ON SOLUTIONS OF LINEAR ORDINARY DIFFERENTIAL EQUATIONS IN THEIR COEFFICIENT FIELD

MANUEL BRONSTEIN

Institut für Wissenschaftliches Rechnen
ETH Zentrum, CH-8092 Zürich, Switzerland

(Received 18 December 1990)

We describe a rational algorithm for finding the denominator of any solution of a linear ordinary differential equation in its coefficient field. As a consequence, there is now a rational algorithm for finding all such solutions when the coefficients can be built up from the rational functions by finitely many algebraic and primitive adjunctions. This also eliminates one of the computational bottlenecks in algorithms that either factor or search for Liouvillian solutions of such equations with Liouvillian coefficients.

INTRODUCTION

A fundamental problem in the theory of differential equations is to determine whether a given differential equation of a certain kind has a "closed form" solution, where the term "closed form" can take on a variety of meanings. In this paper, we consider the following specific subproblem in this area: given a differential field k, $g \in k$, and a linear ordinary differential operator L with coefficients in k, can we decide in a finite number of steps whether $L(y) = g$ has a solution in k, and in the affirmative, can we find one (or all) such solution(s)?

More precisely, we consider the particular case where k is a simple monomial extension of an underlying differential field. This problem was already solved for elementary and (a certain class of) Liouvillian function fields by Singer (1991). In this paper, we make that algorithm rational for towers of algebraic and primitive extensions.

As applications we get,

(i) there is now a rational algorithm for solving Risch differential equations on algebraic curves over algebraic/primitive function fields. That algorithm

is an effective alternative to the ones presented in Risch (1968), Davenport (1984) and Bronstein (1990*a*);
(ii) the linear differential operator factoring algorithm of Schwarz (1989) is now more effective, and can thus be used with more general constant fields.

To get the most general result possible, we use the language of monomial extensions introduced in (Bronstein, 1990*b*). In some sense, this paper continues the theory introduced there by studying the relations between the orders at various places of y and $L(y)$, where L is a linear ordinary differential operator.

1. Valuations

Let k be a field of characteristic 0, and x be transcendental over k. In this section, we recall the notions of order and local ring at a "point" of $k(x)$.

Let $P \in k[x] \setminus k$. We define the **order at P** to be the map $\nu_P : k(x) \to \mathbf{Z} \cup \{+\infty\}$ defined by:

(i) for $Q \in k[x] \setminus \{0\}, \nu_P(Q) = n \geq 0$ such that $P^n \mid Q$ and $P^{n+1} \not| Q$,
(ii) for $f \in k(x) \setminus \{0\}$, $\nu_P(f) = \nu_P(A) - \nu_P(B)$, where for $A, B \in k[x]$, $(A, B) = (1)$ and $f = A/B$,
(iii) $\nu_P(0) = +\infty$.

Note that in general, this order function does not satisfy the logarithmic multiplicative identity that valuations satisfy. For example, $\nu_{x^2+x}(x) = \nu_{x^2+x}(x+1) = 0$, but $\nu_{x^2+x}(x(x+1)) = 1$. If P is irreducible, then ν_P is called the **P-valuation**, and it satisfies the following properties:

(1) for $Q \in k[x], \nu_P(Q) > 0 \Rightarrow \nu_P(\frac{\partial Q}{\partial x}) = \nu_P(Q) - 1$,
(2) for $A, B \in k[x] \setminus \{0\}, \nu_P(\gcd(A, B)) = \min(\nu_P(A), \nu_P(B))$,
(3) for $f, g \in k(x), \nu_P(fg) = \nu_P(f) + \nu_P(g)$,
(4) for $f, g \in k(x), \nu_P(f + g) \geq \min(\nu_P(f), \nu_P(g))$, and equality holds if $\nu_P(f) \neq \nu_P(g)$.

Recall also that the **∞-valuation** is a map $\nu_\infty : k(x) \to \mathbf{Z} \cup \{+\infty\}$ defined by $\nu_\infty(\frac{A}{B}) = \deg(B) - \deg(A)$ for $A, B \in k[x] \setminus \{0\}$, and $\nu_\infty(0) = +\infty$. It satisfies the following properties:

(1) for $Q \in k[x], \deg(Q) > 0 \Rightarrow \nu_\infty(\frac{\partial Q}{\partial x}) = \nu_\infty(Q) + 1$,
(2) for $A, B \in k[x] \setminus \{0\}, \nu_\infty(\gcd(A, B)) \geq \max(\nu_\infty(A), \nu_\infty(B))$,
(3) for $f, g \in k(x), \nu_\infty(fg) = \nu_\infty(f) + \nu_\infty(g)$,
(4) for $f, g \in k(x), \nu_\infty(f + g) \geq \min(\nu_\infty(f), \nu_\infty(g))$, and equality holds if $\nu_\infty(f) \neq \nu_\infty(g)$.

Let $P \in k[x] \setminus \{0\}$. We write ϕ_P for the canonical homomorphism from $k[x]$ onto $k[x]/(P)$ (the *reduction modulo* P). If P is irreducible, then the *local ring at* P is

$$\mathcal{O}_P = \{f \in k(x) \text{ such that } \nu_P(f) \geq 0\}.$$

If P is not irreducible, we define the *local ring at P* to be

$$\mathcal{O}_P = \bigcap_{Q|P} \mathcal{O}_Q$$

where the intersection is taken over all the irreducible factors of P in $k[x]$. ϕ_P can be extended to a ring-homomorphism from $\mathcal{O}_P$ onto $k[x]/(P)$ as follows: let $f \in \mathcal{O}_P$ and write $f = A/B$ where $A, B \in k[x]$ and $(A, B) = (1)$. By definition of $\mathcal{O}_P$, $(B, Q) = (1)$ for any irreducible factor Q of P. Hence, $(B, P) = (1)$, so we can compute (by the extended Euclidean algorithm) $C, R \in k[x]$ such that $BC + PR = 1$. We then define $\phi_P(f)$ to be $\phi_P(AC)$. It is easily checked that ϕ_P is well-defined on $\mathcal{O}_P$ and is a ring-homomorphism.

For an analogue of ϕ_P at infinity, we define the *local ring at infinity* to be

$$\mathcal{O}_\infty = \{f \in k(x) \text{ such that } \nu_\infty(f) \geq 0\}.$$

(x^{-1}) is a maximal ideal of $\mathcal{O}_\infty$, so $\mathcal{O}_\infty/(x^{-1})$ is a field. It is isomorphic to k, and, for any $f \in \mathcal{O}_\infty$, we define the *value of f at infinity* to be the image of f under the canonical map from $\mathcal{O}_\infty$ onto $\mathcal{O}_\infty/(x^{-1}) = k$, and we denote it $\phi_\infty(f)$. We note that if we write $f \in k(x)$ as

$$f = \frac{a_n x^n + \cdots + a_0}{b_m x^m + \cdots + b_0}$$

where $a_i, b_j \in k$, $a_n \neq 0$, and $b_m \neq 0$, then, if $f \in \mathcal{O}_\infty$, $m \geq n$, and $\phi_\infty(f)$ is given by

$$\phi_\infty(f) = \begin{cases} \dfrac{a_n}{b_m}, & \text{if } m = n \\ 0, & \text{if } m > n. \end{cases}$$

It is easily checked that ϕ_∞ is a ring-homomorphism from $\mathcal{O}_\infty$ onto k.

2. Balanced factorization

We present in this section Abramov's (1989) algorithm for computing balanced factorizations. Let k be a field of characteristic 0, and x be transcendental over k.

Definition 2.1. *Let $A, B \in k[x]$. We say that A is* **balanced** *with respect to B if either $B = 0$ or $\nu_P(B) = \nu_Q(B)$ for any two irreducible factors $P \in k[x] \setminus k$ and $Q \in k[x] \setminus k$ of A. We also say that $A = {A_1}^{e_1} \cdots {A_n}^{e_n}$ is a* **balanced factorization** *of A with respect to B, if A_i is balanced w.r.t. B and squarefree for $i = 1 \ldots n$, and $(A_i, A_j) = (1)$ for $i \neq j$.*

We can make the following immediate remarks:

(i) If A is balanced w.r.t. B, then so is every factor of A.
(ii) If $(A, B) = (1)$, then A is balanced w.r.t. B.
(iii) Any $A \in k[x]$ is balanced w.r.t. 0.
(iv) A squarefree factorization of A is a balanced factorization of A w.r.t. A.

The following Lemma shows that we can test whether a polynomial is balanced without computing its irreducible factors.

Lemma 2.2. *Let $A, B \in k[x]$. The following are equivalent:*

(i) *A is balanced w.r.t. B.*
(ii) *Let C be a squarefree factor of A, then $\nu_P(B) = \nu_C(B)$ for any irreducible factor $P \in k[x]$ of C,*
(iii) *$\nu_P(B) = \nu_Q(B)$ for any two squarefree factors P and Q of A.*

Proof. (i) $\Longrightarrow$ (ii): Suppose that A is balanced w.r.t. B, and let C be a squarefree factor of A. Let $C = P_1 \cdots P_n$ be a prime factorization of C. Then, for any i, j in $\{1, \dots, n\}$ we have $\nu_{P_i}(B) = \nu_{P_j}(B)$, so $\nu_C(B) = \nu_{P_1}(B) = \cdots = \nu_{P_n}(B)$.

(ii) $\Longrightarrow$ (iii): Let P and Q be any squarefree factors of A. Let $G = \gcd(P, Q)$ and write $P = G\overline{P}$, $Q = G\overline{Q}$. Since P and Q are squarefree, we have $G, \overline{P}, \overline{Q}$ are squarefree, and $(\overline{P}, G) = (\overline{Q}, G) = (\overline{P}, \overline{Q}) = (1)$. Thus, $C = G\overline{P}\overline{Q}$ is squarefree. Let $P = P_1 \cdots P_n$ and $Q = Q_1 \cdots Q_m$ be prime factorizations of P and Q. Then, for any i in $\{1, \dots, n\}$ and any j in $\{1, \dots, m\}$ we have $P_i \mid C$ and $Q_j \mid C$, so, by (ii), $\nu_{P_i}(B) = \nu_C(B) = \nu_{Q_j}(B)$. Thus, $\nu_P(B) = \nu_C(B) = \nu_Q(B)$.

(iii) $\Longrightarrow$ (i): if $\nu_P(B) = \nu_P(A)$ for any two squarefree factors P and Q of A, then it is also true for any two irreducible factors, so A is balanced w.r.t. B.

We now show how to compute a balanced factorization of a squarefree polynomial w.r.t. any polynomial.

Lemma 2.3. *Let $A \in k[x]$ be squarefree and $B \in k[x]$. Then, using only gcd computations in $k[x]$, one can compute a balanced factorization of A w.r.t. B in finitely many steps.*

Proof. If $B = 0$, then $A = A$ is a balanced factorization of A w.r.t. B. Otherwise, we proceed by induction on $\deg(B)$.

$\deg(B) = 0$: Then, $A = A$ is balanced w.r.t B since $(A, B) = (1)$.

$\deg(B) > 0$: If $(A, B) = (1)$, then $A = A$ is balanced w.r.t. B. Otherwise, let $G = \gcd(A, B)$, and write $A = G\overline{A}$ and $B = G^\beta \overline{B}$ where $\beta = \nu_G(B) > 0$. Since $\deg(G) > 0$, then $\deg(\overline{B}) < \deg(B)$, so let $G = G_1 \cdots G_m$ be a balanced factorization of G w.r.t. $\overline{B}$ by induction. Let $i \in \{1, \dots, m\}$ and P, Q be irreducible factors of G_i. Since G_i is balanced w.r.t. $\overline{B}$, we have $\nu_P(\overline{B}) = \nu_Q(\overline{B})$. Therefore, $\nu_P(B) = \beta + \nu_P(\overline{B}) = \beta + \nu_Q(\overline{B}) = \nu_Q(B)$, so G_i is balanced w.r.t. B. Since A is squarefree, $(G, \overline{A}) = (1)$, so $(G_i, \overline{A}) = (1)$. We also have $(\overline{A}, B) = (1)$, so $\overline{A}$ is balanced w.r.t. B, so $A = \overline{A} G_1 \cdots G_m$ is a balanced factorization of A w.r.t. B.

Definition 2.4. *Let $A \in k[x]$ and $\mathcal{S} \subseteq k[x]$. We say that A is* **balanced** *with respect to $\mathcal{S}$ if A is balanced w.r.t. B for any $B \in \mathcal{S}$. We also say that $A = {A_1}^{e_1} \cdots {A_n}^{e_n}$ is a* **balanced factorization** *of A with respect to $\mathcal{S}$, if A_i is balanced w.r.t. $\mathcal{S}$ and squarefree for $i = 1 \dots n$, and $(A_i, A_j) = (1)$ for $i \neq j$.*

Obviously, if $A \in k[x]$ is balanced w.r.t. $\mathcal{S} \subseteq k[x]$, and A is balanced w.r.t. $\mathcal{T} \subseteq k[x]$, then A is balanced w.r.t. $\mathcal{S} \cup \mathcal{T}$. We now show how to compute a balanced factorization of a squarefree polynomial w.r.t. any finite set of polynomials.

Lemma 2.5. *Let $A \in k[x]$ be squarefree and $\mathcal{S} \subseteq k[x]$ be finite. Then, using only gcd computations in $k[x]$, one can compute a balanced factorization of A w.r.t. $\mathcal{S}$ in finitely many steps.*

Proof. If $\mathcal{S}$ is empty, then $A = A$ is a balanced factorization of A w.r.t. $\mathcal{S}$. Otherwise, we proceed by induction on $|\mathcal{S}|$.

$|\mathcal{S}| = 1$: Then, $S = \{B\}$ for some $B \in k[x]$, so Lemma 2.3 gives us a balanced factorization of A w.r.t. $\mathcal{S}$.

$|\mathcal{S}| > 1$: Let $B \in \mathcal{S}$ and $\mathcal{T} = \mathcal{S} \setminus \{B\}$. Since $|\mathcal{T}| < |\mathcal{S}|$, we compute a balanced factorization $A = A_1 \cdots A_m$ of A w.r.t. $\mathcal{T}$ by induction. Now, for $i = 1 \ldots m$, compute (using Lemma 2.3) a balanced factorization $A_i = A_{i1} \cdots A_{im_i}$ of A_i w.r.t. B. For any i, j, we have A_{ij} is balanced w.r.t. B. But $A_{ij} \mid A_i$ and A_i is balanced w.r.t. $\mathcal{T}$, so A_{ij} is balanced w.r.t. $\mathcal{T}$, so A_{ij} is balanced w.r.t. $\mathcal{S}$. Thus,

$$A = \prod_{i=1}^{m} \prod_{j=1}^{m_i} A_{ij}$$

is a balanced factorization of A w.r.t. $\mathcal{S}$.

We can finally show how to compute a balanced factorization of a polynomial w.r.t. any finite set of polynomials.

Theorem 2.6. *Let $A \in k[x]$ and $\mathcal{S} \subseteq k[x]$ be finite. Then, using only gcd computations in $k[x]$, one can compute a balanced factorization of A w.r.t. $\mathcal{S}$ in finitely many steps.*

Proof. Let $A = A_1 A_2{}^2 \cdots A_n{}^n$ be a squarefree factorization of A. For $i = 1 \ldots n$, compute (using Lemma 2.5) a balanced factorization $A_i = A_{i1} \cdots A_{in_i}$ of A_i w.r.t. $\mathcal{S}$. Then,

$$A = \prod_{i=1}^{n} \prod_{j=1}^{n_i} A_{ij}{}^i$$

is a balanced factorization of A w.r.t. $\mathcal{S}$.

We can extend the notion of balanced to fractions in the natural way.

Definition 2.7. *Let $A \in k[x]$, $f \in k(x)$, and $\mathcal{S} \subseteq k(x)$. We say that A is* **balanced** *with respect to f if A is balanced w.r.t. B and C, where $B, C \in k[x]$, $(B, C) = (1)$ and $f = B/C$. We say that A is* **balanced** *with respect to $\mathcal{S}$ if A is balanced w.r.t. f for any $f \in \mathcal{S}$. We also say that $A = A_1{}^{e_1} \ldots A_n{}^{e_n}$ is a* **balanced factorization** *with respect to f (resp. $\mathcal{S}$), if A_i is balanced w.r.t. f (resp. $\mathcal{S}$) and squarefree for $i = 1 \ldots n$, and $(A_i, A_j) = (1)$ for $i \neq j$.*

This definition is motivated by the following property.

Lemma 2.8. *Let $A \in k[x]$ and $f \in k(x)$. The following are equivalent:*

(i) *A is balanced w.r.t. f.*
(ii) *$\nu_P(f) = \nu_Q(f)$ for any two squarefree factors P and Q of A.*
(iii) *$\nu_P(f) = \nu_Q(f)$ for any two irreducible factors P and Q of A.*

Proof. Let $f \in k(x)$ and write $f = B/C$ where $B, C \in k[x]$ and $(B, C) = (1)$.

$(i) \implies (ii)$: Suppose that A is balanced w.r.t. f, and let P and Q be squarefree factors of A. By Lemma 2.2, $\nu_P(B) = \nu_Q(B)$ and $\nu_P(C) = \nu_Q(C)$. Hence, $\nu_P(f) = \nu_Q(f)$.

$(ii) \implies (iii)$: If $\nu_P(f) = \nu_Q(f)$ for any two squarefree factors P and Q of A, then it is also true for any two irreducible factors of A.

$(iii) \implies (i)$: Suppose that A is not balanced w.r.t. f. Then A is not balanced w.r.t. to at least one of B or C, say B. Thus, there exist two irreducible factors P and Q of A such that $\nu_P(B) \neq \nu_Q(B)$. Then, at least one of $\nu_P(B), \nu_Q(B)$ is non-zero, say $\nu_P(B) > 0$. Since $(B, C) = (1)$, we must have $\nu_P(C) = 0$, so $\nu_P(f) = \nu_P(B) > 0$. If $\nu_Q(B) = 0$, then $\nu_Q(f) \le 0$, so $\nu_P(f) \neq \nu_Q(f)$. Otherwise, $\nu_Q(B) > 0$, so $\nu_Q(C) = 0$, so $\nu_Q(f) = \nu_Q(B) \neq \nu_P(B)$. Thus $\nu_P(f) \neq \nu_Q(f)$ in both cases.

The algorithm of Theorem 2.6 can be used to compute balanced factorizations w.r.t. any finite set of fractions.

Corollary 2.9. *Let $A \in k[x]$ be monic and $\mathcal{S} \subseteq k(x)$ be finite. Then, using only gcd computations in $k[x]$, one can compute a balanced factorization of A w.r.t. $\mathcal{S}$ in finitely many steps.*

Proof. Write each $f \in \mathcal{S}$ as $f = B_f/C_f$ where $B_f, C_f \in k[x]$ and $(B_f, C_f) = (1)$. Using Theorem 2.6, compute a balanced factorization of A w.r.t. $\bigcup_{f \in \mathcal{S}} \{B_f, C_f\}$. This factorization is then balanced w.r.t. $\mathcal{S}$ by definition.

The reason for requiring the factors to be squarefree in a balanced factorization is that non-trivial squarefree balanced polynomials have the following additional properties.

Lemma 2.10. *Let $P \in k[x] \setminus k$ be squarefree and $f, g \in k(x) \setminus \{0\}$. Then,*

(i) *P balanced w.r.t. $f \iff \nu_Q(fP^{-\nu_P(f)}) = 0$ for any irreducible factor Q of P in $k[x]$,*
(ii) *P balanced w.r.t. $f \implies fP^{-\nu_P(f)} \in \mathcal{O}_P$,*
(iii) *P balanced w.r.t. $\{f, g\} \implies \nu_P(fg) = \nu_P(f) + \nu_P(g)$.*

Proof. Let Q be any irreducible factor of P. Since P is squarefree, $\nu_Q(P) = 1$, so $\nu_Q(fP^{-\nu_P(f)}) = \nu_Q(f) - \nu_P(f)\nu_Q(P) = \nu_Q(f) - \nu_P(f)$.

(i): Suppose that P is balanced w.r.t. f. Then, by Lemma 2.8, $\nu_Q(f) = \nu_P(f)$. Hence, $\nu_Q(fP^{-\nu_P(f)}) = 0$. Conversely, suppose that $\nu_Q(fP^{-\nu_P(f)}) = 0$. Then, $\nu_Q(f) = \nu_P(f)$. Since this holds for any irreducible factor Q of P, P is balanced w.r.t. f by Lemma 2.8.

(ii): Suppose that P is balanced w.r.t. f. Then, by (i), $\nu_Q(fP^{-\nu_P(f)}) = 0$, so $fP^{-\nu_P(f)} \in \mathcal{O}_Q$. Since this holds for any irreducible factor Q of P, $f \in \mathcal{O}_P$.

(iii): Let $Q \in k[x]$ be any irreducible factor of P. Then Q is squarefree, and since P is balanced w.r.t. $\{f, g\}$, we have $\nu_Q(f) = \nu_P(f)$ and $\nu_Q(g) = \nu_P(g)$ by Lemma 2.8. But Q is irreducible, so $\nu_Q(fg) = \nu_Q(f) + \nu_Q(g)$. Hence, $\nu_Q(fg) =$

$\nu_P(f)+\nu_P(g)$. Since this holds for any irreducible factor of P and P is squarefree, we have $\nu_P(fg) = \nu_P(f) + \nu_P(g)$.

The converses of (ii) and (iii) do not always hold: let $P = x(x-1)$ which is squarefree, and $f = x^2(x-1)$. Then, $\nu_P(f) = 1$ and $fP^{-1} = x \in \mathcal{O}_P$, but P is not balanced w.r.t. f since $\nu_x(f) = 2$ and $\nu_{x-1}(f) = 1$. Also, $\nu_P(f^2) = 2 = \nu_P(f) + \nu_P(f)$, while P is not balanced w.r.t. $\{f\}$.

Also, Lemma 2.10 is not true for non-squarefree polynomials: let $P = x^2(x+1)$ and $f = x^{-2}(x+1)^{-2}$. Then, $\nu_P(f) = -1$ and P is balanced w.r.t. f, but $fP = (x+1)^{-1}$ so $\nu_{x+1}(fP) = -1$, so (ii) does not hold. Let $P = x^2$ and $f = g = x$. Then P is balanced w.r.t. $\{f, g\}$ and $\nu_P(f) = \nu_P(g) = 0$, but $\nu_P(fg) = 1$, so (iii) does not hold.

The notion of a balanced factorization is connected to the notion of a square-free-gcd-free basis for a set of polynomials.

Definition 2.11. *Let $\mathcal{S} \subseteq k[x]$ be finite. A* **square-free-gcd-free** *(s.f.g.f.) basis for $\mathcal{S}$ is a finite subset $\mathcal{B}$ of $k[x]$ such that:*

(i) *every $B \in \mathcal{B}$ is squarefree,*
(ii) *$(A, B) = (1)$ for $A, B \in \mathcal{B}$, $A \neq B$,*
(iii) *every $A \in \mathcal{S}$ can be written as $A = a\prod_{B\in\mathcal{B}} B^{e_B}$ where $a \in k$ and the e_B's are non-negative integers.*

The following Theorem shows that computing a s.f.g.f. basis for a set $\mathcal{S}$ yields a balanced factorization of any element of $\mathcal{S}$ w.r.t. $\mathcal{S}$.

Theorem 2.12. *Let $\mathcal{S} \subseteq k[x]$ be finite and $\mathcal{B} \subseteq k[x]$ be a square-free-gcd-free basis for $\mathcal{S}$. Then, for any $B \in \mathcal{B}$, B is squarefree and balanced w.r.t. $\mathcal{S}$.*

Proof. Let $B \in \mathcal{B}$, then B is squarefree by definition. Let $A \in \mathcal{S}$. Then, $A = B^e \prod_{C\in\mathcal{B}\setminus\{B\}} C^{e_c}$. Let P and Q be irreducible factors of B. Since B is squarefree, then $\nu_P(B) = \nu_Q(B) = 1$. For $C \in \mathcal{B} \setminus \{B\}$ we have $(B, C) = (1)$, hence $\nu_P(C) = \nu_Q(C) = 0$, so $\nu_P(A) = \nu_Q(A) = e$, so B is balanced w.r.t. A. Hence, B is balanced w.r.t. $\mathcal{S}$.

Thus, s.f.g.f. bases are at least as fine as balanced factorizations, so they can be used instead of balanced factorizations in the algorithms of this paper: given $A \in k[x]$ and $\mathcal{S} \subseteq k[x]$ be finite, one can compute a s.f.g.f. basis $\mathcal{B}$ for $\{A\} \cup \mathcal{S}$ and the expression of A as a product of elements of $\mathcal{B}$ is a balanced factorization of A w.r.t. $\mathcal{S}$ by Theorem 2.12. On the other hand, the following example shows that computing a s.f.g.f. basis requires in general more gcd computations when only one balanced factorization is needed.

Example: Let $k = \mathbf{Q}$ be the rational number field, x be an indeterminate over k, and $A = x^2 - x$, $B = x^3 - x^2 - 2x$ and $C = x^3 + 2x^2 - x - 2$. Computing a balanced factorization of A w.r.t. B we get: $G = \gcd(A, B) = x$, $A = G(x-1)$ and $B = G(x^2 - x - 2)$. Since $\gcd(G, x^2 - x - 2) = 1$, G is balanced w.r.t. $x^2 - x - 2$, so $A = x(x-1)$ is a balanced factorization of A w.r.t. B. Since $\gcd(x, C) = 1$, x is balanced w.r.t. C, and computing a balanced factorization of

$x-1$ w.r.t. C we get: $G = \gcd(x-1, C) = x-1$ and $C = G(x^2+3x+2)$. Since $\gcd(G, x^2+3x+2) = 1$, G is balanced w.r.t. x^2+3x+2 so $x-1$ is balanced w.r.t. C so the above factorization is a balanced factorization of A w.r.t. $\{B, C\}$. But $\{x, x-1, x^2-x-2, x^2+3x+2\}$ is not a s.f.g.f. basis for $\{A, B, C\}$ since $\gcd(x^2-x-2, x^2+3x+2) = x+1$. In fact, a minimal s.f.g.f. basis for $\{A, B, C\}$ is $\{x, x-1, x-2, x+1, x+2\}$.

3. Monomial Extensions

We summarize in this section the basic definitions and results of (Bronstein, 1990*b*) regarding monomial extensions that will be used in this paper. We refer to the above paper for the proofs of all the results stated in this section.

A *differential field* is a field k with a given map $a \to a'$ from k into k, satisfying $(a+b)' = a'+b'$ and $(ab)' = a'b+ab'$. Such a map is called a *derivation* on k. An element $a \in k$ which satisfies $a' = 0$ is called a *constant*. The constants of k form a subfield of k.

A differential field K is a *differential extension of* k if $k \subseteq K$, and the derivation on K extends the one on k.

Definition 3.1. *Let k be a differential field and K be a differential extension of k. $x \in K$ is a* **monomial** *over k (with respect to $'$), if*

(i) *x is transcendental over k,*
(ii) *$k(x)$ and k have the same subfield of constants,*
(iii) *$x' = H(x)$ for some $H \in k[x]$.*

If x is a monomial over k, then the **degree** *of x is $d(x) = \deg(H)$, and the* **leading coefficient** *of x is $lc(x) =$ coefficient of $x^{d(x)}$ in H.*

If x is a monomial over k, then

(1) k must be of characteristic 0,
(2) x is also a monomial over any algebraic extension of k,
(3) $k[x]$ is closed under $'$.

In the rest of this section, $(k, ')$ is a differential field of characteristic 0 and x is a monomial over k.

Definition 3.2. *$P \in k[x]$ is* **normal** *with respect to $'$ if $(P, P') = (1)$. Otherwise, P is* **special** *(with respect to $'$).*

A **split-factorization** *of P is a factorization of the form $P = P_S P_N$ where $P_S, P_N \in k[x]$, every irreducible factor of P_S is special, and every irreducible factor of P_N is normal.*

There is an algorithm that, given $P \in k[x]$, computes a split factorization of P using only gcd computations (Bronstein, 1990*b*).

Let $f = A/D \in k(x)$, where $(A, D) = (1)$, and D is monic. Let $D = D_S D_N$ be a split-factorization of D with D_S and D_N monic. We can then compute $P, B, C \in k[x]$ such that $\deg(B) < \deg(D_S)$, $\deg(C) < \deg(D_N)$, and

$$f = \frac{A}{D} = P + \frac{B}{D_S} + \frac{C}{D_N}.$$

This decomposition is unique and is called it the *canonical representation* of f. We write $f_p = P$ (the *polynomial part* of f), $f_s = B/D_S$ (the *special part* of f), and $f_n = C/D_N$ (the *normal part* of f).

Definition 3.3. *Let $f \in k(x)$, and let $f = f_p + f_s + f_n$ be its canonical representation. We say that*

(i) *f is* **simple** *if f_n has a squarefree (hence normal) denominator,*
(ii) *f is* **reduced** *if $f_n = 0$.*

In the language of poles, $f \in k(x)$ is simple if it has only simple poles at normal places, and reduced if it has no poles at normal places.

4. Remainders

Let $(k, ')$ be a differential field of characteristic 0, and x be a monomial over k.

Notation: for $f \in k(x)$, we write $f', f'', f^{(3)}, \ldots$ for the successive derivatives of f. We also use $f^{(0)}, f^{(1)}$ and $f^{(2)}$ for f, f' and f''. In addition, we write ∂ for $'$ and ∂^i represents the operation of applying $'$ i times. Also, for any quantity Z and any non-negative integer n, we write $Z^{\{n\}}$ as a shorthand for $\prod_{i=0}^{n-1}(Z-i)$. In particular, $Z^{\{0\}} = 1$.

Let $P \in k[x]$. We define the **balance** of P to be

$$\mathcal{B}_P = \{f \in k(x) \text{ such that } P \text{ is balanced w.r.t. } f\}.$$

We can now define an analogue of the residue defined in (Bronstein, 1990*b*) which will be helpful in computing P-adic expansions and indicial equations. With the following definition, we show in this section that the n^{th}-remainder of f at P is essentially the leading coefficient of the P-adic expansion of $f^{(n)}$ at P. Recall that ϕ_P denotes the residue modulo P for elements of $\mathcal{O}_P$.

Definition 4.1. *Let $P \in k[x] \setminus \{0\}$ be squarefree, and $n \geq 0$ be an integer. We define the* **$\mathbf{n}^{\text{th}}$-remainder at** *P to be the map ${}_n\tau_P : \mathcal{B}_P \setminus \{0\} \to k[x]/(P)$ given by ${}_n\tau_P(f) = \phi_P(f\frac{P'^n}{P^{\nu_P(f)}})$.*

By Lemma 2.10, $f \in \mathcal{B}_P$ implies that $fP^{-\nu_P(f)} \in \mathcal{O}_P$, so $fP'^n P^{-\nu_P(f)} \in \mathcal{O}_P$, so ${}_n\tau_P$ is well defined. We note that for an irreducible P, $\mathcal{B}_P = k(x)$, so ${}_n\tau_P$ is defined on $k(x) \setminus \{0\}$ in that case.

The remainders satisfy the following multiplicative formula.

Lemma 4.2. *Let $P \in k[x]$ be squarefree. Then $\mathcal{B}_P$ is closed under multiplication and for any integers $n, m \geq 0$ and $f, g \in \mathcal{B}_P$, we have*

$${}_n\tau_P(f)\,{}_m\tau_P(g) = {}_{n+m}\tau_P(fg).$$

Proof. Let $f, g \in \mathcal{B}_P$ and $Q, R \in k[x]$ be any 2 irreducible factors of P. Then $\nu_Q(fg) = \nu_Q(f) + \nu_Q(g) = \nu_R(f) + \nu_R(g) = \nu_R(fg)$, so $fg \in \mathcal{B}_P$ by Lemma

2.8. Since P is squarefree, $\nu_P(fg) = \nu_P(f) + \nu_P(g)$ by Lemma 2.10, and ϕ_P is a ring-homomorphism, so

$$
\begin{aligned}
{}_n\tau_P(f)\,{}_m\tau_P(g) &= \phi_P(fP'^n P^{-\nu_P(f)})\phi_P(gP'^m P^{-\nu_P(g)}) \\
&= \phi_P(fgP'^{n+m} P^{-\nu_P(fg)}) = {}_{n+m}\tau_P(fg).
\end{aligned}
$$

Lemma 4.3. *Let $P \in k[x]$ be normal and $n \ge 0$. Then ${}_n\tau_P(f) \neq 0$ for any $f \in \mathcal{B}_P$.*

Proof. Let $f \in \mathcal{B}_P$ and Q be any irreducible factor of P. Since P is normal, P is squarefree, so, by Lemma 2.10, $\nu_Q(fP^{-\nu_P(f)}) = 0$. Also, since P is normal, $(P, P') = (1)$, so $(Q, P') = (1)$, so $\nu_Q(P'^n) = 0$. Hence, $\nu_Q(fP'^n P^{-\nu_P(f)}) = 0$, so $\nu_P(fP'^n P^{-\nu_P(f)}) = 0$, so ${}_n\tau_P(f) \neq 0$.

The next Lemma links the n^{th}-remainders and P-adic expansions.

Lemma 4.4. *Let $P \in k[x]$ be monic normal irreducible. Let $y \in k(x) \setminus \{0\}$ and $n = \nu_P(y)$. Let ω be $+\infty$ if $n < 0$ and $n+1$ otherwise. Then the P-adic expansion of $y^{(i)}$ is of the form*

$$y^{(i)} = n^{\{i\}}\,{}_i\tau_P(y)P^{n-i} + \cdots$$

for any integer i such that $0 \le i < \omega$.

Proof. By induction on i.

$i = 0$: Let the P-adic expansion of $y = y^{(0)}$ be of the form

$$y = B_n P^n + \cdots$$

where $B_n \in k[x]$, $B_n \neq 0$, and $\deg(B_n) < \deg(P)$. Then, the P-adic expansion of yP^{-n} is

$$yP^{-n} = B_n + B_{n+1}P + \cdots$$

so $B_n = \phi_P(yP^{-n}) = n^{\{0\}}\phi_P(yP'^0 P^{-n}) = {}_0\tau_P(y)$.

$0 < i < \omega$: Assume that the P-adic expansion of $y^{(i-1)}$ is of the form

$$y^{(i-1)} = n^{\{i-1\}} B P^{n-i+1} + \cdots \qquad (1)$$

where $B = {}_{i-1}\tau_P(y)$. By Lemma 4.3, $B \neq 0$. Also, $n - i + 1 \neq 0$ since $i < \omega$, so applying $'$ to both sides of (1), we get

$$y^{(i)} = n^{\{i-1\}}(n - i + 1)BP'P^{n-i} + \cdots$$

so the P-adic expansion of $y^{(i)}$ is

$$y^{(i)} = n^{\{i\}}\phi_P(BP')P^{n-i} + \cdots$$

We have

$$\phi_P(BP') = \phi_P({}_{i-1}\tau_P(y)P') = \phi_P(\phi_P(yP'^{i-1}P^{-n})P') = \phi_P(yP'^i P^{-n}) = {}_i\tau_P(y),$$

so the P-adic expansion of $y^{(i)}$ is

$$y^{(i)} = n^{\{i\}}\,{}_i\tau_P(y)P^{n-i} + \cdots .$$

5. The reduction at the normal singularities

Let $(k,')$ be a differential field of characteristic 0, and x be a monomial over k.

Let $f_0, \dots, f_{n-1} \in k(x)$ and $L = \partial^n + f_{n-1}\partial^{n-1} + \cdots + f_1\partial + f_0$ be a linear differential operator over $k(x)$. For convenience, we write $L = \sum_{i=0}^n f_i \partial^i$ where $f_n = 1$.

Definition 5.1. *Let $P \in k[x]$ be squarefree, and z be an indeterminate. We define the* **order drop** *of L at P to be:*

$$\mu_P(L) = \max_{0 \le i \le n} (i - \nu_P(f_i)),$$

and the **leading set** *of L at P to be:*

$$\lambda_P(L) = \{i \in \{0, \dots, n\} \text{ such that } i - \nu_P(f_i) = \mu_P(L)\}.$$

Note that $\mu_P(L) \ge n$ since $\nu_P(f_n) = 0$. If P is balanced w.r.t. $\{f_i$ for $i \in \lambda_P(L)\}$, then we define the **indicial equation** *of L at P to be:*

$$E_P(L) = \operatorname{resultant}_x(P, \sum_{i \in \lambda_P(L)} {}_i\tau_P(f_i) z^{\{i\}}) \in k[z].$$

We note that $|\lambda_P(L)| \ge 1$, so, by Lemma 4.3, $E_P(L)$ is not identically 0 for any normal $P \in k[x]$ which is balanced w.r.t. $\{f_i$ for $i \in \lambda_P(L)\}$.

Lemma 5.2. *Let $C \in k[x]$ be squarefree and balanced w.r.t. $\{f_0, \dots, f_n\}$. Then, $E_P(L) \mid E_C(L)$ for any irreducible factor P of C in $k[x]$.*

Proof. Let $P \in k[x]$ be an irreducible factor of C. Since C is squarefree and balanced w.r.t. $\{f_0, \dots, f_m\}$, we have $\nu_P(f_i) = \nu_C(f_i)$ for $i = 0 \dots m$ by Lemma 2.8. Hence, $\mu_P(L) = \mu_C(L)$ and $\lambda_P(L) = \lambda_C(L)$. Write $C = PD$ where $(P, D) = (1)$ since C is squarefree, and let $i \in \lambda_C(L)$. Then,

$$\begin{aligned}
\phi_P({}_i\tau_C(f_i)) &= \phi_P(\phi_C(f C'^i C^{-\nu_C(f_i)})) \\
&= \phi_P(f(P'D + PD')^i P^{-\nu_P(f_i)} D^{-\nu_P(f_i)}) \\
&= \phi_P(f P'^i P^{-\nu_P(f_i)} D^{i-\nu_P(f_i)}) \\
&= \phi_P({}_i\tau_P(f_i) D^{\mu_P(L)})
\end{aligned}$$

so

$${}_i\tau_C(f_i) \equiv D^{\mu_P(L)} {}_i\tau_P(f_i) \pmod P.$$

Let $\overline{k}$ be the algebraic closure of k. For any $\alpha \in \overline{k}$ we have:

$$\sum_{i \in \lambda_C(L)} {}_i\tau_C(f_i)\alpha^{\{i\}} \equiv D^{\mu_P(L)} \sum_{i \in \lambda_P(L)} {}_i\tau_P(f_i)\alpha^{\{i\}} \pmod P.$$

If $E_P(L) \in k$, then $E_P(L) \mid E_C(L)$. Otherwise, let $\alpha \in \overline{k}$ be such that $E_P(L)(\alpha) = 0$. Then, since P is irreducible,

$$\sum_{i \in \lambda_P(L)} {}_i\tau_P(f_i)\alpha^{\{i\}} \equiv 0 \pmod{P},$$

hence

$$\sum_{i \in \lambda_C(L)} {}_i\tau_C(f_i)\alpha^{\{i\}} \equiv 0 \pmod{P},$$

hence $P \mid \gcd(C, \sum_{i \in \lambda_C(L)} {}_i\tau_C(f_i)\alpha^{\{i\}})$, so $E_C(L)(\alpha) = 0$. Since this holds for any root of $E_P(L)$ in $\overline{k}$, $E_P(L) \mid E_C(L)$ in $k[x]$.

The above definition allows us to describe the relation between $\nu_P(y)$ and $\nu_P(L(y))$ for $y \in k(x)$.

Lemma 5.3. *Let $y \in k(x)$ and $P \in k[x]$ be monic normal irreducible. Then, either*

(i) $\nu_P(y) \geq 0$, *or*
(ii) $E_P(L)(\nu_P(y)) = 0$ *(and $\nu_P(L(y)) \geq \nu_P(y) - \mu_P(L)$), or*
(iii) $\nu_P(L(y)) = \nu_P(y) - \mu_P(L)$.

Proof. Let $m = \nu_P(y)$, $m_i = \nu_P(f_i)$ for $i = 1 \dots n$, and suppose that $m < 0$.

By Lemma 4.4, the P-adic expansion of $y^{(i)}$ is

$$y^{(i)} = m^{\{i\}}{}_i\tau_P(y)P^{m-i} + \cdots$$

for any integer $i \geq 0$. Also by Lemma 4.4, the P-adic expansion of f_i for $f_i \neq 0$ is

$$f_i = {}_0\tau_P(f_i)P^{m_i} + \cdots .$$

Hence, the P-adic expansion of $f_i y^{(i)}$ for $f_i \neq 0$ is

$$f_i y^{(i)} = m^{\{i\}}{}_0\tau_P(f_i){}_i\tau_P(y)P^{m-(i-m_i)} + \cdots .$$

By Lemma 4.2,

$${}_0\tau_P(f_i){}_i\tau_P(y) = {}_i\tau_P(f_i y) = {}_0\tau_P(y){}_i\tau_P(f_i)$$

so the P-adic expansion of $L(y)$ is

$$L(y) = \left({}_0\tau_P(y) \sum_{i \in \lambda_P(L)} m^{\{i\}}{}_i\tau_P(f_i)\right) P^{m-\mu_P(L)} + \cdots$$

so $\nu_P(L(y)) \geq \nu_P(y) - \mu_P(L)$.

Suppose that $\nu_P(L(y)) > \nu_P(y) - \mu_P(L)$. Then

$${}_0\tau_P(y) \sum_{i \in \lambda_P(L)} m^{\{i\}}{}_i\tau_P(f_i) \equiv 0 \pmod{P}.$$

Since P is normal, ${}_0\tau_P(y) \neq 0$ by Lemma 4.3. P is also irreducible, so $k[x]/(P)$ is a field and $\mathcal{B}_P = k(x)$. Hence $\sum_{i \in \lambda_P(L)} m^{\{i\}}{}_i\tau_P(f_i) \equiv 0 \pmod{P}$, so $E_P(L)(m) = 0$.

We need to be able to find a lower bound for the integer roots of a polynomial with coefficients in k, so, following Abramov, we call such fields *admissible.*

Definition 5.4. *Let K be a field, and X be an indeterminate over K. We say that K is* **admissible** *if there exists an algorithm that, given $P \in K[X]$ returns an integer $\beta(P)$ such that for any integer n, $P(n) = 0 \implies n \geq \beta(P)$.*

We now have a rational algorithm for reducing the normal singularities of an ordinary linear differential equation over $k(x)$. Recall that $\nu_P(0) = +\infty$ by convention. For use in recursive algorithms, we actually prove the result for parametrized equations. Note that x denotes an arbitrary monomial and not the dependent variable of the differential equation (i.e. $' \neq d/dx$ in general).

Theorem 5.5. *Let k be an admissible differential field of characteristic 0, C be the constant subfield of k, and x be a monomial over k. Let $n, m > 0$ be integers and $f_0, \ldots, f_n, g_1, \ldots, g_m \in k(x)$ with $f_n = 1$. Let $L = \sum_{i=0}^n f_i \partial^i$, and for $i = 0, \ldots, n$, let $f_i = f_{ip} + f_{is} + f_{in}$ be the canonical representation of f_i, where $f_{in} = A_i/D_i$, $A_i, D_i \in k[x]$, $(A_i, D_i) = (1)$, and D_i is monic. For $j = 1, \ldots, m$, let also $g_j = g_{jp} + g_{js} + g_{jn}$ be the canonical representation of g_j, where $g_{jn} = B_j/E_j$, $B_j, E_j \in k[x]$, $(B_j, E_j) = (1)$, and E_j is monic. Let $D = \mathrm{lcm}(D_0, \ldots, D_n)$, $E = \mathrm{lcm}(E_1, \ldots, E_m)$, $G = E/\gcd(E, dE/dx)$ and $H = G/\gcd(G, D/\gcd(D, dD/dx))$. Let ${C_1}^{e_1} \cdots {C_q}^{e_q}$ be a balanced factorization of D with respect to $\{f_{0n}, \ldots, f_{nn}, g_{1n}, \ldots, g_{mn}\}$, and $H_1 \cdots H_r$ be a balanced factorization of H with respect to E. Let*

$$T = {C_1}^{d_1} \cdots {C_q}^{d_q} {H_1}^{q_1} \cdots {H_r}^{q_r}$$

where

$$d_j = \max(0, -\beta(E_{C_j}(L)), \max_{1 \leq s \leq m}(-\nu_{C_j}(g_s)) - \mu_{C_j}(L)) \text{ for } j = 1, \ldots, q,$$

and

$$q_j = \max(0, \nu_{H_j}(E) - n) \quad \text{for } j = 1, \ldots, r.$$

Then, for any $y \in k(x)$ and $c_1, \ldots, c_m \in C$,

$$L(y) = \sum_{j=1}^m c_j g_j \implies yT \text{ is reduced.}$$

Proof. Let $y \in k(x)$, $c_1, \ldots, c_m \in C$ and suppose that $L(y) = g = \sum_{j=1}^m c_j g_j$. If $y = 0$, then $yT = 0$ is reduced, so suppose from now on that $y \neq 0$.

Let $P \in k[x]$ be monic normal irreducible. If $\nu_P(y) \geq 0$, then $\nu_P(yT) \geq 0$, so suppose from now on that $\nu_P(y) < 0$.

Case 1: $E_P(L)(\nu_P(y)) \neq 0$: then, by Lemma 5.3, $\nu_P(L(y)) = \nu_P(y) - \mu_P(L) < 0$. But $L(y) = g$, so $g \neq 0$, and $\nu_P(g) < 0$. We also have

$$\nu_P(g) \geq \min_{1 \leq j \leq m}(\nu_P(g_j)) = -\max_{1 \leq j \leq m}(-\nu_P(g_j)) = -\max_{1 \leq j \leq m}(\nu_P(E_j)) \geq -\nu_P(E)$$

so $\nu_P(g) + \nu_P(E) \geq 0$, and $\nu_P(E) \geq -\nu_P(g) > 0$. Thus $P \mid E$, so $P \mid G$. And, since $g \neq 0$, we have $\nu_P(yT) = \nu_P(y) + \nu_P(T) = \nu_P(g) + \mu_P(L) + \nu_P(T)$.

Suppose first that $(P, D) = (1)$. Then, $\nu_P(f_i) \geq 0$ for $i = 0, \dots, n$, so $\mu_P(L) = n$. Also, $P \mid H$ (since $P \mid G$), so $P \mid H_{j_0}$ for some $j_0 \in \{1, \dots, r\}$. We have $(H_{j_0}, C_j) = (1)$ for any j (since $(P, D) = (1)$), and $(H_{j_0}, H_j) = (1)$ for $j \neq j_0$, and H_{j_0} is squarefree, so $\nu_P(T) = \nu_{H_{j_0}}(T) = q_{j_0} \geq \nu_{H_{j_0}}(E) - n$. But H_{j_0} is balanced w.r.t. E, so $\nu_P(E) = \nu_{H_{j_0}}(E)$, hence $\nu_P(T) \geq \nu_P(E) - n$, so $\nu_P(yT) \geq \nu_P(g) + \nu_P(E) \geq 0$.

Suppose now that $P \mid D$. Then, $P \mid C_{j_0}$ for some $j_0 \in \{1, \dots, q\}$. We write C for C_{j_0}. We have $(C, C_j) = (1)$ for $j \neq j_0$. Since $P \mid G$ and $P \mid D$, $P \mid \gcd(G, D/\gcd(D, dD/dx))$, so $(P, H) = (1)$ since H is squarefree. Thus $(C, H_j) = (1)$ for any j, so $\nu_P(T) = \nu_C(T) = d_{j_0} \geq -\min_{1 \leq j \leq m}(\nu_C(g_j)) - \mu_C(L)$ by definition of d_{j_0}. But C is squarefree and balanced w.r.t. $\{g_1, \dots, g_m\}$, so $\min_{1 \leq j \leq m}(\nu_P(g_j)) = \min_{1 \leq j \leq m}(\nu_C(g))$ by Lemma 2.8. And C is squarefree and balanced w.r.t. $\{f_0, \dots, f_m\}$, so $\mu_P(L) = \mu_C(L)$ by Lemma 2.8. Hence $\nu_P(T) \geq -\min_{1 \leq j \leq m}(\nu_P(g_j)) - \mu_P(L)$, so $\nu_P(yT) \geq 0$.

Case 2: $E_P(L)(\nu_P(y)) = 0$: Suppose that $(P, D) = (1)$. Then, $\nu_P(f_i) \geq 0$ for $i = 0, \dots, n$, so $\mu_P(L) = n$, $\lambda_P(L) = \{n\}$, and

$$E_P(L) = \text{resultant}_x(P, z^{\{n\}}) = {z^{\{n\}}}^{\deg(P)+1} = \prod_{i=0}^{n-1} (z - i)^{\deg(P)+1}$$

which has no negative integer roots in contradiction with $\nu_P(y) < 0$. Hence, $P \mid D$.

Thus, $P \mid C_{j_0}$ for some $j_0 \in \{1, \dots, q\}$. We write C for C_{j_0}. By Lemma 5.2, this implies that $E_P(L) | E_C(L)$, so $E_C(L)(\nu_P(y)) = 0$, so $\nu_P(y) \geq \beta(E_C(L))$. Since $\nu_P(y) < 0$, we have $\beta(E_C(L)) < 0$, so $\nu_C(T) = d_{j_0} \geq -\beta(E_C(L))$. Since $P \mid C$, $\nu_P(T) \geq \nu_C(T)$, hence $\nu_P(T) \geq -\beta(E_C(L))$. Therefore,

$$\nu_P(yT) = \nu_P(y) + \nu_P(T) \geq \beta(E_C(L)) - \beta(E_C(L)) = 0.$$

Since this holds for any monic normal irreducible $P \in k[x]$, yT is reduced.

For non-parametrized inhomogeneous equations, the following criterion is a direct consequence of Lemma 5.3.

Theorem 5.6. *Let k be a differential field of characteristic 0, and x be a monomial over k. Let $m > 0$ be an integer and $g, f_0, \dots, f_m \in k(x)$ with $f_m = 1$. Let $L = \sum_{i=0}^m f_i \partial^i$, and for $i = 0, \dots, m$, let $f_i = f_{ip} + f_{is} + f_{in}$ be the canonical representation of f_i, where $f_{in} = A_i/D_i$, $A_i, D_i \in k[x]$, $(A_i, D_i) = (1)$, and D_i is monic. Let also $g = g_p + g_s + g_n$ be the canonical representation of g, where $g_n = B/E$, $B, E \in k[x]$, $(B, E) = (1)$, and E is monic. Let $D = \operatorname{lcm}(D_0, \dots, D_n)$, $G = E/\gcd(E, dE/dx)$ and $H = G/\gcd(G, D/\gcd(D, dD/dx))$. Then,*

$$L(y) = g \text{ has a solution } y \in k(x) \implies H^{m+1} \mid E.$$

Proof. If $y = 0$, then $g = 0$, so $H = E = 1$, so $H^{m+1} \mid E$, so suppose that $y \neq 0$.

Let $P \in k[x]$ be an irreducible factor of H. Then $P \mid G$. so $P \mid E$, so $\nu_P(L(y)) = \nu_P(g) < 0$. Since G is squarefree, $P \not| \gcd(G, D/\gcd(D, dD/dx))$, so $(P, D) = (1)$. Then, $\nu_P(f_i) \geq 0$ for $i = 0, \ldots, m$, so $\nu_P(y) < 0$ (otherwise we would have $\nu_P(L(y)) \geq 0$). Also, $\mu_P(L) = m$, $\lambda_P(L) = \{m\}$, and $E_P(L)$ has no negative integer roots as in case 2 of the proof of Theorem 5.5. Hence $E_P(L)(\nu_P(y)) \neq 0$, so $\nu_P(E) = -\nu_P(g) = m - \nu_P(y)$ by Lemma 5.3, so $\nu_P(E) > m$, so $P^{m+1} \mid E$. Since this holds for any irreducible factor of H and H is squarefree, we have $H^{m+1} \mid E$.

Example: Consider the equation

$$L(y) = y'' - \frac{8t}{\tan(t)^2 - t^2} y' - \left(12t^2 + 8 + \frac{(18t^4 + 24t^2 + 8)\tan(t)^2 - 10t^6 - 8t^4 - 8t^2}{\tan(t)^4 - 2t^2\tan(t)^2 + t^4}\right) y = 2 \quad (E_1)$$

Let $k = \mathbf{Q}(t)$ where t is transcendental over $\mathbf{Q}$ and the derivation on k be $' = d/dt$. Let x be a monomial over k with $x' = 1 + x^2$ (i.e. $x = \tan(t)$). Following Theorems 5.5 and 5.6 we have $g = 2$, $m = 2$, $f_2 = 1$, $f_1 = -8t/(x^2 - t^2)$ and

$$f_0 = -12t^2 - 8 - \frac{(18t^4 + 24t^2 + 8)x^2 - 10t^6 - 8t^4 - 8t^2}{x^4 - 2t^2x^2 + t^4}.$$

Computing the canonical representations of the f_i's and g we get $A_2 = B = 0$, $D_2 = E = 1$, $A_1 = -8t$, $D_1 = x^2 - t^2$, $D_0 = x^4 - 2t^2x^2 + t^4$ and $A_0 = -(18t^4 + 24t^2 + 8)x^2 + 10t^6 + 8t^4 + 8t^2$. Thus,

$$D = \operatorname{lcm}(D_0, D_1, D_2) = x^4 - 2t^2x^2 + t^4$$

and $G = H = 1$, so $H^3 \mid E$. A balanced factorization of D with respect to $\{f_{0n}, f_{1n}, f_{2n}, g_n\}$ is

$$D = C^2 = (x^2 - t^2)^2$$

so we have to look at the Newton polygon of L at C. We find $\nu_C(f_0) = -2$, $\nu_C(f_1) = -1$ and $\nu_C(f_2) = 0$, so $\mu_C(L) = 2$ and $\lambda_C(L) = \{0, 1, 2\}$. We have $C' = 2x^3 + 2x - 2t$, and the τ_C's are

$$\tau_0 = {}_0\tau_C(f_0) = \phi_C(f_0C^2) = \phi_C(A_0) = -8t^6 - 16t^4,$$

$$\tau_1 = {}_1\tau_C(f_1) = \phi_C(f_1CC') = \phi_C(A_1C') = -16t((t^2 + 1)x - t)$$

and

$$\tau_2 = {}_2\tau_C(f_2) = \phi_C(C'^2) = -4t((2t^2 + 2)x - t^5 - 2t^3 - 2t),$$

so the indicial equation of L at C is

$$\begin{aligned} E_C(L) = \operatorname{resultant}_x(x^2 - t^2, \tau_0 + \tau_1 z + \tau_2 z(z-1)) = \\ 16(t^8 + 2t^6)((t^4 + 2t^2)z^4 - (2t^4 + 4t^2 + 8)z^3 \\ - (3t^4 + 6t^2 + 16)z^2 + (4t^4 + 8t^2 - 8)z + 4t^4 + 8t^2). \end{aligned}$$

We have
$$\gcd(E_C(L)(1,z), E_C(L)(2,z)) = (z+1)^2$$
so $\beta(E_C(L)) \geq -1$. Checking for $z = -1$ we find that $E_C(L)(t,-1) = 0$, so $\beta(E_C(L)) = -1$. We have $\nu_C(g) = 0$, so the bound given by Theorem 5.5 for the exponent of C is $\max(0,1,-2) = 1$, so for any solution $y \in k(x)$ of equation (E_1),
$$Y = yT = y(x^2 - t^2)$$
is reduced.

6. The reduction at infinity

Let $(k, ')$ be a differential field of characteristic 0, and x be a monomial over k.

Notation: for any quantity Z, any non-negative integer n, and any integer m, we write $Z^{\{n,m\}}$ as a shorthand for $\prod_{i=0}^{n-1}(Z - im)$. In particular, $Z^{\{0,m\}} = 1$ and $Z^{\{n,1\}} = Z^{\{n\}}$.

We first define an analogue of the remainders at infinity.

Definition 6.1. *For any integer $n \geq 0$, we define the* **$\mathbf{n^{th}}$-remainder at infinity** *to be the map ${}_n\tau_\infty : k(x) \setminus \{0\} \to k$ given by ${}_n\tau_\infty(f) = (-lc(x))^n \phi_\infty(f x^{\nu_\infty(f)})$.*

Since $\nu_\infty(f x^{\nu_\infty(f)}) = \nu_\infty(f)(1 + \nu_\infty(x)) = 0$, ${}_n\tau_\infty(f) \neq 0$ for any $f \in k(x) \setminus \{0\}$.

Lemma 6.2. *Suppose that $' = d/dx$ (i.e. $x' = 1$ and $k' = 0$ or that $d(x) \geq 2$. Let $y \in k(x) \setminus \{0\}$ and $n = \nu_\infty(y)$. Let ω be $+\infty$ if $n(1-d(x)) \geq 0$ and $1 + (n/(d(x)-1))$ otherwise. Then the series expansion of $y^{(i)}$ at infinity is of the form*
$$y^{(i)} = n^{\{i,d(x)-1\}}\, {}_i\tau_\infty(y) x^{-(n+i(1-d(x)))} + \cdots$$
for any integer i such that $0 \leq i < \omega$.

Proof. By induction on i.

$i = 0$: Let the series expansion of $y = y^{(0)}$ at infinity be of the form
$$y = a_n x^{-n} + \cdots$$
where $a_n \in k$, and $a_n \neq 0$. Then, the expansion of yx^n is
$$yx^n = a_n + a_{n+1}x^{-1} + \cdots$$
so $a_n = \phi_\infty(yx^n) = n^{\{0,d(x)-1\}}\, {}_0\tau_\infty(y)$.

$0 < i < \omega$: Assume that the expansion of $y^{(i-1)}$ is of the form
$$y^{(i-1)} = n^{\{i-1,d(x)-1\}} a x^{-(n+(i-1)(1-d(x)))} + \cdots$$
where $a = {}_{i-1}\tau_\infty(y) \neq 0$. We have $n + (i-1)(1-d(x)) \neq 0$ since $i < \omega$.

If $' = d/dx$, then $a' = 0, d(x) = 0$, and $lc(x) = 1$, so $(ax^{-(n+(i-1))})' = -(n + (i-1))ax^{-(n+i)}$.

Otherwise, $d(x) \geq 2$ so the expansion of $(ax^{-(n+(i-1)(1-d(x)))})'$ is of the form $-(n+(i-1)(1-d(x)))a\ lc(x)x^{-(n+i(1-d(x)))} + \cdots$. Thus we get in both cases

$$y^{(i)} = n^{\{i-1,d(x)-1\}}(n+(i-1)(1-d(x)))(-a)\ lc(x)x^{-(n+i(1-d(x)))} + \cdots.$$

We have

$$\begin{aligned}(-a)\ lc(x) = -{}_{i-1}\tau_\infty(y)lc(x) &= -(-lc(x))^{i-1}\phi_\infty(yx^{\nu_\infty(y)})lc(x) \\ &= (-lc(x))^i\phi_\infty(yx^{\nu_\infty(y)}) = {}_i\tau_\infty(y),\end{aligned}$$

so the expansion of $y^{(i)}$ is

$$y^{(i)} = n^{\{i,d(x)-1\}}{}_i\tau_\infty(y)x^{-(n+i(1-d(x)))} + \cdots.$$

Let $L = \sum_{i=0}^n f_i\partial^i$ where $f_0, \ldots, f_n \in k(x)$ and $f_n = 1$.

Definition 6.3. *Let z be an indeterminate. We define the* **order drop of L at infinity** *to be:*

$$\mu_\infty(L) = \max_{0\leq i\leq n}(i(d(x)-1) - \nu_\infty(f_i)),$$

the **leading set of L at infinity** *to be:*

$$\lambda_\infty(L) = \{i \in \{0,\ldots n\} \text{ such that } i(d(x)-1) - \nu_\infty(f_i) = \mu_\infty(L)\},$$

and the **indicial equation of L at infinity** *to be:*

$$E_\infty(L) = \sum_{i\in\lambda_\infty(L)} {}_i\tau_\infty(f_i)z^{\{i,d(x)-1\}} \in k[z].$$

We note that $|\lambda_\infty(L)| \geq 1$, so $E_\infty(L)$ is not identically 0.

We can now describe the relation between $\nu_\infty(y)$ and $\nu_\infty(L(y))$ for $y \in k(x)$.

Lemma 6.4. *Suppose that $' = d/dx$ or that $d(x) \geq 2$, and let α be 0 if $d(x) \geq 2$, $1-n$ otherwise. Let $y \in k(x)$. Then, either*

(i) *$\nu_\infty(y) \geq \alpha$, or*
(ii) *$E_\infty(L)(\nu_\infty(y)) = 0$ (and $\nu_\infty(L(y)) \geq \nu_\infty(y) - \mu_\infty(L)$), or*
(iii) *$\nu_\infty(L(y)) = \nu_\infty(y) - \mu_\infty(L)$.*

Proof. Let $m = \nu_\infty(y)$, $m_i = \nu_\infty(f_i)$ for $i = 1,\ldots,n$, and suppose that $m < \alpha$. Then $m < 0$, so the ω of Lemma 6.2 is $+\infty$ if $d(x) \geq 2$, or $1-m > 1-\alpha = n$ otherwise. Hence Lemma 6.2 is valid for $0 \leq i \leq n$, so the series expansion of $y^{(i)}$ at infinity is

$$y^{(i)} = m^{\{i,d(x)-1\}}{}_i\tau_\infty(y)x^{-(m+i(1-d(x)))} + \cdots$$

for $0 \le i \le n$. Also by Lemma 6.2, the expansion of f_i for $f_i \ne 0$ is

$$f_i = {}_0\tau_\infty(f_i)x^{-m_i} + \cdots .$$

Hence, the expansion of $f_i y^{(i)}$ for $f_i \ne 0$ is

$$f_i y^{(i)} = m^{\{i,d(x)-1\}}{}_0\tau_\infty(f_i){}_i\tau_\infty(y)x^{-(m+m_i+i(1-d(x)))} + \cdots .$$

But

$${}_0\tau_\infty(f_i){}_i\tau_\infty(y) = \phi_\infty(f_i x^{m_i})(-lc(x))^i\phi_\infty(yx^m) = {}_0\tau_\infty(y){}_i\tau_\infty(f_i)$$

so the expansion of $L(y)$ is

$$L(y) = \left({}_0\tau_\infty(y)\sum_{i\in\lambda_\infty(L)} m^{\{i,d(x)-1\}}{}_i\tau_\infty(f_i)\right)x^{-(m-\mu_\infty(L))} + \cdots$$

so $\nu_\infty(L(y)) \ge \nu_\infty(y) - \mu_\infty(L)$.

Suppose that $\nu_\infty(L(y)) > \nu_\infty(y) - \mu_\infty(L)$. Then

$${}_0\tau_\infty(y)\sum_{i\in\lambda_\infty(L)} m^{\{i,d(x)-1\}}{}_i\tau_\infty(f_i) = 0,$$

hence, since ${}_0\tau_\infty(y) \ne 0$, $E_\infty(L)(m) = 0$.

When $' = d/dx$ or $d(x) \ge 2$, we can bound the degree of the polynomial part of any solution of an ordinary linear differential equation over $k(x)$. Recall that $\nu_\infty(0) = +\infty$ by convention, and that the degree of the polynomial part of any $f \in k(x)$ is $-\nu_\infty(f)$. For use in recursive algorithms, we prove the bound for parametrized equations.

Theorem 6.5. *Let k be an admissible differential field of characteristic 0, C be the constant subfield of k, and x be a monomial over k. Suppose that $' = d/dx$ or that $d(x) \ge 2$, and let $n, m > 0$ be integers. Let $f_0, \dots, f_n, g_1, \dots, g_m \in k(x)$ with $f_n = 1$, and $L = \sum_{i=0}^n f_i\partial^i$. Let α be 0 if $d(x) \ge 2$, $1-n$ otherwise. Then,*

$$L(y) = \sum_{j=1}^m c_j g_j \implies \nu_\infty(y) \ge \min(\alpha, \beta(E_\infty(L)), \mu_\infty(L) + \min_{1\le j\le m}(\nu_\infty(g_j)))$$

for any $y \in k(x)$ and $c_1, \dots, c_m \in C$.

Proof. Let $M = \min(\alpha, \beta(E_\infty(L)), \mu_\infty(L) + \min_{1\le j\le m}(\nu_\infty(g_j)))$. Let $y \in k(x)$, $c_1, \dots, c_m \in C$ and suppose that $L(y) = \sum_{j=1}^m c_j g_j$. Let $q = \nu_\infty(y)$. If $q \ge \alpha$, then $q \ge M$. If $E_\infty(L)(q) = 0$, then $q \ge \beta(E_\infty(L))$, so $q \ge M$. Suppose that $q < \alpha$ and that $E_\infty(L)(q) \ne 0$. Then, by Lemma 6.4, $q = \nu_\infty(\sum_{j=1}^m c_j g_j) + \mu_\infty(L) \ge \mu_\infty(L) + \min_{1\le j\le m}(\nu_\infty(g_j))$, so $q \ge M$.

Example: Continuing the example of the previous section, we have $x' = 1 + x^2$, so $d(x) = 2$ and $lc(x) = 1$. We find that $\nu_\infty(f_0) = 0$, $\nu_\infty(f_1) = 2$ and $\nu_\infty(f_2) = 0$, so $\mu_\infty(L) = 2$ and $\lambda_\infty(L) = \{2\}$. Also ${}_2\tau_\infty(f_2) = (-1)^2\phi_\infty(1) = 1$, so the indicial equation at infinity is $E_\infty(L) = z^{\{2,1\}} = z(z-1)$ which has no negative integer root, so $\beta(E_\infty(L)) = 0$, and the bound given by Theorem 6.5 for the order at infinity is $\min(0,0,2) = 0$, hence $\nu_\infty(y) \geq 0$ for any solution $y \in k(x)$ of equation (E_1).

Since we know from the previous section that $Y = y(x^2 - t^2)$ is reduced for any solution $y \in k(x)$ of equation (E_1), we could also have replaced y by $Y/(x^2 - t^2)$ in equation (E_1), obtaining the following equation for Y:

$$\tilde{L}(Y) = Y'' - 4\frac{x^3 + x + 1}{x^2 - t^2}Y' + 2(x^2 - t^2)Y = 2(x^2 - t^2). \qquad (E_2)$$

Applying the algorithm of this section to $F_0 = G = 2(x^2 - t^2)$, $F_2 = 1$ and $F_1 = -4(x^3 + x + 1)/(x^2 - t^2)$, we get $\nu_\infty(G) = \nu_\infty(F_0) = -2$, $\nu_\infty(F_1) = -1$ and $\nu_\infty(F_2) = 0$, so $\mu_\infty(\tilde{L}) = 2$ and $\lambda_\infty(\tilde{L}) = \{0, 1, 2\}$. Computing the τ_∞'s we get

$$\tau_0 = {}_0\tau_\infty(F_0) = \phi_\infty(F_0/x^2) = 2,$$

$$\tau_1 = {}_1\tau_\infty(F_1) = -\phi_\infty(F_1/x) = 4$$

and

$$\tau_2 = {}_2\tau_\infty(F_2) = \phi_\infty(1) = 1,$$

so the indicial equation of $\tilde{L}$ at infinity is

$$E_\infty(\tilde{L}) = \tau_0 + \tau_1 z + \tau_2 z(z-1) = z^2 + 3z + 2 = (z+1)(z+2).$$

Thus, $\beta(E_\infty(\tilde{L})) = -2$, so the bound given by Theorem 6.5 for the order at infinity is $\min(0, -2, 0) = -2$, so $\nu_\infty(Y) \geq -2$ for any solution $Y \in k(x)$ of equation (E_2). Note that the two bounds are equivalent since $Y = y(x^2 - t^2)$.

Since $\sqrt{-1} \notin k(x)$, the only possible denominator for a reduced element of $k(x)$ is a power of $x^2 + 1$ (Bronstein, 1990*b*), so any reduced solution Y of equation (E_2) must be of the form

$$Y = a_2 x^2 + a_1 x + a_0 + \frac{P}{(x^2+1)^m}$$

where $a_0, a_1, a_2 \in \mathbf{Q}(t)$, $m \geq 0$ and $P \in k[x]$ is either 0 or $\deg(P) < 2m$. For this particular example, (E_2) has the trivial solution $Y = 1$, so a solution in $\mathbf{Q}(t, \tan(t))$ of equation (E_1) is

$$y = \frac{1}{\tan(t)^2 - t^2}.$$

7. Algorithms for Liouvillian extensions

We apply here the results of the previous sections to describe how Singer's (1991) algorithm for finding solutions of $L(y) = g$ in the coefficient field can be made more effective.

Let k be a differential field of characteristic 0 and t be a monomial over k. We recall that t is *Liouvillian* over k if either

(i) $t' \in k$, in which case we say that t is **primitive** over k, or
(ii) $t'/t \in k$.

Let $P \in k[t]$ be squarefree. We recall from (Bronstein, 1990*b*) that

(i) if $t' \in k$ then P is normal,
(ii) if $t'/t \in k$ then P is normal if and only if $t \not| P$.

Consequently, for any $a \in k(t)$,

(i) if $t' \in k$, then a is reduced if and only if $a \in k[t]$,
(ii) if $t'/t \in k$, then a is reduced if and only if $a \in k[t, t^{-1}]$.

Let k be a differential field of characteristic 0, and C be its constant field. Following Singer, we say that we can *effectively solve parametrized linear ordinary differential equations over K* if given $f_0, \dots, f_n, g_0, \dots, g_m \in k(t)$ with $f_n = 1$, we can effectively find $h_1, \dots, h_r \in k$ and a system Δ of $m + r$ linear equations with coefficients in C such that $\sum_{i=0}^n f_i y^{(i)} = \sum_{j=1}^m c_j g_j$ for $y \in k$ and $c_1, \dots, c_m \in C$ if and only if $y = \sum_{l=1}^r y_l h_l$ where $y_1, \dots, y_r \in C$ and $(c_1, \dots, c_m, y_1, \dots, y_r)$ satisfy Δ.

The following Theorem states that Singer's algorithm can be made rational, whenever the coefficients of the equations lie in a tower of algebraic and primitive extensions over the rational function field.

Theorem 7.1. *Let k be an admissible differential field of characteristic 0, C be the constant subfield of k, and $x \in k$ be such that $x' = 1$. Suppose that there exist $\theta_1, \dots, \theta_q \in k$ such that*

(i) $k = C(x, \theta_1, \dots, \theta_q)$,
(ii) *For $i = 1, \dots, q$, θ_i is either algebraic or a primitive monomial over $C(x, \theta_1, \dots, \theta_{i-1})$*

Then there is a rational algorithm for effectively solving parametrized linear ordinary differential equations over k.

Proof. Let $f_0, \dots, f_n, g_0, \dots, g_m \in k$ with $f_n = 1$. We proceed by induction on q.

$q = 0$: Then $k = C(x)$. Let T be given by Theorem 5.5, and $Y = yT$. By Theorem 5.5, $Y \in C[x]$ if $L(y) = \sum_{j=1}^m c_j g_j$. Substituting $y = Y/T$ in $L(y) = \sum_{j=1}^m c_j g_j$ and clearing denominators, we get $\tilde{g}_1, \dots, \tilde{g}_m \in C[x]$ and a linear ordinary differential operator $\tilde{L}$ with coefficients in $C[x]$ such that $L(y) = \sum_{j=1}^m c_j g_j \iff \tilde{L}(Y) = \sum_{j=1}^m c_j \tilde{g}_j$ and $Y \in C[x]$.

By Theorem 6.5, we get an integer B such that $deg(Y) \le B$ if $\tilde{L}(Y) = \sum_{j=1}^m c_j \tilde{g}_j$. Set $Y = y_0 + y_1 x + \cdots y_B x^B$ where $y_0, \dots, y_B \in C$. Substituting in $\tilde{L}(Y) = \sum_{j=1}^m c_j \tilde{g}_j$, we get a system Δ of linear equations over C for

$y_0, \dots, y_B, c_1, \dots, c_m$. If Δ has no solution in C^{m+B+1}, then $L(y) = \sum_{j=1}^m c_j g_j$ has no solution in $C(x)$. Otherwise

$$y = \frac{\sum_{i=0}^B y_i h_i}{T}$$

where $h_i = x^i$, is a solution of $L(y) = \sum_{j=1}^m c_j g_j$ for any solution $(y_0, \dots, y_B, c_1, \dots, c_m)$ of Δ.

$q > 0$: We assume by induction that we can effectively solve parametrized linear ordinary differential equations over $K = C(x, \theta_1, \dots, \theta_{q-1})$. Let $t = \theta_q$. Then t is either algebraic or a primitive monomial over K.

Case 1, t primitive monomial over k: As above, we can compute $T, \tilde{g}_1, \dots, \tilde{g}_m \in K[t]$ and a linear ordinary differential operator $\tilde{L}$ with coefficients in $K[t]$ such that $L(y) = \sum_{j=1}^m c_j g_j \iff \tilde{L}(Y) = \sum_{j=1}^m c_j \tilde{g}_j$ and $Y = yT \in K[t]$. Since $d(t) = 0$, Theorem 6.5 can not be used in general to get an upper bound on $\deg(Y)$. An algorithm for computing such a bound and finding the coefficients of Y is contained in Lemmas 3.8 and 3.2 (second half) of (Singer, 1991). We note that the algorithm as described there finds a linear system $\mathcal{L}$ with coefficients in K, and that one should use the algorithm of Lemma 3.8 of (Bronstein, 1990a) in order to find a linear system Δ with coefficients in C with the same constant solution space as $\mathcal{L}$.

Case 2, t algebraic over K: This is Proposition 3.1 of (Singer, 1991).

We note that Theorem 5.5 can be used when t is monomial over k satisfying $t'/t \in k$ as an effective rational alternative to Lemma 3.2 of (Singer, 1991). This still does not give a rational algorithm for solving parametrized linear ordinary differential equations with elementary (or Liouvillian) coefficients, since the bounding procedure requires solving Ricatti-type equations in their coefficient fields. In the next section, we show how balanced factorizations can be used to get bounds on the singularities of solutions of such equations.

8. Ricatti-type equations

Let $(k, ')$ be a differential field of characteristic 0, and x be a monomial over k. Let $L = \sum_{i=0}^n f_i \partial^i$ where $f_0, \dots, f_{n-1} \in k(x)$ and $f_n = 1$. In this section, we consider the problem of finding non-zero solutions y of $L(y) = 0$ such that $u = y'/y \in k(x)$ (we then write $y = e^{\int u}$). $u \in k(x)$ satisfies then a differential equation which can be found as follows: differentiating $y' = uy$ on both sides several times, one finds that $y^{(i)} = P_i y$, where the P_i's are given by

$$\begin{cases} P_0 = 1 \\ P_i = {P_{i-1}}' + uP_{i-1} \quad \text{for } i > 0. \end{cases} \tag{2}$$

Note that each P_i is a differential polynomial in u of order $i-1$ and with integer coefficients. Substituting for $y^{(i)}$ in $L(y)$, we get

$$L(y) = y \sum_{i=0}^n f_i P_i(u, \dots, u^{(i-1)})$$

hence, for $y \neq 0$, $L(y) = 0 \iff R(u) = 0$ where

$$R(u) = \sum_{i=0}^{n} f_i P_i(u, \dots, u^{(i-1)}) \tag{3}$$

which is a non-linear differential equation of order $n-1$ in u with coefficients in $k(x)$. R is called the *Ricatti equation associated with L*. Thus, the problem of finding non-zero solutions y of $L(y) = 0$ such that $y'/y \in k(x)$ reduces to the problem of finding non-zero solutions $u \in k(x)$ of $R(u) = 0$.

Definition 8.1. *Let $P \in k[x]$. We define the following quantities for L at P:*

$$\Lambda_P(L) = \{(i,j) \in \{0,\dots,n\}^2 \text{ such that } i \neq j \text{ and } \frac{\nu_P(f_i) - \nu_P(f_j)}{i-j} \in \mathbf{Z}\},$$

and

$$\delta_P(L) = \max(1, \max_{(i,j)\in\Lambda_P(L)} (\frac{\nu_P(f_i) - \nu_P(f_j)}{i-j})).$$

The next two Lemmas are contained in the proofs of Lemma 2.2 and Proposition 2.3 of (Singer, 1991).

Lemma 8.2. *Let $P \in k[x]$ be monic normal irreducible. Let $u \in k(x) \setminus \{0\}$ and $m = \nu_P(u)$. Let $P_0, \dots, P_n$ be given by (2), and suppose that $m < 0$. Then the P-adic expansion of $P_i(u, \dots, u^{(i-1)})$ for $i \geq 0$ is of the form*

$$P_i(u, \dots, u^{(i-1)}) = \begin{cases} \phi_P({}_0\tau_P(u)^i) P^{im} + \cdots, & \text{if } m < -1 \\ \phi_P(\prod_{j=1}^{i-1}(uP - jP')) P^{-i} + \cdots, & \text{if } m = -1. \end{cases}$$

Proof. Since P is normal, $(P, P') = (1)$, and this is then Lemma 2.2 (i) of Singer (1991).

Lemma 8.3. *Let $u \in k(x) \setminus \{0\}$ and $P \in k[x]$ be monic normal irreducible. Let $L = \sum_{i=0}^n f_i \partial^i$ where $f_0, \dots, f_n \in k(x)$, $f_n = 1$, and R be given by (3). Then,*

$$R(u) = 0 \implies \nu_P(u) \geq -\delta_P(L).$$

Proof. Let $m = \nu_P(u)$, $m_i = \nu_P(f_i)$ for $i = 1 \dots n$, and suppose that $m < -1$.

By Lemma 8.2, the P-adic expansion of P_i is

$$P_i(u, \dots, u^{(i-1)}) = \phi_P({}_0\tau_P(u)^i) P^{im} + \cdots$$

for any integer $i \geq 0$. By Lemma 4.4, the P-adic expansion of f_i for $f_i \neq 0$ is

$$f_i = {}_0\tau_P(f_i) P^{m_i} + \cdots .$$

Hence, the P-adic expansion of $f_i P_i$ for $f_i \neq 0$ is

$$f_i P_i(u, \dots, u^{(i-1)}) = \phi_P({}_0\tau_P(f_i)\,{}_0\tau_P(u)^i) P^{im+m_i} + \cdots .$$

$\phi_P({}_0\tau_P(f_i)\,{}_0\tau_P(u)^i) \neq 0$ by Lemma 4.3. In particular, $f_n = 1$, so the P-adic expansion of $f_n P_n$ is

$$f_n P_n(u, \dots, u^{(n-1)}) = \phi_P({}_0\tau_P(u)^n) P^{nm} + \cdots .$$

Since $R(u) = 0$ and $nm < 0$, there must exist $i \neq j$ such that $im + m_i = jm + m_j$ (otherwise we would have $\nu_P(R(u)) < 0$), so $m = (m_j - m_i)/(i-j) \geq -\delta_P(L)$.

We can now find a part of the denominator of any non-zero solution $u \in k(x)$ of $R(u) = 0$.

Theorem 8.4. *Let k be a differential field of characteristic 0, and x be a monomial over k. Let $m > 0$ be an integer and $f_0, \dots, f_m \in k(x)$ with $f_m = 1$. Let $L = \sum_{i=0}^m f_i \partial^i$, and for $i = 0, \dots, m$, let $f_i = f_{ip} + f_{is} + f_{in}$ be the canonical representation of f_i, where $f_{in} = A_i/D_i$, $A_i, D_i \in k[x]$, $(A_i, D_i) = (1)$, and D_i is monic. Let ${C_1}^{e_1} \cdots {C_q}^{e_q}$ be a balanced factorization of $D = \operatorname{lcm}(D_0, \dots, D_m)$ with respect to $\{f_{0n}, \dots, f_{mn}\}$, and*

$$T = {C_1}^{\delta_{C_1}(L)} \cdots {C_q}^{\delta_{C_q}(L)}.$$

Let $y \neq 0$ be such that $L(y) = 0$ and $u = y'/y \in k(x)$. Then,

(i) *For any normal $P \in k[x]$, $\nu_P(uT) < 0 \implies (P, D) = (1)$.*
(ii) *uT is simple.*
(iii) *u can be written in the form $R/T + Q'/Q + v$ where $v \in k(x)$ is reduced, $R, Q \in k[x]$, $\deg(R) < \deg(T)$, $(Q, D) = (1)$ and every irreducible factor of Q is normal.*

Proof. Let $y \neq 0$ be such that $L(y) = 0$ and $u = y'/y \in k(x)$. If $u = 0$, then uT is simple and $\nu_P(uT) = +\infty$ for any normal $P \in k[x]$. And $u = 0$ is of the form given by (iii) with $v = R = 0, Q = 1$, so suppose that $u \neq 0$. Since $L(y) = 0$, then $R(u) = 0$, where R is given by (3).

(i) and (ii): Let $P \in k[x]$ be monic normal irreducible. Then, $\nu_P(uT) = \nu_P(u) + \nu_P(T) \geq -\delta_P(L) + \nu_P(T)$ by Lemma 8.3.

$Case 1 : P \mid D$: then $P \mid C_{j_0}$ for some $j_0 \in \{1, \dots, q\}$. We write C for C_{j_0}. We have $(C, C_j) = (1)$ for $j \neq j_0$, and C is squarefree, so $\nu_P(T) = \nu_C(T) = \delta_C(L)$. But C is balanced w.r.t. $\{f_{0n}, \dots, f_{nm}\}$, so $\delta_C(L) = \delta_P(L)$ by Lemma 2.8. Hence, $\nu_P(uT) \geq 0$. Since this holds for any monic normal irreducible $P \in k[x]$, we have $\nu_Q(uT) < 0 \implies (Q, D) = (1)$ for any normal $Q \in k[x]$, which proves (i).

$Case 2 : (P, D) = (1)$: then $\nu_P(f_i) \geq 0$ for $i = 0, \dots, m$. Suppose that $\nu_P(u) < -1$. Then, $\nu_P(f_i P_i) \geq i\nu_P(u)$ for $i = 0, \dots, m-1$ and $\nu_P(f_m P_m) = m\nu_P(u)$ by Lemma 8.2. Hence $\nu_P(R(u)) = m\nu_P(u) < 0$, in contradiction with $R(u) = 0$. Thus, $\nu_P(u) \geq -1$. But $\nu_P(T) = 0$, so $\nu_P(uT) \geq -1$.

Thus, $\nu_P(uT) \geq -1$ in both cases, so uT is simple.

(iii): From (i) and (ii), u can be written in the form

$$u = \frac{R}{T} + \sum_{i=1}^{s} \frac{B_i}{Q_i} + w$$

where $w \in k(x)$ is reduced, $Q_1, \ldots, Q_s \in k[x]$ are monic normal irreducible, $(Q_i, D) = (1)$, $\deg(B_i) < \deg(Q_i)$ and $\deg(R) < \deg(T)$. Let $P = Q_{i0}$ for $i_0 \in \{1, \ldots, s\}$. Then, $\nu_P(u) = -1$, so by Lemmas 8.2 and 4.4, the P-adic expansion of $f_i P_i$ for $f_i \neq 0$ is

$$f_i P_i(u, \ldots, u^{(i-1)}) = \phi_P\left({}_0\tau_P(f_i) \prod_{j=1}^{i-1}(uP - jP')\right)) P^{\nu_P(f_i)-i} + \cdots .$$

But $\nu_P(f_i) \geq 0$ for $i = 0, \ldots, m$ since $(P, D) = (1)$, and $f_m = 1$, so the P-adic expansion of $R(u)$ is

$$R(u) = \phi_P\left(\prod_{j=1}^{m-1}(uP - jP')\right) P^{-m} + \cdots .$$

Hence there exists an integer $j_{i_0} \in \{1, \ldots, m-1\}$ such that $\phi_P(uP) = \phi_P(j_{i_0} P')$. But $\phi_P(uP) = B_{i_0}$, so there exists $H_{i_0} \in k[x]$ such that $j_{i_0} P' = H_{i_0} P + B_{i_0}$, so u is of the form

$$u = \frac{R}{T} + \sum_{i=1}^{s} j_i \frac{Q_i{}'}{Q_i} - \sum_{i=1}^{s} H_i + w = \frac{R}{T} + \frac{Q'}{Q} + v$$

where $v = w - \sum_{i=1}^{s} H_i$ is reduced, and $Q = \prod_{i=1}^{s} Q_i{}^{j_i} \in k[x]$ is such that $(Q, D) = (1)$ and every irreducible factor of Q is normal.

Although Theorem 8.4 gives an ansatz for any solution of $R(u) = 0$, it does not yield a rational algorithm. Clearly, one can set

$$u = \sum_{i=1}^{q} \sum_{j=1}^{\delta_{C_i}(L)} \frac{R_{ij}}{C_i^{\,j}} + \frac{Q'}{Q} + v \tag{4}$$

where the $v \in k(x)$ is reduced, the R_{ij}'s are in $k[x]$, $\deg(R_{ij}) < \deg(C_i)$, and the C_i's and $\delta_{C_i}(L)$'s are given by Theorem 8.4. When x is a Liouvillian monomial, the procedure of Proposition 2.3 of (Singer, 1991) can be used to find bounds for $\nu_\infty(v)$ and $\nu_0(v)$, and (4) can be replaced by an equivalent form with $v \in k$. Looking at the C_i-adic expansion of $R(u)$ (which is well-defined) we can find a polynomial $H_i \in (k[x]/(C_i))[Y]$ such that $H_i(R_{i\delta_{C_i}(L)}) = 0$ in $k[x]/(C_i)$, so $Y - R_{i\delta_{C_i}(L)}$

must divide H_i in $(k[x]/(C_i))[Y]$. In the case where C_i is irreducible over $k[x]$, $k[x]/(C_i)$ is a field, so $(k[x]/(C_i))[Y]$ is a unique factorization domain, so factoring H_i over $k[x]/(C_i)$ yields all its roots. When C_i is reducible, we do not have unique factorization: $Y(Y-2) = (Y-(1+X))(Y-(1-X))$ in $(\mathbf{Q}[X]/(X^2-1))[Y]$. Thus, one is still forced to look at the P-adic expansions of u at all the irreducible factors P of each C_i in order to find the R_{ij}'s. A rational algorithm for finding the solutions in $K = k[X]/(C)$ of algebraic equations with coefficients in K when $C \in k[X]$ is squarefree would however yield a rational algorithm for finding the solutions of $R(u) = 0$ in $k(x)$.

9. Extending the constant field

Let k be a differential field of characteristic 0, C be the constant field of k, L be a linear ordinary differential operator with coefficients in k and $g \in k$. The algorithms presented in this paper do not require C to be algebraically closed, and can be used to find either a solution of $L(y) = g$ in k, or a basis over C for the solutions of $L(y) = 0$ in k. However, algorithms for finding Liouvillian solutions of such equations need to find either a solution in $\overline{C}k$ of $L(y) = g$, or a basis over $\overline{C}$ for the solutions of $L(y) = 0$ in $\overline{C}k$, where $\overline{C}$ is the algebraic closure of C. We show in this section, that it is in fact sufficient to solve those problems without extending C, since a basis over C for the solutions of $L(y) = 0$ in k is also a basis over $\overline{C}$ for the solutions in $\overline{C}k$.

Theorem 9.1. *Let k be a differential field of characteristic 0, $\overline{k}$ be the algebraic closure of k, C be the constant field of k, $\overline{C}$ be the algebraic closure of C, L be a linear ordinary differential operator with coefficients in k and $g \in k$. Then,*

- (i) *if $L(y) = g$ has a solution in $\overline{k}$, then it has one in k,*
- (ii) *let V be the vector space generated over C by the solutions in k of $L(y) = 0$, and $\overline{V}$ be the vector space generated over $\overline{C}$ by the solutions in $\overline{C}k$ of $L(y) = 0$. Then $\dim_C(V) = \dim_{\overline{C}}(\overline{V})$ and any basis for V over C is also a basis for $\overline{V}$ over $\overline{C}$.*

Proof. (i) Let $\alpha \in \overline{k}$ be a solution of $L(y) = g$. $k(\alpha)$ is finite algebraic over k, so applying the trace from $k(\alpha)$ to k, we get

$$ng = Tr_k^{k(\alpha)}(g) = Tr_k^{k(\alpha)}(L(\alpha)) = L(Tr_k^{k(\alpha)}(\alpha))$$

so $\beta = Tr_k^{k(\alpha)}(\alpha)/n$ is a solution in k of $L(y) = g$, where $n = \dim_k(k(\alpha))$.
(ii) Let $m = \dim_{\overline{C}}(\overline{V})$ and $\alpha_1, \dots, \alpha_m$ be a basis for $\overline{V}$ over $\overline{C}$. Let $\alpha \in \overline{C}$ be such that $k(\alpha_1, \dots, \alpha_m) = k(\alpha)$, and let $P = X^n + u_{n-1}X^{n-1} + \cdots + u_1X + u_0 \in k[X]$ be the minimal irreducible polynomial for α over k. Then, $(1, \alpha, \dots, \alpha^{n-1})$ is a basis for $k(\alpha)$ over k. We have

$$0 = P(\alpha) = P(\alpha)' = u'_{n-1}\alpha^{n-1} + \cdots + u'_1\alpha + u'_0$$

so, since P is minimal, $u_i' = 0$ for $i = 0, \ldots, n-1$, so $P \in C[X]$. Since P is irreducible over k, it is also irreducible over C, so $[C(\alpha) : C] = n$ and $(1, \alpha, \ldots, \alpha^{n-1})$ is also a basis for $C(\alpha)$ over C. Since it is a basis for $k(\alpha) = k(\alpha_1, \ldots, \alpha_m)$ over k, write $\alpha_i = \sum_{j=0}^{n-1} a_{ij}\alpha^j$ for $i = 1, \ldots, m$ where the a_{ij}'s are in k. Since L is $\overline{C}$-linear, we have

$$0 = L(\alpha_i) = L(\sum_{j=0}^{n-1} a_{ij}\alpha^j) = \sum_{j=0}^{n-1} L(a_{ij})\alpha^j$$

so $L(a_{ij}) = 0$ hence $a_{ij} \in V$ for $1 \le i \le m$ and $0 \le j < n$. Let $q = \dim_C(V)$ and $(b_1, \ldots, b_q)$ be a basis for V over C and write $a_{ij} = \sum_{l=1}^{q} c_{ijl} b_l$ where the c_{ijl}'s are in C. Let $v \in \overline{V}$, then there exist $d_1, \ldots, d_m \in \overline{C}$ such that $v = \sum_{i=1}^{m} d_i \alpha_i$. We then have

$$v = \sum_{i=1}^{m} d_i\alpha_i = \sum_{i=1}^{m}\sum_{j=0}^{n-1} d_i a_{ij}\alpha^j = \sum_{i=1}^{m}\sum_{j=0}^{n-1}\sum_{l=1}^{q} d_i c_{ijl} b_l \alpha^j = \sum_{l=1}^{q}\left(\sum_{i=1}^{m}\sum_{j=0}^{n-1} d_i c_{ijl}\alpha^j\right) b_l$$

so $(b_1, \ldots, b_q)$ generates $\overline{V}$ over $\overline{C}$.

Suppose now that $\sum_{l=1}^{q} c_l b_l = 0$ for $c_1, \ldots, c_l \in \overline{C}$, and write $c_l = \sum_{j=0}^{n-1} d_{lj}\alpha^j$ where the d_{lj}'s are in C. Then,

$$0 = \sum_{l=1}^{q} c_l b_l = \sum_{l=1}^{q}\sum_{j=0}^{n-1} d_{lj}\alpha^j b_l = \sum_{j=0}^{n-1}\left(\sum_{l=1}^{q} d_{lj} b_l\right)\alpha^j$$

so $\sum_{l=1}^{q} d_{lj} b_l = 0$ for $j = 0, \ldots, n-1$ since $(1, \alpha, \ldots, \alpha^{n-1})$ is a basis for $k(\alpha)$ over k. But $(b_1, \ldots, b_q)$ is a basis for V over C, so $d_{jl} = 0$ for $j = 0, \ldots, n-1$ and $l = 1, \ldots, q$. Hence $c_l = 0$ for $l = 1, \ldots, q$, so $(b_1, \ldots, b_q)$ is linearly independent over $\overline{C}$. Thus it is a basis for $\overline{V}$ over $\overline{C}$ and $q = m$.

Conclusions

We have shown that Abramov's (1989) notion of a balanced factorization can be used in arbitrary monomial extensions to find the denominators of the solutions of linear and Ricatti-type ordinary differential equations. This asnwers question (a) from Singer's paper (1991), making one step of his algorithm for finding solutions of such equations more effective and easier to implement. We have also shown that assuming an algebraically closed constant field is not necessary when Ricatti-type equations do not appear, which is the case when the coefficients of the equation do not involve exponentials. Another consequence is that solving Risch differential equations (i.e. equations of the type $y' + fy = \sum_{j=1}^{m} c_j g_j$) can now be done rationally in algebraic curves over primitive extensions, thereby allowing symbolic integration algorithms to handle transcendental elementary functions over such curves. Although the theory was complete before (Bronstein, 1990a), there has been no reported implementation of a Risch differential equation solver over algebraic curves, even in the so-called "purely algebraic case". A detailed presentation of a rational algorithm for such equations has appeared in a separate paper (Bronstein, 1991).

There still remain effectiveness questions, in particular the number of iterations required in Singer's algorithm for bounding the degree of the polynomial part of a solution in the primitive case is not known. It is hoped that experimenting with an implementation might point to a formula for this number.

Finally, it is yet unclear whether Theorem 8.4 can be used constructively to yield a rational algorithm for solving Ricatti-type equations. In its current state, it only describes the structure of any solution.

I would like to thank John Abbott and Michael Singer for their attentive reading of this paper and for their useful suggestions.

References

Abramov, S.A. (1989), *Rational Solutions of Linear Differential and Difference Equations with Polynomial Coefficients (in russian)*, Journal of Computational Mathematics and Mathematical Physics **29, No.11**, 1611–1620.

Bronstein, M. (1990*a*), *Integration of Elementary Functions*, Journal of Symbolic Computation **9, No.2**, 117–173.

Bronstein, M. (1990*b*), *A Unification of Liouvillian Extensions*, Applicable Algebra in Engineering, Communication and Computing **1, No.1**, 5–24.

Bronstein, M. (1991), *The Risch Differential Equation on an Algebraic Curve*, Proceedings of ISSAC '91, ACM Press, New York, pp. 241–246.

Davenport, J.H. (1984), *Intégration Algorithmique des Fonctions Elémentairement Transcendantes sur une Courbe Algébrique*, Annales de l'Institut Fourier **34, fasc.2**, 271–276.

Risch, R. (1968), *On the Integration of Elementary Functions which are built up using Algebraic Operations,*, Report SP-2801/002/00, System Development Corp., Santa Monica, CA..

Schwarz, F. (1989), *A Factorization Algorithm for Linear Ordinary Differential Equations*, Proceedings of ISSAC '89, ACM Press, New York, pp. 17–25.

Singer, M.F. (1991), *Liouvillian Solutions of Linear Differential Equations with Liouvillian Coefficients*, Journal of Symbolic Computation **11, No.3**, 251–273.