Determining Whether a Multivariate Hyperexponential Function Is Algebraic

Ziming Li and Dabin Zheng

Mathematics-Mechanization Key Laboratory
 Academy of Mathematics and System Sciences
 Chinese Academy of Sciences, Beijing 100080, China
 email: {zmli, zhengdabin}@mmrc.iss.ac.cn

Abstract. Let $F = \mathbb{C}(x_1, \dots, x_\ell, x_{\ell+1}, \dots, x_m)$, where $x_1, \dots, x_\ell$ are continuous variables, and $x_{\ell+1}, \dots, x_m$ are discrete variables. We show that a hyperexponential function, which is algebraic over F , is of form

$$g(x_1, \dots, x_m)q(x_1, \dots, x_\ell)^{\frac{1}{t}}\omega_{j+1}^{x_{\ell+1}} \cdots \omega_m^{x_m}$$

where $g \in F$, $q \in \mathbb{C}(x_1, \dots, x_\ell)$, $t \in \mathbb{Z}^+$ and $\omega_{\ell+1}, \dots, \omega_m$ are roots of unity. Furthermore, we present an algorithm for determining whether a hyperexponential function is algebraic over F .

1. Introduction

Hyperexponential functions in several variables are an abstraction of common properties of exponential functions and hypergeometric terms (see [6]). They play important roles in factoring modules over Laurent-Ore algebras, and in the continuous and discrete versions of Zeilberger’s algorithm for proving combinatorial identities (see [11] and [7], respectively).

Hyperexponential functions can be represented and manipulated by computer algebra systems since their certificates, i.e., their partial “logarithmic derivatives”, are rational functions. In many applications we need to determine whether an algebraic expression involving hyperexponential functions is zero. This motivates us to develop an algorithm, which, for a hyperexponential function given by its certificates, determines whether it is algebraic. We will regard hyperexponential functions as elements in some orthogonal Δ -extensions over the field of rational functions. So hyperexponential functions are called hyperexponential elements in the sequel.

In this article, we characterize algebraic hyperexponential elements by their certificates, describe a normal form of algebraic hyperexponential elements, and present an algorithm for determining whether a hyperexponential element is algebraic.

The rest of this article is organized as follows. In Section 2. we recall the notions of orthogonal Δ -rings and hyperexponential elements. In Section 3. we show that all algebraic-hyperexponential elements are radical, and characterize them by first-order linear differential-difference systems. After studying univariate algebraic-hyperexponential elements in Section 4., we present a characterization on multivariate algebraic-hyperexponential elements by their certificates over the field of rational functions, and describe a normal form of these elements in Section 5.. An algorithm for determining whether a hyperexponential element is algebraic is presented in Section 6..

2. Orthogonal Δ -rings and hyperexponential elements

Let R be a commutative ring. The set of nonzero elements of R is denoted R^* . Let Δ be a finite set of maps from R to itself. A map in Δ is assumed to be either a derivation of R or an automorphism of R . Recall that a derivation δ is an additive map with the multiplicative rule

$$\delta(ab) = a\delta(b) + \delta(a)b \quad \text{for all } a, b \in R.$$

The set Δ is said to be *orthogonal* if the maps in Δ commute pairwise. The pair (R, Δ) is called an orthogonal Δ -ring if Δ is orthogonal.

For a derivation $\delta \in \Delta$, an element c of R is called a *constant* with respect to δ if $\delta(c) = 0$. For an automorphism $\sigma \in \Delta$, c is called a *constant* with respect to σ if $\sigma(c) = c$. An element c of R is called a *constant* if it is a constant with respect to all maps in Δ . The set of constants of R , denoted by C_R , is a subring. The ring C_R is a subfield if R is a field.

Let (F, Δ) be an orthogonal Δ -field and A a commutative F -algebra. The pair (A, Δ) is called an orthogonal Δ -extension of F if all the maps in Δ can be extended to A in such a way that: all derivations of F become derivations of A ; all automorphisms of F become automorphisms of A ; and the extended maps commute pairwise. There are ample instances for orthogonal Δ -extensions, for example, (partial) differential and difference algebras, and Picard-Vessiot extensions of linear functional systems with finite linear dimension (see [3]). Note that an orthogonal Δ -extension is not necessarily an integral domain.

Let (A, Δ) be an orthogonal Δ -extension of F . A nonzero element h of A is said to be *hyperexponential* over F if, for every map $\phi \in \Delta$, there exists $r_\phi \in F$ such that $\phi(h) = r_\phi h$. Note that r_ϕ is nonzero if ϕ is an automorphism. We call r_ϕ the certificate of h with respect to ϕ .

For the differential field $(\mathbb{C}(x), \frac{d}{dx})$, (nonzero) rational, radical and usual exponential functions are hyperexponential elements. For the difference field $(\mathbb{C}(n), \sigma)$, where σ is the shift operator sending n to $n+1$, the terms $n!$, $\binom{n}{2}$ and $(-1)^n$ are examples of hyperexponential elements. Note that the term $(-1)^n$ cannot live in an integral domain because $(-1)^n + 1$ is a zero divisor (see [9, Preface]). For the differential-difference field $(\mathbb{C}(x, n), \{\frac{d}{dx}, \sigma\})$, the expressions x^n , $\exp(x^2 + 1)x^n$ and $\sqrt{x}(-1)^n$ are examples of hyperexponential elements.

An ideal I of an orthogonal ring (R, Δ) is said to be *invariant* if $\phi(I) \subset I$ for all $\phi \in \Delta$. An orthogonal ring (R, Δ) is said to be *simple* if its invariant ideals are (0) and (1) . If R is simple, then every nonzero constant c is invertible since the ideal (c) is invariant. In the same vein, we have

Lemma 2.1 *Let A be an orthogonal extension of (F, Δ) . If A is simple, then every hyperexponential element of A over F is invertible.*

Proof. Let h be a hyperexponential element of A . For every $\phi \in \Delta$, $\phi(h) \in (h)$. Hence (h) is invariant, and, consequently, $(h) = (1)$. $\square$

Note that the product of two hyperexponential elements is again hyperexponential, but the sum of two hyperexponential elements is not necessarily hyperexponential.

3. Algebraic-hyperexponential elements

In this section (F, Δ) is fixed to be an orthogonal Δ -field with characteristic zero. Let A be an orthogonal Δ -extension of F . A nonzero element a of A is said to be *algebraic* over F if $p(a) = 0$ for some $p \in F[z]^*$. The monic polynomial with the minimal degree, for which a is a solution, is called the *minimal polynomial* of a . The minimal polynomial of a is not necessarily irreducible over F , since A is not assumed to be an integral domain. For example, the minimal polynomial of $(-1)^n$ is $z^2 - 1$.

The next lemma asserts that algebraic-hyperexponential elements are radical if the orthogonal extension contains no new constants. It is a straightforward generalization of known results in ordinary differential and difference cases [5, 10].

Lemma 3.1 *Let A be an orthogonal Δ -extension of F and $C_A = C_F$. If an element h of A is hyperexponential and algebraic over F , then the minimal polynomial of h is of the form $z^t - f$ for some $f \in F$.*

Proof. Let the minimal polynomial of h be of degree t . The lemma clearly holds for $t = 1$. Assume that $t > 1$. Then h is not rational. We have

$$h^t + \sum_{i=1}^{t-1} f_i h^i + f_0 = 0 \quad \text{for some } f_{t-1}, \dots, f_0 \in F. \quad (1)$$

Let $\delta \in \Delta$ be a derivation. Apply δ to (1) to get

$$(tr_\delta)h^t + \sum_{i=1}^{t-1} (\delta(f_i) + ir_\delta f_i)h^i + \delta(f_0) = 0,$$

where r_δ is the certificate of h with respect to δ . The minimality of t then implies that

$$\delta(f_i) = (t - i)r_\delta f_i \quad \text{for } i = 1, \dots, t - 1. \quad (2)$$

Similarly, let σ be an automorphism in Δ . Apply σ to (1) to get

$$r_\sigma^t h^t + \sum_{i=1}^{t-1} (\sigma(f_i) r_\sigma^i h^i) + \sigma(f_0) = 0,$$

where r_σ is the certificate of h with respect to σ . By the minimality of t ,

$$\sigma(f_i) = r_\sigma^{t-i} f_i \quad \text{for } i = 1, \dots, t - 1. \quad (3)$$

If f_i is nonzero for some i with $1 \leq i \leq t - 1$, then (2) and (3) imply that the ratio of h^{t-i} and f_i is a constant. It follows from the assumption $C_A = C_F$ that h satisfies a polynomial of degree $(t - i)$ over F , a contradiction to the minimality of t . Hence, $f_i = 0$ for all i with $1 \leq i \leq t - 1$. $\square$

Notation. Let A be an orthogonal Δ -extension of F . For every $\phi \in \Delta$ and $a \in A$, which is invertible, the ratio $\frac{\phi(a)}{a}$ is denoted by $\text{l}\phi(a)$.

Some useful properties of the operator $\text{l}\phi$ are given in the next lemma whose proof is straightforward.

Lemma 3.2 *Let A be an orthogonal Δ -ring and $a, b \in A$ be invertible. Let δ and σ be a derivation and an automorphism in Δ , respectively. Then*

1. $\text{ld}(ab) = \text{ld}(a) + \text{ld}(b)$ and $\text{ls}(ab) = \text{ls}(a)\text{ls}(b)$;
2. $\text{ld}(a^n) = n\text{ld}(a)$ and $\text{ls}(a^n) = \text{ls}(a)^n$ for all $n \in \mathbb{Z}$;

If $h \in A$ is invertible and hyperexponential, then, for every $\phi \in \Delta$, $\text{ls}(\phi(h))$ is the certificate of h with respect to ϕ . The following proposition characterizes invertible algebraic-hyperexponential elements.

Proposition 3.3 *Let A be an orthogonal Δ -extension of F and $C_A = C_F$. If an element h of A is invertible and hyperexponential over F , then h is algebraic over F if and only if there exists a positive integer t and a nonzero element f of F such that*

$$t \text{ld}(h) = \text{ld}(f) \quad \text{for all derivations } \delta \in \Delta \quad (4)$$

and

$$\text{ls}(h)^t = \text{ls}(f) \quad \text{for all automorphisms } \sigma \in \Delta. \quad (5)$$

In addition, the minimal integer t such that (4) and (5) hold for some nonzero $f \in F$, is the degree of the minimal polynomial of h .

Proof. If h is algebraic, then $h^t = f$ for some positive integer t and $f \in F$, which is nonzero since h is invertible. Applying ld and ls to $h^t = f$ yields (4) and (5), respectively. Conversely, a straightforward application of Lemma 3.2 shows that $\frac{h^t}{f}$ is a constant, which is in F since $C_A = C_F$. $\square$

One might wonder the existence of orthogonal Δ -extensions of F that contain no new constants. In fact, all Picard-Vessiot extensions of F are such extensions, provided that F is of characteristic zero with an algebraically closed field of constants. In addition, Picard-Vessiot extensions are simple (see [8, 9] for the ordinary case and [3] for the partial case).

By a *minimal solution* of the system consisting of equations in (4) and (5) we mean a pair $(t, f) \in \mathbb{Z}^+ \times F$ such that (t, f) solves the system and $t \leq \tilde{t}$ if $(\tilde{t}, \tilde{f}) \in \mathbb{Z}^+ \times F$ also solves the system. Determining whether a given hyperexponential element h is algebraic, amounts to computing a (minimal) solution of (4) and (5) by Proposition 3.3. To find a minimal solution effectively, we have to restrict ourselves to the case in which the ground field F is the field of rational functions.

4. Ordinary case

In this section we present some properties of univariate algebraic exponential functions and hypergeometric terms. In the rest of the article, C stands for a field of characteristic zero.

Proposition 4.1 *Let $\Delta = \{\delta = \frac{d}{dx}\}$. For a nonzero $r \in C(x)$, there exist $t \in \mathbb{Z}^+$ and $f \in C(x)$ such that $tr = \text{ld}(f)$ if and only if the squarefree partial fraction decomposition of r can be written as a finite sum $\sum_i c_i \text{ld}(p_i)$, where $p_i \in C[x]$ and $c_i \in \mathbb{Q}$.*

Proof. The proposition follows from the fact that, for every $f \in C(x)^*$, the squarefree partial fraction decomposition of $\text{ld}(f)$ is a $\mathbb{Z}$ -linear combination of logarithmic derivatives of polynomials in $C[x]$. $\square$

If $r = \sum_i \frac{n_i}{k} \text{ld}(p_i)$ with $p_i \in C[x]$, $n_i \in \mathbb{Z}^*$, and $k \in \mathbb{Z}^+$ as small as possible, then $(k, \prod_i p_i^{n_i})$ is a minimal solution of $tr = \text{ld}(f)$.

To consider the ordinary difference case, we introduce a multiplicative decomposition of a rational function. For $t \in \mathbb{Z}^+$, a nonzero rational function $f \in C(x)$ can be written as $f = q^t p$, where $q \in C(x)$ and $p \in C[x]$ whose factors have multiplicities less than t . We call the product $q^t p$ a *multiplicative decomposition of f with respect to t* .

Example 4.2 Consider $f = \frac{7x^4(x-1)^3}{(x+1)^8(x+2)}$ and $t = 3$. Let

$$q = \frac{x(x-1)}{(x+1)^3(x+2)} \quad \text{and} \quad p = 7x(x+1)(x+2)^2.$$

Then $r = q^3 p$ is a multiplicative decomposition of r with respect to 3.

In general, such a decomposition can be found by the squarefree decomposition of the numerator and denominator of r and a rearrangement of the squarefree factors.

Proposition 4.3 Assume that C contains all roots of unity. Let $(C(x), \{\sigma\})$ be an orthogonal Δ -field where $\sigma(x) = x + c$ for some $c \in C$ and σ is the identity map on C . For a nonzero $r \in C(x)$, there exist $t \in \mathbb{Z}^+$ and $f \in C(x)^*$ such that $r^t = \text{ld}(f)$ if and only if $r = \omega \text{ld}(q)$ where $\omega^t = 1$ and $q \in C(x)$.

Proof. Assume that $r^t = \text{ld}(f)$ for some $t \in \mathbb{Z}^+$ and $f \in C(x)$. Let $f = q^t p$ be a multiplicative decomposition with respect to t . Then

$$r^t = \text{ld}(q)^t \text{ld}(p). \quad (6)$$

Since both $\sigma(p)$ and p are polynomials whose squarefree factors have multiplicities less than t , we conclude that $\text{ld}(p)$ is an element of C . But $\sigma(p)$ and p have the same leading coefficients. So this element has to be one. It follows from (6) that $r = \omega \text{ld}(q)$, where $\omega^t = 1$. The converse holds evidently. $\square$

The case in which σ is not a shift operator, is rather involved. Recall the well-known fact that a C -automorphism σ of $C(x)$ is given by

$$\sigma(x) = \frac{ax + b}{cx + d}, \quad \text{where } a, b, c, d \in C \text{ with } ad - bc \neq 0. \quad (7)$$

Proposition 4.4 Let C be an algebraically closed field. Let σ be an automorphism of $C(x)$ given by (7). If there are functions f and r in $C(x)$ such that $r^t = \text{ld}(f)$ for some integer $t > 1$, then there exist $\alpha \in C^*$ and $g \in C(x)$ such that $r = \alpha \text{ld}(g)$.

Proof. Let $f = q^t p$ be a multiplicative decomposition with respect to t . Then $r^t = \text{ld}(q)^t \text{ld}(p)$. The proof is similar to that of Proposition 4.3 if either $\text{ld}(p)$ is in C or c in (7) is zero. Thus, we may further assume that $\deg_x(p) = m > 0$ and $c \neq 0$. Let $\bar{p} = (cx + d)^m \sigma(p)$. Then $\bar{p}$ is a polynomial. Write

$$p = p_m(x - \beta_1)^{m_1} \cdots (x - \beta_k)^{m_k},$$

where $p_m \in C^*$, $\beta_1, \dots, \beta_k$ are distinct and $m_1, \dots, m_k$ are positive integers less than t . Then

$$\bar{p} = p_m((a - \beta_1 c)x - (\beta_1 d - b))^{m_1} \cdots ((a - \beta_k c)x - (\beta_k d - b))^{m_k}.$$

The condition $ad - bc \neq 0$ then implies that all the roots of $\bar{p}$ have multiplicities less than t . By the definition of $\bar{p}$, $\text{ls}(p) = \frac{1}{(cx+d)^m} \bar{p}$. Thus, a multiplicative decomposition of $\text{ls}(p)$ with respect to t is of form $\left(\frac{e}{(cx+d)^s}\right)^t \frac{u}{v}$, where $e \in C$, $s \in \mathbb{N}$ and u, v are monic polynomials whose roots have multiplicities less than t . Since $r^t = \text{ls}(q)^t \text{ls}(p)$, $\text{ls}(p)$ is a t th power of some rational function. Consequently, $\text{ls}(p) = \left(\frac{e}{(cx+d)^s}\right)^t$. We claim that

$$\frac{e}{(cx+d)^s} = \lambda \text{ls}(w) \quad \text{for some } \lambda \in C \text{ and } w \in C[x]. \quad (8)$$

To see this, we set $w = (x + \mu)^s$ where $\mu \in C$ is to be determined by (8). An easy calculation shows that

$$\text{ls}(w) = \left((\mu c + a) \frac{x + \frac{\mu d + b}{\mu c + a}}{(x + \mu)(cx + d)} \right)^s.$$

Thus we may choose $\mu \in C$ such that $\mu = \frac{\mu d + b}{\mu c + a}$, i.e. $c\mu^2 + (a - d)\mu - b = 0$ and $\mu c + a \neq 0$. Such a solution μ always exists since C is algebraically closed. Moreover, we set $\lambda = \frac{e}{(\mu c + a)^s}$. Our claim is proved. Let $g = qw$. Then $r^t = \lambda \text{ls}(g)^t$. Thus $r = \alpha \text{ls}(g)$ with $\alpha^t = \lambda$. $\square$

Unfortunately, Proposition 4.4 is merely a necessary condition. It is not clear for us when $r^t = \text{ls}(f)$ for some $t \in \mathbb{Z}^+$ and $f \in C(x)$ if $r = \alpha \text{ls}(g)$ for some $\alpha \in C$ and $g \in C(x)$.

5. Partial case

To consider the partial case, we let $\Delta = \{\delta_1, \dots, \delta_\ell, \sigma_{\ell+1}, \dots, \sigma_m\}$ and F to be the field $C(x_1, \dots, x_\ell, x_{\ell+1}, \dots, x_m)$, where C is a subfield of $\mathbb{C}$ and contains all roots of unity. Let $\delta_i = \frac{\partial}{\partial x_i}$, $i = 1, \dots, \ell$, and let $\sigma_j(x_j) = x_j + c_j$, $j = \ell + 1, \dots, m$, where c_j is a nonzero rational function free of x_j . A special property of this setting is that

$$\delta_i(f) = 0 \iff f \in C(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_m)$$

for all i with $1 \leq i \leq \ell$, and

$$\sigma_j(f) = f \iff f \in C(x_1, \dots, x_{j-1}, x_{j+1}, \dots, x_m)$$

for all j with $\ell + 1 \leq j \leq m$. This property makes it clear what are constants with respect to a map in Δ . Note that F is a partial differential field if $\ell = m$ and a partial difference field if $\ell = 0$.

Clearly (F, Δ) is an orthogonal Δ -field. Let A be an orthogonal Δ -extension of F with $C_A = C_F$, and $h \in A$ be invertible and hyperexponential over F . Denote $\text{ld}_i(h)$ by r_i , $i = 1, \dots, \ell$, and $\text{ls}_j(h)$ by r_j , $j = \ell + 1, \dots, m$. By Proposition 3.3, h is algebraic over F if and only if there exist $t \in \mathbb{Z}^+$ and $f \in F$ such that

$$tr_i = \text{ld}_i(f), \quad i = 1, \dots, \ell, \quad \text{and} \quad r_j^t = \text{ls}_j(f), \quad j = \ell + 1, \dots, m. \quad (9)$$

It is important to note that the commutativity of Δ implies the following compatibility conditions:

$$\delta_i(r_k) = \delta_k(r_i), \quad 1 \leq i < k \leq \ell, \quad (10)$$

$$\sigma_j(r_k)r_j = \sigma_k(r_j)r_k, \quad \ell + 1 \leq j < k \leq m, \quad (11)$$

and

$$\sigma_j(r_i)r_j = r_i r_j + \delta_i(r_j), \quad 1 \leq i \leq \ell \text{ and } \ell + 1 \leq j \leq m. \quad (12)$$

Our goal is to search for a minimal solution of (9) under the assumption that (10), (11) and (12) hold.

The next lemma is Proposition 3 in [6] without invoking the notion of Ore rings.

Lemma 5.1 *The system*

$$\{\delta_i(z) = r_i z, \quad i = 1, \dots, \ell \quad \text{and} \quad \sigma_j(z) = r_j z, \quad j = \ell + 1, \dots, m\},$$

where the r_i are in F , and (10), (11) and (12) hold, has a (nonzero) rational solution if and only if there exist $s_1, \dots, s_\ell, s_{\ell+1}, \dots, s_m \in F$ such that

$$r_i = \text{l}\delta_i(s_i), \quad i = 1, \dots, \ell, \quad \text{and} \quad r_j = \text{l}\sigma_j(s_j), \quad j = \ell + 1, \dots, m.$$

Proof. Let $R = F[\partial_1, \dots, \partial_m]$ be the Ore ring corresponding to the set Δ . Then the left ideal generated by $\partial_1 - r_1, \dots, \partial_m - r_m$ is of rank one by (10), (11) and (12). The lemma then follows from Proposition 3 in [6]. $\square$

Our main result is given in the next proposition, which extends Propositions 4.1 and 4.3.

Proposition 5.2 *Let $r_1, \dots, r_m$ in F satisfy (10), (11) and (12). Then (9) has a solution in $\mathbb{Z}^+ \times F$ if and only if*

1. *for all i with $1 \leq i \leq \ell$, $r_i = k_i \text{l}\delta_i(f_i)$ for some $k_i \in \mathbb{Q}$ and $f_i \in F$; and*
2. *for all j with $\ell + 1 \leq j \leq m$, $r_j = \omega_j \text{l}\sigma_j(f_j)$ for some unitary root ω_j and $f_j \in F$.*

Proof. If (9) has a solution, then Propositions 4.1 and 4.3 imply the two assertions. Conversely, for all i with $1 \leq i \leq \ell$, the squarefree partial fraction decomposition of r_i can be written as

$$r_i = \sum_{k=1}^{s_i} n_{ki} \text{l}\delta_i(p_{ki}) \quad (13)$$

where $n_{ki} \in \mathbb{Q}$ and $p_{ki} \in C(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_m)[x_i]$. Let n be the least common denominator of all the n_{ki} . Moreover, let t be the least common multiple of n and the orders of the ω_j . Then, for all i with $1 \leq i \leq \ell$ and j with $\ell + 1 \leq j \leq m$, $tr_i = \text{l}\delta_i(q_i)$ and $r_j^t = \text{l}\sigma_j(q_j)$ for some $q_i, q_j \in F$. A straightforward calculation shows that (10), (11) and (12) hold when r_i and r_j are replaced by tr_i and r_j^t , respectively. By Lemma 5.1 there exists $f \in F$ such that $\text{l}\delta_i(q_i) = \text{l}\delta_i(f)$ and $\text{l}\sigma_j(q_j) = \text{l}\sigma_j(f)$. Consequently, (t, f) is a solution of (9). $\square$

Remark 5.3 If $\alpha \text{l}\sigma_j(u) = \beta \text{l}\sigma_j(v)$, where $\alpha, \beta \in C^*$ and $u, v \in F$, then α equals β . This is because $\frac{\alpha}{\beta}$ is a ratio of two polynomials in x_j with equal leading coefficients. Moreover, if $r = k \text{l}\delta_i(f)$ where $k \in \mathbb{Q}^*$ and $f \in F$, then the denominator of k is a common denominator of the n_{ik} given in (13). These two observations imply that the solution (t, f) constructed in the proof of Proposition 5.2 is minimal.

In fact, a solution of (9) has a special form described in the next lemma. This form allows us not only to present minimal solutions of (9) compactly but also to compute minimal polynomials efficiently.

Lemma 5.4 Let $F_\ell = C(x_1, \dots, x_\ell)$. If (10), (11) and (12) hold, and (9) has a minimal solution (t, f) , then $f = qg^t$ where $q \in F_\ell$ and $g \in F$.

Proof. By Proposition 5.2, $r_j = \omega_j \text{l}\sigma_j(f_j)$ for all j with $\ell + 1 \leq j \leq m$. The equality (11) implies that

$$\sigma_k(\text{l}\sigma_j(f_j)) \text{l}\sigma_k(f_k) = \sigma_j(\text{l}\sigma_k(f_k)) \text{l}\sigma_j(f_j), \quad \ell + 1 \leq j \leq k \leq m.$$

In other words, the system $\{\sigma_j(z) = \text{l}\sigma_j(f_j)z \mid \ell + 1 \leq j \leq m\}$ is fully integrable over the difference field $(F_\ell(x_{\ell+1}, \dots, x_m), \{\sigma_{\ell+1}, \dots, \sigma_m\})$. By Lemma 5.1 there exists $g \in F$ such that $\text{l}\sigma_j(f_j) = \text{l}\sigma_j(g)$. Hence

$$r_j = \omega_j \text{l}\sigma_j(g), \quad j = \ell + 1, \dots, m. \quad (14)$$

We claim that $q_i = r_i - \text{l}\delta_i(g)$ is in F_ℓ for $i = 1, \dots, \ell$. It suffices to show that $\sigma_j(q_i) = q_i$ for all i with $1 \leq i \leq \ell$ and j with $\ell + 1 \leq j \leq m$. By (12) and (14), $\sigma_j(q_i + \text{l}\delta_i(g))(\omega_j \text{l}\sigma_j(g)) = (q_i + \text{l}\delta_i(g))(\omega_j \text{l}\sigma_j(g)) + \delta_i(\omega_j \text{l}\sigma_j(g))$. It follows that

$$\begin{aligned} \sigma_j(q_i) - q_i &= \text{l}\delta_i(g) - \sigma_j(\text{l}\delta_i(g)) + \text{l}\delta_i(\text{l}\sigma_j(g)) \quad (\text{by Lemma 3.2}) \\ &= \text{l}\delta_i(\sigma_j(g)) - \sigma_j(\text{l}\delta_i(g)) \quad (\text{since } \sigma_j \circ \delta_i = \delta_i \circ \sigma_j) \\ &= 0. \end{aligned}$$

The claim is proved. On the other hand, (10) and $\delta_i \circ \delta_k = \delta_k \circ \delta_i$ imply

$$\delta_i(tq_k) = \delta_k(tq_i) \quad \text{for all } 1 \leq i < k \leq \ell. \quad (15)$$

Lemma 5.1 and the above claim then imply that the system

$$\{\delta_1(z) = tq_1z, \dots, \delta_\ell(z) = tq_\ell z\}$$

has a rational solution in F_ℓ . In other words, there exists $q \in F_\ell$ such that $q_i = \frac{1}{t} \text{l}\delta_i(q)$ for all i with $1 \leq i \leq \ell$. Therefore,

$$r_i = \frac{1}{t} \text{l}\delta_i(q) + \text{l}\delta_i(g) = \frac{1}{t} \text{l}\delta_i(qg^t)$$

which, together with (14), implies that (t, qg^t) is a solution of (9). $\square$

In the algorithm **IsAlgebraic** for computing a minimal solution of (9) in Section 6.3., we will compute q and g so as to avoid constructing the fully expanded expression qg^t , which may be large for $t > 1$.

As another consequence, an algebraic hyperexponential function is a product of some simpler functions.

Corollary 5.5 *Let A be an orthogonal Δ -extension of F with $C_A = C$. Let h be an invertible and hyperexponential element of A . Then h is algebraic if and only if*

$$h = gH,$$

where $g \in F$, $\text{ld}_i(H) \in C(x_1, \dots, x_\ell)$ is a product of a rational number and a logarithmic derivative of a rational function with respect to x_i for $i = 1, \dots, \ell$, and $\text{ls}_j(H)$ is a root of unity for $j = \ell + 1, \dots, m$.

Proof. By Proposition 5.2 and Lemma 5.4, h is algebraic if and only if (9) has a solution (t, qg^t) where $t \in \mathbb{Z}^+$, $q \in C(x_1, \dots, x_\ell)$ and $g \in F$. Setting $H = \frac{h}{g}$ yields the corollary. $\square$

Informally, an algebraic-hyperexponential function h can be written as

$$h(x_1, \dots, x_m) = g(x_1, \dots, x_m)q(x_1, \dots, x_\ell)^{\frac{1}{t}}\omega_{j+1}^{x_{j+1}} \cdots \omega_m^{x_m}$$

where both g and q are rational, and $\omega_j^t = 1$ for all j with $\ell + 1 \leq j \leq m$.

6. Algorithms

In this section, we let $F = C(x_1, \dots, x_\ell, x_{\ell+1}, \dots, x_m)$ where C is a subfield of $\mathbb{C}$ and contains all roots of unity. Let $\delta_i = \frac{\partial}{\partial x_i}$ for $i = 1, \dots, \ell$, and let σ_j be the usual shift operator with respect to x_j , i.e. $\sigma_j(x_j) = x_j + 1$ for $j = \ell + 1, \dots, m$. The restriction on the σ_j 's allows us to use the notion of shift normal forms of rational functions introduced in [1, 2].

6.1. Differential and shift normal forms

We recall two normal forms for rational functions in [4] and [1, 2], respectively. Let E be a field of characteristic zero. Let $\delta = \frac{d}{dx}$ and σ be the automorphism of $E(x)$ that sends x to $x + 1$.

Let $(a, b) \in E[x] \times E[x]$ with $ab \neq 0$. We say that the ordered pair (a, b) is *differential-reduced* if $\gcd(b, a - i\delta(b)) = 1$ for all $i \in \mathbb{Z}$. A rational function f in $E(x)$ is *differential-reduced* if the ordered pair composed of its numerator and denominator is differential-reduced (0 is evidently differential-reduced). For every $r \in E(x)^*$, there exist $K, S \in E(x)$ such that $r = K + \text{ld}(S)$ where K is differential-reduced and has a monic denominator. The pair (K, S) is called a differential normal form of r .

Lemma 6.1 *Let $r \in E(x)$ equal $\text{ld}(f)$ for some $f \in E(x)$. If (K, S) is a differential normal form of r , then $K = 0$ and $\frac{S}{f} \in E$.*

Proof. Clearly, $(0, \text{ld}(f))$ is a differential normal form of r . By Lemma 4 in [4] the denominator of K is one. So $K = 0$, for otherwise $K = \text{ld}\left(\frac{f}{S}\right)$, which is not in $E[x]$, a contradiction. Since $\text{ld}(f) - \text{ld}(S) = 0$, the ratio of S and f is in E . $\square$

Let $(a, b) \in E[x] \times E[x]$ with $ab \neq 0$. We say that the ordered pair (a, b) is *shift-reduced* if $\gcd(a, \sigma^i(b)) = 1$ for all $i \in \mathbb{Z}$. A nonzero f in $E(x)$ is *shift-reduced* if its ordered pair formed by its numerator and denominator is shift-reduced. For every nonzero $r \in E(x)$, there exist $K, S \in E(x)$ such that $r = K\mathfrak{l}\sigma(S)$ where K is shift-reduced and has a monic denominator. The pair (K, S) is called a shift normal form of r .

Lemma 6.2 *Let $r \in E(x)$ equal $e\mathfrak{l}\sigma(f)$ for some $e \in E$ and $f \in E(x)$. If (K, S) is a shift normal form of r , then $K = e$ and $\frac{S}{f} \in E$.*

Proof. Clearly, $(e, \mathfrak{l}\sigma(f))$ is a shift normal form of r . By the first and third assertions of Theorem 2 in [2], we conclude that $K = e$. It follows that $\mathfrak{l}\sigma(f) = \mathfrak{l}\sigma(S)$. Consequently, the ratio of S and f is in E . $\square$

6.2. Is a hyperexponential element rational ?

Determining whether a hyperexponential element is rational is equivalent to finding a solution $(1, f)$ of (9). In other words, we need to compute a rational solution of the system

$$\delta_i(z) = r_i z, \quad i = 1, \dots, \ell \quad \text{and} \quad \sigma_j(z) = r_j z, \quad j = \ell + 1, \dots, m, \quad (16)$$

where the r_i and r_j satisfy the compatibility conditions (10), (11) and (12).

The following criterion is immediate from Lemmas 5.1, 6.1 and 6.2.

Proposition 6.3 *Let (K_i, S_i) be a differential normal form of r_i relative to x_i and δ_i for $i = 1, \dots, \ell$. Let (K_j, S_j) be a shift normal form of r_j relative to x_j and σ_j for $j = \ell + 1, \dots, m$. Then (16) has a rational solution if and only if $K_1 = \dots = K_\ell = 0$ and $K_{\ell+1} = \dots = K_m = 1$.*

First, let us compute a rational solution of the first ℓ equations in (16). Let (K_1, S_1) be a differential normal form of r_1 relative to x_1 and δ_1 . If K_1 is nonzero then (16) has no rational solutions. Otherwise, every rational solution of (16) equals yS_1 where $y \in C(x_2, \dots, x_m)$. Substituting yS_1 for z in (16) yields

$$\delta_i(y) = (r_i - \mathfrak{l}\delta_i(S_1))y, \quad i = 2, \dots, \ell. \quad (17)$$

If $r_i - \mathfrak{l}\delta_i(S_1)$ is not in $C(x_2, \dots, x_m)$, then (16) has no rational solutions. Otherwise, we compute rational solutions of (17) in $C(x_2, \dots, x_m)$ recursively. In this way, we obtain rational solutions of the first ℓ equations of (16). Suppose that u is such a rational solution (set $u = 1$ when $\ell = 0$). Then every rational solution of (16) is of form yu where $y \in C(x_{\ell+1}, \dots, x_m)$. Substituting yu for z in the last $(m - \ell)$ equations of (16), we have

$$\sigma_j(y) = \frac{r_j}{\mathfrak{l}\sigma_j(u)}y, \quad j = \ell + 1, \dots, m, \quad (18)$$

If $\frac{r_j}{\mathfrak{l}\sigma_j(u)}$ is not in $C(x_{\ell+1}, \dots, x_m)$, then (16) has no rational solutions. Otherwise, we compute a shift normal form $(\hat{K}_{\ell+1}, \hat{S}_{\ell+1})$ of $\frac{r_{\ell+1}}{\mathfrak{l}\sigma_{\ell+1}(u)}$ relative to $x_{\ell+1}$ and $\sigma_{\ell+1}$. If $\hat{K}_{\ell+1}$ is not equal to one, then (16) has no rational solutions. Otherwise, every rational solution of (18) is equal to $w\hat{S}_{\ell+1}$ where $w \in C(x_{\ell+2}, \dots, x_m)$. Substituting $w\hat{S}_{\ell+1}$ for y in (18), we have

$$\sigma_j(w) = \frac{r_j}{\mathfrak{l}\sigma_j(u\hat{S}_{\ell+1})}w, \quad j = \ell + 2, \dots, m, \quad (19)$$

If $\frac{r_j}{\mathfrak{l}\sigma_j(u\hat{S}_{\ell+1})}$ is not in $C(x_{\ell+2}, \dots, x_m)$ for some j with $\ell + 2 \leq j \leq m$, then (16) has no rational solutions. Otherwise, we compute rational solutions of (19) in $C(x_{\ell+2}, \dots, x_m)$ recursively.

6.3. Is a hyperexponential element algebraic ?

The next proposition is a restatement of Proposition 5.2 in terms of differential and shift normal forms.

Proposition 6.4 *Let $F = C(x_1, \dots, x_m)$, where C is a subfield of $\mathbb{C}$ containing all roots of unity. Let $\Delta = \{\delta_1, \dots, \delta_\ell, \sigma_{\ell+1}, \dots, \sigma_m\}$, where $\delta_i = \frac{\partial}{\partial x_i}$, and σ_j is the usual partial shift operator with respect to x_j . Let A be a simple orthogonal Δ -extension of (F, Δ) with $C_A = C$, and h be a hyperexponential element of A . Let (K_i, S_i) be a differential normal form of $\delta_i(h)$ for $i = 1, \dots, \ell$, and (K_j, S_j) be a shift normal form of $\sigma_j(h)$ for $j = \ell + 1, \dots, m$. Then h is algebraic over F if and only if the following conditions hold:*

1. *For all i with $1 \leq i \leq \ell$, the squarefree partial fraction decomposition of K_i is a $\mathbb{Q}$ -linear combination of logarithmic derivatives of some rational functions with respect to δ_i .*
2. *For all j with $\ell + 1 \leq j \leq m$, K_j is a root of unity.*

Proof. Let $r_i = \delta_i(h)$ for $i = 1, \dots, \ell$ and $r_j = \sigma_j(h)$ for $j = \ell + 1, \dots, m$. Then the r_i and r_j satisfy (10), (11) and (12). Thus h is algebraic if and only if (9) has a solution in $\mathbb{Z}^+ \times F$. The proposition then follows from Proposition 5.2. $\square$

At last, we present an algorithm to determine whether a given hyperexponential element h is algebraic, and compute its minimal polynomial when it is. Note that h is given by its certificates $r_1, \dots, r_\ell, r_{\ell+1}, \dots, r_m$, and it is understood as an element in a simple orthogonal Δ -extension A of (F, Δ) described in Proposition 6.4.

Algorithm IsAlgebraic. Given a list of rational functions $r_1, \dots, r_\ell, r_{\ell+1}, \dots, r_m \in F$, determine whether there exists a hyperexponential element h in a proper orthogonal Δ -extension of (F, Δ) such that the certificates of h are the given rational functions and h is algebraic over F . If the answer is affirmative, compute the minimal polynomial of h .

1. *[check compatibility].* Check whether $r_1, \dots, r_\ell, r_{\ell+1}, \dots, r_m$ satisfy (10), (11) and (12). If these conditions are not satisfied, then exit [*h is not well-defined*].
2. *[compute shift normal forms].* For $j = \ell + 1, \dots, m$, compute a shift normal form (K_j, S_j) of r_j ; if K_j is not a root of unity, then exit [*h is not algebraic*].
3. *[compute differential normal forms].* For $i = 1, \dots, \ell$, compute a differential normal form (K_i, S_i) of r_i ; compute the squarefree partial fraction decomposition of K_i . If the decomposition is not a $\mathbb{Q}$ -linear combination of logarithmic derivatives of rational functions with respect to x_i , then exit [*h is not algebraic*]. Otherwise set the decomposition to be

$$K_i = \sum_{k=1}^{s_i} n_{ki} \delta_i(p_{ki}) \quad \text{where } n_{ki} \in \mathbb{Q} \text{ and } p_{ki} \in F. \quad (20)$$

[At this point we have known that h is algebraic over F .]

4. *[compute the degree of the minimal polynomial].* Set u to be the least common denominator of all rational numbers n_{ki} in (20), set v to be the least common multiple of the orders of the K_j 's, and set t to be $\text{lcm}(u, v)$ and d to be $\frac{t}{u}$.

5. [compute the minimal polynomial]. Compute a rational solution g of the system

$$\{\sigma_j(z) = \text{l}\sigma_j(S_j)z, \quad j = \ell + 1, \dots, m\}.$$

Set $q_i = r_i - \text{l}\delta_i(g)$ for $i = 1, \dots, \ell$. Compute a rational solution p of the system

$$\{\delta_i(z) = uq_iz, \quad i = 1, \dots, \ell\}.$$

6. Return $(t, p^d g^t)$ [the minimal polynomial is $z^t - p^d g^t$].

The correctness of the algorithm follows from Proposition 6.4 and the proof of Lemma 5.4.

Remark 6.5 *Hyperexponential elements with the same certificates may differ by a multiplicative constant. Thus, the output $(t, p^d g^t)$ of the algorithm **IsAlgebraic** implies the following two assertions:*

1. *All hyperexponential elements with certificates $r_1, \dots, r_m$ are algebraic with degree t , and that*
2. *One of such elements has the minimal polynomial $z^t - p^d g^t$, while other elements have the minimal polynomial $z^t - cp^d g^t$ for some $c \in C$.*

Remark 6.6 *The rational solutions of the first system in step 5 may differ by a multiplicative element in $C(x_1, \dots, x_\ell)$. Thus, g and p in step 5 are not unique, whereas the product $p^d g^t$ is unique up to a multiplicative constant in C .*

Example 6.7 *Let $F = \mathbb{C}(x, y, n)$ and $\Delta = \{\delta_1, \delta_2, \sigma_3\}$, where $\delta_1 = \frac{\partial}{\partial x}$, $\delta_2 = \frac{\partial}{\partial y}$, and σ_3 sends n to $n + 1$. We apply the algorithm **IsAlgebraic** to determine whether there exists an algebraic-hyperexponential element whose respective certificates are*

$$r_1 = \frac{3x + 1}{2x(x + 1)}, \quad r_2 = \frac{n - 2y}{3y(n + y)}, \quad r_3 = -\frac{n + y}{n + 1 + y}.$$

In step 1, the algorithm asserts that r_1, r_2 and r_3 satisfy (10), (11) and (12). Hence, there exists an invertible hyperexponential element h in an orthogonal Δ -extension A over F . Moreover, $C_A = \mathbb{C}$. A typical example of such an extension is the Picard-Vessiot extension defined by the fully integrable system $\{\delta_1(z) = r_1 z, \delta_2(z) = r_2 z, \sigma_3(z) = r_3 z\}$.

In step 2, the algorithm decomposes the certificate r_3 into

$$r_3 = -1 \cdot \frac{\sigma_3(S_3)}{S_3} \quad \text{where} \quad S_3 = \frac{1}{n + y}.$$

In step 3, the algorithm decomposes the certificates r_1 and r_2 into

$$r_1 = \frac{1}{2x} + \frac{\delta_1(S_1)}{S_1} \quad \text{where} \quad S_1 = x + 1,$$

$$r_2 = \frac{1}{3y} + \frac{\delta_2(S_2)}{S_2} \quad \text{where} \quad S_2 = \frac{1}{n + y}, \text{ respectively.}$$

It follows from Proposition 6.4 that h is algebraic over F . Furthermore, the minimal degree of the part corresponding to δ_1 and δ_2 is 6, which is u in step 4, and the minimal degree of the part corresponding to σ_3 is 2, which is v in step 4. So the degree of the minimal polynomial of h is 6.

In step 5, the algorithm computes the rational part of h , which is

$$g = \frac{1}{n+y},$$

and then the part corresponding to δ_1 and δ_2 , which is

$$p = (x+1)^6 x^3 y^2.$$

Hence, the minimal polynomial of h is $z^6 - pg^6$. Moreover, Corollary 5.5 implies

$$h = c g p^{\frac{1}{6}} (-1)^n = c \left(\frac{x+1}{n+y} \right) x^{\frac{1}{2}} y^{\frac{1}{3}} (-1)^n \quad \text{for some } c \in \mathbb{C}^*.$$

Example 6.8 Let $F = \mathbb{C}(x, y, n, m)$ and $\Delta = \{\delta_1, \delta_2, \sigma_3, \sigma_4\}$, where $\delta_1 = \frac{\partial}{\partial x}$, $\delta_2 = \frac{\partial}{\partial y}$, σ_3 sends n to $n+1$, and σ_4 sends m to $m+1$. We apply the algorithm **IsAlgebraic** to determine whether there exists an algebraic-hyperexponential element whose respective certificates are

$$\begin{aligned} r_1 &= \frac{(24x^2n^2y^2 + 8m^3x^2 + 3x^2nm^2 + 3ym^3x + 15xn^2y^3 - y^4mn)y}{4x(xm^2 + y^3n)(3xn - ym)(2x + y)}, \\ r_2 &= \frac{9y^4mn - 8m^3x^2 - 72x^2n^2y^2 - 3x^2nm^2 + 16xy^3mn - 3ym^3x - 39xn^2y^3}{4(xm^2 + y^3n)(3xn - ym)(2x + y)}, \\ r_3 &= \frac{(-1 + \sqrt{-3})(3xn + 3x - ym)(xm^2 + y^3n)}{2(xm^2 + y^3n + y^3)(3xn - ym)}, \\ r_4 &= -\frac{(3xn - ym - y)(xm^2 + y^3n)}{(xm^2 + 2xm + x + y^3n)(3xn - ym)}. \end{aligned}$$

In step 1, the algorithm asserts that $r_1, \dots, r_4$ satisfy (10), (11) and (12). So the desired hyperexponential element h exists in some simple orthogonal ring as in Example 6.7.

In step 2, the algorithm decomposes the certificates r_3 and r_4 into

$$\begin{aligned} r_3 &= \frac{-1 + \sqrt{-3}}{2} \cdot \frac{\sigma_3(S_3)}{S_3}, \quad \text{where } S_3 = \frac{y^3(3nx - ym)}{3x(ny^3 + xm^2)}, \\ r_4 &= -1 \cdot \frac{\sigma_4(S_4)}{S_4} \quad \text{where } S_4 = -\frac{x(3nx - ym)}{y(ny^3 + xm^2)}, \quad \text{respectively.} \end{aligned}$$

In step 3, the algorithm decomposes the certificates r_1 and r_2 into

$$\begin{aligned} r_1 &= \frac{y}{4x(2x + y)} + \frac{\delta_1(S_1)}{S_1} \quad \text{where } S_1 = \frac{m^2(3nx - ym)}{3n(ny^3 + xm^2)}, \\ r_2 &= \frac{-1}{4(2x + y)} + \frac{\delta_2(S_2)}{S_2} \quad \text{where } S_2 = -\frac{n(3xn - ym)}{m(m^2x + y^3n)}, \quad \text{respectively.} \end{aligned}$$

It follows from Proposition 6.4 that h is algebraic over F . Furthermore, the minimal degree of the part corresponding to σ_3 and σ_4 is 6, which is v in step 4, the minimal degree of the part corresponding to δ_1 and δ_2 is 4, which is u in step 4,. So the degree of the minimal polynomial of h is 12.

In step 5, the algorithm computes the rational part of h , which is

$$g = \frac{3xn - my}{3(m^2x + ny^3)},$$

and then the part corresponding to δ_1 and δ_2 , which is

$$p = \frac{2x}{2x + y}.$$

Hence the minimal polynomial of h is $z^{12} - p^3 g^{12}$. Moreover, Corollary 5.5 implies

$$h = c g p^{\frac{1}{4}} (-1)^m \left(\frac{-1 + \sqrt{-3}}{2} \right)^n \quad \text{for some } c \in \mathbb{C}^*.$$

Acknowledgement

We thank Dr. R. Feng for his valuable suggestions on the proof of Proposition 4.4, and thank Dr. M. Wu for her helpful comments and corrections on an early version of this paper.

References

- [1] S.A. Abramov and M. Petkovšek. Rational normal forms and minimal decompositions of hypergeometric terms. *J. Symb. Comput.*, 33:521–543, 2002.
- [2] S.A. Abramov, H. Le, and M. Petkovšek. Rational canonical forms and efficient representations of hypergeometric terms. *Proc. ISSAC 2003*, ACM Press, 7–14.
- [3] M. Bronstein, Z. Li and M. Wu. Picard-Vessiot extensions of linear functional systems. *Proc. ISSAC 2005*, ACM Press, 68–75.
- [4] K. Geddes, H. Le and Z. Li. Differential rational normal forms and a reduction algorithm for hyperexponential functions. *Proc. ISSAC 2004*, ACM Press, 183–190.
- [5] E. R. Kolchin. Algebraic matrix groups and the Picard-Vessiot theory of homogeneous linear ordinary differential equations. *Annal. Math.*, 49:1–42, 1948.
- [6] G. Labahn and Z. Li. Hyperexponential solutions of finite-rank ideals in orthogonal Ore rings. *Proc. ISSAC 2004*, ACM Press 213–220.
- [7] M. Petkovšek, H. Wilf and D. Zeilberger. *A = B*. AK Peters, 1996.
- [8] M. van der Put and M. Singer. *Galois Theory of Difference Equations*. Lecture Notes in Mathematics 1666, Springer, 1997.
- [9] M. van der Put and M. Singer. *Galois Theory of Linear Differential Equations*. Grundlehren der Mathematischen Wissenschaften 328, Springer, 2003.
- [10] C. Schneider. Product representations of $\sum \prod$ -fields. *Annals of Combinatorics*, 9:75–99, 2005.
- [11] M. Wu. *On Solutions of Linear Functional Systems and Factorizations of Modules over Laurent-Ore Algebras*. PhD Thesis, Chinese Academy of Sciences and Université de Nice, France, 2005.