Integral Bases for P-Recursive Sequences*

Shaoshi Chen[a,b], Lixin Du[a,b,c], Manuel Kauers[c], and Thibaut Verron[c]

[a]KLMM, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China

[b]School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing 100049, China

[c]Institute for Algebra, Johannes Kepler University, Linz, A4040, Austria

schen@amss.ac.cn,dulixin17@mails.ucas.ac.cn

manuel.kauers@jku.at,thibaut.verron@jku.at

ABSTRACT

In an earlier paper, the notion of integrality known for algebraic number fields and fields of algebraic functions has been extended to D-finite functions. The aim of the present paper is to extend the notion to the case of P-recursive sequences. In order to do so, we formulate a general algorithm for finding all integral elements for valued vector spaces and then show that this algorithm includes not only the algebraic and the D-finite cases but also covers the case of P-recursive sequences.

CCS CONCEPTS

• **Computing methodologies → Algebraic algorithms**.

ACM Reference Format:

Shaoshi Chen[a,b], Lixin Du[a,b,c], Manuel Kauers[c], and Thibaut Verron[c]. 2020. Integral Bases for P-Recursive Sequences. In *International Symposium on Symbolic and Algebraic Computation (ISSAC '20), July 20–23, 2020, Kalamata, Greece.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3373207.3404004

1 INTRODUCTION

Singularities play an essential role in algorithms for analyzing recurrence or differential equations, and for symbolic summation and integration. The "local" behaviour at a singularity typically gives rise to severe restrictions of the possible "global" shape of a solution, and such restrictions are exploited in the design of algorithms for finding such solutions. It is therefore important to have access to information about what is going on at the singularities. Integral bases provide such access.

For algebraic number fields and algebraic function fields, this is a classical notion. Let $k = C(x)$ be the field of rational functions in x over a field C and $K = k(\alpha)$ be an algebraic extension of k. Every element of K has a minimal polynomial $m \in C[x][y]$. An element of K is called *integral* if all its series expansions only involve terms with nonnegative exponents. The integral elements of K form a $C[x]$-submodule of K, which somehow plays the role in K that $\mathbb{Z}$ plays in $\mathbb{Q}$. An integral basis of K is a k-vector space basis of K which at the same time is a $C[x]$-module basis of the module of integral elements.

Trager [2–4, 17] used integral bases in his integration algorithm for algebraic functions. This was one of the motivations for introducing the notion of integral D-finite functions [14], which were then used not only for integration [5] but also for solving differential equations in terms of hypergeometric series [11, 12]. Also for D-finite functions, integrality is defined in terms of the exponents appearing in the series expansions. The goal of the present paper is to introduce a notion of integrality for the recurrence case. Our hope is that this work will subsequently be useful for the development of new summation algorithms.

A major difference between the differential case and the shift case is the fact that singularities are no longer isolated points $\alpha \in C$. Instead, as pointed out for instance in [19], singularities should be viewed as orbits $\alpha + \mathbb{Z} \in C/\mathbb{Z}$ consisting of some $\alpha \in C$ together with all elements of C that have integer distance to α. Instead of certain kinds of series solutions at α of differential operators or algebraic equations, we have to consider certain kinds of sequence solutions $\alpha+\mathbb{Z} \to C$ of a recurrence operator. This makes the matter considerably more technical.

We proceed in two stages. In the first stage (Sections 2 and 3), we give a general formulation of the algorithm proposed by van Hoeij for algebraic function fields [18] and adapted to D-finite functions by Kauers and Koutschan [14]. The general formulation applies to arbitrary valued vector spaces, and we identify the computational assumptions on which the correctness and termination arguments of the algorithms are based. In Section 4, we show how it indeed generalizes the previous algorithms. In the second stage (Section 5), we show how the general setting developed in Sections 2 and 3 can be applied to the shift case.

2 VALUE FUNCTIONS AND INTEGRAL ELEMENTS

In this section, we recall basic terminologies about valuations on fields and vector spaces from [10, 16, 20]. Let k be a field of characteristic zero and Γ be a totally ordered abelian group, written additively, and let $\Gamma_\infty = \Gamma \cup \{\infty\}$ in which $\alpha + \infty = \infty + \alpha = \infty$ for all $\alpha \in \Gamma_\infty$ and $\beta < \infty$ for all $\beta \in \Gamma$. A mapping $\nu : k \to \Gamma_\infty$ is called a *valuation* on k if for all $a, b \in k$,

(*i*) $\nu(a) = \infty$ if and only if $a = 0$;

*S. Chen was supported by the NSFC grants 11871067, 11688101 and the Fund of the Youth Innovation Promotion Association, CAS. L. Du was supported by the NSFC grant 11871067 and the Austrian FWF grant P31571-N32. M. Kauers was supported by the Austrian FWF grants F5004 and P31571-N32. T. Verron was supported by the Austrian FWF grant P31571-N32.

ISSAC '20, July 20–23, 2020, Kalamata, Greece

ACM ISBN 978-1-4503-7100-1/20/07…$15.00

https://doi.org/10.1145/3373207.3404004

(ii) $\nu(ab) = \nu(a) + \nu(b)$;
(iii) $\nu(a + b) \geq \min\{\nu(a), \nu(b)\}$.

The pair (k, ν) is called a *valued field* and $\nu(k \setminus \{0\}) \subseteq \Gamma$ is called the *value group* of ν. The set $O_{(k,\nu)} := \{a \in k \mid \nu(a) \geq 0\}$ forms a subring of k that is called the *valuation ring* of ν.

Example 1. *A typical example of a valued field is the field of rational functions. Let C be a field of characteristic 0 and $\Gamma = \mathbb{Z}$. For any irreducible $p \in C[x]$ and $f \in C(x) \setminus \{0\}$, we can always write $f = p^m a/b$ for some $m \in \mathbb{Z}$ and $a, b \in C[x]$ with $\gcd(a, b) = 1$ and $p \nmid ab$. The valuation $\nu_p(f)$ of f at p is defined as the integer m. Set $\nu_p(0) = \infty$. Then $(C(x), \nu_p)$ is a valued field with $O_{(C(x),\nu_p)} = \{f \in C(x) \mid \nu_p(f) \geq 0\}$ being a local ring with its maximal ideal generated by p. The valuation ν_∞ defined by $\nu_\infty(f) = \deg_x(b) - \deg_x(a)$ for any $f = a/b \in C(x)$ is called the valuation at ∞. Any valuation ν on the field $C(x)$ is either ν_∞ or ν_p for some irreducible $p \in C[x]$ (see [6, Chapter 1, § 3] in the language of places). When $p = x - z$ with $z \in C$, we will write ν_z instead of ν_p. For $z \in C$, the field of formal Laurent series $C((x - z))$ admits a valuation $\nu_{(z)}$, defined as $\nu_{(z)}\left(\sum_{i\geq n} c_i(x - z)^i\right) = n$, where $c_n \neq 0$. Any $r \in C(x)$ admits a representation r_L in $C((x - z))$ with $\nu_z(r) = \nu_{(z)}(r_L)$.*

Definition 2. *Let V be a vector space over a valued field (k, ν). A map $\mathrm{val} : V \to \Gamma_\infty$ is called a* value function *on V if for all $x, y \in V$ and $a \in k$,*

(i) *$\mathrm{val}(x) = \infty$ if and only if $x = 0$;*
(ii) *$\mathrm{val}(ax) = \nu(a) + \mathrm{val}(x)$;*
(iii) *$\mathrm{val}(x + y) \geq \min\{\mathrm{val}(x), \mathrm{val}(y)\}$.*

The pair (V, val) is called a valued vector space *over k. An element $x \in V$ is said to be* integral *if $\mathrm{val}(x) \geq 0$.*

Remark 3. *Let U be any subspace of a valued vector space (V, val). Then the restriction of val on U is also a value function on U, which makes (U, val) a valued vector space.*

Proposition 4. *Let (k, ν) be a valued field and (V, val) be a valued vector space over k. The set $O_{(V,\mathrm{val})} \subseteq V$ of all integral elements in V forms an $O_{(k,\nu)}$-module.*

Proof. For any $a, b \in O_{(k,\nu)}$ and $x, y \in O_{(V,\mathrm{val})}$, we have

$$\begin{aligned}\mathrm{val}(ax + by) &\geq \min\{\mathrm{val}(ax), \mathrm{val}(by)\}\\ &= \min\{\nu(a) + \mathrm{val}(x), \nu(b) + \mathrm{val}(y)\}.\end{aligned}$$

Since $\nu(a), \nu(b) \geq 0$ and $\mathrm{val}(x), \mathrm{val}(y) \geq 0$, we have $\mathrm{val}(ax + by) \geq 0$. So $ax + by \in O_{(V,\mathrm{val})}$. ■

A k-vector space basis of a valued vector space (V, val) which is at the same time an $O_{(k,\nu)}$-module basis of $O_{(V,\mathrm{val})}$ is called a *(local) integral basis* with respect to val. Assume that the module $O_{(V,\mathrm{val})}$ has a local integral basis $\{x_1, \ldots, x_r\}$ and $x = a_1x_1 + \cdots + a_rx_r \in V$. Then $\mathrm{val}(x) \geq 0$ if and only if $\nu(a_i) \geq 0$ for all $i = 1, \ldots, r$. When does a local integral basis exist and how to construct such a basis are the main problems we study in this paper. Value functions and integral bases for algebraic function fields have been extensively studied both theoretically [6, 9, 16] and algorithmically [17–19] and have also been extended to the D-finite case [14].

Example 5. *(See [16, Example 3.3]) Any finite dimensional k-vector space can be equipped with a valuation. More precisely, let V be a vector space over a valued field (k, ν) of dimension r. Let $\{B_1, \ldots, B_r\}$ be a basis of V. Take values $\gamma_1, \ldots, \gamma_r$ in Γ and define $\mathrm{val} : V \to \Gamma \cup \{\infty\}$ by for all $a_1, \ldots, a_r \in k$,*

$$\mathrm{val}\left(\sum_{i=1}^{r} a_iB_i\right) = \min\{\gamma_1 + \nu(a_1), \ldots, \gamma_r + \nu(a_r)\}.$$

It is easy to check that val is a value function on V.

Example 6. *Let C be an algebraically closed field of characteristic 0, $k = C(x)$ and ν_z be the valuation of k at $z \in C$ as in Example 1. Then (k, ν_z) is a valued field. Let $K = k(\beta)$ with β being algebraic over $C(x)$. Let $\beta_1, \ldots, \beta_r$ be all conjugates of β over k and each conjugate β_ℓ can be expanded as a Puiseux series around z. We extend the valuation ν_z on k to a nonzero Puiseux series*

$$P = \sum_{i\geq 0} c_i(x - z)^{r_i},$$

defined as $\nu_z(P) = r_0$, where $c_i \in C$ with $c_0 \neq 0$ and $r_i \in \mathbb{Q}$ with $r_0 < r_1 < \cdots$. Any element $B \in K$ can be uniquely written as $B = f(\beta)$ with $f = f_0 + f_1y + \ldots + f_{r-1}y^{r-1} \in k[y]$. The value function $\mathrm{val}_z : K \to \mathbb{Q} \cup \{\infty\}$ is then defined by $\mathrm{val}_z(B) = \min_{\ell=1}^{r}\{\nu_z(f(\beta_\ell))\}$. In this setting, $O_{(K,\mathrm{val}_z)}$ is a free $C[x]$-module.

Example 7. *Let C be an algebraically closed field of characteristic 0 and consider a linear differential operator $L = \ell_0 + \cdots + \ell_rD^r \in C(x)[D]$ with $\ell_r \neq 0$. The quotient module $V = C(x)[D]/\langle L\rangle$ is a $C(x)$-vector space with $1, D, \ldots, D^{r-1}$ as a basis. Its element 1 is a solution of L. If $z \in C$ is a so-called regular singular point of L [13], then there are r linearly independent solutions in the C-vector space generated by*

$$C[[[x - z]]] := \bigcup_{\nu\in C}(x - z)^\nu C[[x - z]][\log(x - z)].$$

Following [14], we construct a value function val_z on V as follows. First choose a function $\iota\colon C/\mathbb{Z} \times \mathbb{N} \to C$ with $\iota(\nu + \mathbb{Z}, j) \in \nu + \mathbb{Z}$ for every $\nu \in C$ and $j \in \mathbb{N}$, with

$$\iota(\nu_1 + \mathbb{Z}, j_1) + \iota(\nu_2 + \mathbb{Z}, j_2) - \iota(\nu_1 + \nu_2 + \mathbb{Z}, j_1 + j_2) \geq 0$$

for every $\nu_1, \nu_2 \in C$ and $j_1, j_2 \in \mathbb{N}$, and with $\iota(\mathbb{Z}, 0) = 0$. This function picks from each $\mathbb{Z}$-equivalence class in C a canonical representative.

Using this auxiliary function, the valuation $\mathrm{val}_z(t)$ of a term $t := (x-z)^{\nu+i}\log(x-z)^j$ is the integer $\nu+i-\iota(\nu+i, j)$, and the valuation $\mathrm{val}_z(f)$ of a series $f \in C[[[x-z]]]$ is the minimum of the valuations of all the terms appearing in it (with nonzero coefficients). The valuation of 0 is defined as ∞.

The value function $\mathrm{val}_z(\cdot)\colon V \to \mathbb{Z} \cup \{\infty\}$ is then defined as the smallest valuation of a series $B \cdot f$, when f runs through all solutions of L. We now check that the function val_z is indeed a value function.

(i) *Let $B \in V$. Clearly if $B = 0$, $\mathrm{val}_\alpha(B) = \infty$ for all $\alpha \in C$. Conversely, assume that $\mathrm{val}_\alpha(B) = \infty$, then by definition $\mathrm{val}_\alpha(B \cdot f) = \infty$ and so $B \cdot f = 0$ for all $f \in \mathrm{Sol}_\alpha(L)$, which implies that the dimension of the solution space of B is at least r. But the order of B is less than r, and the dimension of the solution space of a nonzero operator cannot exceed its order, so it follows that $B = 0$.*
(ii) *For any $a \in C(x) \subseteq C[[[x-\alpha]]]$ and $f \in C[[[x-\alpha]]]$, the valuation of af is the sum of the valuations of a and f by definition. Then for any $B \in V$, $\mathrm{val}_\alpha(aB) = \min_{f\in\mathrm{Sol}_\alpha(L)}\{\mathrm{val}_\alpha(aB \cdot f)\}$, which is then equal to $\nu_\alpha(a) + \mathrm{val}_\alpha(B)$.*

(*iii*) *By* $\mathrm{val}_\alpha((B_1+B_2)\cdot f)) \geq \min\{\mathrm{val}_\alpha(B_1\cdot f), \mathrm{val}_\alpha(B_1\cdot f)\}$ *for all* $f \in \mathrm{Sol}_\alpha(L)$*, we have for any* $B_1, B_2 \in V$*,*

$$\mathrm{val}_\alpha(B_1+B_2) \geq \min\{\mathrm{val}_\alpha(B_1), \mathrm{val}_\alpha(B_2)\}.$$

When $\Gamma = \mathbb{Z}$, the valued field (k, ν) can be endowed with a topology. We summarize here the relevant constructions, more details can be found in [15, Chapter 2]. For $a \in k$, let $|a| = \mathrm{e}^{-\nu(a)}$. The properties of the valuation ensure that $|\cdot|$ is an absolute value, called the ν-adic absolute value. This absolute value defines a topology on k, in which elements are "small" if their valuation is "large".

Recall that a sequence of elements $(c_n) \in k^{\mathbb{N}}$ is said to be Cauchy if for each $\epsilon > 0$, there exists $N \in \mathbb{N}$ such that for every $m, n > N$, $|c_m - c_n| < \epsilon$, or, equivalently, if for each $M \in \mathbb{Z}$, there exists $N \in \mathbb{N}$ such that for every $m, n > N$, $\nu(c_m - c_n) > M$. The field k is said to be complete if every Cauchy sequence is convergent.

The completion of k is a minimal field extension k_ν which is complete. It can be constructed as follows. As a set, let k_ν be the set of all Cauchy sequences in k, modulo the equivalence relation $(c_n) \equiv (d_n) \Leftrightarrow (c_n - d_n)$ converges to 0 at infinity. The field k is contained in k_ν via the constant sequences. Ring operations on k extend to k_ν component-wise, and make k_ν a field. The valuation on k extends to k_ν by taking the limit of the valuations of the terms of the sequences, we use the same letter ν for that valuation.

An important feature of the topology on k and k_ν is that the ν-adic absolute value is ultrametric: it satisfies the stronger triangular condition $|a+b| \leq \max(|a|, |b|)$. In particular, any series $\sum_{n=0}^{\infty} a_n$ with $a_n \in k_\nu$ and $|a_n| \to 0$ is convergent in k_ν.

Example 8. *The completion of* $C(x)$ *w.r.t. the valuation* ν_z *is* $C((x-z))$*, and its completion w.r.t.* ν_∞ *is* $C((1/x))$*.*

These definitions extend naturally to a valued k-vector space. Just like in the case of fields, the hypotheses *(i)* and *(iii)* of Definition 2 ensure that we can define a norm on V by setting $||v|| = \mathrm{e}^{-\mathrm{val}(v)}$. This turns V into a topological vector space: addition and scalar multiplication are continuous.

Part *(ii)* of Definition 2 further ensures that $||cv|| = |c| \cdot ||v||$ for $c \in k$, $v \in V$. In particular, if a sequence $(a_n)_{n\in\mathbb{N}}$ in k converges to 0, then $(a_n v)_{n\in\mathbb{N}}$ converges to 0 in V.

More generally, if $B_1, \dots, B_r \in V$ and $(a_n^{(1)}), \dots, (a_n^{(r)})$ are sequences in k converging to $a_\infty^{(1)}, \dots, a_\infty^{(r)}$, respectively, then the sequence $(a_n^{(1)}B_1 + \cdots + a_n^{(r)}B_r)$ in V converges to $a_\infty^{(1)}B_1 + \cdots + a_\infty^{(r)}B_r$.

Let V_ν be the k_ν-vector space obtained from scalar extension of V. If V is finite dimensional and $B_1, \dots, B_r$ is a basis, V_ν can be seen as the k_ν-vector space generated by $B_1, \dots, B_r$, identifying its elements with elements of V whenever possible, and it is the completion of V with respect to the above topology.

Remark 9. *The inequality* $\dim_{k_\nu} V_\nu \leq \dim_k V$ *always holds, but it may happen that the inequality is strict. For example, consider* $C((x))$ *as a* $C(x)$*-vector space, with valuation* $\nu = \nu_0$*, and let* V *be a* r*-dimensional sub-vector space of* $C((x))$*. Then* $V_\nu = C((x))$ *has dimension* 1 *over* $C((x))$*.*

3 COMPUTING INTEGRAL BASES

In this section, we present a general algorithm for computing local and global integral bases of valued vector spaces and conditions on the termination of this algorithm.

3.1 The local case

Given a valued field (k, ν), a basis of a k-vector space V of dimension r, and a value function val on V, our goal is to compute a local integral basis of V if it exists. The algorithm described below is based on the algorithm given by van Hoeij [18] for computing integral bases of algebraic function fields. It also covers the adaption by Kauers and Koutschan to D-finite functions [14]. For simplicity, we restrict to the case $\Gamma = \mathbb{Z}$.

For the algorithm to apply in the general setting, we need to make the following assumptions.

(A) Arithmetic in k and V is constructive, and ν and val are computable.
(B) We know an element $x \in k$ with $\nu(x) = 1$.
(C) For any given $B_1, \dots, B_d \in V$, we can find $\alpha_1, \dots, \alpha_{d-1}$ in k such that
$$\mathrm{val}(\alpha_1 B_1 + \cdots + \alpha_{d-1}B_{d-1} + B_d) > 0$$
or prove that no such α_i's exist.
(D) The completion V_ν of V has dimension r.

Algorithm 10. *INPUT: a* k*-vector space basis* $B_1, \dots, B_r$ *of* V
OUTPUT: a local integral basis of V *w.r.t.* val

1 *for* $d = 1, \dots, r$*, do:*
2   *replace* B_d *by* $x^{-\mathrm{val}(B_d)}B_d$*.*
3   *while there exist* $\alpha_1, \dots, \alpha_{d-1} \in k$ *such that*
$$\mathrm{val}(\alpha_1 B_1 + \cdots + \alpha_{d-1}B_{d-1} + B_d) > 0,$$
4   *choose such* $\alpha_1, \dots, \alpha_{d-1}$*.*
5   *replace* B_d *by* $x^{-1}(\alpha_1 B_1 + \cdots + \alpha_{d-1}B_{d-1} + B_d)$*.*
6 *return* $B_1, \dots, B_r$*.*

Theorem 11. *Alg. 10 is correct.*

Proof. We show by induction on d that for every $d = 1, \dots, r$, the output elements $B_1, \dots, B_d$ form a local integral basis for the subspace of V generated by the input elements $B_1, \dots, B_d$. From the updates in lines 2 and 5, it is clear that the output elements generate the same subspace, so the only claim to be proven is that they are also module generators for the module of integral elements.

For $d = 1$, line 2 ensures that $\mathrm{val}(B_1) = 0$, and no further change is going to happen in the while loop. When $\mathrm{val}(B_1) = 0$, then the integral elements of the subspace generated by B_1 are precisely the elements uB_1 for $u \in k$ with $\nu(u) \geq 0$, so B_1 is an integral basis.

Now assume that d is such that $B_1, \dots, B_{d-1}$ is an integral basis, and let $B_d \in V$. After executing line 2, we may assume $\mathrm{val}(B_d) \geq 0$. After termination of the while loop, we know that there are no $\alpha_1, \dots, \alpha_{d-1} \in k$ such that $\mathrm{val}(\alpha_1 B_1 + \cdots + \alpha_{d-1}B_{d-1} + B_d) > 0$. Let $\alpha_1, \dots, \alpha_d \in k$ be such that $A = \alpha_1 B_1 + \cdots + \alpha_d B_d$ is an integral element. We have to show that $\nu(\alpha_i) \geq 0$ for $i = 1, \dots, d$.

We cannot have $\nu(\alpha_d) < 0$, otherwise, $\mathrm{val}(\alpha_d^{-1}A) > 0$, which would contradict the termination condition of the while loop. Thus $\nu(\alpha_d) \geq 0$. But then, $\mathrm{val}(\alpha_d B_d) \geq 0$, so $A - \alpha_d B_d$ is also integral. Since $A - \alpha_d B_d$ is in the k-subspace generated by $B_1, \dots, B_{d-1}$ and the latter is an integral basis by induction hypothesis, it follows that $\nu(\alpha_i) \geq 0$ for $i = 1, \dots, d-1$. ■

We prove that under the assumptions (A), (B), (C), the termination of Alg. 10 is equivalent to assumption (D). It is moreover equivalent to the the existence of a discriminant function, which is defined as follows and generalizes the corresponding notion for fields of algebraic numbers or functions. With such a function at hand, we can also bound the number of iterations of the main loop.

Definition 12. *Let* (V, val) *be a valued vector space of finite dimension* r *over a valued field* (k, v) *with the value group* $\mathbb{Z}$. *Let* $x \in k$ *be such that* $v(x) = 1$ *and* $\mathbb{B}_V$ *denote the set of all bases of* V. *A map* $\mathrm{Disc} : \mathbb{B}_V \to \mathbb{Z}$ *is called a* discriminant function *on* V *if for every basis* $B_1, \ldots, B_r$ *of* V, *we have*

(i) $\gamma := \mathrm{Disc}(\{B_1, \ldots, B_r\}) \geq 0$ *if all the* B_i*'s are integral in* V

(ii) for all $\alpha_1, \ldots, \alpha_{d-1} \in k$ *with* $d \leq r$,

$$\mathrm{Disc}(B_1, \ldots, B_{d-1}, \alpha_1 B_1 + \cdots + \alpha_{d-1} B_{d-1} + B_d, B_{d+1}, \ldots, B_r) = \gamma$$

(iii) $\mathrm{Disc}(B_1, \ldots, B_{d-1}, x^{-1} B_d, B_{d+1}, \ldots, B_r) < \gamma$.

Theorem 13. *Let* (V, val) *be a valued vector space of finite dimension* r *over a valued field* (k, v) *with the value group* $\mathbb{Z}$. *Then the following four statements are equivalent under the hypotheses* (A), (B), (C)*:*

(a) *There is a local integral basis of* V *w.r.t.* val.
(b) *There is a discriminant function* $\mathrm{Disc} : \mathbb{B}_V \to \mathbb{Z}$.
(c) *Alg. 10 terminates.*
(d) *The topological assumption* (D) *on* V *is satisfied.*

Proof. $(c) \Rightarrow (a)$ follows from Theorem 11.

$(a) \Rightarrow (b)$: Given a local integral basis $\{C_1, \ldots, C_r\}$ and a basis $B = \{B_1, \ldots, B_r\}$ of V with $B_i = \sum_{j=1}^r b_{i,j} C_j$ for some $b_{i,j} \in k$, the discriminant function can be defined as

$$\mathrm{Disc}(B) := v(\det((b_{i,j})_{i,j=1}^r)).$$

$(b) \Rightarrow (c)$: By assumption (B), there exists $x \in k$ such that $v(x) = 1$. Let $\{B_1, \ldots, B_r\}$ be any basis of V over k. We may always assume that $\mathrm{val}(B_i) = 0$ by replacing B_i by $x^{-\mathrm{val}(B_i)} B_i$ for all i. It suffices to show that Alg. 10 terminates on $\{B_1, \ldots, B_r\}$. Let $\gamma = \mathrm{Disc}(\{B_1, \ldots, B_r\}) \in \mathbb{N}$. At any intermediate step of Alg. 10, $B_1, \ldots, B_r$ are always integral and form a basis of V. If α_i's exist in the while loop, γ decreases strictly. So there can be at most γ basis updates, which implies that Alg. 10 terminates.

$(d) \Rightarrow (c)$: Assume that for some $d \in \{1, \ldots, r\}$, the inner loop does not terminate. Let $B_{d,i}$ be the value of B_d before entering the ith iteration, and let $\tilde{B}_{d,i} = x^i B_{d,i}$. The operation for computing $B_{d,i}$ from $B_{d,i-1}$ (step 5) ensures that for all i, $\mathrm{val}(B_{d,i}) \geq 0$ and $\mathrm{val}(\tilde{B}_{d,i}) \geq i$. For all $i \in \mathbb{N}$, there exists $a_{j,i} \in k$ for $j \in \{0, \ldots, d-1\}$ such that

$$\tilde{B}_{d,i} = x^i \cdot \frac{1}{x}\left(B_{d,i-1} + \sum_{j=0}^{d-1} a_{j,i} B_j\right) = \tilde{B}_{d,i-1} + x^{i-1} \sum_{j=0}^{d-1} a_{j,i} B_j$$

and $B_{d,i}$ has valuation 0. We can unroll the sum as

$$\tilde{B}_{d,i} = B_{d,0} + \sum_{j=0}^{d-1}\left(\sum_{\ell=0}^{i-1} x^\ell a_{j,\ell}\right) B_j.$$

Viewing this equality in V_v and taking the limit as $i \to \infty$ yields

$$\tilde{B}_{d,\infty} := \lim_{i\to\infty} \tilde{B}_{d,i} = B_{d,0} + \sum_{j=0}^{d-1}\left(\sum_{\ell=0}^{\infty} x^\ell a_{j,\ell}\right) B_j.$$

Furthermore, $\tilde{B}_{d,\infty}$ has valuation ∞, so it is zero and

$$B_{d,0} = -\sum_{j=0}^{d-1}\left(\sum_{\ell=0}^{\infty} x^\ell a_{j,\ell}\right) B_j \quad \text{in } V_v.$$

But by hypothesis (D), V_v has dimension r, so $B_1, \ldots, B_r$ must be linearly independent over k_v too, a contradiction. So the loop terminates.

$(c) \Rightarrow (d)$: Let $B_1, \ldots, B_r$ be the output of Alg. 10. If the dimension falls, then there exist some $a_i \in k_v$ and $d \leq r$ such that $B_d = \sum_{i=1}^{d-1} a_i B_i$. For each i, let $a_{i,j}$ be a sequence in k converging to a_i. Let $\tilde{B}_{d,j} = B_d - \sum_{i=1}^{d-1} a_{i,j} B_i$. By assumption, $\tilde{B}_{d,j}$ goes to 0 when j goes to infinity, so its valuation goes to infinity. We can assume $\mathrm{val}(\tilde{B}_{d,j}) \geq j$. Then $B_{d,j} := x^{-j} \tilde{B}_{d,j}$ is an infinite sequence such that Alg. 10 does not terminate, a contradiction. ∎

3.2 The global case

In a next step, we seek integral bases with respect to several valuations simultaneously. Instead of a single valuation $\mathrm{val}\colon V \to \mathbb{Z} \cup \{\infty\}$, we have a set of valuations $v_z\colon k \to \mathbb{Z} \cup \{\infty\}$ $(z \in Z)$ and a set of value functions $\mathrm{val}_z\colon V \to \mathbb{Z} \cup \{\infty\}$ $(z \in Z)$ and want to find a vector space basis $B_1, \ldots, B_r$ of V that is also an $O_{(k, v_z)}$-module basis of $O_{(V, \mathrm{val}_z)}$ for every $z \in Z$. The idea is to apply Alg. 10 repeatedly. In order to make this work, we impose the following additional assumptions:

(B′) For every $z \in Z$ we know an element $x_z \in k$ with $v_z(x_z) = 1$ and $v_\zeta(x_z) = 0$ for all $\zeta \in Z \setminus \{z\}$.
(C′) For every $z \in Z$ and any given $B_1, \ldots, B_d \in V$, we can compute $\alpha_1, \ldots, \alpha_{d-1} \in k$ with $v_\zeta(\alpha_i) \geq 0$ for all i and all $\zeta \in Z \setminus \{z\}$ such that
$$\mathrm{val}_z(\alpha_1 B_1 + \cdots + \alpha_{d-1} B_{d-1} + B_d) > 0,$$
or prove that no such α_i's exist.
(D′) For every $z \in Z$, the completion V_{v_z} of V has dimension r.
(E) We know a finite set $Z_0 \subseteq Z$ and a basis $B_1, \ldots, B_r$ of V that is an integral basis for all $z \in Z \setminus Z_0$.

Under these circumstances, we can proceed as follows.

Algorithm 14. *INPUT: a* k*-vector space basis* $B_1, \ldots, B_r$ *of* V *which is an integral basis for all* $z \in Z \setminus Z_0$
OUTPUT: an integral basis for all $z \in Z$
1 *for all* $z \in Z_0$, *do:*
2 *apply Alg. 10 to* $B_1, \ldots, B_r$, *using* v_z, val_z *and* x_z *in place of* v, val, *and* x, *and ensuring in step 3 that* $v_\zeta(\alpha_i) \geq 0$ *for all* i *and all* $\zeta \in Z$.
3 *replace* $B_1, \ldots, B_r$ *by the output of Alg. 10.*
4 *return* $B_1, \ldots, B_r$.

Theorem 15. *Alg. 14 is correct.*

Proof. We only have to show that one application of Alg. 10 does not destroy the integrality properties arranged in earlier calls. To see that this is the case, consider the effects of steps 2 and 5 with respect to a value function other than val_z. If val_ζ is such a function, then by (B′), we have $v_\zeta(x_z) = 0$, so $B_1, \ldots, B_{d-1}, B_d$ and $B_1, \ldots, B_{d-1}, x_z^e B_d$ generate the same $O_{(k, v_\zeta)}$-module, for any $e \in \mathbb{Z}$. Hence this step is safe. Likewise, by the choice of the α_i

in step 5, $\{B_1, \dots, B_{d-1}, B_d\}$ and $\{B_1, \dots, B_{d-1}, B_d + \sum_{i=1}^{d-1} \alpha_i B_i\}$ generate the same $O_{(k,\nu_\zeta)}$-module. So this step is safe too. ∎

3.3 Avoiding constant field extensions

We shall discuss one more refinement, which also appears already in earlier versions of the algorithm [11, 14, 18]. In applications, we typically have $k = \bar{C}(x)$ where C is a field and $\bar{C}$ is an algebraic closure of C, with the usual valuation ν_z for $z \in \bar{C}$ (see Example 1). For this valuation, $x_z = x - z$ is a canonical choice.

For theoretical purposes it is advantageous to work with vector spaces over k, but computationally it would be preferable to work with coefficients in $C(x)$ rather than $\bar{C}(x)$. It is therefore desirable to ensure that the basis elements returned by Alg. 14 have coefficients in $C(x)$ with respect to the input basis.

Note that in this setting, we have the following properties:

Lemma 16. (1) *For every automorphism $\sigma\colon \bar{C} \to \bar{C}$ leaving C fixed, for every $z \in Z$, and for every $u \in \bar{C}(x)$, we have $\nu_z(u) = \nu_{\sigma(z)}(\sigma(u))$, where $\sigma(u)$ is the element of $\bar{C}(x)$ obtained by applying σ to the coefficients of u.*

(2) *For every $u \in \bar{C}(x) \setminus \{0\}$, and for every $z \in Z$, u admits a unique Laurent series expansion*

$$u = c_z(x-z)^{\nu_z(u)} + (x-z)^{\nu_z(u)+1} r$$

with $c_z \in \bar{C} \setminus \{0\}$ and $\nu_z(r) \geq 0$.

The constant c_z in item 2 is called the *leading coefficient* of u.

The second property of the lemma ensures that the coefficients $\alpha_1, \dots, \alpha_{d-1} \in \bar{C}(x)$ from (C) and (C′) can be chosen in $\bar{C}$. Indeed, we can replace α_i by its leading coefficient if $\nu_z(\alpha_i) = 0$ and by zero otherwise, because whenever $\alpha_1, \dots, \alpha_{d-1} \in \bar{C}(x)$ is a solution and $\beta_1, \dots, \beta_{d-1} \in \bar{C}(x)$ are arbitrary with $\nu_z(\beta_i) \geq 1$ for all i, then also $\alpha_1 + \beta_1, \dots, \alpha_{d-1} + \beta_{d-1}$ is a solution.

If we restrict $\alpha_1, \dots, \alpha_{d-1}$ to $\bar{C}$, then there can be at most one solution whenever we seek a solution in step 3 of Alg. 10, because the difference of any two distinct solutions would be a nontrivial $\bar{C}$-linear combination of $B_1, \dots, B_{d-1}$, and by the invariant of the outer loop, $B_1, \dots, B_{d-1}$ already form an integral basis of the k-subspace they generate.

We shall adopt the following last assumption, stating that we can apply σ on V:

(F) We know a basis $B_1, \dots, B_r$ as in (E) such that for every automorphism $\sigma\colon \bar{C} \to \bar{C}$ fixing C, and for all $\alpha_1, \dots, \alpha_r \in k$, we have $\mathrm{val}_z(\alpha_1 B_1 + \dots + \alpha_r B_r) = \mathrm{val}_{\sigma(z)}(\sigma(\alpha_1)B_1 + \dots + \sigma(\alpha_r)B_r)$.

Using this assumption, it can further be shown that the unique elements $\alpha_1, \dots, \alpha_{d-1} \in \bar{C}$ from (C′) must in fact belong to $C(z)$ (if they exist at all). This is because if some α_i were in $\bar{C} \setminus C(z)$, then there would be some automorphism $\sigma\colon \bar{C} \to \bar{C}$ fixing $C(z)$ but moving α_i, and (F) would imply that $\sigma(\alpha_1), \dots, \sigma(\alpha_d)$ would be another solution to (C′), in contradiction to the uniqueness.

In order to ensure that the output elements of Alg. 14 are $C(x)$-linear combinations of the input elements, we adjust Alg. 10 as follows. Let G be the Galois group of $C(z)$ over C. In step 2, instead of replacing B_d by $x_z^{-\mathrm{val}_z(B_d)}$, we replace B_d by

$$\Big(\prod_{\sigma \in G} \sigma(x_z)^{-\mathrm{val}_z(B_d)}\Big) B_d.$$

Note that $\prod_{\sigma\in G} \sigma(x_z) = \prod_{\sigma \in G} \sigma(x-z)$ is the minimal polynomial of z in $C[x]$.

In step 5 of Alg. 10, we choose $\alpha_1, \dots, \alpha_{d-1} \in C(z)$ (if there are any), and instead of replacing B_d by $x_z^{-1}(\alpha_1 B_1 + \dots + \alpha_{d-1}B_{d-1} + \alpha_d B_d)$ (with $\alpha_d = 1$), we replace B_d by

$$A := \sum_{i=1}^{d}\Big(\sum_{\sigma \in G} \sigma\left(\frac{\alpha_i}{x_z}\right)\Big) B_i.$$

Proposition 17. *When the steps 2 and 5 of Alg. 10 are adjusted as indicated, Alg. 14 returns an integral basis of V whose elements are $C(x)$-linear combinations of the input elements.*

Proof. By Galois theory, $\prod_{\sigma\in G} \sigma(x_z) = \prod_{\sigma\in G} \sigma(x-z) \in C(x)$ and $\tilde{\alpha}_i := \sum_{\sigma \in G} \sigma(\alpha_i/(x-z)) \in C(x)$ for every i. Therefore, all updates in the modified Alg. 10 replace certain basis elements by $C(x)$-linear combinations of basis elements.

It remains to show that the output is an integral basis for all $z \in Z$. To see this, we have to check the effect of Alg. 10 concerning val_z and concerning val_ζ for $\zeta \in Z \setminus \{z\}$. For the latter, we distinguish the case when ζ is conjugate to z and when it is not.

By part 1 of Lemma 16, for all $\zeta \in Z$ that are not conjugate to z we have $\nu_\zeta(\tilde{\alpha}_i) \geq 0$ for $i = 1, \dots, d-1$ and $\nu_\zeta(\tilde{\alpha}_d) = 0$. Therefore, $B_1, \dots, B_{d-1}$ and A generate the same $O_{(k,\nu_\zeta)}$-module as $B_1, \dots, B_{d-1}$ and B_d, for every $\zeta \in Z$ that is not conjugate to z. This settles the case when ζ is not conjugate to z.

Next, observe that $\mathrm{val}_z(x_z^{-1}(\alpha_1 B_1 + \dots + \alpha_d B_d)) \geq 0$ by the assumptions on $x_z, \alpha_1, \dots, \alpha_d$. Moreover, by part 1 of Lemma 16, $\nu_z(\sigma(x-z)) = \nu_{\sigma^{-1}(z)}(x-z) = 0$ for every $\sigma \in G \setminus \{\mathrm{id}\}$, and $\nu_z(\sigma(\alpha_i)) = \nu_{\sigma^{-1}(z)}(\alpha_i) \geq 0$ because $\nu_\zeta(\alpha_i) \geq 0$ for all ζ. Therefore $\mathrm{val}_z(\sigma(x_z^{-1})(\sigma(\alpha_1)B_1 + \dots + \sigma(\alpha_d)B_d) \geq 0$ for every $\sigma \in G \setminus \{\mathrm{id}\}$. It follows that

$$\mathrm{val}_z(A) \geq \max_{\sigma \in G} \mathrm{val}_z\Big(\sum_{i=1}^{d} \sigma\left(\frac{\alpha_i}{x-z}\right) B_i\Big) \geq 0.$$

Moreover, since $\alpha_d = 1$ and $\mathrm{val}_{\sigma(z)}(x_z) = 0$ for all $\sigma \neq \mathrm{id}$, we have that $B_1, \dots, B_{d-1}$ and A generate the same $O_{(k,\nu_z)}$-module as $B_1, \dots, B_{d-1}$ and $x_z^{-1}(\alpha_1 B_1 + \dots + \alpha_d B_d)$. This settles the concern about val_z.

Finally, if ζ is conjugate to z, say $\zeta = \sigma(z)$ for some automorphism $\sigma \in G$, then $\mathrm{val}_\zeta(A) = \mathrm{val}_\zeta(\sigma(A)) = \mathrm{val}_z(A) \geq 0$ by assumption (F), because A is a $C(x)$-linear combination of the original basis elements. So A belongs to the $O_{(k,\nu_\zeta)}$-module of all integral elements (w.r.t. val_ζ) of the subspace generated by $B_1, \dots, B_d$ in V, so we are not making the module larger than we should. Conversely, the old B_d belongs to the $O_{(k,\nu_\zeta)}$-module generated by $B_1, \dots, B_{d-1}$ and A, so by updating B_d to A, the module generated by $B_1, \dots, B_d$ does not become smaller. ∎

Informally, what happens by taking the sums over the Galois group is that the algorithm working locally at z simultaneously works at all its conjugates. If for a certain z, the set Z_0 contains z as well as its conjugates, it is fair (and advisable) to discard all the conjugates from Z_0 and only keep z. More precisely, the whole process requires only knowing the minimal polynomial of z in $C[x]$, so for applications where the set Z_0 is computed as the set of roots of some polynomial $p \in C[x]$, the algorithms can proceed with the factors of p instead of all its roots.

4 THE ALGEBRAIC AND D-FINITE CASES

We will see below how the algorithms in [14, 18] for computing integral bases are special cases of the general formulation in Section 3. Let C be a computable subfield of $\mathbb{C}$ and $k = \bar{C}(x)$ with a valuation ν_z for $z \in \bar{C}$. The value function val_z on $V = k(\beta)$ with $\beta \in \overline{C(x)}$ is defined in Example 6 and on $V = \bar{C}(x)[D]/\langle L\rangle$ with $L \in C[x][D]$ and all local exponents ν of solutions contained in C is defined in Example 7. We show that the assumptions imposed on value functions in Section 3 are fulfilled in the algebraic and D-finite settings. Note that (B), (C), (D) are subsumed in (B′), (C′), (D′), respectively.

(A) It is assumed that C is a computable field, so it is clear that arithmetic in $\bar{C}(x)$ and V are computable, and that ν_z on $\bar{C}(x)$ is also computable. The value functions val_z for algebraic and D-finite functions are computable since we can determine first few terms of Puiseux or generalized series solutions by algorithms in [8, 13].

(B′) For every $z \in Z$, we can take $x_z = x - z$ such that $\nu_z(x_z) = 1$ and $\nu_\zeta(x_z) = 0$ for all $\zeta \in Z \setminus \{z\}$.

(C′) Done in [14, Section 4].

(D′) Clear.

(E) In the algebraic case, we can choose as Z_0 the set of singularities of $\beta \in \overline{C(x)}$ which is clearly a finite set. In the D-finite case, we can choose as Z_0 the set of zeros of ℓ_r which are the only possible singularities by [14, Lemma 9].

(F) If α and $\bar{\alpha}$ are conjugates, let σ be an element of the Galois group of $\bar{C}/C$ such that $\bar{\alpha} = \sigma(\alpha)$. In particular $\sigma(L) = L$ and $\sigma(B) = B$. For all $i \in \{1, \ldots, r\}$, $\sigma(f_{\alpha,i}) \in \bar{C}[[[x - \bar{\alpha}]]]$ is a solution of $\sigma(L) = L$. Since σ is an automorphism, the $\sigma(f_{\alpha,i})$ form a fundamental system of L in $\bar{C}[[[x - \bar{\alpha}]]]$. For all $i \in \{1, \ldots, r\}$, $B\cdot\sigma(f_{\alpha,i}) = \sigma(B)\cdot\sigma(f_{\alpha,i}) = \sigma(B\cdot f_{\alpha,i})$, and the equality of the valuations follows. In the algebraic case, this equality follows from the property of Duval's rational Puiseux series (see the remarks on [8, page 120]).

The termination of the general algorithm 10 in the algebraic and D-finite cases have been shown in [14, 18] by using classical discriminants and generalized Wronskians. The discriminant functions in these cases can be taken as the compositions of the valuation ν_z and these functions. More precisely, for a basis $B_1, \ldots, B_r$ of $V = k(\beta)$, the discriminant function Disc in the algebraic setting is defined as

$$\mathrm{Disc}(\{B_1, \ldots, B_r\}) = \nu_z(\det(\mathrm{Tr}(B_i B_j))),$$

where Tr is the trace map from V to $\bar{C}(x)$. If $B_1, \ldots, B_r$ are integral, $\det(\mathrm{Tr}(B_i B_j)) \in \bar{C}[x]$ and then $\mathrm{Disc}(\{B_1, \ldots, B_r\}) \in \mathbb{N}$. Let $\alpha_1, \ldots, \alpha_{d-1} \in k$, replacing B_d by $\alpha_1 B_1 + \cdots + \alpha_{d-1} B_{d-1} + B_d$ is equivalent to multiplying the matrix $(\mathrm{Tr}(B_i B_j))$ left and right by elementary transformation matrices with determinant 1, so the determinant (and its valuation) are constant. Similarly, replacing B_d by $(x - z)^{-1} B_d$ is equivalent to multiplying the matrix $(\mathrm{Tr}(B_i B_j))$ left and right by a matrix with determinant $(x - z)^{-1}$, so the discriminant decreases by 2. So Disc is indeed a discriminant function on $k(\beta)$.

In the case of D-finite functions, for any basis $B = \{B_1, \ldots, B_r\}$ of $V = \bar{C}(x)[D]/\langle L\rangle$ and fundamental series solutions $b_1, \ldots, b_r \in \bar{C}[[[x - z]]]$ of L , the generalized Wronskian is defined as

$$\mathrm{wr}_{L,z}(B) := \det(((B_i \cdot b_j))_{i,j=1}^r) \in \bar{C}[[[x - z]]].$$

The discriminant function Disc can be defined as the valuation of $\mathrm{wr}_{L,z}(B)$ at z. By the proof of Theorem 18 in [14], Disc is indeed a discriminant function on $\bar{C}(x)[D]/\langle L\rangle$.

5 THE P-RECURSIVE CASE

5.1 Solution Spaces

For the case of recurrence operators, we use a setting that has already been used for instance in [1, 7, 19] in the context of finding hypergeometric solutions. The relevant parts of the construction are summarized in this section. We consider the Ore algebra $C(x)[S]$ with the commutation rule $Sx = (x + 1)S$. We fix an operator $L = \ell_0 + \ell_1 S + \cdots + \ell_r S^r \in C(x)[S]$ with $\ell_0, \ell_r \neq 0$, and we consider the vector space $V = \bar{C}(x)[S]/\langle L\rangle$, where $\langle L\rangle = \bar{C}(x)[S]L$. The operator L acts on a sequence $f\colon \alpha + \mathbb{Z} \to \bar{C}$ through $(L \cdot f)(z) := \ell_0(z)f(z) + \cdots + \ell_r(z)f(z + r)$ for all $z \in \alpha + \mathbb{Z}$. This action turns $\bar{C}^{\alpha+\mathbb{Z}}$ into a (left) $C[x][S]$-module, but not to a (left) $C(x)[S]$-module, because a sequence $f\colon \alpha + \mathbb{Z} \to \bar{C}$ cannot meaningfully be divided by a polynomial which has a root in $\alpha + \mathbb{Z}$. In order to obtain a $C(x)[S]$-module, consider the space $\bar{C}((q))^{\alpha+\mathbb{Z}}$ of all sequences $f\colon \alpha + \mathbb{Z} \to \bar{C}((q))$ whose terms are Laurent series in a new indeterminate q, and define the action of $L = \ell_0 + \cdots + \ell_r S^r \in C(x)[S]$ on a sequence $f\colon \alpha + \mathbb{Z} \to \bar{C}((q))$ through $(L \cdot f)(z) := \ell_0(z + q)f(z) + \cdots + \ell_r(z + q)f(z + r)$ for all $z \in \alpha + \mathbb{Z}$. Note that no $\ell_i \in C(x)$ can have a pole at $z + q$ for any $z \in \alpha + \mathbb{Z}$ when $\alpha \in \bar{C}$ and $q \notin \bar{C}$.

For a fixed operator $L = \ell_0 + \cdots + \ell_r S^r \in C[x][S]$ with $\ell_0, \ell_r \neq 0$, the set $\mathrm{Sol}(L) := \{\, f\colon \alpha + \mathbb{Z} \to \bar{C}((q)) : L \cdot f = 0 \,\}$ is a $\bar{C}((q))$-vector space of dimension r. Indeed, a basis $b_1, \ldots, b_r$ is given by specifying the initial values $b_i(\alpha + j) = \delta_{i,j}$ for $i, j = 1, \ldots, r$ and observing that the operator L uniquely extends any choice of initial values indefinitely to the left as well as to the right. The reason is again that $q \notin \bar{C}$ implies $\ell_0(z + q), \ell_r(z + q) \neq 0$ for every $z \in \alpha + \mathbb{Z}$, so there is no danger that computing a certain sequence term $b_i(z)$ from $b_i(z + 1), \ldots, b_i(z + r)$ or from $b_i(z - 1), \ldots, b_i(z - r)$ could produce a division by zero. Instead of a division by zero, we can only observe a division by q.

The valuation $\nu_q(a)$ of a nonzero Laurent series $a \in \bar{C}((q))$ is the smallest $n \in \mathbb{Z}$ such that the coefficient $[q^n]a$ of q^n in a is nonzero. We further define $\nu_q(0) = +\infty$. For a nonzero solution $f\colon \alpha + \mathbb{Z} \to \bar{C}((q))$ of an operator $L \in C[x][S]$, we will be interested in how the valuation changes as z ranges through $\alpha + \mathbb{Z}$. As we have noticed, there can be occasional divisions by q as we extend f towards the left or the right, so $\nu_q(f(z))$ can go up and down as z moves through $\alpha + \mathbb{Z}$. In fact, it can go up and down arbitrarily often, as the solution $f\colon \mathbb{Z} \to \bar{C}((q))$, $f(z) = 1 + q + (-1)^z$ of the operator $L = S^2 - 1$ shows. However, only when z is a root of ℓ_0 we can have

$$\nu_q(f(z)) < \min\{\nu_q(f(z + 1)), \ldots, \nu_q(f(z + r))\},$$

and only when z is a root of $\ell_r(x - r)$ we can have

$$\nu_q(f(z)) < \min\{\nu_q(f(z - 1)), \ldots, \nu_q(f(z - r))\}.$$

Since the nonzero polynomials ℓ_0, ℓ_r have at most finitely many roots in $\alpha + \mathbb{Z}$, we can conclude that both

$$\liminf_{n\to-\infty} \nu_q(f(\alpha + n)) \quad \text{and} \quad \liminf_{n\to+\infty} \nu_q(f(\alpha + n))$$

are well-defined for every solution $f\colon \alpha+\mathbb{Z}\to\bar{C}((q))$ of L. Their difference

$$\operatorname{vg} f := \liminf_{n\to+\infty} \nu_q(f(\alpha+n)) - \liminf_{n\to-\infty} \nu_q(f(\alpha+n))$$

is called the *valuation growth* of f.

5.2 A Valuation Function

In our context, solutions with negative valuation growth are troublesome, because we want to define the valuation of a residue class $B\in\bar{C}(x)[S]/\langle L\rangle$ at z in terms of the valuations of the sequence terms $(B\cdot b)(z)\in\bar{C}((q))$, where b runs through $\operatorname{Sol}(L)$. When $b\in\operatorname{Sol}(L)$ has negative valuation growth, then we can have $\nu_q((B\cdot b)(z))<0$ for infinitely many z, which makes it hard to meet assumption (E). Moreover, if all solutions have positive valuation growth, we have $\nu_q((B\cdot b)(z))>0$ for infinitely many z, which is also in conflict with assumption (E). In order to circumvent this problem, we let $Z\subseteq\bar{C}$ be such that for each orbit $\alpha+\mathbb{Z}$ with $Z\cap(\alpha+\mathbb{Z})\neq\emptyset$ and for which L has a solution in $\bar{C}((q))^{\alpha+\mathbb{Z}}$ with nonzero valuation growth, the set $Z\cap(\alpha+\mathbb{Z})$ has a (computable) right-most element. We then define the value function $\operatorname{val}_z\colon V\to\mathbb{Z}\cup\{\infty\}$ by

$$\operatorname{val}_z(B) := \min_{b\in\operatorname{Sol}(L)}\Big(\nu_q((B\cdot b)(z)) - \liminf_{n\to\infty}\nu_q(b(z-n))\Big).$$

We use the convention $\infty-\infty=\infty$.

Proposition 18. *val_z is a value function for every $z\in Z$.*

Proof. We check the conditions of Def. 2.

(*i*) If $B=0$, then $B\cdot b$ is the zero sequence for every $b\in\operatorname{Sol}(L)$, so $\nu_q((B\cdot b)(z))=\infty$ for all $n\in\mathbb{Z}$.
Conversely, let $B\in\bar{C}(x)[S]$ be such that $\operatorname{val}_z([B])=\infty$. We may assume that the order of B is less than r, so that $[B]=0$ is equivalent to $B=0$. By $\operatorname{val}_z([B])=\infty$ we have $\nu_q((B\cdot b)(z))=\infty$ for all $b\in\operatorname{Sol}(L)$, i.e., $(B\cdot b)(z)=0$ for all $b\in\operatorname{Sol}(L)$.
If $b_1,\dots,b_r$ is a basis of $\operatorname{Sol}(L)$, then the matrix
$$M=((b_j(z+i-1)))_{i,j=1}^r\in\bar{C}((q))^{r\times r}$$
is regular. Now if B were nonzero and β_kS^k is a nonzero term appearing in B, then multiplying the kth row of M by β_k and adding suitable multiples of other rows to the kth row, we obtain a matrix whose kth row is 0, because $(B\cdot b_1)(z)=\dots=(B\cdot b_r)(z)=0$. On the other hand, the determinant of this matrix is equal to $\beta_k\det(M)\neq0$, so B cannot be nonzero.

(*ii*) Clear by $\nu_q((uf)(z))=\nu_q(u)+\nu_q(f(z))$ for all $u\in\bar{C}((q))$ and $f\in\bar{C}((q))^{z+\mathbb{Z}}$.

(*iii*) Clear by $\nu_q(((B_1+B_2)\cdot u)(z))=\nu_q((B_1\cdot u)(z)+(B_2\cdot u)(z))\geq\min(\nu_q((B_1\cdot u)(z)),\nu_q((B_2\cdot u)(z)))$ for all $u\in\bar{C}((q))^{z+\mathbb{Z}}$. ■

Next, we show that we can meet the computability assumptions of Section 3. Note again that (B), (C), (D) are subsumed in (B′), (C′), (D′), respectively.

(A) It is assumed that C is a computable field, so it is clear that arithmetic in $\bar{C}(x)$ and V are computable, and that ν_z is computable. We show that val_z is computable as well.
Let $\zeta\in z+\mathbb{Z}$ be such that all roots of $\ell_0\ell_r$ contained in $z+\mathbb{Z}$ are to the right of ζ, and consider the basis $b_1,\dots,b_r$ of $\operatorname{Sol}(L)$ in $\bar{C}((q))^{z+\mathbb{Z}}$ defined by the initial values $b_j(\zeta+i-1)=\delta_{i,j}$ $(i,j=1,\dots,r)$. We shall prove that for all $\eta\in z+\mathbb{Z}$,
$$\operatorname{val}_\eta(B)=\min_{j=1}^r\nu_q((B\cdot b_j)(\eta)).$$
Since we can compute $(B\cdot b_j)(\eta)$ for any $j=1,\dots,r$ and $\eta\in z+\mathbb{Z}$, this implies that val_η is computable. In particular, val_z is then computable.
We have $\min_{i=1}^r\nu_q(b_j(\zeta+i-1))=0$ for $j=1,\dots,r$ by construction, and in fact $\liminf_{n\to+\infty}\nu_q(b_j(\zeta-n))=0$ for $j=1,\dots,r$, because at no position $\zeta-n$ the valuation can be smaller than the minimum valuation of its r neighbors to the right or than the minimum valuation of its r neighbors to the left, due to the lack of roots of $\ell_0\ell_r$ in the range under consideration.
Let now $b=c_1b_1+\dots+c_rb_r$ for coefficients $c_1,\dots,c_r\in\bar{C}((q))$. Let $v:=\min_{j=1}^r\nu_q(c_j)$. Assume that $v=0$, and let j_0 be such that $\nu_q(c_{j_0})=0$. Then for all $\eta\in z+\mathbb{Z}$,
$$\nu_q(b(\eta))\geq\min_{j=1}^r\nu_q(b_j(\eta))$$
and $\nu_q((B\cdot b)(\eta))\geq\min_{j=1}^r\nu_q((B\cdot b_j)(\eta))$.
Furthermore, by construction of the basis of b_j's, for all $i\in\{1,\dots,r\}$, $b(\zeta+i-1)=c_i$, so $\min_{i=1}^r\nu_q(b(\zeta+i-1))=0$. Again, for lack of roots of $\ell_0\ell_r$ left of ζ, it implies that
$$\liminf_{n\to+\infty}\nu_q(b(\zeta-n))=0.$$
It follows from the above that
$$\nu_q((B\cdot b)(\eta))-\liminf_{n\to+\infty}\nu_q(b(\eta-n))\geq\min_{j=1}^r\nu_q((B\cdot b_j)(\eta)).$$
Assume now that $v\neq0$. In that case, consider $q^{-v}b=q^{-v}c_1b_1+\dots+q^{-v}c_rb_r$, with $\min_{j=1}^r\nu_q(q^{-v}c_j)=0$. From the above,
$$\begin{aligned}&\nu_q((B\cdot q^{-v}b)(\eta))-\liminf_{n\to+\infty}\nu_q(q^{-v}b(\eta-n))\\&\geq\min_{j=1}^r\nu_q((B\cdot b_j)(\eta)).\end{aligned}$$
Since for all $\eta\in z+\mathbb{Z}$ we have $\nu_q(q^{-v}b(\eta))=\nu_q(b(\eta))-v$ and
$\nu_q((B\cdot q^{-v}b)(\eta))=\nu_q((q^{-v}B\cdot b)(\eta))=\nu_q((B\cdot b)(\eta))-v$, it still holds that
$$\nu_q((B\cdot b)(\eta))-\liminf_{n\to+\infty}\nu_q(b(\eta-n))\geq\min_{j=1}^r\nu_q((B\cdot b_j)(\eta)),$$
so that indeed $\operatorname{val}_\eta(B)=\min_{j=1}^r\nu_q((B\cdot b_j)(\eta))$.

(B′) We can take $x_z=x-z$.

(C′) Let $B_1,\dots,B_d\in\bar{C}(x)[S]/\langle L\rangle$ be given. We can then compute $v:=\min_{i=1}^d\operatorname{val}_z(B_i)$ and we can find the required $\alpha_1,\dots,\alpha_{d-1}\in\bar{C}$ by equating the coefficients of q^n for $n\leq v$ in the linear combination $\alpha_1(B_1\cdot b_j)(z)+\dots+\alpha_{d-1}(B_{d-1}\cdot b_j)(z)+(B_d\cdot b_j)(z)$ to zero and solving the resulting inhomogeneous linear system for $\alpha_1,\dots,\alpha_{d-1}$.

(D′) Clear.

(E) First we shall prove that if $\alpha+\mathbb{Z}$ does not contain a root of $\ell_0\ell_r$, then $\mathcal{B}=\{1,S,\dots,S^{r-1}\}$ is an integral basis for all $z\in Z\cap\alpha+\mathbb{Z}$. For such z, consider the basis $b_1,\dots,b_r$ of

$\mathrm{Sol}(L) \subseteq \bar{C}((q))^{\alpha+\mathbb{Z}}$ with $b_j(z+i-1) = \delta_{i,j}$ $(i, j = 1, \ldots, r)$. By the discussion of (A), for any operator $A \in V$, we have

$$\mathrm{val}_z(A) = \min_{j=1}^{r} \nu_q((A \cdot b_j)(z)).$$

Let $A = p_0 + \cdots + p_{r-1}S^{r-1}$ be an operator in $V = \bar{C}(x)[S]/\langle L\rangle$. By the construction of the basis b_j's, for all $j = \{1, \ldots, r\}$, $(A \cdot b_j)(z) = p_{j-1}(x + q - z)$. It imples that

$$\min_{j=1}^{r} \nu_q((A \cdot b_j)(z)) = \min_{j=0}^{r-1} \nu_z(p_j).$$

So A is integral if and only if $\nu_z(p_j) \geq 0$ for all j and $\mathcal{B}$ is an integral basis at z. Since $\ell_0\ell_r$ can only have at finitely many roots, we can restrict Z_0 to finitely many orbits $\alpha + \mathbb{Z}$. In each of these orbits, there is a natural bound for Z_0 to the left after lack of roots of $\ell_0\ell_r$ by the similar argument as above. If L has a solution with nonzero valuation growth, then the bound to the right is given by the choice of Z. Now suppose all solutions of L in $\bar{C}((q))^{\alpha+\mathbb{Z}}$ have zero valuation growth. Let $\zeta \in \alpha + Z$ be such that all roots of $\ell_0\ell_r$ are contained to the left. For each $z = \zeta + n$ with $n \geq 0$, choosing the basis $b_j(z+i-1) = \delta_{i,j}(i, j = 1, \ldots, r)$, we get

$$\liminf_{n\to+\infty} \nu_q(b_j(z+n)) = \min_{i=1}^{r} \nu_q(b_j(z+i-1)) = 0$$

for all $j = 1, \ldots, r$. Then $\liminf_{n\to+\infty} \nu_q(b_j(z-n)) = 0$. For any operator $A \in V$, it again follows that $\mathrm{val}_z(A) = \min_{j=1}^{r} \nu_q((A \cdot b_j)(z))$ and hence $\mathcal{B}$ is an integral basis at such a point z for the same reason.

(F) We can take any basis of $V = \bar{C}(x)[S]/\langle L\rangle$ whose basis elements belong to $C(x)[S]/\langle L\rangle$, for example $1, S, \ldots, S^{r-1}$. If $z, \tilde{z} \in \bar{C}$ are conjugates, let σ be an element of the Galois group of $\bar{C}$ over C that maps z to $\tilde{z}$. Then for every solution $f \in \bar{C}((q))^{z+\mathbb{Z}}$ of L also $\sigma(f) \in \bar{C}((q))^{\tilde{z}+\mathbb{Z}}$ is a solution of L, because L has coefficients in C, so $\sigma(L) = L$.
Since we have

$$\begin{aligned}&\sigma((\alpha_0 + \cdots + \alpha_{r-1}S^{r-1})(f))\\ &= (\sigma(\alpha_0) + \cdots + \sigma(\alpha_{r-1})S^{r-1})(\sigma(f))\end{aligned}$$

for any $\alpha_0, \ldots, \alpha_{r-1} \in \bar{C}(x)$, it follows that $\mathrm{val}_z(\alpha_0 + \cdots + \alpha_{r-1}S^{r-1}) \geq \mathrm{val}_{\tilde{z}}(\sigma(\alpha_0) + \cdots + \sigma(\alpha_{r-1})S^{r-1})$. Equality follows by exchanging z and $\tilde{z}$.

We now define the discriminant function in the shift setting. For each $\alpha \in Z$, by the item (A), we can choose a basis $b_1, \ldots, b_r$ of $\mathrm{Sol}(L)$ such that $\mathrm{val}_\alpha(B) = \min_{j=1}^{r} \nu_q((B \cdot b_j)(\alpha))$. For any k-vector space basis $B = \{B_1, \ldots, B_r\}$ of $V = \bar{C}(x)[S]/\langle L\rangle$, we can take

$$\mathrm{Disc}_\alpha(B) := \nu_q(\det(((B_i \cdot b_j)(\alpha))_{i,j=1}^{r})) \in \mathbb{Z}.$$

It is well-defined since the matrix $((B_i \cdot b_j)(\alpha)) = (p_{i,\ell}) \cdot (b_j(\alpha + \ell - 1))$ is regular, where $B_i = \sum_{j=1}^{r} p_{i,\ell}S^{\ell-1}$ with $p_{i,\ell} \in \bar{C}(x)$. If B_i's are integral for α, then $\nu_q((B_i \cdot b_j)(\alpha)) \geq 0$ for all $i, j = 1, \ldots, r$. It follows that $\mathrm{Disc}_\alpha(B) \geq 0$.

Let $\alpha_1, \ldots, \alpha_{d-1} \in k$, replacing B_d by $\alpha_1B_1 + \cdots + \alpha_{d-1}B_{d-1} + B_d$ (resp. by $(x-\alpha)^{-1}B_d$) is equivalent to multiplying the matrix $((B_i \cdot b_j)(\alpha))$ by a matrix with determinant 1 (resp. with determinant $(x-\alpha)^{-1}$) and it follows that the valuation of the determinant is constant (resp. is strictly decreasing).

Example 19. *Let $L = (x+2)^2 + xS^2 + (x+2)S^3$. For every $\alpha \notin \mathbb{Z}$, we have that $\{1, S, S^2\}$ is a local integral basis for $V = C(x)[S]/\langle L\rangle$ at $\alpha + \mathbb{Z}$. For the orbit $\mathbb{Z}$, choosing $b_j(-2+i-1) = \delta_{i,j}$ for $i, j = 1, 2, 3$, we obtain a basis of the solution space in $C((q))^{\mathbb{Z}}$:*

n	$\cdots$	-2	-1	0	1	2	$\cdots$
$b_1(n)$	$\cdots$	1	0	0	$-q$	$\frac{q(q-1)}{q+1}$	$\cdots$
$b_2(n)$	$\cdots$	0	1	0	0	$-q-1$	$\cdots$
$b_3(n)$	$\cdots$	0	0	1	$\frac{-q+2}{q}$	$\frac{q^2-3q+2}{q(q+1)}$	$\cdots$

Then $\mathrm{val}_\alpha(B) = \min_{j=1}^{3} \nu_q((B \cdot b_j)(\alpha))$ for any operator $B \in V$ and $\alpha \in \mathbb{Z}$. Since the solution b_3 has negative valuation growth, for a global integral basis the set Z has to be bounded on the right in the orbit $\mathbb{Z}$. Take $Z = C \setminus \{1, 2, \ldots\}$. At $\alpha = 0$, we have 1 is locally integral, but S, S^2 are not since $\mathrm{val}_0(S) = \mathrm{val}_0(S^2) = -1$. However, xS, xS^2 are locally integral. By Alg. 10, we can find a local integral basis at 0:

$$\left\{1, \tfrac{x-2}{x^2} + \tfrac{1}{x}S, \tfrac{-2}{x} + S^2\right\}.$$

Using such a basis as an input, continue to find all locally integral elements at $\alpha = -1$. Similarly replace $B_3 = \frac{-2}{x} + S^2$ by $(x+1)B_3$ since $\mathrm{val}_1(B_3) = -1$. This operation does change the local integrality at $Z \setminus \{-1\}$, because $x+1$ is invertible in the localization of $C[x]$ at any $z \neq -1$. So the output local integral basis at $\alpha = -1$ is also a global integral basis for Z:

$$\left\{1, \tfrac{x-2}{x^2} + \tfrac{1}{x}S, \tfrac{-x+2}{x^2} + \tfrac{-3x-1}{x(x+1)^2}S + \tfrac{1}{x+1}S^2\right\}.$$

Acknowledgement. We thank the referees for their careful reading and their valuable suggestions, in particular the referee who pointed out the implication $(a) \Rightarrow (b)$ in Theorem 13.

REFERENCES

[1] Sergei A. Abramov, Moulay A. Barkatou, Mark van Hoeij, and Marko Petkovsek. Subanalytic solutions of linear difference equations and multidimensional hypergeometric sequences. *J. Symb. Comput.*, 46(11):1205–1228, 2011.
[2] M. Bronstein. The lazy Hermite reduction. Technical Report 3562, INRIA, 1998.
[3] Manuel Bronstein. Symbolic integration tutorial. ISSAC'98, 1998.
[4] Shaoshi Chen, Manuel Kauers, and C. Koutschan. Reduction-based creative telescoping for algebraic functions. In *Proc. ISSAC'16*, pages 175–182, 2016.
[5] Shaoshi Chen, Mark van Hoeij, Manuel Kauers, and Christoph Koutschan. Reduction-based creative telescoping for fuchsian D-finite functions. *J. Symb. Comput.*, 85:108–127, 2018.
[6] Claude Chevalley. Introduction to the Theory of Algebraic Functions of One Variable. AMS Mathematical Surveys, 1951.
[7] Thomas Cluzeau and Mark van Hoeij. Computing hypergeometric solutions of linear recurrence equations. *AAECC*, 17:83–115, 2006.
[8] Dominique Duval. Rational Puiseux expansions. *Compositio Mathematica*, 70(2):119–154, 1989.
[9] Antonio J. Engler and Alexander Prestel. *Valued Fields*. Springer, 2005.
[10] László Fuchs. Vector spaces with valuations. *J. of Algebra*, 35(1-3):23–38, 1975.
[11] Erdal Imamoglu. *Algorithms for Solving Linear Differential Equations with Rational Function Coefficients*. PhD thesis, Florida State University, 2017.
[12] Erdal Imamoglu and Mark van Hoeij. Computing hypergeometric solutions of second order linear differential equations using quotients of formal solutions and integral bases. *J. Symb. Comput.*, 83:254–271, 2007.
[13] Edward L. Ince. *Ordinary Differential Equations*. Dover, 1926.
[14] Manuel Kauers and Christoph Koutschan. Integral D-finite functions. In *Proc. ISSAC'15*, pages 251–258, 2015.
[15] Jean-Pierre Serre. Local fields. *Graduate Texts in Mathematics*, 1979.
[16] Jean Pierre Tignol and Adrian R. Wadsworth. *Value Functions on Simple Algebras, and Associated Graded Rings*. Springer, 2015.
[17] Barry M. Trager. *Integration of Algebraic Functions*. PhD thesis, MIT, 1984.
[18] Mark van Hoeij. An algorithm for computing an integral basis in an algebraic function field. *Journal of Symbolic Computation*, 18(4):353–363, 1994.
[19] Mark van Hoeij. Finite singularities and hypergeometric solutions of linear recurrence equations. *Journal of Pure and Applied Algebra*, 139:109–131, 1999.
[20] G. Zeng. Valuations on a module. *Communic. Algebra*, 35(8):2341–2356, 2007.