Effective algebraic independence of values of E-functions

S. Fischler and T. Rivoal

June 13, 2019

Abstract

E-functions are entire functions with algebraic Taylor coefficients satisfying certain arithmetic conditions, and which are also solutions of linear differential equations with coefficients in $\overline{\mathbb{Q}}(z)$. They were introduced by Siegel in 1929 to generalize the Diophantine properties of the exponential and Bessel's functions. The Siegel-Shidlovskii Theorem (1956) deals with the algebraic (in)dependence of values at algebraic points of E-functions solutions of a differential system. In this paper, we prove the existence of an algorithm to perfom the following three tasks. Given as inputs some E-functions $F_1(z), \dots, F_p(z)$,

(1) it computes a system of generators of the ideal of polynomial relations between $F_1(z), \dots, F_p(z)$ with coefficients in $\overline{\mathbb{Q}}(z)$;

(2) given any $\alpha \in \overline{\mathbb{Q}}$, it computes a system of generators of the ideal of polynomial relations between the values $F_1(\alpha), \dots, F_p(\alpha)$ with coefficients in $\overline{\mathbb{Q}}$;

(3) if $F_1(z), \dots, F_p(z)$ are algebraically independent over $\overline{\mathbb{Q}}(z)$, it determines the finite set of all $\alpha \in \overline{\mathbb{Q}}$ such that the values $F_1(\alpha), \dots, F_p(\alpha)$ are algebraically dependent over $\overline{\mathbb{Q}}$.

The existence of this algorithm relies on a variant of the Hrushovski-Feng algorithm (to compute polynomial relations between solutions of differential systems) and on Beukers' lifting theorem (an optimal refinement of the Siegel-Shidlovskii theorem) in order to reduce the problem to an effective elimination procedure in multivariate polynomial rings. The latter is then performed using Gröbner bases.

1 Introduction

A power series $F(z) = \sum_{n=0}^{\infty} \frac{a_n}{n!} z^n \in \overline{\mathbb{Q}}[[z]]$ is an E-function if

(*i*) $F(z)$ is solution of a non-zero linear differential equation with coefficients in $\overline{\mathbb{Q}}(z)$.

(*ii*) There exists $C > 0$ such that for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and any $n \geq 0$, $|\sigma(a_n)| \leq C^{n+1}$.

(*iii*) There exists $D > 0$ and a sequence of integers d_n, with $1 \leq d_n \leq D^{n+1}$, such that $d_n a_m \in \mathcal{O}_{\overline{\mathbb{Q}}}$ for all $m \leq n$.

Above and below, we fix an embedding of $\overline{\mathbb{Q}}$ into $\mathbb{C}$. Siegel introduced in 1929 the notion of E-function as a generalization of the exponential and Bessel functions. His definition was in fact slightly more general than above (see the end of this introduction). Note that (i) implies that the a_n's all lie in a certain number field $\mathbb{K}$, so that in (ii) there are only finitely many Galois conjugates $\sigma(a_n)$ of a_n to consider, with $\sigma \in \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ (assuming for simplicity that $\mathbb{K}$ is a Galois extension of $\mathbb{Q}$). An E-function is transcendental over $\mathbb{C}(z)$ if and only if $a_n \neq 0$ for infinitely many n. For more informations about E-functions, we refer the reader to the survey [18].

Siegel proved in [20] a result on the Diophantine nature of the values taken by Bessel functions at algebraic points. He generalized it to E-functions in 1949 in [21] under a technical hypothesis (*Siegel's normality*), which was eventually removed by Shidlovskii in 1959, see [19].

Theorem 1 (Siegel-Shidlovskii)**.** *Let $Y(z) = {}^t(F_1(z), \dots, F_n(z))$ be a vector of E-functions such that $Y'(z) = A(z)Y(z)$ where $A(z) \in M_n(\overline{\mathbb{Q}}(z))$. Let $T(z) \in \overline{\mathbb{Q}}[z] \setminus \{0\}$ be such that $T(z)A(z) \in M_n(\overline{\mathbb{Q}}[z])$. Then for any $\alpha \in \overline{\mathbb{Q}}$ such that $\alpha T(\alpha) \neq 0$,*

$$\mathrm{degtr}_{\overline{\mathbb{Q}}}\overline{\mathbb{Q}}(F_1(\alpha), \dots, F_n(\alpha)) = \mathrm{degtr}_{\overline{\mathbb{Q}}(z)}\overline{\mathbb{Q}}(z)(F_1(z), \dots, F_n(z)).$$

The next step was the following result [16] which essentially says that a numerical polynomial relation between values of E-functions at an algebraic point cannot be sporadic and must arise from a functional counterpart between these E-functions.

Theorem 2 (Nesterenko-Shidlovskii, 1996)**.** *With the notations of Theorem 1, there exists a finite set S (depending a priori on $Y(z)$) such that for any $\alpha \in \overline{\mathbb{Q}} \setminus S$, the following holds. For any homogeneous polynomial $P \in \overline{\mathbb{Q}}[X_1, \dots, X_n]$ such that $P(F_1(\alpha), \dots, F_n(\alpha)) = 0$, there exists a polynomial $Q \in \overline{\mathbb{Q}}[Z, X_1, \dots, X_n]$, homogeneous in the variables $X_1, \dots, X_n$, such that $Q(\alpha, X_1, \dots, X_n) = P(X_1, \dots, X_n)$ and $Q(z, F_1(z), \dots, F_n(z)) = 0$.*

The indetermination of the set S is a problem. It was lifted by Beukers [10] using André's theory of E-operators [2].

Theorem 3 (Beukers, 2006)**.** *With the notations of Theorems 1 and 2, one may choose $S = \{\alpha \in \overline{\mathbb{Q}} : \alpha T(\alpha) = 0\}$.*

A natural question is whether it is possible to determine algorithmically the (in)existence of a polynomial relation between values of given E-functions at algebraic points, and between these E-functions themselves. A difficult point is that we may be interested in E-functions $F_1, \dots, F_p$ for which the vector $Y(z) = {}^t(F_1(z), \dots, F_p(z))$ *is not* a solution of any differential system of the form $Y'(z) = A(z)Y(z)$. Our main result answers this question.

Theorem 4. *There exists an algorithm to perform the following three tasks. Given as inputs an integer $p \geq 1$ and some E-functions $F_1(z)$, …, $F_p(z)$,*

- *(i) it computes a system of generators of the ideal of polynomial relations between $F_1(z)$, …, $F_p(z)$ with coefficients in $\overline{\mathbb{Q}}(z)$;*

(*ii*) *given any* $\alpha \in \overline{\mathbb{Q}}$*, it computes a system of generators of the ideal of polynomial relations between the values* $F_1(\alpha)$, ..., $F_p(\alpha)$ *with coefficients in* $\overline{\mathbb{Q}}$*;*

(*iii*) *if* $F_1(z)$, ..., $F_p(z)$ *are algebraically independent over* $\overline{\mathbb{Q}}(z)$*, it determines the finite set of all* $\alpha \in \overline{\mathbb{Q}}$ *such that the values* $F_1(\alpha)$, ..., $F_p(\alpha)$ *are algebraically dependent over* $\overline{\mathbb{Q}}$*.*

See [1, §2.1] for an explanation of how an E-function is *given* by a differential equation with coefficients in $\overline{\mathbb{Q}}(z)$ and sufficiently many Taylor coefficients to compute any of them from the differential equation. A complex algebraic number β is *determined* or *computed* if we know an explicit non-zero polynomial $P \in \mathbb{Q}[X]$ such that $P(\beta) = 0$, together with a numerical approximation of β sufficiently accurate to distinguish β from the other roots of P.

In Theorem 4, let us assume that the output of the algorithm in (*i*) is that $F_1(z)$, ..., $F_p(z)$ are algebraically independent over $\overline{\mathbb{Q}}(z)$. Though it is not an assumption of Theorem 4 that ${}^t(F_1(z), \dots, F_p(z))$ be a solution of a differential system $Y'(z) = A(z)Y(z)$ with $A(z) \in M_p(\overline{\mathbb{Q}}(z))$, let us further assume that this is the case. Then, by Theorem 3, the finite set of algebraic numbers in (*iii*) is a subset of $\{\alpha \in \overline{\mathbb{Q}} : \alpha T(\alpha) = 0\}$; it contains 0 since $F_1(0)$, ..., $F_p(0)$ are algebraic numbers. In other words, the algorithm determines in (*iii*) which roots ξ of T provide a polynomial relation between $F_1(\xi)$, ..., $F_p(\xi)$ with coefficients in $\overline{\mathbb{Q}}$, and then for each ξ, (*ii*) describes all such relations. The problem in the general setting of Theorem 4 is that no finite set S containing the values α of (*iii*) is known in advance. The most difficult part of the proof of Theorem 4 is to construct such a finite set. Moreover, the putative algebraic independence of the functions F_j's can be proven by various *ad hoc* means, and not necessarily by the complicated algorithm in (*i*). The latter is a variation of the Hrushovski-Feng algorithm which, to the best of our knowledge, has not yet been implemented in any computer algebra system.

The case $p = 1$ of Theorem 4 has been proved in [1]:

Theorem 5 (Adamczewski-R., 2018)**.** *There exists an algorithm to perform the following tasks. Given* $F(z)$ *an* E*-function as input, it first says whether* $F(z)$ *is transcendental over* $\overline{\mathbb{Q}}(z)$ *or not. If it is transcendental, it then outputs the finite list of algebraic numbers* α *such that* $F(\alpha)$ *is algebraic, together with the corresponding list of values* $F(\alpha)$*.*

The proof of Theorem 4 shares certain characteristics with that of Theorem 5, in particular Beukers' lifting results in [10] will form our starting point concerning E-functions, and we shall also need to compute the minimal non-zero differential equation satisfied by an E-function. But our proof is not an adaptation, as we need new ideas. Indeed, we shall make an important use of methods coming from commutative algebra (in particular Gröbner bases), which *a contrario* were not used in [1]. In particular, in the case $p = 1$ Theorem 4 provides an algorithm different from the one of Theorem 5.

The paper is organized as follows. In §2, we recall certain standard facts in elimination theory we shall need in the proof of Theorem 4 in the subsequent sections. In §3, we

explain part (i), which is not really new and the proof of which is given for the reader's convenience. In §4, we show that we can assume in (ii) and (iii) that $F_1(z), \dots, F_p(z)$ are linearly independent over $\overline{\mathbb{Q}}(z)$. In §5, we then reduce parts (ii) and (iii) to a problem of commutative algebra using Beukers' lifting results. We solve this problem (which may be of independent interest) in §6 by modifying Buchberger's algorithm. At last, §7 is devoted to examples.

We conclude with the following remark. In his original paper, Siegel gave a slightly more general definition of E-functions: the upper bounds $|\sigma(a_n)| \leq C^{n+1}$ and $1 \leq d_n \leq D^{n+1}$ in (ii) and (iii) were replaced with $|\sigma(a_n)| \leq n!^{\varepsilon}$ and $1 \leq d_n \leq n!^{\varepsilon}$ for any $\varepsilon > 0$, provided n is large enough with respect to ε. Theorems 1 and 2 hold in this more general setting. Beukers' proof of Theorem 3 does not, but André has proved [3] a general result, valid for E-functions in Siegel's sense, which contains Theorem 3. In the present paper we shall use also an effective result due to Beukers [10, Theorem 1.5] to get rid of non-zero singularities, which has been recently generalized to E-functions in Siegel's sense by Lepetit [15]. Therefore all results we prove in this paper are valid in this setting, and the same remark applies to Theorem 5 proved in [1].

2 Gröbner bases and elimination: standard facts

In this section, we recall standard facts about Gröbner bases and elimination. We refer to any textbook on this topic (for instance [5, 8, 11]) for details and proofs.

Let $\mathbb{L}$ be a field, and I be an ideal of the polynomial ring $\mathbb{L}[T_1, \dots, T_N]$. Let $i \in \{1, \dots, N\}$ be an integer, fixed throughout this section: in Proposition 1 below we shall compute a system of generators of the intersection $I \cap \mathbb{L}[T_1, \dots, T_i]$.

A *monomial* is an element of $\mathbb{L}[T_1, \dots, T_N]$ of the form $\underline{T}^{\underline{a}} = T_1^{a_1} \dots T_N^{a_N}$ with $\underline{a} = (a_1, \dots, a_N) \in \mathbb{N}^N$. Given $\underline{a}, \underline{b} \in \mathbb{N}^N$ we say that $\underline{T}^{\underline{a}}$ is less than $\underline{T}^{\underline{b}}$, and we write $\underline{T}^{\underline{a}} < \underline{T}^{\underline{b}}$, if either $\sum_{j=1}^{i} a_j < \sum_{j=1}^{i} b_j$ or: ($\sum_{j=1}^{i} a_j = \sum_{j=1}^{i} b_j$ and $\underline{a}$ is less than $\underline{b}$ in the lexicographical order on $\mathbb{N}^N$). This specific order, called the *i-th elimination order*, is useful to us because our purpose is to study $I \cap \mathbb{L}[T_1, \dots, T_i]$ (see Proposition 1 below). A monomial $\underline{T}^{\underline{a}}$ is said to be *divisible* by $\underline{T}^{\underline{b}}$ if $c_j = a_j - b_j$ is non-negative for any $j \in \{1, \dots, N\}$; then we write $\frac{\underline{T}^{\underline{a}}}{\underline{T}^{\underline{b}}} = \underline{T}^{\underline{c}}$.

Any non-zero polynomial $P \in \mathbb{L}[T_1, \dots, T_N]$ can be written in a unique way as a linear combination $\lambda_1 \underline{T}^{\underline{a}_1} + \dots + \lambda_r \underline{T}^{\underline{a}_r}$ with non-zero coefficients $\lambda_1, \dots, \lambda_r \in \mathbb{L}$ of decreasing monomials $\underline{T}^{\underline{a}_1} > \dots > \underline{T}^{\underline{a}_r}$. Then $\underline{T}^{\underline{a}_1}$ is called the *leading monomial* of P, and we write $\underline{T}^{\underline{a}_1} = \mathrm{lmon}(P)$. In the same way, $\underline{a}_1 = \mathrm{lexp}(P)$ is the *leading exponent*, $\lambda_1 = \mathrm{lcoeff}(P)$ is the *leading coefficient*, and $\lambda_1 \underline{T}^{\underline{a}_1} = \mathrm{lterm}(P)$ is the *leading term* of P.

A Gröbner basis (or standard basis) of I, with respect to the order $<$ we have chosen, is a family $(P_1, \dots, P_r)$ of non-zero elements of I with the following property: for any $P \in I \setminus \{0\}$ there exists $k \in \{1, \dots, r\}$ such that $\mathrm{lmon}(P)$ is divisible by $\mathrm{lmon}(P_k)$. An important property is that any Gröbner basis generates the ideal I. However no minimality

property is assumed: adding arbitrary elements of $I\setminus\{0\}$ to a Gröbner basis always provides a Gröbner basis. Starting with a system of generators of I, a usual way to construct a Gröbner basis is Buchberger's algorithm (i.e., lines 1 and 2 of Algorithm 1 presented below). To state it we need some more notation.

Given any family $P, P_1, \ldots, P_r \in \mathbb{L}[T_1, \ldots, T_N]$ of non-zero polynomials, we consider the following operation. Choose (if possible) an index $k \in \{1, \ldots, r\}$ such that $\mathrm{lmon}(P)$ is divisible by $\mathrm{lmon}(P_k)$, and replace P with $P - \frac{\mathrm{lterm}(P)}{\mathrm{lterm}(P_k)} P_k$. After repeating this operation as many times as possible, P is replaced with a polynomial $\widetilde{P}$ such that there is no index k for which $\mathrm{lmon}(P)$ is divisible by $\mathrm{lmon}(P_k)$; possibly $\widetilde{P} = 0$. This polynomial $\widetilde{P}$ is called a *remainder* in the weak division of P by $P_1, \ldots, P_r$. Note that different choices of k at some steps may lead to different remainders.

Given non-zero polynomials $P, Q \in \mathbb{L}[T_1, \ldots, T_N]$, their *S-polynomial* or *syzygy polynomial* is defined by

$$S(P, Q) = \frac{\mathrm{lterm}(Q)P - \mathrm{lterm}(P)Q}{\gcd(\mathrm{lmon}(P), \mathrm{lmon}(Q))}$$

where $\gcd(\underline{T}^{\underline{a}}, \underline{T}^{\underline{b}}) = \underline{T}^{\underline{c}}$ with $c_j = \min(a_j, b_j)$ for any $j \in \{1, \ldots, N\}$.

We can now state the algorithm we are interested in in this section.

Input: a generating system F of an ideal I of $\mathbb{L}[T_1, \ldots, T_N]$.
Output: a Gröbner basis H of $I \cap \mathbb{L}[T_1, \ldots, T_i]$.
1. $G := F$
2. Repeat:
    a. $G' := G$
    b. For $P, Q \in G'$ with $P \neq Q$ do:
        (i). Compute a remainder R in the weak division of $S(P, Q)$ by G'
        (ii). If $R \neq 0$:
            $G := G \cup \{R\}$
Until $G = G'$
3. $H := G \cap \mathbb{L}[T_1, \ldots, T_i]$

Algorithm 1: Computation of a Gröbner basis of $I \cap \mathbb{L}[T_1, \ldots, T_i]$.

Lines 1 and 2 of Algorithm 1 are known as Buchberger's algorithm: the output G is a Gröbner basis of I. Line 3 means that H contains those polynomials in G which depend only on the variables $T_1, \ldots, T_i$. Then H is a Gröbner basis of $I \cap \mathbb{L}[T_1, \ldots, T_i]$ by the following result (see [8, Exercise 24.4]), which concludes the proof that Algorithm 1 works as announced.

Proposition 1. *Let $P_1, \ldots, P_r$ be a Gröbner basis of I with respect to the i-th elimination order. Then those P_j which depend only on the variables $T_1, \ldots, T_i$ make up a Gröbner basis of $I \cap \mathbb{L}[T_1, \ldots, T_i]$.*

We conclude this section with basic facts about polynomials in $T_1, \ldots, T_N$ that depend on an auxiliary parameter z; this will be the setting of the proof of part (i) of Proposition 3 in §6 below.

Let $\mathbb{K}$ be a subfield of $\mathbb{C}$, and $\mathbb{L} = \mathbb{K}(z)$. We fix $W(z) \in \mathbb{K}[z] \setminus \{0\}$ and consider polynomials $P \in \mathbb{K}[z, \frac{1}{W(z)}, T_1, \ldots, T_N] \subset \mathbb{L}[T_1, \ldots, T_N]$. We also fix $\alpha \in \mathbb{K}$ such that $W(\alpha) \neq 0$. Then any such P can be evaluated at $z = \alpha$; we denote by $P_\alpha \in \mathbb{K}[T_1, \ldots, T_N]$ the polynomial obtained in this way.

An easy (but already instructive) example is the following: $P = (z-1)T_1 + T_2$. Assume that $i \geq 2$ and consider as above the i-th elimination order, so that $T_1 > T_2$. Then in $\mathbb{L}[T_1, \ldots, T_N]$ we have $\mathrm{lmon}(P) = T_1$. However the leading monomial of P_α depends on α: it is T_1 if $\alpha \neq 1$, but T_2 if $\alpha = 1$. In general, $\mathrm{lmon}(P_\alpha)$ can be easily determined for almost all values of α:

$$\mathrm{lmon}(P_\alpha) = \mathrm{lmon}(P) \quad \text{if } (\mathrm{lcoeff}(P))(\alpha) \neq 0.$$

In particular, $(\mathrm{lcoeff}(P))(\alpha) \neq 0$ implies $P_\alpha \neq 0$.

In the same way we have

$$S(P,Q)_\alpha = S(P_\alpha, Q_\alpha) \quad \text{if } (\mathrm{lcoeff}(P))(\alpha) \neq 0 \text{ and } (\mathrm{lcoeff}(Q))(\alpha) \neq 0.$$

3 Algebraic relations between $F_1(z), \ldots, F_p(z)$

In this section, we briefly explain the proof of part (i) in Theorem 4. It is a modification of one of the steps in Feng's algorithm [12] to compute differential Galois groups, which is itself based on Hrushovski's algorithm [13].

For any $1 \leq i \leq p$, we are given a differential equation of order n_i satisfied by F_i. Then the vector Y with $n = n_1 + \ldots + n_p$ coordinates $F_i^{(j)}$, where $1 \leq i \leq p$ and $0 \leq j \leq n_i - 1$, is a solution of a differential system $Y' = AY$ with $A \in M_n(\overline{\mathbb{Q}}(z))$. Let $Y_1 = Y$, Y_2, $\ldots$, Y_n be a basis of solutions of this differential system; in other words, the matrix with columns $Y_1, \ldots, Y_n$ is a fundamental matrix of solutions. As pointed out to us by Feng, Algorithm 4.1 of [12] in which Step (h) is replaced with [12, Proposition 3.6] provides an algorithm to compute a system of generators of the ideal of algebraic relations over $\overline{\mathbb{Q}}(z)$ among the coordinates of $Y_1, \ldots, Y_n$ (i.e., among the coefficients of this fundamental matrix of solutions). Using Gröbner bases (see Algorithm 1 in §2), we then deduce a system of generators of the ideal of algebraic relations over $\overline{\mathbb{Q}}(z)$ among $F_1, \ldots, F_p$, since they are amongst the coordinates of Y_1.

This concludes the proof of part (i) of Theorem 4.

4 Linear dependence relations between E-functions

In this section, we prove that in parts (ii) and (iii) of Theorem 4, we may assume that $F_1(z), \ldots, F_p(z)$ are $\overline{\mathbb{Q}}(z)$-linearly independent. Let us start with a lemma, of independent interest, in the statement of which it is not necessary to assume that the functions y_j are E-functions.

Lemma 1. *Let $Y = {}^t(y_1, \dots, y_n)$ be a solution of a differential system $Y' = AY$ with $A \in M_n(\overline{\mathbb{Q}}(z))$. Let*

$$\mathcal{R}_Y = \{(P_1, \dots, P_n) \in \overline{\mathbb{Q}}(z)^n,\ P_1(z)y_1(z) + \dots + P_n(z)y_n(z) = 0\}$$

be the $\overline{\mathbb{Q}}(z)$-vector space of $\overline{\mathbb{Q}}(z)$-linear relations between $y_1(z)$, …, $y_n(z)$. Then there is an algorithm to compute a basis of this vector space; accordingly it enables one to know whether y_1, …, y_n are linearly independent over $\overline{\mathbb{Q}}(z)$ or not.

Proof. The cyclic vector theorem provides an invertible matrix $P \in \mathrm{GL}_n(\overline{\mathbb{Q}}(z))$ (which depends only on A) such that $V = PY$ satisfies $V' = CV$, where $C \in M_n(\overline{\mathbb{Q}}(z))$ is a companion matrix. In other words, letting $V = {}^t(v_1(z), \dots, v_n(z))$ we have $v_i = v_1^{(i-1)}$ for any $1 \le i \le n$, and $Lv_1 = 0$ for some differential operator $L \in \overline{\mathbb{Q}}(z)[\frac{d}{dz}]$ of order n. Moreover P and L can be computed effectively (see for instance [17, Chapter 2, §2.1]).

Let $L_0 \neq 0$ denote a differential operator in $\overline{\mathbb{Q}}(z)[\frac{d}{dz}]$ such that $L_0 v_1 = 0$, of minimal order k. Then [9, Theorems 1-2] provides an explicit integer D for which such an L_0 exists of the form $\sum_{i=0}^{k} Q_i(z)(\frac{d}{dz})^i$ with $Q_i \in \overline{\mathbb{Q}}[z]$ of degree at most D. Using the multiplicity estimate of [6, Théorème 1] completed by [7, Lemma 3.1], an algorithm to compute explicitly such an L_0 is given in [1, §3], and we refer to the discussion surrounding [9, Theorem 3] for further details about it.

Then v_1, v_1', …, $v_1^{(k-1)}$ are linearly independent over $\overline{\mathbb{Q}}(z)$, and we have

$$v_1^{(k)}(z) = -\sum_{i=0}^{k-1} \frac{Q_i(z)}{Q_k(z)} v_1^{(i)}(z).$$

Taking successive derivatives of this relation we can express each $v_j = v_1^{(j-1)}$, with $k+1 \le j \le n$, as a $\overline{\mathbb{Q}}(z)$-linear combination of v_1, v_1', …, $v_1^{(k-1)}$. Since $Y = P^{-1}V$ we deduce an explicit expression of y_1, …, y_n as $\overline{\mathbb{Q}}(z)$-linear combinations of the $\overline{\mathbb{Q}}(z)$-linearly independent functions v_1, v_1', …, $v_1^{(k-1)}$. Therefore Lemma 1 boils down to the problem of finding linear relations between the columns of a matrix: it can be easily solved using Gaussian elimination. □

We now apply Lemma 1 to prove that in parts (*ii*) and (*iii*) of Theorem 4 we may assume that $F_1(z)$, …, $F_p(z)$ are $\overline{\mathbb{Q}}(z)$-linearly independent.

Let $F_1(z)$, …, $F_p(z)$ be E-functions. Using Lemma 1 we may compute a maximal subset $F_{i_1}(z)$, …, $F_{i_t}(z)$ of $\overline{\mathbb{Q}}(z)$-linearly independent functions among $F_1(z)$, …, $F_p(z)$, and an expression

$$F_i(z) = \sum_{j=1}^{t} Q_{i,j}(z) F_{i_j}(z) \text{ for each } i \in \{1, \dots, p\} \setminus \{i_1, \dots, i_t\} \tag{4.1}$$

with $Q_{i,j}(z) \in \overline{\mathbb{Q}}(z)$.

If $t < p$ then part (iii) of Theorem 4 is empty; to prove part (ii) in this case, it is enough to compute a system of generators of the ideal of polynomial relations between F_{i_1}, ..., F_{i_t} over $\overline{\mathbb{Q}}(z)$. Indeed adding the relations (4.1) to this system provides a system of generators of the ideal of polynomial relations between $F_1(z)$, ..., $F_p(z)$.

Therefore, to complete the proof of Theorem 4 what remains to do (taking §3 into account) is to prove parts (ii) and (iii) under the additional assumption that $F_1(z)$, ..., $F_p(z)$ are linearly independent over $\overline{\mathbb{Q}}(z)$.

5 Reduction of parts (ii) and (iii) of Theorem 4 to statements in commutative algebra

The following proposition shows how to reduce parts (ii) and (iii) of Theorem 4 (in the case where $F_1(z)$, ..., $F_p(z)$ are linearly independent over $\overline{\mathbb{Q}}(z)$) to a problem in commutative algebra, that we shall solve in §6. To begin with, we point out that $F_1(0)$, ..., $F_p(0)$ are algebraic numbers so that $\alpha = 0$ always belongs to the set of part (iii), and part (ii) is trivial for $\alpha = 0$. Therefore throughout this section, α denotes a non-zero algebraic number.

We denote by $\underline{X}$ the set of variables X_1, ..., X_N. In the following result, by "compute an ideal I" we mean "compute a system of generators of I".

Proposition 2. *Let $F_1(z)$, ..., $F_p(z)$ be E-functions linearly independent over $\overline{\mathbb{Q}}(z)$. There exists an algorithm to compute an integer $N \geq 1$, an ideal I of $\overline{\mathbb{Q}}[z, X_1, \ldots, X_N]$ and $\overline{\mathbb{Q}}[z]$-linearly independent polynomials $\varphi_1, \ldots, \varphi_p \in \overline{\mathbb{Q}}[z][\underline{X}]$ homogeneous of degree 1 with respect to $X_1, \ldots, X_N$ with the following properties:*

(*a*) *For any $R \in \overline{\mathbb{Q}}[z, Y_1, \ldots, Y_p]$ we have:*

$$R(z, F_1(z), \ldots, F_p(z)) = 0 \quad \text{if, and only if,} \quad R(z, \varphi_1(z, \underline{X}), \ldots, \varphi_p(z, \underline{X})) \in I.$$

(*b*) *For any $S \in \overline{\mathbb{Q}}[Y_1, \ldots, Y_p]$ and any $\alpha \in \overline{\mathbb{Q}}^*$ we have $S(F_1(\alpha), \ldots, F_p(\alpha)) = 0$ if, and only if, there exists $Q \in I$ such that*

$$S(\varphi_1(\alpha, \underline{X}), \ldots, \varphi_p(\alpha, \underline{X})) = Q(\alpha, X_1, \ldots, X_N).$$

In particular, F_1, ..., F_p are algebraically independent over $\overline{\mathbb{Q}}(z)$ if, and only if,

$$I \cap \overline{\mathbb{Q}}[z, \varphi_1(z, \underline{X}), \ldots, \varphi_p(z, \underline{X})] = \{0\}.$$

In this section we prove Proposition 2 by applying two results of Beukers [10] on E-functions.

Proof. Let $F_1, \ldots, F_p$ be E-functions linearly independent over $\overline{\mathbb{Q}}(z)$. Recall that each F_i is given with a differential equation of order n_i it satisfies. Let $\mathcal{F}$ denote the $\overline{\mathbb{Q}}(z)$-vector space generated by the E-functions $F_i^{(j)}$, $1 \leq i \leq p$, $0 \leq j \leq n_i - 1$. Lemma 1 enables us to compute the dimension of $\mathcal{F}$, denoted by N. Since $F_1, \ldots, F_p$ are linearly independent over $\overline{\mathbb{Q}}(z)$ we have $N \geq p$. Moreover Lemma 1 shows also how to pick up E-functions F_{p+1}, $\ldots$, F_N among the $F_i^{(j)}$ (with $j \geq 1$) such that $(F_1, \ldots, F_p, F_{p+1}, \ldots, F_N)$ is a basis of $\mathcal{F}$ over $\overline{\mathbb{Q}}(z)$.

Since $\mathcal{F}$ is stable under derivation, each F_i' (with $1 \leq i \leq N$) is a linear combination of $F_1, \ldots, F_N$ with coefficients in $\overline{\mathbb{Q}}(z)$: the vector $Y = {}^t(F_1, \ldots, F_N)$ is a solution of a differential system $Y' = AY$ with $A \in M_N(\overline{\mathbb{Q}}(z))$. Moreover the derivatives of $F_1, \ldots, F_N$ are explicit linear combinations of the $F_i^{(j)}$, and therefore of $F_1, \ldots, F_N$ using Lemma 1: the matrix A is effectively computable.

Our strategy is to apply Beukers' Theorem 3. However α might be a singularity of the differential system $Y' = AY$ (i.e., $T(\alpha) = 0$ in the notation of Theorem 3): to do this we have to get rid of all non-zero singularities first. With this aim in view, we apply [10, Theorem 1.5] to the differential system $Y' = AY$ satisfied by the vector $Y = {}^t(F_1, \ldots, F_N)$ of which the coordinates are $\overline{\mathbb{Q}}(z)$-linearly independent E-functions. It provides E-functions $g_1, \ldots, g_N$ and a matrix $M = (m_{j,k}(z))_{j,k} \in M_N(\overline{\mathbb{Q}}[z])$ such that:

(*i*) For any $j \in \{1, \ldots, N\}$ we have $F_j(z) = \sum_{k=1}^N m_{j,k}(z) g_k(z)$.

(*ii*) The vector $Z = {}^t(g_1, \ldots, g_N)$ is a solution of a differential system $Z' = BZ$ with $B \in M_N(\overline{\mathbb{Q}}[z, 1/z])$.

The point here is that 0 is the only possible finite singularity of the differential system $Z' = BZ$. Moreover, the E-functions $g_1, \ldots, g_N$, the polynomials $m_{j,k}(z)$ and the matrix B are effectively computable (see [1, §5]).

Recall from (*i*) that $F_j(z) = \sum_{k=1}^N m_{j,k}(z) g_k(z)$ for any $j \in \{1, \ldots, N\}$; this relation is specially interesting for $j \leq p$, since $F_1, \ldots, F_p$ are the E-functions involved in the statement of Proposition 2. We let

$$\varphi_j(z, X_1, \ldots, X_N) = \sum_{k=1}^N m_{j,k}(z) X_k \in \overline{\mathbb{Q}}[z, X_1, \ldots, X_N] \text{ for } 1 \leq j \leq p,$$

so that

$$F_j(z) = \varphi_j(z, g_1(z), \ldots, g_N(z)) \text{ for } 1 \leq j \leq p. \tag{5.1}$$

Then $\varphi_1, \ldots, \varphi_p$ are linearly independent over $\overline{\mathbb{Q}}[z]$ because $F_1, \ldots, F_p$ are.

As mentioned in §3 above, Feng's algorithm provides a system of generators of the ideal I of polynomial relations between $g_1, \ldots, g_N$:

$$I = \{Q \in \overline{\mathbb{Q}}[z, X_1, \ldots, X_N] \quad \text{such that} \quad Q(z, g_1(z), \ldots, g_N(z)) = 0\}.$$

Now for any $R \in \overline{\mathbb{Q}}[z, Y_1, \ldots, Y_p]$, Eq. (5.1) yields:

$$R(z, F_1(z), \ldots, F_p(z)) = R(z, \varphi_1(z, \underline{g}(z)), \ldots, \varphi_p(z, \underline{g}(z)));$$

here and below we write $\underline{g}(z)$ for the tuple $g_1(z), \ldots, g_N(z)$. Therefore $R(z, F_1(z), \ldots, F_p(z))$ is identically zero if and only if $R(z, \varphi_1(z, \underline{X}), \ldots, \varphi_p(z, \underline{X})) \in I$, thereby proving part (a) of Proposition 2.

To prove part (b), let $\alpha \in \overline{\mathbb{Q}}^*$ and $S \in \overline{\mathbb{Q}}[Y_1, \ldots, Y_p]$. To begin with, assume that

$$S(\varphi_1(\alpha, \underline{X}), \ldots, \varphi_p(\alpha, \underline{X})) = Q(\alpha, X_1, \ldots, X_N)$$

for some $Q \in I$. Then we have:

$$\begin{aligned} S(F_1(\alpha), \ldots, F_p(\alpha)) &= S(\varphi_1(\alpha, \underline{g}(\alpha)), \ldots, \varphi_p(\alpha, \underline{g}(\alpha))) \quad \text{using Eq. (5.1)} \\ &= Q(\alpha, g_1(\alpha), \ldots, g_N(\alpha)) \\ &= 0 \quad \text{since } Q \in I. \end{aligned}$$

Conversely, assume that $S(F_1(\alpha), \ldots, F_p(\alpha)) = 0$. Using Eq. (5.1) we have

$$S(\varphi_1(\alpha, \underline{g}(\alpha)), \ldots, \varphi_p(\alpha, \underline{g}(\alpha))) = 0.$$

Consider the polynomial $P \in \overline{\mathbb{Q}}[X_1, \ldots, X_N]$ defined by

$$P(\underline{X}) = S(\varphi_1(\alpha, \underline{X}), \ldots, \varphi_p(\alpha, \underline{X}))$$

so that we have

$$P(g_1(\alpha), \ldots, g_N(\alpha)) = 0.$$

Now $\alpha \neq 0$ is not a singularity of the differential system $Z' = BZ$ satisfied by $Z = {}^t(g_1, \ldots, g_N)$. Therefore Beukers' version of the Siegel-Shidlovskii theorem (namely [10, Theorem 1.3] or Theorem 3 above) provides $Q \in \overline{\mathbb{Q}}[z, X_1, \ldots, X_N]$ such that

$$Q(z, g_1(z), \ldots, g_N(z)) = 0 \text{ and } Q(\alpha, \underline{X}) = P(\underline{X}) = S(\varphi_1(\alpha, \underline{X}), \ldots, \varphi_p(\alpha, \underline{X})).$$

By definition of I we have $Q \in I$. This concludes the proof of Proposition 2. □

6 Completion of the proof of Theorem 4: an algorithm in commutative algebra

In this section, we complete the proof of Theorem 4.

Let $\mathbb{K}$ be a subfield of $\mathbb{C}$ on which arithmetic operations are implemented; it need not necessarily be $\overline{\mathbb{Q}}$ or a number field at this stage. We denote by $\underline{X}$ the set of variables X_1, $\ldots$, X_N.

Let $\varphi_1, \ldots, \varphi_p \in \mathbb{K}[z, \underline{X}]$ be homogeneous of degree 1 with respect to $X_1, \ldots, X_N$ (i.e., linear forms in $X_1, \ldots, X_N$ with coefficients in $\mathbb{K}[z]$); assume that $\varphi_1, \ldots, \varphi_p$ are linearly independent over $\mathbb{K}[z]$.

Let I be an ideal of $\mathbb{K}[z, \underline{X}]$, generated by $Q_1, \ldots, Q_\ell$. For any $\alpha \in \mathbb{K}$, denote by J_α the set of all polynomials $S \in \mathbb{K}[Y_1, \ldots, Y_p]$ for which there exists $Q \in I$ with

$$S(\varphi_1(\alpha, \underline{X}), \ldots, \varphi_p(\alpha, \underline{X})) = Q(\alpha, \underline{X}).$$

If $\mathbb{K} = \overline{\mathbb{Q}}$ and N, I, $\varphi_1, \ldots, \varphi_p$ are provided by Proposition 2, then for any $\alpha \in \overline{\mathbb{Q}}$

$$J_\alpha = \{S \in \overline{\mathbb{Q}}[Y_1, \ldots, Y_p],\ S(F_1(\alpha), \ldots, F_p(\alpha)) = 0\}$$

is the ideal considered in Theorem 4. Therefore combining Proposition 2 and Proposition 3 below concludes the proof of Theorem 4 (recall that the case $\alpha = 0$ is trivial since $F_1(0), \ldots, F_p(0)$ are algebraic numbers).

In the following statement, both algorithms take $\varphi_1, \ldots, \varphi_p$, $Q_1, \ldots, Q_\ell$ as inputs, and also α for (ii).

Proposition 3. *In this setting:*

- (i) *If $I \cap \mathbb{K}[z, \varphi_1(z, \underline{X}), \ldots, \varphi_p(z, \underline{X})] = \{0\}$, then there exists an algorithm to compute a non-zero polynomial $W \in \mathbb{K}[z]$ with the following property: for any $\alpha \in \mathbb{K}$ such that $J_\alpha \neq \{0\}$, we have $W(\alpha) = 0$.*
- (ii) *There exists an algorithm that, given $\alpha \in \mathbb{K}$, computes a system of generators of the ideal J_α. In particular it enables one to know whether J_α is equal to $\{0\}$ or not.*

Nota Bene: In assertion (ii), we do not need to assume that

$$I \cap \mathbb{K}[z, \varphi_1(z, \underline{X}), \ldots, \varphi_p(z, \underline{X})] = \{0\};$$

this assumption is needed in (i) to ensure that W is non-zero. Moreover, after computing W in (i), it is possible to apply (ii) to all roots of W: this allows one to determine exactly the (finite) set of all $\alpha \in \mathbb{K}$ such that $J_\alpha \neq \{0\}$.

The polynomial W plays the role of the polynomial u_0 in [1].

In the rest of this section we shall prove Proposition 3.

We denote by I_α the ideal of $\mathbb{K}[\underline{X}]$ consisting in all polynomials $Q(\alpha, \underline{X})$ with $Q \in I$, and by χ_α the linear map $\mathbb{K}[Y_1, \ldots, Y_p] \to \mathbb{K}[X_1, \ldots, X_N]$ defined by

$$\chi_\alpha(S(Y_1, \ldots, Y_p)) = S(\varphi_1(\alpha, \underline{X}), \ldots, \varphi_p(\alpha, \underline{X})).$$

Then we have $J_\alpha = \chi_\alpha^{-1}(I_\alpha)$.

Proof of part (ii) of Proposition 3. Fix $\alpha \in \mathbb{K}$. Denote by r the dimension of the $\mathbb{K}$-vector space spanned by the linear forms $\varphi_j(\alpha, \underline{X})$ with $1 \leq j \leq p$; we have $0 \leq r \leq \min(p, N)$. There exist effectively computable indices $1 \leq j_1 < \ldots < j_r \leq p$ and $1 \leq i_1 < \ldots < i_{N-r} \leq N$ such that $\varphi_{j_1}(\alpha, \underline{X})$, ..., $\varphi_{j_r}(\alpha, \underline{X})$, X_{i_1}, ..., $X_{i_{N-r}}$ is a basis of the N-dimensional vector space of $\mathbb{K}$-linear combinations of $X_1, \ldots, X_N$. In general there are several such tuples $(i_1, \ldots, i_{N-r}, j_1, \ldots, j_r)$; we choose (arbitrarily) the least in lexicographical order. We let $T_1 = \varphi_{j_1}(\alpha, \underline{X})$, ..., $T_r = \varphi_{j_r}(\alpha, \underline{X})$, $T_{r+1} = X_{i_1}$, ..., $T_N = X_{i_{N-r}}$. In this way $T_1, \ldots, T_N$ are linearly independent linear forms in $X_1, \ldots, X_N$, and are therefore algebraically independent. We have $\mathbb{K}[\underline{X}] = \mathbb{K}[\underline{T}]$ where $\underline{T}$ stands for $T_1, \ldots, T_N$, and any polynomial in $\mathbb{K}[\underline{X}]$ can be written in a unique way as a polynomial in $T_1, \ldots, T_N$ with coefficients in $\mathbb{K}$. Algorithm 1 described in §2, with $\mathbb{L} = \mathbb{K}$ and $i = r$, enables one (starting with $Q_1(\alpha, \underline{X}), \ldots, Q_\ell(\alpha, \underline{X})$) to compute a Gröbner basis of $I_\alpha \cap \mathbb{K}[T_1, \ldots, T_r] = I_\alpha \cap \mathrm{Im}(\chi_\alpha)$. Each element of this Gröbner basis is of the form $P(T_1, \ldots, T_r)$, and we have

$$\chi_\alpha(P(Y_{j_1}, \ldots, Y_{j_r})) = P(T_1, \ldots, T_r).$$

Let $\mathcal{B}_1$ be the set of all polynomials $P(Y_{j_1}, \ldots, Y_{j_r})$ for $P(T_1, \ldots, T_r)$ in this Gröbner basis; then $\chi_\alpha(\mathcal{B}_1)$ is a set of generators of $I_\alpha \cap \mathrm{Im}(\chi_\alpha)$. On the other hand, for each $j \in \{1, \ldots, p\} \setminus \{j_1, \ldots, j_r\}$ there exist scalars $\lambda_{j,t} \in \mathbb{K}$ (for $1 \leq t \leq r$) such that $\varphi_j(\alpha, \underline{X}) = \sum_{t=1}^r \lambda_{j,t} \varphi_{j_t}(\alpha, \underline{X})$; we let $\mathcal{B}_2$ be the set of all linear polynomials $Y_j - \sum_{t=1}^r \lambda_{j,t} Y_{j_t}$ for $j \in \{1, \ldots, p\} \setminus \{j_1, \ldots, j_r\}$. Then $\mathcal{B}_2$ is a set of generators of the ideal $\ker(\chi_\alpha)$, so that $\mathcal{B}_1 \cup \mathcal{B}_2$ is a set of generators of the ideal $J_\alpha = \chi_\alpha^{-1}(I_\alpha)$. This set is empty if, and only if, $J_\alpha = \{0\}$. This concludes the proof of part (*ii*) of Proposition 3. □

Proof of part (i) of Proposition 3. We first point out that the algorithm described above for part (*ii*) depends on α in many ways, through r, i_1, ..., i_{N-r}, j_1, ..., j_r, and at each step of Algorithm 1 (whenever a remainder or a syzygy polynomial is computed, or the equality of two polynomials is tested). We refer to the end of §2 for examples where $\mathrm{lmon}(P(\alpha, \underline{X}))$ or $S(P(\alpha, \underline{X}), Q(\alpha, \underline{X}))$ depend on $\alpha \in \mathbb{K}$. The general idea when several polynomials $P \in \mathbb{K}(z)[\underline{X}]$ are involved is that if none of their leading coefficients vanishes at α, then everything goes smoothly: the leading monomial of each $P(\alpha, \underline{X})$ is independent from α. Since the algorithm involves finitely many steps, only finitely many polynomials are computed: the strategy is to compute a common multiple $W \in \mathbb{K}[z] \setminus \{0\}$ of the numerators of the leading coefficients of all polynomials $P \in \mathbb{K}(z)[T_1, \ldots, T_N]$ that appear during the algorithm. Then for any $\alpha \in \mathbb{K}$ such that $W(\alpha) \neq 0$, the algorithm described above for part (*ii*) takes place exactly in the same way, independently of α: actually it follows exactly the same steps as if it were worked out over $\mathbb{K}(z)$. We refer to the end of §7 for an example.

To make this strategy more precise, let $M_0(z) = (m_{j,k}(z)) \in M_{p,N}(\mathbb{K}[z])$ denote the matrix defined by $\varphi_j(z, \underline{X}) = \sum_{k=1}^N m_{j,k}(z) X_k$ for any $j \in \{1, \ldots, p\}$. Since φ_1, ..., φ_p are linearly independent over $\mathbb{K}[z]$, the matrix $M_0(z)$ has rank p: there exists a minor $W_0(z)$ of $M_0(z)$, of size p, which is not identically zero. If $\alpha \in \mathbb{K}$ is such that $W_0(\alpha) \neq 0$, then

$M_0(\alpha)$ has rank p and the integer r defined in the proof of part (ii) (in terms of α) is equal to p.

Let $\widetilde{\imath}_1, \ldots, \widetilde{\imath}_{N-p}$ denote the indices of the columns of $M_0(z)$ which do not appear in the submatrix of which $W_0(z)$ is the determinant, with $1 \leq \widetilde{\imath}_1 < \ldots < \widetilde{\imath}_{N-p} \leq N$. Choosing $W_0(z)$ properly among all non-zero minors of $M_0(z)$ of size p, we may assume that $(\widetilde{\imath}_1, \ldots, \widetilde{\imath}_{N-p})$ is least possible with respect to lexicographic order (i.e., all tuples less than $(\widetilde{\imath}_1, \ldots, \widetilde{\imath}_{N-p})$ correspond to zero minors). Then for any $\alpha \in \mathbb{K}$ such that $W_0(\alpha) \neq 0$, we have $i_1 = \widetilde{\imath}_1, \ldots, i_{N-r} = \widetilde{\imath}_{N-p}$ where $i_1, \ldots, i_{N-r}$ have been constructed in terms of α in the proof of part (ii) (recall also the equality $r = p$, already noticed). Moreover, by definition we have $j_1 = 1, \ldots, j_r = p$ for such an α.

As in the proof of part (ii), we let $T_1 = \varphi_1(z, \underline{X}), \ldots, T_p = \varphi_p(z, \underline{X})$, $T_{p+1} = X_{\widetilde{\imath}_1}, \ldots, T_N = X_{\widetilde{\imath}_{N-p}}$. In this way, $T_1, \ldots, T_N$ make up a basis of the $\mathbb{K}(z)$-vector space generated by $X_1, \ldots, X_N$, and are therefore algebraically independent over $\mathbb{K}(z)$; we have $\mathbb{K}(z)[\underline{X}] = \mathbb{K}(z)[\underline{T}]$ where $\underline{T}$ stands for $T_1, \ldots, T_N$. By definition of $W_0(z)$ and $\widetilde{\imath}_1, \ldots, \widetilde{\imath}_{N-p}$, each X_i with $1 \leq i \leq N$ can be written as $\sum_{k=1}^{N} \lambda_{i,k}(z) T_k$ with $W_0(z)\lambda_{i,k}(z) \in \mathbb{K}[z]$. In particular we have $\mathbb{K}[z, \underline{X}] \subset \mathbb{K}[z, \frac{1}{W_0(z)}, \underline{T}]$.

Now we run Algorithm 2 below, in which all multivariate polynomials are seen in $\mathbb{K}(z)[\underline{T}]$; we use the notation of §2 with $\mathbb{L} = \mathbb{K}(z)$ and $i = p$. The input involves the set F of polynomials $Q_k(z, \underline{X})$ with $1 \leq k \leq \ell$ which generate I; they belong to $\mathbb{K}[z, \underline{X}] \subset \mathbb{K}[z, \frac{1}{W_0(z)}, \underline{T}] \subset \mathbb{K}(z)[\underline{T}]$ but not necessarily to $\mathbb{K}[z][\underline{T}]$. The leading coefficient of any non-zero $P \in \mathbb{K}(z)[\underline{T}]$ is a non-zero rational function $R(z) = N(z)/D(z)$ with $N, D \in \mathbb{K}[z] \setminus \{0\}$, $\gcd(N, D) = 1$ and D monic. Its numerator $N(z)$ is denoted by $\operatorname{num}\operatorname{lcoeff}(P)$, and more generally we define $\operatorname{num}(R)$ in this way for any non-zero $R \in \mathbb{K}(z)$.

Except for line 5 and the computation of $W(z)$, Algorithm 2 below follows exactly Buchberger's algorithm (i.e., Algorithm 1 over $\mathbb{L} = \mathbb{K}(z)$ without the last step): at the end, G is a Gröbner basis of the ideal $\widetilde{I}$ of $\mathbb{K}(z)[\underline{T}]$ generated by the input F. In particular it terminates (we shall prove later that line $5a$ can be carried out).

Input: Integers $1 \leq p \leq N$, a non-zero polynomial $W_0 \in \mathbb{K}[z]$ as above, and a finite subset F of $\mathbb{K}[z, \frac{1}{W_0(z)}, \underline{T}] \setminus \{0\}$.
Output: a non-zero polynomial $W(z) \in \mathbb{K}[z]$ as in part (i) of Proposition 3.
1. $G := F$
2. $W := W_0$
3. For $P \in G$ do:
$W := \mathrm{lcm}(W, \mathrm{num\,lcoeff}(P))$
4. Repeat:
a. $G' := G$
b. For $P, Q \in G'$ with $P \neq Q$ do:
(i). $W := \mathrm{lcm}(W, \mathrm{num\,lcoeff}(P - Q))$
(ii). $S := S(P, Q)$
(iii). If $S \neq 0$:
$W := \mathrm{lcm}(W, \mathrm{num\,lcoeff}(S))$
(iv). While $S \neq 0$ and there exists $P_1 \in G'$ such that $\mathrm{lmon}(P_1)$ divides $\mathrm{lmon}(S)$:
κ. $S := S - \frac{\mathrm{lterm}(S)}{\mathrm{lterm}(P_1)} P_1$
η. If $S \neq 0$:
$W := \mathrm{lcm}(W, \mathrm{num\,lcoeff}(S))$
(v). If $S \neq 0$:
$G := G \cup \{S\}$
Until $G = G'$
5. For $P \in G$ do:
a. Find $\underline{a} \in \mathbb{N}^N$ such that $a_i \geq 1$ for at least one integer $i \geq p + 1$ and the coefficient $\lambda_{\underline{a}}(z)$ of $\underline{T}^{\underline{a}}$ in $P(z, \underline{T})$ is non-zero.
b. $W := \mathrm{lcm}(W, \mathrm{num}(\lambda_{\underline{a}}(z)))$

Algorithm 2: Computation of $W(z)$ in part (i).

At the end of Algorithm 2, W is a non-zero polynomial that we denote by W_{end}. We shall now prove that W_{end} satisfies the property (i) of Proposition 3.

Notice that W_{end} is constructed by taking least common multiples repeatedly, so that at each step of the algorithm W divides W_{end}. We claim that throughout the algorithm,

$$P \in \mathbb{K}\left[z, \frac{1}{W_{\mathrm{end}}(z)}, \underline{T}\right] \quad \text{and} \quad \mathrm{num\,lcoeff}(P) \text{ divides } W_{\mathrm{end}} \text{ for any } P \in G. \tag{6.1}$$

This is true at line 1 using line 3 and the assumption $F \subset \mathbb{K}[z, \frac{1}{W_0(z)}, \underline{T}]$ where W_0 divides W_{end} using line 2. Whenever a new element S is added to G on line $4b(v)$, it is constructed in lines $4b(ii)$ and $4b(iv)\kappa$ in such a way that $S \in \mathbb{K}[z, \frac{1}{W_{\mathrm{end}}(z)}, \underline{T}]$ (since on line $4b(iv)\kappa$, P_1 has been inserted in G previously so that $\mathrm{num\,lcoeff}(P_1)$ divides W_{end}), and $\mathrm{num\,lcoeff}(S)$

divides W_{end} using line $4b(iv)\eta$. This proves the claim. From now on, we fix $\alpha \in \mathbb{K}$ such that $W_{\mathrm{end}}(\alpha) \neq 0$. Claim (6.1) shows that at any step of the algorithm,

$$\text{for any } P(z,\underline{T}) \in G,\ P(\alpha,\underline{T}) \text{ exists and } (\mathrm{lcoeff}(P))(\alpha) \neq 0.$$

For any $Q = Q(z,\underline{T}) \in \mathbb{K}[z, \frac{1}{W_{\mathrm{end}}(z)}, \underline{T}]$, denote by $Q_\alpha = Q(\alpha,\underline{T}) \in \mathbb{K}[\underline{T}]$ the polynomial obtained by evaluating at $z = \alpha$ (recall that $W_{\mathrm{end}}(\alpha) \neq 0$, so that α is not a pole of any coefficient of Q). Then at each step of the algorithm, for any $P \in G$, P_α exists and we have $\mathrm{lmon}(P_\alpha) = \mathrm{lmon}(P)$ since $(\mathrm{lcoeff}(P))(\alpha) \neq 0$. In the same way, at each step, for any $P, Q \in G'$ with $P \neq Q$ we have $\mathrm{lmon}(P_\alpha - Q_\alpha) = \mathrm{lmon}(P - Q)$ so that $P_\alpha \neq Q_\alpha$ (using line $4b(i)$ to check that $\mathrm{lmon}(P - Q)(\alpha) \neq 0$). Lines $4b(iii)$ and $4b(iv)\eta$ show that $\mathrm{lmon}(\widetilde{R}) = \mathrm{lmon}(R)$, where R is the remainder in the weak division of $S(P,Q)$ by G' computed over $\mathbb{K}(z)$, and $\widetilde{R}$ is the remainder in the weak division of $S(P_\alpha, Q_\alpha)$ by the set of H_α with $H \in G'$ (where the weak division is computed following the same steps as the one of $S(P,Q)$ by G').

Actually to obtain this property, we assume that at each step the set G' is ordered in a deterministic way, and that elements $P_1 \in G'$ are tested in this order so that the first one such that $\mathrm{lmon}(P_1)$ divides $\mathrm{lmon}(S)$ is used in line $4b(iv)$. In the same way we assume that the pairs $P, Q \in G'$ are taken in a deterministic order at line $4b$. Then Algorithm 2 starting with $Q_1(z,\underline{X}), \ldots, Q_\ell(z,\underline{X})$ follows exactly the same steps as Algorithm 1 over $\mathbb{L} = \mathbb{K}$ starting with $Q_1(\alpha,\underline{X}), \ldots, Q_\ell(\alpha,\underline{X})$ – recall that we assume $W_{\mathrm{end}}(\alpha) \neq 0$. In more precise terms, each time a polynomial P is considered in Algorithm 2, the polynomial P_α is considered at the same step of Algorithm 1, and we have $\mathrm{lmon}(P_\alpha) = \mathrm{lmon}(P)$.

At the end of Algorithm 2, $G = \{P^{[1]}(z,\underline{T}), \ldots, P^{[s]}(z,\underline{T})\}$ is a Gröbner basis of the ideal $\widetilde{I}$ of $\mathbb{K}(z)[\underline{T}]$ generated by I because Algorithm 2 follows exactly the same steps as Algorithm 1 over $\mathbb{L} = \mathbb{K}(z)$. Proposition 1 (with $\mathbb{L} = \mathbb{K}(z)$ and $i = p$) shows that the set $\mathcal{P}$ of those $P^{[j]}(z,\underline{T})$ which depend only on $T_1, \ldots, T_p$ (and not on $T_{p+1}, \ldots, T_N$) is a Gröbner basis of $\widetilde{I} \cap \mathbb{K}(z)[T_1, \ldots, T_p] = \widetilde{I} \cap \mathbb{K}(z)[\varphi_1, \ldots, \varphi_p]$. In part (i) of Proposition 3, we assume that $I \cap \mathbb{K}[z][\varphi_1, \ldots, \varphi_p] = \{0\}$, so that $\widetilde{I} \cap \mathbb{K}(z)[T_1, \ldots, T_p] = \{0\}$ and $\mathcal{P} = \emptyset$. Therefore for each j there exists $\underline{a}^{(j)} \in \mathbb{N}^N$ such that $\underline{a}_i^{(j)} \geq 1$ for at least one $i \in \{p+1, \ldots, N\}$ and the coefficient $\lambda_{\underline{a}^{(j)}}(z)$ of $\underline{T}^{\underline{a}^{(j)}}$ in $P^{[j]}(z,\underline{T})$ is non-zero. This proves that line $5a$ of Algorithm 2 can be carried out. Moreover, since $W_{\mathrm{end}}(\alpha) \neq 0$ we have $\lambda_{\underline{a}^{(j)}}(\alpha) \neq 0$ (using line $5b$), so that $P^{[j]}(\alpha,\underline{T}) \notin \mathbb{K}[T_1, \ldots, T_p]$.

Now since $W_{\mathrm{end}}(\alpha) \neq 0$, lines 1 and 2 of Algorithm 1 over $\mathbb{L} = \mathbb{K}$ run exactly in the same way as lines 1–4 of Algorithm 2. Therefore $P^{[1]}(\alpha,\underline{T}), \ldots, P^{[s]}(\alpha,\underline{T})$ is the output of lines 1–2 of Algorithm 1: it is a Gröbner basis of I_α. Then Proposition 1 (with $\mathbb{L} = \mathbb{K}$ and $i = p$) shows that the set of those $P^{[j]}(\alpha,\underline{T})$ which depend only on $T_1, \ldots, T_p$ and not on $T_{p+1}, \ldots, T_N$ is a Gröbner basis of $I_\alpha \cap \mathbb{K}[T_1, \ldots, T_p]$. Now we have seen that this set is empty (namely $P^{[j]}(\alpha,\underline{T}) \notin \mathbb{K}[T_1, \ldots, T_p]$ for any j), so that $I_\alpha \cap \mathbb{K}[T_1, \ldots, T_p] = \{0\}$. Since $\mathrm{Im}(\chi_\alpha) = \mathbb{K}[T_1, \ldots, T_p]$ we deduce that $J_\alpha = \chi_\alpha^{-1}(I_\alpha)$ is equal to $\ker(\chi_\alpha)$. Now $W_{\mathrm{end}}(\alpha) \neq 0$ implies $W_0(\alpha) \neq 0$, so that the linear forms $\varphi_1(\alpha,\underline{X}), \ldots, \varphi_p(\alpha,\underline{X})$ are linearly independent over $\mathbb{K}$: the map χ_α is injective, and $J_\alpha = \{0\}$. This concludes the proof of Proposition 3. □

7 Examples

In this section, we give two different illustrations of our algorithm. The first one illustrates Proposition 2, whereas the second one sheds light on Proposition 3 and Algorithm 2 used in its proof.

Consider the E-functions $f(z) = e^{-iz} + (z-1)^2 e^z$ and $f'(z) = -ie^{-iz} + (z^2-1)e^z$. We want do determine for which $\alpha \in \overline{\mathbb{Q}}^*$ the numbers $f(\alpha)$ and $f'(\alpha)$ are algebraically dependent. We first observe that $f(z)$ and $f'(z)$ are $\overline{\mathbb{Q}}(z)$-algebraically independent, because 1 and $-i$ are $\mathbb{Q}$-linearly independent. To apply Beukers' lifting results, we set $g_1(z) = e^z$ and $g_2(z) = e^{-iz}$ which are such that

$$\begin{pmatrix} f \\ f' \end{pmatrix} = \begin{pmatrix} (z-1)^2 & 1 \\ z^2-1 & -i \end{pmatrix} \begin{pmatrix} g_1 \\ g_2 \end{pmatrix}, \qquad \begin{pmatrix} g_1 \\ g_2 \end{pmatrix}' = \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} g_1 \\ g_2 \end{pmatrix}.$$

We introduce the two $\overline{\mathbb{Q}}[z]$-linearly independent linear forms

$$\varphi_1(z, X_1, X_2) = (z-1)^2 X_1 + X_2, \quad \varphi_2(z, X_1, X_2) = (z^2-1)X_1 - iX_2.$$

Since g_1, g_2 are $\overline{\mathbb{Q}}(z)$-algebraically independent (which our algorithm would have first determined), the ideal

$$I := \{Q \in \overline{\mathbb{Q}}[z, X_1, X_2] \quad \text{such that} \quad Q(z, g_1(z), g_2(z)) \equiv 0\}$$

is reduced to $\{0\}$.

Let now $\alpha \in \overline{\mathbb{Q}}^*$ be such that there exists $S \in \overline{\mathbb{Q}}[X, Y] \backslash \{0\}$ such that $S(f(\alpha), f'(\alpha)) = 0$. By Proposition 2, this is equivalent to the fact that $S(\varphi_1(\alpha, X_1, X_2), \varphi_2(\alpha, X_1, X_2)) = Q(\alpha, X_1, X_2)$ for some $Q \in I$, i.e. that

$$S\big((\alpha-1)^2 X_1 + X_2, (\alpha^2-1)X_1 - iX_2\big) \equiv 0$$

as a polynomial in $\overline{\mathbb{Q}}[X_1, X_2]$. Hence

$$S(f(\alpha), f'(\alpha)) = 0 \Longleftrightarrow S\big((\alpha-1)^2 X_1 + X_2, (\alpha^2-1)X_1 - iX_2\big) \equiv 0 \text{ in } \overline{\mathbb{Q}}[X_1, X_2].$$

We now set

$$D(\alpha) := \begin{vmatrix} (\alpha-1)^2 & 1 \\ \alpha^2-1 & -i \end{vmatrix}.$$

If on the one hand, $D(\alpha) \neq 0$, the linear forms $(\alpha-1)^2 X_1 + X_2$ and $(\alpha^2-1)X_1 - iX_2$ are $\overline{\mathbb{Q}}$-linearly independent so that $S(X, Y)$ must in fact be identically zero in $\overline{\mathbb{Q}}[X, Y]$. In other words, the numbers $f(\alpha)$ and $f'(\alpha)$ are $\overline{\mathbb{Q}}$-algebraically independent.

If on the other hand $D(\alpha) = 0$, i.e. if $\alpha = 1$ or $\alpha = i$, the linear forms $(\alpha-1)^2 X_1 + X_2$ and $(\alpha^2-1)X_1 - iX_2$ are $\overline{\mathbb{Q}}$-linearly dependent. If $\alpha = 1$, we must have $S(X_2, -iX_2) \equiv 0$, which means that $S(X, Y)$ is in the principal ideal $(iX + Y)$ of $\overline{\mathbb{Q}}[X, Y]$. If $\alpha = i$, we must have $S(-2iX_1 + X_2, -2X_1 - iX_2) \equiv 0$, which means that $S(X, Y)$ is again in the

principal ideal $(iX+Y)$ of $\overline{\mathbb{Q}}[X,Y]$. In both cases, we can indeed take $S(X,Y)=iX+Y$ because it is readily checked that $f(1)=if'(1)$ and $f(i)=if'(i)$. Note that $f(1)=e^{-i}$ and $f(i)=e+(i-1)^2e^i$ are both transcendental by the Lindemann-Weierstrass Theorem, and this could also be proved by our algorithm or by that in [1].

With the notations of §§5 and 6, we have $N=p=2$ and the polynomial $W_0(z)$ defined in the proof of Proposition 3 is equal to $D(z)$. Since I is the zero ideal, it is generated by $F=\emptyset$. Running Algorithm 2 with this input is trivial: the output is $W(z)=W_0(z)=D(z)$. Moreover for each root α of this polynomial, the algorithm computes the linear relation $f(\alpha)=if'(\alpha)$.

As a second illustration, consider the transcendental E-function, of hypergeometric type,

$$f(z):={}_1F_2\left[\begin{matrix}1/2\\1/3,2/3\end{matrix};z^2\right]=\sum_{n=0}^{\infty}\frac{(2n)!}{n!(3n)!}\left(\frac{27z^2}{4}\right)^n.$$

It is a solution of the differential equation (of minimal order for f)

$$9z^2y'''(z)+9zy''(z)-(36z^2+1)y'(z)-36zy(z)=0. \tag{7.1}$$

A basis of local solutions at $z=0$ of (7.1) is given by

$$f(z),\quad z^{2/3}\,{}_1F_2\left[\begin{matrix}5/6\\2/3,4/3\end{matrix};z^2\right],\quad z^{4/3}\,{}_1F_2\left[\begin{matrix}7/6\\4/3,5/3\end{matrix};z^2\right].$$

Using the algorithm in [4], J.-A. Weil confirmed to us that the differential Galois group ([1]) of (7.1) is $SO(3,\mathbb{C})$ and the ideal of polynomial relations in $\overline{\mathbb{Q}}[z][X_1,X_2,X_3]$ between $f(z),f'(z),f''(z)$ is principal, generated by the first integral

$$f(z)^2-\frac{1}{4}f'(z)^2+\frac{9z^2}{4}\big(4f(z)-f''(z)\big)^2=1. \tag{7.2}$$

In particular, $f(z)$ and $f'(z)$ are $\overline{\mathbb{Q}}(z)$-algebraically independent. Let us prove, following our algorithm, that $\alpha=0$ is the only algebraic number such that $f(\alpha)$ and $f'(\alpha)$ are algebraically dependent over $\overline{\mathbb{Q}}$.

We assume that Feng's algorithm provides the generator

$$Q(z,\underline{X})=X_1^2-\frac{1}{4}X_2^2+\frac{9z^2}{4}(4X_1-X_3)^2-1$$

of the ideal

$$I=\{T\in\overline{\mathbb{Q}}[z,X_1,X_2,X_3],\,T(z,f(z),f'(z),f''(z))=0\}.$$

Let us follow Algorithm 2 that appears in the proof of Proposition 3 (see §6), with $N=3$, $p=2$, $\varphi_1(z,\underline{X})=X_1$, $\varphi_2(z,\underline{X})=X_2$, and $T_i=X_i$. The input is $F=\{Q\}$ and $W_0=1$. The second elimination order is such that $X_1^2>X_2^2>X_1X_3>X_3^2$ so that

[1] The possible differential Galois groups of hypergeometric equations are classified in [14].

lcoeff$(Q) = 1 + 36z^2$. After Step 3 of Algorithm 2 we have $W(z) = z^2 + \frac{1}{36}$ by choosing the monic least common multiple. Then W does not change at Step 4 since $G = F = \{Q\}$ contains only one element. In Step $5a$ we may choose $\underline{a} = (0, 0, 2)$; then after line $5b$ we have $W(z) = z^2(z^2 + \frac{1}{36})$. This is the polynomial we obtain such that property (i) of Proposition 3 holds. Therefore if $\alpha \in \overline{\mathbb{Q}}^*$ is such that that $f(\alpha)$ and $f'(\alpha)$ are algebraically dependent over $\overline{\mathbb{Q}}$, then α is a root of W: $\alpha = \pm i/6$.

Now we follow the proof of part (ii) of Proposition 3 to determine, for each of these values of α, whether $f(\alpha)$ and $f'(\alpha)$ are algebraically dependent or not. For $\alpha = \pm i/6$, the ideal I_α defined after the statement of Proposition 3 is generated by

$$Q_\alpha(\underline{X}) = Q(\alpha, \underline{X}) = -\frac{1}{4}X_2^2 - \frac{1}{16}X_3^2 + \frac{1}{2}X_1X_3 - 1.$$

Since $Q_\alpha \notin \overline{\mathbb{Q}}[T_1, T_2] = \overline{\mathbb{Q}}[X_1, X_2]$ we obtain that the empty set is a Gröbner basis of the ideal J_α defined in §6, so that it is equal to $\{0\}$: $f(\alpha)$ and $f'(\alpha)$ are algebraically independent over $\overline{\mathbb{Q}}$. This concludes the proof that 0 is the only algebraic number α such that $f(\alpha)$ and $f'(\alpha)$ are algebraically dependent.

We point out that the apparently exceptional points $\alpha = \pm i/6$ have appeared in the above computation because the leading monomial of $Q_\alpha(\underline{X})$ is equal to X_2^2 for these values, whereas it is X_1^2 for $\alpha \neq \pm i/6$. This illustrates the general situation in the proof of part (i) of Proposition 3: all agebraic points α where the computations take place in a non-generic way are gathered in the set of roots of the polynomial W; then part (ii) enables one, for each such α, to see whether the E-functions under consideration take algebraically dependent values at α or not.

References

[1] B. Adamczewski, T. Rivoal, *Exceptional values of E-functions at algebraic points*, Bull. London Math. Soc. **50**.4 (2018), 697–908.

[2] Y. André, *Séries Gevrey de type arithmétique I. Théorèmes de pureté et de dualité*, Annals of Math. **151** (2000), 705–740.

[3] Y. André, *Solution algebras of differential equations and quasi-homogeneous varieties: a new differential Galois correspondence*, Annales scientifiques ENS (2014) **47**.2, 449–467.

[4] M. Barkatou, T. Cluzeau, L. Di Vizio and J.-A. Weil, *Computing the Lie Algebra of the Differential Galois Group of a Linear Differential System*, Proceedings of the 2016 ACM International Symposium on Symbolic and Algebraic Computation (ISSAC), 63–70.

[5] T. Becker, V. Weispfenning, *Gröbner bases. A computational approach to commutative algebra*, Graduate Texts in Mathematics 141, Springer-Verlag, New York, 1993.

[6] D. Bertrand, F. Beukers, *Équations différentielles linéaires et majorations de multiplicités*, Annales scientifiques ENS (1985) **18**.1 (1985), 181–192.

[7] D. Bertrand, V. Chirskii, J. Yebbou, *Effective estimates for global relations on Euler-type series*, Annales de la Faculté des sciences de Toulouse : Mathématiques, Sér. 6, **13**. 2 (2004), 241–260.

[8] A. Bostan, F. Chyzak, M. Giusti, R. Lebreton, G. Lecerf, B. Salvy, É. Schost, *Algorithmes Efficaces en Calcul Formel*, 686 pages, 2017.

`https://hal.archives-ouvertes.fr/AECF/`

[9] A. Bostan, T. Rivoal, B. Salvy, *Explicit degree-bounds for factors of linear differential operators*, preprint, 11 pages, 2019.

`https://hal.archives-ouvertes.fr/hal-02154679`

[10] F. Beukers, *A refined version of the Siegel-Shidlovskii theorem*, Annals of Math. **163** (2006), 369–379.

[11] D. Cox, J. Little, D. O'Shea, *Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra*, 2nd ed., Undergraduate Texts in Mathematics, Springer-Verlag, 1996.

[12] R. Feng, *Hrushovski's algorithm for computing the Galois group of a linear differential equation*, Adv. Appl. Math. **65** (2015), 1–37.

[13] E. Hrushovski, *Computing the Galois group of a linear differential equation*, Banach Center Publications **58** (2002), 97–138.

[14] N. Katz, *Exponential sums and differential equations*, Annals of Mathematical Studies, Princeton, 1990.

[15] G. Lepetit, *G-opérateurs au sens large et application à un théorème d'André sur les E-fonctions au sens large*, preprint, 23 pages, 2019.

`https://arxiv.org/abs/1902.07049`

[16] Yu. V. Nesterenko, A. B. Shidlovskii, *On the linear independence of values of E-functions*, Math. Sb. **187** (1996), 93–108 (in russian), translated in english in Sb. Math. **187** (1996), 1197–1211.

[17] M. van der Put, M. Singer, *Galois Theory of Linear Differential Equations*, Grundlehren der math. Wiss. 328, Springer, 2003.

[18] T. Rivoal, *Les E-fonctions et G-fonctions de Siegel*, prépublication, 76 pages, 2019.

[19] A. B. Shidlovskii, *On a criterion for algebraic independence of the values of a class of integral functions*, Izvestia Akad. Nauk SSSR **23** (1959), 36–66.

[20] C. L. Siegel, *Über einige Anwendungen diophantischer Approximationen*, vol. 1 S. Abhandlungen Akad., Berlin, 1929.

[21] C. L. Siegel, *Transcendental Numbers*, Annals of Mathematical Studies **16**, Princeton University Press, 1949.

S. Fischler, Laboratoire de Mathématiques d'Orsay, Univ. Paris-Sud, CNRS, Université Paris-Saclay, 91405 Orsay, France.

T. Rivoal, Institut Fourier, CNRS et Université Grenoble Alpes, CS 40700, 38058 Grenoble cedex 9, France.

Keywords: E-functions, Algebraic independence, Differential equations, Gröbner bases, Algorithm.

MSC 2000: 11J91, 13P10, 33E30, 34M05.