Evaluation and interpolation over multivariate skew polynomial rings

Umberto Martínez-Peñas *1 and Frank R. Kschischang †2

1Dept. of Mathematical Sciences, Aalborg University, Denmark
2Dept. of Electrical & Computer Engineering, University of Toronto, Canada

Abstract

In this work, we extend the concepts of evaluation and interpolation from univariate skew polynomials to multivariate skew polynomials. To extend these concepts in a natural way, we consider multivariate skew polynomial rings whose multiplication is additive on degrees, but which are not in principle iterated skew polynomial rings, and where the variables are never commutative with each other, except for the case of multivariate conventional polynomials. Our main objectives and results are descriptions of the sets of zeros of these multivariate skew polynomials, the families of functions that such skew polynomials define, and how we can perform Lagrange interpolation with them. To obtain these descriptions, we extend the existing concepts of P-closed sets, P-independence, P-bases and skew Vandermonde matrices from the univariate case to the multivariate one.

Keywords: Derivations, free polynomial rings, Lagrange interpolation, Newton interpolation, skew polynomials, Vandermonde matrices.

MSC: 08B20, 11C08, 12E10.

1 Introduction

Univariate skew polynomial rings, introduced in [18], are those “non-commutative polynomial rings” over division rings (that is, non-commutative fields) whose addition is the usual one, but whose multiplication is arbitrary with the following restrictions: the ith power of the variable x corresponds to the monomial “x^i”, and the degree of a product of two arbitrary polynomials is the sum of their degrees.

An extension of the concept of evaluation to these rings was first given in [11] and further developed in [12, 13]. Such extension is natural in the sense that it is based on the “Remainder Theorem” for conventional polynomials and it is analogous to projecting on a quotient ring defined by a maximal ideal, as in algebraic geometry: Since a skew
polynomial ring is a right-Euclidean domain \[18\], we may define the evaluation of \( F(x) \) on a point \( a \) as the remainder of the Euclidean division of \( F(x) \) by \( x - a \) on the right.

When the coefficients lie in more general rings, one can obtain iterated skew polynomial rings \[5, \text{Section 8.8}\]. However, this does not seem to be the right context in which to define and study evaluations of multivariate skew polynomials (see Appendix \[B\]). Furthermore, even different variables cannot be commutative with each other except for the case of multivariate conventional polynomials (see Appendix \[A\]).

In this work, we define free multivariate skew polynomial rings following Ore’s idea: The product of two monomials consists in appending them, and the degree of a product of two skew polynomials is the sum of their degrees. Thanks to this definition, we show that we may define the evaluation of a skew polynomial \( F(x_1, x_2, \ldots, x_n) \) on an affine point \((a_1, a_2, \ldots, a_n)\) as the remainder of the Euclidean division of \( F(x_1, x_2, \ldots, x_n) \) by \( x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n \), on the right. Once this is done, we may define general (non-free) skew polynomial rings, where evaluation is still natural, as quotients of the free ring by ideals of skew polynomials that vanish at every point (Definition \[7\]).

Our main objective is to describe the functions obtained by evaluating multivariate skew polynomials, under some finiteness conditions. This problem is closely related to that of interpolation in the sense of Lagrange, which has been studied previously in the univariate case \[9, 11, 15, 21\].

Our main results are as follows: We obtain a description of the family of such functions, when defined on a finitely generated set of zeros (\(P\)-closed set), as a vector space over the field of coefficients, and we find its dimension and a basis (Theorem \[5\]). For this, we first obtain a Lagrange-type interpolation theorem (Theorem \[4\]) on \(P\)-closed sets. To this end, we need to extend first the concept of \(P\)-basis \[12, \text{Section 4}\] of a \(P\)-closed set and define finitely generated \(P\)-closed sets as those with a finite \(P\)-basis. For that purpose, we need to introduce ideals of zeros, whose properties are based on extensions to the multivariate case of tools from \[11, 12, 13\]: A multiplication that is additive on degrees (Theorem \[1\]), an iterative evaluation on monomials (Theorem \[2\]) and a product rule (Theorem \[3\]).

Apart from its own interest, our main motivations to develop this theory come from the theory of error-correcting codes \[9\] over finite fields \[14\]. The use of univariate skew polynomials over finite fields \[17\] has provided two interesting families of error-correcting codes: Skew cyclic codes with good parameters \[11, 12, 17\] and evaluation codes using skew polynomials \[5, 10, 16, 19\], which include optimal codes for both the Hamming metric and the rank metric. However, the lack of a satisfactory theory of evaluation for multivariate skew polynomials has resulted in the lack of multivariate evaluation codes (such as a Reed-Muller-type code \[9, \text{Section 13.2.3}\]) and Guruswami-Sudan-type list-decoding algorithms \[20\] for skew Reed-Solomon codes, among other results.

The results and ideas in this work are presented linearly, that is, each section is based on the previous sections. The organization is as follows. In Section \[2\] we show which multiplications are additive on degrees over “free multivariate polynomial rings” (Theorem \[1\], extending \[15\] Eq. (3), (4) & (5)). In Section \[3\] we show how to define evaluations as remainders of Euclidean divisions and give a recursive formula for mono-
mials (Theorem 2), extending [13, Lemma 2.4] and [13, Eq. (2.3)]. In Section 4, we show how the product of two skew polynomials is preserved after evaluation (Theorem 3), extending [13, Theorem 2.7]. In Section 5, we define P-closed sets and ideals of zeros, and give their basic properties. Using them, we define in Section 6 non-free multivariate skew polynomial rings (Definition 7). In Section 7, we extend the crucial concepts of P-independence and P-bases from [12, Section 4] to our context. In Section 8, we give the first main result of the paper: The existence of Lagrange interpolating skew polynomials (Theorem 4). In Section 9, we give the second main result of the paper: We obtain the dimension and bases of the vector space of skew polynomial functions over a finitely generated P-closed set (Theorem 5). In Section 10, we give explicit computational methods to find such dimensions and bases and to perform Lagrange interpolation, via an extension of the Vandermonde matrices considered in [11, 13]. The complexity for finding ranks and P-bases is exponential in general, but given a P-basis, the complexity of finding Lagrange interpolating polynomials is polynomial.

Notation

Throughout this paper, $\mathbb{F}$ will denote a commutative field. However, before Section 8 our results extend readily to the case where $\mathbb{F}$ is an arbitrary non-commutative ring. Furthermore, assuming $\mathbb{F}$ to be finite avoids all other finiteness assumptions.

For positive integers $m$ and $n$, $\mathbb{F}^{m\times n}$ will denote the set of $m \times n$ matrices over $\mathbb{F}$, and $\mathbb{F}^n$ will denote the set of column vectors of length $n$ over $\mathbb{F}$. That is, $\mathbb{F}^n = \mathbb{F}^{n \times 1}$.

On a non-commutative ring $\mathcal{R}$, we will denote by $(A) \subseteq \mathcal{R}$ the left ideal generated by a set $A \subseteq \mathcal{R}$, and on a vector space $\mathcal{V}$ over $\mathbb{F}$, we will denote by $\langle B \rangle \subseteq \mathcal{V}$ the $\mathbb{F}$-linear vector space generated by a set $B \subseteq \mathcal{V}$ (or left module if $\mathbb{F}$ is a non-commutative ring).

All rings in this work will be assumed to have multiplicative identity, including the zero ring, where both additive and multiplicative identities coincide.

2 Free skew polynomial rings, matrix morphisms and vector derivations

In this section, we show which multiplications over a free non-commutative polynomial ring consist in appending monomials and are additive on degrees. See Section 3 and Appendix A to see why we cannot assume that the variables are commutative with each other, unless we are dealing with the conventional multivariate polynomial ring. See Appendix B to see why we do not consider iterated skew polynomial rings.

Fix a positive integer $n$ from now on, let $x_1, x_2, \ldots, x_n$ be $n$ distinct characters, and denote by $\mathcal{M}$ the set of all finite strings using these characters. We assume that the characters are not commutative (that is, $x_i x_j \neq x_j x_i$ if $i \neq j$) and we also consider the empty string, which will be denoted by $1$. A character $x_i$ will be called a variable, an element $m \in \mathcal{M}$ will be called a monomial, and we will define its degree, denoted by $\deg(m)$, as its length as a string.
Let \( \mathcal{R} \) be the vector space over \( F \) with basis \( \mathcal{M} \). That is, every element \( F \in \mathcal{R} \) can be expressed uniquely as a linear combination (with coefficients on the left)
\[
F = \sum_{m \in \mathcal{M}} F_m m,
\]
where \( F_m \in F \), for \( m \in \mathcal{M} \), and \( F_m = 0 \) except for a finite number of monomials.

An element \( F \in \mathcal{R} \) will be called a \((\text{multivariate}) \text{ skew polynomial}\), and we will define its \textit{degree}, denoted by \( \text{deg}(F) \), as the maximum degree of a monomial \( m \in \mathcal{M} \) such that \( F_m \neq 0 \), if \( F \neq 0 \). We will define \( \text{deg}(F) = \infty \) if \( F = 0 \).

Formally, our objective is to provide \( \mathcal{R} \) with an inner product \( \mathcal{R} \times \mathcal{R} \rightarrow \mathbb{R} \) that turns it into a non-commutative algebra over \( F \) via \( a \mapsto a1 \), restricts to the operation \( \mathcal{M} \times \mathcal{M} \rightarrow \mathcal{M} \) that consists in appending strings, and where the degree of a product of two skew polynomials is the sum of their degrees.

First observe that, by identifying \( a \in F \) with \( a1 \in \mathcal{R} \), we may assume that \( F \subseteq \mathcal{R} \), with the elements in \( F \) called \textit{constants}. Next, by inspecting constants and variables, we see that we need functions \( \sigma_{i,j} : F \rightarrow F \) and \( \delta_i : F \rightarrow F \), for \( i, j = 1, 2, \ldots, n \), such that
\[
x_i a = \sum_{j=1}^{n} \sigma_{i,j}(a) x_j + \delta_i(a), \tag{1}
\]
for \( i = 1, 2, \ldots, n \), and for all \( a \in F \). This defines two maps
\[
\sigma : F \rightarrow F^{n \times n} : a \mapsto \begin{pmatrix}
\sigma_{1,1}(a) & \sigma_{1,2}(a) & \cdots & \sigma_{1,n}(a) \\
\sigma_{2,1}(a) & \sigma_{2,2}(a) & \cdots & \sigma_{2,n}(a) \\
\vdots & \vdots & \ddots & \vdots \\
\sigma_{n,1}(a) & \sigma_{n,2}(a) & \cdots & \sigma_{n,n}(a)
\end{pmatrix}, \tag{2}
\]
and
\[
\delta : F \rightarrow F^n : a \mapsto \begin{pmatrix}
\delta_1(a) \\
\delta_2(a) \\
\vdots \\
\delta_n(a)
\end{pmatrix}. \tag{3}
\]

With this more compact notation, we may write Equation (1) as
\[
xa = \sigma(a)x + \delta(a), \tag{4}
\]
where \( x \) is a column vector containing \( x_i \) in the \( i \)-th row, for \( i = 1, 2, \ldots, n \). We have the following result, which extends the discussion in the case \( n = 1 \) given at the beginning of [18].
Theorem 1. If an inner product in $\mathcal{R}$ turns it into a non-commutative algebra over $\mathbb{F}$ via $a \mapsto a_1$, consists in appending monomials when restricted to $\mathcal{M}$ and is additive on degrees, then it is given on constants and variables as in (1), the map $\sigma : \mathbb{F} \rightarrow \mathbb{F}^{n \times n}$ in (4) is a ring morphism, and the map $\delta : \mathbb{F} \rightarrow \mathbb{F}^n$ in (3) is additive and satisfies that
\[\delta(ab) = \sigma(a)\delta(b) + \delta(a)b,\] for all $a, b \in \mathbb{F}$.

Conversely, for any two such maps $\sigma : \mathbb{F} \rightarrow \mathbb{F}^{n \times n}$ and $\delta : \mathbb{F} \rightarrow \mathbb{F}^n$, there exists a unique inner product in $\mathcal{R}$ satisfying the properties in the previous paragraph. Furthermore, two such inner products are equal if, and only if, the corresponding maps are equal.

Proof. First assume that a given inner product in $\mathcal{R}$ satisfies the properties in the first paragraph. The additive properties of $\sigma$ and $\delta$ then follow from
\[x_i(a + b) = (x_i a) + (x_i b),\] for all $a, b \in \mathbb{F}$ and all $i = 1, 2, \ldots, n$, their multiplicative properties follow from
\[x_i(ab) = (x_i a)b,\] for all $a, b \in \mathbb{F}$ and all $i = 1, 2, \ldots, n$, and $\sigma(1) = I$ follows from $x_i 1 = 1 x_i$ for all $i = 1, 2, \ldots, n$.

Next, the uniqueness and equality properties in the second paragraph are straightforward using Equations (1) or (4).

Finally, given a ring morphism $\sigma : \mathbb{F} \rightarrow \mathbb{F}^{n \times n}$ and an additive map $\delta : \mathbb{F} \rightarrow \mathbb{F}^n$ satisfying (3), we may define the desired inner product in $\mathcal{R}$ as follows. First, constants in $\mathbb{F}$ act on the left as scalars ($(a1)F = aF$, for all $F \in \mathcal{R}$). Now given $m, n \in \mathcal{M}$, we define recursively on $m$ the products
\[(m x_i)(an) = \sum_{j=1}^n m(\sigma_{i,j}(a)(x_j n)) + m(\delta_i(a)n),\] for all $i = 1, 2, \ldots, n$ and all $a \in \mathbb{F}$, where $mx_i$ and $x_j n$ denote appending of monomials. Observe that this already defines, recursively on $m$, the products of monomials as appending them, by choosing $a = 1$.

Finally, given general skew polynomials $F = \sum_{m \in M} F_m m$ and $G = \sum_{n \in M} G_n n$, where $F_m, G_m \in \mathcal{R}$, for all $m \in \mathcal{M}$, we define
\[FG = \sum_{m \in M} \sum_{n \in M} F_m (m(G_n n)).\] We give the proof of all the properties of such an inner product in Appendix C. This motivates the following definitions:
Definition 1 (Matrix morphisms and vector derivations). We call every ring morphism $\sigma : F \rightarrow F^{n \times n}$ a matrix morphism (over $F$), and we say that a map $\delta : F \rightarrow F^n$ is a $\sigma$-vector derivation (over $F$) if it is additive and satisfies

$$\delta(ab) = \sigma(a)\delta(b) + \delta(a)b,$$

for all $a, b \in F$.

Definition 2 (Free multivariate skew polynomial rings). Given a matrix morphism $\sigma : F \rightarrow F^{n \times n}$ and a $\sigma$-vector derivation $\delta : F \rightarrow F^n$, we define the free (multivariate) skew polynomial ring corresponding to $\sigma$ and $\delta$ as the unique ring $R = F[x; \sigma, \delta]$ with the inner product given by (1).

Observe that the conventional free multivariate polynomial ring on the variables $x_1, x_2, \ldots, x_n$ is obtained by choosing $\sigma = \text{Id}$ and $\delta = 0$, where we define $\text{Id}(a) = aI$, for all $a \in F$. Moreover, observe that this is the only case where constants and variables commute.

We conclude the section with some particular instances of matrix morphisms and vector derivations of interest:

Example 1. A matrix morphism $\sigma : F \rightarrow F^{n \times n}$ satisfies $\sigma_{i,j}(a) = 0$, for all $a \in F$ and all $i \neq j$ if, and only if, there exist field endomorphisms $\sigma_i : F \rightarrow F$, for $i = 1, 2, \ldots, n$, such that

$$\sigma(a) = \begin{pmatrix}
\sigma_1(a) & 0 & \ldots & 0 \\
0 & \sigma_2(a) & \ldots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \ldots & \sigma_n(a)
\end{pmatrix},$$

for all $a \in F$.

Example 2. Let $\sigma : F \rightarrow F^{n \times n}$ be a matrix morphism, and let $\beta \in F^n$. The map $\delta : F \rightarrow F^n$ defined by

$$\delta(a) = (\sigma(a) - aI)\beta,$$

for all $a \in F$, is a $\sigma$-vector derivation. When $n = 1$, these vector derivations are called inner derivations in the literature. Observe that, if $F$ is non-commutative, we need to define $\delta(a) = \sigma(a)\beta - \beta a$, for all $a \in F$.

3 Evaluations of multivariate skew polynomials

In this section, we show how to define evaluation maps $E_a : F[x; \sigma, \delta] \rightarrow F$, for all $a \in F^n$, that can be considered natural or standard. We will first require that these maps are linear forms over $F$. We may then define the total evaluation map as

$$E : F[x; \sigma, \delta] \rightarrow F^n : F \mapsto (E_a(F))_{a \in F^n}.$$
which is again linear. By linearity, we have that

\[ E_a \left( \sum_{m \in \mathcal{M}} F_m m \right) = \sum_{m \in \mathcal{M}} F_m N_m(a), \]

for all \( a \in \mathbb{F}^n \), all \( F_m \in \mathbb{F} \), and for functions

\[ N_m : \mathbb{F}^n \rightarrow \mathbb{F} : a \rightarrow E_a(m), \]

where \( m \in \mathcal{M} \). Therefore, giving a total evaluation map \( E \) is equivalent to giving the family of functions \( (N_m)_{m \in \mathcal{M}} \), thus these will be called fundamental functions of the evaluation \( E \). When \( n = 1 \), the fundamental functions \( N_i = N_{x^i} \), for \( i = 0, 1, 2, \ldots \), coincide with those in [11, 13].

As stated in Section 1, a standard way of understanding evaluations of multivariate conventional polynomials is by giving a canonical ring isomorphism

\[ \mathbb{F}[x_1, x_2, \ldots, x_n]/(x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n) \rightarrow \mathbb{F}, \]

for all \( a_1, a_2, \ldots, a_n \in \mathbb{F} \), due to the “Remainder Theorem”. The same idea is used in classical algebraic geometry to define evaluations as projections to a quotient ring given by a maximal ideal, which would be isomorphic to the so-called residue field. In Appendix A, we will show why this approach does not work if we allow the variables to be commutative with each other, unless \( \sigma = \text{Id} \) and \( \delta = 0 \).

To obtain such an isomorphism, we give a Euclidean-type division for linear skew polynomials:

**Lemma 1.** For any \( a_1, a_2, \ldots, a_n \in \mathbb{F} \) and any \( F \in \mathbb{F}[x; \sigma, \delta] \), there exist unique \( G_1, G_2, \ldots, G_n \in \mathbb{F}[x; \sigma, \delta] \) and \( b \in \mathbb{F} \) such that

\[ F = \sum_{i=1}^{n} G_i(x_i - a_i) + b. \]  

(7)

**Proof.** Existence is proven by a Euclidean division algorithm as usual. We next prove the uniqueness property. We only need to prove that if

\[ \sum_{i=1}^{n} G_i(x_i - a_i) + b = 0, \]  

(8)

then \( G_1 = G_2 = \ldots = G_n = b = 0 \). Assume the opposite. Without loss of generality, we may assume that \( G_n \neq 0 \) and \( \deg(G_n) \geq \deg(G_i) \), for all \( i \) with \( G_i \neq 0 \).

Let \( \prec \) denote the graded lexicographic (from right to left) ordering in \( \mathcal{M} \) with \( x_1 \prec x_2 \prec \ldots \prec x_n \), and denote by \( \text{LM}(G) \in \mathcal{M} \) the leading monomial of a skew polynomial \( G \in \mathbb{F}[x; \sigma, \delta] \) with respect to \( \prec \). Then we see that the monomial \( \text{LM}(G_n(x_n - a_n)) = \text{LM}(G_n)x_n \) cannot be cancelled by any other monomial on the left-hand side of (8). This is absurd and thus \( G_i = 0 \), for all \( i = 1, 2, \ldots, n \). Hence \( b = 0 \) and we are done. \( \square \)
Remark 1. Observe that the facts that the product in $\mathbb{F}[x; \sigma, \delta]$ consists in appending monomials and is additive on degrees are crucial in the proof of the previous lemma, since they allow us to state that $\text{LM}(G_n(x_n - a_n)) = \text{LM}(G_n)x_n$ for the graded lexicographic ordering. These properties also ensure that the division algorithm does not run indefinitely.

We may then define a standard evaluation as follows, which extends the case $n = 1$ from [11, 13]:

Definition 3 (Standard evaluation). For $a = (a_1, a_2, \ldots, a_n) \in \mathbb{F}^n$ and a skew polynomial $F \in \mathbb{F}[x; \sigma, \delta]$, we define its $(\sigma, \delta)$-evaluation, denoted by

$$F(a) = E_{\sigma, \delta}^a(F),$$

as the unique element $F(a) \in \mathbb{F}$ such that

$$F - F(a) \in (x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n).$$

We denote the corresponding total evaluation map by $E_{\sigma, \delta}$, and we use the notations $E_a$ and $E$ when there is no confusion about $\sigma$ and $\delta$.

These evaluation maps are well-defined and linear by Lemma 1. To conclude, we give a recursive formula on the fundamental functions of the total evaluation map $E_{\sigma, \delta}$, which is of computational interest. This result is an extension of the case $n = 1$ given in [13] Lemma 2.4 and [13] Eq. (2.3).

Theorem 2. The fundamental functions $N_m^{\sigma, \delta} = N_m : \mathbb{F}^n \rightarrow \mathbb{F}$, for $m \in \mathcal{M}$, of the $(\sigma, \delta)$-evaluation $E_{\sigma, \delta}$ in Definition 3 are given recursively as follows: $N_1(a) = 1$, and

$$
\begin{pmatrix}
N_{x_1m}(a) \\
N_{x_2m}(a) \\
\vdots \\
N_{xm}(a)
\end{pmatrix} = \sigma(N_m(a))a + \delta(N_m(a)),
$$

for all $m \in \mathcal{M}$ and all $a \in \mathbb{F}^n$.

Proof. We will use the compact matrix/vector notation in [4], and we proceed recursively on $m \in \mathcal{M}$, for fixed $a \in \mathbb{F}^n$.

Obviously, $N_1(a) = 1$. Assume now that it is true for a monomial $m \in \mathcal{M}$. Therefore, there exist skew polynomials $P_1, P_2, \ldots, P_n \in (x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n)$ such that, if we denote by $P$ the column vector whose $i$th row is $P_i$, for $i = 1, 2, \ldots, n$, then

$$xm = P + xN_m(a) = P + \sigma(N_m(a))x + \delta(N_m(a))$$

$$= P + \sigma(N_m(a))(x - a) + (\sigma(N_m(a))a + \delta(N_m(a))),$$

and the result follows by Lemma 1.

We recall that in the case $n = 1$ and $\delta = 0$, we have that $N_1(a) = N_{x^i}(a) = \sigma^{i-1}(a) \cdots \sigma(a)a$, for $i = 1, 2, \ldots$, hence the notation $N_m$ is a reminder of its similarity with the “norm” function [14].
4 Conjugacy and the product rule

From the previous section, we know that the \( (\sigma, \delta) \)-evaluation \( E_{\sigma, \delta} \) is linear. In this section, we will use the multiplicative properties of \( \sigma, \delta \) and the fundamental functions of \( E_{\sigma, \delta} \) to show that it preserves products of skew polynomials in a certain way. This property will be used in the next section to define ideals of zeros and to characterize which of them are bilateral (Proposition 3). It will be especially important in Section 8 for constructing skew polynomials of restricted degree with a given set of zeros.

We need the concept of conjugacy, where the case \( n = 1 \) was given in [13, Eq. (2.5)].

**Definition 4 (Conjugacy).** Given \( a \in \mathbb{F}^n \) and \( c \in \mathbb{F}^* \), we define the \( (\sigma, \delta) \)-conjugate, or just conjugate if there is no confusion, of \( a \) with respect to \( c \) as
\[
a^c = \sigma(c)ac^{-1} + \delta(c)c^{-1} \in \mathbb{F}^n.
\] (11)

We have the following properties, which extend the case \( n = 1 \) given in [13, Eq. (2.6)].

**Lemma 2.** Given \( a, b \in \mathbb{F}^n \) and \( c, d \in \mathbb{F}^* \), the following properties hold:

1. \( a^1 = a \) and \( (a^c)^d = a^{dc} \).

2. The relation \( a \sim b \) if, and only if, there exist \( e \in \mathbb{F}^* \) with \( b = ae \), is an equivalence relation on \( \mathbb{F}^n \).

If \( \mathbb{F} \) is a non-commutative ring, \( n = 1 \), \( \sigma = \text{Id} \) and \( \delta = 0 \), then the previous notion of conjugacy coincides with the usual one on the multiplicative monoid of \( \mathbb{F} \), which explains the terminology.

We may now establish and prove the product rule. The case \( n = 1 \) was first given in [13, Theorem 2.7]. We follow their proof using our matrix/vector notation.

**Theorem 3 (Product rule).** Given skew polynomials \( F, G \in \mathbb{F}[x; \sigma, \delta] \) and \( a \in \mathbb{F}^n \), if \( G(a) = 0 \), then \( (FG)(a) = 0 \), and if \( c = G(a) \neq 0 \), then
\[
(FG)(a) = F(a^c)G(a).
\] (12)

**Proof.** It is obvious from Lemma 11 and Definition 3 that, if \( G(a) = 0 \), then \( (FG)(a) = 0 \). Now assume that \( c = G(a) \neq 0 \). First observe that
\[
(x - a^c)c = \sigma(c)(x - a).
\]

Second, by Definition 3 there exist skew polynomials \( P_i, Q_i \in \mathbb{F}[x; \sigma, \delta] \), for \( i = 1, 2, \ldots, n \), such that
\[
F = P^T(x - a^c) + F(a^c), \quad \text{and} \quad G = Q^T(x - a) + G(a),
\]
where \( P \) and \( Q \) denote the column vectors whose \( i \)th rows are \( P_i \) and \( Q_i \), respectively, for \( i = 1, 2, \ldots, n \). Combining these facts, we obtain that
\[
FG = FQ^T(x - a) + FG(a)
\]
\( = (FQ^T + P^T \sigma(c)) (x - a) + F(a^c)G(a), \)

and we are done. 😄

This theorem can be stated when \( F \) is an arbitrary non-commutative ring by considering only the cases where \( c = 0 \) or \( c \) is a unit. The fact that only one of these two cases happen when \( F \) is a division ring or a field will be crucial in Proposition 3 and from Section 8 onwards.

5 Zeros of multivariate skew polynomials

In this section, we will define and give the basic properties of sets of zeros of multivariate skew polynomials and, conversely, sets of skew polynomials that vanish at a certain set of affine points, which will be crucial in Section 8 for Lagrange interpolation. Conceptually, they will also be important in Section 6 to define general skew polynomial rings with relations on the variables (non-free) and where evaluation still works in a natural way.

Observe that at this point our theory loses most of its analogies with the univariate case [11, 12, 13], since \( F[x; \sigma, \delta] \) is not a principal ideal domain if \( n > 1 \), hence the use of minimal skew polynomials as in [11, 12] is not possible. On the other hand, we gain analogy with respect to classical algebraic geometry:

**Definition 5 (Zeros of skew polynomials).** Given a set \( A \subseteq F[x; \sigma, \delta] \), we define its zero set as

\[
Z(A) = \{ a \in F^n \mid F(a) = 0, \forall F \in A \}.
\]

And given a set \( \Omega \subseteq F^n \), we define its associated ideal as

\[
I(\Omega) = \{ F \in F[x; \sigma, \delta] \mid F(a) = 0, \forall a \in \Omega \}.
\]

Observe that the ideal associated to a subset of \( F^n \) is indeed a left ideal:

**Proposition 1.** For any \( \Omega \subseteq F^n \), it holds that \( I(\Omega) \subseteq F[x; \sigma, \delta] \) is a left ideal.

*Proof.* It follows directly from the product rule (Theorem 3). Alternatively, it can be proven by noting that \( I(\Omega) = \bigcap_{a \in \Omega} (x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n) \).

We next list some basic properties of zero sets and ideals of zeros that follow from the definitions, in the same way as in classical algebraic geometry.

**Proposition 2.** Let \( \Omega, \Omega_1, \Omega_2 \subseteq F^n \) and \( A, A_1, A_2 \subseteq F[x; \sigma, \delta] \) be arbitrary sets. The following properties hold:

1. \( I(\{a\}) = (x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n) \) and \( Z(x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n) = \{a\} \), for all \( a = (a_1, a_2, \ldots, a_n) \in F^n \).
2. \( I(\emptyset) = (1) \) and \( Z(1) = \emptyset \).
3. \( I(F^n) \subseteq I(\Omega) \) and \( Z(\{0\}) = F^n \). That is, \( I(F^n) \) is the minimal ideal of zeros.
4. If $\Omega_1 \subseteq \Omega_2$, then $I(\Omega_2) \subseteq I(\Omega_1)$.

5. If $A_1 \subseteq A_2$, then $Z(A_2) \subseteq Z(A_1)$.

6. $I(\Omega_1 \cup \Omega_2) = I(\Omega_1) \cap I(\Omega_2)$.

7. $Z(A) = Z((A))$ and $Z(A_1 \cup A_2) = Z((A_1) + (A_2)) = Z(A_1) \cap Z(A_2)$.

8. $\Omega \subseteq Z(I(\Omega))$, and equality holds if, and only if, $\Omega = Z(B)$ for some $B \subseteq \mathbb{F}[x; \sigma, \delta]$.

9. $A \subseteq (A) \subseteq I(Z(A))$, and equality holds if, and only if, $A = I(\Psi)$ for some $\Psi \subseteq \mathbb{F}^n$.

Item 8 in the previous proposition motivates the definition of $P$-closed sets, where the case $n = 1$ was given in [11, 13]:

**Definition 6 (P-closures).** Given a subset $\Omega \subseteq \mathbb{F}^n$, we define its $P$-closure as

$$\overline{\Omega} = Z(I(\Omega)),$$

and we say that $\Omega$ is $P$-closed if $\overline{\Omega} = \Omega$.

By Proposition 2, Item 8, $P$-closed sets correspond to sets of zeros of sets of skew polynomials, and we have the following:

**Lemma 3.** Given a subset $\Omega \subseteq \mathbb{F}^n$, it holds that $\overline{\Omega}$ is the smallest $P$-closed subset of $\mathbb{F}^n$ containing $\Omega$.

### 6 General and minimal skew polynomial rings

In this section, we define general skew polynomial rings as those with a set of relations on the variables and where evaluation is still as in Definition 3. In particular, by considering a maximum set of such relations, we may define minimal skew polynomial rings.

Note that the whole space $\mathbb{F}^n$ is $P$-closed, and Item 3 in Proposition 2 says that, for evaluation purposes, we may just consider the quotient left module

$$\mathbb{F}[x; \sigma, \delta]/I(\mathbb{F}^n),$$

which is a ring if $I(\mathbb{F}^n)$ is a bilateral ideal, and in such case we obtain the above mentioned minimal skew polynomial ring where the $(\sigma, \delta)$-standard evaluation is still defined.

In the following proposition, we characterize when an ideal of zeros is bilateral, which includes in particular the ideal $I(\mathbb{F}^n)$:

**Proposition 3.** Given a subset $\Omega \subseteq \mathbb{F}^n$, the following are equivalent:

1. $I(\Omega)$ is a bilateral ideal.

2. If $F \in I(\Omega)$ and $c \in \mathbb{F}$, then $Fc \in I(\Omega)$.

3. If $a \in \overline{\Omega}$, then $a^c \in \overline{\Omega}$, for all $c \in \mathbb{F}^*$.
4. If \( a \in \Omega \), then \( a^c \in \Omega \), for all \( c \in F^* \).

In particular, \( I(F^n) \) is a bilateral ideal.

**Proof.** We prove the following implications:

1) \( \implies \) 2): Trivial.

2) \( \implies \) 3): Let \( a \in \Omega \), \( F \in I(\Omega) \) and \( c \in F^* \). First, it holds that \( I(\Omega) = I(\Omega) \) by Items 8 and 9 in Proposition 2 and \( Fc \in I(\Omega) \) by hypothesis. Thus

\[
0 = (Fc)(a) = F(a^c)c
\]

by the product rule (Theorem 3). Hence \( a^c \in Z(I(\Omega)) = \Omega \).

3) \( \implies \) 4): Trivial from \( \Omega \subseteq \Omega \).

4) \( \implies \) 1): Let \( F \in I(\Omega) \) and \( G \in F[x; \sigma, \delta] \), fix \( a \in \Omega \) and define \( c = G(a) \). If \( c = 0 \), then \((FG)(a) = 0\) by the product rule. If \( c \neq 0 \), by hypothesis and the product rule, we have that

\[
(FG)(a) = F(a^c)G(a) = 0,
\]

since \( a^c \in \Omega \) and \( F \in I(\Omega) = I(\Omega) \). Hence \((FG)(a) = 0\) for any \( a \in \Omega \) and thus \( FG \in I(\Omega) \), and we are done. \( \square \)

Observe that, to prove 4) \( \implies \) 1), we need \( F \) to be a division ring, since we use that every \( c \in F \setminus \{0\} \) is invertible.

We may now define (non-free) general skew polynomial rings and, in particular, a minimal one.

**Definition 7 (Skew polynomial rings).** For any bilateral ideal \( I \subseteq I(F^n) \), we say that the quotient ring

\[
F[x; \sigma, \delta]/I
\]

is a skew polynomial ring with matrix morphism \( \sigma \) and vector derivation \( \delta \). The minimal skew polynomial ring with matrix morphism \( \sigma \) and vector derivation \( \delta \) is defined as that obtained when \( I = I(F^n) \).

This is exactly what happens with conventional multivariate polynomial rings (the case \( \sigma = \text{Id} \) and \( \delta = 0 \)). One can consider the free multivariate polynomial ring and define the conventional evaluation on it. In that case, \( I(F^n) \) contains the bilateral ideal \( J \) generated by all polynomials \( m - n \), where \( m, n \in M \) are such that \( n \) is obtained from \( m \) by a permutation of the variables. If \( F \) is infinite, then \( I(F^n) = J \), whereas

\[
I(F^n) = J + (x_1^q - x_1, x_2^q - x_2, \ldots, x_n^q - x_n)
\]

(13) if \( F \) is finite and has \( q \) elements. The results in the following sections will be proven for the free multivariate skew polynomial ring. By projecting onto the quotient, they can also be stated for any multivariate skew polynomial ring.

We conclude this section by showing that skew polynomial rings can form iterated sequences of rings by adding variables, even though we do not consider iterated skew polynomial rings in the standard way, as shown in Appendix. The proof of the following result is straightforward.
Proposition 4. Let $0 < r < n$ be a positive integer, let $\tau : F \to F^{r \times r}$ and $\nu : F \to F^{(n-r) \times (n-r)}$ be matrix morphisms and let $\delta_\tau : F \to F^r$ and $\delta_\nu : F \to F^{(n-r)}$ be a $\tau$-vector derivation and a $\nu$-vector derivation, respectively. Define $\sigma : F \to F^{n \times n}$ and $\delta_\sigma : F \to F^n$ by

$$\sigma(a) = \begin{pmatrix} \tau(a) & 0 \\ 0 & \nu(a) \end{pmatrix} \quad \text{and} \quad \delta_\sigma(a) = \begin{pmatrix} \delta_\tau(a) \\ \delta_\nu(a) \end{pmatrix},$$

for all $a \in F$. Then $\sigma$ is a matrix morphism and $\delta_\sigma$ is a $\sigma$-vector derivation. Consider now the natural inclusion map

$$\rho : F[x_1, x_2, \ldots, x_r; \tau, \delta_\tau] \to F[x_1, x_2, \ldots, x_n; \sigma, \delta_\sigma].$$

The following properties hold:

1. $\rho$ is a one to one ring morphism.

2. For all $F \in F[x_1, x_2, \ldots, x_r; \tau, \delta_\tau]$, all $a_\tau \in F^r$ and all $a_\nu \in F^{n-r}$, it holds that

$$E_{a_\sigma}^{\tau, \delta_\tau}(F) = E_{a_\tau}^{\sigma, \delta_\sigma}(\rho(F)),$$

where $a_\sigma = (a_\tau, a_\nu) \in F^n$.

3. For any bilateral ideal $J \subseteq I(F^n)$, it holds that $\rho^{-1}(J) \subseteq I(F^r)$ is a bilateral ideal and $\rho$ can be restricted to a one to one ring morphism

$$\rho : F[x_1, x_2, \ldots, x_r; \tau, \delta_\tau]/\rho^{-1}(J) \to F[x_1, x_2, \ldots, x_n; \sigma, \delta_\sigma]/J.$$

This holds in particular for $J = I(F^n)$, where $\rho^{-1}(J) = I(F^r)$.

In particular, if $\sigma$ is given as in Example 1, then $F[x; \sigma, \delta]$ contains a sequence of $n$ nested skew polynomial rings, where the first one is the univariate skew polynomial ring $F[x; \sigma_1, \delta]$. 

7 P-generators, P-independence and P-bases

The main feature of P-closed sets is that they can be “generated” by certain subsets, called P-bases, that control the possible values given by a function defined by a skew polynomial on such sets, as we will show in the next section. These concepts were defined for the case $n = 1$ in [11, 12]. We start with the main definitions:

**Definition 8 (P-generators).** Given a P-closed set $\Omega \subseteq F^n$, we say that $G \subseteq \Omega$ generates it if $G = \Omega$, and it is called a set of P-generators for $\Omega$. We say that $\Omega$ is finitely generated if it has a finite set of P-generators.

**Definition 9 (P-independence).** We say that $a \in F^n$ is P-independent from $\Omega \subseteq F^n$ if it does not belong to $\Omega$. A set $\Omega \subseteq F^n$ is called P-independent if every $a \in \Omega$ is P-independent from $\Omega \setminus \{a\}$. In general, P-dependent means not P-independent.
**Definition 10 (P-bases).** Given a P-closed set $\Omega \subseteq \mathbb{F}^n$, we say that a subset $B \subseteq \Omega$ is a P-basis of $\Omega$ if it is P-independent and $\overline{B} = \Omega$.

The following is the main result of this section, where Item 3 will be crucial in order to perform Lagrange interpolation recursively.

**Proposition 5.** Given sets $B \subseteq \Omega \subseteq \mathbb{F}^n$, where $\Omega = \overline{B}$, the following are equivalent:

1. $B$ is a P-basis of $\Omega$.
2. If $G \subseteq B$ and $\overline{G} = \Omega$, then $G = B$. That is, $B$ is a minimal set of P-generators of $\Omega$.
3. (If $B$ is finite) For any ordering $b_1, b_2, \ldots, b_M$ of the elements in $B$ and for $i = 0, 1, 2, \ldots, M - 1$, it holds that $b_{i+1}$ is P-independent from $B_i = \{b_1, b_2, \ldots, b_i\}$, where $B_0 = \emptyset$.

**Proof.** We prove each implication separately:

1) $\implies$ 2): Assume that there exists $G \subsetneq B$ with $\overline{G} = \Omega$ and let $a \in B \setminus G$. Then

$$a \in \Omega = \overline{G} = \overline{B \setminus \{a\}},$$

hence Item 1 does not hold.

2) $\implies$ 1): Assume that $B$ is not P-independent and take $a \in B$ with $a \in \overline{B \setminus \{a\}}$. Define $G = B \setminus \{a\} \subsetneq B$. It holds that

$$B = \{a\} \cup (B \setminus \{a\}) \subseteq \overline{G},$$

hence $\overline{G} = \Omega$ and Item 2 does not hold.

1) $\implies$ 3): Assume that $b_{i+1}$ is P-dependent from $B_i$ for a given $i$ and a given ordering of $B$. Then

$$b_{i+1} \in \overline{B_i} \subseteq \overline{B \setminus \{b_{i+1}\}},$$

hence Item 1 does not hold.

3) $\implies$ 1): Assume that $a$ is P-dependent from $B \setminus \{a\}$ and order the $M$ elements in $B$ in such a way that $b_M = a$. Then $b_M$ is P-dependent from $B_{M-1}$ and Item 3 does not hold.

We have the following important immediate consequence of Item 2 in the previous proposition:

**Corollary 1.** If a P-closed set is finitely generated, then it admits a finite P-basis.
8 Skew polynomial functions and Lagrange interpolation

In this section, we give the first main result of this paper. We show, in a Lagrange-type interpolation theorem, what values a function given by a skew polynomial can take when evaluated on a finitely generated P-closed set (Theorem 4). This result will be crucial in the next section to describe the image and kernel of the evaluation map. On the way, we derive other important results on P-closed sets.

Observe first that the total \((\sigma, \delta)\)-evaluation gives a linear map
\[
E_{\Omega}^{\sigma, \delta} : \mathbb{F}[x; \sigma, \delta] \rightarrow \mathbb{F}^\Omega,
\]
when restricted to evaluating over a subset \(\Omega \subseteq \mathbb{F}^n\) or, in other words, by composing \(E_{\Omega}^{\sigma, \delta} = \pi_\Omega \circ E_{\Omega}^{\sigma, \delta}\), where \(\pi_\Omega : \mathbb{F}^\Omega \rightarrow \mathbb{F}^\Omega\) is the canonical projection map.

Hence \(E_{\Omega}^{\sigma, \delta}\) gives a correspondence between multivariate skew polynomials \(F \in \mathbb{F}[x; \sigma, \delta]\) and some particular functions \(f = E_{\Omega}^{\sigma, \delta}(F) : \Omega \rightarrow \mathbb{F}\). Such functions will be called multivariate skew polynomial functions over \(\Omega\).

Formally, the objective of this section and the next one is to describe the kernel and image of the map \(E_{\Omega}^{\sigma, \delta}\) when \(\Omega\) is P-closed and finitely generated. We start with the following lemma, which is a key tool in Lagrange interpolation:

**Lemma 4.** Let \(\mathcal{B} \subseteq \mathbb{F}^n\) be a finite P-independent set and let \(b \notin \overline{\mathcal{B}}\). There exists \(F \in I(\mathcal{B}) \setminus I(\mathcal{B} \cup \{b\})\) such that \(\deg(F) \leq \#\mathcal{B}\).

**Proof.** First we prove that \(I(\mathcal{B}) \setminus I(\mathcal{B} \cup \{b\}) \neq \emptyset\). Assume the opposite. Then
\[
\overline{\mathcal{B}} = Z(I(\mathcal{B})) = Z(I(\mathcal{B} \cup \{b\})),
\]
and \(\mathcal{B} \cup \{b\} \subseteq Z(I(\mathcal{B} \cup \{b\}))\) by Item 8 in Proposition \(\Box\). Thus \(b \in \overline{\mathcal{B}}\), which is a contradiction.

Now let \(\mathcal{B} = \{b_1, b_2, \ldots, b_M\}\) with \(M = \#\mathcal{B}\), let \(\prec\) be any ordering of \(\mathcal{M}\) preserving degrees, and take \(F \in I(\mathcal{B}) \setminus I(\mathcal{B} \cup \{b\})\) such that \(\text{LM}(F)\) is minimum possible with respect to \(\prec\). Assume that \(\deg(F) \geq M + 1\), which implies that \(\deg(\text{LM}(F)) \geq M + 1\) by the choice of the ordering \(\prec\).

Let \(\text{LM}(F) = mx_{i_1}x_{i_2} \cdots x_{i_{M+1}}\), for some \(m \in \mathcal{M}\). By the product rule (Theorem \(\Box\)), we may choose elements \(a_1, a_2, \ldots, a_{M+1} \in \mathbb{F}\) such that
\[
G = m(x_{i_1} - a_1)(x_{i_2} - a_2) \cdots (x_{i_{M+1}} - a_{M+1})
\]
satisfies that \(G(b_i) = 0\), for \(i = 1, 2, \ldots, M + 1\), denoting \(b_{M+1} = b\). In particular, there exists \(a \in \mathbb{F}\) such that \(H = F - aG\) satisfies \(\text{LM}(H) \prec \text{LM}(F)\), since \(\text{LM}(F) = \text{LM}(G)\). Now, by the definition of \(G\), it holds that
\[
H = F - aG \in I(\mathcal{B}) \setminus I(\mathcal{B} \cup \{b\}),
\]
which is absurd by the minimality of \(\text{LM}(F)\). Therefore \(\deg(F) \leq M\) and we are done. \(\Box\)
Observe that in the previous proof, we are making use of Theorem 3 in its full form to obtain \( G \). Moreover, this proof does not work if \( F \) is not a division ring, since we need, for given \( c \in F \), that either \( c = 0 \) or \( c \) is invertible.

The main result of this section is a Lagrange-type interpolation theorem in \( F[x; \sigma, \delta] \), whose proof is given by an iterative Newton-type algorithm thanks to Item 3 in Proposition 5. This result extends the case \( n = 1 \) given in [11, Theorem 8] (see also the beginning of [13, Section 5]). Newton-type iterative algorithms have been given in [21] for univariate skew polynomials, and in [15] for their free left modules.

**Theorem 4 (Lagrange interpolation).** Let \( \Omega \subseteq F^n \) be a finitely generated \( P \)-closed set with finite \( P \)-basis \( \mathcal{B} = \{ b_1, b_2, \ldots , b_M \} \). The following hold:

1. If \( E_{\mathcal{B}}^{\sigma, \delta}(F) = E_{\Omega}^{\sigma, \delta}(G) \), then \( E_{\Omega}^{\sigma, \delta}(F) = E_{\Omega}^{\sigma, \delta}(G) \), for all \( F, G \in F[x; \sigma, \delta] \). That is, the values of a skew polynomial function \( f : \Omega \to F \) are uniquely given by \( f(b_1), f(b_2), \ldots , f(b_M) \).

2. For every \( a_1, a_2, \ldots , a_M \in F \), there exists \( F \in F[x; \sigma, \delta] \) such that \( \deg(F) < M \) and \( F(b_i) = a_i \), for \( i = 1, 2, \ldots , M \).

**Proof.** We prove each item separately.

1. We just need to prove that \( E_{\mathcal{B}}^{\sigma, \delta}(F) = 0 \) implies \( E_{\Omega}^{\sigma, \delta}(F) = 0 \). By definition, \( \mathcal{B} \subseteq Z(F) \), and by Proposition 2 it holds that \( I(Z(F)) \subseteq I(\mathcal{B}) \) and \( \Omega = \overline{\mathcal{B}} = Z(I(\mathcal{B})) \subseteq Z(I(Z(F))) = Z(F) \), and the result follows.

2. Let \( \mathcal{B} = \{ b_1, b_2, \ldots , b_M \} \) as in Proposition 3 Item 3. We prove the result iteratively for each of the \( P \)-independent sets \( \mathcal{B}_i \), \( i = 1, 2, \ldots , M \), as in Newton’s algorithm.

We start by defining the skew polynomial \( F_1 = a_1 \), which obviously satisfies \( F_1(b_1) = a_1 \) and \( \deg(F_1) < 1 \). Now assume that \( M > 1, 1 \leq i \leq M - 1 \) and there exists a skew polynomial \( F_i \) such that \( F_i(b_j) = a_j \), for \( j = 1, 2, \ldots , i \), and \( \deg(F_i) < i \). By Lemma 4 there exists \( G \in I(\{ b_1, b_2, \ldots , b_i \}) \setminus I(\{ b_1, b_2, \ldots , b_{i+1} \}) \) such that \( \deg(G) < i + 1 \). The skew polynomial

\[
F_{i+1} = F_i + (a_{i+1} - F_i(b_{i+1})) G(b_{i+1})^{-1} G
\]

satisfies that \( F_{i+1}(b_j) = a_j \), for \( j = 1, 2, \ldots , i + 1 \), and \( \deg(F_{i+1}) < i + 1 \).

In the rest of the section, we derive some important consequences of this theorem. We start with the concept of dual \( P \)-bases.
Definition 11 (Dual P-bases). Given a finite P-basis $\mathcal{B} = \{b_1, b_2, \ldots, b_M\}$ of a P-closed set $\Omega \subseteq \mathbb{F}^n$, we say that a set of skew polynomials $\mathcal{B}^* = \{F_1, F_2, \ldots, F_M\} \subseteq \mathbb{F}[x; \sigma, \delta]$ is a dual P-basis of $\mathcal{B}$ if $F_i(b_j) = \delta_{ij}$ for all $i, j = 1, 2, \ldots, M$.

We have the following immediate consequence of Theorem 4 on the existence and uniqueness of dual P-bases:

**Corollary 2.** Any finite P-basis, with $M$ elements, of a P-closed set $\Omega$ admits a dual P-basis consisting of $M$ skew polynomials of degree less than $M$. Moreover, any two dual P-bases of the same P-basis define the same skew polynomial functions over $\Omega$.

An important consequence of Theorem 4 is the following result on the sizes of P-bases:

**Corollary 3.** Any two P-bases of a finitely generated P-closed set are finite and have the same number of elements.

**Proof.** Given a finite P-basis $\mathcal{B} = \{b_1, b_2, \ldots, b_M\}$ of size $M$ of a P-closed set $\Omega$, we will show first that $\text{Im}(E^\sigma_\Omega)$ is a vector subspace of $\mathbb{F}^\Omega$ with basis

$$\{ E^\sigma_\Omega(F_1), E^\sigma_\Omega(F_2), \ldots, E^\sigma_\Omega(F_M) \},$$

for any dual P-basis $\{F_1, F_2, \ldots, F_M\}$ of $\mathcal{B}$. Assume that there exist $\lambda_1, \lambda_2, \ldots, \lambda_M \in \mathbb{F}$ such that $\sum_{i=1}^n \lambda_i E^\sigma_\Omega(F_i) = 0$. Defining $F = \sum_{i=1}^n \lambda_i F_i$, it follows that

$$E^\sigma_\Omega(F) = E^\sigma_\Omega \left( \sum_{i=1}^n \lambda_i F_i \right) = \sum_{i=1}^n \lambda_i E^\sigma_\Omega(F_i) = 0,$$

thus $\lambda_i = F(b_i) = 0$, for $i = 1, 2, \ldots, M$, and the set in (15) is linearly independent. Now, given $F \in \mathbb{F}[x; \sigma, \delta]$, define $G = F - \sum_{i=1}^n F(b_i) F_i$. By definition, we have that $E^\sigma_{\mathcal{B}}(G) = 0$. Therefore $E^\sigma_\Omega(G) = 0$ by Theorem 4 thus

$$E^\sigma_\Omega(F) = \sum_{i=1}^n F(b_i) E^\sigma_\Omega(F_i),$$

and we conclude that the set in (15) is a basis of $\text{Im}(E^\sigma_\Omega)$.

In particular, $\dim(\text{Im}(E^\sigma_\Omega)) = M$ and the result follows for finite P-bases, since $\dim(\text{Im}(E^\sigma_\Omega))$ is independent of the choice of finite P-basis.

Finally, if there exists an infinite P-basis $\mathcal{B}'$ of $\Omega$, we may take a P-independent subset $\mathcal{C} \subseteq \mathcal{B}'$ of size $M + 1$, define $\Psi = \mathcal{C} \subseteq \Omega$ and we would have that $\dim(\text{Im}(E^\sigma_\Psi)) = M + 1$, and the canonical projection map

$$\pi_\Psi : \text{Im}(E^\sigma_\Omega) \longrightarrow \text{Im}(E^\sigma_\Psi)$$

is onto. This is absurd and the result follows. \qed
We conclude with the following natural definition, which is motivated by the previous corollary. It is an extension of the case \( n = 1 \) given in [11, 13].

**Definition 12 (Rank of P-closed sets).** Given a finitely generated P-closed set \( \Omega \subseteq \mathbb{F}^n \), we define its rank, denoted by \( \text{Rk}(\Omega) \), as the size of any of its P-bases.

9 The image and kernel of the evaluation map

In this section, we give the second main result of this paper. We describe the vector space of skew polynomial functions and, to that end, we obtain the dimensions and some bases of the image and kernel of the evaluation map (Theorem 5). As a conclusion to the section, we also deduce a vector space description of quotients of a skew polynomial ring, which includes the minimal skew polynomial ring when \( \mathbb{F} \) is a finite field.

We need the following auxiliary lemmas. The first can be seen as a refinement of Item 1 in Theorem 4:

**Lemma 5.** Let \( \Omega \subseteq \mathbb{F}^n \) be a finitely generated P-closed set and let \( \mathcal{G} \subseteq \Omega \). It holds that \( \Omega = \mathcal{G} \) if, and only if,
\[
\dim(\text{Im}(E_{\Omega}^{\sigma,\delta})) = \dim(\text{Im}(E_{\mathcal{G}}^{\sigma,\delta})).
\]

**Proof.** First, recall that the given dimensions are finite due to the proof of Corollary 3. The direct implication is in essence Item 1 in Theorem 4. For the reversed implication, the equality on dimensions implies that the projection map \( \text{Im}(E_{\Omega}^{\sigma,\delta}) \to \text{Im}(E_{\mathcal{G}}^{\sigma,\delta}) \) is a vector space isomorphism. Thus \( I(\mathcal{G}) = I(\Omega) \), which implies that
\[
\mathcal{G} = Z(I(\mathcal{G})) = Z(I(\Omega)) = \Omega.
\]

The next lemma is a further refinement of Proposition 5:

**Lemma 6.** If \( \mathcal{B} \subseteq \mathbb{F}^n \) is finite and P-independent, and \( a \in \mathbb{F}^n \setminus \overline{\mathcal{B}} \), then \( \mathcal{B}' = \mathcal{B} \cup \{a\} \) is P-independent.

As a consequence, a finite subset \( \mathcal{B} \subseteq \mathbb{F}^n \) is a P-basis of a finitely generated P-closed set \( \mathcal{B} \subseteq \Omega \subseteq \mathbb{F}^n \) if, and only if, the following property holds: \( \mathcal{B} \) is P-independent, and if \( \mathcal{B} \subseteq \mathcal{G} \subseteq \Omega \) and \( \mathcal{G} \) is P-independent, then \( \mathcal{G} = \mathcal{B} \). That is, \( \mathcal{B} \) is a maximal P-independent set in \( \Omega \).

**Proof.** Since \( a \notin \overline{\mathcal{B}} \), it holds that \( I(\mathcal{B}) \setminus I(\mathcal{B}') \neq \emptyset \), as in the proof of Lemma 4. Thus
\[
\dim(\text{Im}(E_{\mathcal{B}'}^{\sigma,\delta})) \geq \dim(\text{Im}(E_{\mathcal{B}}^{\sigma,\delta})) + 1.
\]

By the previous lemma and the proof of Corollary 5, we conclude that \( \text{Rk}(\overline{\mathcal{B}'}) = \text{Rk}(\overline{\mathcal{B}}) + 1 \). Again by Corollary 5 and its proof, we conclude that \( \mathcal{B}' \) is a P-basis of \( \overline{\mathcal{B}'} \) and, in particular, it is P-independent. 

\[18\]
Before giving the main result of this section, we need another consequence of Theorem 4, which will allow us to define the concepts of complementary $P$-closed sets and $P$-bases:

**Corollary 4.** Let $\Psi \subseteq \Omega \subseteq \mathbb{F}^m$ be $P$-closed sets. If $\Omega$ is finitely generated, then so is $\Psi$. Moreover, for any finite $P$-basis $B$ of $\Psi$, there exists a finite $P$-independent set $C \subseteq \Omega$ such that $B \cap C = \emptyset$ and $B \cup C$ is a $P$-basis of $\Omega$. In particular, if $\Phi = C$, then

$$\text{Rk}(\Omega) = \text{Rk}(\Psi) + \text{Rk}(\Phi).$$

**Proof.** Assume that $\Psi$ is not finitely generated. Using Lemma 6, we may construct iteratively a $P$-independent set $D \subseteq \Psi$ of size $\text{Rk}(\Omega) + 1$. This is absurd by the same argument as in the proof of Corollary 3.

Now, we may extend $B$ to a maximal $P$-independent subset of $\Omega$ by adding iteratively to it elements $c_1, c_2, \ldots, c_N \in \Omega$, again by Lemma 6, which would be a $P$-basis of $\Omega$ by maximality (again by Lemma 6). By defining $C = \{c_1, c_2, \ldots, c_N\}$, the rest of the claims in the corollary follow.

**Definition 13 (Complementary $P$-closed sets and $P$-bases).** If $\Psi \subseteq \Omega \subseteq \mathbb{F}^n$ are finitely generated $P$-closed sets and $B$ and $C$ are as in the previous Corollary, then we say that $\Phi = C \subseteq \Omega$ is a complementary $P$-closed set of $\Psi$ in $\Omega$, and $C$ is a complementary $P$-basis of $B$ in $\Omega$.

We may now state and prove the second main result of the paper, which describes the image and kernel of $E_{\sigma, \delta}^\Omega$ as vector spaces over $\mathbb{F}$ with some particular bases.

**Theorem 5.** Given a finitely generated $P$-closed set $\Omega \subseteq \mathbb{F}^n$ with finite $P$-basis $B$, we have that

1. $\text{Im}(E_{\sigma, \delta}^\Omega)$ is a vector space over $\mathbb{F}$ of dimension $M = \text{Rk}(\Omega)$ with basis

   $$E_{\sigma, \delta}^\Omega(B^*) = \left\{ E_{\sigma, \delta}^\Omega(F_1), E_{\sigma, \delta}^\Omega(F_2), \ldots, E_{\sigma, \delta}^\Omega(F_M) \right\},$$

   where $B^* = \{F_1, F_2, \ldots, F_M\}$ is a dual $P$-basis of $B$. Observe that, by Corollary 2, $E_{\sigma, \delta}^\Omega(B^*)$ depends only on $B$ and not on the choice of the dual $P$-basis.

2. If $\mathbb{F}^n$ is finitely generated as $P$-closed set, $C$ is a complementary $P$-basis of $B$ in $\mathbb{F}^n$, and $C^* = \{G_1, G_2, \ldots, G_N\}$ is a dual $P$-basis of $C$ that is part of a dual $P$-basis $(B \cup C)^*$ of $B \cup C$, then

   $$\text{Ker}(E_{\sigma, \delta}^\Omega) = I(\mathbb{F}^n) \oplus \langle G_1, G_2, \ldots, G_N \rangle,$$

   as vector spaces over $\mathbb{F}$, and $G_1, G_2, \ldots, G_N$ are linearly independent over $\mathbb{F}$.

**Proof.** The proof of Item 1 was given in the proof of Corollary 3. Now we prove Item 2:

First, $G_1, G_2, \ldots, G_N$ are linearly independent over $\mathbb{F}$ by Item 1, since so are their evaluations over $\Phi = C$.
Now we show that, if \( F \in I(F^n) \cap \langle G_1, G_2, \ldots, G_N \rangle \), then \( F = 0 \). To that end, write \( F = \sum_{i=1}^{N} \lambda_i G_i \), for some \( \lambda_i \in F \) and all \( i = 1, 2, \ldots, N \). Since \( F \in I(F^n) \) it holds that \( E^{\sigma, \delta}_F(G) = 0 \), and since \( E^{\sigma, \delta}_F(G_1), E^{\sigma, \delta}_F(G_2), \ldots, E^{\sigma, \delta}_F(G_M) \) are linearly independent by Item 1, we conclude that \( F = 0 \).

Next let \( F \in \text{Ker}(E^{\sigma, \delta}_\Omega) \). Then by Theorem 4, it holds that \( F = -\sum_{i=1}^{N} F(c_i)G_i \in I(F^n) \), since this skew polynomial vanishes at \( B \cup C \), and this set is a P-basis of \( F^n \). Hence \( F \in I(F^n) \oplus \langle G_1, G_2, \ldots, G_N \rangle \).

Conversely, let \( F \in I(F^n) \oplus \langle G_1, G_2, \ldots, G_N \rangle \). By the assumptions, we have that \( F(b) = 0 \), for all \( b \in \mathcal{B} \). Hence \( F \in \text{Ker}(E^{\sigma, \delta}_\Omega) \) again by Theorem 4.

We conclude with the following consequence, which describes the quotient left modules over the ideal associated to a finitely generated P-closed set. Such quotient left modules include the minimal skew polynomial ring if \( F^n \) is finitely generated, which is the case if \( F \) is finite.

**Corollary 5.** If \( \{ F_1, F_2, \ldots, F_M \} \) is a dual P-basis of a finitely generated P-closed set \( \Omega \subseteq F^n \), then
\[
F[x; \sigma, \delta]/I(\Omega) \cong \langle F_1, F_2, \ldots, F_M \rangle
\]
as vector spaces, where the isomorphism is given by inverting the projection to the quotient ring. Moreover, \( F_1, F_2, \ldots, F_M \) are linearly independent, and hence
\[
\dim(F[x; \sigma, \delta]/I(\Omega)) = \text{Rk}(\Omega).
\]

In particular, the minimal skew polynomial ring \( F[x; \sigma, \delta]/I(F^n) \) is a finite-dimensional vector space over \( F \) of dimension \( \text{Rk}(F^n) \) if \( F^n \) is finitely generated.

**Proof.** Again, it follows directly from Item 1 in Theorem 5 that \( F_1, F_2, \ldots, F_M \) are linearly independent over \( F \), since so are their evaluations over \( \Omega \).

Now consider the linear projection map \( \rho : \langle F_1, F_2, \ldots, F_M \rangle \rightarrow F[x; \sigma, \delta]/I(\Omega) \). To show that it is onto, it suffices to observe that, given \( F \in F[x; \sigma, \delta] \), it holds that
\[
\rho(F) = \rho \left( \sum_{i=1}^{M} F(b_i)F_i \right),
\]
by Item 1 in Theorem 4 where \( \mathcal{B} = \{ b_1, b_2, \ldots, b_M \} \) is the P-basis of \( \Omega \) associated to \( \{ F_1, F_2, \ldots, F_M \} \).

Finally, the evaluation map \( F[x; \sigma, \delta]/I(\Omega) \rightarrow \text{Im}(E^{\sigma, \delta}_\Omega) \) is a vector space isomorphism by definition, thus by Item 1 in Theorem 5 it holds that
\[
\dim(\langle F_1, F_2, \ldots, F_M \rangle) = M = \dim(\text{Im}(E^{\sigma, \delta}_\Omega)) = \dim(F[x; \sigma, \delta]/I(\Omega)).
\]

Hence \( \rho \) is a vector space isomorphism, and we are done.
As shown in Equation (13), if $F$ is finite and has $q$ elements, then
\[
\dim(F[x]/I(F^n)) = q^n = \text{Rk}(F^n),
\]
since $\text{Rk}(F^n) = \#F^n = q^n$ in the conventional case. Hence the previous corollary extends this well-known result for finite fields.

10 Skew Vandermonde matrices and how to find P-bases

In the univariate case ($n = 1$), Vandermonde matrices are a crucial tool to explicitly compute Lagrange interpolating polynomials. The multivariate case works similarly, although only existence of interpolating skew polynomials may be derived, and not their uniqueness. This is due to the non-square form of multivariate Vandermonde matrices.

In this section, we extend the concept of skew Vandermonde matrix from the univariate case in [11, 13] to the multivariate case. As applications and thanks to the recursive formula in Theorem 2, we show how to explicitly compute P-bases, dual P-bases and Lagrange interpolating skew polynomials over finitely generated P-closed sets.

The case $n = 1$ in the following definition was given in [13, Eq. (4.1)], and previously in [11]:

**Definition 14 (Skew Vandermonde matrices).** Let $\mathcal{N} \subseteq \mathcal{M}$ be a finite set of monomials and let $\Omega = \{b_1, b_2, \ldots, b_M\} \subseteq F^n$. We define the corresponding $(\sigma, \delta)$-skew Vandermonde matrix, denoted by $V_{\mathcal{N}}^{\sigma,\delta}(\Omega)$, as the $(\#\mathcal{N}) \times M$ matrix over $F$ whose rows are given by
\[
(N_m(b_1), N_m(b_2), \ldots, N_m(b_M)) \in F^M,
\]
for all $m \in \mathcal{N}$, in some given order. If $d$ is a positive integer, we define $\mathcal{M}_d$ as the set of monomials of degree less than $d$, and we denote
\[
V_{\mathcal{M}_d}^{\sigma,\delta}(\Omega) = V_{\mathcal{M}_d}(\Omega).
\]

An important consequence of Theorem 3 is finding the rank and a P-basis of a given finitely generated P-closed set:

**Proposition 6.** Given a finite set $\mathcal{G} \subseteq F^n$ with $M$ elements, and $\Omega = \overline{\mathcal{G}}$, it holds that
\[
\text{Rk} \left( V_{\mathcal{M}}^{\sigma,\delta}(\mathcal{G}) \right) = \text{Rk}(\Omega).
\]
Moreover, a subset $\mathcal{B} \subseteq \mathcal{G}$ is a P-basis of $\Omega$ if, and only if, $\#\mathcal{B} = \text{Rk}(\Omega) = \text{Rk}(V_{\#\mathcal{B}}^{\sigma,\delta}(\mathcal{B}))$.

Hence applying Gaussian elimination to the matrix $V_{\mathcal{M}}^{\sigma,\delta}(\mathcal{G})$, we may find the rank of $\Omega$ and at least one of its P-bases.

**Proof.** First, by Corollary 2 and Theorem 4, it holds that $\text{Im}(E^{\sigma,\delta}_\Omega)$ is the vector space generated by the evaluations $(N_m(a))_{a \in \Omega}$, for $m \in \mathcal{M}_M$. By Lemma 5 to calculate $\dim(\text{Im}(E^{\sigma,\delta}_\Omega))$, we may restrict such evaluations to points in $\mathcal{G}$, and the first claim follows.
Now we prove the second claim. If \( \mathcal{B} \) is a P-basis of \( \Omega \), then \( \# \mathcal{B} = \text{Rk}(\Omega) \) by definition, and \( \text{Rk}(\Omega) = \text{Rk}(V_{\# \mathcal{B}}^{\sigma, \delta}(\mathcal{B})) \) by the first claim.

Conversely, if \( \# \mathcal{B} = \text{Rk}(\Omega) = \text{Rk}(V_{\# \mathcal{B}}^{\sigma, \delta}(\mathcal{B})) \), then by Theorem 5 it holds that

\[
\dim(\text{Im}(E_{\Omega}^{\sigma, \delta})) = \text{Rk}(\Omega) = \text{Rk}(V_{\# \mathcal{B}}^{\sigma, \delta}(\mathcal{B})) \leq \dim(\text{Im}(E_{\mathcal{B}}^{\sigma, \delta})).
\]

Since the opposite inequality always holds, it follows from Lemma 5 that \( \overline{\mathcal{B}} = \Omega \). Now, \( \mathcal{B} \) is a minimal set of P-generators of \( \Omega \), since \( \# \mathcal{B} = \text{Rk}(\Omega) \), all minimal sets of P-generators are P-bases by Proposition 4 and all have the same size by Corollary 3. Hence we conclude that \( \mathcal{B} \) is a P-basis of \( \Omega \).

A classical way of stating the Lagrange interpolation theorem by means of Vandermonde matrices is as follows, which is an immediate consequence of Theorem 4:

**Corollary 6.** Let \( \Omega \subseteq \mathbb{F}^n \) be a finitely generated P-closed set with P-basis \( \mathcal{B} = \{b_1, b_2, \ldots, b_M\} \). There exists a solution to the linear system

\[
(F_m)_{m \in \mathcal{M}_M} V_{\mathcal{M}}^{\sigma, \delta} (\mathcal{B}) = (a_1, a_2, \ldots, a_M),
\]

for any \( a_1, a_2, \ldots, a_M \in \mathbb{F} \). For any solution, the corresponding skew polynomial \( F = \sum_{m \in \mathcal{M}_M} F_m m \) satisfies that \( F(b_i) = a_i \), for \( i = 1, 2, \ldots, M \), and \( \deg(F) < M \).

Another important immediate consequence is the following:

**Corollary 7.** Given a P-basis \( \mathcal{B} \), with \( M \) elements, of a P-closed set, one can obtain a dual P-basis of \( \mathcal{B} \), consisting of skew polynomials of degree less than \( M \), by solving \( M \) systems of \( M \) linear equations whose coefficients are taken from linearly independent rows in \( V_{\mathcal{M}}^{\sigma, \delta} (\mathcal{B}) \).

In conclusion, to find a P-basis of a P-closed set \( \Omega \subseteq \mathbb{F}^n \) with \( M = \text{Rk}(\Omega) \) and generated by a finite set \( \mathcal{G} \), we need to find \( M \) linearly independent columns in \( V_{\mathcal{M}}^{\sigma, \delta} (\mathcal{G}) \). Using Gaussian elimination, such method has exponential complexity in \( M \) if \( n > 1 \), since the number of rows in \( V_{\mathcal{M}}^{\sigma, \delta} (\mathcal{G}) \) is \( \# \mathcal{M}_M \), which is exponential in \( M \).

Fortunately, if we are given or have precomputed a P-basis of \( \Omega \), we may find Lagrange interpolating skew polynomials over \( \Omega \) with complexity \( O(M^3) \), and find a dual P-basis with complexity \( O(M^4) \).

### 11 Conclusion and open problems

In this paper, we have introduced free multivariate skew polynomial rings with coefficients over non-commutative rings. We have given a natural definition of evaluation (Definition 3), which extends the univariate case studied in [11, 12, 13]. Due to the product rule (Theorem 4), we assume eventually that coefficients lie on division rings or even fields. With these notions and assumptions, we were able to define general non-free multivariate skew polynomial rings (Definition 7), where evaluation is still natural. We
have described (by giving dimensions and bases) in Theorem 5 the vector spaces of func-
tions defined by multivariate skew polynomials, when defined over a finitely generated
P-closed set (set of zeros). This has been done thanks to a Lagrange-type interpolation
theorem (Theorem 4). The following problems are left open:

1. Find explicit descriptions of general multivariate skew polynomial rings. In other
words, find explicit descriptions of matrix morphisms, vector derivations and bi-
lateral ideals contained in $I(\mathbb{F}^n)$.

2. The previous item is particularly interesting in the case of finite fields, where the
minimal skew polynomial ring is generated by a finite collection of skew poly-
nomials. A complete explicit classification of all matrix morphisms and vector
derivations would also be of interest, as in the case $n = 1$.

3. Although we have given computational methods to find ranks, P-bases, dual P-
bases and Lagrange interpolating skew polynomials, it would be interesting to
obtain explicit formulas for such objects. Algorithms for finding P-bases with
polynomial complexity are also interesting, as well as reducing the complexity of
finding Lagrange interpolating skew polynomials.

4. Investigate how to perform Euclidean-type divisions over multivariate skew poly-
nomial rings, which would extend Lemma 4. A notion of Gröbner basis may be
possible and useful in this context.

Acknowledgement

The first author gratefully acknowledges the support from The Danish Council for In-
dependent Research (Grant No. DFF-4002-00367 and Grant No. DFF-5137-00076B,
“EliteForsk-Rejsestipendium”).

Appendices

A Why variables do not commute

In this appendix, we will show why we may not assume the commutativity of the variables
if our goal is to define a standard evaluation map as in Definition 3. As explained in
Section 3, it is usually considered standard to define the evaluation map on a point
$a = (a_1, a_2, \ldots, a_n) \in \mathbb{F}^n$ by defining a ring isomorphism

$$\mathbb{F}[x_1, x_2, \ldots, x_n]/(x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n) \rightarrow \mathbb{F}.$$ 

Now assume that $n > 1$ and we add to the ring $R$ in Section 2 the commutativity
property on the variables: $x_i x_j = x_j x_i$, for all $i, j = 1, 2, \ldots, n$. Observe that the rest
of the properties of $R$ still imply the existence of the matrix morphism $\sigma : \mathbb{F} \rightarrow \mathbb{F}^{n \times n}$
and the $\sigma$-vector derivation $\delta : \mathbb{F} \rightarrow \mathbb{F}^n$ by inspecting constants and variables.
Next take \( a_1, a_2, \ldots, a_n \in \mathbb{F} \). For fixed \( 1 \leq i < j \leq n \), we have that

\[
x_j(x_i - a_i) - x_i(x_j - a_j) = x_i a_j - x_j a_i = \sum_{k=1}^{n} (\sigma_{i,k}(a_j) - \sigma_{j,k}(a_i)) (x_k - a_k)
\]

\[
+ \left( \sum_{k=1}^{n} (\sigma_{i,k}(a_j) - \sigma_{j,k}(a_i)) a_k \right) + \delta_i(a_j) - \delta_j(a_i).
\]

(17)

Thus if the term (17) is not zero for all \( 0 \leq i < j \leq n \), then \( (x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n) = \mathcal{R} \). This means that the quotient ring is the zero ring and all polynomials would give the value 0 when evaluated on \((a_1, a_2, \ldots, a_n) \in \mathbb{F}^n\). Therefore it would be desirable that the term (17) equals 0 for all \((a_1, a_2, \ldots, a_n) \in \mathbb{F}^n\) and all \( 0 \leq i < j \leq n \).

In the following result, we show that this is the case only when \( \sigma \) is the identity matrix morphism and \( \delta \) is identically zero, in other words, only when \( \mathcal{R} \) is the conventional commutative polynomial ring over \( \mathbb{F} \) in the variables \( x_1, x_2, \ldots, x_n \).

**Proposition 7.** Given a matrix morphism \( \sigma : \mathbb{F} \rightarrow \mathbb{F}^{n \times n} \) and a \( \sigma \)-vector derivation \( \delta : \mathbb{F} \rightarrow \mathbb{F}^n \), it holds that the term (17) equals 0 for all \( a_1, a_2, \ldots, a_n \in \mathbb{F} \) and all \( 0 \leq i < j \leq n \) if, and only if, \( \sigma = \text{Id} \) and \( \delta = 0 \).

**Proof.** If \( \sigma = \text{Id} \) and \( \delta = 0 \), then it is easy to check that (17) always equals 0. Now assume that (17) always equals 0. Fix \( 1 \leq i < j \leq n \) and assume that \( a_k = 0 \) if \( k \neq i \) and \( k \neq j \). If \( a_j = 1 \), then it follows from (17) = 0 and the properties of \( \sigma \) and \( \delta \) that

\[
\delta_j(a_i) = (1 - \sigma_{j,i}(a_i)) a_i - \sigma_{j,j}(a_i),
\]

and similarly, choosing \( a_i = 1 \) instead, it holds that

\[
\delta_i(a_j) = (1 - \sigma_{i,j}(a_j)) a_j - \sigma_{i,i}(a_j).
\]

(18)

(19)

Substituting now the value of \( \delta_i(a_j) - \delta_j(a_i) \) obtained from these two equations in the equation (17) = 0, we obtain that

\[
a_i - a_j = (a_i - 1) \sigma_{i,i}(a_j) - (a_j - 1) \sigma_{j,j}(a_i).
\]

(20)

Taking separately \( a_j = 0 \) and \( a_i = 0 \) in (20), we obtain that \( \sigma_{j,j}(a_i) = a_i \) and \( \sigma_{i,i}(a_j) = a_j \), respectively.

Together with Equation (18), it implies that \( \delta_j(a_i) = -a_i \sigma_{j,i}(a_i) \). Using this and the facts that \( \sigma_{j,i}(a_i + 1) = \sigma_{j,i}(a_i) \) and \( \delta_j(a_i + 1) = \delta_j(a_i) \), we see that \( \sigma_{j,j}(a_i) = \delta_j(a_i) = 0 \), and similarly interchanging \( i \) and \( j \).

In conclusion, given \( a \in \mathbb{F} \) and \( 1 \leq i \leq n \), we have proven that \( \sigma_{i,i}(a) = a \) and \( \delta_i(a) = 0 \), and if \( i < j \leq n \), then \( \sigma_{i,j}(a) = \sigma_{j,i}(a) = 0 \), which means that \( \sigma = \text{Id} \) and \( \delta = 0 \), and we are done. \( \square \)
B Why iterated skew polynomial rings are not all included

In this appendix, we briefly show why not all iterated skew polynomial rings are skew polynomial rings in the sense of Definition 7.

If $S$ is an arbitrary ring, we may still define the univariate skew polynomial ring $R = S[x; \sigma, \delta]$, for a ring endomorphism $\sigma : S \rightarrow S$ and a $\sigma$-derivation $\delta : S \rightarrow S$.

If $S = F[x_1; \sigma_1, \delta_1]$ is in turn a skew polynomial ring over a field $F$, then we may define the iterated bivariate skew polynomial ring

$$ R = S[x_2; \sigma_2, \delta_2] = (F[x_1; \sigma_1, \delta_1])[x_2; \sigma_2, \delta_2]. $$

Choose arbitrary field automorphisms $\sigma_1, \sigma_2 : F \rightarrow F$ such that $\sigma_1 \sigma_2 = \sigma_2 \sigma_1$. Now extend $\sigma_2$ to $S = F[x_1; \sigma_1, 0]$ by

$$ \sigma_2 \left( \sum_{i \geq 0} F_i x_1^i \right) = \sum_{i \geq 0} \sigma_2(F_i) x_1^i, $$

where $F_i \in F$, for $i = 0, 1, 2, \ldots$. It holds that $\sigma_2 : F[x_1; \sigma_1, 0] \rightarrow F[x_1; \sigma_1, 0]$ is a ring automorphism (use that $\sigma_1 \sigma_2 = \sigma_2 \sigma_1$). Therefore, the ring

$$ R = (F[x_1; \sigma_1, 0])[x_2; \sigma_2, 0] $$

is a “non-commutative polynomial ring” as in the previous appendix, that is, where addition is as usual, multiplication is additive on degrees and the variables commute:

$$ x_2 x_1 = \sigma_2(x_1) x_2 + \delta_2(x_1) = (1 x_1) x_2 + 0 = x_1 x_2. $$

Therefore, by Proposition 7 there exist $a_1, a_2 \in F$ such that $(x_1 - a_1, x_2 - a_2) = R$ unless $\sigma_1 = \sigma_2 = \text{Id}$.

C Proof of Theorem 1

In this appendix, we will repeatedly use the compact notation in Equation (4).

First, the product is well-defined, since $\deg(F) = d$ and $\deg(G) = e$ imply that the coefficient of $m$ in $FG$ is zero whenever $\deg(m) > d + e$, for all $F, G \in R$ and all $m \in M$.

Once we prove that $R$ is a ring, it follows that it is an algebra over $F$ via $a \mapsto a1$ by definition.

Fixing $F \in R$, it also follows by definition that $1F = F$. Now, iteratively on $m \in M$, it follows by definition that $m1 = m$ since $\sigma(1) = I$ and $\delta(1) = 0$. Thus we conclude that $F1 = F$, and 1 is the multiplicative identity.

Next fix $F, G, H \in R$. The distributive law $(F + G)H = FH + GH$ is trivial by definition. To prove the distributive law $F(G + H) = FG + FH$, we only need to show recursively on $m \in M$ that $m((a + b)n) = m(an) + m(bn)$, for all $a, b \in F$ and all $n \in M$, which follows from the additive properties of $\sigma$ and $\delta$.  

25
The difficult part to prove is the associative law. By repeated use of the distributive laws, we just need to prove that

\[ m((an)(bp)) = (m(an))(bp), \]  

(21)

for fixed \( a, b \in F \) and \( m, n, p \in M \). We first show that

\[ (mn)(bp) = m(n(bp)). \]  

(22)

The cases \( n = 1 \) and \( n = x_i \), for \( i = 1, 2, \ldots, n \), follow from the definitions. Hence recursively on \( n \), it follows that

\[ (m(nx))(bp) = ((mn)x)(bp) = (mn)(x(bp)) = m(n(x(bp))) = m((nx)(bp)), \]

where in * we may expand \( x(bp) \) and use the distributive laws.

Next we prove simultaneously and recursively on \( n \) that

\[ n(ab) = (na)b, \text{ and} \]

(23)

\[ (na)p = n(ap). \]  

(24)

First, we leave for the reader to show (using the distributive laws) that, if [23] and [24] hold for all monomials \( n \) of degree at most \( d \), then the following also holds for such monomials:

\[ (na)F = n(aF), \]

(25)

for any \( F \in \mathcal{R} \).

Now, [23] and [24] follow easily from the definitions for \( n = 1 \) and \( n = x_i \), for \( i = 1, 2, \ldots, n \). We leave for the reader to prove [24] recursively on \( n \). We now do that for [23]:

\[ ((nx)a)b = (n(\sigma(a)x))b + (n\delta(a))b = ((n\sigma(a))x)b + (n\delta(a))b \]

(22)

\[ (n\sigma(a))(xb) + (n\delta(a))b = (n\sigma(a))(\sigma(b)x + \delta(b)) + (n\delta(a))b \]

(22)

\[ n(\sigma(ab)x) + (n\sigma(a))\delta(b) + (n\delta(a))b = n(\sigma(ab)x + \delta(ab)) = (nx)(ab). \]

To conclude, [21] follows from the following chain of equalities:

\[ m((an)(bp)) = m(a(n(bp))) \quad \text{[20]} \quad (ma)(n(bp)) \quad \text{[22]} \quad ((ma)n)(bp) \quad \text{[24]} \quad (m(an))(bp). \]

References

[1] D. Boucher, W. Geiselmann, and F. Ulmer. Skew-cyclic codes. *Applicable Algebra in Engineering, Communication and Computing*, 18(4):379–389, 2007.

[2] D. Boucher and F. Ulmer. Coding with skew polynomial rings. *Journal of Symbolic Computation*, 44(12):1644–1656, 2009. Gröbner Bases in Cryptography, Coding Theory, and Algebraic Combinatorics.
[3] D. Boucher and F. Ulmer. Linear codes using skew polynomials with automorphisms and derivations. *Designs, Codes and Cryptography*, 70(3):405–431, 2014.

[4] L. Chaussade, P. Loidreau, and F. Ulmer. Skew codes of prescribed distance or rank. *Designs, Codes and Cryptography*, 50(3):267–284, 2009.

[5] P. M. Cohn. *Free rings and their relations*. London: Academic Press, 1971.

[6] A. Lj. Erič. Polynomial interpolation problem for skew polynomials. *Applicable Analysis and Discrete Mathematics*, 1(2):403–414, 2007.

[7] E. M. Gabidulin. Theory of codes with maximum rank distance. *Problems Information Transmission*, 21, 1985.

[8] E. M. Gabidulin. Rank q-cyclic and pseudo-q-cyclic codes. In *Proc. 2009 IEEE International Symposium on Information Theory (ISIT 2009)*, pages 2799–2802, 2009.

[9] W. C. Huffman and V. Pless. *Fundamentals of error-correcting codes*. Cambridge University Press, Cambridge, 2003.

[10] A. Kshevetskiy and E. M. Gabidulin. The new construction of rank codes. In *Proc. 2005 IEEE International Symposium on Information Theory (ISIT 2005)*, pages 2105–2108, Sept 2005.

[11] T. Y. Lam. A general theory of Vandermonde matrices. *Expositiones Mathematicae*, 4:193–215, 1986.

[12] T. Y. Lam and A. Leroy. Algebraic conjugacy classes and skew polynomial rings. In *Perspectives in Ring Theory*, pages 153–203. Springer, 1988.

[13] T. Y. Lam and A. Leroy. Vandermonde and Wronskian matrices over division rings. *Journal of Algebra*, 119(2):308–336, 1988.

[14] R. Lidl and H. Niederreiter. *Finite Fields*, volume 20. Encyclopedia of Mathematics and its Applications. Addison-Wesley, Amsterdam, 1983.

[15] S. Liu, F. Manganiello, and F. R. Kschischang. Kötter interpolation in skew polynomial rings. *Designs, Codes and Cryptography*, 72(3):593–608, September 2014.

[16] S. Liu, F. Manganiello, and F. R. Kschischang. Construction and decoding of generalized skew-evaluation codes. In *Proc. 2015 IEEE 14th Canadian Workshop on Information Theory (CWIT)*, pages 9–13, July 2015.

[17] O. Ore. On a special class of polynomials. *Transactions American Mathematical Society*, 35(3):559–584, 1933.

[18] O. Ore. Theory of non-commutative polynomials. *Annals of Mathematics (2)*, 34(3):480–508, 1933.
[19] R. M. Roth. Maximum-rank array codes and their application to crisscross error correction. *IEEE Transactions on Information Theory*, 37(2):328–336, March 1991.

[20] M. Sudan. Decoding of Reed-Solomon codes beyond the error-correction bound. *Journal of Complexity*, 13(1):180–193, 1997.

[21] Y. Zhang. A secret sharing scheme via skew polynomials. In *2010 International Conference on Computational Science and Its Applications*, pages 33–38, March 2010.