Computing Valuations of the Dieudonné Determinants[*]

Taihei Oki[†]

February 17, 2021

Abstract

This paper addresses the problem of computing valuations of the Dieudonné determinants of matrices over discrete valuation skew fields (DVSFs). Under a reasonable computational model, we propose two algorithms for a class of DVSFs, called split. Our algorithms are extensions of the combinatorial relaxation of Murota (1995) and the matrix expansion by Moriyama–Murota (2013), both of which are based on combinatorial optimization. While our algorithms require an upper bound on the output, we give an estimation of the bound for skew polynomial matrices and show that the estimation is valid only for skew polynomial matrices.

We consider two applications of this problem. The first one is the noncommutative weighted Edmonds' problem (nc-WEP), which is to compute the degree of the Dieudonné determinants of matrices having noncommutative symbols. We show that the presented algorithms reduce the nc-WEP to the unweighted problem in polynomial time. In particular, we show that the nc-WEP over the rational field is solvable in time polynomial in the input bit-length. We also present an application to analyses of degrees of freedom of linear time-varying systems by establishing formulas on the solution spaces of linear differential/difference equations.

Keywords: valuation skew fields, Dieudonné determinants, skew polynomials, differential equations, difference equations, combinatorial relaxation, matrix expansion

---

[†]Department of Mathematical Informatics, Graduate School of Information Science and Technology, University of Tokyo, Tokyo 113-8656, Japan. E-mail: `taihei_oki@mist.i.u-tokyo.ac.jp`

Contents

1 Introduction

A (*real*) *valuation* on a field F is a map $v : F \to \mathbb{R} \cup \{+\infty\}$ such that

(V1) $v(ab) = v(a) + v(b)$ for $a, b \in F$,

(V2) $v(a + b) \geq \min\{v(a), v(b)\}$ for $a, b \in F$,

(V3) $v(1) = 0$,

(V4) $v(0) = +\infty$.

A valuation is called *discrete* if $v(F) = \mathbb{Z} \cup \{+\infty\}$. For example, the minus of the degree is a discrete valuation on the rational function field $K(s)$ over a field K, where $\deg p/q :=\deg p - \deg q$ for $p, q \in K[s]$. The p-adic valuation on rationals $\mathbb{Q}$ is another example. A field equipped with a discrete valuation is called a *discrete valuation field* (DVF).

Valuations of determinants of matrices over a DVF often appear as matrix formulations of combinatorial optimization problems. For example, *weighted Edmonds' problem* (WEP), which is to compute the degree of the determinant of a polynomial matrix having symbols, reduces to the weighted bipartite matching problem and the weighted linear matroid intersection and parity problems depending on symbols' pattern [27]. Conversely, the degree of the determinant of an arbitrary polynomial matrix serves as a lower bound on the maximum weight of a perfect matching in the associated edge-weighted bipartite graph. Based on this relation, the *combinatorial relaxation* algorithm of Murota [42] computes the degree of the determinant of a polynomial matrix by iteratively solving the weighted bipartite matching problem.

Computing valuations of determinants is also applied to linear differential equations. Consider a linear differential equation

$$A_0 y + A_1 y' + \cdots + A_\ell y^{(\ell)} = 0 \tag{1}$$

for $y : \mathbb{R} \to \mathbb{C}^n$, where $A_0, \ldots, A_\ell \in \mathbb{C}^{n \times n}$. The set of all solutions of (1) forms a vector space over $\mathbb{C}$. Classical Chrystal's theorem [8] states that the dimension of the solution space of (1) is equal to the degree of the determinant of $A_0 + A_1 s + \cdots + A_\ell s^\ell \in \mathbb{C}[s]^{n \times n} \hookrightarrow \mathbb{C}(s)^{n \times n}$. Hence one can analyze the degrees of freedom of linear time-invariant systems by computing valuations of determinants of matrices over a DVF.

This paper addresses a noncommutative generalization of computing valuations of determinants. A *discrete valuations skew field* (DVSF) is naturally defined as in the commutative case [62]. The *Dieudonné determinant* [14], denoted by Det, is a generalization of the determinant for matrices over skew fields (see Section 3.1 for definition). The Dieudonné determinant retains useful properties of the usual determinant such as $\mathrm{Det}\, AB = \mathrm{Det}\, A\, \mathrm{Det}\, B$. While $\mathrm{Det}\, A$ for $A \in F^{n \times n}$ is no longer an element in a skew field F, when F is a DVSF, its valuation $\zeta(A) := v(\mathrm{Det}\, A)$ is well-defined.

In the following of this introduction, we first describe applications of valuations of the Dieudonné determinants in Sections 1.1 and 1.2. Then Section 1.3 states a computational model which we use and Section 1.4 presents our contributions. Related work and organization of this paper are described in Section 1.5 and Section 1.6, respectively.

1.1 Weighted Edmonds' Problem

In 1967, Edmonds [18] posed a question whether there exists a polynomial-time algorithm to compute the rank of a *linear (symbolic) matrix* B over a field K, which is in the form

$$B = B_0 + B_1 x_1 + \cdots + B_m x_m,$$

where $B_0, B_1 \ldots, B_m \in K^{n \times n}$ and $x_1, \ldots, x_m$ are commutative symbols. Here, B is regarded as a matrix over the polynomial ring $K[x_1, \ldots, x_m]$ or the rational function field $K(x_1, \ldots, x_m)$. In case where B is the Edmonds or Tutte matrix of a bipartite or nonbipartite graph G, the rank computation for B corresponds to solving the maximum matching problem on G. More generally, Lovász [40] showed that Edmonds' problem is equivalent to a linear matroid intersection problem if all B_i are of rank 1, and to a linear matroid parity problem if all B_i are skew-symmetric matrices of rank 2. For general linear matrices, the celebrated Schwartz–Zippel lemma [52] provides a simple randomized algorithm if $|K|$ is large enough [40]. However, no deterministic polynomial-time algorithm still has been known; the existence of such an algorithm would imply nontrivial circuit complexity lower bounds [33, 56].

Recent studies [21, 25, 30] address the noncommutative version of Edmonds' problem (nc-Edmonds' problem). This is a problem of computing the *noncommutative rank* (nc-rank) of B, which is the rank defined by regarding $x_1, \ldots, x_m$ as pairwise noncommutative, i.e., $x_i x_j \neq x_j x_i$ if $i \neq j$. In this way, B is viewed as a matrix over the free ring $K\langle x_1, \ldots, x_m \rangle$ generated by noncommutative symbols $x_1, \ldots, x_m$. The nc-rank of B is precisely the rank of B over a skew (noncommutative) field $K \langle\!\langle x_1, \ldots, x_m \rangle\!\rangle$, called a *free skew field*, which is the quotient of $K\langle x_1, \ldots, x_m \rangle$ defined by Amitsur [2]. We call a linear matrix over K having noncommutative symbols an *nc-linear matrix* over K. The recent studies [21, 25, 30] revealed that nc-Edmonds' problem is deterministically tractable. For the case where K is the set $\mathbb{Q}$ of rational numbers, Garg et al. [21] proved that Gurvits' *operator scaling algorithm* [24] deterministically computes the nc-rank of B in $\mathrm{poly}(n, m)$ arithmetic operations on $\mathbb{Q}$. Algorithms over general field K were later given by Ivanyos et al. [30] and Hamada–Hirai [25] exploiting the min-max theorem established for nc-rank. When $K = \mathbb{Q}$, these algorithms run in time polynomial in the bit-length of the input.

Hirai [27] introduced a weighted version of Edmonds' problem. First, consider commutative symbols $x_1, \ldots, x_m$ and an extra commutative symbol s. Define a matrix

$$A = A_\ell + A_{\ell-1} s + \cdots + A_0 s^\ell, \tag{2}$$

where $A_d = A_{d,0} + A_{d,1} x_1 + \cdots + A_{d,m} x_m \in K[x_1, \ldots, x_m]^{n \times n}$ is a linear matrix over K for $d = 0, \ldots, \ell$. We call (2) a *linear polynomial matrix* over K. The *weighted Edmonds' problem* (WEP) is the problem to compute the degree (in s) of the determinant of A. Analogously to Edmonds' problem, WEP includes a bunch of weighted combinatorial optimization problems as special cases, such as a maximum weighted perfect matching problem, a weighted linear matroid intersection problem and a weighted linear matroid parity problem; see [27, Section 5].

Next, let $x_1, \ldots, x_m$ be noncommutative symbols and s an extra symbol that commutes with any element in $K\langle x_1, \ldots, x_m \rangle$. An *nc-linear polynomial matrix* A over K is a matrix in the form of (2) with each A_d regarded as an nc-linear matrix. Then A can be viewed as a matrix over the rational function (skew) field $F := K\langle\!\langle x_1, \ldots, x_m \rangle\!\rangle(s)$. Now F is a DVSF equipped with discrete valuation $- \deg$. *Noncommutative weighted Edmonds' problem* (nc-WEP) is the problem to compute $\deg \mathrm{Det}$ of a given nc-linear polynomial matrix. Hirai [27] formulated the dual problem of nc-WEP as the minimization of an *L-convex function* on a *uniform modular lattice*, and gave an algorithm based on the steepest gradient descent. Hirai's algorithm uses $\mathrm{poly}(n, m, \ell)$ arithmetic operations on K while no bit-length bound has been given for $K = \mathbb{Q}$.

1.2 Linear Differential/Difference Equations

Polynomials in differential or difference operators give rise to noncommutative valuations. Let K be a skew field, $\sigma : K \to K$ a ring automorphism, and $\delta : K \to K$ a (*left*) σ-*derivation*; that is, it is additive, i.e., $\delta(a + b) = \delta(a) + \delta(b)$, and $\delta(ab) = \sigma(a)\delta(b) + \delta(a)b$ for $a, b \in K$. A *skew polynomial*, or an *Ore polynomial* due to Ore [47], over (K, σ, δ) in indeterminate s is a polynomial over K with the usual addition and a twisted multiplication defined by the

commutation rule

$$sa = \sigma(a)s + \delta(a) \tag{3}$$

for $a \in K$. The *skew polynomial ring* over (K, σ, δ) is denoted by $K[s; \sigma, \delta]$. Besides the polynomial ring $K[s]$, the ring $\mathbb{C}(t)[\partial; \text{id},']$ of differential operators is an example of a skew polynomial ring, where $' : \mathbb{C}(t) \to \mathbb{C}(t)$ is the usual differentiation. Another example is the ring $\mathbb{C}(t)[S; \tau, 0]$ of shift operators, where $\tau : \mathbb{C}(t) \to \mathbb{C}(t)$ is defined by $f(t) \mapsto f(t+1)$ for $f \in \mathbb{C}(t)$. The degree of a skew polynomial is naturally defined and it extends to the *skew rational function field* $K(s; \sigma, \delta)$, which is the *Ore quotient skew field* of $K[s; \sigma, \delta]$. Then $K(s; \sigma, \delta)$ is a DVSF with valuation $-\deg$.

Let K be a field of characteristic 0 equipped with an (id-)derivation δ. Consider a linear differential equation

$$A_0 y + A_1 \delta(y) + \cdots + A_\ell \delta^\ell(y) = 0 \tag{4}$$

for $y \in K^n$ with $A_0, \ldots, A_\ell \in K^{n \times n}$. Taelman [55] showed that the dimension of the solution space (over an adequate field extension of K) of (4) is equal to $\deg \operatorname{Det} A$ with $A := A_0 + A_1 s + \cdots + A_\ell s^\ell \in K[s; \text{id}, \delta]^{n \times n}$. This is a "time-varying" generalization of Chrystal's theorem. We show that the assumption on the characteristic can be removed and a similar formula holds for linear difference equations using two kinds of valuations (see Section 9). In this way, computing valuations of the Dieudonné determinants of matrices over DVSFs can be applied to analysis of time-varying linear differential or difference equations.

1.3 Computational Model

We design algorithms to compute $\zeta(A)$ for a matrix A over a DVSF F without restricting F to a skew rational function field so that the algorithms can be applied as widely as possible. Here we need to clarify a computational model to deal with representation of elements in F and operations on F. The simplest model is the arithmetic model on F, i.e., an element in F is stored in a unit memory cell and we can perform arithmetic operations on F in constant time. In this model, one can compute $\zeta(A)$ in $O(n^\omega)$-time by the Gaussian elimination, where ω is the exponent in the time complexity of multiplying two matrices. However, this model is too simplified and cannot catch the computational cost needed in the standard representation of some DVSF like $F = K(s)$.

As a representation of elements in F, we adopt the π-*adic expansion*, in which each $a \in F$ is expressed as a formal Laurent series

$$a = \sum_{d=\ell}^{\infty} a_d \pi^d.$$

Here, $\ell \in \mathbb{Z}$, $\pi \in F$ is a fixed element with $v(\pi) = 1$ called a *uniformizer*, and $a_\ell, a_{\ell+1}, \ldots$ are elements in a fixed subset $Q \subseteq F$, called a *representative set*. The representative set is selected so that the π-adic expansion is unique; such Q exists for any DVSF. While we would like to adopt the "arithmetic model on Q", the set Q might not be a skew field, i.e., arithmetic operations on Q might not be closed. We thus require F to have a representative set that is a skew subfield of F. Such a DVSF is called *split* [17].

Let F be a split DVSF with a closed representative set K, called the *coefficient skew subfield*. The ring structure of F is completely determined from the commutation rule between a uniformizer $\pi \in F$ and each $a \in K$. The element πa is uniquely expressed as

$$\pi a = \sum_{d=0}^{\infty} \delta_d(a) \pi^{d+1}, \tag{5}$$

where $\delta_d : K \to K$ is a map satisfying the axioms of *higher σ-derivations* [50]. We also assume the oracle access to each δ_d, i.e., we can compute $\delta_d(a)$ in constant time for each $d \in \mathbb{N}$ and $a \in K$.

1.4 Contributions

Under the above setting, this paper presents two algorithms to compute $\zeta(A)$ for $A \in F^{n \times n}$, both of which are based on combinatorial optimization. The first algorithm is a generalization of the *combinatorial relaxation* of Murota [42] that computes $\deg \det$ of polynomial matrices over a field. Constructing an edge-weighted bipartite graph $G(A)$ from A reflecting the valuation of each entry, one can show that $\zeta(A)$ is lower bounded by the minimum weight of a perfect matching of $G(A)$. Based on this relation, the combinatorial relaxation algorithm computes $\zeta(A)$ by iteratively solving the weighted matching problem.

The second algorithm generalizes the *matrix expansion*, which reduces the computation of $\zeta(A)$ to the rank computation of a block matrix over K obtained by arranging coefficient matrices of $\pi^i A$ with $i \in \mathbb{N}$. The correctness of the matrix expansion essentially relies on the *Legendre conjugacy* between integer sequences of the valuations of minors of A and ranks of block matrices. The Legendre conjugacy is an important duality relation on discrete convex and concave functions treated in *discrete convex analysis* [44]. Our matrix expansion generalizes algorithms of Van Dooren et al. [59] for $\deg \det$ on $\mathbb{C}(s)$ and Moriyama–Murota [41] for $\deg \det$ on $K(s)$ with a field K.

The running times of our algorithms are estimated as follows.

Theorem 1.1. *Let F be a split DVSF with uniformizer π and coefficient skew subfield K. Let $A = \sum_{d=0}^{\ell} A_d \pi^d \in F^{n \times n}$ be a square matrix over F with $A_0, \dots, A_\ell \in K^{n \times n}$. Given $A_0, \dots, A_\ell$ and $M \in \mathbb{N}$ such that $\zeta(A) \le M$ or A is singular, we can compute $\zeta(A)$ by the combinatorial relaxation algorithm in $\mathrm{O}(M^3 n^2 + M^2 n^\omega + M n^{2.5})$-time and by the matrix expansion algorithm in $\mathrm{O}(M^3 n^2 + M^\omega n^\omega)$-time.*

As shown in Theorem 1.1, our algorithms additionally require an upper bound M on $\zeta(A)$ by technical reasons. While estimating such M seems to be difficult for general DVSFs, one can adopt $M := \ell n$ for $A = \sum_{d=0}^{\ell} A_\ell s^d \in K[s]^{n \times n}$ with K being a field. This indeed holds for skew polynomial rings and it yields the following corollary:

Theorem 1.2. *Let $A = \sum_{d=0}^{\ell} A_\ell s^d \in K[s; \sigma, \delta]^{n \times n}$ be a square skew polynomial matrix over a skew field K. Under the arithmetic model on K and oracle access to σ^{-1} and δ, we can compute $\deg \mathrm{Det}\, A$ in $\mathrm{O}(\ell^2 n^{\omega+2} + \ell n^{4.5})$-time by the combinatorial relaxation algorithm and in $\mathrm{O}(\ell^\omega n^{2\omega})$-time by the matrix expansion algorithm.*

We further show that the converse holds, i.e., $\zeta(A) \le \ell n$ for any nonsingular $A \in F^{n \times n}$ only if F is isomorphic to (an extension of) a skew rational function field. This fact indicates that skew polynomial rings are characterized as the most general ring structure that admits natural extensions of the combinatorial relaxation and matrix expansion algorithms.

We cannot directly apply Theorem 1.1 to weighted Edmonds' problem because arithmetic operations on $K(x_1, \dots, x_m)$ nor $K \langle\!\langle x_1, \dots, x_m \rangle\!\rangle$ cannot be performed in constant time under the arithmetic model on K. However, using the min-max formula on nc-Edmonds' problem by Fortin–Reutenauer [20], we can modify the combinatorial relaxation algorithm so that it can be used for reducing the nc-WEP to the unweighted problem. This algorithm coincides with that given by Hirai [27]. Furthermore, the matrix expansion algorithm can be used for reductions of both commutative and noncommutative problems. Using polynomial-time algorithms for nc-Edmonds' problem, we show:

Theorem 1.3. *The nc-WEP over a field K can be deterministically solved using polynomially many arithmetic operations on K. When $K = \mathbb{Q}$, the algorithm runs in time polynomial in the binary encoding length of the input.*

1.5 Related Work

In computer algebra, algorithms were proposed for computing various kinds of canonical forms of a skew polynomial matrix $A \in K[s; \sigma, \delta]^{n \times n}$ such as the *Jacobson normal form* [39], the *Hermite normal form* [22], the *Popov normal form* [34] and their weaker form called a *row-reduced form* [1, 3]. One can use these algorithms to calculate $\deg \operatorname{Det} A$ since it is immediately obtained from the canonical forms of A. These algorithms iteratively solve systems of linear equations over K. Our algorithms are faster than the existing algorithms. The fastest known algorithm given by Giesbrecht–Kim [22] runs in $\mathrm{O}(\ell^\omega n^{2\omega+2} \log \ell n)$-time, whereas our two algorithms require only $\mathrm{O}(\ell^2 n^{\omega+2} + \ell n^{4.5})$-time and $\mathrm{O}(\ell^\omega n^{2\omega})$-time as seen in Theorem 1.2.

Hamada–Hirai [25] presents an algorithm for nc-Edmonds' problem over $\mathbb{Q}$ that runs in time polynomial in the bit-length of the input. They introduce a quantity conceptually corresponding to p-adic valuations of the Dieudonné determinants for matrices over $F := \mathbb{Q}\langle\!\langle x_1, \ldots, x_m \rangle\!\rangle$ and the algorithm computes it based on the procedure of the combinatorial relaxation. Since $\mathbb{Q}$ with the p-adic valuation is not split, their algorithm can be seen as a kind of an extension of the combinatorial relaxation to a special but non-split DVSF, except that the quantity has not been proved to be some discrete valuation of the Dieudonné determinants on F indeed.

1.6 Organization

The rest of this paper is organized as follows. Sections 2 and 3 describe preliminaries on valuation skew fields and matrices over them, respectively. Section 4 explains that relations between matrices over valuation fields and combinatorial optimization problems, which are well-known for the commutative case, still hold in the noncommutative case. Sections 5 and 6 propose our algorithms, the combinatorial relaxation and matrix expansion algorithms, respectively. Section 7 discusses an estimation of the upper bound M on $\zeta(A)$. Finally, Sections 8 and 9 describe applications to weighted Edmonds' problem and linear differential/difference equations, respectively.

2 Preliminaries on Valuation Skew Fields

We denote the set of nonnegative integers by $\mathbb{N}$, the integers by $\mathbb{Z}$, the rational numbers by $\mathbb{Q}$, the real numbers by $\mathbb{R}$, and the complex numbers by $\mathbb{C}$. For $n \in \mathbb{N}$, define $[n] := \{1, 2, \ldots, n\}$ and $[0, n] := \{0, 1, 2, \ldots, n\}$. All rings are assumed to have the multiplicative identity.

2.1 Valuation Skew Fields

A *skew field*, or a *division ring* is a ring F such that every nonzero element has a multiplicative inverse in F. A (*real*) *valuation skew field* [62, Chapter IV] is a skew field F endowed with a (*real*) *valuation*, that is, a map $v : F \to \mathbb{R} \cup \{+\infty\}$ satisfying (V1)–(V4). A valuation skew field is called a *valuation field* if it is a field. The value $v(a)$ for $a \in F$ is called the *valuation* of a.

By (V1) and (V3), it holds $v(-a) = v(a)$ and $v(a^{-1}) = -v(a)$ for all $a \in F^\times$, where $F^\times = F \setminus \{0\}$ is the multiplicative group of F. In particular, we have $v(a) < +\infty$ for $a \in F^\times$. The equality in (V2) is attained whenever $v(a) \neq v(b)$; otherwise, if $v(a) < v(a + b)$ and $v(a) < v(b)$, it holds

$$v(a) = v((a + b) - b) \geq \min\{v(a + b), v(-b)\} = \min\{v(a + b), v(b)\} > v(a),$$

a contradiction.

The (*invariant*) *valuation ring* of a valuation skew field F with respect to a valuation v is a set

$$R := \{a \in F \mid v(a) \geq 0\}.$$

Then R is a subring of F by (V1) and (V2), and is a *domain*, i.e., R has no zero-divisors. It also satisfies the following [36, Chapter 1]:

(VR1) either $a \in R$ or $a^{-1} \in R$ for $a \in F^{\times}$,

(VR2) $aR = Ra$ for $a \in F^{\times}$.

In addition, R is a *local ring*, i.e., it has a unique maximal right (and indeed a unique maximal left) ideal $J(R)$, which coincides with $R \setminus R^{\times}$ with $R^{\times} = \{a \in F \mid v(a) = 0\}$. Namely, it holds

$$J(R) = \{a \in F \mid v(a) > 0\}. \tag{6}$$

The quotient ring $R \,/\, J(R)$ forms a skew field, called the *residue skew field* of F (or a *residue field* if it is a field).

A *representative set* of F is a subset Q of R such that $0 \in Q$ and the restriction to Q of the canonical homomorphism from R to the residue skew field $K := R \,/\, J(R)$ is a bijection from Q to K. Then for $a \in R$, there uniquely exists $a_0 \in Q$ such that $a \in a_0 + J(R)$. Hence $a - a_0 \in J(R)$, which means:

Proposition 2.1. *Let F be a valuation skew field with valuation v, valuation ring R, and representative set Q. Then any $a \in R$ is uniquely expressed as $a = a_0 + \tilde{a}$, where $a_0 \in Q$ and $\tilde{a} \in J(R)$.*

The *value group* of v is the additive subgroup $v(F^{\times})$ of $\mathbb{R}$. A *discrete valuation* is a valuation F whose value group is $\mathbb{Z}$. A valuation skew field equipped with a discrete valuation is called a *discrete valuation skew field* (DVSF), which is of the main interest of this thesis. If F is a field, we call F a *discrete valuation field* (DVF).

Let F be a DVSF with discrete valuation v and the valuation ring R. Then (6) is

$$J(R) = \{a \in F \mid v(a) \geq 1\}. \tag{7}$$

Any element $\pi \in R$ with $v(\pi) = 1$ is called a *uniformizer* or a *prime element* of F. In addition to (VR1) and (VR2), R enjoys the following properties [36, Chapter 1]:

(DVR1) $J(R) = \pi R = R\pi$,

(DVR2) $\bigcap\limits_{d=1}^{\infty} J(R)^d = \{0\}$.

Note that it holds

$$J(R)^d = \pi^d R = R\pi^d = \{a \in F \mid v(a) \geq d\} \tag{8}$$

by (7) and (DVR1) for $d \in \mathbb{N}$. In addition, any right ideal and left ideal of R are two-sided and are in the form of (8). This mean that R is a (right and left) *principal ideal domain* (PID), which is a domain whose every (right and left) ideal is generated by one element. More strongly, any DVR is a (right and left) *Euclidean domain* [6] as is well-known for commutative DVRs. Here, a domain R is said to be *Euclidean* if there exists a map $f : R \to \mathbb{N} \cup \{-\infty\}$, called an *Euclidean map*, such that for every $a, b \in R$ with $b \neq 0$, there exist $q, r, q', r' \in R$ such that $a = bq + r = q'b + r'$ and $f(r), f(r') < f(b)$. In case of a valuation ring of a DVSF, $-v$ serves as an Euclidean map. We remark that Euclidean domains are proper subclass of PIDs even for noncommutative rings [6].

Remark 2.2. In general, a local ring R satisfying (DVR1) and (DVR2) for some non-nilpotent element $\pi \in R$ is called a *discrete (invariant) valuation ring* (DVR). Here, an element $a \in R$ is said to be *nilpotent* if $a^k = 0$ for some $k \in \mathbb{N}$ and *non-nilpotent* if not. The valuation ring of any DVSF is a DVR as described above. Indeed, any DVR R is the valuation ring of some

DVSF [36]; here we give a construction of the DVSF briefly. First, it follows from (DVR1) and (DVR2) that R is a PID. Then R is also a (right and left) *Ore domain*, which is a domain such that for each $s, t \in R \setminus \{0\}$, there exist $x, y, z, w \in R \setminus \{0\}$ satisfying $sx = ty$ and $zs = wt$ [23, Corollary 6.7]. This property enables for R to have the *Ore quotient skew field F*, which is a skew field of fractions each of whose elements $a \in F$ is expressed as $a = sx^{-1} = y^{-1}t$ for some $s, t \in R$ and $x, y \in R \setminus \{0\}$. In particular, $a \in F^{\times}$ can be uniquely expressed as $a = \pi^k p = q\pi^k$ for some $p, q \in R^{\times}$ and $k \in \mathbb{Z}$. Denote this k by $v(a)$ for $a \in F^{\times}$ and let $v(0) := +\infty$. Then $v : F \to \mathbb{Z} \cup \{+\infty\}$ is a discrete valuation on F, whose valuation ring coincides with R. We refer to the restriction of v onto R as the valuation of R and a representative set of R means that of F. See [36, Chapter 1] for details of DVRs and [23, Chapter 6] for Ore domains and quotient skew fields.

Let F be a DVSF with valuation v and uniformizer π. For an arbitrary real number $c > 1$, we define $d : F \times F \to \mathbb{R}$ as

$$d(a, b) := c^{-v(a-b)}$$

for $a, b \in F$ (where $c^{-\infty} := 0$). Then d forms a metric on F. The *π-adic topology* is the ring topology on F induced by d, which does not depend on the choice of c. On this topology, $\{a + J(R)^k \mid k \in \mathbb{N}\}$ is an open neighborhood system of $a \in F$ by (8). A DVSF is said to be *complete* if it is complete as a metric space. Then any DVSF can be extended to a complete DVSF as follows.

Theorem 2.3 ([62, Theorem 17.2]). *Let F be a DVSF with discrete valuation v. Then there uniquely exists a complete DVSF $\hat{F}$ with discrete valuation $\hat{v}$ such that $\hat{F}$ contains F as a dense subring and $\hat{v}$ extends v. In addition, the residue skew field of $\hat{F}$ is isomorphic to that of F.*

The complete DVSF $\hat{F}$ in Theorem 2.3 is called the *completion* of F. By Theorem 2.3, it is convenient to consider complete DVSFs from the beginning. See [62] for details of topological rings and the π-adic topology.

Let F be a DVSF with uniformizer π, valuation ring R, and representative set Q. By Proposition 2.1 and (DVR1), we can express $a \in R$ as $a = a_0 + a'\pi$ by some $a_0 \in Q$ and $a' \in R$. By the same argument, there are unique $a_1 \in Q$ and $a'' \in R$ such that $a' = a_1 + a''\pi$. Therefore, we have $a = a_0 + a_1\pi + a''\pi^2$. Repeating this argument, we can represent a as a power series in π with coefficient Q, which is formally stated as follows.

Proposition 2.4 ([62, Theorem 18.5]). *Let F be a DVSF with discrete valuation v and let π and Q be a uniformizer and a representative set of F, respectively.*

(1) *For every $a \in F$, there uniquely exists a sequence $(a_d)_{d \in \mathbb{Z}}$ of elements in Q such that $a_d = 0$ for all but finitely many $d < 0$ and a power series*

$$\sum_{d \in \mathbb{Z}} a_d \pi^d \tag{9}$$

converges to a in the π-adic topology. If $\ell := v(a) \in \mathbb{Z}$, then $a_d = 0$ for $d < \ell$ and $a_{\ell} \neq 0$.

(2) *If F is complete and $(a_d)_{d \in \mathbb{Z}}$ is a sequence of elements in Q such that $a_d = 0$ for all but finitely many $d < 0$, the power series (9) converges to an element a of F. Its valuation $v(a)$ is equal to the minimum $\ell \in \mathbb{Z}$ such that $a_d = 0$ for $d < \ell$ and $a_{\ell} \neq 0$.*

We call (9) the *π-adic expansion* of $a \in F$.

2.2 Examples of Valuation Skew Fields

We present several examples of valuation skew fields. All examples are DVSFs except for Example 2.6.

Example 2.5 (formal Laurent series). Let K be a skew field. Denote by $K[s]$ the polynomial ring over K in indeterminate s that commutes with any element of K. Since $K[s]$ is an Ore domain, it has the quotient skew field $K(s)$, called the *rational function* (skew) *field*. The *order* $\operatorname{ord} p$ of $p \in K[s] \setminus \{0\}$ is the minimum $d \in \mathbb{N}$ such that the coefficient of s^d in p is nonzero. We also define $\operatorname{ord} f$ for $f \in K(s) \setminus \{0\}$ as $\operatorname{ord} f := \operatorname{ord} p - \operatorname{ord} q$, where $f = p/q$ with $p, q \in K[s] \setminus \{0\}$. Set $\operatorname{ord} 0 := +\infty$. Then it is well-known that the order is a discrete valuation on $K(s)$ and the residue skew field is K. A canonical (but not unique) choice of a uniformizer is s. The completion of $K(s)$ is the *formal Laurent series* (skew) *field* $K((s))$ over K in s, whose each element is expressed as

$$f = \sum_{d=\ell}^{\infty} a_d s^d \tag{10}$$

with $\ell \in \mathbb{Z}$ and $a_\ell, a_{\ell+1}, \ldots \in K$. If $a_\ell \neq 0$, then $\ell = \operatorname{ord} f$. The valuation ring of $K((s))$ is called the *formal power series* (skew) *field* $K[[s]]$ over K in s, which is the subring of $K((s))$ consisting of formal power series

$$f = \sum_{d=0}^{\infty} a_d s^d \tag{11}$$

with $a_0, a_1, \ldots \in K$.

Similarly, the *degree* $\deg p$ of $p \in K[s] \setminus \{0\}$ is defined by replacing "minimum" with "maximum" in the definition of $\operatorname{ord} p$. Define $\deg f$ for $f = p/q \in K(s)^\times$ with $p, q \in K[s] \setminus \{0\}$ as $\deg f := \deg p - \deg q$ and $\deg 0 := -\infty$ as well. Since $\deg f(s) = -\operatorname{ord} f(s^{-1})$, the minus of the degree is a discrete valuation on $K(s)$ with uniformizer s^{-1} and residue skew field K. The completion of $K(s)$ with respect to the minus degree is $K((s^{-1}))$, which is a field isomorphic to $K((s))$. □

Example 2.6 (formal Laurent series with real exponents). Let K be a skew field. A subset X of $\mathbb{R}$ is said to be *well-ordered* if any nonempty subset of X has the minimum element. We consider *formal Laurent series with real exponents*, each of which is in the following form

$$f = \sum_{x \in X} a_x s^x, \tag{12}$$

where $X \subsetneq \mathbb{R}$ is well-ordered, $a_x \in K^\times$ for $x \in X$, and s is a formal "indeterminate" that satisfies $s^{x+y} = s^x s^y$ and $as^x = s^x a$ for $x, y \in \mathbb{R}$ and $a \in K$. Addition on these series is naturally defined, and the multiplication of $f = \sum_{x \in X} a_x s^x$ and $g = \sum_{y \in Y} b_y s^y$ is given by

$$fg := \sum_{z \in \mathbb{R}} \left(\sum_{\substack{x \in X, y \in Y \\ x+y=z}} a_x b_y \right) s^z.$$

For every $z \in \mathbb{R}$, the number of $(x, y) \in X \times Y$ satisfying $x + y = z$ is finite from the assumption that X and Y are well-ordered, and the set

$$\{ z \in \mathbb{R} \mid \text{the coefficient of } s^z \text{ in } fg \text{ is nonzero} \}$$

is well-ordered as well. Hence fg is a formal Laurent series again in the sense defined above. By these operations, the set Σ of formal Laurent series with real exponents forms a skew field [46, Theorem 5.7].

Define the *order* $\operatorname{ord} f$ of (12) as the minimum $x \in X$. We also define $\operatorname{ord} 0 := +\infty$. Then as Neumann [46] indicated, ord is a valuation on Σ that is not discrete. The residue skew field of Σ is K. The skew field Σ contains $K((s))$ as a subfield, and the restrictions of the order onto $K((s))$ coincides that on $K((s))$. Reversing the ordering of $\mathbb{R}$, we can also define $\deg f$ consistent with $K((s^{-1}))$ in the completely analogous way. □

Example 2.7 (*p*-adic numbers)**.** Let p be a prime number. The *p-adic valuation* $v_p(n)$ of $n \in \mathbb{Z} \setminus \{0\}$ is the maximum $k \in \mathbb{N}$ such that p^k divides n, and is extended to $\mathbb{Q}^\times$ as $v_p(x) \coloneqq v_p(n) - v_p(m)$ for $x = n/m \in \mathbb{Q}^\times$ with $n, m \in \mathbb{Z} \setminus \{0\}$. Also we define $v_p(0) \coloneqq +\infty$. Then v_p is a discrete valuation on $\mathbb{Q}$ with uniformizer p. The residue field is $\mathbb{F}_p$. The completion of $\mathbb{Q}$ with respect to v_p is the field $\mathbb{Q}_p$ of *p-adic numbers*. $\qquad\square$

Example 2.8 (skew (inverse) Laurent series)**.** Let K be a skew field, $\sigma : K \to K$ a ring automorphism, and $\delta : K \to K$ a *left σ-derivation*; that is, it is additive, i.e., $\delta(a+b) = \delta(a) + \delta(b)$, and it satisfies $\delta(ab) = \sigma(a)\delta(b) + \delta(a)b$ for all $a, b \in K$. The (*left*) *skew polynomial ring*, or the *Ore polynomial ring* due to Ore [47] over (K, σ, δ) in indeterminate s, which is denoted by $K[s; \sigma, \delta]$, is a polynomial ring over K with the usual addition and a twisted multiplication defined by the commutation rule (3) for $a \in K$. Elements in $K[s; \sigma, \delta]$ are called *skew polynomials*. If $\delta = 0$, then $K[s; \sigma, 0]$ is denoted by $K[s; \sigma]$. When σ is the identity map id and $\delta = 0$, the skew polynomial ring is nothing but the polynomial ring $K[s]$, which means $K[s] = K[s; \mathrm{id}]$. A typical nontrivial example of skew polynomial rings is the ring $\mathbb{C}(t)[\partial; \mathrm{id}, {}']$ of differential operators, where ${}' : \mathbb{C}(t) \to \mathbb{C}(t)$ is the usual differentiation. Another example of skew polynomial rings the ring $\mathbb{C}(t)[S; \tau]$ of shift operators, where $\tau : \mathbb{C}(t) \to \mathbb{C}(t)$ is defined by $f(t) \mapsto f(t+1)$ for $f \in \mathbb{C}(t)$.

Applying the commutation rule (3) iteratively, we can uniquely represent any skew polynomial $p \in K[s; \sigma, \delta] \setminus \{0\}$ as $p = a_0 + a_1 s + \cdots + a_\ell s^\ell$, where $\ell \in \mathbb{N}$ and $a_0, \ldots, a_\ell \in K$ with $a_\ell \neq 0$. This ℓ is called the *degree* of p and is denoted by $\deg p$. We set $\deg 0 \coloneqq -\infty$. Since a skew polynomial ring $K[s; \sigma, \delta]$ is an Ore domain (see, e.g., [23, Exercise 6F]), it has the quotient skew field $K(s; \sigma, \delta)$, called the *skew rational function field*. Its element $f \in K(s; \sigma, \delta)$, called a *skew rational function*, has the degree defined by $\deg f \coloneqq \deg p - \deg q$ with $f = pq^{-1}$ and $p, q \in K[s; \sigma, \delta]$. Then $-\deg$ is a discrete valuation on $K(s; \sigma, \delta)$ with residue skew field K. Its completion is the *skew inverse Laurent series field* $K((s^{-1}; \sigma, \delta))$, which is the skew field of formal power series over K in the form of

$$f = \sum_{d=\ell}^{\infty} a_d s^{-d}$$

for some $\ell \in \mathbb{Z}$ and $a_\ell, a_{\ell+1}, \ldots \in K$ [12, Section 2.3]. This skew field has the natural addition and a multiplication defined by (3) and

$$s^{-1}a = \sum_{d=0}^{\infty} \delta_d(a) s^{-(d+1)}$$

for $a \in K$, where

$$\delta_d \coloneqq \sigma^{-1}\left(-\delta\sigma^{-1}\right)^d \tag{13}$$

for $d \in \mathbb{N}$ (the multiplication of maps means the composition) [49]. This is determined so that $ss^{-1}a = a$.

One can define the *order* $\mathrm{ord}\,p$ of a skew polynomial $p \in K[s; \sigma, \delta]$ similarly to the usual polynomials, i.e., $\mathrm{ord}\,p$ is the minimum $\ell \in \mathbb{N}$ such that p is represented as $p = a_\ell s^\ell + \cdots + a_L s^L$ for some $L \in \mathbb{N}$ and $a_\ell, \ldots, a_L \in K$ with $a_\ell \neq 0$. Set $\mathrm{ord}\,0 \coloneqq +\infty$ in the same way. However, if $a \in K^\times$ satisfies $\delta(a) \neq 0$, then $\mathrm{ord}\,s = 1$, $\mathrm{ord}\,a = 0$ and $\mathrm{ord}\,sa = \mathrm{ord}(\sigma(a)s + \delta(a)) = 0$, which violate (V1). Thus ord cannot be extended to a discrete valuation on $K(s; \sigma, \delta)$. Nevertheless, in case of $\delta = 0$, the order satisfies (V1)–(V3) and thus $K(s; \sigma) \coloneqq K(s; \sigma, 0)$ becomes a DVSF equipped with a discrete valuation $\mathrm{ord}\,f \coloneqq \mathrm{ord}\,p - \mathrm{ord}\,q$ for $f = pq^{-1} \in K(s; \sigma)$ with $p, q \in K[s; \sigma]$. This is because the change of variable $\varphi : f(s) \mapsto f(s^{-1})$ provides an isomorphism between $K(s; \sigma)$ and $K(s; \sigma^{-1})$ and $\mathrm{ord}\,f = -\deg\varphi(f)$ for $f \in K(s; \sigma)$. The completion of $K(s; \sigma)$ with respect to ord is the *skew Laurent series field* $K((s; \sigma))$, whose elements are

11

represented as formal Laurent series (10) [12, Section 2.3]. The residue skew field of $K((s; \sigma))$ is clearly K.

See [12, Chapter 2], [13, Section 7.3], and [23, Chapter 2] for details of skew polynomials, [49] for skew inverse Laurent series fields. □

2.3 Split DVSFs

A DVSF F is said to be *spilt* if it has a representative set Q such that it is a subring of the valuation ring R of F. Similarly, a DVR R is called *split* if its quotient skew field F (see Remark 2.2) is split. Such Q is called a *coefficient skew subfield* or a *Cohen skew subfield* of F and of R.

Let F be a split DVSF with coefficient skew subfield Q and residue skew field K. Since elements in Q and K correspond bijectively, Q and K must be isomorphic skew fields. We thus call Q "the" coefficient skew subfield of F. This observation also implies that F could be split only if F is *equicharacteristic*, i.e., F and K have the same characteristic. For example, the field of p-adic numbers is not split as the characteristics of $\mathbb{Q}$ and $\mathbb{F}_p$ are different. Indeed, if F is a field, then F is split if and only if F is equicharacteristic [9, Theorem 9]. Therefore, by Proposition 2.4, a complete split DVF F is isomorphic to the Laurent series field $K((s))$ over the residue field K of F. This is a special case of the Cohen structure theorem for complete commutative Noetherian local rings [9].

The situation is much more complicated in the general noncommutative case. No characterization of a DVSF to be split is yet known; Vidal [61] gave an equicharacteristic but non-split example of a DVSF. Nevertheless, as we have seen in Section 2.2, a skew inverse Laurent series field $K((s^{-1}; \sigma, \delta))$ and a skew Laurent series field $K((s; \sigma))$ over a skew field K are split, where their coefficient skew subfields are both K.

Let F be a complete split DVSF, K the coefficient skew subfield and π a uniformizer. Then Proposition 2.4 implies that the commutation rule between π and each $a \in K$ completely determines the ring structure of F. The element πa can be uniquely expressed as (5), where $\delta_d : K \to K$ is some map for all $d \in \mathbb{N}$. The family of maps $(\delta_d)_{d \in \mathbb{N}}$ satisfies the following [50]:

(HD1) δ_d is additive for $d \in \mathbb{N}$.

(HD2) $\delta_d(ab) = \sum_{i=0}^{d} \delta_i(a) \Delta_i^d(b)$ for $d \in \mathbb{N}$ and $a, b \in K$, where $\Delta_i^d : K \to K$ is defined by

$$\Delta_i^d := \sum_{\substack{j_0, \dots, j_i \in \mathbb{N} \\ j_0 + \cdots + j_i = d-i}} \delta_{j_0} \cdots \delta_{j_i}$$

for $d \in \mathbb{N}$ and $0 \in [0, d]$.

(HD3) δ_0 is an automorphism on K.

In fact, (HD1) and (HD2) are derived from the distributive law $\pi(a + b) = \pi a + \pi b$ and the associative law $\pi(ab) = (\pi a)b$, respectively [19, 54]. From (HD1), (HD2) for $d = 0$, and $\delta_0(1) = 1$ by $\pi 1 = 1\pi$, the leading map δ_0 must be a homomorphism on K. It further must be surjective by (DVR1), which implies (HD3).

Generally, a sequence $(\delta_d)_{d \in \mathbb{N}}$ of maps on a skew field K is called a *higher σ-derivation* [19, 54] of K (with $\sigma := \delta_0$) if it satisfies (HD1)–(HD3). For a higher σ-derivation $(\delta_d)_{d \in \mathbb{N}}$, we denote by $K[[s; (\delta_d)]]$ the ring of formal power series over K in indeterminate s, whose every element f is uniquely expressed as (11). The addition on $K[[s; (\delta_d)]]$ is naturally defined and the multiplication is induced from

$$sa = \sum_{d=0}^{\infty} \delta_d(a) s^{d+1}$$

for $a \in K$. This ring is an Ore domain and thus has a quotient skew field $K((s; (\delta_d)))$. As the usual formal power series ring, each $f \in K((s; (\delta_d)))$ is represented as a formal Laurent series

$$f = \sum_{d=\ell}^{\infty} a_d s^d$$

with $a_d \in K$ for every $d \in \mathbb{Z}$. Defining the *order* of $f \in K((s; (\delta_d)))$ as the minimum $\ell \in \mathbb{N}$ with $a_\ell \neq 0$, the skew field $K((s; (\delta_d)))$ becomes a complete split DVSF with respect to the order [50]; its valuation ring is $K[[s; (\delta_d)]]$, its (one choice of a) uniformizer is s, and its coefficient skew subfield is K. Conversely, as seen above, we have:

Proposition 2.9 ([50, Proposition 1.6 in p. 292]). *Let F be a complete split DVSF with coefficient skew subfield K. Then F is isomorphic to $K((s; (\delta_d)))$, where $(\delta_d)_{d \in \mathbb{N}}$ is the higher δ_0-derivation of K determined by* (5).

Corollary 2.10. *Let R be a complete split DVR with coefficient skew subfield K. Then R is isomorphic to , where $(\delta_d)_{d \in \mathbb{N}}$ is the higher δ_0-derivation of K determined by* (5).

Note that since any split DVSF F and DVR R are a skew subfield and a subring of a complete split DVSF and DVR (see Theorem 2.3, F and R are isomorphic to a skew subfield of $K((s; (\delta_d)))$ and a subring of $K((s; (\delta_d)))$, respectively.

Example 2.11. We give some examples of higher σ-derivations and corresponding complete split DVSFs. Let K be a skew field and σ an automorphism on K. Then $(\sigma, 0, 0, \dots)$ is a higher σ-derivation and $K((s; (\sigma, 0, 0, \dots))) = K((s; \sigma))$. In particular, the case when K is a field and $\sigma = \mathrm{id}$ corresponds to the representation of complete equicharacteristic described above. More generally, let δ be a *right σ-derivation*, i.e., an additive map satisfying $\delta(ab) = \delta(a)\sigma(b) + a\delta(b)$ for $a, b \in K$. Then $(\sigma, \sigma\delta, \sigma\delta^2, \dots)$ is a higher σ-derivation [10, Section 2.1]. If δ is a left σ-derivation instead of the right one, $-\sigma^{-1}\delta$ is a right σ^{-1}-derivation, and hence $(\delta_d)_{d \in \mathbb{N}}$ defined by (13) is a higher σ^{-1}-derivation; this is consistent with the fact that $K((s^{-1}; \sigma, \delta))$ is isomorphic to $K((t; (\delta_d)))$. Another type of a higher σ-derivation is given in [7]. Dumas [17] provides a survey for higher σ-derivations. $\square$

The following lemma provides a relation between coefficients in the π-adic expansions of $a \in R$ and πa.

Lemma 2.12. *Let R be a split DVR with coefficient skew subfield K and uniformizer π, and (δ_d) the higher δ_0-derivation such that R is isomorphic to $K[[s; (\delta_d)]]$ For $a = \sum_{d=0}^{\infty} a_d \pi^d \in R$ with $a_0, a_1, \dots \in K$, the coefficient b_d of π^d in the π-adic expansion of πa satisfies*

$$b_d = \begin{cases} \sum_{k=0}^{d-1} \delta_k(a_{d-k-1}) & (d \geq 1), \\ 0 & (d = 0). \end{cases} \tag{14}$$

Proof. Using (5), we can rewrite πa as

$$\pi a = \sum_{d=0}^{\infty} \pi a_d \pi^d = \sum_{d=0}^{\infty} \left(\sum_{k=0}^{\infty} \delta_k(a_d) \pi^{k+1} \right) \pi^d = \sum_{d=1}^{\infty} \left(\sum_{k=0}^{d-1} \delta_k(a_{d-k-1}) \right) \pi^d$$

as required. $\square$

Let F be a split DVSF with coefficient skew subfield K and associated higher δ_0-derivative $(\delta_d)_{d \in \mathbb{N}}$. As a computational model, we adopt the arithmetic model on K and assume that one can compute $\delta_d(a)$ for every $d \in \mathbb{N}$ and $a \in K$ in constant time. In this model, if we know the leading $M + 1$ coefficients $a_0, \dots, a_M$ in the π-adic expansion of $a \in K$, we can compute those of πa in $\mathrm{O}(M^2)$-time by (14).

3 Preliminaries on Matrices

For a ring R and $n, n' \in \mathbb{N}$, we denote the ring of $n \times n'$ matrices over R by $R^{n \times n'}$. We also denote by $Q^{n \times n'}$ the set of all $n \times n'$ matrices over a subset Q of R. A square matrix $A \in R^{n \times n}$ is said to be *invertible* if there (uniquely) exists an $n \times n$ matrix over R, denoted by A^{-1}, such that $AA^{-1} = A^{-1}A = I_n$, where I_n is the identity matrix of order n. When R can be extended to a skew field F, we call A *nonsingular* if A is invertible over F and *singular* if not; the nonsingularity does not depend on the choice of F. We denote by $\mathrm{GL}_n(R)$ the group of $n \times n$ invertible matrices over R, i.e., $\mathrm{GL}_n(R) := (R^{n \times n})^{\times}$.

For $a \in R^{\times}$ and $\alpha = (\alpha_i)_{i \in [n]} \in \mathbb{Z}^n$, we define $D(a^{\alpha}) := \mathrm{diag}(a^{\alpha_i})_{i \in [n]}$, where diag denotes the diagonal matrix. For an additive map $\varphi : R \to R$ and $A \in R^{n \times n'}$, let $\varphi(A)$ denote the $n \times n'$ matrix over R obtained by applying φ to each entry in A.

Let $A \in R^{n \times n'}$ be a matrix. For $I \subseteq [n]$ and $J \subseteq [n']$, we denote by $A[I, J]$ the submatrix of A consisting of rows I and columns J. When $I = [n]$, we simply write $A[J] := A[[n], J]$.

3.1 Matrices over Skew Fields

Let F be a skew field. A right (left) F-module is especially called a *right (left) F-vector space.* The *dimension* of a right (left) F-vector space V is defined as the rank of V as a module, that is, the cardinality of any basis of V. The usual facts from linear algebra on independent sets and generating sets in vector spaces are valid even on skew fields [38].

The *rank* rank A of a matrix $A \in F^{n \times n'}$ is the dimension of the right F-vector space spanned by the column vectors of A, and is equal to the dimension of the left F-vector space spanned by the row vectors of A. The rank is invariant under (right and left) multiplication of nonsingular matrices. It is observed that a square matrix $A \in F^{n \times n}$ is nonsingular if and only if rank $A = n$. The rank of $A \in F^{n \times n'}$ is equal to the minimum $r \in \mathbb{N}$ such that there exists a decomposition $A = BC$ by some $B \in F^{n \times r}$ and $C \in F^{r \times n'}$ [11]. Here we give another characterization of the rank, which is well-known on the commutative case.

Proposition 3.1. *The rank of a matrix $A \in F^{n \times n'}$ over a skew field F is equal to the maximum $r \in \mathbb{N}$ such that A has a nonsingular $r \times r$ submatrix. In addition, A has a nonsingular $k \times k$ submatrix for all $k \in [0, r]$.*

Proof. We first show the latter part. For $k \in [0, \mathrm{rank}\, A]$, we can take a column subset $J \subseteq [n']$ of cardinality k such that the column vectors of $A[J]$ are linearly independent. Since rank $A[J] = k$, there must be $I \subseteq [n]$ of cardinality k such that the row vectors of $A[I, J]$ is linearly independent. Then $A[I, J]$ is a $k \times k$ nonsingular submatrix of A due to rank $A[I, J] = k$.

The former part is shown as follows. Let $r \in \mathbb{N}$ be the maximum size of a nonsingular submatrix of A. It holds rank $A \leq r$ by the latter part of the claim. To show rank $A \geq r$, take an $r \times r$ nonsingular submatrix $A[I, J]$ of A. Since rank $A[I, J] = r$, the set of column vectors of A indexed by J is linearly independent. Thus we have rank $A \geq r$. $\qquad\square$

We next define the *Dieudonné determinant* for nonsingular matrices over a skew field. To describe this, we introduce the *Bruhat decomposition* as follows. A lower (upper) unitriangular matrix is a lower (resp. upper) triangular matrix whose diagonal entries are 1.

Proposition 3.2 (Bruhat decomposition [13, Theorem 9.2.2]). *A square matrix $A \in F^{n \times n}$ over a skew field F can be decomposed as $A = LDPU$, where L is lower unitriangular, D is diagonal, P is a permutation matrix, and U is upper unitriangular. If A is nonsingular, this decomposition is unique.*

Let $F_{\mathrm{ab}}^{\times} := F^{\times} / [F^{\times}, F^{\times}]$ denote the abelianization of $F^{\times}$, where $[F^{\times}, F^{\times}] := \langle \{aba^{-1}b^{-1} \mid a, b \in F^{\times}\} \rangle$ is the commutator subgroup of $F^{\times}$. The *Dieudonné determinant* $\mathrm{Det}\, A$ of $A \in \mathrm{GL}_n(F)$, which is decomposed as $A = LDPU$ by Proposition 3.2, is an element of $F_{\mathrm{ab}}^{\times}$ defined

by

$$\text{Det } A := \text{sgn}(P)e_1 e_2 \cdots e_n \text{ mod } [F^\times, F^\times],$$

where $\text{sgn}(P) \in \{+1, -1\}$ is the sign of the permutation P and $e_1, \ldots, e_n \in F^\times$ are the diagonal entries of D [14]. In case where F is commutative, the Dieudonné determinant coincides with the usual determinant.

An *elementary matrix* over F is a unitriangular matrix $E_n(i, j; e) \in \text{GL}_n(F)$ whose the (i, j)th entry $(i \neq j)$ is $e \in F$ and other off-diagonal entries are 0. An *elementary operation* on $A \in F^{n \times m}$ is the (left or right) multiplication of A by an elementary matrix, which corresponds to adding a left (right) multiple of a row (resp. column) to another row (resp. column) of A. Denote by $\text{E}_n(F)$ the subgroup of $\text{GL}_n(F)$ generated by elementary matrices. If F is a field, $\text{E}_n(F)$ is nothing but the special linear group $\text{SL}_n(F) := \{A \in \text{GL}_n(F) \mid \det A = 1\}$ [13, Theorem 3.5.1]. This can be extended to the Dieudonné determinant as follows:

Theorem 3.3 ([13, Theorem 9.2.6])**.** *For a skew field F and $n \in \mathbb{N}$, the Dieudonné determinant gives rise to an exact sequence of groups*

$$1 \longrightarrow \text{E}_n(F) \longrightarrow \text{GL}_n(F) \xrightarrow{\text{Det}} F^\times_{\text{ab}} \longrightarrow 1.$$

Namely, $\text{Det} : \text{GL}_n(F) \to F^\times_{\text{ab}}$ is a surjective map satisfying

(D1) $\text{Det } AB = \text{Det } A \, \text{Det } B$ for $A, B \in \text{GL}_n(F)$,

(D2) $\text{Det } A = 1$ for $A \in \text{E}_n(F)$,

where the inverse of (D2) also holds, i.e., $\text{E}_n(F) = \{A \in \text{GL}_n(F) \mid \text{Det } A = 1\}$. It further follows immediately from the definition of Det that

(D3) $\text{Det } \text{diag}(e_1, \ldots, e_n) = \prod_{i=1}^{n} e_i \text{ mod } [F^\times, F^\times]$ for $e_1, \ldots, e_n \in F^\times$,

where $\text{diag}(e_1, \ldots, e_n)$ is the diagonal matrix with diagonal entries $e_1, \ldots, e_n$. Indeed, Det is the unique map satisfying (D1)–(D3) since unitriangular matrices are in $\text{E}_n(F)$ and any permutation matrix P can be brought into $\text{diag}(\text{sgn}(P), 1, \ldots, 1)$ by elementary operations.

3.2 Matrices over Valuation Skew Fields

Let F be a valuation skew field with valuation v. For any $A \in \text{GL}_n(F)$, we denote by $\zeta(A)$ the valuation of any representative of Det A; this is well-defined because all commutators of $F^\times$ have valuation 0. We also define $\zeta(A) := +\infty$ for singular $A \in F^{n \times n}$. By (V1), (V3) and (D1)–(D3), it holds

(VD1) $\zeta(AB) = \zeta(A) + \zeta(B)$ for $A, B \in F^{n \times n}$,

(VD2) $\zeta(A) = 0$ for $A \in \text{E}_n(F)$,

(VD3) $\zeta(\text{diag}(d_1, \ldots, d_n)) = \sum_{i=1}^{n} v(d_i)$ for $d_1, \ldots, d_n \in F$.

By the Bruhat decomposition, $\zeta : F^{n \times n} \to \mathbb{R} \cup \{+\infty\}$ is the unique map satisfying (VD1)–(VD3), as Taelman [55] observed for $\deg \text{Det}$ of skew polynomials.

Let $\text{M}(F)$ denote the set of all square matrices of finite order over F. If we see ζ as a function on $\text{M}(F)$, it satisfies the (real) *matrix valuation* axioms. To describe this, we shall define the *determinantal sum* for two matrices $A, B \in F^{n \times n'}$ such that their columns are identical except for the first columns. The *determinantal sum* of A and B with respect to the first column is

an $n \times n'$ matrix over F whose first column is the sum of those of A and B, and other columns are the same as A. The determinantal sums with respect to other columns and rows are also defined. We denote the determinantal sum of A and B (with respect to an appropriate column or row) by $A \nabla B$.

A (real) *matrix valuation* [26] on a skew field F is a map $V : \mathrm{M}(F) \to \mathbb{R} \cup \{+\infty\}$ that satisfies

(MV1) $V \begin{pmatrix} A & O \\ O & B \end{pmatrix} = V(A) + V(B)$ for $A, B \in \mathrm{M}(F)$, where O denotes the zero matrix of appropriate size,

(MV2) $V(A \nabla B) \geq \min\{V(A), V(B)\}$ for $A, B \in \mathrm{M}(F)$ such that $A \nabla B$ is defined,

(MV3) $V(1) = 0$,

(MV4) $V(A) = +\infty$ for singular $A \in \mathrm{M}(F)$,

(MV5) $V(A)$ is unchanged if a column or a row of A is multiplied by -1.

These axioms derive extra useful formulas as follows.

Proposition 3.4 ([26]). *For a matrix valuation V on a skew field F, the following hold:*

(1) $V(AB) = V(A) + V(B)$ for $A, B \in F^{n \times n}$.

(2) $V \begin{pmatrix} A & * \\ O & B \end{pmatrix} = V \begin{pmatrix} A & O \\ * & B \end{pmatrix} = V(A) + V(B)$ for $A, B \in \mathrm{M}(F)$, where $*$ denotes any matrix of appropriate size.

(3) *The equality in* (MV2) *holds whenever $V(A) \neq V(B)$.*

By Proposition 3.4 (1) and (MV2)–(MV4), a matrix valuation V restricted to F (1×1 matrices) is exactly a valuation v on F. This can be extended to $\mathrm{M}(F)$ as ζ, i.e., $V = \zeta$ holds. In general, for any valuation v of F, ζ is a matrix valuation on F [26]; the correspondence between v and V is clearly bijective. Therefore, a matrix valuation is nothing but a valuation of the Dieudonné determinant. See also [12, Section 9.3].

For a matrix $A \in F^{n \times n'}$ over a valuation skew field F with valuation v, we define

$$\zeta_k(A) := \min\{\zeta(A[I, J]) \mid I \subseteq [n], J \subseteq [n'], |I| = |J| = k\} \tag{15}$$

for $k \in [0, \min\{n, n'\}]$. Note that $\zeta_0(A) = 0$, $\zeta_1(A)$ is equal to the minimum of the valuation of an entry in A, and $\zeta_n(A) = \zeta(A)$ for $A \in F^{n \times n}$. In addition, $\zeta_k(A) \neq +\infty$ if and only if $k \leq \mathrm{rank}\, A$ by Proposition 3.1.

Propositions 2.1 and 2.4 are naturally extended to matrices over valuation skew fields and DVSFs as follows.

Proposition 3.5. *Let F be a valuation skew field with valuation v, valuation ring R, and representative set Q. Then any $A \in R^{n \times n'}$ is uniquely expressed as $A = A_0 + \tilde{A}$, where $A_0 \in Q^{n \times n'}$ and $\tilde{A} \in J(R)^{n \times n'}$.*

Proposition 3.6. *Let F be a DVSF with discrete valuation v and let π and Q be a uniformizer and a representative set of F, respectively.*

(1) *For every $A \in F^{n \times n'}$, there uniquely exists a sequence $(A_d)_{d \in \mathbb{Z}}$ of $n \times n'$ matrices over Q such that $A_d = O$ for all but finitely many $d < 0$ and*

$$A = \sum_{d \in \mathbb{Z}} A_d \pi^d$$

in the π-adic topology. If $\ell := \zeta_1(A) \in \mathbb{Z}$, then $A_d = O$ for $d < \ell$ and $A_\ell \neq O$.

(2) *If F is complete and $(A_d)_{d\in\mathbb{Z}}$ is a sequence of elements in Q such that $A_d = O$ for all but finitely many $d < 0$, the power series (9) converges to an $n \times n'$ matrix A over F.*

For a matrix A over a DVR, the matrices A_0 in Propositions 3.5 and 3.6 are the same.

3.3 Canonical Forms

Let F be a valuation skew field with valuation ring R. A matrix over F is called *proper* if its entries are in R. A proper matrix $A \in F^{n\times n}$ is particularly called *biproper* if it is nonsingular and its inverse is also proper, i.e., $A \in \mathrm{GL}_n(R)$. The (right or left) multiplication by biproper matrices are called *biproper transformations*. We establish the *Smith–McMillan form* of matrices over F, which is a canonical form under biproper transformations. This is well-known for matrices over $\mathbb{C}(s)$ as the *Smith–McMillan form at infinity* [45, 60] in the context of control theory.

Proposition 3.7 (Smith–McMillan form). *Let F be a valuation skew field with valuation v and valuation ring R. For $A \in F^{n\times n'}$ of rank r, there exist $S \in \mathrm{GL}_n(R)$, $T \in \mathrm{GL}_{n'}(R)$ and $d_1, \ldots, d_r \in F^\times$ such that $v(d_1) \leq \cdots \leq v(d_r)$ and*

$$SAT = \begin{pmatrix} \mathrm{diag}(d_1,\ldots,d_r) & O \\ O & O \end{pmatrix}. \tag{16}$$

In addition, the element d_i for $i \in [r]$ is unique up to multiplication by a unit of R and its valuation satisfies

$$v(d_i) = \zeta_i(A) - \zeta_{i-1}(A). \tag{17}$$

Proof. We first construct the desired diagonalization. Suppose that $A \neq O$ and $d_1 \in F^\times$ is an entry in A such that $v(d_1) = \zeta_1(A)$. Multiplying permutation matrices to A from left and right, we move d_1 to the top-left entry. Note that permutation matrices are clearly biproper. Then we eliminate the first column of A other than the top entry using d_1. This can be achieved by multiplying an elementary matrix $E_n(1, i; ad_1^{-1})$ to A from left for $i = 2, \ldots, n$, where a is the $(i,1)$st entry of A. Since $ad_1^{-1} \in R$ by $v(d_1) \leq v(a)$, this elementary matrix is biproper. We similarly eliminate the first row of A other than the left entry. Now A is in the form $\begin{pmatrix} d_1 & 0 \\ 0 & B \end{pmatrix}$ with $B \in F^{(n-1)\times(n'-1)}$. Iteratively applying the same operation for B as long as $B \neq O$, we obtain the decomposition (16). Note that $\zeta_1(A) \leq \zeta_1(B)$ by (V1) and (V2) and hence $v(d_1) \leq \cdots \leq v(d_r)$.

We next show the uniqueness part. Since units of R has valuation 0, the formula (17) implies the uniqueness of $v(d_1), \ldots, v(d_r)$. Let D be the diagonal matrix constructed above. By the ordering of $d_1, \ldots, d_r$, it holds $v(d_i) = \zeta_i(D) - \zeta_{i-1}(D)$. Therefore, it suffices to show that $\zeta_k(A)$ is invariant throughout the above procedure for $k \in [0, r]$. It is clear that $\zeta_k(A)$ does not change by row and column permutations. Consider multiplying an elementary matrix $E_n(i, j; a)$ to A from left, where $i, j \in [n]$ with $i \neq j$ and $a \in R$. This corresponds to the operation of adding the ith row multiplied by a to the jth row. Put $A' := E_n(i, j; e)A$ and consider a submatrix with rows $I \subseteq [n]$ and columns $J \subseteq intsetn'$ of cardinality k. If $j \notin I$, then $A'[I, J] = A[I, J]$. If $i, j \in I$, then $A[I, J] = EA[I, J]$ for some elementary matrix E of order k, which means $\zeta(A'[I, J]) = \zeta(A[I, J])$ by (VD1) and (VD2). In the remaining case, i.e., $i \notin I \ni j$, we have

$$A'[I, J] = A[I, J] \,\nabla\, (FA[I', J]),$$

where $I' := (I \cup \{i\}) \setminus \{j\}$ and $C \in F^{n\times n}$ is the diagonal matrix having a for the ith diagonal entry and 1 for other diagonals. By (MV2), it holds

$$\zeta(A'[I, J]) \geq \min\{\zeta(A[I, J]), \zeta(CA[I', J])\} \tag{18}$$
$$= \min\{\zeta(A[I, J]), \zeta(A[I', J]) + v(a)\}.$$

17

Since $a \in R$, we have $\zeta(A'[I, J]) \geq \zeta_k(A)$. Suppose $\zeta_k(A) = \zeta(A[I, J])$. If $\zeta_k(A) > \zeta(A[I', J]) + v(a)$, the equality of (18) is attained. If $\zeta_k(A) = \zeta(A[I', J]) + v(a)$, then $\zeta_k(A) = \zeta(A[I', J])$ by $v(a) \geq 0$ and $\zeta(A[I', J]) \geq \zeta_k(A)$. In addition, we have $\zeta(A'[I', J]) = \zeta(A[I', J])$ from $j \notin I'$, which means $\zeta(A'[I', J]) = \zeta_k(A)$. Hence we have $\zeta_k(A') = \zeta_k(A)$ in all cases. The proof of the right multiplication of elementary matrices is the same. □

Solving (17) for $\zeta_k(A)$, we have

$$\zeta_k(A) = \sum_{i=1}^{k} v(d_i) \tag{19}$$

for $k \in [0, \operatorname{rank} A]$. It is worth mentioning that $v(d_i) \geq 0$ for any $A \in R^{n \times n'}$ and $i \in [\operatorname{rank} A]$ since $v(d_1) = \zeta_1(A) \geq 0$.

If A is a matrix over a DVSF F, diagonal entries of the Smith–McMillan form of A can be taken as powers of a uniformizer of F as follows.

Proposition 3.8 (Smith–McMillan form for DVSFs)**.** *Let F be a DVSF with valuation ring R and uniformizer π. For $A \in F^{n \times n'}$ of rank r, there exist $S \in \operatorname{GL}_n(R)$, $T \in \operatorname{GL}_{n'}(R)$, and unique $\alpha = (\alpha_i)_{i \in [r]} \in \mathbb{Z}^r$ such that $\alpha_1 \leq \cdots \leq \alpha_r$ and*

$$SAT = \begin{pmatrix} D(\pi^\alpha) & O \\ O & O \end{pmatrix}. \tag{20}$$

For $i \in [r]$, the integer α_i is determined by

$$\alpha_i = \zeta_i(A) - \zeta_{i-1}(A). \tag{21}$$

Proof. Let $D = S'AT$ be the Smith–McMillan form of A given in Proposition 3.7. For $i \in [r]$, we define α_i as the valuation of the ith diagonal entry d_i of D. Then (21) follows from (17). Define a biproper matrix

$$W := \begin{pmatrix} \operatorname{diag}\left(\pi^{\alpha_1} d_1^{-1}, \ldots, \pi^{\alpha_r} d_r^{-1}\right) & O \\ O & I_{n-r} \end{pmatrix} \in \operatorname{GL}_n(R).$$

Then $WD = WS'AT = UAV$ with $S := WS'$ is equal to the right hand side of (20), as required. □

The equation (19) is rewritten as

$$\zeta_k(A) = \sum_{i=1}^{k} \alpha_i \tag{22}$$

for $k \in [0, \operatorname{rank} A]$. This equation plays an important role in Section 6.1.

We present two propositions for matrices over R which are obtained as corollaries of the Smith–McMillan form. The first one claims that $\zeta_k(A)$ is nonnegative for any proper matrix $A \in R^{n \times n'}$.

Proposition 3.9. *Let R be the valuation ring of a valuation skew field. For $A \in R^{n \times n'}$ and $k \in [0, \min\{n, n'\}]$, it holds $\zeta_k(A) \geq 0$.*

Proof. If $k > r$ with $r := \operatorname{rank} A$, we have $\zeta_k(A) = +\infty > 0$. If $k \leq r$, the claim holds from (19) and $v(d_1), \ldots, v(d_r) \geq 0$. □

The second proposition is a characterization of biproper matrices.

Proposition 3.10. *Let F be a valuation skew field with valuation ring R, residue skew field K, and representative set Q, and let $\varphi : R \to K$ be the natural homomorphism. Also, let $A \in R^{n \times n}$ be a square proper matrix and $A_0 \in Q^{n \times n}$ the matrix in Proposition 3.5 with respect to A. Then the following are equivalent:*

(1) *A is biproper.*

(2) $\zeta(A) = 0$.

(3) $\varphi(A_0)$ *is nonsingular.*

Proof. Let $SAT = D := \mathrm{diag}(d_1, \ldots, d_n)$ be the Smith–McMillan form of A. Since S and T are biproper, A is biproper if and only if so is D. This is equivalent to $v(d_i) = 0$ for all $i \in [n]$, where v is the valuation of F. Since $v(d_i)$ is nonnegative for $i \in [n]$, this condition is further equivalent to $\zeta(A) = \sum_{i=1}^{n} v(d_i) = 0$, where the first equality is from (19). Thus (1) and (2) are equivalent.

We next consider (3). Let $D_0 \in Q^{n \times n}$ be the matrix obtained from D by Proposition 3.5. By the above argument, A is biproper if and only if $v(d_i) = 0$ for every $i \in [n]$. This is equivalent to the nonsingularity of $\varphi(D)$ because for $i \in [n]$, the ith diagonal of $\varphi(D)$ is nonzero if and only if $v(d_i) = 0$. Applying φ to $D = SAT$ and $A = S^{-1}DT^{-1}$, we obtain $\varphi(D) = \varphi(S)\varphi(A)\varphi(T)$ and $\varphi(A) = \varphi(S^{-1})\varphi(D)\varphi(T^{-1})$. These imply $\mathrm{rank}\,\varphi(D) = \mathrm{rank}\,\varphi(A)$. In addition, it holds $\varphi(A) = \varphi(A_0)$ and $\varphi(D) = \varphi(D_0)$ from $A - A_0, D - D_0 \in J(R)^{n \times n}$. Thus all the statements in Proposition 3.10 are equivalent. $\qquad\square$

Finally, we introduce the *Jacobson normal form* for matrices over PIDs. As stated in Section 2.1, any DVR is a PID. For a commutative PID R, the *Smith normal form* is a celebrated canonical form of matrices over R under transformations by $\mathrm{GL}_n(R)$. The *Jacobson normal form* [32] is its generalization to general noncommutative PIDs. It can also be seen as a generalization of the Smith–McMillan form over DVRs. Recall from [13, 32] that a nonzero element c of a domain R is said to be *invariant* if $cR = Rc$ and $a \in R \setminus \{0\}$ is called a *total divisor* of $b \in R \setminus \{0\}$ if there exists invariant $c \in R$ such that $bR \subseteq cR \subseteq aR$.

Proposition 3.11 (Jacobson normal form [32, Theorem 16 in Chapter 3]; see [13, Theorem 7.2.1])**.** *Let $A \in R^{n \times m}$ be a matrix of rank r over a PID R[1]. There exist $U \in \mathrm{GL}_n(R)$, $V \in \mathrm{GL}_m(R)$ and $e_1, \ldots, e_r \in R \setminus \{0\}$ such that e_i is a total divisor of e_{i+1} for $i \in [r-1]$ and*

$$UAV = \begin{pmatrix} \mathrm{diag}(e_1, \ldots, e_r) & O \\ O & O \end{pmatrix}.$$

We can also prove Proposition 3.8 by using Proposition 3.11. Namely, the Smith–McMillan form over a DVR R can also be seen as a variant of the Jacobson normal form over R regarded as a PID.

4 Combinatorial Aspects of Valuations and Matrices

4.1 Bipartite Matchings and Matrix Ranks

Let $G = (V, E)$ be an undirected graph. A *matching* of G is an edge subset $M \subseteq E$ such that no two distinct edges in M share the same end. A matching M is said to be *perfect* if every vertex of G is covered by some edge in G. The *matching problem* on G is to find a maximum-cardinality matching of M. An undirected graph is called *bipartite* if there exists a bipartition of vertices such that every edge is between different parts in the bipartition. The *Kőnig–Egerváry theorem* is a min-max theorem for the bipartite matching problem. To describe it, we shall define a *vertex cover* of a graph G as a vertex subset that includes at least one end of every edge of G.

Theorem 4.1 (Kőnig–Egerváry theorem [35]; see [51, Theorem 16.2])**.** *The maximum size of a matching in a bipartite graph G is equal to the minimum size of a vertex cover of G.*

---

[1] As explained in Section 2.1, any PID is an Ore domain, i.e., R can be extended to a skew field F. Thus the rank of A can be defined as that of a matrix over F.

Bipartite matching and ranks of matrices are closely related. Let $A = (A_{i,j}) \in F^{n \times n'}$ be a matrix over a skew field F. We associate to A a bipartite graph $G(A)$ with vertex set $[n] \sqcup [n']$ and edge set

$$E(A) \coloneqq \{(i,j) \mid i \in [n], j \in [n'], A_{i,j} \neq 0\}.$$

The *term-rank* of A, introduced by Ore [48], is the maximum size of a matching in $G(A)$. We denote the term-rank of A by t-rank A. By Theorem 4.1, t-rank A is equal to the optimal value of the following problem:

$$
\begin{array}{ll}
\text{minimize} & n + n' - s - t \\
\text{subject to} & A \text{ has a zero block of size } s \times t, \\
& s \in [0, n], t \in [0, n'].
\end{array}
$$

Indeed, t-rank A serves as a combinatorial upper bound on rank A as we well see below. When F is a field, it immediately follows from the definition of the determinant.

Proposition 4.2. *Let $A \in F^{n \times n'}$ be a matrix over a skew field F. Then it holds* rank $A \leq$ t-rank A.

Proof. Permuting rows and columns of A, we assume that A is in form of $A = \left(\begin{smallmatrix} X & Y \\ Z & O \end{smallmatrix} \right)$, where O is the zero matrix of size $s \times t$ and t-rank $A = n + n' - s - t$. Then we can decompose A as

$$A = \begin{pmatrix} X & Y \\ Z & O \end{pmatrix} = \begin{pmatrix} X & I_{n'-t} \\ Z & O \end{pmatrix} \begin{pmatrix} I_{n-s} & O \\ O & Y \end{pmatrix}. \tag{23}$$

The size of matrices in the right hand side of (23) is $n \times p$ and $p \times n'$ with $p \coloneqq$ t-rank A. Hence rank $A \leq$ t-rank A by the characterization of rank A (see Section 3.1). $\qquad\square$

4.2 Weighted Bipartite Matchings and Valuations of Determinants

We next consider the weighted bipartite matching problem, which is also called the *assignment problem*. Let $G = (U \cup V, E)$ be a bipartite graph with $n \coloneqq |U| = |V|$ and $w : E \to \mathbb{R}$ an edge weight. The *minimum-weight perfect matching problem*, or simply the *weighted matching problem*, on G with respect to w is defined as the problem of finding a perfect matching M of G having the minimum weight $w(M)$ among all perfect matchings of G. The dual problem of the linear programming (LP) relaxation of the weighted bipartite matching problem on G is the following (see [51, Theorem 17.5]):

$$
\begin{array}{lll}
\text{maximize} & \displaystyle\sum_{i \in U} p_i + \sum_{j \in V} q_j & \\
\text{subject to} & p_i + q_j \leq w(e) & (i \in U, j \in V, e = \{i, j\} \in E), \\
& p_i, q_j \in \mathbb{R} & (i \in U, j \in V).
\end{array}
$$

By the strong duality of linear programming, the optimal value of the dual problem is equal to the minimum-weight of a perfect matching in G. In addition, if w is integer-valued, then we can take optimal (p, q) as integer vectors.

The following *complementarity theorem* plays an important role in the combinatorial relaxation algorithm. Let $G = (U \cup V, E)$ be a bipartite graph equipped with an edge weight $w : E \to \mathbb{R}$. For a dual feasible solution (p, q), we define a bipartite graph $G^{\#} = (U \cup V, E^{\#})$ by

$$E^{\#} \coloneqq \{e \in E \mid p_i + q_j = w(e) \text{ with } e = \{i, j\}, i \in U, j \in V\}. \tag{24}$$

Namely, $G^{\#}$ is the subgraph of G obtained by collecting only the "tight" edges. Then the following holds from the complementarity theorem of linear programming.

Proposition 4.3 (complementarity theorem; see [42, Lemma 2.6])**.** *Under the above setting, (p, q) is optimal if and only if $G^{\#}$ has a perfect matching.*

Analogously to the relation between the bipartite matching problem and the rank computation, solving the weighted bipartite matching problem corresponds to computing the valuation of the Dieudonné determinant. Let $A = (A_{i,j}) \in F^{n \times n}$ be a square matrix over a valuation skew field F with valuation v. Recall from Section 3.2 that $\zeta(A)$ denotes the valuation of the Dieudonné determinant of A. For the bipartite graph $G(A)$ associated with A, we set an edge weight $w : E(A) \to \mathbb{R}$ as $w(e) := v(A_{i,j})$ for $e = \{i, j\} \in E(A)$. We denote by $\hat{\zeta}(A)$ the minimum-weight of a perfect matching in $G(A)$ with respect to the edge weight w. If $G(A)$ has no perfect matching, put $\hat{\zeta}(A) := +\infty$. If F is a field, then $\hat{\zeta}(A) \leq \zeta(A)$ by the definition of the determinant and the axioms (V1), (V2) of valuations. This inequality is indeed valid even for noncommutative matrices:

Proposition 4.4. *Let $A \in F^{n \times n}$ be a square matrix over a valuation skew field F. Then it holds $\hat{\zeta}(A) \leq \zeta(A)$.*

Proof. By Proposition 4.2, $\hat{\zeta}(A) = +\infty$ implies $\zeta(A) = +\infty$. Suppose $\hat{\zeta}(A) < +\infty$, i.e., $G(A)$ has a perfect matching. Let (p, q) be a dual optimal solution of the maximum-weight perfect matching problem on A. We take diagonal matrices $P, Q \in \mathrm{GL}_n(F)$ such that the valuation of the ith and the jth diagonal entries of P and Q are p_i and q_j, respectively, for every $i, j \in [n]^2$. Put $B := P^{-1}AQ^{-1}$. Then the valuation of the (i, j)th entry of B is $w(\{i, j\}) - p_i + q_j \geq 0$ for all $\{i, j\} \in E(A)$. Thus B is a matrix over the valuation ring of F, and hence $\zeta(B) \geq 0$ by Proposition 3.9. By $\zeta(B) = \zeta(A) - \hat{\zeta}(A)$, the desired inequality is proved. $\square$

4.3 Valuated Matroids

A *valuated matroid*, introduced by Dress–Wenzel [15, 16], on a finite set E is a function $\omega : 2^E \to \mathbb{R} \cup \{-\infty\}$ satisfying the following condition:

(VM) For any $j \in X \setminus Y$, there exists $j' \in Y \setminus X$ such that $\omega(X) + \omega(Y) \leq \omega(X \cup \{j'\} \setminus \{j\}) + \omega(Y \cup \{j\} \setminus \{j'\})$.

It is easily confirmed that the family $\{X \subseteq E \mid \omega(X) > -\infty\}$ forms a base family of a matroid over E (assuming the family is nonempty), which means that valuated matroids are a generalization of matroids. In addition, valuated matroids can be maximized by a greedy algorithm. Conversely, $\omega : 2^E \to \mathbb{R} \cup \{-\infty\}$ is a valuated matroid if and only if $\omega + p$ is maximized by the greedy algorithm for any linear function $p : 2^E \to \mathbb{R} \cup \{-\infty\}$ [15]. In this way, valuated matroids are recognized as a kind of "concave function" on $2^E \simeq \{0, 1\}^n$.

A typical example of valuated matroids arises from the valuation of determinants of matrices over a valuation field [15, 16]. Since the proof essentially relies on the *Grassmann–Plücker identity*, which is an expansion formula of determinants, it cannot be directly applied to valuation skew fields. Nevertheless, Hirai [27, Proposition 2.12] presented another proof which is valid for the degree of rational functions over skew fields. This can be straightforwardly extended to general valuation skew fields as follows.

Proposition 4.5. *Let $A \in F^{n \times n'}$ be a matrix over a valuation skew field F. The function $\omega : 2^{[n']} \to \mathbb{R} \cup \{-\infty\}$ given by*

$$\omega(J) := \begin{cases} -\zeta(A[X]) & (|J| = n), \\ -\infty & (otherwise) \end{cases}$$

for $X \subseteq [n']$ is a valuated matroid on $[n']$.

---

[2] By the existence of augmenting path algorithms for the weighted matching problem, we can assume that every component of p and q are integer combination of edge weights. Therefore, for every $i, j \in [n]$, there must exist $a, b \in F$ such that $v(a) = p_i$ and $v(b) = q_j$, where v is the valuation on F. The matrices P and Q are obtained by arranging these elements in diagonals.

Proof. A local characterization [45, Theorem 5.2.25] of valuated matroids claims that ω is a valuated matroid if and only if (i) $\{X \subseteq [n'] \mid \omega(X) \neq -\infty\}$ forms a base family of a matroid and (ii) ω satisfies (VM) for $X, Y \subseteq [n']$ with $|X \setminus Y| = |Y \setminus X| = 2$. The condition (i) holds since the linear independence of column vectors of A defines a matroid.

We show the condition (ii). Let $X, Y \subseteq E$ with $\omega(X), \omega(Y) \neq -\infty$ and $|X \setminus Y| = |Y \setminus X| = 2$. Put $A' := A[X \cup Y]$. By a column permutation, we arrange columns of $X \cap Y$ in the left $n - 2$ columns of A' without changing ω. In addition, by elementary row operations, we can assume without changing ω that A' is in the form of $\left(\begin{smallmatrix} S & T \\ O & U \end{smallmatrix} \right)$, where S is a nonsingular $(n-2) \times (n-2)$ matrix, T is an $(n-2) \times 4$ matrix, and U is a 2×4 matrix. Assume that $X \setminus Y = \{1, 2\}$ and $Y \setminus X = \{3, 4\}$. For distinct $j, j' \in \{1, 2, 3, 4\}$, define $u_{j,j'}$ as the valuation of the Dieudonné determinant of the 2×2 submatrix of U with column set $\{j, j'\}$. Then $\omega((X \cap Y) \cup \{j, j'\}) = -\zeta(S) - u_{j,j'}$ for any distinct $j, j' \in \{1, 2, 3, 4\}$. Hence (VM) is equivalent to the following:

(4PT) The minimum value of $u_{1,2} + u_{3,4}$, $u_{1,3} + u_{2,4}$, $u_{1,4} + u_{2,3}$ is attained at least twice.

Now $u_{1,2} \neq -\infty$ by $\omega(X) \neq -\infty$. By a column permutation, we assume that the $(1,1)$st entry of U is nonzero. In addition, we make the $(2,1)$st entry of U zero using an elementary row operation. If the $(2,3)$rd entry is nonzero, make the $(1,3)$rd entry zero in the same way. Then U is in form of either

$$U = \begin{pmatrix} a & c & d & e \\ 0 & b & 0 & f \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} a & c & 0 & e \\ 0 & b & d & f \end{pmatrix}.$$

In the left case, $u_{1,2} + u_{3,4} = u_{1,4} + u_{2,3} = v(a) + v(b) + v(d) + v(f)$ and $u_{1,3} + u_{2,4} = +\infty$, where v is the valuation of F. In the right case, $u_{1,2} + u_{3,4} = v(a) + v(b) + v(d) + v(e)$, $u_{1,4} + u_{2,3} = v(a) + v(f) + v(c) + v(d)$ and $u_{1,3} + u_{2,4} = v(a) + v(d) + \zeta(\begin{smallmatrix} c & e \\ b & f \end{smallmatrix}) \geq v(a) + v(d) + \max\{v(c) + v(f), v(b) + v(e)\}$ by Proposition 3.4 (3). The equality is attained if $v(c) + v(f) \neq v(b) + v(e)$. Hence (4PT) is satisfied for all cases. $\qquad\square$

Let R and C be finite sets. Murota [43] introduced a *valuated bimatroid* over (R, C) as a function $w : 2^R \times 2^C \to \mathbb{R} \cup \{-\infty\}$ satisfying the following conditions:

(VBM1) For any $i' \in I' \setminus I$, at least one of the following holds:

   (a1) $\exists j' \in J' \setminus J$: $w(I, J) + w(I', J') \leq w(I \cup \{i'\}, J \cup \{j'\}) + w(I' \setminus \{i'\}, J' \setminus \{j'\})$,

   (b1) $\exists i \in I \setminus I'$: $w(I, J) + w(I', J') \leq w(I \cup \{i'\} \setminus \{i\}, J) + w(I \cup \{i\} \setminus \{i'\}, J')$.

(VBM2) For any $j' \in J' \setminus J$, at least one of the following holds:

   (a2) $\exists i \in I \setminus I'$: $w(I, J) + w(I', J') \leq w(I \setminus \{i\}, J \setminus \{j\}) + w(I' \cup \{i\}, J' \cup \{j\})$,

   (b2) $\exists j' \in J' \setminus J$: $w(I, J) + w(I', J') \leq w(I, J \cup \{j'\} \setminus \{j\}) + w(I', J \cup \{j\} \setminus \{j'\})$.

The following is a noncommutative generalization of [43, Remark 2].

Proposition 4.6. *Let $A \in F^{n \times n'}$ be a matrix over a valuation skew field F. Define $w : 2^{[n]} \times 2^{[n']} \to \mathbb{R} \cup \{-\infty\}$ as*

$$w(I, J) := \begin{cases} -\zeta(A[I, J]) & (|I| = |J|), \\ -\infty & (\textit{otherwise}) \end{cases}$$

for $I \subseteq [n]$ and $J \subseteq [n']$. Then w is a valuated bimatroid.

Proof. To distinguish rows and columns of A, we identify the rows and columns of A with distinct sets R and C, respectively. Consider an $n \times (n + n')$ skew function matrix $B := \begin{pmatrix} I_n & A \end{pmatrix}$ with row set R and column set $E := R \cup C$. Then there is a one-to-one correspondence between a

submatrix of A and a submatrix of B with row set R given by $2^R \times 2^C \ni (I, J) \mapsto (R, (R \setminus I) \cup J) \in 2^R \times 2^E$. In particular, if $|I| = |J| =: k$, then $|R| = |(R \setminus I) \cup J|$ and

$$\zeta(B[(R \setminus I) \cup J]) = \zeta\begin{pmatrix} I_k & A[R \setminus I, J] \\ O & A[I, J] \end{pmatrix} = \zeta(A[I, J]) = -w(I, J).$$

Define a map $\omega : E \to \mathbb{R} \cup \{-\infty\}$ by

$$\omega(X) := \begin{cases} -\zeta(B[X]) \ (= w(R \setminus X, X \cap C)) & (|X| = n), \\ -\infty & \text{(otherwise)} \end{cases}$$

for $X \subseteq E$. Then w satisfies (VBM1) and (VBM2) if and only if ω is a valuated matroid, which was already shown in Proposition 4.5. $\qquad \square$

Let w be a valuated bimatroid over (R, C). By a kind of greedy algorithm, one can obtain sequences $\varnothing = I_0 \subseteq I_1 \subseteq \cdots I_{n^*} \subseteq R$ and $\varnothing = J_0 \subseteq J_1 \subseteq \cdots J_{n^*} \subseteq C$ with $n^* := \min\{|R|, |C|\}$ such that (I_k, J_k) is a maximizer of the right-hand side in

$$d_k := \{w(I, J) \mid |I| = |J| = k\}$$

for every $k \in [0, n^*]$ [43]. Therefore, from Proposition 4.6, any algorithm to compute valuations of the Dieudonné determinants can be applied to compute $\zeta_k(A)$ defined by (15).

5 Combinatorial Relaxation Algorithm

Let F be a split DVSF with valuation v, uniformizer π, valuation ring R, coefficient skew subfield K, and associated higher δ_0-derivations $(\delta_d)_{d \in \mathbb{N}}$. Let $A = (A_{i,j}) \in F^{n \times n}$ be a square matrix given as the π-adic expansion

$$A = \sum_{d=0}^{\ell} A_d \pi^d, \tag{25}$$

where $\ell \in \mathbb{N}$ and $A_0, \ldots, A_\ell \in K^{n \times n}$. Note that A is a matrix over R. This section describes the combinatorial relaxation algorithm for computing $\zeta(A)$.

5.1 Truncating Higher-Valuation Terms

By technical reasons, our algorithm requires an upper bound M on $\zeta(A)$ (or $\zeta(A) = +\infty$). Indeed, we can assume $\ell = \mathrm{O}(M)$ by the following proposition:

Proposition 5.1. Let F be a DVSF with uniformizer π and let $A = \sum_{d=0}^{\ell} A_d \pi^d \in F^{n \times n}$ be a matrix in form of (25). For any $M \in \mathbb{N}$ and $\tilde{A} := \sum_{d=0}^{M} A_d \pi^d$, the following hold:

(1) If $\zeta(A) \le M$, then $\zeta(A) = \zeta(\tilde{A})$.

(2) If $\zeta(A) > M$, then $\zeta(\tilde{A}) > M$.

Proof. Let v and R be the valuation and the valuation ring of F, respectively. Recall $J(R) = \pi R = R\pi$ from (DVR1) and let $\varphi : R \to R/J(R)^{M+1}$ be the natural homomorphism. It is easily checked that $\varphi(a) \ne 0$ if and only if $v(a) \le M$ and $\varphi(a) = \varphi(b) \ne 0$ implies $v(a) = v(b) \le M$ for $a, b \in R$.

Let $P = (P_{i,j}), Q = (Q_{i,j}) \in R^{n \times n}$ be any square matrices over R with $\varphi(P) = \varphi(Q)$. Let D and E be the Smith–McMillan forms of P and Q, respectively. We show $\varphi(D) = \varphi(E)$ by tracing the procedure to obtain the Smith–McMillan forms D, E given in the proof of Proposition 3.7. First, we find a matrix entry having the minimum valuation of each P and Q, and move it

to the top-left. If the minimum valuation $\zeta_1(P)$ of an entry in P is larger than M, then $\varphi(P) = O$ and thus $\varphi(Q) = O$ by $\varphi(P) = \varphi(Q)$. Thus $\varphi(D) = \varphi(E) = O$ in this case. Suppose $v(P_{i,j}) = \zeta_1(P) \le M$. By $\varphi(P_{i,j}) = \varphi(Q_{i,j}) \neq 0$, it holds $v(P_{i,j}) = v(Q_{i,j})$ and $\zeta_1(P) = \zeta_1(Q)$. Hence the top-left entries of $\varphi(D)$ and $\varphi(E)$ are the same. After moving the (i,j)th entries in P and Q to the top-left, we eliminate the first row and columns except for the top-left entries. Since φ is a homomorphism, $\varphi(P)$ remains to be the same as $\varphi(Q)$ after this elimination. Applying the above arguments to the bottom-right $(n-1) \times (n-1)$ submatrix recursively, we have $\varphi(D) = \varphi(E)$.

Let $\mathrm{diag}(d_1, \dots, d_n)$ and $\mathrm{diag}(\tilde{d}_1, \dots, \tilde{d}_n)$ be the Smith–McMillan forms of A and $\tilde{A}$, respectively. By $\varphi(A) = \varphi(\tilde{A})$ and the above arguments, the images of their Smith–McMillan forms by φ are the same, i.e., $\varphi(d_i) = \varphi(\tilde{d}_i)$ for $i \in [n]$.

Suppose that $\zeta(A) \le M$. From $\sum_{i=1}^n v(d_i) = \zeta(A) \le M$ and $v(d_i) \ge 0$ for $i \in [n]$, it holds $v(d_i) \le M$ and thus $\varphi(\tilde{d}_i) = \varphi(d_i) \neq 0$. This means $v(d_i) = v(\tilde{d}_i)$ for $i \in [n]$. Hence $\zeta(A) = \sum_{i=1}^n v(d_i) = \sum_{i=1}^n v(\tilde{d}_i) = \zeta(\tilde{A})$

Next, suppose that $\zeta(A) > M$. If $v(d_i) \le M$ for all $i \in [n]$, then $v(d_i) = v(\tilde{d}_i)$ and $\zeta(\tilde{A}) = \zeta(A) > M$ in the same way as above. If $v(d_n) > M$, then $\varphi(\tilde{d}_n) = \varphi(d_n) = 0$, which implies $\zeta(\tilde{A}) \ge v(\tilde{d}_n) > M$. $\qquad\square$

From Proposition 5.1, we can compute $\zeta(A)$ by computing it for $\tilde{A} := \sum_{d=0}^M A_d \pi^d$ instead of A. Hence we can assume $\ell = \mathrm{O}(M)$ by truncating higher-valuation terms in A.

5.2 Faithful Algorithm

This section describes the combinatorial relaxation algorithm which is faithful to the original algorithm of Murota [42]. Recall from Section 4.2 that A is associated with the bipartite graph $G(A)$ equipped with an integral edge weight and $\hat{\zeta}(A)$ denotes the minimum weight of a perfect matching in $G(A)$. By Proposition 4.4, $\hat{\zeta}(A)$ serves as a lower bound on $\zeta(A)$. We say that A is *upper-tight* if $\hat{\zeta}(A) = \zeta(A)$. The combinatorial relaxation algorithm to compute $\zeta(A)$ is the following:

Faithful Combinatorial Relaxation Algorithm

Phase 0a. Set $A^1 \leftarrow A$ and $k \leftarrow 1$.

Phase 1a. Compute $\hat{\zeta}(A^k)$ by solving the minimum-weight perfect matching problem. If $\hat{\zeta}(A^k) > M$, output $+\infty$ and halt.

Phase 2a. If A is upper-tight, output $\hat{\zeta}(A^k)$ and halt.

Phase 3a. Find $A^{k+1} \in F^{n \times n}$ such that $\zeta(A^k) = \zeta(A^{k+1})$ and $\hat{\zeta}(A^k) < \hat{\zeta}(A^{k+1})$. Set $k \leftarrow k + 1$ and go back to Phase 1a.

Since the input matrix A is over R, each edge in $G(A)$ has a nonnegative weight, from which $\hat{\zeta}(A) \ge 0$ holds. Therefore, the number of iterations is at most $\zeta(A) \le M$. In the remaining of this section, we explain details of the upper-testing testing in Phase 2a and the matrix modification in Phase 3a.

First, we consider Phase 2a. Denote by $\mathrm{D}(A^k)$ the dual problem of the minimum-weight perfect matching problem on $G(A^k)$ given in Section 4.2. For $p, q \in \mathbb{Z}^n$, put

$$B = (B_{i,j}) := D(\pi^{-p}) A^k D(\pi^{-q}). \qquad (26)$$

Then for every $i, j \in [n]$, we have

$$v(B_{i,j}) = v(\pi^{-p_i} A_{i,j}^k \pi^{-q_j}) = v(A_{i,j}^k) - p_i - q_j,$$

which is nonnegative if (p, q) is feasible to $\mathrm{D}(A^k)$. In particular, if (p, q) is feasible, then $B \in R^{n \times n}$.

The *tight coefficient matrix* $A^{\#} = (A_{i,j}^{\#})$ of A^k with respect to a feasible solution (p, q) of $\mathrm{D}(A)$ is the coefficient matrix of π^0 in the π-adic expansion of B. In particular, when F is a field, $A_{i,j}^{\#}$ is equal to the coefficient of $\pi^{p_i + q_j}$ in the π-adic expansion of $A_{i,j}$ for $i, j \in [n]$. Note that $A^{\#}$ depends on (p, q). Then $A^{\#}$ can be used for characterizing the optimality of (p, q) and the upper-tightness of A^k as follows:

Proposition 5.2. *Let $A^{\#}$ be the tight coefficient matrix of A^k with respect to an integral feasible solution (p, q) of $\mathrm{D}(A^k)$. Then (p, q) is optimal if and only if t-rank $A^{\#} = n$.*

Proof. For $i, j \in [n]$, the element $A_{i,j}^{\#}$ is nonzero if and only if $v(A_{i,j}^{\#}) = 0$, which is equivalent to $v(A_{i,j}^k) = p_i + q_j$. Thus $G(A^{\#})$ coincides with the subgraph $G^{\#}$ of $G(A^k)$ defined by (24) with respect to (p, q). By Proposition 4.3, having a perfect matching for $G(A^{\#})$ is equivalent to the optimality of (p, q). $\qquad\square$

Proposition 5.3. *Let $A^{\#}$ be the tight coefficient matrix of A^k with respect to an integral optimal solution (p, q) of $\mathrm{D}(A^k)$. Then A^k is upper-tight if and only if $A^{\#}$ is nonsingular.*

Proof. Since $\zeta(B) = \zeta(A^k) - \hat{\zeta}(A^k)$, the matrix A is upper-tight if and only if $\zeta(C) = 0$. This is equivalent to the nonsingularity of $A^{\#}$ by Proposition 3.10. $\qquad\square$

By Proposition 5.3, we can check the upper-tightness of A^k just by checking the nonsingularity of $A^{\#}$.

Modification in Phase 3a is as follows. Suppose that A^k is not upper-tight. Since the tight coefficient matrix $A^{\#}$ with respect to an integral dual optimal solution (p, q) is singular by Proposition 5.3, there exists $U \in \mathrm{GL}_n(K)$ such that

$$\text{t-rank } U A^{\#} = \operatorname{rank} U A^{\#} = \operatorname{rank} A^{\#} < n. \tag{27}$$

This U can be obtained by the Gaussian elimination applied to $A^{\#}$. We put $A^{k+1} := U'A^k$, where $U' := D(\pi^p) U D(\pi^{-p})$.

Lemma 5.4. *It holds $\zeta(A^k) = \zeta(A^{k+1})$ and $\hat{\zeta}(A^k) < \hat{\zeta}(A^{k+1})$.*

Proof. We have

$$\zeta(U') = \zeta(D(\pi^p)) + \zeta(U) + \zeta(D(\pi^{-p})) = \zeta(U) = 0$$

and hence $\zeta(A^k) = \zeta(A^{k+1})$.

To prove $\hat{\zeta}(A^k) < \hat{\zeta}(A^{k+1})$, it suffices to show that (p, q) is feasible but not optimal to $\mathrm{D}(A^{k+1})$. We first show the feasibility. Using B defined by (26), we can rewrite A^{k+1} as

$$A^{k+1} = U'A^k = D(\pi^p) U D(\pi^{-p}) D(\pi^p) B D(\pi^q) = D(\pi^p) C D(\pi^q), \tag{28}$$

where

$$C := UB. \tag{29}$$

Since $U, B \in R^{n \times n}$, the matrix C is also over R. Thus we have $v(A_{i,j}^{k+1}) \geq p_i + q_j$. Hence (p, q) is feasible to $\mathrm{D}(A^{k+1})$.

By (28), the tight coefficient matrix of A^{k+1} with respect to (p, q) is $U A^{\#}$. Therefore, by Proposition 5.2, (p, q) is not optimal to $\mathrm{D}(A^{k+1})$. $\qquad\square$

5.3 Improved Algorithm

To compute A^{k+1} in Phase 3a, we need to multiply $D(\pi^{-p})$, U, and $D(\pi^p)$ in this order from left to A^k. This operation includes the computation of the coefficients in the π-adic expansion

of $\pi^{-1}a$ for $a \in R$. This, however, is impossible for the computational model assumed in Section 1.3 because the oracle of computing the inverse of δ_0 is needed.

To avoid left-multiplying π^{-1}, we slightly improve the above faithful procedure of combinatorial relaxation. The improved algorithm does not modify the input matrix A. Instead, the algorithm keeps track of $\hat{\zeta}(A^k)$ and the matrix $C \in R^{n \times n}$ defined by (29). The improved algorithm is outlined as follows.

Improved Combinatorial Relaxation Algorithm over DVSFs

Phase 0b. Set $\gamma^0 := 0$, $C^0 := A$, and $k \leftarrow 0$.

Phase 1b. Compute an integral optimal solution $(\Delta p, \Delta q)$ of $\mathrm{D}(C^k)$ such that Δp is non-positive. Set $\gamma^{k+1} := \gamma^k + \hat{\zeta}(C^k)$. If $\gamma^{k+1} > M$, report $\zeta(A) = +\infty$ and halt. Set

$$B^{k+1} := D(\pi^{-\Delta p})C^k D(\pi^{-\Delta q}). \tag{30}$$

Phase 2b. If the coefficient matrix $A^{\#} := B_0^{k+1}$ of π^0 in the π-adic expansion of B^{k+1} is nonsingular, report $\zeta(A) = \gamma^{k+1}$ and halt.

Phase 3b. Take $U \in \mathrm{GL}_n(K)$ satisfying (27) and set $C^{k+1} := UB^{k+1}$. Put $k \leftarrow k+1$ and go back to Phase 1b.

The validity of the improved algorithm is guaranteed by the following lemma. We denote by $\Pi(p,q)$ the objective function of the dual of the bipartite matching problem, i.e.,

$$\Pi(p,q) := \sum_{i=1}^{n} p_i + \sum_{j=1}^{n} q_j.$$

Lemma 5.5. *For $k \geq 1$, we have $\gamma^k = \Pi(p,q)$ and $B^k = D(\pi^{-p})A^k D(\pi^{-q})$ for some integral optimal solution (p,q) of $\mathrm{D}(A^k)$.*

Proof. We show the claim by induction on k. The claim is clear when $k = 1$. Suppose that the claim holds for some $k \geq 1$. By the inductive assumption, $A^{\#} := B_0^k$ is the tight coefficient matrix of A^k with respect to an optimal solution (p,q) of $\mathrm{D}(A^k)$. Let $U \in \mathrm{GL}_n(K)$ be a matrix satisfying (27). We have $A^{k+1} = D(\pi^p)UD(\pi^{-p})A^k$ and $C^k = UB^k$. Let $(\Delta p, \Delta q)$ be an optimal solution of $\mathrm{D}(C^k)$ and put $\bar{p} := p + \Delta p$ and $\bar{q} := q + \Delta q$. Then we have

$$C^k = UB^k = UD(\pi^{-p})A^k D(\pi^{-q}) = D(\pi^{-p})A^{k+1}D(\pi^{-q}).$$

This means that $G(C^k) = G(A^{k+1})$ and edge weights $w_{C^k}(e)$ and $w_{A^{k+1}}(e)$ for $e = \{i,j\} \in E(C^k) = E(A^{k+1})$ satisfy

$$w_{C^k}(e) = w_{A^{k+1}}(e) - p_i - q_j$$

for $i, j \in [n]$. Therefore, $(\bar{p}, \bar{q})$ is optimal to $\mathrm{D}(A^{k+1})$ if and only if $(\Delta p, \Delta q)$ is optimal to $\mathrm{D}(C^k)$. Thus we have

$$\gamma^{k+1} = \gamma^k + \hat{\zeta}(C^k) = \gamma^k + \Pi(\Delta p, \Delta q) = \Pi(\bar{p}, \bar{q})$$

and

$$\begin{aligned}
B^{k+1} &= D(\pi^{-\Delta p})C^k D(\pi^{-\Delta q}) \\
&= D(\pi^{-\Delta p})D(\pi^{-p})A^{k+1}D(\pi^{-q})D(\pi^{-\Delta q}) \\
&= D(\pi^{-\bar{p}})A^{k+1}D(\pi^{-\bar{q}}),
\end{aligned}$$

as required. $\qquad \square$

Corollary 5.6. *The improved combinatorial relaxation algorithm correctly outputs $\zeta(A)$.*

Proof. Follows from Propositions 5.3 and 4.4 and Lemmas 5.4 and 5.5, and the assumption on M. □

We require Δp in Phase 1b to be nonpositive so that we can avoid left-multiplying π^{-1} in the computation of (30). Here we describe how we can obtain such an optimal solution $(\Delta p, \Delta q)$ of $\mathrm{D}(C^k)$. First, we initialize Δp and Δq as zero vectors, which is feasible to $\mathrm{D}(C^k)$ as the edge weight is nonnegative. We then iterate the following procedure. Construct the subgraph $G^{\#} = ([n] \sqcup [n], E^{\#})$ of $G(C^k)$ defined by (24) with respect to $(\Delta p, \Delta q)$. If $G^{\#}$ has a perfect matching, then $(\Delta p, \Delta q)$ is optimal from Proposition 4.3 and we are done. Otherwise, by Theorem 4.1, there exists $I, J \subseteq [n]$ with $|I| + |J| < n$ such that $(i, j) \in E^{\#}$ implies $i \in I$ or $j \in J$. We change $(\Delta p, \Delta q)$ into $(\Delta p', \Delta q')$ by

$$\Delta p_i' := \begin{cases} \Delta p_i - 1 & (i \in I), \\ \Delta p_i & (i \in [n] \setminus I), \end{cases} \qquad \Delta q_j' := \begin{cases} \Delta q_j & (j \in J), \\ \Delta q_j + 1 & (j \in [n] \setminus J). \end{cases} \tag{31}$$

Note that $\Delta p_i' \leq 0$ by $\Delta p_i \leq 0$ for $i \in [n]$. The following lemma is well-known:

Lemma 5.7 ([37]). *Let $(\Delta p, \Delta q)$ be a feasible but not optimal dual solution. Then $(\Delta p', \Delta q')$ given by (31) is also feasible and $\Pi(\Delta p, \Delta q) < \Pi(\Delta p', \Delta q')$.*

By Lemma 5.7, the updated $(\Delta p, \Delta q)$ is an improved feasible solution of $\mathrm{D}(C^k)$. If $\gamma^k + \Pi(\Delta p, \Delta q) > M$, then report $\zeta(A) = +\infty$ and halt immediately. Otherwise, go back to the construction of $G^{\#}$ with respect to the updated $(\Delta p, \Delta q)$.

One more implementation issue on computing (30) is left: since the π-adic expansions of entries in B^{k+1} might have infinitely many terms, we cannot store all of them. We thus truncate higher-valuation terms relying on Proposition 5.1. Let

$$\tilde{B}^{k+1} := \sum_{d=0}^{M - \gamma^{k+1}} B_d^{k+1} \pi^d,$$

where $B_d^{k+1} \in K^{n \times n}$ is the coefficient matrix of π^d in the π-adic expansion of B^{k+1} for $d \in \mathbb{N}$. We replace B^{k+1} with $\tilde{B}^{k+1}$ in Phase 1b. This operation is called the *truncation*.

Lemma 5.8. *The improved algorithm returns $\zeta(A)$ even if the above truncation procedure is executed.*

Proof. We assume that the truncation is executed only at the kth iteration; the general statement follows from this by induction. From Corollary 5.6, this algorithm outputs $\zeta(\tilde{B}^{k+1}) + \gamma^{k+1}$ if $\zeta(\tilde{B}^{k+1}) + \gamma^{k+1} \leq M$ and $+\infty$ otherwise.

Suppose $\zeta(A) < M$. Since $\zeta(A) = \zeta(C^{k+1}) + \gamma^{k+1} = \zeta(B^{k+1}) + \gamma^{k+1}$ by Lemma 5.5, it holds $\zeta(B^{k+1}) \leq M - \gamma^{k+1}$. This means $\zeta(B^{k+1}) = \zeta(\tilde{B}^{k+1})$ by Proposition 5.1. Thus, the output of the improved algorithm with truncation coincides with $\zeta(A)$. Conversely, suppose $\zeta(A) = +\infty$. Then we have $\zeta(B^{k+1}) = +\infty > M - \gamma^{k+1}$, which implies $\zeta(\tilde{B}^{k+1}) > M - \gamma^{k+1}$ by Proposition 5.1 again. Thus, the improved algorithm with truncation outputs $+\infty$. □

Now the first half of Theorem 1.1 is proved as follows. Recall that ω denotes the exponent in the time complexity to multiply two matrices over K.

Proof (of the first half of Theorem 1.1). The validity of the algorithm follows from Lemma 5.8. We analyze the running time.

Suppose that the algorithm is implemented in a way that $C \in R^{n \times n}$ and $\gamma \in \mathbb{N}$ is updated repeatedly. Let m be the number of times the algorithm applied (31) in total. We have $m \leq M$ because one application of (31) increases γ at least by 1. In each application, we solve the bipartite matching problem, which can be solved in $\mathrm{O}(n^{2.5})$-time by the Hopcroft–Karp algorithm [29]. Thus the total time complexity of this part is $\mathrm{O}(mn^{2.5}) = \mathrm{O}(Mn^{2.5})$.

For every $i, j \in [n]$, the (i,j)th entry in C is multiplied by π from left at most m times because one application of (31) increases Δp_i by at most 1. We compute the leading $\mathrm{O}(M)$ coefficients in the π-adic expansion of each entry in πC. This can be done in $\mathrm{O}(M^2)$-time by (14). Since C has n^2 entries, the total running time of this process is $\mathrm{O}(mM^2n^2) = \mathrm{O}(M^3n^2)$.

Matrix computations in Phase 2b and Phase 3b can be done in $\mathrm{O}(Mn^\omega)$-time per each iteration as B^{k+1} contains $\mathrm{O}(M)$ terms due to the truncation. Summing it over $\mathrm{O}(M)$ iterations, we obtain $\mathrm{O}(M^2n^\omega)$-time in total. Thus the desired time complexity is attained. $\qquad\square$

6 Matrix Expansion Algorithm

Let F be a split DVSF with valuation v, uniformizer π, valuation ring R, coefficient skew subfield K, and associated higher δ_0-derivations $(\delta_d)_{d\in\mathbb{N}}$. Let $A = (A_{i,j}) \in F^{n\times n}$ be a square matrix given as the π-adic expansion (25) and suppose that $\zeta(A) \leq M$ or $\zeta(A) = +\infty$. This section describes the matrix expansion algorithm for computing $\zeta(A)$.

6.1 Expanded Matrices

For $i, d \in \mathbb{N}$, let $A_d^{(i)} \in K^{n\times n}$ denote the coefficient matrix of π^d in the π-adic expansion of $\pi^i A$. Namely, for $i \in \mathbb{N}$, the matrix $\pi^i A$ is written as

$$\pi^i A = \sum_{d=0}^{\infty} A_d^{(i)} \pi^d.$$

Note that $A_d^{(i)} = O$ for $d < i$ as the valuations of entries in $\pi^i A$ are at least i. For $\mu \in \mathbb{N}$, we define the μth-order expanded matrix $\Omega_\mu(A)$ of A as the following $\mu n \times \mu n$ block matrix

$$\Omega_\mu(A) := \begin{pmatrix} A_0^{(0)} & A_1^{(0)} & \cdots\cdots\cdots\cdots\cdots\cdots & A_{\mu-1}^{(0)} \\ O & A_1^{(1)} & A_2^{(1)} & \cdots\cdots\cdots\cdots & A_{\mu-1}^{(1)} \\ \vdots & & \ddots & \ddots & & \vdots \\ \vdots & & & \ddots & \ddots & \vdots \\ \vdots & & & & A_{\mu-2}^{(\mu-2)} & A_{\mu-1}^{(\mu-2)} \\ O & \cdots\cdots\cdots\cdots\cdots & O & A_{\mu-1}^{(\mu-1)} \end{pmatrix} \in K^{\mu n \times \mu n}. \tag{32}$$

Expanded matrices satisfy the multiplicativity as follows (see also [17, Section 1.2]). This is an extension of the result in [59] for rational function matrices over $\mathbb{C}$.

Lemma 6.1. *Let $A \in R^{n\times n}$ and $B \in R^{n\times n}$ be matrices over a split DVR R. Then it holds*

$$\Omega_\mu(AB) = \Omega_\mu(A)\Omega_\mu(B)$$

for $\mu \in \mathbb{N}$.

Proof. Fix $i \in [0, \mu-1]$ and let $\pi^i A = \sum_{d=0}^{\infty} A_d^{(i)} \pi^d$ be the π-adic expansion of $\pi^i A$, where π is a uniformizer of R. Similarly, for $d \in [0, \mu-1]$, let $\pi^d B = \sum_{j=0}^{\infty} B_j^{(d)} \pi^j$ be the π-adic expansion of $\pi^d B$. Then it holds

$$\pi^i AB = \left(\sum_{d=0}^{\infty} A_d^{(i)} \pi^d\right) B = \sum_{d=0}^{\infty} A_d^{(i)} \left(\sum_{j=0}^{\infty} B_j^{(d)} \pi^j\right) = \sum_{j=0}^{\infty} \left(\sum_{d=0}^{j} A_d^{(i)} B_j^{(d)}\right) \pi^j, \tag{33}$$

where the inner sum of the last term stops at $d = j$ by $B_j^{(d)} = O$ for $j < d$. The equality (33) implies that the coefficient matrix of π^j in the π-adic expansion of $\pi^i AB$ is

$$\sum_{d=0}^{j} A_d^{(i)} B_j^{(d)} = \sum_{d=0}^{\mu-1} A_d^{(i)} B_j^{(d)}$$

for $j < \mu$, which is equal to the $(i+1, j+1)$st entry of $\Omega_\mu(A)\Omega_\mu(B)$. $\qquad\square$

Let $\omega_\mu(A)$ denote the rank of $\Omega_\mu(A)$. The following lemma claims that $\omega_\mu(A)$ coincides with that of the Smith–McMillan form (see Proposition 3.8) of A.

Lemma 6.2. *Let $A \in R^{n \times n}$ be a matrix over a split DVR R. Then it holds $\omega_\mu(A) = \omega_\mu(D)$ for $\mu \in \mathbb{N}$, where D is the Smith–McMillan form of A.*

Proof. Let $S \in R^{n \times n}$ and $T \in R^{n \times n}$ be biproper matrices such that $SAT = D$. From Lemma 6.1, we have

$$\omega_\mu(D) = \operatorname{rank} \Omega_\mu(SAT) = \operatorname{rank} \Omega_\mu(S)\Omega_\mu(A)\Omega_\mu(T).$$

For $i \in \mathbb{N}$, let $S_i^{(i)}$ be the coefficient matrix of π^i in the π-adic expansion of $\pi^i S$, where π is a uniformizer of R. Then $S_i^{(i)}$ is equal to the coefficient matrix of π^0 in the π-adic expansion of $\pi^{-i} S \pi^i$. Now $\pi^{-i} S \pi^i$ is biproper by $(\pi^{-i} S \pi^i)^{-1} = \pi^{-i} S^{-1} \pi^i$. Thus, $S_i^{(i)}$ is nonsingular from Proposition 3.10. Since $\Omega_\mu(S)$ is a block triangular matrix having $S_i^{(i)}$ for the $(i+1)$st diagonal block, it is nonsingular. Similarly, $\Omega_\mu(T)$ is nonsingular. Therefore, we have $\omega_\mu(D) = \omega_\mu(A)$. $\qquad\square$

Let $0 \leq \alpha_1 \leq \cdots \leq \alpha_r$ be the exponents of the Smith–McMillan form of $A \in R^{n \times n}$ with $r := \operatorname{rank} A$. Put

$$N_d := |\{i \in [r] \mid \alpha_i \leq d\}| \tag{34}$$

for $d \in \mathbb{N}$. Lemma 6.2 leads us to the following lemma; a similar result based on the Kronecker canonical form is also known for matrix pencils over a field [31, Theorem 2.3].

Lemma 6.3. *Let $A \in R^{n \times n}$ be a matrix over a split DVR R. For $\mu \in \mathbb{N}$, it holds*

$$\omega_\mu(A) = \sum_{d=0}^{\mu-1} N_d, \tag{35}$$

where N_d is defined by (34).

Proof. Let D be the Smith–McMillan form of A and $D_d^{(i)} \in R^{n \times n}$ the coefficient matrix of π^d in the π-adic expansion of $\pi^i D$ for $i, d \in \mathbb{N}$. Since entries of D are powers of π, the matrix D commutes with π. This implies $D_d^{(i)} = D_{d-i}^{(0)} =: D_{d-i}$ for $d \geq i$. Now $\Omega_\mu(D)$ is in the form

$$\Omega_\mu(D) = \begin{pmatrix} D_0 & D_1 & \cdots\cdots & D_{\mu-2} & D_{\mu-1} \\ O & \ddots & \ddots & \ddots & D_{\mu-2} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & D_1 \\ O & \cdots\cdots\cdots & O & D_0 \end{pmatrix}. \tag{36}$$

Let $\alpha_1, \ldots, \alpha_r$ be the exponents of the Smith–McMillan form D, where $r := \operatorname{rank} A$. The ith diagonal entry of D_d is 1 if $i \leq r$ and $\alpha_i = d$, and 0 otherwise. Thus from (36), each row and column in $\Omega_\mu(D)$ has at most one nonzero entry. Hence $\omega_\mu(D)$, which is equal to $\omega_\mu(A)$ by Lemma 6.2, is equal to the number of nonzero entries in $\Omega_\mu(D)$. It is easily checked that the $(\mu-d)$th block row of $\Omega_\mu(D)$ contains N_d nonzero entries for $d \in [0, \mu-1]$. $\qquad\square$

The equality (35) is a key identity that connects $\omega_\mu(A)$ and the Smith–McMillan form of A. We remark that (35) can be rewritten as

$$N_d = \omega_{d+1}(A) - \omega_d(A) \tag{37}$$

for $d \in \mathbb{N}$.

6.2 Legendre Conjugacy

Let $A \in R^{n \times n}$ be a matrix of rank r and $\alpha_1 \leq \ldots \leq \alpha_r$ the exponents of the Smith–McMillan form of A. Put $\zeta_k := \zeta_k(A)$ for $k = [0, r]$, where $\zeta_k(A)$ is defined by (15). From $\alpha_k \leq \alpha_{k+1}$ and (21), an inequality $\zeta_{k-1} + \zeta_{k+1} \geq 2\zeta_k$ holds for all $k \in [r-1]$. In addition, for $\mu \in \mathbb{N}$ put $\omega_\mu := \omega_\mu(A)$ and define N_μ by (34). From $N_{\mu-1} \leq N_\mu$ and (37), we have $\omega_{\mu-1} + \omega_{\mu+1} \geq 2\omega_\mu$ for all $\mu \geq 1$. These two inequalities for d_k and ω_μ indicate the *convexity* of ζ_k and ω_μ in the following sense. A (discrete) function $f : \mathbb{Z} \to \mathbb{Z} \cup \{+\infty\}$ is said to be *convex* if

$$f(x-1) + f(x+1) \geq 2f(x)$$

for all $x \in \mathbb{Z}$. We call a function $g : \mathbb{Z} \to \mathbb{Z} \cup \{-\infty\}$ *concave* if $-g$ is convex. An integer sequence $(a_k)_{k \in K}$ indexed by $K \subseteq \mathbb{Z}$ can be identified with a function $\check{a} : \mathbb{Z} \to \mathbb{Z} \cup \{+\infty\}$ by letting $\check{a}(k)$ be a_k if $k \in K$ and $+\infty$ otherwise. We can also identify a with $\hat{a} : \mathbb{Z} \to \mathbb{Z} \cup \{-\infty\}$ defined by $\hat{a}(k) := a_k$ if $k \in K$ and $\hat{a}(k) := -\infty$ otherwise. In this way, we identify $(\zeta_0, \zeta_1, \ldots, \zeta_r)$ and $(\omega_0, \omega_1, \omega_2, \ldots)$ with discrete functions $\check{\zeta} : \mathbb{Z} \to \mathbb{Z} \cup \{-\infty\}$ and $\hat{\omega} : \mathbb{Z} \to \mathbb{Z} \cup \{+\infty\}$, respectively. From the argument in the previous paragraph, both $(\zeta_0, \zeta_1, \ldots, \zeta_r)$ and $(\omega_0, \omega_1, \omega_2, \ldots)$ are convex. Let $f : \mathbb{Z} \to \mathbb{Z} \cup \{+\infty\}$ be a function such that $f(x) \in \mathbb{Z}$ for some $x \in \mathbb{Z}$. The *concave conjugate* of f is a function $f^\circ : \mathbb{Z} \to \mathbb{Z} \cup \{-\infty\}$ defined by

$$f^\circ(y) := \inf_{x \in \mathbb{Z}} (f(x) - xy)$$

for $y \in \mathbb{Z}$. Similarly for a function $g : \mathbb{Z} \to \mathbb{Z} \cup \{-\infty\}$ with $g(y) \in \mathbb{Z}$ for some $y \in \mathbb{Z}$, the *convex conjugate* of g is a function $g^\bullet : \mathbb{Z} \to \mathbb{Z} \cup \{+\infty\}$ given by

$$g^\bullet(x) := \sup_{y \in \mathbb{Z}} (g(y) + xy)$$

for $x \in \mathbb{Z}$. The maps $f \mapsto f^\circ$ and $g \mapsto g^\bullet$ are referred to as the *concave* and *convex discrete Legendre transform*, respectively. In general f° is concave and $g^\bullet$ is convex. If f is convex and g is concave,

$$(f^\circ)^\bullet = f, \quad (g^\bullet)^\circ = g \tag{38}$$

hold. Hence the Legendre transformation establishes a one-to-one correspondence between discrete convex and concave functions. See [44] for details of discrete convex/concave functions and their Legendre transform.

Indeed, the sequences of ζ_k and $-\omega_\mu$ are in the relation of Legendre conjugate. This can be shown from the key identities (22) and (35) that connect $\zeta_k(A)$ and $\omega_\mu(A)$ through the Smith–McMillan form of A.

Theorem 6.4. *Let $A \in R^{n \times n}$ be a matrix of rank r over a split DVR R. Then it holds*

$$\zeta_k(A) = \max_{\mu \geq 0} (k\mu - \omega_\mu(A)) \quad (0 \leq k \leq r), \tag{39}$$

$$\omega_\mu(A) = \max_{0 \leq k \leq r} (k\mu - \zeta_k(A)) \quad (\mu \geq 0). \tag{40}$$

Proof. Put $\zeta_k := \zeta_k(A)$ for $k \in [0, r]$ and $\omega_\mu := \omega_\mu(A)$ for $\mu \in \mathbb{N}$. Since $(\zeta_0, \zeta_1, \ldots, \zeta_r)$ is convex and $(-\omega_0, -\omega_1, -\omega_2, \ldots)$ is concave, (39) and (40) are equivalent by (38). We show (40) as follows.

First we give an equality

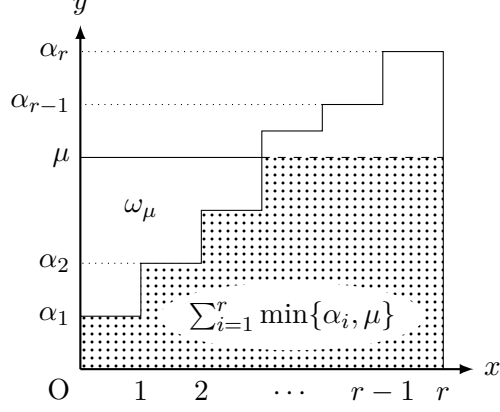$$\omega_\mu = r\mu - \sum_{i=1}^{r} \min\{\alpha_i, \mu\} \tag{41}$$

Figure 1: Graphic explanation of (41).

for $\mu \in \mathbb{N}$, where $\alpha_1 \leq \cdots \leq \alpha_r$ are the exponents of the Smith–McMillan form of A. Figure 1 graphically shows this equality. Let x and y be the coordinates along the horizontal and vertical axes in Figure 1, respectively. For $i \in [r]$, the height of the dotted rectangle with $i - 1 \leq x < i$ is $\min\{\alpha_i, \mu\}$. Hence the area of the dotted region is equal to $\sum_{i=1}^r \min\{\alpha_i, \mu\}$. In addition, the width of the white rectangle with $d \leq y < d + 1$ is equal to N_d for $d = 0, \ldots, \mu - 1$, where N_d is defined by (34). Hence the area of the white stepped region is equal to $N_0 + \cdots + N_{\mu-1} = \omega_\mu$ by (35). Now we have (41) since the sum of the areas of these two regions is $r\mu$.

Substituting (22) into the right hand side of (40), we have

$$\max_{0 \leq k \leq r} (k\mu - \zeta_k) = \max_{0 \leq k \leq r} \sum_{i=1}^k (\mu - \alpha_i) = k^*\mu - \sum_{i=1}^{k^*} \alpha_i, \tag{42}$$

where k^* is the maximum $0 \leq k \leq r$ such that $\alpha_k \leq \mu$. Since $\min\{\alpha_i, \mu\}$ is α_i if $i \leq k^*$ and μ if $i > k^*$, it holds

$$\sum_{i=1}^r \min\{\alpha_i, \mu\} = (r - k^*)\mu + \sum_{i=1}^{k^*} \alpha_i. \tag{43}$$

From (42) and (43), we have

$$\max_{0 \leq k \leq r} (k\mu - \zeta_k) = r\mu - \sum_{i=1}^r \min\{\alpha_i, \mu\},$$

in which the right hand side is equal to ω_μ by (41). $\qquad\square$

6.3   Reduction and Algorithm

We finally apply Theorem 6.4 to the computation of $\zeta(A)$ via the following lemma.

Lemma 6.5. *Let $A \in F^{n \times n}$ be a matrix (25) of rank r over a split DVSF F such that $\zeta(A) \leq M$ or $\zeta(A) = +\infty$. Then A is nonsingular if and only if $\omega_{M+1}(A) - \omega_M(A) = n$. Furthermore, if A is nonsingular, then it holds*

$$\zeta(A) = Mn - \omega_M(A). \tag{44}$$

Proof. It holds $\omega_{M+1}(A) - \omega_M(A) = N_M \leq n$ by (37). If A is singular, then N_M must be less than n. If A is nonsingular, then α_i is at most M for all $i \in [r]$, which means $N_M = n$.

31

Suppose that A is nonsingular. From (35) and (39), it holds

$$\zeta(A) = \max_{\mu \geq 0} \sum_{d=0}^{\mu-1} (n - N_d). \tag{45}$$

Since $N_0 \leq N_1 \leq \cdots \leq N_M = N_{M+1} = \cdots = n$, the maximum value of the right hand side of (45) is attained by $\mu = M$. Thus we have (44). $\qquad\square$

From Lemma 6.5, we can compute $\zeta(A)$ just by calculating $\omega_M(A)$ and $\omega_{M+1}(A)$; we call this the *matrix expansion algorithm*. These matrices can be constructed in $\mathrm{O}(M^3 n^2)$-time by repeatedly applying (14) and the rank computation can be done in $\mathrm{O}(M^\omega n^\omega)$ arithmetic operations on K. Thus we have the last half of Theorem 1.2.

7 Estimating Upper Bounds

7.1 Bounds for Skew Polynomial Rings

Let R be a split DVR with coefficient skew subfield K. In the algorithms presented in Sections 5 and 6, we assume that an upper bound M of $\zeta(A)$ is known beforehand (or $\zeta(A) = +\infty$) for $A \in R^{n \times n}$. How can we know such M? Recall that entries in the input matrix $A \in R^{n \times n}$ in (25) contain terms having valuations at most ℓ. One optimistic estimation of the upper bound is ℓn. From the definition of the determinant, this is valid when R is commutative, or equivalently, R is isomorphic to a subring of $K[[s]]$. This can be extended to the case of skew polynomial rings as follows.

Let K be a skew field equipped with an automorphism σ and a left σ-derivation δ. As stated in Example 2.8, the skew inverse Laurent series field $K((s^{-1}; \sigma, \delta))$ forms a complete split DVR with valuation $-\deg$ and uniformizer s^{-1}. We denote by $K[[s^{-1}; \sigma, \delta]]$ the valuation ring of $K((s^{-1}; \sigma, \delta))$. From Example 2.11, $K[[s^{-1}; \sigma, \delta]]$ is isomorphic to $K[[t; (\delta_d)]]$ by an isomorphism $s^{-1} \mapsto t$, where δ_d is given by (13) for $d \in \mathbb{N}$.

Proposition 7.1. *Let* $F := K((s^{-1}; \sigma, \delta))$ *be a skew inverse Laurent field over a skew field* K. *For a nonsingular matrix* $A = \sum_{d=0}^{\ell} A_d s^{-d} \in F^{n \times n}$ *with* $A_0, \ldots, A_\ell \in K^{n \times n}$, *we have* $\zeta(A) = -\deg \operatorname{Det} A \leq \ell n$.

Proof. Consider

$$B := A s^\ell = \sum_{d=0}^{\ell} A_{\ell-d} s^d \in K[s; \sigma, \delta]^{n \times n}.$$

Since $\zeta(B) = \zeta(A) + \zeta(I_n s^\ell) = \zeta(A) + n\ell$, it suffices to show $-\zeta(B) = \deg \operatorname{Det} B$ is nonnegative.

The skew polynomial ring $K[s; \sigma, \delta]$ is known to be a (left and right) PID [23, Theorem 2.8] as the usual polynomial ring $K[s]$. Let $D = UBV$ be the Jacobson normal form of B (see Proposition 3.11). Here, $U, V \in \mathrm{GL}_n(K[s; \sigma, \delta]) \subseteq \mathrm{GL}_n(K[[s^{-1}; \sigma, \delta]])$ are biproper matrices. By Proposition 3.10, we have $\zeta(D) = \zeta(U) + \zeta(B) + \zeta(V) = \zeta(B)$. Since diagonal entries in D are nonzero skew polynomials, they have nonnegative degrees. Thus we have $\zeta(B) = \zeta(D) \geq 0$. $\qquad\square$

A *skew polynomial matrix* over K refers to a matrix over a skew polynomial ring over K. As we have shown in the proof of Proposition 7.1, for a skew polynomial matrix $A = \sum_{d=0}^{\ell} A_{\ell-d} s^\ell \in K[s; \sigma, \delta]^{n \times n}$, we can reduce the computation of $\deg \operatorname{Det} A$ into that of $-\det \operatorname{Det} A s^{-\ell}$, where

$$A s^{-\ell} = \sum_{d=0}^{\ell} A_d s^{-d} \in K((s^{-1}; \sigma, \delta))^{n \times n}.$$

From Proposition 7.1, we can set $M := \ell n$ for $A s^{-\ell}$. The coefficients of $s^{-1} a$ satisfy the following recursion formula.

Lemma 7.2. *Let* $a = \sum_{d=0}^{\infty} a_d s^{-d} \in K[[s^{-1}; \sigma, \delta]]$ *with* $a_d \in K$ *for* $d \in \mathbb{N}$. *The coefficient* b_d *of* s^{-d} *in* $s^{-1}a$ *satisfies*

$$b_d = \begin{cases} \sigma^{-1}(a_{d-1} - \delta(b_{d-1})) & (d \geq 1), \\ 0 & (d = 0). \end{cases} \tag{46}$$

Proof. By (3), we have

$$\begin{aligned} a &= s(s^{-1}a) \tag{47} \\ &= s \sum_{d=0}^{\infty} b_d s^{-d} \\ &= \sum_{d=0}^{\infty} (\sigma(b_d)s + \delta(b_d))s^{-d} \\ &= \sigma(b_0)s + \sum_{d=0}^{\infty} (\sigma(b_{d+1}) + \delta(b_d))s^{-d}. \end{aligned}$$

The equation (47) means $\sigma(b_0) = 0$ and $\sigma(b_{d+1}) + \delta(b_d) = a_d$ for $d \in \mathbb{N}$, which imply (46). $\square$

From (46), we can compute the leading M coefficients of $s^{-1}a$ by $\mathrm{O}(M)$ applications of σ^{-1} and δ. This is improved from $\mathrm{O}(M^2)$ based on (14). Applying this improvement and plugging ℓn into M in the time complexities in Theorem 1.1, we obtain Theorem 1.2. We can compute $\mathrm{ord}\,\mathrm{Det}$ of matrices over $K[s; \sigma]$ in the same way. See Section 9 for an application of these computations to differential equations.

7.2 Characterizing Split DVSFs with Bounds

In Section 7.1, we described that the valuation of the Dieudonné determinant of nonsingular $A = \sum_{d=0}^{\ell} A_d \pi^d \in F^{n \times n}$ is bounded by ℓn when F is a skew inverse Laurent series field. Indeed, the converse also holds in the following sense.

Theorem 7.3. *Let* F *be a complete split DVSF with coefficient skew subfield* K *and uniformizer* π. *Then every* $A = \sum_{d=0}^{\ell} A_d \pi^{\ell} \in \mathrm{GL}_n(F)$ *with* $A_0, \dots, A_d \in K^{n \times n}$ *satisfies* $\zeta(A) \leq \ell n$ *if and only if* F *is isomorphic to* $K((s^{-1}; \sigma, \delta))$ *with some automorphism* σ *and left* σ-*derivation* δ *on* K.

Proof. The "if" part was shown in Proposition 7.1. We show the "only if" part. Let $(\delta_d)_{d \in \mathbb{N}}$ be the higher δ_0-derivatives corresponding to a complete split DVSF F. We put $\sigma := \delta_0^{-1}$ and $\delta := -\delta_0^{-1}\delta_1\delta_0^{-1}$. The motivation of these notations is the following: if F is isomorphic to $K((s^{-1}; \sigma', \delta'))$, then $\sigma' = \sigma$ and $\delta' = \delta$ by (13). We can check that σ is an automorphism and δ is a left σ-derivation.

For $a \in K$, we put $\pi^{-1}a\pi =: a' = \sum_{d=0}^{\infty} a'_d \pi^d$ with $a'_0, a'_1, \dots \in K$. We first show that if $a'_d = 0$ for any $a \in K$ and $d \geq 2$, then F is isomorphic to $K((s^{-1}; \sigma, \delta))$. Suppose that F satisfies this assumption and put $s := \pi^{-1}$. Then it holds

$$sa = \pi^{-1}a = a'\pi^{-1} = a'_0\pi^{-1} + a'_1 = a'_0s + a'_1 \tag{48}$$

for $a \in K$. From $a = \pi a' \pi^{-1}$ and (14) for $d = 0, 1$, we have $a = \delta_0(a'_0)$ and $0 = \delta_0(a'_1) + \delta_1(a'_0)$. Solving these qualities for a'_0 and a'_1, we obtain

$$a'_0 = \delta_0^{-1}(a) = \sigma(a), \tag{49}$$

$$a'_1 = \delta_0^{-1}(-\delta_1(a'_0)) = -(\delta_0^{-1}\delta_1\delta_0^{-1})(a) = \delta(a). \tag{50}$$

Substituting (49) and (50) into (48), we have

$$sa = \sigma(a)s + \delta(a),$$

33

which is nothing but the commutation rule (3) of the skew polynomial ring $K[s; \sigma, \delta]$. Hence the ring generated by π^{-1} over K, its Ore quotient skew field, and its completion F with respect to the π-adic topology are isomorphic to $K[s; \sigma, \delta]$, $K(s; \sigma, \delta)$, and $K((s^{-1}; \sigma, \delta))$, respectively.

Next, suppose that F is not isomorphic to $K((s^{-1}; \sigma, \delta))$. From the contraposition of the above proof, there exists $a \in K$ such that $a'_d \neq 0$ for some $d \geq 2$; take such a and let $k \geq 2$ be the minimum number with $a'_k \neq 0$. Consider

$$A := \begin{pmatrix} 0 & 0 \\ 1 & a'_0 \end{pmatrix} + \begin{pmatrix} 1 & a \\ 0 & a'_1 \end{pmatrix} \pi = \begin{pmatrix} \pi & a\pi \\ 1 & a'_0 + a'_1\pi \end{pmatrix} \in F^{2 \times 2}.$$

The values of ℓ and n for A are $\ell = 1$ and $n = 2$. Multiplying an elementary matrix, we can transform A into

$$B := \begin{pmatrix} 1 & 0 \\ -\pi^{-1} & 1 \end{pmatrix} A = \begin{pmatrix} \pi & a\pi \\ 0 & a'_0 + a'_1\pi - \pi^{-1}a\pi \end{pmatrix} = \begin{pmatrix} \pi & a\pi \\ 0 & -\sum_{d=k}^{\infty} a'_d \pi^d \end{pmatrix}.$$

Thus, A is nonsingular and it holds

$$\zeta(A) = \zeta(B) = v(\pi) + v\left(\sum_{d=k}^{\infty} a'_d \pi^d\right) = 1 + k > 2 = \ell n,$$

where v is the valuation on F. $\qquad\square$

Theorem 7.3 means that the condition "$\zeta(A) \leq \ell n$ for any $A = \sum_{d=0}^{\ell} A_d \pi^d \in \mathrm{GL}_n(F)$" serves as a characterization of skew inverse Laurent series fields. In this way, skew polynomials arise not only from an algebraic abstraction of linear differential/difference equations but also from the most natural condition for which the combinatorial relaxation and the matrix expansion algorithms are applicable.

8 Application 1: Weighted Edmonds' Problem

This section describes applications of our algorithm to (commutative/noncommutative) weighted Edmonds' problem (WEP). Throughout this section, we assume the arithmetic model on a field K.

Let $A = \sum_{d=0}^{\ell} A_{d-\ell} s^d$ be a square commutative or noncommutative linear polynomial matrix (2) over K. That is, A is in $L(s)^{n \times n}$, where $L := K(x_1, \ldots, x_m)$ in the commutative case and $L := K\langle\!\langle x_1, \ldots, x_m \rangle\!\rangle$ in the noncommutative case. Note that $L(s)$ is a split DVSF with valuation $-\deg$. Instead of A, we deal with the following matrix

$$As^{-\ell} = \sum_{d=0}^{\ell} A_d s^{-d}.$$

Then we can compute $\zeta(A) = -\deg \mathrm{Det}\, A$ from $\zeta(As^{-\ell})$ by $\zeta(A) = \zeta(As^{-\ell}) - \ell n$. Since $L(s)$ is a special case of skew rational function fields over L, i.e., $L(s) = L(s; \mathrm{id}, 0)$, we have $\zeta(As^{-\ell}) \leq \ell n$ when A is nonsingular by Proposition 7.1.

First, consider the combinatorial relaxation algorithm presented in Section 5. Since one cannot perform arithmetic operations on L efficiently, it is not immediate to apply the combinatorial relaxation algorithm to $As^{-\ell}$. In particular, the procedure of finding the matrix $U \in \mathrm{GL}_n(L)$ in Phase 3b based on the Gaussian elimination on L requires exponential number of arithmetic operations on K. Nevertheless, in the noncommutative case, we can make use of the following property on nc-linear matrices given by Fortin–Reutenauer [20].

Theorem 8.1 ([20, Theorem 1]). *For an nc-linear matrix $B \in K\langle\!\langle x_1, \ldots, x_m \rangle\!\rangle^{n \times n'}$ over a field K, there exist $U \in \mathrm{GL}_n(K)$ and $V \in \mathrm{GL}_{n'}(K)$ such that* t-rank $UBV = \mathrm{rank}\, B$.

The problem of finding U and V satisfying t-rank $UBV = \operatorname{rank} B$, which is a variant of nc-Edmonds' problem by Theorem 8.1, is called the *maximum vanishing subspace problem* (MVSP) due to Hamada–Hirai [25]. The MVSP can be solved in deterministic polynomial-time [25, 30]. Therefore, by using the algorithms in [25, 30] as oracles, we obtain a deterministic polynomial-time algorithm for the nc-WEP. This algorithm indeed coincides with the steepest gradient descent algorithm given by Hirai [27].

Theorem 8.2 ([27, Theorem 4.4])**.** *The nc-WEP for over a field K can be solved in deterministic* $\mathrm{O}\big(\ell^2 mn^{\omega+2} + T_{\mathrm{MVSP}}(n,m)\ell n\big)$*-time, where $T_{\mathrm{MVSP}}(n,m)$ denotes the time needed to solve the MVSP for an $n \times n$ nc-linear matrix with m symbols over K.*

Proof. In Phase 3b of each iteration, we solve the MVSP to obtain $U, V \in \mathrm{GL}_n(K)$ and put $C^{k+1} \coloneqq UB^{k+1}V$. This matrix multiplication can be done in $\mathrm{O}(\ell mn^{\omega+1})$ arithmetic operations on K. Since the number of iterations is $\mathrm{O}(\ell n)$, we obtain the desired time complexity. $\square$

We remark that the time complexity in Theorem 8.2 is in terms of the arithmetic model on K. In case of $\mathbb{K} = \mathbb{Q}$, the bit-lengths of intermediate numbers are not bounded, even if an algorithm for MVSP guarantees the bounded bit-length. In addition, since Theorem 8.2 relies on Theorem 8.1, we cannot apply the combinatorial relaxation for the commutative problem.

We next apply the matrix expansion algorithm in Section 6 to the WEP. This application is rather immediate than that of the combinatorial relaxation algorithm. Namely, if A is a commutative (noncommutative) linear polynomial matrix over a field K, then the expanded matrix $\Omega_\mu(As^{-\ell})$ given by (32) is a commutative (resp. noncommutative) linear matrix. Hence the rank computation of $\Omega_\mu(As^{-\ell})$ is nothing but solving the commutative (resp. noncommutative) Edmonds' problem. By Lemma 6.5 and Proposition 7.1, we obtain the following:

Theorem 8.3. *The commutative (noncommutative) WEP over a field K can be solved in deterministic* $\mathrm{O}\big(T_{\mathrm{EP}}(\ell n^2, m)\big)$*-time, where $T_{\mathrm{EP}}(n,m)$ denotes the time needed to solve commutative (resp. noncommutative) Edmonds' problem for an $n \times n$ commutative (resp. noncommutative) linear matrix with m symbols over K.*

The algorithms of Gurvits [24] and Ivanyos et al. [30] deterministically solve nc-Edmonds' problem with polynomially bounded bit complexity when $K = \mathbb{Q}$. Using these algorithm as oracles, we obtain Theorem 1.3.

Remark 8.4. In view of combinatorial optimization, the algorithm given in Theorem 1.3 is regarded as pseudo-polynomial time algorithms since the running time depends on a polynomial of the maximum exponent ℓ of s instead of poly$(\log \ell)$. Recently, Hirai–Ikeda [28] presented algorithms to solve the nc-WEP over K for an nc-linear polynomial matrix in form of

$$A = \sum_{k=0}^{m} A_k x_k s^{w_k}, \tag{51}$$

where $A_1, \ldots, A_m \in K^{n \times n}$ and $w_1, \ldots, w_m \in \mathbb{Z}$. The nc-WEP for (51) includes the weighted linear matroid intersection problem. An algorithm of Hirai–Ikeda runs in strongly polynomial time, i.e., it runs in time polynomial of n and m.

As an extension of a different direction, it is natural to try to solve the (commutative) WEP for

$$A = \sum_{k=0}^{m} A_k s^{w_k}, \tag{52}$$

where $A_1, \ldots, A_m \in K^{n \times n}$ and $w_1, \ldots, w_m \in \mathbb{Z}$. However, setting $w_k \coloneqq (n+1)^k$ for $k \in [m]$ would make the rank of (52) the same as that of a linear matrix $\sum_{k=0}^{m} A_k x_k \in K[x_1, \ldots, x_m]^{n \times n}$ (the *Kronecker substitution*). Since giving a deterministic polynomial-time algorithm for Edmonds' problem has been open for more than half a century, computing $\deg \det$ of (52) is also quite challenging.

9 Application 2: Linear Differential/Difference Equations

In this section, we explain that dimensions of solution spaces of linear differential and difference equations can be characterized as valuations of the Dieudonné determinants. These formulas provide applications of our algorithms to analyses of linear time-varying systems.

9.1 σ-Differential Equations

Let R be a commutative ring endowed with a ring automorphism $\sigma : R \to R$ and a left σ-derivation $\delta : R \to R$. A σ-*differential ring* is the triple (R, σ, δ), or R itself when σ and δ are clear. A σ-*differential field* is a σ-differential ring which is a field. If $\sigma = \mathrm{id}$, then σ-differential rings and fields are simply called *differential* rings and fields. Similarly, σ-differential rings and fields with $\delta = 0$ are called *difference* rings and fields.

A *constant* of a σ-differential ring (R, σ, δ) is an element $a \in R$ such that $\sigma(a) = a$ and $\delta(a) = 0$. The set of all constants of (R, σ, δ) is denoted by $\mathrm{Const}_{\sigma, \delta}(R)$ or by $\mathrm{Const}(R)$. It is easily checked that $\mathrm{Const}(R)$ is a subring of R, and if R is a field, so is $\mathrm{Const}(R)$.

An additive map $\theta : R \to R$ is said to be *pseudo-linear* if it satisfies

$$\theta(ab) = \sigma(a)\theta(b) + \delta(a)b \tag{53}$$

for all $a, b \in R$. Recall from Example 2.8 that $R[s; \sigma, \delta]$ denotes the skew polynomial ring over (R, σ, δ). Then θ induces a left $R[s; \sigma, \delta]$-module structure on R, where the action $\bullet : R[s; \sigma, \delta] \times R \to R$ is defined by

$$\left(\sum_{d=0}^{\ell} a_d s^d\right) \bullet b := \sum_{d=0}^{\ell} a_d \theta^d(b) \tag{54}$$

for $a_0, \ldots, a_\ell, b \in R$. It can be checked that $\bullet$ satisfies the axioms of actions; for example, by (3) and (53), it holds

$$(sa) \bullet b = (\sigma(a)s + \delta(a)) \bullet b = \sigma(a)\theta(b) + \delta(a)b = \theta(ab) = s \bullet (ab)$$

for $a, b \in R$. Abusing notations, we represent by θ in place of s the indeterminate of the skew polynomial ring that acts on R by (54). We also write $p \bullet b$ as $p(b)$ for $p \in R[\theta; \sigma, \delta]$.

An ℓth-order (scalar) *linear σ-differential equation* over R is an equation for $y \in R$ in the form of

$$a_0 y + a_1 \theta(y) + \cdots + a_{\ell-1}\theta^{\ell-1}(y) + a_\ell \theta^\ell(y) = f, \tag{55}$$

where $a_0, \ldots, a_\ell, f \in R$. The equation (55) can be written as $p(y) = f$ by using a skew polynomial $p := a_0 + a_1\theta + \cdots + a_\ell\theta^\ell \in R[\theta; \sigma, \delta]$. We call θ in (55) the σ-*differential operator*. If $\sigma = \mathrm{id}$ and $\theta = \delta$, then σ-differential equations are called *linear differential equations*. Similarly, if $\delta = 0$ and $\theta = \sigma$, then σ-differential equations are said to be *linear difference equations*. The equation (55) is said to be *homogeneous* when $f = 0$ and *inhomogeneous* when $f \neq 0$.

Let $\theta(y)$ denotes $(\theta(y_i))_{i \in [n]}$ for $y = (y_i)_{i \in [n]} \in R^n$. An ℓth-order n-dimensional (matrix) *linear σ-differential equation* over R is an equation for $y \in R^n$ in form of

$$A_0 y + A_1 \theta(y) + \cdots + A_{\ell-1}\theta^{\ell-1}(y) + A_\ell \theta^\ell(y) = f, \tag{56}$$

where $A_0, \ldots, A_\ell \in R^{n \times n}$ and $f \in R^n$. Using a skew polynomial matrix $A := A_0 + A_1\theta + \cdots + A_\ell\theta^\ell \in R[\theta; \sigma, \delta]^{n \times n}$, the equation (56) is simply expressed as

$$A(y) = f. \tag{57}$$

The *solution space* of (57) is defined as $V := \{y \in R^n \mid A(y) = f\}$. It is easily checked that V forms an affine module[3] over $\mathrm{Const}(R)$ unless $V = \varnothing$.

Suppose that R is a field K. Indeed, any σ-differential equation over a σ-differential field is essentially either a (usual) differential or difference equation. This follows from the following facts.

Proposition 9.1 ([4, Lemma 5], [5, Lemma 1])**.** *Let (K, σ, δ) be a σ-differential field. Then the following hold:*

(1) *An additive map $\theta : K \to K$ is pseudo-linear if and only if it is in the form of $\gamma\sigma + \delta$ for some $\gamma \in K$.*

(2) *If $\sigma \neq \mathrm{id}$, then there exists $\alpha \in K$ such that $\delta = \alpha(\sigma - \mathrm{id})$.*

By Proposition 9.1, a pseudo-linear map θ can be written as $\theta = \delta + \gamma$ if $\alpha = \mathrm{id}$ and as $\theta = (\alpha + \gamma)\sigma + \alpha$ if $\sigma \neq \mathrm{id}$. Expanding θ^d for $d = 1, \ldots, \ell$ using these equations, any σ-differential equation $p(y) = 0$ with $p \in K[\theta; \sigma, \delta]$ is represented as $q(y) = 0$ for some $q \in K[\delta; \mathrm{id}, \delta]$ if $\sigma = \mathrm{id}$ and as $q'(y) = 0$ for some $q' \in K[\sigma; \sigma, 0]$ if $\sigma \neq \mathrm{id}$. A typical example of this reduction is the replacement of the difference operator in a difference equation by the shift operator. Therefore, it essentially suffices to consider only differential equations ($\theta = \delta$) over a differential field and difference equations ($\theta = \sigma$) over a difference field. Nonetheless, we make use of the notion of σ-differential equations whenever possible since it provides a useful framework unifying differential and difference equations.

9.2 Dimensions of Solution Spaces

Let (K, σ, δ) be a differential ($\sigma = \mathrm{id}$) or difference ($\delta = 0$) field. We put $\theta := \delta$ in the differential case and $\theta := \sigma$ in the difference case. Consider a differential or difference equation (57) over K and suppose that (57) has at least one solution. The solution space V of (57) forms an affine space over $C := \mathrm{Const}(K)$ as stated above. Now our question is how large the dimension $\dim_C V$ of V over C is. This quantity is rephrased as the number of values we must designate to determine a solution of (57) uniquely. An upper bound on $\dim_C V$ is given in terms of $\deg \mathrm{Det}$ and $\mathrm{ord}\,\mathrm{Det}$ of A as follows. This is partially given in [58, Lemma 1.10], [53, Corollary 4.9], [1, Theorem 6], and [55, Corollary 2.2], whereas they assume $\mathrm{ch}(K) = 0$ which is not needed to show the following. Here, we describe complete a proof based on their proofs.

Proposition 9.2. *Let (K, σ, δ) be a differential or difference field with $C := \mathrm{Const}(K)$. Let V be the solution space of $A(y) = f$ with $A \in K[\theta; \sigma, \delta]^{n \times n}$ and $f \in K^n$ and suppose $V \neq \varnothing$. Then the following hold:*

(1) *If the field extension K / C is infinite, then $\dim_C V$ is finite if and only if A is nonsingular.*

(2) *If A is nonsingular, it holds $\dim_C V \leq \deg \mathrm{Det}\,A$ in the differential case and $\dim_C V \leq \deg \mathrm{Det}\,A - \mathrm{ord}\,\mathrm{Det}\,A$ in the difference case.*

Proof. For any $v \in V$, the C-vector space $V - v := \{y - v \mid y \in V\}$ is the solution space of $A(y) = 0$. Hence it suffices to consider only homogeneous equations. Our proof consists of three steps: we show the claims for first-order homogeneous equations in Step 1, for scalar homogeneous equations in Step 2, and for general homogeneous equations in Step 3.

(Step 1) Consider the case when $A = A_0 + I_n\theta$ and $f = 0$, i.e., the corresponding linear σ-differential equation is

$$\theta(y) = -A_0 y. \tag{58}$$

---

[3]Affine modules are a generalization of affine spaces obtained by replacing tangent vector spaces with modules. They are nothing but affine spaces if $\mathrm{Const}(R)$ is a field.

We further require A_0 to be nonsingular only in the difference case. Since A is nonsingular, it suffices to show only (2). Then $A\theta^{-1} = A_0\theta^{-1} + I_n$ is proper as a matrix over $K(\theta; \sigma, \delta)$ with valuation $-\deg$. Since I_n is nonsingular, it holds $\deg \mathrm{Det}\, A\theta^{-1} = 0$ by Proposition 3.10 and thus $\deg \mathrm{Det}\, A = n$. Similarly, in the difference case, it holds $\mathrm{ord}\, \mathrm{Det}\, A = 0$ by the nonsingularity of A_0. Therefore, our goal is to show $\dim_C V \leq n$ in both cases. Since $\dim_K V \leq n$ is clear, it suffices to prove $\dim_K V = \dim_C V$.

Let $v_1, \dots, v_m \in V$ be solutions of (58) that are linearly dependent over K. We show that they are also dependent over C, which implies $\dim_K V = \dim_C V$. Without loss of generality, we assume that $v_2, \dots, v_m$ are linearly independent over K. Then there uniquely exists $c_2, \dots, c_m \in K$ such that $v_1 = \sum_{i=2}^m c_i v_i$. Then it holds

$$
\begin{aligned}
0 = \theta\left(v_1 - \sum_{i=2}^m c_i v_i\right) &= \theta(v_1) - \sum_{i=2}^m \theta(c_i v_i) \\
&= -A_0 v_1 - \sum_{i=2}^m (\sigma(c_i)\theta(v_i) + \delta(c_i)v_i) \\
&= -A_0 \sum_{i=2}^m c_i v_i - \sum_{i=2}^m (-\sigma(c_i)A_0 v_i + \delta(c_i)v_i) \\
&= A_0 \sum_{i=2}^m (\sigma(c_i) - c_i)v_i - \sum_{i=2}^m \delta(c_i)v_i.
\end{aligned}
$$

In the differential case, we have $0 = -\sum_{i=2}^m \delta(c_i)v_i$ by $\sigma = \mathrm{id}$. From the independence of $v_2, \dots, v_m$, it must holds $\delta(c_i) = 0$, which means $c_i \in C$ for $i = 2, \dots, m$. In the difference case, we have $0 = \sum_{i=2}^m (\sigma(c_i) - c_i)v_i$ from $\delta = 0$ and the assumption that A_0 is nonsingular. Hence we obtain $\sigma(c_i) = c_i$ and thus $c_i \in C$ for $i = 2, \dots, m$. Thus $v_1, \dots, v_m$ are also linearly dependent over C in both cases.

(Step 2) Consider a scalar homogeneous linear differential or difference equation $p(y) = 0$ with $p = \sum_{d=0}^{\ell} a_d \theta^d \in K[\theta; \sigma, \delta]$. When $p = 0$, the solution space V coincides with K. Thus $\dim_C V = \dim_C K$ is infinite when K / C is infinite. Suppose that $p \neq 0$ and $\deg p = \ell$, i.e., $a_\ell \neq 0$. In the difference case, as $\theta = \sigma$ is bijective, $p(y) = 0$ and $p'(y) = 0$ with $p' := \theta^{-\mathrm{ord}\, p} p$ have the same solution spaces. Moreover, by $\deg p' = \deg p - \mathrm{ord}\, p$ and $\mathrm{ord}\, p' = 0$, it holds $\deg p' - \mathrm{ord}\, p' = \deg p - \mathrm{ord}\, p$. Therefore, in the difference case, we can assume $\mathrm{ord}\, p = 0$ (i.e., $a_0 \neq 0$) without loss of generality.

We construct the following ℓ-dimensional matrix linear differential or difference equation:

$$
\theta \begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_{\ell-2} \\ y_{\ell-1} \end{pmatrix} = \begin{pmatrix} 0 & & 1 & & 0 & \cdots & \cdots & \cdots & 0 \\ \vdots & & & \ddots & & & & & \vdots \\ \vdots & & & & \ddots & & & & \\ \vdots & & & & & \ddots & & & 0 \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 & & & 1 \\ -\frac{a_0}{a_\ell} & -\frac{a_1}{a_\ell} & \cdots & \cdots & -\frac{a_{\ell-2}}{a_\ell} & & -\frac{a_{\ell-1}}{a_\ell} \end{pmatrix} \begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_{\ell-2} \\ y_{\ell-1} \end{pmatrix}. \tag{59}
$$

If $y \in K$ is a solution of $p(y) = 0$, then $(y, \theta(y), \dots, \theta^{\ell-1}(y))^\top \in K^n$ is a solution of (59). Conversely, any solution of (59) is obtained in this way. Therefore, the solution space W of (59) is isomorphic to V as C-vector spaces. In the differential case, $\dim_C W = \ell = \deg p$ by the above proof of Step 1. In the difference case, the matrix in the right-hand side of (59) is nonsingular by $a_0 \neq 0$. Hence $\dim_C W = \ell = \deg p - \mathrm{ord}\, p$ again from Step 1.

(Step 3) Consider a matrix homogeneous differential or difference equation $A(y) = 0$ with $A \in K[\theta; \sigma, \delta]^{n \times n}$. Let $D = UAW = \mathrm{diag}(d_1, \dots, d_n)$ be the Jacobson normal form of A over $K[\theta; \sigma, \delta]$. Putting $z = (z_1, \dots, z_n) := W(y)$, the solution space sof $A(y) = 0$ and $D(z) = 0$ are isomorphic as C-vector spaces. Since D is diagonal, the solution space of $D(z) = 0$ is the direct

38

sum of the solution space V_i of $d_i(z_i) = 0$ for $i \in [n]$. Namely, it holds

$$\dim_C V = \sum_{i=1}^n \dim_C V_i. \tag{60}$$

If A (and thus D) is singular, there exists $i \in [n]$ such that $d_i = 0$. Thus $\dim_C V$ is infinite when K / C is infinite by the above Step 2 and (60). Suppose that A is nonsingular. Since U and W are invertible over $K[\theta; \sigma, \delta]$, they are biproper over $K(\theta; \sigma, \delta)$ with valuation deg and over $K(\theta; \sigma, 0)$ with valuation ord in the difference case. Thus $\deg \mathrm{Det}$ of U and W are 0, which means $\deg \mathrm{Det}\, A = \deg \mathrm{Det}\, D = \sum_{i=1}^n \deg d_i$. Therefore, by Step 2 and (60), we have $\dim_C V \le \deg \mathrm{Det}\, A$ in the differential case, as desired. The completely analog holds in the difference case by replacing $\deg \mathrm{Det}$ with $\deg \mathrm{Det} - \mathrm{ord}\, \mathrm{Det}$. □

The upper bound on $\dim_C V$ given in Proposition 9.2 may not be attained on some equations. For example, consider a first-order linear differential equation $y' + y = 0$ over $\mathbb{C}(t)$ with the usual differentiation $'$. The solution of this equation over $\mathbb{C}(t)$ is only $y = 0$ and thus the dimension of the solution space is 0. However, if the differential field $\mathbb{C}(t)$ is extended to $\mathbb{C}(t, \mathrm{e}^t)$, the solution space becomes $V := \{c\mathrm{e}^{-t} \mid c \in \mathbb{C}\}$, which has dimension 1 over $\mathbb{C}$. This is analogous to the situation of extending a field to its algebraic closure in order for nth-order algebraic equations to have n solutions. We explain such an extension briefly.

Let (K, σ, δ) be a differential or difference field. A differential or difference ring $(R, \bar{\sigma}, \bar{\delta})$ is called a *differential* or *difference extension* of K if K is a subring of R and $\bar{\sigma}$ and $\bar{\delta}$ coincides with σ and δ on K, respectively. A differential or difference equation $A(y) = f$ over K is naturally extended to that over R. Following [1], we call an extension R of K *adequate* if it satisfies the following:

(AE1) $C := \mathrm{Const}(R)$ is a field.

(AE2) Any scalar homogeneous differential or difference equation $p(y) = 0$ with $p \in K[\theta; \sigma, \delta] \setminus \{0\}$ has the solution space V over R such that $\dim_C V = \deg p$ in the differential case and $\dim_C V = \deg p - \mathrm{ord}\, p$ in the difference case.

Let K be a differential field. If $\mathrm{Const}(K)$ is algebraically closed, then there exists an adequate extension R of K such that $\mathrm{Const}(R) = \mathrm{Const}(K)$, called the *universal* (*differential*) *Picard–Vessiot ring* of K [58, Section 3.2]. In addition, any differential field K of characteristic 0 has a difference extension whose constant field is the algebraic closure of $\mathrm{Const}(K)$ [1]; see also [58, Exercise 1.5, 2:(c),(d), 3:(c)]. Therefore, there always exists an adequate extension of any differential field of characteristic 0.

Next, suppose that K is a difference field. If $\mathrm{Const}(K)$ is algebraically closed, there exists an adequate extension R of K such that $\mathrm{Const}(R) = \mathrm{Const}(K)$, called the *universal* (*difference*) *Picard–Vessiot ring* of K [57, Section 1.4]. Indeed, for any difference field K of characteristic 0, an adequate difference extension R can be easily constructed [1, Proposition 4], while $\mathrm{Const}(R) = \mathrm{Const}(K)$ is no longer guaranteed.

We then turn to matrix, inhomogeneous equations. As we will see below, (AE2) is indeed equivalent to the following:

(AE2') Any matrix differential or difference equation $A(y) = f$ with $A \in \mathrm{GL}_n(K[\theta; \sigma, \delta])$ and $f \in K^n$ has the solution space V over R such that $\dim_C V = \deg \mathrm{Det}\, A$ in the differential case and $\dim_C V = \deg \mathrm{Det}\, A - \mathrm{ord}\, \mathrm{Det}\, A$ in the difference case.

Lemma 9.3. (AE2) *and* (AE2') *are equivalent.*

Proof. It is clear that (AE2') implies (AE2); we show the converse holds. Let (K, σ, δ) be a differential or difference field and R its extension satisfying (AE1) and (AE2). As stated in the proof of Proposition 9.2, a matrix differential and difference equation is essentially reduced

to n scalar equations by considering the Jacobson normal form. This means that it suffices to consider only a scalar inhomogeneous equation $p(y) = f$ with $p \in K[\theta; \sigma, \delta] \setminus \{0\}$ and $f \in K \setminus \{0\}$. In addition, the solution space of $p(y) = f$ over R is the translation of the solution space of $p(y) = 0$ over R by any solution of $p(y) = f$. Therefore, our goal is to show that $p(y) = f$ has at least one solution over R.

We first deal with the differential case. Let $q := \theta f^{-1} p$. Then any solution $y \in R$ of $q(y) = 0$ is also a solution of $p(y) = cf$ for some $c \in C := \mathrm{Const}(R)$ (see [58, Exercise 1.14, 1]). By (AE2), the dimension of the solution space W of $q(y) = 0$ is $\deg q = \deg p + 1$, whereas that of $p(y) = 0$ is $\deg p < \deg q$. Therefore, there exists $v \in W$ that is not a solution of $p(v) = 0$, i.e., $p(v) = cf$ for some nonzero $c \in C^\times$. Then $c^{-1} v$ is a solution of $p(y) = f$, as required. The difference case can be in the same way by considering $q := (\theta - 1)(f^{-1} p) = \theta f^{-1} p - f^{-1} p$. $\qquad\square$

Proposition 9.2 and Lemma 9.3 lead us to the following consequence.

Theorem 9.4. *Let (K, σ, δ) be a differential or difference field, R its adequate extension, and $C := \mathrm{Const}(R)$. Let V be the solution space of $A(y) = f$ over R with $A \in \mathrm{GL}_n(K[\theta; \sigma, \delta])$ and $f \in K^n$. Then it holds $\dim_C V = \deg \mathrm{Det}\, A$ in the differential case and $\dim_C V = \deg \mathrm{Det}\, A - \mathrm{ord}\, \mathrm{Det}\, A$ in the difference case.*

Since deg and ord are discrete valuations, we can apply our algorithms to compute the dimension of solution spaces of linear differential or difference equations over an adequate extension.

Acknowledgments

References

[1] S. A. Abramov and M. A. Barkatou. On solution spaces of products of linear differential or difference operators. *ACM Communications in Computer Algebra*, 48(4):155–165, 2014.

[2] S. A. Amitsur. Rational identities and applications to algebra and geometry. *Journal of Algebra*, 3(3):304–359, 1966.

[3] B. Beckermann, H. Cheng, and G. Labahn. Fraction-free row reduction of matrices of Ore polynomials. *Journal of Symbolic Computation*, 41(5):513–543, 2006.

[4] M. Bronstein. On solutions of linear ordinary differential equations in their coefficient field. *Journal of Symbolic Computation*, 29(6):841–877, 2000.

[5] M. Bronstein and M. Petkovšek. An introduction to pseudo-linear algebra. *Theoretical Computer Science*, 157(1):3–33, 1996.

[6] H. H. Brungs. Left Euclidean rings. *Pacific Journal of Mathematics*, 45(1):27–33, 1973.

[7] H. H. Brungs and G. Törner. Skew power series rings and derivations. *Journal of Algebra*, 87(2):368–379, 1984.

[8] G. Chrystal. A fundamental theorem regarding the equivalence of systems of ordinary linear differential equations, and its application to the determination of the order and the systematic solution of a determinate system of such equations. *Transactions of the Royal Society of Edinburgh*, 38(1):163–178, 1897.

[9] I. S. Cohen. On the structure and ideal theory of complete local rings. *Transactions of the American Mathematical Society*, 59(1):54, 1946.

[10] P. M. Cohn. *Skew Field Constructions.* London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge, 1977.

[11] P. M. Cohn. *Free Rings and Their Relations*, volume 19 of *London Mathematical Society Monograph.* Academic Press, London, 2nd edition, 1985.

[12] P. M. Cohn. *Skew Fields: Theory of General Division Rings*, volume 57 of *Encyclopedia of Mathematics and Its Applications.* Cambridge University Press, Cambridge, 1995.

[13] P. M. Cohn. *Further Algebra and Applications.* Springer, London, 2003.

[14] J. Dieudonné. Les déterminants sur un corps non commutatif. *Bulletin de la Société Mathématique de France*, 71:27–45, 1943.

[15] A. W. M. Dress and W. Wenzel. Valuated matroids: a new look at the greedy algorithm. *Applied Mathematics Letters*, 3(2):33–35, 1990.

[16] A. W. M. Dress and W. Wenzel. Valuated matroids. *Advances in Mathematics*, 93(2):214–250, 1992.

[17] F. Dumas. Skew power series rings with general commutation formula. *Theoretical Computer Science*, 98(1):99–114, 1992.

[18] J. Edmonds. Systems of distinct representatives and linear algebra. *Journal of Research of the National Bureau of Standards*, 71B(4):241–245, 1967.

[19] S. Elliger. Potenzbasiserweiterungen. *Journal of Algebra*, 7(2):254–262, 1967.

[20] M. Fortin and C. Reutenauer. Commutative/noncommutative rank of linear matrices and subspaces of matrices of low rank. *Séminaire Lotharingien de Combinatoire*, 52, 2004.

[21] A. Garg, L. Gurvits, R. Oliveira, and A. Wigderson. A deterministic polynomial time algorithm for non-commutative rational identity testing. In *Proceedings of the 57th Annual IEEE Symposium on Foundations of Computer Science (FOCS '16)*, pages 109–117, 2016.

[22] M. Giesbrecht and M. S. Kim. Computing the Hermite form of a matrix of Ore polynomials. *Journal of Algebra*, 376:341–362, 2013.

[23] K. R. Goodearl and R. B. Warfield, Jr. *An Introduction to Noncommutative Noetherian Rings.* Cambridge University Press, Cambridge, second edition, 2004.

[24] L. Gurvits. Classical complexity and quantum entanglement. *Journal of Computer and System Sciences*, 69(3):448–484, 2004.

[25] M. Hamada and H. Hirai. Computing the nc-rank via discrete convex optimization on CAT(0) spaces, 2020.

[26] M. M. Hezavehi. Matrix valuations and their associated skew fields. *Results in Mathematics*, 5(1-2):149–156, 1982.

[27] H. Hirai. Computing the degree of determinants via discrete convex optimization on Euclidean buildings. *SIAM Journal on Applied Geometry and Algebra*, 3(3):523–557, 2019.

[28] H. Hirai and M. Ikeda. A cost-scaling algorithm for computing the degree of determinants, 2020.

[29] J. E. Hopcroft and R. M. Karp. An $n^{5/2}$ algorithm for maximum matchings in bipartite graphs. *SIAM Journal on Computing*, 2:225–231, 1973.

[30] G. Ivanyos, Y. Qiao, and K. V. Subrahmanyam. Constructive non-commutative rank computation is in deterministic polynomial time. *Computational Complexity*, 27(4):561–593, 2018.

[31] S. Iwata and R. Shimizu. Combinatorial analysis of generic matrix pencils. *SIAM Journal on Matrix Analysis and Applications*, 29(1):245–259, 2007.

[32] N. Jacobson. *The Theory of Rings*, volume 2 of *Mathematical Surveys and Monographs*. AMS, Providence, RI, 1943.

[33] V. Kabanets and R. Impagliazzo. Derandomizing polynomial identity tests means proving circuit lower bounds. *Computational Complexity*, 13(1–2):1–46, 2004.

[34] M. Khochtali, J. Rosenkilde né Nielsen, and A. Storjohann. Popov form computation for matrices of Ore polynomials. In *Proceedings of the 42nd International Symposium on Symbolic and Algebraic Computation (ISSAC '17)*, pages 253–260, New York, NY, 2017. ACM Press.

[35] D. König. Gráfok és mátrixok. *Matematikai és Fizikai Lapok*, 38:116–119, 1931.

[36] P. A. Krylov and A. A. Tuganbaev. *Modules over Discrete Valuation Domains*, volume 145 of *de Gruyter Expositions in Mathematics*. Walter de Gruyter, Berlin, 2008.

[37] H. W. Kuhn. The Hungarian method for the assignment problem. *Naval Research Logistics Quarterly*, 2:83–97, 1955.

[38] T. Y. Lam. *Lectures on Modules and Rings*, volume 189 of *Graduate Texts in Mathematics*. Springer, New York, NY, 1999.

[39] V. Levandovskyy and K. Schindelar. Computing diagonal form and Jacobson normal form of a matrix using Gröbner bases. *Journal of Symbolic Computation*, 46(5):595–608, 2011.

[40] L. Lovász. Singular spaces of matrices and their application in combinatorics. *Boletim da Sociedade Brasileira de Matemática*, 20(1):87–99, 1989.

[41] S. Moriyama and K. Murota. Discrete Legendre duality in polynomial matrices (in Japanese). *The Japan Society for Industrial and Applied Mathematics*, 23(2):183–202, 2013.

[42] K. Murota. Computing the degree of determinants via combinatorial relaxation. *SIAM Journal on Computing*, 24(4):765–796, 1995.

[43] K. Murota. Finding optimal minors of valuated bimatroids. *Applied Mathematics Letters*, 8(4):37–41, 1995.

[44] K. Murota. *Discrete Convex Analysis*. SIAM, Philadelphia, 2003.

[45] K. Murota. *Matrices and Matroids for Systems Analysis*, volume 20 of *Algorithms and Combinatorics*. Springer, Berlin, 2010.

[46] B. H. Neumann. On ordered division rings. *Transactions of the American Mathematical Society*, 66(1):202, 1949.

[47] O. Ore. Theory of non-commutative polynomials. *Annals of Mathematics*, 34(3):480–508, 1933.

[48] O. Ore. Graphs and matching theorems. *Duke Mathematical Journal*, 22(4):625–639, 1955.

[49] K. Paykan and A. Moussavi. Study of skew inverse Laurent series rings. *Journal of Algebra and Its Applications*, 16(12):1750221, 2017.

[50] B. Roux. Anneaux non commutatifs de valuation discrète ou finie. *Comptes Rendus de l'Académie des Sciences, Série I*, 302(9):259–262 and 291–293, 1986.

[51] A. Schrijver. *Combinatorial Optimization*, volume 24 of *Algorithms and Combinatorics*. Springer, Berlin, 2003.

[52] J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM*, 27(4):701–717, 1980.

[53] M. F. Singer. Algebraic and algorithmic aspects of linear difference equations. In *Galois Theories of Linear Difference Equations: An Introduction*, volume 211 of *Mathematical Surveys and Monograph*, pages 1–41. AMS, Providence, RI, 2016.

[54] T. H. M. Smits. Skew polynomial rings. *Indagationes Mathematicae*, 30(1):209–224, 1968.

[55] L. Taelman. Dieudonné determinants for skew polynomial rings. *Journal of Algebra and Its Applications*, 5(1):89–93, 2006.

[56] L. G. Valiant. Completeness classes in algebra. In *Proceedings of the 11th Annual ACM Symposium on Theory of Computing (STOC '79)*, pages 249–261, New York, NY, 1979. ACM Press.

[57] M. van der Put and M. F. Singer. *Galois Theory of Difference Equations*, volume 1666 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1997.

[58] M. van der Put and M. F. Singer. *Galois Theory of Linear Differential Equations*, volume 328 of *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag, Berlin, 2003.

[59] P. M. Van Dooren, P. Dewilde, and J. Vandewalle. On the determination of the Smith-Macmillan form of a rational matrix from its Laurent expansion. *IEEE Transactions on Circuits and Systems*, 26(3):180–189, 1979.

[60] G. C. Verghese and T. Kailath. Rational matrix structure. *IEEE Transactions on Automatic Control*, 26(2):434–439, 1981.

[61] R. Vidal. Anneaux de valuation discrète complets non commutatifs. *Transactions of the American Mathematical Society*, 267(1):65–81, 1981.

[62] S. Warner. *Topological Rings*, volume 178 of *North-Holand Mathematics Studies*. Elsevier, North Holland, 1993.