{a}}}(\Omega^{\mathcal{D}}).$$

The following important consequence follows immediately:

Corollary 3.3. *Let $\mathbf{a} \in \mathbb{F}^n$. The conjugacy class $C(\mathbf{a}) \subseteq \mathbb{F}^n$ is P-closed and finitely generated if, and only if, $\mathbb{F}$ is a finite-dimensional right vector space over $K_{\mathbf{a}}$.*

4. Hilbert 90 theorems with multivariate norms

As observed in [3], generalizations of Hilbert's Theorem 90 can be understood as any effective criterion for conjugacy. Thus we can give a general statement from Corollary 3.3.

Theorem 4.1 (**Multivariate Hilbert 90**). *Let $\mathbf{a} \in \mathbb{F}^n$, assume that $\mathbb{F}$ is a finite-dimensional right vector space over $K_{\mathbf{a}}$, and let $\{F_j\}_{j\in J}$ be generators of $I(C(\mathbf{a}))$ as a left ideal. For $\mathbf{b} \in \mathbb{F}^n$, there exists $\beta \in \mathbb{F}^*$ such that*

$$\mathbf{b} = \mathcal{D}_{\mathbf{a}}(\beta)\beta^{-1},$$

if and only if, $F_j(\mathbf{b}) = 0$, for all $j \in J$, where evaluation is as in [5, Def. 3].

Assume now that $\mathbb{F}$ is a field, $\mathbf{a} = \mathbf{1} = (1, 1, \ldots, 1)$, $\delta = 0$ and $\sigma = \operatorname{diag}(\sigma_1, \sigma_2, \ldots, \sigma_n)$, for field automorphisms $\sigma_i : \mathbb{F} \longrightarrow \mathbb{F}$, for $i = 1, 2, \ldots, n$ (as in [5, Ex. 1]). Then $K = K_{\mathbf{1}} = \mathbb{F}^G$ is the field of invariant elements of $\mathbb{F}$ by the group G generated by $\sigma_1, \sigma_2, \ldots, \sigma_n$. If G is finite and $K \subseteq \mathbb{F}$ is a Galois extension, we can easily prove, using Theorem 2.4, that the set

$$\{\mathfrak{m} - \mathfrak{n} \in \mathbb{F}[\mathbf{x}; \sigma, \delta] \mid \mathfrak{m}, \mathfrak{n} \in \mathcal{M}, \mathfrak{m}(\sigma) = \mathfrak{n}(\sigma)\}$$

generates $I(C(\mathbf{1}))$, where $\mathfrak{m}(\sigma)$ is the conventional symbolic evaluation of $\mathfrak{m}$ in $(\sigma_1, \sigma_2, \ldots, \sigma_n)$. Thus we deduce the following generalization of Hilbert 90 for Galois field extensions.

Corollary 4.2. *Let $K \subseteq \mathbb{F}$ be a Galois extension of fields with Galois group G generated by $\sigma_1, \sigma_2, \ldots, \sigma_n$. For a list $\mathbf{b} = (b_1, b_2, \ldots, b_n) \in (\mathbb{F}^*)^n$, there exists $\beta \in \mathbb{F}^*$ such that*

$$b_i = \sigma_i(\beta)\beta^{-1}, \quad \text{for all } i = 1, 2, \ldots, n,$$

if and only if, the following equations are satisfied:

$$N_{\mathfrak{m}}(\mathbf{b}) = N_{\mathfrak{n}}(\mathbf{b}), \quad \text{whenever } \mathfrak{m}(\sigma) = \mathfrak{n}(\sigma),$$

where $N_{\mathfrak{m}}(\mathbf{b}) = \mathfrak{m}(\mathbf{b})$ and $N_{\mathfrak{n}}(\mathbf{b}) = \mathfrak{n}(\mathbf{b})$ can be computed recursively as in [5, Th. 2].

Acknowledgement: This work is supported by The Independent Research Fund Denmark under Grant No. DFF-7027-00053B.

References

[1] T. Y. Lam. A general theory of Vandermonde matrices. *Expositiones Mathematicae*, 4:193–215, 1986.
[2] T. Y. Lam and A. Leroy. Vandermonde and Wronskian matrices over division rings. *Journal of Algebra*, 119(2):308–336, 1988.
[3] T. Y. Lam and A. Leroy. Hilbert 90 theorems over divison rings. *Transactions of the American Mathematical Society*, 345(2):595–622, 1994.
[4] U. Martínez-Peñas. Skew and linearized Reed-Solomon codes and maximum sum rank distance codes over any division ring. *Journal of Algebra* (In press), 2018.
[5] U. Martínez-Peñas and F. R. Kschischang. Evaluation and interpolation over multivariate skew polynomial rings. pages 1–28, 2017. Submitted. Available: `https://arxiv.org/abs/1710.09606`.
[6] O. Ore. Theory of non-commutative polynomials. *Annals of Mathematics (2)*, 34(3):480–508, 1933.

Dept. of Electrical & Computer Engineering, University of Toronto, Canada
E-mail address: `umberto@math.aau.dk`