Solving linear ordinary differential equations over $C(x, e^{\int f(x)dx})$

Manuel Bronstein
INRIA – Projet CAFÉ
2004 Route des Lucioles, BP 93
F-06902 Sophia Antipolis Cedex
Manuel.Bronstein@sophia.inria.fr

Anne Fredet
Laboratoire GAGE
Ecole Polytechnique
F-91128 Palaiseau Cedex
fredet@ariana.polytechnique.fr

January 10, 1999

Abstract

We describe a new algorithm for computing the solutions in $F = C(x, e^{\int f(x)dx})$ of linear ordinary differential equations with coefficients in F. Compared to the general algorithm of [6], our algorithm avoids the computation of exponential solutions of equations with coefficients in $C(x)$, as well as the solving of linear differential systems over $C(x)$. Our method is effective and has been implemented.

1 Introduction

Definition 1 *Let K be a differential field of characteristic* 0 *and $L = \sum_{i=0}^{n} a_i \partial^i$ be a linear ordinary differential operator with coefficients in K. A* rational solution *of L is any element $y \in K$ such that $Ly = 0$, and an* exponential solution *of L is any element $u \in K$ such that $Le^{\int u} = 0$.*

Although our main goal is to compute the rational solutions of such equations, it turns out to be more useful to solve the following, slightly more general problem.

Definition 2 *We say that we can* effectively solve parameterized linear differential equations over K *if given any linear ordinary differential operator $L = \sum_{i=0}^{n} a_i \partial^i$ with coefficients in K and $g_1, \dots, g_m$ in K, we can effectively find $h_1, \dots, h_r$ in K and a matrix M with $r + m$ columns and coefficients in $C(K)$ such that $Ly = \sum_{j=1}^{m} c_j g_j$ for $y \in K$ and $c_1, \dots, c_m \in C(K)$ if and only if $y = \sum_{k=1}^{r} y_k h_k$ where $y_1, \dots, y_r \in C(K)$ and $M(y_1, \dots, y_r, c_1, \dots, c_m)^T = 0$.*

In [6], Singer gave an algorithm that reduced the problem of solving parameterized linear differential equations over a Liouvillian extension $E = K(t)$

of K to solving such equations over K *and,* in the case where t is exponential over K, to compute all the exponential solutions of linear ordinary differential equations over K. His method, although algorithmic, suffers from several difficulties, mainly the requirement to compute exponential solutions in Liouvillian towers, and the reduction to linear differential systems rather than scalar equations once the order and degree of (Laurent–)polynomial solutions are bounded. To our knowledge, that method has not been implemented, even for the case where $K = \mathbb{Q}(x)$. In this paper, we describe an alternative algorithm that does not require computing exponential solutions over $C(x)$ when E is of the form $C(x, e^{\int f(x)dx})$ and $' = d/dx$. Furthermore, for exponential extensions of an arbitrary differential field K, our algorithm directly produces scalar equations over K (without increasing the order) rather than differential systems.

Let now C be an arbitrary field of characteristic 0, x be transcendental over C and $E = C(x,t)$ be a differential extension of $(C(x), d/dx)$ where $dt/dx = ft$ for some $f \in C(x)$, *i.e.* $t = e^{\int f(x)dx}$. We write $'$ for d/dx throughout this paper. There are three separate steps in solving the parametrized equation $Ly = \sum_{j=1}^{m} c_j g_j$ for $y \in E$ and $c_1, \ldots, c_m \in C$:

1. compute the "denominator" of y, *i.e.* compute $q \in C(x)[t]$ such that $qy \in C(x)[t, t^{-1}]$ for any solution y. Replacing y by Y/q in the parameterized equation, this reduces the problem to solving a similar equation for $Y \in C(x)[t, t^{-1}]$;

2. bound the degree and order of Y, *i.e.* compute integers $\delta \leq \gamma$ such that any solution $Y \in C(x)[t, t^{-1}]$ must be of the form
$$Y = y_\delta t^\delta + \ldots + y_\gamma t^\gamma \quad \text{where } y_\delta, \ldots, y_\gamma \in C(x)\,,$$

3. compute the solution Y knowing δ and γ.

In the case when t is transcendental over $C(x)$ and the constant subfield of E is C (we will eventually ensure those conditions), then the first step is done using either Lemma 3.2 of [6] or Theorem 5.5 of [3], so we address only the last two steps in this paper. The third step is done in [6] by replacing Y by $\sum_{i=\delta}^{\gamma} y_i t^i$ in the equation and computing the rational solutions of the resulting linear differential system for the y_i's.

The rest of this paper is organized as follows: some preliminary results about exponential extensions are given in section 2, then simplified bounding algorithms are described in sections 3 and 4, and a new algorithm for the third step in arbitrary exponential extensions is described in section 5.

Notation: for any field k, Z transcendental over k, and any $f \in k(Z)^*$, let $\sum_{i\geq 0} a_i Z^{d+i}$ and $\sum_{j\geq 0} b_j Z^{e-i}$ be the Laurent expansions of f at $Z = 0$ and $Z = \infty$ respectively where $a_0 \neq 0 \neq b_0$. We write $d = \nu_Z(f)$ (the order of f), $e = \deg_Z(f)$ (the degree of f) and $b_0 = \mathrm{lc}_Z(f)$ (the leading coefficient of f). For any nonzero linear ordinary diffential operator with coefficients in $k(Z)$, $L = a_n\partial^n + a_{n-1}\partial^{n-1} + \ldots + a_0$, we write $\deg_Z(L) = \max_{0\leq i\leq n}(\deg_Z(a_i))$ and $\nu_Z(L) = \min_{0\leq i\leq n}(\nu_Z(a_i))$. We omit the subscripts when the context is clear (to prevent confusion, we never use $\deg(L)$ for the order of L).

2 Preliminaries

We group in this section some known results about exponential extensions that will be used by our algorithm. Let $(K,')$ be an arbitrary differential field of characteristic 0.

Lemma 1 *For any $a_0, \ldots, a_n, a, b \in K$ with $b \neq 0$,*

$$\left(\sum_{i=0}^{n} a_i \partial^i\right)(ab) = b\left(\sum_{i=0}^{n} a_i \left(\partial + \frac{b'}{b}\right)^i\right) a\,.$$

Proof. The formula is trivial for $n = 0$, so assumes it holds for operators of order up to $n - 1$. We have

$$\begin{aligned} b\left(\sum_{i=0}^{n} a_i \left(\partial + \frac{b'}{b}\right)^i\right) a &= b a_0 a + b\left(\sum_{i=0}^{n-1} a_{i+1} \left(\partial + \frac{b'}{b}\right)^i\right)\left(a' + \frac{b'}{b} a\right) \\ &= a_0 a b + \left(\sum_{i=0}^{n-1} a_{i+1} \partial^i\right)(a'b) + \left(\sum_{i=0}^{n-1} a_{i+1} \partial^i\right)(ab') \\ &= \left(\sum_{i=0}^{n} a_i \partial^i\right)(ab)\,. \end{aligned}$$

Lemma 2 *Let E be a differential extension of K and $t \in E^*$ be such that $t'/t \in K$. Then, for any linear ordinary differential operator L with coefficients in K,*

$$\frac{L(at^m)}{t^m} \in K \quad \textit{for any integer } m \textit{ and any } a \in K\,.$$

Proof. Write $L = \sum_{i=0}^{n} a_i \partial^i$ where the a_i's are in K. By Lemma 1,

$$L(at^m) = \left(\sum_{i=0}^{n} a_i \partial^i\right)(at^m) = t^m \left[\left(\sum_{i=0}^{n} a_i \left(\partial + m\frac{t'}{t}\right)^i\right) a\right] = t^m b$$

where $b \in K$ since $t'/t \in K$. $\square$

We now introduce the construction of "projected" operators: let E be a differential extension of K and $t \in E \setminus K$ be transcendental over K. We can uniquely decompose any linear ordinary differential operator L with coefficients in $K[t]$ as

$$L = \sum_{k=\nu(L)}^{\deg(L)} t^k L_k \tag{1}$$

where the L_k's are linear ordinary diffential operators with coefficients in K (the "projections" of L with respect to t). Note that $L_{\nu(L)} \neq 0 \neq L_{\deg(L)}$.

The following, whose proof is present in [6], is the basis of all the algorithms for bounding the order and degree of (Laurent–)polynomial solutions.

Proposition 1 *Let E be a differential extension of K, $t \in E$ be transcendental and exponential over K, L be a linear ordinary diffential operators with coefficients in $K[t]$ and $b_1, \dots, b_m \in K(t)$. If there are integers $\delta \le \gamma$, $y_\delta, \dots, y_\gamma \in K$ and $c_1, \dots, c_m \in C(K)$ such that $y_\delta \neq 0 \neq y_\gamma$ and*

$$L\big(y_\delta t^\delta + \ldots + y_\gamma t^\gamma\big) = c_1 b_1 + \ldots + c_m b_m\,, \tag{2}$$

then,

(i) either $\delta \ge \min_{1\le j\le m}(\nu(b_j)) - \nu(L)$ or $L_{\nu(L)}(y_\delta t^\delta) = 0$;

(ii) either $\gamma \le \max_{1\le j\le m}(\deg(b_j)) - \deg(L)$ or $L_{\deg(L)}(y_\gamma t^\gamma) = 0$;

where the minimum and maximum are taken over the nonzero b_j's.

Proof. Using the decomposition (1) we have

$$L\big(y_\delta t^\delta + \ldots + y_\gamma t^\gamma\big) = \sum_{k=\nu(L)}^{\deg(L)} t^k L_k\left(\sum_{i=\delta}^{\gamma} y_i t^i\right) = \sum_{k=\nu(L)}^{\deg(L)} \sum_{i=\delta}^{\gamma} z_{ki} t^{k+i} \tag{3}$$

where $z_{ki} = L_k(y_i t^i)/t^i$ is in K by Lemma 2.
(i) Suppose that $\delta < \min_{1\le j\le m}(\nu(b_j)) - \nu(L)$. It then follows from (2) and (3) that $z_{\nu(L)\delta} = 0$, hence that $L_{\nu(L)}(y_\delta t^\delta) = 0$.
(ii) Suppose that $\gamma > \max_{1\le j\le m}(\deg(b_j)) - \deg(L)$. It then follows from (2) and (3) that $z_{\deg(L)\delta} = 0$, hence that $L_{\deg(L)}(y_\gamma t^\gamma) = 0$. □

This reduces the problem to bounding the integers m such that $L(at^m) = 0$ for $a \in K^*$ and L an operator with coefficients in K.

Definition 3 *Let $K(z)$ be a differential field with z transcendental over K and E be a differential extension of $K(z)$. We say that $t \in E^*$ is* effectively exponential over $K(z)$ *if*

$$\frac{t'}{t} + c\frac{f'}{f} \in K(z) \setminus K \quad \forall c \in \mathbb{Q}, \forall f \in K(z)^*\,.$$

We also say that a differential extension F of $K(z)$ is effectively exponential over $K(z)$ *if $F = K(z,t)$ where $t \in F^*$ is effectively exponential over $K(z)$.*

Note that if t is effectively exponential over $K(z)$, then it is exponential over $K(z)$ and $nt'/t \neq v'/v$ for any nonzero integer n and any $v \in K(z)^*$. This implies ([4, Theorem 5.1.2]) that t is transcendental over $K(z)$, that the constants fields of $K(z)$ and $K(z,t)$ are the same, and that the only monic irreducible $p \in K(z)[t]$ that divides its derivative in $K(z)[t]$ is $p = t$. In the sequel, we use different bounding algorithms for effectively exponential and non–effectively exponential extensions of $(C(x), d/dx)$.

3 Non–effectively exponential extensions

We now return to the case $E = C(x,t)$, a differential extension of $(C(x), d/dx)$ with $t'/t \in C(x)$. Since we do not not offer any improvement for the algebraic case of [6], we make the additional assumption that t is transcendental over $C_E(x)$ where C_E is the constant field of E. Assume in this section that t not effectively exponential over $C(x)$. Then, there exist $f \in C(x)^*$, $r \in C$ and $M, N \in \mathbb{Z}$ with $N \neq 0$ such that $t'/t = r + (M/N)(f'/f)$. If $r = 0$, then $c = t^N/f^M$ is a constant and t is algebraic over $C(c)(x)$ in contradiction with our hypothesis, so we can assume that $r \neq 0$, which implies that the Laurent expansion at $x = \infty$ of t'/t has the form

$$\frac{t'}{t} = r + \sum_{i>0} r_i x^{-i}\,. \tag{4}$$

In addition, our hypothesis that t'/t is not of the form qg'/g for $q \in \mathbb{Q}$ and $g \in C(x)^*$ implies ([4, Theorem 5.1.2]) that the constant field of E is C. As a consequence of Proposition 1, we only have to bound the integers h such that $L(at^h) = 0$ for $a \in C(x)^*$ given any operator L with coefficients in $C(x)$. Let $L = a_n\partial^n + a_{n-1}\partial^{n-1} + \ldots + a_0$ be such an operator. We define the r-characteristic equation of L at infinity to be

$$E_r(L) = \sum_{i \mid \deg_x(a_i) = \deg_x(L)} \mathrm{lc}_x(a_i) r^i Z^i \quad \in C[Z]\,.$$

Lemma 3 *If $L(at^h) = 0$ for an operator L with coefficients in $C(x)$, an integer h and $a \in C(x)^*$, then $E_r(L)(h) = 0$.*

Proof. If $L(at^h) = 0$, then, using Lemma 1 and that $t \neq 0$, we have

$$\left(\sum_{i=0}^{n} a_i \left(\partial + h\frac{t'}{t}\right)^i\right) a = 0\,. \tag{5}$$

Let $a = \sum_{k\geq 0} c_k x^{e-k}$ be the Laurent expansion of a at $x = \infty$ where $c_0 \neq 0$. Then, using (4), the Laurent expansion of $a_i(\partial + ht'/t)^i a$ has the form

$$\mathrm{lc}_x(a_i) h^i r^i c_0 x^{e+\deg_x(a_i)} + \ldots$$

and the Laurent expansion of the left side of (5) is of the form

$$E_r(L)(h) c_0 x^{e+\deg_x(L)} + \ldots$$

which implies that $E_r(L)(h) = 0$. □

Theorem 1 *Let L be a linearly differential operator with coefficients in $C(x,t)$ and $b_1, \ldots, b_m \in C(x,t)$. If there are integers $\delta \leq \gamma$, $y_\delta, \ldots, y_\gamma \in C(x)$ and $c_1, \ldots, c_m \in C$ such that $y_\delta \neq 0 \neq y_\gamma$ and*

$$L\big(y_\delta t^\delta + \ldots + y_\gamma t^\gamma\big) = c_1 b_1 + \ldots + c_m b_m \tag{6}$$

then,

(i) *either* $\delta \geq \min_{1\leq j\leq m}(\nu_t(b_j)) - \nu_t(L)$ *or* $E_r(L_{\nu_t(L)})(\delta) = 0$;

(ii) *either* $\gamma \leq \max_{1\leq j\leq m}(\deg_t(b_j)) - \deg_t(L)$ *or* $E_r(L_{\deg_t(L)})(\gamma) = 0$,

where $L_{\nu_t(L)}$ *and* $L_{\deg_t(L)}$ *are given by (1), and the minimum and maximum are taken over the nonzero* b_j*'s.*

Proof. This follows immediately from Proposition 1 and Lemma 3. □

As a consequence, if we have an algorithm for computing the integer roots of polynomials in $C[Z]$, then we can bound the order and degree of the solutions in $C(x)[t, t^{-1}]$ of parameterized linear differential equations with coefficients in $C(x, t)$.

4 Effectively exponential extensions

We now consider the case $E = C(x, t)$ where t is effectively exponential over $(C(x), d/dx)$, which implies that t is transcendental over $C(x)$ and that the constant subfield of E is C. Let $u \in C(x)$ and $y = e^{\int u dx}$. Then, $y^{(i)} = P_i(u, u', \ldots, u^{(i-1)})y$ where the P_i's are polynomials with integer coefficients given by

$$P_0 = 1 \quad \text{and} \quad P_i = P'_{i-1} + uP_{i-1} \quad \text{for } i > 0\,. \tag{7}$$

Let $L = \sum_{i=0}^{n} a_i \partial^i$ be a linear ordinary differential operator with coefficients in $C(x)$. If $Le^{\int u dx} = 0$, then

$$a_n P_n(u, \ldots, u^{(n-1)}) + a_{n-1} P_{n-1}(u, \ldots, u^{(n-2)}) + \ldots + a_0 = 0\,,$$

and the above equation is called the *Riccati equation associated with* L. We need the following 2 Lemmas, which are special cases of Lemma 2.2 of [6] and whose proofs can be found there.

Lemma 4 ([6]) *Let* $p \in C[x]$ *be irreducible, and* $u \in C(x)$ *have* p*-adic expansion of the form* $u = u_\gamma/p^\gamma + \ldots$ *where* $\gamma > 0$, $u_\gamma \neq 0$ *and* $\deg u_\gamma < \deg p$. *Then, for* $i \geq 1$ *the* p*-adic expansion of* $P_i(u, \ldots, u^{(i-1)})$ *has the form*

$$\begin{cases} v_{i\gamma}/p^{i\gamma} + \ldots & \textit{where } v_{i\gamma} \equiv u_\gamma^i \pmod p & \textit{if } \gamma > 1\,, \\ v_i/p^i + \ldots & \textit{where } v_i \equiv \prod_{j=0}^{i-1}(u_1 - jp') \pmod p & \textit{if } \gamma = 1\,. \end{cases}$$

Lemma 5 ([6]) *Let* $u \in C(x)$ *have a Laurent expansion at* $x = \infty$ *of the form* $u = \sum_{i\geq 0} u_i x^{\gamma - i} + \ldots$ *where* $\gamma \geq 0$ *and* $u_\gamma \neq 0$. *Then, for* $i \geq 1$ *the Laurent expansion at* $x = \infty$ *of* $P_i(u, \ldots, u^{(i-1)})$ *has the form*

$$\begin{cases} u_0^i x^{i\gamma} + \ldots & \textit{if } \gamma > 0\,, \\ P_i(u_0, \ldots, u_0^{(i-1)}) + \ldots & \textit{if } \gamma = 0\,. \end{cases}$$

During the bounding process, we may have to compute the integer solutions of some algebraic equations. The following Lemma shows that the systems that arise have finitely many such solutions.

Lemma 6 *Let $K \subset F$ be fields of characteristic 0 and $p \in F[Z]$ be irreducible with $\deg(p) = m$. Let $a_0, \dots, a_n \in F[Z]$ and $q, u \in F[Z]$ be linearly independent over K and such that $\deg(q) < m$ and $\deg(u) < m$. If $p \not| \gcd(a_0, \dots, a_n)$, then the set*

$$S = \{(\gamma, \alpha) \in K^2 \text{ such that } \sum_{i=0}^{n} a_i(\gamma u + \alpha q)^i \equiv 0 \pmod{p}\}$$

is finite with at most n elements.

Proof. Let $\pi : F[Z] \to F[Z]/(p)$ be the canonical projection and $Q = \sum_{i=0}^{n} \pi(a_i)T^i \in (F[Z]/(p))[T]$. Since $p \not| \gcd(a_0, \dots, a_n)$, Q is not identically 0 and has degree at most n, so let $\beta_1, \dots, \beta_k$ with $k \le n$ be its distinct roots in $F[Z]/(p)$, and let $p_1, \dots, p_k \in F[Z]$ be such that $\deg(p_j) < m$ and $\pi(p_j) = \beta_j$ for each j. For any $(\gamma, \alpha) \in S$, we have $Q(\gamma\pi(u) + \alpha\pi(q)) = 0$, which implies that $\pi(\gamma u + \alpha q) = \pi(p_j)$ for some j, hence that $\gamma u + \alpha q = p_j$ since the degrees of u, q and p_j are strictly less than m. But for each j, there is at most one pair $(a, b) \in K^2$ such that $au + bq = p_j$, since the difference of two such relations with distinct pairs would yield a linear dependence over K for u and q. Therefore, S has at most n elements. □

We now return to bounding the integers h such that $L(at^h) = 0$ for $a \in C(x)^*$ and any operator L with coefficients in $C(x)$. For effectively exponential extensions, we replace the search for exponential solutions over $C(x)$ by the following adaptation of the algorithm of Proposition 2.3 of [6]. Our modification computes only the potential degrees of "monomial" solutions rather than all the exponential solutions.

Proposition 2 *Suppose that $E = C(x, t)$ where t is effectively exponential over $(C(x), d/dx)$, that we know a vector space basis for C over $\mathbb{Q}$, that we can factor polynomials in $C[Z]$ and compute their integer roots. Then, for any nonzero linear ordinary differential operator L with coefficients in $C(x)$, we can compute a finite set $\beta(L) \subset \mathbb{Z}$ such that if $L(at^\gamma) = 0$ for an integer γ and $a \in C(x)^*$, then $\gamma \in \beta(L)$.*

Proof. Write

$$L = A_n\partial^n + \ldots + A_0 \quad \text{where } A_i \in C[x], A_n \neq 0\,,$$

and

$$g = \frac{t'}{t} = G + \frac{A}{D} \quad \text{where } G, A, D \in C[x], D \neq 0 \text{ and } \deg(A) < \deg(D)\,.$$

Suppose that $L(at^\gamma) = 0$ for some $a \in C(x)^*$ and an integer γ. By adding 0 to $\beta(L)$, we can assume without loss of generality that $\gamma \neq 0$. We have

$$\sum_{i=0}^{n} A_i P_i(u, u', \dots, u^{(i-1)}) = 0 \tag{8}$$

where $u = a'/a + \gamma g$ and the P_i's are given by (7). Note that for any irreducible $p \in C[x]$, the p-adic expansion of a'/a is $a'/a = \nu q p^{-1} + \ldots$ where $\nu \in \mathbb{Z}$ is the order of a at p and $q \in C[x]$ is nonzero, has degree strictly less that $\deg(p)$ and satisfies $p' \equiv q \pmod{p}$. We distinguish several cases.

1. If $M = \deg(G) > 0$, then the Laurent expansion of g at $x = \infty$ has the form, $\mathrm{lc}(G)x^M + \ldots$, so the expansion of u is $\gamma \mathrm{lc}(G)x^M + \ldots$, and by Lemma 5, the expansion of $P_i(u, u', \ldots, u^{(i-1)})$ is $\gamma^i \mathrm{lc}(G)^i x^{iM} + \ldots$. Therefore, the expansion of the left-hand side of (8) is

$$\left(\sum_{i \mid \deg(A_i) + iM = \mu} \mathrm{lc}(A_i)\gamma^i \mathrm{lc}(G)^i \right) x^\mu + \ldots$$

where $\mu = \max_i(\deg(A_i) + iM)$. It follows that $Q(\gamma) = 0$ where

$$Q = \sum_{i \mid \deg(A_i) + iM = \mu} \mathrm{lc}(A_i)\mathrm{lc}(G)^i Z^i \quad \in C[Z]$$

and $\beta(L)$ is the set of all the integer roots of Q.

2. If there is an irreducible $p \in C[x]$ such that $p^2 \mid D$, then let $g = u_\beta / p^\beta + \ldots$ be the p-adic expansion of g where $\beta \geq 2$ and $u_\beta \in C[x]$ is nonzero and has degree strictly less than $\deg(p)$. The p-adic expansion of u is then $\gamma u_\beta / p^\beta + \ldots$, so by Lemma 4, the p-adic expansion of $P_i(u, u', \ldots, u^{(i-1)})$ is $v_{i\beta}/p^{i\beta} + \ldots$ where $v_{i\beta} \equiv \gamma^i u_\beta^i \pmod{p}$. Let

$$A_i = a_{\alpha_i} p^{\alpha_i} + \ldots \tag{9}$$

with $\alpha_i \geq 0$ be the p-adic expansion of each nonzero A_i and $\mu = \min_i(\alpha_i - i\beta)$. Then, the p-adic expansion of the left-hand side of (8) is

$$\left(\sum_{i \mid \alpha_i - i\beta = \mu} w_i \right) p^\mu + \ldots$$

where $w_i \equiv a_{\alpha_i} \gamma^i u_\beta^i \pmod{p}$. It follows that $Q(\gamma) \equiv 0 \pmod{p}$ where

$$Q = \sum_{i \mid \alpha_i - i\beta = \mu} a_{\alpha_i} u_\beta^i Z^i \quad \in C[x][Z]\,.$$

Computing the remainder of Q by p in $C[Z][x]$ (the leading coefficient of p being a unit in C[Z]) and equating each coefficient of x^j to 0, we get a system of polynomial equations $Q_0(\gamma) = \ldots = Q_{\deg(p)-1}(\gamma) = 0$, hence, $H(\gamma) = 0$ where $H = \gcd(Q_0, \ldots, Q_{\deg(p)-1}) \in C[Z]$. Note that H is not identically 0, since the leading coefficient of Q is $a_{\alpha_I} u_\beta^I \in (C[x]/(p))^*$ where $I = \max\{i \mid \alpha_i - i\beta = \mu\}$. As earlier, $\beta(L)$ is the set of all the integer roots of Q.

3. If there is an irreducible $p \in C[x]$ such that $p \mid D$, $p^2 \nmid D$ and u_1 and q are linearly independent over $\mathbb{Q}$, where $u_1, q \in C[x] \setminus \{0\}$ are given by $\deg(u_1) < \deg(p)$, $\deg(q) < \deg(p)$, $p' \equiv q \pmod{p}$ and $g = u_1 p^{-1} + \ldots$ is the p-adic expansion of g. Then, the p-adic expansion of u is $(\gamma u_1 + \nu q)p^{-1} + \ldots$, where $\nu \in \mathbb{Z}$ (note that ν can be 0 if p does not divide the numerator or denominator of a). By Lemma 4, the p-adic expansion of $P_i(u, u', \ldots, u^{(i-1)})$ is $v_i/p^i + \ldots$ where $v_i \equiv \prod_{j=0}^{i-1}(\gamma u_1 + \nu q - jp')$ $\pmod{p}$. Using (9), the p-adic expansion of the left-hand side of (8) is

$$\left(\sum_{i \mid \alpha_i - i = \mu} w_i\right) p^{\mu} + \ldots$$

where $\mu = \min_i(\alpha_i - i)$ and $w_i \equiv a_{\alpha_i} \prod_{j=0}^{i-1}(\gamma u_1 + \nu q - jp') \pmod{p}$. It follows that $Q(\gamma u_1 + \nu q) \equiv 0 \pmod{p}$ where

$$Q = \sum_{i \mid \alpha_i - i = \mu} a_{\alpha_i} \prod_{j=0}^{i-1} (Z - jp') \quad \in C[x][Z]\,.$$

As in the previous case, computing the remainder of Q by p in $C[Z][x]$ and equating it to 0, we get a system of polynomial equations $Q_0(\gamma, \nu) = \ldots = Q_{\deg(p)-1}(\gamma, \nu) = 0$ with coefficients in C. If that system has dimension 0, then we can compute (via resultants or Gröbner bases) a nontrivial univariate equation $H(\gamma) = 0$ where $H \in C[Z]$ is in the ideal generated by $Q_0, \ldots, Q_{\deg(p)-1}$. In that case, $\beta(L)$ is as earlier the set of all the integer roots of H. If the system has a stricly positive dimension, we then write $Q = \sum_{i=0}^{n} Q_i Z^i$ where $Q_0, \ldots, Q_n \in C[x]$. Since the leading coefficient of Q is a_{α_I} where $I = \max\{i \mid \alpha_i - i = \mu\}$ and $\deg(a_{\alpha_I}) < \deg(p)$, it follows that $p \nmid \gcd(Q_0, \ldots, Q_n)$, so by Lemma 6, the equation $Q(\gamma u_1 + \nu q) \equiv 0 \pmod{p}$ has a finite set of rational solutions, which we can compute in the following way: since we can factor elements of $C[Z]$, we can also factor elements of $(C[x]/(p))[Z]$ [5, §8.8], so the roots $\beta_1, \ldots, \beta_k$ of Q in $C[x]/(p)$ can be computed from its linear factors over $C[x]/(p)$. For each β_j, equating the powers of x on both sides of the equation $\gamma u_1 + \alpha q = \beta_j$ yields a linear system $A_j(\gamma, \alpha)^T = \mathbf{v_j}$ with coefficients in C for γ and α. Projecting that system on our basis for C over $\mathbb{Q}$, we get a matrix B_j and a vector $\mathbf{w_j}$, both with coefficients in $\mathbb{Q}$ such that the rational solutions of $A_j(\gamma, \alpha)^T = \mathbf{v_j}$ and $B_j(\gamma, \alpha)^T = \mathbf{w_j}$ are the same. If B_j is nonsingular, then that system has a unique solution, which we compute. Otherwise, that system has no solution since its set of rational solutions is finite. Selecting the integer solutions from the rational ones yields the set $\beta(L)$.

Suppose that none of the above cases is applicable, then $G \in C$ and every irreducible factor p of D must satisfy the following conditions: $p^2 \nmid D$, and $\{u_1, q\}$ are linearly dependent over $\mathbb{Q}$, where u_1 and q are defined as in the third case.

This linear dependence implies that for each such p, there is a rational number $r_p \in \mathbb{Q}$ such that p does not divide the denominator of $g - r_p p'/p$. Therefore, $\tilde{g} = g - \sum_{p|D} r_p p'/p \in C[x]$, where the sum is taken over all the irreducible factors of D. But the polynomial part of $\tilde{g}$ is $G \in C$, so $\tilde{g} \in C$. Writing $r_p = n_p/m$ for a common denominator m, we get $\tilde{g} = g - m^{-1}f'/f$ where $f = \prod_{p|D} p^{n_p} \in C(x)^*$, in contradiction with t effectively exponential over $C(x)$. $\square$

Theorem 2 *Suppose that $E = C(x,t)$ where t is effectively exponential over $(C(x), d/dx)$, that we know a vector space basis for C over $\mathbb{Q}$, that we can factor polynomials in $C[Z]$ and compute their integer roots. Then, for any nonzero linear ordinary differential operator L with coefficients in E and $b_1, \dots, b_m \in E$, we can compute finite sets $\Delta \subset \mathbb{Z}$ and $\Gamma \subset \mathbb{Z}$ such that if there are integers $\delta \le \gamma$, $y_\delta, \dots, y_\gamma \in C(x)$ and $c_1, \dots, c_m \in C$ such that $y_\delta \neq 0 \neq y_\gamma$ and*

$$L\big(y_\delta t^\delta + \ldots + y_\gamma t^\gamma\big) = c_1 b_1 + \ldots + c_m b_m\,,$$

then $\delta \in \Delta$ and $\gamma \in \Gamma$.

Proof. This follows immediately from Propositions 1 and 2. $\square$

5 Computing the solutions

We now turn back to the third step, namely computing the solutions once bounds on their degree and order are known. Throughout this section, let K be an arbitrary differential field of characteristic 0 and t be transcendental and exponential over K. Suppose that $C(K(t)) = C(K)$ and that we can effectively solve parameterized linear differential equations over K. Let L be a linear ordinary differential operator with coefficients in $K[t]$, $b_1, \dots, b_m \in K(t)$ and integers $\delta \le \gamma$ be given. We look for $y_\delta, \dots, y_\gamma \in K$ and $c_1, \dots, c_m \in C(K)$ such that $L\big(\sum_{i=\delta}^{\gamma} y_i t^i\big) = \sum_{j=1}^m c_j b_j$. Let $z = t^{-\delta} y$. We have $z \in K[t]$, $\deg(z) \le N = \gamma - \delta$ and, by Lemma 1, $Ly = L(t^\delta z) = t^\delta \tilde{L} z$ where $\tilde{L}$ is also an operator with coefficients in $K[t]$. It is thus sufficient to look for solutions $p \in K[t]$ of degree at most $N \ge 0$ of $Lp = \sum_{j=1}^m c_j b_j$. Dividing both sides by a power of t if necessary, we can assume that $\nu(L) = 0$. Let $d \in K[t]$ be a common denominator for the b_i's and write $b_i = f_i + g_i/d$ where $f_i, g_i \in K[t]$ and $\deg(g_i) < \deg(d)$. If $Lp = \sum_{j=1}^m c_j b_j$ for $p \in K[t]$, then

$$\frac{\sum_{j=1}^m c_j g_j}{d} = Lp - \sum_{j=1}^m c_j f_j \quad \in K[t]$$

which implies that $Lp = \sum_{j=1}^m c_j f_j$ and that $\sum_{j=1}^m c_j g_j = 0$. Equating the coefficients of each t^i to 0 in that last condition yields a matrix A with coefficients in K such that $A(c_1, \dots, c_m)^T = 0$. Using Lemma 7.1.2 of [4] and the associated algorithm, we construct a matrix B with coefficients in $C(K)$ such that the constant solutions of $A\mathbf{x} = 0$ and $B\mathbf{x} = 0$ are the same.

We are reduced to solving $Lp = \sum_{j=1}^{m} c_j f_j$ where $p, f_1, \ldots, f_m \in K[t]$ and $\deg(p) \le N$ for a given N.

If $N = 0$, then $p \in K$, so using the decomposition (1) our equation becomes

$$\sum_{k=0}^{\deg(L)} t^k L_k p = \sum_{j=1}^{m} c_j f_j$$

and equating the coefficients of each t^k on both sides we get either new linear constraints for the c_j's (if $k > \deg(L)$ or $L_k = 0$), or parameterized linear differential equations over K for p (if $L_k \neq 0$), which we can solve using the induction hypothesis.

If $N > 0$, write $p = p_0 + tq$ where $p_0 = p(0) \in K$ and $q \in K[t]$ with $\deg(q) < N$. Since $t'/t \in K$, the ideal (t) of $K[t]$ is closed under $'$, so the canonical projection $\pi : K[t] \to K = K[t]/(t)$, which sends $h \in K[t]$ to $h(0)$ is a differential homomorphism [4, Theorem 4.2.1]. Applying it to our equation we get $L_0 p_0 = \sum_{j=1}^{m} c_j f_j(0)$ where $L_0 = L_{\nu(L)}$ is given by the decomposition (1). It is a nonzero linear ordinary differential operator with coefficients in K, so using the induction hypothesis we compute $h_1, \ldots, h_r \in K$ and a matrix M with coefficients in $C(K)$ such that for any solution $p_0 \in K$ we must have $p_0 = \sum_{i=1}^{r} e_i h_i$ and $M(e_1, \ldots, e_r, c_1, \ldots, c_m)^T = 0$. Replacing p by $\sum_{i=1}^{r} e_i h_i + tq$ in the equation, we get

$$\sum_{j=1}^{m} c_j f_j = Lp = Lp_0 + L(tq) = \sum_{j=1}^{m} c_j f_j(0) + (L - L_0)\left(\sum_{i=1}^{r} e_i h_i\right) + t\tilde{L}q$$

where $\tilde{L}$ is given by Lemma 1. Therefore,

$$\tilde{L}q = \sum_{j=1}^{m} c_j \frac{f_j - f_j(0)}{t} - \sum_{i=1}^{r} e_i \frac{1}{t}(L - L_0) h_i \,.$$

The above is a parameterized equation with right–hand side in $K[t]$ and we solve it with the bound $N - 1$ for $\deg(q)$ using the same method. This process eventually terminates since the degree bound is reduced at each step.

Together with the algorithms of [3, 6] for the denominator up to a power of t, the bounding methods of the previous sections, and the known algorithms for solving parameterized linear differential equations over $C(x)$ [1, 2, 3, 6], the above algorithm proves the following result:

Theorem 3 *Let C be any field of characteristic 0, and $E = C(x,t)$ where t is transcendental and exponential over $(C(x), d/dx)$. If we know a vector space basis for C over $\mathbb{Q}$ and if we can factor polynomials in $C[Z]$ and compute their integer roots, then we can effectively solve parameterized linear differential equations over E.*

Note that the requirement of factoring over an algebraic extension of C appears only in one branch of the bounding method for effectively exponential extensions, and only when the nonlinear system considered for γ and ν has stricly positive dimension.

6 Example

We consider $\mathbb{Q}(x, e^{\int x+1/x}) = \mathbb{Q}(x,t)$ where $t'/t = x + 1/x$, so t is effectively exponential over $\mathbb{Q}(x)$, and look for solutions $y \in \mathbb{Q}(x)[t, t^{-1}]$ of $Ly = 0$ where

$$\begin{aligned} L = \quad & (2t^2x^2 + t^2x^4 - x^3 - x)\partial^2 \\ & +(-11x^3t^2 - 6xt^2 - 3x^5t^2 + 3x^2 + x^4)\partial \\ & +9t^2x^4 + 11t^2x^2 + 2t^2x^6 + 6t^2 \,. \end{aligned}$$

- Bounding the degree and order of y:
  - Bounding the degree: $\deg_t(L) = 2$ so $L_2(at^{\deg_t(y)}) = 0$ for some $a \in \mathbb{Q}(x)$ where

    $$L_2 = (2x^2 + x^4)\partial^2 + (-11x^3 - 6x - 3x^5)\partial + 9x^4 + 11x^2 + 2x^6 + 6 \,.$$

    We have $t'/t = x + 1/x$ whose polynomial part has degree 1, so $Q(\deg_t(y)) = 0$ where

    $$Q = Z^2 - 3Z + 2 = (Z-1)(Z-2)$$

    so $\deg_t(y) \le 2$.
  - Bounding the order: $\nu_t(L) = 0$ so $L_0(at^{\nu_t(y)}) = 0$ for some $a \in \mathbb{Q}(x)$ where

    $$L_0 = (-x - x^3)\partial^2 + (x^4 + 3x^2)\partial \,. \tag{10}$$

    As before, the polynomial part of t'/t is x, so

    $$Q = -Z^2 + Z = Z(1-Z)$$

    so $\nu_t(y) \ge 0$.
- Computing the solution: from the bounding step, we conclude that any solution $y \in \mathbb{Q}(x)[t, t^{-1}]$ of $Ly = 0$ must be of the form $y = y_0 + y_1 t + y_2 t^2$.
  - Reducing modulo t, we have $L_0 y_0 = 0$ where L_0 is given by (10). Recursively solving that equation over $\mathbb{Q}(x)$ we find that $y_0 = c_1$ where c_1 is an arbitrary constant. We have

    $$\frac{1}{t}(L - L_0)1 = (9x^4 + 11x^2 + 2x^6 + 6)t \,,$$

    so, replacing y by $c_1 + tz$ where $z = y_1 + y_2 t$ we get the new equation

    $$\tilde{L}z = -c_1(9x^4 + 11x^2 + 2x^6 + 6)t$$

    where

    $$\begin{aligned} \tilde{L} = \quad & (2t^2x^2 + t^2x^4 - x^3 - x)\left(\partial + x + \tfrac{1}{x}\right)^2 \\ & +(-11x^3t^2 - 6xt^2 - 3x^5t^2 + 3x^2 + x^4)\left(\partial + x + \tfrac{1}{x}\right) \\ & +9t^2x^4 + 11t^2x^2 + 2t^2x^6 + 6t^2 \\ = \quad & (2t^2x^2 + t^2x^4 - x^3 - x)\partial^2 \\ & +(-5x^3t^2 - 2xt^2 - x^5t^2 - x^4 - x^2 - 2)\partial \end{aligned}$$

– Reducing modulo t, we have $\tilde{L}_0 y_1 = 0$, where

$$\tilde{L}_0 = \left(-x^3 - x\right)\partial^2 + \left(-2 - x^4 - x^2\right)\partial\,.$$

Recursively solving that equation over $\mathbb{Q}(x)$ we find that $y_1 = c_2$ where c_2 is an arbitrary constant. We have $1/t(\tilde{L} - \tilde{L}_0)1 = 0$, so, replacing z by $c_2 + ty_2$ we get the new equation

$$\left(t^2\overline{L}_2 + \overline{L}_0\right)y_2 = -c_1(9x^4 + 11x^2 + 2x^6 + 6) \tag{11}$$

where

$$\overline{L}_2 = (2x^2 + x^4)\partial^2 + (x^5 + x^3 + 2x)\partial - 2 - x^4 - x^2\,,$$

and

$$\overline{L}_0 = \left(-x^3 - x\right)\partial^2 + \left(-5x^2 - 4 - 3x^4\right)\partial - 2\frac{3x^2 + x^6 + 3x^4 + 1}{x}\,.$$

– Equating the coefficients of t^2 and t^0 on both sides of (11) we get the equations $\overline{L}_2 y_2 = 0$ and

$$\overline{L}_0 y_2 = -c_1(9x^4 + 11x^2 + 2x^6 + 6)\,.$$

Recursively solving those equations over $\mathbb{Q}(x)$ we find that $y_2 = c_3 x$ with the linear constraint $c_3 - c_1 = 0$. Therefore, the general solution of $Ly = 0$ is

$$y = c_1\left(1 + xe^{2\int x + 1/x}\right) + c_2 e^{\int x + 1/x}$$

where c_1 and c_2 are arbitrary constants.

References

[1] Sergei Abramov, Manuel Bronstein, and Marko Petkovšek. On polynomial solutions of linear operator equations. In *Proceedings of ISSAC'95*, pages 290–296. ACM Press, 1995.

[2] Sergei A. Abramov and K. Yu. Kvashenko. Fast algorithms to search for the rational solutions of linear differential equations with polynomial coefficients. In Stephen Watt, editor, *Proceedings of ISSAC'91*, pages 267–270. ACM Press, 1991.

[3] Manuel Bronstein. On solutions of linear ordinary differential equations in their coefficient field. *Journal of Symbolic Computation*, 13(4):413–440, April 1992.

[4] Manuel Bronstein. *Symbolic Integration I – Transcendental Functions.* Springer, Heidelberg, 1997.

[5] Keith Geddes, Stephen Czapor, and George Labahn. *Algorithms for Computer Algebra*. Kluwer Academic Publishers, Boston, 1992.

[6] Michael Singer. Liouvillian solutions of linear differential equations with liouvillian coefficients. *Journal of Symbolic Computation*, 11:251–273, 1991.