RICAM-Report No. 2015-02

M. Kauers, C. Koutschan

Integral D-Finite Functions
ABSTRACT
We propose a differential analog of the notion of integral
closure of algebraic function fields. We present an algorithm
for computing the integral closure of the algebra defined
by a linear differential operator. Our algorithm is a direct
analog of van Hoeij’s algorithm for computing integral bases
of algebraic function fields.

Categories and Subject Descriptors
I.1.2 [Computing Methodologies]: Symbolic and Alge-
braic Manipulation—Algorithms

General Terms
Algorithms

Keywords
Differential Operators, Holonomic Functions

1. INTRODUCTION

The notion of integrality is a classical concept in the the-
ory of algebraic field extensions. If $R$ is an integral domain
and $k$ a field containing $R$ and if $K$ is an algebraic extension
of $k$, then an element $\alpha$ of $K$ is called integral if its monic
minimal polynomial $M$ has coefficients in $R$. While $K$ forms
a $k$-vector space of dimension $\deg(M)$, the set of all integral
elements of $K$ forms an $R$-module, called the integral clo-
sure (or normalization) of $R$ in $K$, and commonly denoted
by $\mathcal{O}_K$. A $k$-vector space basis of $K$ which at the same time
generates $\mathcal{O}_K$ as $R$-module is called an integral basis. For
example, when $R = \mathbb{Z}$, $k = \mathbb{Q}$, and $K = \mathbb{Q}(\alpha)$ with $\alpha = \sqrt{2}$,
then the canonical vector space basis $\{ 1, \alpha, \alpha^2 \}$ of $K$ is not
an integral basis, because $\frac{1}{2} \alpha^2 = \sqrt{2}$ is an integral element

of $K$ (its minimal polynomial is $X^2 - 2$) but not a $\mathbb{Z}$-linear
combination of $1, \alpha, \alpha^2$. An integral basis in this example is
$\{ 1, \alpha, \frac{1}{2} \alpha^2 \}$.

The concept of integral closure has been studied in rather
general domains [9, 6]. To compute an integral basis for an
algebraic number field, special algorithms have been devel-
oped [7, 5]. At least two different approaches are known
for algebraic function fields, i.e., the case when $R = \mathbb{C}[x]$ for
some field $C$, $k = C(x)$, and $K = k[Y]/(M)$ for some irreducible polynomial $M \in k[Y]$. The algorithm derived by
Trager [10] in his thesis is an adaption of an algorithm for
number fields, and the algorithm by van Hoeij [12] is based
on the idea of successively canceling lower order terms of
Puiseux series.

The theory of algebraic functions parallels in many ways
the theory of D-finite functions, i.e., the theory of solutions
of linear differential operators. It is therefore natural to ask
what corresponds to the notion of integrality in this latter
theory. In the present paper, we propose such a definition
and give an algorithm which computes integral bases accord-
ing to this definition. Our algorithm and the arguments un-
derlying its correctness are remarkably similar to van Hoeij’s
algorithm for computing integral bases of algebraic function
fields.

In view of the key role that integral bases play for in-
definite integration (Hermite reduction) of algebraic func-
tions [10, 3, 2], we have hope that results presented below
will help to develop new algorithms for indefinite integration
of D-finite functions. An example pointing in this direction
is given in the end.

2. INTEGRAL FUNCTIONS,
INTEGRAL CLOSURE, AND
INTEGRAL BASES

Throughout this paper, let $C$ be a computable field of
characteristic zero, $\mathbb{C}$ an algebraically closed field contain-
ing $C$ (not necessarily the smallest), and $x$ transcendental
over $C$. When $R$ is a subring of $C(x)$, we write $R[D]$ for the
algebra of differential operators with coefficients in $R$, i.e.,
the algebra of all (formal) polynomials $\ell_0 + \ell_1 D + \cdots + \ell_r D^r$
with $\ell_0, \ldots, \ell_r \in R$. This algebra is equipped with the natu-
ral addition and the unique noncommutative multiplication
respecting the commutation rules $Dc = cD$ for all $c \in R \cap C$
and $Dx = xD + 1$. Typical choices of $R$ will be $C[x], C[z],
C(x)$, or $C(z)$ in the following.

For an operator $L = \ell_0 + \ell_1 D + \cdots + \ell_r D^r \in C[x][D]$ with $\ell_r \neq 0$ we denote by $\text{ord}(L) = r$ the order of $L$. Recall
that such an operator with \( x \mid \ell \) admits a fundamental system of formal power series, i.e., the vector space \( V \subseteq \mathbb{C}[x] \) consisting of all the power series \( f \) with \( L \cdot f = 0 \) has dimension \( r \). When \( x \mid \ell \neq 0 \), there is still always a fundamental system of generalized series solutions of the form \( \exp(x^{-1/4})x^\alpha(x^{1/4}, \log(x)) \) for some \( s \in \mathbb{N}, p \in \mathbb{C}[\alpha], \nu \in \mathbb{C}, a \in \mathbb{C}[x][y] \). (This notation is not meant to imply that \( a \) has a nonzero constant term, so the series in general does not start at \( x^0 \) but at \( x^{+\nu} \) where \( i \in \mathbb{N} \) is such that \( x^i \) is the lowest order term of \( a \)). We restrict our attention here to the case where \( p = 0, s = 1 \) and \( \nu \in \mathbb{C} \), i.e., to operators \( L \) which admit a fundamental system in \( \bigcup_{\nu \in \mathbb{C}} x^{\nu} \mathbb{C}[[x]][\log(x)] \). It is well known [8] how to determine the first terms of a basis of such solutions for a given operator \( L \in \mathbb{C}[x] \). By a linear change of variables, the same techniques can also be used to find the first terms of a fundamental system in \( \bigcup_{\nu \in \mathbb{C}} (x - \alpha)^\nu \mathbb{C}[[x]][\log(x - \alpha)] \), for any given \( \alpha \in \mathbb{C} \). More precisely, if \( L \) belongs to \( \mathbb{C}[x] \) and \( \alpha \in \mathbb{C} \), then there is a fundamental system in \( \bigcup_{\nu \in \mathbb{C}} (x - \alpha)^\nu \mathbb{C}(\alpha)[x - \alpha][\log(x - \alpha)] \). For a field \( K \) with \( C \subseteq K \subseteq \mathbb{C} \) we will use the notation

\[
K[[x - \alpha]] = \bigcup_{\nu \in \mathbb{C}} (x - \alpha)^\nu K[[x - \alpha]][\log(x - \alpha)].
\]

Observe that this is not a ring or a \( K \)-vector space. Also observe that the exponents \( \nu \) are restricted to the small field \( C \subseteq K \), although the dependence on the choice of \( C \) is not reflected by the notation. We hope that the intended field \( C \) will always be clear from the context.

An operator \( L \in \mathbb{C}[x][D] \) shall be considered integral if all the terms in all its series solutions remain above a certain threshold. In the algebraic case, where series solutions involve at worst only fractional exponents, the stipulation of having only nonnegative exponents in all the solutions happens to be equivalent to the requirement that the monic minimal polynomial has polynomial coefficients. In the differential case however, where irrational exponents as well as logarithmic terms can appear, and where solutions involving fractional exponents cause factors in the leading coefficient of the operator regardless of whether the exponents are positive or negative, it is less clear which constraints on the exponents should be used to define integrality. Fortunately, it turns out that we can partly leave the choice to the reader.

**Definition 1.** Let \( \iota: C/Z \times N \to C \) be a function such that
1. \( \iota(\nu + Z, j) \in \nu + Z \) for every \( \nu \in C \) and \( j \in \mathbb{N} \),
2. \( \iota(\nu_1 + Z, j_1) + \iota(\nu_2 + Z, j_2) - \iota(\nu_1 + \nu_2 + Z, j_1 + j_2) \geq 0 \) for every \( \nu_1, \nu_2 \in C \) and \( j_1, j_2 \in \mathbb{N} \),
3. \( \iota(Z, 0) = 0 \).

A series \( f \in \mathbb{C}[[x - \alpha]] \) is called integral with respect to \( \iota \) if for all terms \( (x - \alpha)^\nu \log(x - \alpha)^j \) occurring with a nonzero coefficient in \( f \) we have \( \mu - (\mu + Z, j) \geq 0 \).

The function \( \iota(\cdot, \cdot) \) specifies for each \( Z \)-orbit of \( C \) the smallest element \( \nu \) such that \( x^\nu \log(x) \) should be considered integral. If \( \iota(\nu + Z, j) = \nu \), then \( x^\nu \log(x)^1, x^{\nu + 1} \log(x)^1, \ldots \) are integral and \( x^{\nu - 1} \log(x)^1, x^{\nu - 2} \log(x)^2, \ldots \) are not. The condition \( \iota(Z, 0) = 0 \) implies that formal Laurent series are integral if and only if they are in fact formal power series.

**Example 2.** A natural choice for \( F \subseteq C \) is perhaps \( \iota(z + Z, 0) = z \) for all \( z \in C \) with \( 0 \leq \Re(z) < 1 \), and \( \iota(z + Z, j) = z \) for all \( z \in C \) with \( 0 < \Re(z) \leq 1 \) when \( j \geq 1 \). With this convention, \( 1, x, x^2, x^3 \) \log(x) all are integral, in accordance with the fact that the corresponding functions are bounded in a small neighborhood of the origin while \( x^{-1}, x^{3/2}, \log(x) \) are not. Unless otherwise stated, we shall always assume this choice of \( \iota \) in the examples given below.

**Proposition 3.** Let \( \alpha \in \mathbb{C} \) and let \( R \) be the set of all \( \mathbb{C} \)-linear combinations of series in \( (x - \alpha)^\nu \mathbb{C}[[x - \alpha]][\log(x - \alpha)] \), \( \nu \in C \). Then:

1. In every series \( f \in R \) there are at most finitely many terms \( (x - \alpha)^\nu \log(x - \alpha)^j \) which are not integral.
2. The set \( R \) together with the natural addition and multiplication forms a ring, and \( \{ f \in R \mid f \text{ is integral} \} \) forms a subring of \( R \).

**Proof.** 1. First consider the case when \( f \in (x - \alpha)^\nu \mathbb{C}[[x - \alpha]][\log(x - \alpha)] \) for some \( \nu \in C \). Let \( \deg(f) \) denote the highest power of \( \log(x - \alpha) \) in \( f \). Then the only possible non-integral terms in \( f \) are \( (x - \alpha)^\nu \log(x - \alpha)^j \) for \( j \in \{0, \ldots, \deg(f)\} \) and \( \nu \in \{0, \ldots, \mu + Z, j \neq \nu - 1\} \). These are finitely many. In general, if \( f \) is a linear combination of some series in \( (x - \alpha)^\nu \mathbb{C}[[x - \alpha]][\log(x - \alpha)] \) with possibly distinct \( \nu \in C \), the set of all non-integral terms is still a finite union of finite sets of non-integral terms, and therefore finite.

2. It is clear that \( R \) is a ring. To see that the integral elements form a subring, let \( f, g \in R \) be integral. Then the series \( f + g \) cannot contain any term which is not present in at least one of the two summands, so all terms of \( f + g \) are integral and \( f + g \) as a whole is integral. Now consider multiplication: for any term \( (x - \alpha)^\nu \log(x - \alpha)^j \) in \( f \cdot g \) there must be some terms \( \tau \) in \( f \) and \( \sigma \) in \( g \) such that \( \sigma \tau = (x - \alpha)^\mu \log(x - \alpha)^\mu \), say \( \tau = (x - \alpha)^\nu \log(x - \alpha)^j \) and \( \sigma = (x - \alpha)^\mu \log(x - \alpha)^\mu \). Since \( f \) and \( g \) are integral, we have \( \mu_1 - (\mu_1 + Z, j_1) \geq 0 \) and \( \mu_2 - (\mu_2 + Z, j_2) \geq 0 \). The assumption on \( \iota \) in Definition 1 implies that \( (\mu_1 + \mu_2) - (\mu_1 + \mu_2 + Z, j_1 + j_2) = \mu - (\mu + Z, j) \geq 0 \). Hence all terms of \( f \cdot g \) are integral, so also the product of two integral elements is integral.

**Definition 4.** Let \( L \in \mathbb{C}(x)[D] \) and \( \iota \) be as in Definition 1.

1. We call \( L \) regular if it has a fundamental system in \( \mathbb{C}[[x - \alpha]] \) for every \( \alpha \in \mathbb{C} \).
2. \( L \) is called (locally) integral at \( \alpha \) with respect to \( \iota \) if it admits a fundamental system in \( \mathbb{C}[[x - \alpha]] \) whose elements all are integral.
3. \( L \) is called (globally) integral with respect to \( \iota \) if it is locally integral at \( \alpha \) in the sense of part 1 for every \( \alpha \in \mathbb{C} \).

Of course part 2 of this definition is independent of the choice of the fundamental system. In fact, \( L \) is locally integral at \( \alpha \) iff all its series solutions in \( x - \alpha \) are integral and form a \( C \)-vector space of dimension \( \dim(D) \).

**Example 5.** 1. The operator \( (2 - x)(2 - 2x + 2x^2)^2D^2 + 4(x - 1)x^D^2 \in Q[x][D] \) is locally integral at \( \alpha = 0 \), because its two linearly independent solutions

\[
1 - \frac{1}{2}x - \frac{1}{24}x^3 - \frac{7}{384}x^4 - \frac{53}{384}x^5 + O(x^6),
\]
Example 7. Basis $\{x, 1\}$ is an integral basis. It is also locally integral at $\alpha = 1$, because its two linearly independent solutions

\[(x-1)^{1/2} + O((x-1)^3), \quad 1 - \frac{1}{2}(x-1) + \frac{1}{8}(x-1)^3 + O((x-1)^4)\]

are integral. The operator is also globally integral because at all $\alpha \in \mathbb{C} \setminus \{0, 1\}$ it has a fundamental system of formal power series, and formal power series are always integral.

2. The operator $1 + xD \in \mathbb{Q}[x][D]$ is not locally integral at $\alpha = 0$, because it has the non-integral solution $\frac{1}{x}$. It is therefore also not globally integral.

3. The operator $(-1 - 2x) + (x + 2x^2)D + (x^3 + x^4)D^2 \in \mathbb{Q}[x][D]$ is not locally integral at $\alpha = 0$ although all its series solutions are. The reason is that it has only one series solution in $\mathbb{C}[[x]]$ while our definition requires that the number of linearly independent series solutions must match the order of the operator. In other words, generalized series solutions involving exponential terms, like the solution $\exp(\frac{1}{x})$ in the present example, are always considered as not integral.

Let $L = t_0 + \cdots + t_r D^r \in \mathbb{C}[x][D]$ with $t_r \neq 0$ and consider the quotient algebra $\mathbb{C}(x)[D]/(L)$, where $\langle L \rangle := \mathbb{C}(x)[D]$ denotes the left ideal generated by $L$ in $\mathbb{C}(x)[D]$. The algebra $\mathbb{C}(x)(\mathbb{C}[x][D])/\langle L \rangle$ generated as a $\mathbb{C}(x)$-vector space by the basis $\{1, D, \ldots, D^{r-1}\}$. It is also a $\mathbb{C}(x)$-$\mathbb{C}$-algebra.

Definition 6. Let $L = t_0 + \cdots + t_r D^r \in \mathbb{C}[x][D]$ with $t_r \neq 0$ be a regular operator and let $i$ be as defined in Definition 1.

1. An element $P \in A = \mathbb{C}(x)[D]/\langle L \rangle$ is called integral (with respect to $i$) if $P \cdot f$ is integral (with respect to $i$) for every series solution $f$ of $L$.

2. The $\mathbb{C}(x)$-$\mathbb{C}$-algebra $\mathcal{O}_L$ of all integral elements of $A$ is called the integral closure of $\mathbb{C}(x)$ in $A$.

3. A $\mathbb{C}(x)$-$\mathbb{C}$-vector space basis $\{B_1, \ldots, B_k\} \subseteq \mathbb{C}(x)[D]/\langle L \rangle$ is called an integral basis if it also generates $\mathcal{O}_L$ as a $\mathbb{C}(x)$-$\mathbb{C}$-algebra.

It is easy to see that $\mathcal{O}_L$ is a $\mathbb{C}(x)$-$\mathbb{C}$-algebra. Note however that $\mathcal{O}_L$ is in general not a $\mathbb{C}(x)[D]$-$\mathbb{C}$-algebra.

Example 7. 1. The operator $L = 1 - D \in \mathbb{Q}[x][D]$ has for every $\alpha \in \mathbb{C}$ one solution of the form $f = 1 + O(x-\alpha)$. Since $f$ is integral we have $1 \in \mathcal{O}_L$. Since $(x-\alpha)^{-1} f$ is not integral for any $\alpha$, we have in fact that $\{1\}$ is an integral basis.

2. The operator $L = 1 + xD$ has the solution $f = \frac{1}{x}$. It is integral for every $\alpha \neq 0$, but not integral at $\alpha = 0$. However, $xf = 1$ is integral, hence $x \in \mathcal{O}_L$, and in fact $\{x\}$ is an integral basis.

3. Whenever $L$ has power series solutions at every $\alpha \in \mathbb{C}$, we clearly have $\{1, D, \ldots, D^{r-1}\} \subseteq \mathcal{O}_L$. However, there may still be integral elements that are not $\mathbb{C}(x)$-linear combinations of these. For example, observe that for the operator $L = (x-1) + D - xD^2$, which has two solutions $1 + x + \frac{1}{2}x^2 + O(x^3)$ and $x^2 + O(x^3)$ at $\alpha = 0$, we have the nontrivial element $\frac{1}{2}(1 - D) \in \mathcal{O}_L$.

4. It can also happen that $1 \in \mathcal{O}_L$ but $D \notin \mathcal{O}_L$. For example, for $L = ((-1 + 2x) + (1 - 4x)D + 2x^2)D$ we have two solutions $1 + x + \frac{1}{2}x^2 + O(x^3)$ and $x^3 + 2x^3 + \frac{1}{8}x^{5/2} + O(x^3)$ at $\alpha = 0$. Since both are integral and there are two linearly independent power series solutions for every $\alpha \neq 0$ we have $1 \in \mathcal{O}_L$. However, $D \notin \mathcal{O}_L$, because the derivative of the second solution is $\frac{5}{2}x^{-1/2} + \frac{1}{2}x^{1/2} + \frac{1}{8}x^{3/2} + O(x^3)$, which is not integral since it involves the term $x^{-1/2}$. An integral basis in this case turns out to be $\{1, xD\}$.

5. We have produced a prototype implementation in Mathematica of the algorithm described below. The code is available on the homepage of the first author. For the operator $L = xD^3 + xD - 1$, it finds the integral basis $\{x, xD, xD^2 - D + \frac{1}{x}\}$. A fundamental system of $L$ is $\{x, x \log(x), x \log(x)^2\}$.

6. Let $L = 24x^3D^3 - 134x^2D^2 + 373xD - 450$. This operator has the solutions $x^{1/3}$, $x^{10/3}$, and $x^{15/3}$. Our code finds the integral basis $\{\frac{1}{x}, x^2D - \frac{3}{2}x^3, \frac{1}{2}x^2D^2 - \frac{7}{2}x^3D + \frac{9}{2}x^4\}$.

In the analogy with algebraic functions, the integral operators from Definition 4 correspond to the monic minimal polynomials with coefficients in a ring, and the integral elements of Definition 6 correspond to integral elements of an algebraic function field. Definitions 4 and 6 are obviously connected as follows.

Proposition 8. Let $L \in \mathbb{C}[x][D]$ and $\hat{L} \in \mathbb{C}(x)[D]$ be regular and assume that there exists $P \in \mathbb{C}(x)[D]$ such that for every $\alpha \in \mathbb{C}$ we have

$$\{f \mid \hat{L} \cdot f = 0\} = \{P \cdot f \mid L \cdot f = 0\}$$

where $f$ runs over $\mathbb{C}[[x-\alpha]]$ on both sides. Then $P + (L) \in \mathbb{C}(x)[D]/(L)$ is integral in the sense of Definition 6 if and only if $\hat{L}$ is integral in the sense of Definition 4.

Lemma 9. Let $L = t_0 + \cdots + t_r D^r \in \mathbb{C}[x][D]$ with $t_r \neq 0$ be a regular operator. Let $p_0, \ldots, p_{r-1} \in \mathbb{C}(x)$ and let $p = x - \alpha \in \mathbb{C}(x)$ be a factor of the common denominator of $p_0, \ldots, p_{r-1}$. If $p_0 + \cdots + p_{r-1}D^{r-1} \in \mathcal{O}_L$ then $p \in \mathcal{O}_L$.

Proof. After performing a change of variables, we may assume that $p = x$. By a classical result about linear differential equations (e.g., [8]), $x | \ell_i$ implies that $L$ admits a fundamental system $b_0, \ldots, b_{r-1} \in \mathbb{C}[x]$ with $b_i = x^i + O(x^r)$ for $i = 0, \ldots, r-1$. Then $D \cdot b_i = i(-1) \cdots (i-j+1)x^{i-j} + O(x^{i-j+1})$ for $i = 0, \ldots, r-1$ and $j = 0, \ldots, r-1$. Let $c_i$ be the largest integer such that $x^{c_i}$ divides the denominator
of \( p_i \), let \( e = \max \{ e_0, \ldots, e_{r-1} \} \), and let \( i \in \{ 0, \ldots, r-1 \} \) be some index with \( e_i = e \). Then \( p_i D' b_i = t \alpha x^{e+i} + O(x^{e+i+1}) \) and \( p_i D'' b_i = O(x^{e+i+1}) \) for all \( j \not= i \). Hence \( (p_0 + p_1 D + \cdots + p_{r-1} D^{r-1}) b_i = t \alpha x^{e+i} + O(x^{e+i+1}) \) is not integral because \( -e - i(e + Z, 0) = -e - i(Z, 0) = -e < 0 \), and hence \( p_0 + p_1 D + \cdots + p_{r-1} D^{r-1} \not\in O_L \). ■

3. ALGORITHM OUTLINE

We shall now discuss how to construct an integral basis \( \{ B_0, \ldots, B_{r-1} \} \) for a given regular operator \( L \in C[x][D] \). The key observation is that van Hoeij’s algorithm for computing integral bases for algebraic function fields as well as the arguments justifying its correctness and termination carry over almost literally to the present setting. The rephrasing integral bases for algebraic function fields as well as the determinant

\[ W = \begin{vmatrix} f_1(x) & f_2(x) & \cdots & f_r(x) \\ f'_1(x) & f'_2(x) & \cdots & f'_r(x) \\ \vdots & \vdots & \ddots & \vdots \\ f^{(r-1)}_1(x) & f^{(r-1)}_2(x) & \cdots & f^{(r-1)}_r(x) \end{vmatrix} \]

**Definition 11.** Let \( L \in C[x][D] \) be regular and let \( b_1, \ldots, b_r \) be a fundamental system of \( L \) in \( C[[x - \alpha]] \) for some \( \alpha \in C \). For \( B_0, \ldots, B_{r-1} \in C(x)[D]/(L) \) we define the generalized Wronskian at \( \alpha \), as

\[ \text{wr}_{L, \alpha}(B_0, \ldots, B_{r-1}) := \begin{vmatrix} B_0 \cdot b_1 & \cdots & B_0 \cdot b_r \\ \vdots & \ddots & \vdots \\ B_{r-1} \cdot b_1 & \cdots & B_{r-1} \cdot b_r \end{vmatrix} \]

Note that the generalized Wronskian \( \text{wr}_{L, \alpha}(B_0, \ldots, B_{r-1}) \) belongs to \( C[[x - \alpha]] \) and that the choice of a different fundamental system instead of \( b_1, \ldots, b_r \) only changes its value by a nonzero multiplicative constant, which will be irrelevant for our purpose.

For the special choice \( B_i = D^i \), the generalized Wronskian \( \text{wr}_{L, \alpha}(1, D, \ldots, D^{r-1}) \) reduces to the Wronskian (1) with \( f_i = b_i \). It is well-known and easy to check that the classical Wronskian (1) of \( b_1, \ldots, b_r \) satisfies the first-order exponential. This means \( E \) strictly smaller.

8 Return \( \{ B_0, \ldots, B_{r-1} \} \).

In order to justify this algorithm, three issues have to be addressed:

- Termination of the loop in lines 5–7. See Section 4.
- The existence and construction of an element \( A \) with the properties requested in step 6 whenever \( E \not= \emptyset \). Section 5 has the existence argument, and Section 6 the construction.
- How to decide \( E \not= \emptyset \) for recognizing the termination of the loop in lines 5–7. This will also be discussed in Section 6.

Except for these three points, the correctness of the algorithm is obvious.

4. TERMINATION

The termination of van Hoeij’s algorithm (12) is established by the observation that the degree of a certain polynomial, starting with the discriminant \( \text{Res}_Y (M, \frac{\partial M}{\partial Y}) \), decreases in each iteration of the main loop. In the case of \( D \)-finite functions, the role of the discriminant is played by the Wronskian and a generalized version of it. Recall that the Wronskian of the functions \( f_1(x), \ldots, f_r(x) \) is defined as the determinant

**Theorem 12.** Algorithm 10 terminates.

**Proof.** First observe that during the whole execution of the algorithm, \( B_0, \ldots, B_{r-1} \in C(x)[D]/(L) \) are integral, i.e., \( B_0 \cdot f_1, \ldots, B_{r-1} \cdot f \) are integral for any series solution \( f \) of \( L \) according to Definition 6. (Actually, the \( B_i \)'s are constructed one after the other, but they can be initialized with \( B_d = s^d D^d B_0 \).) This means that, at any time and for any \( \alpha \in C \), the generalized Wronskian \( \text{wr}_{L, \alpha}(B_0, \ldots, B_{r-1}) \) is integral, as it is the sum of products of integral series (see Proposition 3). Since it is hyperexponential, it follows
Lemma 13. If $E \neq \emptyset$, then there exists $A \in E$ of the form

$$A = \frac{1}{x - \alpha}(a_0b_0 + \cdots + a_d b_d)$$

with $\alpha \in \bar{C}$, $a_0, \ldots, a_d \in \bar{C}[x]$.

Proof. Let $A \in E$, say $A = a_0b_0 + \cdots + a_d b_d$ for some $a_i \in \bar{C}(x)$. Since $A \notin \bar{C}[x]B_0 + \cdots + \bar{C}[x]B_d$, at least one $a_i$ must be in $\bar{C}(x) \setminus \bar{C}[x]$. Let $p \in \bar{C}[x]$ be the common denominator of all the $a_i$, and let $\alpha \in \bar{C}$ be a root of $p$. Then $\frac{1}{x - \alpha}$ has the required form. To see that it belongs to $E$, notice that $\frac{1}{x - \alpha} \in \bar{C}[x]$ and $\mathcal{O}_L$ is a $\bar{C}[x]$-module, and that $\frac{1}{x - \alpha} \notin \bar{C}[x]B_0 + \cdots + \bar{C}[x]B_d$.

Lemma 14. If $A \in E$ and $P \in \bar{C}[x]B_0 + \cdots + \bar{C}[x]B_d$, then $A + P \in E$.

Proof. $A \in E \subseteq \mathcal{O}_L$ and $P \in \bar{C}[x]B_0 + \cdots + \bar{C}[x]B_d \subseteq \mathcal{O}_L$ implies that $A + P \in \mathcal{O}_L$. It is also clear that $\text{ord}(A + P) \leq d$, because $\text{ord}(A) \leq d$ and $\text{ord}(P) \leq d$. Finally, to show that $A + P \notin \bar{C}[x]B_0 + \cdots + \bar{C}[x]B_d$, assume otherwise. Then also $A = (A + P) - P \in \bar{C}[x]B_0 + \cdots + \bar{C}[x]B_d$ in contradiction to $A \in E$.

Lemma 15. If $E$ contains an element of the form (2), then it also contains such an element with $a_0, \ldots, a_d \in \bar{C}$.

Proof. Let $A = \frac{1}{x - \alpha}(a_0b_0 + \cdots + a_d b_d) \in E$ be of the form (2). For each $i = 0, \ldots, d$, write $a_i = (x - \alpha) p_i + a'_i$ with $p_i \in \bar{C}[x]$ and $a'_i \in \bar{C}$. By Lemma 14, $A \in E$ implies $A' \in E$ for

$$A' = \frac{1}{x - \alpha}(a'_0b_0 + \cdots + a'_{d-1}b_{d-1} + a'_d b_d).$$

Since $B_0, \ldots, B_{d-1}$ are assumed to generate the submodule of all the elements of $\mathcal{O}_L$, of order at most $d - 1$, we have $a'_{d-1} = 0$. Dividing $A'$ by $a'_{d}$ yields an element of $E$ of the requested form.

Lemma 16. If $E$ contains an element of the form (2) with $a_0, \ldots, a_{d-1} \in \bar{C}$ and $a_d = 1$, then it also contains such an element with $a_0, \ldots, a_{d-1} \in \bar{C}(\alpha)$ and $a_d = 1$.

Proof. Let $E$ be of the form (2) with $a_0, \ldots, a_{d-1} \in \bar{C}$ and $a_d = 1$. Since $\bar{C}$ is necessarily a $\bar{C}(\alpha)$-vector space, there are some $\bar{C}(\alpha)$-linearly independent elements $e_0, \ldots, e_n$ of $C$ such that $a_0, \ldots, a_d$ all belong to $V = a_0C(\alpha) + \cdots + e_nC(\alpha)$. We may assume $e_0 = 1$. Consider a fundamental system $b_1, \ldots, b_n \in C(\alpha)[[x - \alpha]]$ of $L$. Then each $A \cdot b_j$ has coefficients in $V$ and, since $A \in E \subseteq \mathcal{O}_L$, only involves integral terms. By the linear independence of the $e_i$ over $C(\alpha)$, also the series $e_i(A \cdot b_j) = [e_i(A) \cdot b_j$ obtained from $A \cdot b_j$ by replacing each coefficient by its $e_i$-coordinate will be integral. In particular, the operator $a_0 = [e_0]A \in C(\alpha)[[x]]/D$ must belong to $E$. Because of $[e_0]a_d = [e_0]1 = 1$, it meets all the requirements.

Lemma 17. If $E$ contains an element of the form (2) with $a_0, \ldots, a_{d-1} \in C(\alpha)$ and $a_d = 1$, then it also contains such an element with $a_0, \ldots, a_{d-1} \in C[x]$ and $a_d = 1$.

Proof. For every $n > 0$ we have $x - \alpha | x^n - \alpha^n$ in $\bar{C}(\alpha)$, and thus also $x - \alpha | p(x) - p(\alpha)$ for $p \in \bar{C}[\alpha] \setminus \bar{C}[x]$. Therefore, if we view the $a_i \in C(\alpha)$ as polynomials in $\alpha$, then replacing $\alpha$ in them by $x$ amounts to adding some polynomial multiple of $(x - \alpha)$ to them. This change means for $A = \frac{1}{x - \alpha}(a_0b_0 + \cdots + a_{d-1}b_{d-1} + b_d)$ that adding a suitable element $P \in C(\alpha)[x]B_0 + \cdots + C(\alpha)[x]B_{d-1} \subseteq \mathcal{O}_L$ turns $A$ into an operator of the requested form. By Lemma 14, this new operator also belongs to $E$.

Theorem 18. If $E \neq \emptyset$, then there exists an element $A \in E$ of the form

$$A = \frac{1}{p}(a_0b_0 + \cdots + a_{d-1}b_{d-1} + b_d)$$

with $p \in C[x]$ an irreducible factor of $\ell$, and $a_0, \ldots, a_{d-1} \in C[x]$ such that $\text{deg}(a_i) < \text{deg}(p)$ for all $i$.

Proof. The assumption $E \neq \emptyset$ in combination with Lemmas 13, 15, 16, and 17 implies that $E$ contains an element of the form (2) with $a_0, \ldots, a_{d-1} \in C[x]$ and $a_d = 1$. Furthermore, Lemma 9 implies that $\alpha$ is a root of $\ell$. Let $p | \ell$, be the minimal polynomial of $\alpha$. We claim that $A := \frac{1}{p} B \in E$ where $B := a_0b_0 + \cdots + a_{d-1}b_{d-1} + b_d$. To prove this, we have to show that for every $\tilde{\alpha} \in \bar{C}$ and every solution $\tilde{b} \in C(\alpha)[[[x - \tilde{\alpha}]])$ of $L$ we still have that $A \cdot \tilde{b}$ is integral. When $\tilde{\alpha}$ is not a root of $p$, this is clear because $1/p$ admits an expansion in $C[x - \tilde{\alpha}]$, and multiplication of the integral series $B \cdot \tilde{b}$ by a formal power series preserves integrability by Proposition 3. When $\tilde{\alpha} = \alpha$, write $p = (x - \alpha)q$ for some $q \in C[x]$ with $x - \alpha | q$ and note that $1/q$ admits an expansion in $C[x - \alpha]$ and $\frac{1}{\alpha} B \cdot \tilde{b}$ is integral too. When $\tilde{\alpha}$ is a conjugate
of \( \alpha \), note that \( \frac{1}{p} \cdot \tilde{b} \cdot \tilde{b} \) must be integral, because if it were not, then for the series \( b \in C(\alpha)[[x - \alpha]] \) obtained from \( \tilde{b} \) via the conjugation map that sends \( \tilde{\alpha} \) to \( \alpha \) we would have that \( \frac{1}{p} \cdot \tilde{b} \cdot \tilde{b} \) is also not integral, in contradiction to our choice of \( a_0, \ldots, a_d \). Therefore the same argument as in the case \( \tilde{\alpha} = \alpha \) applies.

This completes the proof of the claim. To complete the proof of the theorem, note that the claimed degree bounds on \( a_i \) can be ensured by Lemma 14. ■

6. CONSTRUCTION OF \( A \) IN STEP 6

In the previous section we have demonstrated that in step 6 of the algorithm it suffices to search for an integral element \( A \) of the form

\[
A = \frac{1}{p}(a_0B_0 + \cdots + a_{d-1}B_{d-1} + B_d)
\]

where \( a_0, \ldots, a_{d-1}, p \in C[x], p \mid \ell_r \). Conversely, this means that if no such \( A \) exists, the set \( E \) is empty.

For each irreducible factor \( p \) of \( \ell_r \), one can set up an ansatz for \( A \) with undetermined coefficients \( a_0, \ldots, a_{d-1} \). We want to find \( a_0, \ldots, a_{d-1} \) such that \( A \cdot f \) is integral for all solutions \( f \) of \( L \).

Note that we need to enforce integrality only for series solutions in \( x - \alpha \) where \( \alpha \) is a root of \( p \). Choosing a fundamental system \( b_1, \ldots, b_r \) of such solutions, computing the first terms of \( B_j \cdot b_i \), plugging them into the ansatz, and equating the coefficients of all non-integral terms to zero yields a linear system for \( a_0, \ldots, a_{d-1} \). If this system does not admit a solution, one knows that no such \( A \) with denominator \( p \) exists.

In summary, the loop in lines 5–7 of Algorithm 10 can be described in more detail as follows:

5a Let \( Q \subseteq \tilde{C} \) be a set containing exactly one root \( \alpha \in \tilde{C} \) for each irreducible factor \( p \) of \( \ell_r \).
5b While \( Q \neq \emptyset \), do the following:
5c For all \( \alpha \in Q \), do the following:
6a Let \( b_1, \ldots, b_r \) be a fundamental system of \( L \) in \( C(\alpha)[[x - \alpha]] \).
6b With variables \( a_0, \ldots, a_{d-1} \), form the series

\[
(a_0B_0 + \cdots + a_{d-1}B_{d-1} + B_d)b_i
\]

for \( i = 1, \ldots, r \).
6c Construct a linear system for \( a_0, \ldots, a_{d-1} \) by equating the coefficients of all the non-integral terms in these series to zero.
7a If the system has a solution \( (a_0, \ldots, a_{d-1}) \in C(\alpha)^d \).
7b Let \( p \) be the minimal polynomial of \( \alpha \) over \( C \).
7c Replace each \( a_i \in C(\alpha) = C[x]/(p) \) by the corresponding polynomial in \( C[x] \) of degree less than \( \deg(p) \).
7d Replace \( B_d \) by \( \frac{1}{p}(a_0B_0 + \cdots + a_{d-1}B_{d-1} + B_d) \).
7e Otherwise discard \( \alpha \) from \( Q \).

Despite being more detailed than the listing given in Algorithm 10, these lines are still somewhat conceptual. An actual implementation cannot just “let” \( b_i \) be some infinite series object, and it does not need to. What we need are only the terms of \( b_i \) that give rise to some non-integral terms of \( (a_0B_0 + \cdots + a_{d-1}B_{d-1} + B_d)b_i \). These are only finitely many by Proposition 3, and in the next section we address the question how many terms of \( b_i \) we need to compute.

7. BOUNDS

In the algebraic case, van Hoeij [12] derives a-priori bounds on the orders to which the \( b_i \) have to be calculated. He then computes their terms once and for all at the very beginning of the algorithm to avoid their recomputation inside the loop. He also suggests that the terms of \( B_j \cdot b_i \) for \( j < d \) should not be recomputed but cached.

Nowadays, in an object-oriented programming environment, the algorithm can be implemented in such a way that recomputations of series terms are avoided even when no a-priori bound on the truncation order is available, via the paradigm of lazy series [4, 11].

Nevertheless it is desirable to have a-priori bounds available also in the D-finite case. A rough bound follows immediately from the discussion in Section 4: as we have seen, the Wronskian \( w_{r, \alpha} \) \( (B_0, sDB_0, \ldots, s^{r-1}D^{r-1}B_0) \) gives a denominator bound for the elements of the integral basis. More refined bounds are elaborated in the following.

Let \( \alpha \in \tilde{C} \) be a root of the leading coefficient \( \ell_r \) and \( \{b_1, \ldots, b_r\} \subseteq C(\alpha)[[x - \alpha]] \) be a fundamental system of \( L \):

\[
b_i = \sum_{k=0}^{\infty} b_{i,k}(\log(x - \alpha))^{v_i+k}, \quad b_{i,0} \neq 0, \quad (3)
\]

where \( b_{i,k} \in C(\alpha)[\log(x - \alpha)] \) are polynomials in log\((x - \alpha)\) such that for each \( i \) the degrees of \( b_{i,0}, b_{i,1}, \ldots \) are bounded by some integer \( d_i \). According to step 5c, we have to consider each \( \alpha \in Q \) separately, so for the rest of this section we fix such an \( \alpha \).

In step 6a we want to replace \( b_1, \ldots, b_r \) by truncated series \( t_1, \ldots, t_r \) of the form

\[
t_i = \sum_{k=0}^{N_i} b_{i,k}(\log(x - \alpha))^{v_i+k} \quad \text{with } N_i \in \mathbb{N}. \quad (4)
\]

The bounds \( N_i \) must be chosen such that this replacement does not change the result of the algorithm. The only critical step is when \( b_1, \ldots, b_r \) to test the integrality of certain elements from the algebra \( C(\alpha)[D]/(L) \), which are not known in advance. Theorem 20 gives a sufficient condition that allows us to use \( t_i \) instead of \( b_i \) in the integrality test, by asserting that its answer does not change, whatever element of \( C(\alpha)[D]/(L) \) we consider. For brevity, let \( R \) denote the ring \( C(\alpha)[[x - \alpha]]/\log(x - \alpha)] \) in the subsequent reasoning.

Lemma 19. Let \( \{b_1, \ldots, b_r\} \subseteq C(\alpha)[[x - \alpha]] \) be a fundamental system of the form \( (3) \) with \( v_i \) as above, and let \( W_k = (D^{r-1}b_1)_{1 \leq i \leq r, 0 \leq j < r} \). Then there exists an \( m \in \mathbb{N} \) such that

\[
det(W_k) = \sum_{k=0}^{\infty} w_k (x - \alpha)^{v_1+\cdots+v_r-r(r-1)/2+m+k}
\]

with \( w_0 \neq 0 \).

Proof. For the \((i, j)\)-entry of \( W_k \) we have

\[
(W_k)_{i,j} = D^{r-1} \cdot b_i \in (x - \alpha)^{v_i+1}R
\]

and therefore

\[
det(W_k) \in (x - \alpha)^{v_1+\cdots+v_r-r(r-1)/2}R.
\]
Note that \( \det(W_b) \neq 0 \) because it is precisely the Wronskian of \( b_1, \ldots, b_r \). It follows that a unique \( m \geq 0 \) with the desired property exists.

**Theorem 20.** Let \( L \in C(x)[D] \) be an operator of order \( r \) and \( b_1, \ldots, b_r \in C(\alpha) [[x - \alpha]] \) be a fundamental system of \( L \) with \( \nu_i \) and \( d_i \) as above. Moreover, let \( m \in \mathbb{N} \) be as in Lemma 19 and let \( N_1, \ldots, N_r \in \mathbb{N} \) be given by

\[
N_i = m + \max_{0 \leq j \leq d_i + r} \left( (\nu_i - \nu_j + \mathbb{Z}, k) - (\nu_i - \nu_j) \right).
\]

If \( t_i \) is the truncation (4) of \( b_i \) at order \( N_i \), for \( 1 \leq i \leq r \), then for all \( b \in C(x)[D]/(L) \) we have the equivalence:

\[
\forall i \colon B \cdot b_i \text{ is integral} \iff \forall i \colon B \cdot t_i \text{ is integral}. \quad (5)
\]

**Proof.** We introduce the matrix \( W_b = (D^j \cdot b_i)_{1 \leq i \leq r, 0 \leq j < r} \) as before, and the short notation \( B \cdot b = (B \cdot b_1, \ldots, B \cdot b_r) \). Analogously we define \( W_t \) and \( B \cdot t \). A vector resp. matrix is called integral if all its entries are integral. If \( c \) is the coefficient vector of \( B \cdot b \), i.e., \( c \cdot (1, D, \ldots, D^{r-1}) = B \cdot t \), then we have \( B \cdot b = W_b c \) and \( B \cdot t = W_t c \). Combining these two equations we get

\[
B \cdot t = W_t W_b^{-1} (B \cdot b).
\]

Setting \( Z = W_b - W_t \) yields

\[
W_t W_b^{-1} = \text{Id}_r - ZW_b^{-1}. \quad (7)
\]

The proof is split into two parts, according to the two directions of the equivalence (5).

**Part 1:** If we assume that \( B \cdot b \) is integral, then (6) exhibits that the integrality of \( W_t W_b^{-1} \) is a sufficient condition to conclude that also \( B \cdot t \) is integral, using Proposition 3. By (7) it suffices to show that \( ZW_b^{-1} \) is integral. First of all we have to argue that \( W_b^{-1} \in C(\alpha) [[x - \alpha]]^{r \times r} \) since otherwise Definition 1 would not be applicable. In Section 4 we have remarked that the Wronskian \( \det(W_b) \) is hyperexponential. In particular, it involves no logarithmic terms and therefore is invertible in \( C(\alpha) [[x - \alpha]] \). Using Cramer’s rule we find that

\[
(W_b^{-1})_{i,j} = (-1)^{i+j} \frac{\det W_b^{[i,j]}}{\det W_b} \in (x - \alpha)^{i+j-r-1} R, \]

where \( W_b^{[i,j]} \) is the matrix obtained by deleting row \( j \) and column \( i \) from \( W_b \). So the entries of \( W_b^{-1} \) are series in \( C(\alpha) [[x - \alpha]] \). The fact that \( \det W_b^{[i,j]} \) satisfies a differential equation of order less than or equal to \( r \) implies that the highest power of \( log(x - \alpha) \) that can appear in the entries of \( W_b^{-1} \) is \( r - 1 \). On the other hand, it is easy to see that \( Z_{i,j} \in (x - \alpha)^{i+j-N_i-r-2} R \), so it follows that

\[
(ZW_b^{-1})_{i,j} \in (x - \alpha)^{i+j-r-\nu_i - n_i-m+1} R, \quad (8)
\]

and that herein \( \log(x - \alpha) \) appears with exponent at most \( d_i + r - 1 \). By our choice of \( N_i \) the series in (8) is integral for all \( 1 \leq i, j \leq r \) and therefore the whole matrix \( ZW_b^{-1} \).

**Part 2:** Now assume that \( B \cdot b \) is not integral. Then from

\[
B \cdot t = (\text{Id}_r - ZW_b^{-1})(B \cdot b) = B \cdot b - (ZW_b^{-1})(B \cdot b)
\]

it follows that \( B \cdot t \) is non-integral as well. To see this, let \( n \) be the largest integer such that a term of the form \( (x - \alpha)^{n(x+r+k)+\mathbb{Z},\alpha} \log(x - \alpha)^{k} \) appears in \( B \cdot b \) for some \( \mu \in \mathbb{C} \) and \( k \in \mathbb{N} \). Let \( i \) be an index such that the term of the given form appears in \( B \cdot b \) with nonzero coefficient. This term cannot be canceled in

\[
B \cdot t_i = B \cdot b_i - \sum_{j=1}^{r} (ZW_b^{-1})_{i,j}(B \cdot b_j)
\]

because all terms of the series \((ZW_b^{-1})_{i,j}\) are of the form \((x - \alpha)^{\nu_i - \nu_j + \mathbb{Z}, \alpha} \log(x - \alpha)^{\nu_i - \nu_j} \).

\[
\text{8. COMPARISON WITH THE ALGEBRAIC CASE}
\]

We have shown that the underlying ideas of van Hoeij’s algorithm for computing integral bases of algebraic function fields apply in a more general context. Indeed, it is fair to regard van Hoeij’s algorithm as a special case of our algorithm, since every algebraic function field is also D-finite. Recall that an algebraic function field \( C(x)[Y]/\langle M \rangle \) with some irreducible polynomial \( M \) of degree \( d \) becomes a differential field if we set \( D \cdot c = 0 \) for all \( c \in C \), \( D \cdot x = 1 \), and

\[
D \cdot Y := \frac{\partial M}{\partial x} \mod M.
\]

Since \( C(x)[Y]/\langle M \rangle \) is also a \( C(x) \)-vector space of dimension \( d \), it is clear that any \( d + 1 \) elements must be \( C(x) \)-linearly independent. This implies the existence of an operator \( L \in C(x)[D] \) of order at most \( d \) with \( L \cdot Y = 0 \). Usually there is no such operator of lower order, which means that \( Y, D \cdot Y, \ldots, D^{d-1} \cdot Y \) are \( C(x) \)-linearly independent and thus a basis of \( C(x)[Y]/\langle M \rangle \). In this case, a vector space basis \( \{B_1, \ldots, B_d \} \subseteq C(x)[Y]/\langle M \rangle \) is an integral basis in the sense of Definition 6 if and only if \( \{B_1 \cdot Y, \ldots, B_d \cdot Y \} \subseteq C(x)[Y]/\langle M \rangle \) is an integral basis of the algebraic function field in the classical sense.

When \( Y \in C(x)[Y]/\langle M \rangle \) is annihilated by an operator \( L \) of order less than \( d \), we can compute the minimal-order operators \( L_0, \ldots, L_{d-1} \) which annihilate \( Y^n, \ldots, Y^{d-1} \), respectively, and take \( L = \text{lcm}(L_0, \ldots, L_{d-1}) \). Then the \( C(x) \)-vector space generated by all solutions of \( L \) is the whole field \( C(x)[Y]/\langle M \rangle \), and if \( \{B_1, \ldots, B_d \} \) is an integral basis for \( L \), then \( \{B_1 \cdot Y, \ldots, B_d \cdot Y \} \) generates the \( C(x) \)-module of all integral elements of \( C(x)[Y]/\langle M \rangle \). As a less brutal approach, we can simply replace \( Y \) by some other generator of the field. In practice, most field generators will have an annihilating operator of order \( d \), but none of smaller order.

**Example 21.** An integral basis for the field \( \mathbb{Q}(x)[Y]/\langle M \rangle \) with \( M = Y^3 - x^2 \) is \( \{1, Y, \frac{1}{2} Y^2 \} \). The lowest-order differential operator annihilating \( Y \) is \( L = 3x \cdot D - 2 \), which is not useful because its order is less than the degree of \( M \).

Instead, let us try \( Z := 1 + Y + Y^2 \) as generator. We have \( \mathbb{Q}(x)[Y]/\langle M \rangle = \mathbb{Q}(x)[Z]/\langle N \rangle \), where \( N = Z^3 - 3Z^2 - 3(x^2 - 1)Z - x^2 + 2x^2 - 1 \) is the minimal polynomial of \( Z \). Given \( N \) instead of \( M \) as input, hoeij’s algorithm finds the following integral basis for \( \mathbb{Q}(x)[Z]/\langle N \rangle \):

\[
\left\{ 1, Z, \frac{Z^2}{x(x - 1)(x + 1)}, -\frac{x^2 + 2x^2}{x(x - 1)(x + 1)} - \frac{1}{x} \right\}. \quad (9)
\]

The lowest order annihilating operator of \( Z \) is \( L = 9x^2 D^3 + 9x D^2 - D \). It has the right order and our Mathematica im-
For the derivatives of \( y \) and taking the whole equation mod \( Z \):
\[
D \cdot Z = -2Z^2 + 2(2x^2 + 1)Z \quad \text{for} \quad D = 3x(x^2 - 1)\]
\[
D^2 \cdot Z = -6Z^2 + 2(2(x^2 + 7))Z + 8(x^2 - 1) \quad \text{for} \quad 9x^2(x^2 - 1).
\]

Plugging these expressions into \( (9) \) yields the following integral basis for the algebraic function field \( \mathbb{Q}(x)[Z]/(N) \):
\[
\left\{ -2x^2 + 2(2x^2 + 1)Z, 8(-Z^2 + (x^2 + 2)Z + x^2 - 1) \right\} \quad \text{for} \quad 9x(x-1)(x+1)Z.
\]

Applying a change of basis with the unimodular matrix
\[
\begin{pmatrix}
1 & 8 & -12 & 9x \\
8 & 0 & 0 & 0 \\
0 & 0 & -9 & 0
\end{pmatrix}
\]
gives the integral basis \( (9) \) computed by Maple.

One of the features of integral bases for algebraic function fields is that they allow an extension of the classical Hermite reduction for integration of rational functions to the case of algebraic functions. This was observed by Trager [10]. In order to make this work, Trager requires that both the integral basis as well as the integrand should be “normal at infinity”. This corresponds to the condition in the rational case that the rational function to be integrated must not have a polynomial part. Trager shows that normality of the integrand can always be achieved by applying a suitable change of variables, and he gives an algorithm that turns an arbitrary integral basis into one that is normal at infinity. After that, the Hermite reduction process looks very similar to the rational case. We give here an example for a non-algebraic \( D \)-finite function.

**Example 22.** Let \( L = (2x + 1) - (4x^2 + 1)D + 2(2x - 1)xD^2 \) and write \( y \) for a solution of \( L \). An integral basis of \( \mathcal{O}_L \) is given by \( \{1, \frac{1}{2x^2 - 1}(2xD - 1)\} \). Let \( \omega_0 := y \) and \( \omega_1 := \frac{1}{x^2 - 1}(2xD - 1) \cdot y \) and consider the function
\[
f = \frac{a_0 \omega_0 + a_1 \omega_1}{uv^m}
\]
where \( a_0 = 4x^2 + 37x - 11, a_1 = -28x^3 + 40x^2 - x - 1, u = 4, v = (x - 1)x, m = 2.\)

Hermite reduction consists in finding \( b_0, b_1, c_0, c_1 \in \mathbb{Q}[x] \) with
\[
\frac{a_0 \omega_0 + a_1 \omega_1}{uv^m} = \left( b_0 \omega_0 + b_1 \omega_1 \right) + \left( c_0 \omega_0 + c_1 \omega_1 \right).
\]

After working out the differentiation, multiplying by \( uv^m \), and taking the whole equation mod \( v \) we are left with the constraint
\[
a_0 \omega_0 + a_1 \omega_1 \equiv b_0 uv^m \left( \omega_0 \frac{\omega_1}{uv^m} \right) + b_1 uv^m \left( \omega_1 \frac{\omega_0}{uv^m} \right) \mod v
\]

For the derivatives of \( \omega_0 \) and \( \omega_1 \) we have
\[
D\omega_0 = \frac{1}{2x} \omega_0 - \frac{1}{2x} \omega_1, \quad D\omega_1 = \omega_1,
\]
so that the previous constraint can be rewritten to
\[
a_0 \omega_0 + a_1 \omega_1 \equiv -\frac{1}{2} b_0 uv(3\omega_0 + \omega_1) - 2b_1 u \omega_1 \mod v.
\]

Plugging in \( a_0, a_1 \) and \( u \) and comparing coefficients of \( \omega_i \) leads to the linear system
\[
\begin{pmatrix}
41x - 11 \\
11x - 1
\end{pmatrix} \equiv \begin{pmatrix}
2 - 6x \\
0
\end{pmatrix} \begin{pmatrix}
b_0 \\
b_1
\end{pmatrix} \mod v
\]

which has the solution \( b_0 = \frac{1}{2}(4x + 11), b_1 = \frac{5}{2}(2x - 1) \). Next we find that
\[
f - \frac{b_0 \omega_0 + b_1 \omega_1}{uv^m} = c_0 \omega_0 + c_1 \omega_1
\]
for \( c_0 = 0, c_1 = 0 \). Consequently, we have found that
\[
\int f = (11 + 4x)\omega_0 + 5(2x - 1)\omega_1
\]
\[
\frac{5}{x - 1} y' - \frac{2x + 3}{(x - 1)^2} y.
\]
The same answer could have been found using an algorithm of Abramov and van Hoeij [1], using a completely different approach.

9. REFERENCES