

# Lazy Hermite Reduction and Creative Telescoping for Algebraic Functions\*

Shaoshi Chen<sup>a,b</sup>, Lixin Du<sup>a,b,c</sup>, Manuel Kauers<sup>c</sup>

<sup>a</sup>KLMM, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China

<sup>b</sup>School of Mathematical Sciences, University of Chinese Academy of Sciences, Beijing 100049, China

<sup>c</sup>Institute for Algebra, Johannes Kepler University, Linz, A4040, Austria

schen@amss.ac.cn, dulixin17@mails.ucas.ac.cn, manuel.kauers@jku.at

## ABSTRACT

Bronstein’s lazy Hermite reduction is a symbolic integration technique that reduces algebraic functions to integrands with only simple poles without the prior computation of an integral basis. We sharpen the lazy Hermite reduction by combining it with the polynomial reduction to solve the decomposition problem of algebraic functions. The sharpened reduction is then used to design a reduction-based telescoping algorithm for algebraic functions in two variables.

## CCS CONCEPTS

• **Computing methodologies** → **Algebraic algorithms.**

## KEYWORDS

Symbolic integration; integral bases; polynomial reduction

## ACM Reference Format:

Shaoshi Chen<sup>a,b</sup>, Lixin Du<sup>a,b,c</sup>, Manuel Kauers<sup>c</sup>. 2021. Lazy Hermite Reduction and Creative Telescoping for Algebraic Functions. In *Proceedings of the 2021 International Symposium on Symbolic and Algebraic Computation (ISSAC ’21), July 18–23, 2021, Virtual Event, Russian Federation*. ACM, New York, NY, USA, 8 pages. <https://doi.org/10.1145/3452143.3465528>

## 1 INTRODUCTION

The integration problem for algebraic functions has a long history that can be traced back at least to the work of Euler and others on elliptic integrals [4]. In 1826, Abel initiated the study of general integrals of algebraic functions, which are now called abelian integrals [2]. Liouville in 1833 proved that if the integral of an algebraic function is an elementary function, then it must be the sum of an algebraic function and a linear combination of logarithms of algebraic functions (see [31, Chapter IX] for a detailed historical overview).

\*S. Chen was partially supported by the NSFC grants 11871067, 11688101, the Fund of the Youth Innovation Promotion Association, CAS, and the National Key Research and Development Project 2020YFA0712300. L. Du was supported by the NSFC grant 11871067 and the Austrian FWF grant P31571-N32. M. Kauers was supported by the Austrian FWF grant P31571-N32.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from [permissions@acm.org](mailto:permissions@acm.org).  
ISSAC ’21, July 18–23, 2021, Virtual Event, Russian Federation

© 2021 Copyright held by the owner/author(s). Publication rights licensed to ACM.  
ACM ISBN 978-1-4503-8382-0/21/07...\$15.00  
<https://doi.org/10.1145/3452143.3465528>

In 1948, Ritt presented an algebraic approach to the problem of integration in finite terms in his book [36]. Based on Liouville’s theorem and some developments in differential algebra [37], Risch in 1970 finally solved this classical problem by giving a complete algorithm [35]. After Risch’s work, more efficient algorithms have been given due to the emerging developments in symbolic computation [12, 15, 22, 39]. Passing from indefinite integration to definite integration with parameters, the central problem shifts to finding linear differential equations satisfied by the integrals of algebraic functions with parameters. In this direction, the first work was started by Picard in [34] and later a systematical method was developed by Manin in his work on proving the function-field analogue of Mordell’s conjecture [32]. In the 1990s, another powerful method was developed by Almkvist and Zeilberger [5] by including the trick of differentiating under the integral sign in the framework of creative telescoping [43].

In a given differential ring  $R$  with the derivation  $D$ , one can ask two fundamental problems: one is the *integrability problem*, i.e., deciding whether a given element  $f \in R$  is of the form  $D(g)$  for some  $g \in R$ , if such a  $g$  exists, we say that  $f$  is *integrable* in  $R$ ; another is the *decomposition problem*, i.e., decomposing a given element  $f \in R$  into the form  $D(g) + r$  with  $g, r \in R$  and  $r$  is minimal in a certain sense and  $r = 0$  if and only if  $f$  is integrable in  $R$ . For algebraic functions, the integrability problem was studied by Liouville [31]. Hermite reduction [24] solves the decomposition problem for rational functions. Trager in his thesis [39] extended Hermite reduction to the algebraic case. His algorithm requires the computation of an integral basis in the beginning. In order to avoid this expensive step, Bronstein [13] introduced the lazy Hermite reduction that partially solves the decomposition problem. The first contribution in this paper is a sharpened version of the lazy Hermite reduction. We combine the lazy Hermite reduction with a further reduction, namely the polynomial reduction [8, 17, 19], in order to solve the decomposition problem completely.

When a differential ring  $R$  is equipped with two derivations  $D_1, D_2$ , one can also consider the *creative telescoping* problem: for a given element  $f \in R$ , decide whether there exist  $c_0, \dots, c_r \in R$ , not all zero, such that  $D_2(c_i) = 0$  for all  $i \in \{0, \dots, r\}$  and

$$c_r D_1^r(f) + \dots + c_0 f = D_2(g) \quad \text{for some } g \in R.$$

The operator  $L = c_r D_1^r + \dots + c_0$  if exists is called a *telescoper* for  $f$ . For every algebraic function there exists such a telescoper, and many construction algorithms have been developed in [11, 17, 18, 32, 42]. Our second contribution is an adaption of the reduction-based approach from [17] using the sharpened lazy Hermite reduction.

The remainder of this paper is organized as follows. First we recall Bronstein's idea of lazy Hermite reduction in Section 2. Instead of an integral basis, it uses a so-called "suitable basis" of the function field. In Section 3 we have a closer look at these bases. After developing the polynomial reduction in Section 4, we present the telescoping algorithm for algebraic functions based on the sharpened lazy Hermite reduction in Section 5. We conclude our paper by some experimental comparisons among several telescoping algorithms in Section 6.

## 2 LAZY HERMITE REDUCTION

Trager's generalization of Hermite reduction to algebraic functions works as follows [14, 17, 23, 39]. Let  $K$  be a field of characteristic zero and  $m \in K(x)[y]$  be an irreducible polynomial over  $K(x)$ . Then  $A = K(x)[y]/\langle m \rangle$  is an algebraic extension of  $K(x)$ . Its elements are called *algebraic functions*. When there is no ambiguity, we also use  $y$  to represent the element  $y + \langle m \rangle$  in  $A$ , which can be viewed as a root of  $m$ . An element  $f \in A$  is called *integral* over  $K[x]$  if the minimal polynomial of  $f$  in  $K[x, y]$  is monic with respect to  $y$ . If  $n = \deg_y(m)$ , then  $A$  is a finite extension of degree  $n$  over  $K(x)$  and the set of all integral elements in  $A$  is a free  $K[x]$ -module of rank  $n$ . A basis for this module is called an *integral basis* of  $A$ . Such bases exist, and several algorithms dedicate to computing them [6, 38, 39, 41]. Let  $W = (\omega_1, \dots, \omega_n)$  be an integral basis of  $A$ . Let  $f = \frac{1}{uv^d} \sum_{k=1}^n a_k \omega_k \in A$  with  $d > 1$  and  $u, v, a_1, \dots, a_n \in K[x]$  such that  $\gcd(u, v) = \gcd(v, v') = \gcd(v, a_1, \dots, a_n) = 1$ . We seek  $b_1, \dots, b_n, c_1, \dots, c_n \in K[x]$  such that  $f = g' + h$  for  $g = \frac{1}{v^{d-1}} \sum_{k=1}^n b_k \omega_k$  and  $h = \frac{1}{uv^{d-1}} \sum_{k=1}^n c_k \omega_k$ . The  $g$  in this decomposition can be found by solving a certain linear system over  $K[x]/\langle v \rangle$ , and once  $g$  is known,  $h$  can be computed as  $h = f - g'$ . Let  $e \in K[x]$  and  $M \in K[x]^{n \times n}$  be such that  $eW' = MW$ , and assume (without loss of generality) that  $e \mid uv$ . Then the coefficient vector  $b = (b_1, \dots, b_n)$  of  $v^{d-1}g$  satisfies

$$b(uve^{-1}M - (d-1)uv'I_n) \equiv (a_1, \dots, a_n) \pmod{v}, \quad (1)$$

where  $I_n$  is the identity matrix in  $K[x]^{n \times n}$ . Using that  $W$  is an integral basis, it can be shown that this linear system has a unique solution, see [17, 39] for further details. Applying the process repeatedly, we can eliminate all multiple poles from the integrand, i.e., we can find  $g$  and  $h$  such that  $f = g' + h$  and  $h = q^{-1} \sum_{k=1}^n p_k \omega_k$  for some polynomials  $p_1, \dots, p_n, q$  with  $q$  squarefree.

If  $W$  is not an integral basis, the linear system (1) may or may not have a unique solution.

EXAMPLE 1. Let  $m = y^2 - x$  and  $f = \frac{y}{(x+1)x^2}$ .

(1) For  $W = (x, xy)$  we have  $e = 2x$  and  $M = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$ . Applying

the reduction to  $f = \frac{1}{(x+1)x^3}xy$  leads to the linear system

$$b \underbrace{\begin{pmatrix} (x+1)x(2x)^{-1} & \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} & -(3-1)(x+1) & 1 & \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ \underbrace{\phantom{(x+1)x(2x)^{-1}}}_{=u} & \underbrace{\phantom{\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}}}_{=M} & \underbrace{\phantom{-(3-1)(x+1)}}_{=d} & \underbrace{\phantom{1}}_{=u} & \underbrace{\phantom{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}}}_{=I_2} \end{pmatrix}}_{\equiv (0, 1) \pmod{x}} \equiv (0, 1) \pmod{x}$$

$$= \begin{pmatrix} -(x+1) & 0 \\ 0 & -\frac{1}{2}(x+1) \end{pmatrix}$$

which has a unique solution.

(2) For  $W = (x, y)$  we have  $e = 2x$  and  $M = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ . Applying the reduction to  $f = \frac{1}{x^2(x+1)}y$  leads to the linear system

$$b \begin{pmatrix} 0 & 0 \\ 0 & -(x+1) \end{pmatrix} \equiv (0, 2) \pmod{x},$$

which is solvable, but not uniquely.

(3) For  $W = (x, (x+1)y)$  we have  $e = 2x(x+1)$  and  $M = \begin{pmatrix} 2(x+1) & 0 \\ 0 & 3x+1 \end{pmatrix}$ . Applying the reduction to

$$f = \frac{1}{x^2(x+1)^2}(x+1)y$$

leads to the linear system

$$b \begin{pmatrix} -2x & 0 \\ 0 & -(x+1) \end{pmatrix} \equiv (0, 2) \pmod{x(x+1)}$$

which has no solutions.

Note that none of the bases in the example above is an integral basis because 1 is an integral element of  $A$  but does not belong to the  $K[x]$ -module generated by any one of the bases. However, all the bases consist of integral elements and have the property that  $e$  is squarefree. Bronstein [13] calls such a basis a *suitable basis* and observes that whenever we apply Hermite reduction to a suitable basis and find that the linear system (1) has no solution, then we can construct from any unsolvable system an integral element of  $A$  that does not belong to the  $K[x]$ -module generated by the elements of  $W$ . We can then replace  $W$  by a suitable basis of an enlarged  $K[x]$ -module and proceed with the reduction.

EXAMPLE 2. We continue the previous example.

- (1) For  $W = (x, xy)$ , no basis update is needed because the linear system has a unique solution.
- (2) For  $W = (x, y)$ , the right kernel element  $(1, 0)$  of the matrix in the linear system translates into the new integral element  $x+1$ , which does not belong to the  $K[x]$  module generated by  $x$  and  $y$  in  $A$ . A basis of the module generated by  $x, y$ , and  $x+1$  is  $(1, y)$ .
- (3) For  $W = (x, (x+1)y)$ , from the lack of solutions of the linear system it can be deduced that  $xy$  is an integral element not belonging to the module generated by  $x$  and  $(x+1)y$  in  $A$ . A basis of the module generated by  $x, (x+1)y$ , and  $xy$  is  $(x, y)$ .

Starting from a basis  $W$  consisting of integral elements, there can be at most finitely many basis updates before we reach an integral basis. Therefore, it takes at most finitely many basis updates (and possibly fewer than needed for reaching an integral basis) to complete the reduction process. This variant of Hermite reduction, which avoids the potentially expensive computation of an integral basis at the beginning, is called *lazy Hermite reduction*. Its final result is a suitable basis  $\tilde{W}$  of  $A$  and  $g, h \in A$  such that  $f = g' + h$  and the coefficients of  $h$  with respect to  $\tilde{W}$  are rational functions with a squarefree common denominator. In the examples above, we may find  $\tilde{W} = (1, y)$ ,  $g = -\frac{2y}{x}$ , and  $h = -\frac{y}{x(x+1)}$ .

One of the key features of Hermite reduction is that we can decide the integrability problem. For example, if we write a rational function  $f \in K(x)$  in the form  $f = g' + h$  for some  $g, h \in K(x)$  where  $h$  has a squarefree denominator and numerator degree less than

denominator degree, then  $f$  admits an integral in  $K(x)$  if and only if  $h = 0$ . Trager generalizes this criterion to algebraic functions as follows. By a change of variables, he first ensures that the integrand  $f$  has a double root at infinity. Then he performs Hermite reduction with respect to an integral basis that is normal at infinity. If this gives  $g, h$  such that  $f = g' + h$ , then  $f$  is integrable in  $A$  if and only if  $h = 0$  [17, 39].

Unfortunately, this criterion does not extend to the lazy version of Hermite reduction. Even if we produce a double root of the integrand at infinity and make the suitable basis normal at infinity (which amounts to a local integral basis computation that we actually would prefer to avoid altogether), a nonzero remainder  $h$  does not imply that  $f$  is not integrable.

EXAMPLE 3. Let  $m = y^2 - x$  and  $f = \frac{y}{x^3}$ . For  $W = (1, (x^2 + 1)y)$  we have  $e = 2x(x^2 + 1)$  and  $M = \begin{pmatrix} 0 & 0 \\ 0 & 5x^2 + 1 \end{pmatrix}$ . The lazy Hermite reduction finds  $g = -\frac{2(1+x^2)y}{3x^2}$  and  $h = \frac{y}{3x}$ . Here  $f = \left(-\frac{2y}{3x^2}\right)'$  is integrable and has a root of order  $\geq 2$  at infinity, but  $h$  is nonzero.

Somewhat surprisingly, Bronstein does not address this issue in his report [13]. He just guarantees that  $h$  has only simple roots and makes no further claims about it. In the following sections, we extend his idea to a complete integrability test.

### 3 SUITABLE BASES

Let  $A = K(x)[y]/\langle m \rangle$  with  $m \in K[x, y]$  being an irreducible polynomial over  $K(x)$ . Let  $\bar{K}$  be the algebraic closure of  $K$ . If  $n = \deg_y(m)$ , there are  $n$  distinct solutions in the field

$$\bar{K}\langle\langle x - a \rangle\rangle := \bigcup_{r \in \mathbb{N} \setminus \{0\}} \bar{K}((x - a)^{1/r})$$

of formal Puiseux series at  $a \in \bar{K}$ . There are also  $n$  distinct solutions in the field

$$\bar{K}\langle\langle x^{-1} \rangle\rangle := \bigcup_{r \in \mathbb{N} \setminus \{0\}} \bar{K}((x^{-1})^{1/r})$$

of formal Puiseux series at  $\infty$ . For a fixed  $a \in \bar{K} \cup \{\infty\}$ , let  $y_1, \dots, y_n$  be all  $n$  roots of  $m$  in  $\bar{K}\langle\langle x - a \rangle\rangle$  (or  $\bar{K}\langle\langle x^{-1} \rangle\rangle$  if  $a = \infty$ ). There are  $n$  distinct  $K(x)$ -embeddings  $\sigma_1, \dots, \sigma_n$  of  $A$  into  $\bar{K}\langle\langle x - a \rangle\rangle$  (or  $\bar{K}\langle\langle x^{-1} \rangle\rangle$  if  $a = \infty$ ) such that  $\sigma_i(f(y)) = f(y_i)$  for any  $f \in A$ . Then for each  $a \in \bar{K} \cup \{\infty\}$ , we can associate  $f \in A$  with  $n$  series  $\sigma_i(f)$  for  $i = 1, \dots, n$ . Moreover, if we equip the fields  $A, \bar{K}\langle\langle x - a \rangle\rangle$  and  $\bar{K}\langle\langle x^{-1} \rangle\rangle$  with natural differentiations with respect to  $x$ , then each embedding  $\sigma_i$  is a differential homomorphism, i.e.,  $\sigma_i(f') = \sigma_i(f)'$  for any  $f \in A$ .

A nonzero Puiseux series at  $a \in \bar{K}$  can be written as

$$P = \sum_{i \geq 0} c_i(x - a)^{r_i},$$

where  $c_i \in \bar{K}, c_0 \neq 0$  and  $r_i \in \mathbb{Q}$  with  $r_0 < r_1 < \dots$ . The valuation map  $v_a$  on  $\bar{K}\langle\langle x - a \rangle\rangle$  is defined by  $v_a(P) = r_0$  if  $P$  is nonzero and  $v_a(0) = \infty$ . Replacing  $x - a$  by  $\frac{1}{x}$ , we get the valuation map  $v_\infty$  on  $\bar{K}\langle\langle x^{-1} \rangle\rangle$ . A series  $P$  in  $\bar{K}\langle\langle x - a \rangle\rangle$  or  $\bar{K}\langle\langle x^{-1} \rangle\rangle$  is called *integral* if its valuation is nonnegative. The value function  $\text{val}_a : A \rightarrow \mathbb{Q} \cup \{\infty\}$  is defined by

$$\text{val}_a(f) := \min_{i=1}^n v_a(\sigma_i(f))$$

for any  $f \in A$ . An element  $f \in A$  is called (*locally*) *integral* at  $a \in \bar{K} \cup \{\infty\}$  if  $\text{val}_a(f) \geq 0$ , i.e., every series associated to  $f$  (at  $a$ ) is integral. An element  $f \in A$  is called (*globally*) *integral* if  $\text{val}_a(f) \geq 0$  for all  $a \in \bar{K}$ , i.e.,  $f$  is locally integral at every  $a \in \bar{K}$  ("at all finite places"). This definition of integrality is equivalent to that in Section 2. The elements of  $A$  that are locally integral at some point  $a \in \bar{K}$  form a  $K(x)_a$  module, where  $K(x)_a$  is the subring of  $K(x)$  consisting of all rational functions which do not have a pole at  $a$ . In the case  $a = \infty$ ,  $K(x)_a$  is the ring of all rational functions  $p/q$  with  $\deg_x(p) \leq \deg_x(q)$ . A basis of the  $K(x)_a$ -module of locally integral elements of  $A$  is called a *local integral basis* at  $a$ .

For a series  $P \in \bar{K}\langle\langle x - a \rangle\rangle$ , the smallest positive integer  $r$  such that  $P \in \bar{K}((x - a)^{1/r})$  is called the *ramification index* of  $P$ . If  $r > 1$ , the series  $P$  is said to be *ramified*. For an element  $f \in A$ , a point  $a \in \bar{K}$  is called a *branch point* of  $f$  if one of the series associated to  $f$  at  $a$  is ramified.

Let  $W = (\omega_1, \dots, \omega_n)$  be a  $K(x)$ -vector space basis of  $A$ . Throughout this section, let  $e \in K[x]$  and  $M = ((m_{i,j}))_{i,j=1}^n \in K[x]^{n \times n}$  be such that  $eW' = MW$  and  $\gcd(e, m_{1,1}, m_{1,2}, \dots, m_{n,n}) = 1$ . As already mentioned,  $W$  is called a *suitable basis* if  $e$  is squarefree and  $\omega_i$ 's are integral for each  $i$ . Every integral basis is suitable, see [17, Lemma 3]. Now we explore further properties of such bases.

LEMMA 4. Let  $W$  be an integral basis of  $A$ . Let  $e \in K[x]$  and  $M \in K[x]^{n \times n}$  be such that  $eW' = MW$ . If  $a \in \bar{K}$  is a root of  $e$ , there exists  $\omega \in W$  such that  $a$  is a branch point of  $\omega$ .

PROOF. Let  $W = (\omega_1, \dots, \omega_n)$  and  $M = ((m_{i,j}))_{i,j=1}^n \in K[x]^{n \times n}$ , and let  $a$  be a root of  $e$ . By  $\gcd(e, m_{1,1}, m_{1,2}, \dots, m_{n,n}) = 1$ , there exists an index  $i \in \{1, \dots, n\}$  such that

$$\omega_i' = \frac{1}{e} \sum_{j=1}^n m_{i,j} \omega_j,$$

where  $a$  is not a common root of  $m_{i,1}, \dots, m_{i,n}$ . From the above expression of  $\omega_i'$ , we get that  $\omega_i'$  does not belong to the module generated by  $W$  over  $K[x]$ . Since  $W$  is a local integral basis at  $a$ , it follows that  $\omega_i$  is not locally integral at  $a$ . Thus  $\text{val}_a(\omega_i') < 0$ .

We claim that  $a$  is a branch point of  $\omega_i$ . Otherwise all Puiseux series associated to  $\omega_i$  at  $a$  are power series. So all Puiseux series associated to its derivative  $\omega_i'$  at  $a$  are also power series, which implies  $\text{val}_a(\omega_i') \geq 0$ . This leads to a contradiction. ■

In order to give a converse of Lemma 4, we consider the series associated to an algebraic function. For a ramified Puiseux series  $P = \sum_{i \geq 0} c_i(x - a)^{r_i} \in \bar{K}\langle\langle x - a \rangle\rangle$ , let

$$\delta(P) := \min\{r_i \mid r_i \in \mathbb{Q} \setminus \mathbb{Z}, i \geq 0\}$$

be the minimal fractional exponent of  $P$ . Define  $\delta(P) = \infty$  if the series  $P$  is not ramified. Then  $\delta(P') = \delta(P) - 1$ . Similar as the valuation of a series, the function  $\delta$  satisfies  $\delta(P + Q) \geq \min\{\delta(P), \delta(Q)\}$  for any  $P, Q \in \bar{K}\langle\langle x - a \rangle\rangle$ .

LEMMA 5. Let  $W$  be a  $K(x)$ -vector space basis of  $A$ . Let  $e \in K[x]$  and  $M \in K[x]^{n \times n}$  be such that  $eW' = MW$ . Let  $a \in \bar{K}$ . If there exists some  $\omega \in W$  such that  $a$  is a branch point of  $\omega$ , then  $a$  is a root of  $e$ .

PROOF. Suppose that  $a$  is a branch point of some  $\omega \in W$ . It implies that for such an element  $\omega$ , there is a  $K(x)$ -embedding  $\sigma$  of  $A$  into the field of Puiseux series (at  $a$ ) such that the series

$\sigma(\omega)$  is ramified. Let  $r = \min\{\delta(\sigma(\omega)) \mid \omega \in W\}$ . Then  $r \in \mathbb{Q} \setminus \mathbb{Z}$ . Choose an element  $\omega_i \in W$  such that  $\delta(\sigma(\omega_i)) = r$ . Then  $\sigma(\omega_i)$  must be ramified. After differentiating the series  $\sigma(\omega_i)$ , its minimal fractional exponent decreases strictly by 1. This means

$$\delta(\sigma(\omega_i)') = \delta(\sigma(\omega_i)) - 1 = r - 1.$$

Let  $M = ((m_{i,j}))_{i,j=1}^n \in K[x]^{n \times n}$ . Since  $\sigma$  is a differential homomorphism and a  $K(x)$ -embedding, we have

$$\sigma(\omega_i)' = \sigma(\omega_i') = \frac{1}{e} \sum_{j=1}^n m_{i,j} \sigma(\omega_j).$$

After multiplying by a polynomial, the minimal fractional exponent of a series will not decrease. So if  $a$  is not a root of  $e$ , then

$$\delta(\sigma(\omega_i)') \geq \min_{j=1}^n \delta(m_{i,j} \sigma(\omega_j)) \geq \min_{j=1}^n \delta(\sigma(\omega_j)) = r.$$

This leads to a contradiction. Thus  $a$  must be a root of  $e$ . ■

We now show that the polynomial  $e$  does not depend on the choice of the basis of  $A$  but only on the  $K[x]$ -submodule it generates. Let  $U$  and  $V$  be two  $K(x)$ -vector space bases of  $A$ . Let  $e_u, e_v \in K[x]$  and  $M_u, M_v \in K[x]^{n \times n}$  be such that  $e_u U' = M_u U$  and  $e_v V' = M_v V$ . Suppose that  $U$  and  $V$  generate the same submodule of  $A$  over  $K[x]$ . Then there exists a matrix  $T \in K[x]^{n \times n}$  such that  $U = TV$  and  $T$  is an invertible matrix over  $K[x]$ . Taking derivatives, we get

$$U' = \left( T' T^{-1} + T \frac{1}{e_v} M_v T^{-1} \right) U = \frac{1}{e_u} M_u U.$$

Since  $T, T^{-1} \in K[x]^{n \times n}$ , we have  $e_u$  divides  $e_v$ . Similarly the fact that  $V = RU$  with  $R = T^{-1} \in K[x]^{n \times n}$  implies that  $e_v$  divides  $e_u$ . Thus  $e_u = e_v$  when  $e_u, e_v$  are monic.

**LEMMA 6.** *Let  $W$  be a suitable basis and  $U$  be an integral basis of  $A$ . Let  $W = TU$  with  $T \in K[x]^{n \times n}$ . Let  $e \in K[x]$  and  $M \in K[x]^{n \times n}$  be such that  $eW' = MW$ . If  $a \in \bar{K}$  is a root of  $\det(T)$ , then  $x - a \mid e$ . So if  $W$  is not a local integral basis at  $a \in \bar{K}$ , then  $a$  is a root of  $e$ .*

**PROOF.** First we shall make a change of bases. Consider the Smith normal form of the matrix  $T$ . This means there are two matrices  $P, Q \in K[x]^{n \times n}$  such that both  $P$  and  $Q$  are invertible over  $K[x]$  and  $PTQ = \Lambda$  for some diagonal matrix  $\Lambda \in K[x]^{n \times n}$ . Then  $W = P^{-1} \Lambda Q^{-1} U$  and hence  $PW = \Lambda(Q^{-1} U)$ . Replacing  $PW$  and  $Q^{-1} U$  by  $W$  and  $U$ , respectively, we may assume  $W = TU$  with  $T = \text{diag}(r_1, \dots, r_n) \in K[x]^{n \times n}$ . This operation does not change the module generated by  $W$  or  $U$ , respectively. Note that  $\det(PTQ)$  and  $\det(T)$  are equal up to a unit in  $K$ . It suffices to prove the result for such special bases  $W$  and  $U$ .

Let  $e_u \in K[x]$  and  $M_u = ((a_{i,j}))_{i,j=1}^n \in K[x]^{n \times n}$  be such that  $e_u U' = M_u U$ . Differentiating both sides of  $W = TU$  yields that

$$W' = \left( T' T^{-1} + T \frac{1}{e_u} M_u T^{-1} \right) W = \frac{1}{e} MW. \quad (2)$$

Substituting  $T = \text{diag}(r_1, \dots, r_n)$  and  $M_u = ((a_{i,j}))_{i,j=1}^n$  into (2), we get the the  $i$ -th diagonal entry of  $\frac{1}{e} M$  is  $\frac{r_i'}{r_i} + \frac{a_{i,i}}{e_u}$ .

Let  $a \in \bar{K}$  be a root of  $\det(T)$ . Since  $\det(T) = r_1 r_2 \cdots r_n$ , there is an  $i \in \{1, 2, \dots, n\}$  such that  $a$  is a root of  $r_i$ . If  $a$  is not a root of  $e_u$ , then  $a$  must be a pole of the entry  $\frac{r_i'}{r_i} + \frac{a_{i,i}}{e_u}$ . Since  $e$  is a common multiple of the denominator of all the entries of  $\frac{1}{e} M$ , we have  $a$

is a root of  $e$ . Now suppose that  $a$  is a root of  $e_u$ . Since  $U$  is an integral basis, Lemma 4 implies that there is  $u \in U$  such that  $a$  is a branch point of  $u$ . Then one of the series associated to  $u$  is ramified. In other words, such a series has at least one fractional exponent. Since  $W = TU$  for some invertible matrix  $T$  in  $K(x)^{n \times n}$ , there is  $\omega \in W$  such that one of the series associated to  $\omega$  is also ramified. Therefore,  $a$  is a branch point of  $\omega$ . By Lemma 5,  $a$  is root of  $e$ . ■

Since the inverse of the matrix  $T$  is  $T^{-1} = \frac{1}{\det(T)} T^*$ , where  $T^*$  is the adjoint matrix of  $T$ , the least common multiple of the denominator of the entries of  $T^{-1}$  divides  $\det(T)$ . By investigating Equation (2), we see a possible root of  $e$  must come from  $\det(T)$  and  $e_u$ . Combining this with the last paragraph in the argument of Lemma 6, we get those roots of  $\det(T)$  and  $e_u$  are exactly roots of  $e$ . In particular, when  $W$  is a suitable basis, the corresponding polynomial  $e$  is the squarefree part of the product  $\det(T)e_u$ . Therefore, if  $W_1, W_2$  are two suitable bases and the  $K[x]$ -submodule generated by  $W_1$  is larger than that generated by  $W_2$ , then  $e_1$  divides  $e_2$ , where  $e_i \in K[x]$  such that  $e_i W_i' = M_i W_i$  with  $M_i \in K[x]^{n \times n}$  for  $i = 1, 2$ .

**EXAMPLE 7.** *Let  $A = K(x)[y]/\langle y^2 - x \rangle$ . For an integral basis  $U = (1, y)$ , we have  $e_u = 2x$  and  $M_u = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ . A branch point of  $y$  is  $a = 0$ , which is a root of  $e_u$ . For a suitable basis  $W = TU$  with  $T = \begin{pmatrix} 1 & 0 \\ 0 & x+1 \end{pmatrix}$ , we have  $e = 2x(x+1)$  and  $M = \begin{pmatrix} 0 & 0 \\ 0 & 3x+1 \end{pmatrix}$ . Here  $e = \det(T)e_u$ .*

## 4 POLYNOMIAL REDUCTION

Polynomial reduction is a postprocessing step for Hermite reduction which was first introduced for hyperexponential terms [8] and has later been formulated for algebraic and Fuchsian D-finite functions [17, 19]. For the latter cases, like for Trager's criterion, integral bases that are normal at infinity are employed. Our goal in this section is to relax this requirement to suitable bases, so as to obtain a version of polynomial reduction which can serve as a natural continuation of the lazy Hermite reduction process and which provides the feature that the final remainder is zero if and only if the integrand is integrable.

Let  $h \in A$  be the remainder of lazy Hermite reduction (see Section 2) with respect to a suitable basis  $W = (\omega_1, \dots, \omega_n)$ . Then  $h$  can be written in the form

$$h = \sum_{i=1}^n \frac{h_i}{d e} \omega_i \quad (3)$$

with  $h_i, d \in K[x]$  such that  $\gcd(d, e) = \gcd(h_1, \dots, h_n, d) = 1$  and  $d$  is squarefree. If  $h$  is integrable in  $A$ , we shall prove that  $d$  is a constant in  $K$ . When  $W$  is an integral basis, this result was proved in [17, Lemma 9]. The following lemma is a local version.

**LEMMA 8.** *Let  $h \in A$  be in the form (3). If  $h$  is integrable in  $A$  and  $W$  is a local integral basis at  $a \in \bar{K}$ , then  $d$  has no root at  $a$ .*

**PROOF.** Suppose  $h$  is integrable in  $A$ . Then there exists  $H = \sum_{i=1}^n b_i \omega_i \in A$  with  $b_i \in K(x)$  such that  $h = H'$ . It suffices to show that every  $b_i$  has no pole at  $a$ . Otherwise  $H$  has a pole at  $a$ , because  $W$  is a local integral basis at  $a$ . Then  $h$  has at least a double pole at  $a$ . This contradicts the fact that  $d, e$  are squarefree. Thus  $d$  has no root at  $a$ . ■

**THEOREM 9.** Let  $h \in A$  be in the form (3). If  $h$  is integrable in  $A$ , then  $d$  is in  $K$ .

**PROOF.** Suppose that  $h$  is integrable in  $A$ . In order to show that  $d$  is a constant, we show that for any  $a \in \bar{K}$ ,  $a$  is not a root of  $d$ . If  $W$  is a local integral basis at  $a$ , then the conclusion follows from Lemma 8. Now we assume that  $W$  is not a local integral basis at  $a$ . By Lemma 6, we know that  $a$  is a root of  $e$ . Since  $\gcd(d, e) = 1$ , it follows that  $a$  is not a root of  $d$ . ■

To further reduce the lazy Hermite remainder, we derive a multiple of the denominator of any hypothetical integral of  $h$  in  $A$ . This multiple does not depend on the integrand  $h$ , but only on the discriminant of a suitable basis in its representation.

Recall that the *discriminant* of  $n$  elements  $U = (u_1, \dots, u_n)$  of  $A$  is defined by the determinant  $\text{Disc}(U) = \det((\text{Tr}(u_i u_j))_{i,j=1}^n)$ , where  $\text{Tr}$  is the trace map from  $A$  to  $K(x)$ . If the  $u_i$ 's are integral functions, then their traces are polynomials, and thus the discriminant is a polynomial. If  $W = TU$  where  $T$  is a matrix in  $K(x)^{n \times n}$ , then  $\text{Disc}(W) = \text{Disc}(U) \det(T)^2$ .

**LEMMA 10.** Let  $h \in A$  be in the form (3). Let  $U$  be an integral basis of  $A$  and let  $T \in K[x]^{n \times n}$  be such that  $W = TU$ . If  $h$  is integrable in  $A$ , i.e., there exist  $u \in K[x]$  and  $q = (q_1, \dots, q_n) \in K[x]^n$  such that

$$h = \left( \sum_{i=1}^n \frac{q_i}{u} \omega_i \right)'$$

and  $\gcd(q_1, \dots, q_n, u) = 1$ , then  $u$  divides  $\det(T)$ . Hence  $u^2$  divides  $\text{Disc}(W)/\text{Disc}(U)$ .

**PROOF.** Since  $h$  has a squarefree denominator with respect to  $W$  and  $W = TU$  with  $T \in K[x]^{n \times n}$ , it follows that  $h$  has a squarefree denominator with respect to  $U$ . This means  $h$  is also a remainder with respect to the integral basis  $U$ . Assume that  $h$  is integrable in  $A$ . Then Lemma 8 implies that  $h = (\sum_{i=1}^n a_i u_i)'$  with  $a_i \in K[x]$ . Write  $U = \frac{1}{r} RW$  with  $r \in K[x]$ ,  $R = ((b_{i,j}))_{i,j=1}^n \in K[x]^{n \times n}$  and  $\gcd(r, b_{1,1}, b_{1,2}, \dots, b_{n,n}) = 1$ . Then

$$\sum_{i=1}^n a_i u_i = \sum_{i=1}^n a_i \frac{1}{r} \sum_{j=1}^n b_{i,j} \omega_j = \sum_{j=1}^n \frac{1}{r} \left( \sum_{i=1}^n a_i b_{i,j} \right) \omega_j.$$

Thus  $u$  divides  $r$  because  $a_i, b_{i,j} \in K[x]$  and two antiderivatives of  $h$  only differ by a constant.

Since  $W = TU$ , we have  $\frac{1}{r} R = T^{-1} = \frac{1}{\det(T)} T^*$ . So  $r \mid \det(T)$  and hence  $u \mid \det(T)$ . Moreover,  $\text{Disc}(W) = \text{Disc}(U) \det(T)^2$ . Since  $u_i$ 's and  $\omega_i$ 's are integral elements, the discriminants  $\text{Disc}(W), \text{Disc}(U)$  are polynomials in  $K[x]$ . Therefore  $\det(T)^2$  divides the polynomial  $\text{Disc}(W)/\text{Disc}(U)$ , so does  $u^2$ . ■

If we already know that  $W$  is an integral basis, then the quotient  $\text{Disc}(W)/\text{Disc}(U)$  is a unit in  $K$ . By Lemma 10, we see  $u$  is a constant. If no integral basis is available, then from the condition  $u^2$  divides  $\text{Disc}(W)$ , a multiple of  $u$  can be chosen as the product over  $p^{[r/2]}$  where  $p$  runs through the irreducible factors of  $\text{Disc}(W)$  and  $r$  is the multiplicity of  $p$  in  $\text{Disc}(W)$ .

**EXAMPLE 11.** Let  $m = y^2 - x$  and  $h = \frac{y}{x}$ .

- (1) For  $W = (1, y)$ , we have  $\text{Disc}(U) = 4x$ . So we can choose  $u = 1$ . In fact,  $W$  is an integral basis and  $h = (2y)'$ .

- (2) For  $W = (1, (x^2 + 1)y)$ , we have  $\text{Disc}(W) = 4x(x^2 + 1)^2$ . So  $x^2 + 1$  is a multiple of  $u$ . In fact,  $h = (\frac{1}{x^2+1} 2(x^2 + 1)y)'$ .

If  $h$  is integrable in  $A$ , we shall reduce  $h$  to zero, otherwise we hope to remove all possible integrals whose denominators are factors of  $u$ . Before that we write  $h$  as two parts with denominators  $d$  and  $e$ , respectively. By the extended Euclidean algorithm, there are polynomials  $r_i, s_i \in K[x]$  such that  $h_i = r_i d + s_i e$  and  $\deg_x(r_i) < \deg_x(d)$ . Then the lazy Hermite remainder  $h$  decomposes as

$$h = \sum_{i=1}^n \frac{h_i}{de} \omega_i = \sum_{i=1}^n \frac{r_i}{d} \omega_i + \sum_{i=1}^n \frac{s_i}{e} \omega_i. \quad (4)$$

Our second goal is to confine the  $s_i$ 's to a finite-dimensional vector space over  $K$ , which generalizes the *polynomial reduction* in [17]. In this process, we shall rewrite the second term of  $h$  in (4) with respect to another basis. The new basis is used to perform the polynomial reduction and obtain the following additive decomposition.

**DEFINITION 12.** Let  $f$  be an element in  $A$ . Let  $W$  and  $V$  be two  $K(x)$ -vector space bases of  $A$ . Let  $e, a \in K[x]$  and  $M, B \in K[x]^{n \times n}$  be such that  $eW' = MW$  and  $aV' = BV$ . Suppose that  $f$  can be decomposed into

$$f = g' + \frac{1}{d} PW + \frac{1}{a} QV, \quad (5)$$

where  $g \in A$ ,  $d \in K[x]$  is squarefree and  $\gcd(d, e) = 1$ ,  $P, Q \in K[x]^n$  with  $\deg_x(P) < \deg_x(d)$  and  $Q \in N_V$ , which is a finite-dimensional  $K$ -vector space. The decomposition in (5) is called an additive decomposition of  $f$  with respect to  $x$  if it satisfies the condition that  $P, Q$  are zero if and only if  $f$  is integrable in  $A$ .

**EXAMPLE 13.** For  $f = \frac{y}{x^2(x+2)} \in A = K(x)[y]/(y^3 - x(x+1))$  and  $V = W = (1, y, y^2)^T$  an additive decomposition is

$$f = \underbrace{\left( \frac{-3y}{4x} \right)'}_{=g} + \underbrace{\frac{1}{x+2}}_{=1/d} \underbrace{(0, \frac{1}{4}, 0)}_{=P} W + \underbrace{\frac{1}{x(x+1)}}_{=1/a} \underbrace{(0, \frac{1}{8}, 0)}_{=Q} V.$$

The role of  $N_V$  will become clear shortly.

Given an algebraic function, its additive decomposition always exists for some integral basis  $W$  and some basis  $V$  which is a local integral basis at infinity, see [17, Theorem 14]. We shall show below that we can always find an additive decomposition with respect to certain suitable bases.

Let  $V$  be a  $K(x)$ -vector space basis of  $A$ , and let  $a \in K[x]$  and  $B = ((b_{i,j}))_{i,j=1}^n \in K[x]^{n \times n}$  be such that  $aV' = BV$ . We do not require that  $\gcd(a, b_{1,1}, b_{1,2}, \dots, b_{n,n}) = 1$ . Let  $u \in K[x]$  and  $p \in K[x]^n$ . A direct calculation yields that

$$\left( \frac{p}{u} V \right)' = \left( \frac{p}{u} \right)' V + \frac{p}{u} V' = \frac{aup' - au'p + upB}{u^2 a} V. \quad (6)$$

This motivates the following definition.

**DEFINITION 14.** For a given polynomial  $u \in K[x]$ , let the map  $\phi_V : K[x]^n \rightarrow u^{-2} K[x]^n$  be defined by

$$\phi_V(p) = \frac{1}{u^2} (aup' - au'p + upB)$$

for any  $p \in K[x]^n$ . We call  $\phi_V$  the map for polynomial reduction with respect to  $u$  and  $V$ , and call the subspace

$$\text{im}(\phi_V) = \{ \phi_V(p) \mid p \in K[x]^n \} \subseteq u^{-2} K[x]^n$$

the subspace for polynomial reduction with respect to  $u$  and  $V$ .

Note that, by construction, if  $q = \phi_V(p)$ , then  $\frac{q}{a}V = (\frac{p}{u}V)'$ . So  $\frac{q}{a}V$  is integrable.

We can view an element of  $K[x]^n$  (resp.  $K[x]^{n \times n}$ ) as a polynomial in  $x$  with coefficients in  $K^n$  (resp.  $K^{n \times n}$ ). Let  $\{e_1, \dots, e_n\}$  be the standard basis of  $K^n$ . Then the  $K[x]$ -module  $K[x]^n$  viewed as  $K$ -vector space is generated by

$$S := \{e_i x^j \mid 1 \leq i \leq n, j \in \mathbb{N}\}.$$

Assume  $e_1 > e_2 > \dots > e_n$ . The term over position monomial order on  $S$  is defined as  $e_{i_1} x^{j_1} > e_{i_2} x^{j_2}$  if and only if  $j_1 > j_2$  or  $j_1 = j_2$  and  $i_1 < i_2$ . Let  $\text{lt}(\cdot)$  denote the leading term of a vector (resp. matrix). For example, if  $p = 3(e_1 + e_2)x^2 + 10e_1x \in K[x]^2$ , then  $\text{lt}(p) = e_1x^2$  and  $\deg(p) = 2$  (which is the degree in  $x$ ).

DEFINITION 15. Let  $N_V$  be the  $K$ -subspace of  $K[x]^n$  generated by

$$\{t \in S \mid t \neq \text{lt}(p) \text{ for all } p \in \text{im}(\phi_V) \cap K[x]^n\}$$

Then  $K[x]^n = (\text{im}(\phi_V) \cap K[x]^n) \oplus N_V$ . We call  $N_V$  the standard complement of  $\text{im}(\phi_V)$  in  $K[x]^n$ . For any  $p \in K[x]^n$ , there exist  $p_1 \in K[x]^n$  and  $p_2 \in N_V$  such that

$$\frac{p}{a}V = \left(\frac{p_1}{u}V\right)' + \frac{p_2}{a}V.$$

This decomposition is called the polynomial reduction of  $p$  with respect to  $u$  and  $V$ .

If  $u = 1$ , then the polynomial reduction with respect to  $u$  falls back to the situation discussed in [17].

PROPOSITION 16. Let  $a \in K[x]$  and  $B \in K[x]^{n \times n}$  be such that  $aV' = BV$ , as before. If  $\deg_x(B) \leq \deg_x(a) - 1$ , then  $N_V$  is a finite dimensional  $K$ -vector space.

PROOF. Consider the map  $\tilde{\phi}_V : K[x]^n \rightarrow K[x]^n$  defined by

$$\tilde{\phi}_V(p) = aup' - au'p + upB$$

for any  $p \in K[x]^n$ . Then  $\tilde{\phi}_V(p) = u^2\phi_V(p)$ . It is easy to check that  $\text{im}(\phi_V) \cap K[x]^n$  and  $\text{im}(\tilde{\phi}_V) \cap u^2K[x]^n$  are isomorphic as  $K$ -vector spaces via the multiplication by  $u^2$ . Considering the codimension of subspaces in  $K[x]^n$  over  $K$ , we have the formula

$$\begin{aligned} \dim_K(N_V) &= \text{codim}_K(\text{im}(\phi_V) \cap K[x]^n) \\ &= \text{codim}_K(\text{im}(\tilde{\phi}_V) \cap u^2K[x]^n) \\ &\leq \text{codim}_K(\text{im}(\tilde{\phi}_V)) + \text{codim}_K(u^2K[x]^n). \end{aligned}$$

Let  $\mu := \deg_x(a) - 1$ ,  $\ell := \deg_x(u)$  and  $s := \deg_x(p)$ . Since  $\deg_x(aup') = \deg_x(au'p) = s + \ell + \mu$ , we have

$$\deg_x(\tilde{\phi}_V(p)) \leq s + \ell + \max\{\mu, \deg_x(B)\}.$$

By an argument analogous to [17, Proposition 12], we distinguish two cases  $\deg_x(B) < \mu$  and  $\deg_x(B) = \mu$ , and get the codimension of  $\text{im}(\tilde{\phi}_V)$  is finite. Since  $K[x]^n / (u^2K[x]^n) \cong (K[x] / u^2K[x])^n$ , the codimension of  $u^2K[x]^n$  is also finite. ■

The condition  $\deg_x(B) \leq \deg_x(a) - 1$  is satisfied if  $V$  is a local integral basis at infinity, but may not hold for an arbitrary basis. So we introduce a weaker basis that satisfies the degree condition. This is an analogue of suitable basis at infinity.

DEFINITION 17. A basis  $V$  of  $A$  is called suitable at infinity if for  $a \in K[x]$  and  $B \in K[x]^{n \times n}$  such that  $aV' = BV$  we have  $\deg_x(B) < \deg_x(a)$ .

There always exists a basis which is suitable at infinity. We can find such a basis as follows. Start from an arbitrary  $K(x)$ -basis  $V = (v_1, \dots, v_n)$  of the function field  $A$ . We can make its elements  $v_1, \dots, v_n$  integral at infinity by replacing each  $v_i$  by  $x^{-\tau}v_i$  for a sufficiently large  $\tau \in \mathbb{N}$ . Consider  $a \in K[x]$  and  $B \in K[x]^{n \times n}$  be such that  $aV' = BV$ . If  $\deg_x(B) < \deg_x(a)$ , we are done. If not, consider a row  $b$  in  $B$  with  $\deg_x(b) \geq \deg_x(a)$  and set  $v = xa^{-1}bV$ . Then  $v$  is integral at infinity (because at infinity differentiating increases the valuation) but it does not belong to the  $K(x)_\infty$ -module generated by  $V$  (because of  $\deg_x(b) \geq \deg_x(a)$ ). Therefore the  $K(x)_\infty$ -module generated by  $V$  and  $v$  is strictly larger than the  $K(x)_\infty$ -module generated by  $V$ . Replace  $V$  by a basis of this enlarged module, and update  $a$  and  $B$  such that  $aV' = BV$ . If we now have  $\deg_x(B) < \deg_x(a)$ , we are done, otherwise repeat the process just described.

The iteration will terminate because with every update of  $V$  the  $K(x)_\infty$ -module generated by it gets enlarged, and since all these modules are contained in the module of elements of  $A$  that are integral at infinity, after at most finitely many updates  $V$  will be a local integral basis at infinity. At least then, the desired degree condition must hold, because otherwise there would be an integral element which is not a  $K(x)_\infty$ -linear combination of the basis elements, in contradiction to the basis being integral at infinity.

THEOREM 18. Let  $f$  be an element in  $A$ . Let  $V$  be a basis of  $A$  which is suitable at infinity. Then there exists a suitable basis  $W$  of  $A$  such that  $f$  admits an additive decomposition in (5) with respect to the bases  $W$  and  $V$ .

PROOF. We present a constructive proof to show the existence of an additive decomposition of  $f$ . After performing the lazy Hermite reduction on  $f$ , we get

$$f = \tilde{g}' + \frac{1}{d}PW + \frac{1}{e}UW$$

where  $\tilde{g} \in A$ ,  $d, e \in K[x]$ ,  $W$  is a suitable basis,  $P = (r_1, \dots, r_n) \in K[x]^n$  and  $U = (s_1, \dots, s_n) \in K[x]^n$  with  $r_i, s_i$  introduced in (4). Let  $W = \frac{1}{b}CV$  for some  $b \in K[x]$  and  $C \in K[x]^{n \times n}$ . Let  $a \in K[x]$  and  $B \in K[x]^{n \times n}$  be such that  $aV' = BV$ . Multiplying  $a$  and  $B$  by some polynomial, we may assume that  $a$  is a common multiple of  $e$  and  $b$ . Rewriting the remainder in terms of the new basis  $V$ , we get

$$\frac{1}{e}UW = \frac{1}{eb}UCV = \frac{1}{a}\tilde{U}V, \quad (7)$$

for some  $\tilde{U} \in K[x]^n$ . By Lemma 10, if  $f$  is integrable, there exist  $\tilde{u} \in K[x]$  and  $R \in K[x]^n$  such that

$$\frac{1}{e}UW = \left(\frac{RW}{\tilde{u}}\right)' = \left(\frac{RCV}{u}\right)', \quad (8)$$

where  $u = \tilde{u}b$ . Next, we apply the polynomial reduction with respect to the polynomial  $u$  and decompose  $\tilde{U}$  into  $\phi_V(\tilde{U}_1) + \tilde{U}_2$  with  $\tilde{U}_1 \in K[x]^n$  and  $\tilde{U}_2 \in N_V$ . Then we have

$$\frac{1}{a}\tilde{U}V = \left(\frac{1}{u}\tilde{U}_1V\right)' + \frac{1}{a}\tilde{U}_2V. \quad (9)$$

Setting  $g = \tilde{g} + \frac{1}{u}\tilde{U}_1V$  and  $Q = \tilde{U}_2$ , we get the decomposition (5).

Assume that  $f$  is integrable. Then Theorem 9 implies  $d \in K$ . Since  $\deg_x(P) < \deg_x(d)$ , we have  $P = 0$ . Combining (9), (7) and (8) yields that

$$\frac{1}{a}QV = \frac{1}{a}\tilde{U}V - \left(\frac{1}{u}\tilde{U}_1V\right)' = \left(\frac{1}{u}\tilde{Q}V\right)', \quad (10)$$

where  $\tilde{Q} = RC - \tilde{U}_1$ . So  $Q = \phi_V(\tilde{Q}) \in \text{im}(\phi_V) \cap K[x]^n$ . Since  $\text{im}(\phi_V) \cap K[x] \cap N_V = \{0\}$ , it follows that  $Q = 0$ . ■

**EXAMPLE 19.** We continue with Example 3 by applying the polynomial reduction to the lazy Hermite remainder  $h = \frac{1}{3x(x^2+1)}(x^2+1)y$ . Since  $\text{Disc}(W) = 4x(x^2+1)^2$ , we choose  $u = x^2+1$ . Note that  $W$  is already a suitable basis at infinity. The map for the polynomial reduction with respect to  $W$  and  $u$  is  $\phi(p) = \frac{1}{u^2}(eup' - eu'p + epM)$  for any  $p \in K[x]^n$ . Then  $h = (\frac{1}{3(x^2+1)}2(x^2+1)y)'$  reduces to 0.

## 5 REDUCTION-BASED TELESCOPING

Lazy Hermite reduction combined with the polynomial reduction just described can be used for deciding whether a given algebraic function admits an algebraic integral. Most algebraic functions don't. The next question of interest may then be whether the algebraic function at hand can be deformed in some way to a related one that is algebraically integrable. Creative telescoping produces such a deformation. It is applicable to functions  $f$  which besides the integration variable  $x$  involve some other parameter  $t$ . The task of creative telescoping is to find a nonzero operator  $L(t, D_t)$  such that  $L(t, D_t) \cdot f$  is integrable. Such an  $L$  is called a *telescoper* for  $f$ .

Several techniques are known for computing such a telescoper. The so-called reduction based approach is one of them, and it has attracted a lot of attention in recent years. It was first proposed for rational functions [7]. Let  $C$  be a field of characteristic zero. Given  $f = p/q \in K(x)$  with  $K = C(t)$ , we can use Hermite reduction to find  $g_i, h_i \in K(x)$  ( $i = 0, 1, 2, \dots$ ) such that  $D_t^i f = D_x g_i + h_i$ . If  $c_0, \dots, c_r \in K$  are such that  $c_0 h_0 + \dots + c_r h_r = 0$ , then

$$(c_0 + \dots + c_r D_t^r) \cdot f = D_x \cdot (c_0 g_0 + \dots + c_r g_r),$$

so the operator  $L = c_0 + \dots + c_r D_t^r$  is a telescoper for  $f$ .

Some recomputation can be avoided by observing that instead of  $D_t^i f$  we may as well integrate  $D_t h_{i-1}$ , because  $D_x$  and  $D_t$  commute. With this optimization, reduction based telescoping can be summarized as follows.

**ALGORITHM 20.** *Input: an algebraic function  $f$  in  $x$  and  $t$ ;*

*Output: a telescoper for  $f$*

- 1 find  $g_0, h_0$  such that  $f = g_0' + h_0$ .
- 2 for  $r = 1, 2, 3, \dots$  do:
- 3 if  $h_0, \dots, h_{r-1}$  are linearly dependent over  $K$
- 4 return  $c_0 + c_1 D_t + \dots + c_{r-1} D_t^{r-1}$  with  $c_i$  not all zero and  $\sum_{i=0}^{r-1} c_i h_i = 0$ .
- 5 find  $g_r, h_r$  such that  $D_t h_{r-1} = g_r' + h_r$

The termination of this procedure can be secured in two ways. One way is to ensure that the remainders  $h_0, h_1, \dots$  belong to a finite dimensional  $K$ -vector space. Then the remainders must eventually become linearly dependent. The second way is to ensure that the map which sends  $f$  to  $h$  such that  $f = g' + h$  for some  $g$  is  $K$ -linear and has the set of all integrable elements as its kernel. It is

then guaranteed that the procedure will not miss a telescoper, so it will terminate because we know that for every bivariate algebraic function, i.e., every element of a field  $C(x, t)[y]/\langle m \rangle$ , there does exist a telescoper.

Besides for rational functions, both arguments have been worked out for various larger classes of functions [8, 9, 16, 19, 40], including the class of algebraic functions [17]. The version for algebraic functions uses Trager's Hermite reduction followed by a polynomial reduction, both steps requiring an integral basis of the function field. Using Theorem 18, we will argue that reduction based telescoping also works with lazy Hermite reduction and the variant of polynomial reduction developed in the previous section, with the obvious advantage that no integral bases computation is needed.

For doing so, we must take into consideration that lazy Hermite reduction takes a suitable basis as input but may return the result with respect to an adjusted suitable basis. Let  $W_0, W_1, \dots$  denote the suitable bases with respect to which the result of the  $i$ th call to lazy Hermite reduction is returned. By supplying  $W_{i-1}$  as input to the  $i$ th call, we can ensure that the  $K[x]$ -module generated by  $W_{i-1}$  is contained in the  $K[x]$ -module generated by  $W_i$ , for every  $i$ . Therefore, if  $W_r \neq W_{r-1}$  for some  $r$ , we can rewrite all remainders  $h_0, \dots, h_{r-1}$  in the bases  $W_r$  and  $V$  without introducing new denominators. (Note that no update is required for  $V$ .) In order to meet the conditions specified in Theorem 18, it may be necessary to rerun the polynomial reduction on the new representations of the old remainders. The termination of the algorithm then follows via the second way indicated above. In order to also justify termination in the first way, it suffices to observe that we can keep  $V$  fixed throughout the computation, so the termination follows directly from the finite dimension of  $N_V$ .

## 6 EXPERIMENTS

For the paper [18] in 2012, a collection of about 100 integration problems was compiled, mostly originating from applications in combinatorics [10, 33], and the performance of six different approaches was compared, including Chyzak's algorithm [20, 21, 28] as implemented by Koutschan [25, 27], Koutschan's ansatz-based method [26], as well as the method based on residue elimination proposed in [18]. The result of the evaluation was somewhat inconclusive. Most algorithms outperformed the other algorithms at least for some examples. At the same time, the timing differences can be significant. It would be interesting to also include Lairez' method [30] into this comparison, but unfortunately we do not have a Mathematica implementation of it.

For the present paper, we have evaluated the performance of reduction based creative telescoping using integral basis and using lazy Hermite reduction on the benchmark set from 2012. The runtime was taken on the same computer (a 64bit Linux server with 24 cores running at 3GHz; in 2012 it had 100G RAM, meanwhile it was upgraded to 700G). The new experiments were performed with a more recent version of Mathematica (Mathematica 12.1.1). Timings and code are available on our website [1].

The timings indicate a clear advantage of lazy Hermite reduction. The computation of integral bases suffers from computations in high degree algebraic extensions of the constant field which appear in the analysis of Puiseux series solutions of the minimal

polynomial of the field generator. The main bottleneck for the lazy approach are the module extensions, which can lead to lengthy coefficients (but never require enlarged fields). For most of the examples in the collection, only few module extensions are needed, i.e., the reduction tends to succeed long before an integral basis is reached. Module extensions can happen for three reasons: (a) for constructing a suitable basis, (b) when the linear system (1) has no solution, (c) when the linear system (1) has more than one solution. Most module extensions we observed were caused by (b), some by (a), and none by (c). It is also worth noting that the module extensions tend to occur close to the beginning of the process. For example, in the notation of Sect. 5, we never encountered the situation that  $W_r \neq W_{r-1}$ , i.e., all module extensions happen in the first iteration. Note that our test cases are “meaningful”; the behaviour for “generic” input may be different. In order to get a better understanding of the generic behaviour, it would be interesting to also work out complexity analysis of both the lazy and the non-lazy version of Hermite reduction, using known results about the complexity for computing integral bases [3] and for computing Hermite normal forms of polynomial matrices [29].

In comparison to the earlier methods, we found reduction based creative telescoping using lazy Hermite reduction to be competitive but not superior. Its inclusion to the set of methods does not change the diffuse result that most methods outperform all the others on some examples, and each method is outperformed by all others on some examples. The timing differences can be significant, even for seemingly similar input.

EXAMPLE 21. Consider the rational function

$$f(x, y, t) = (1 - x - y - t + \frac{3}{4}(xy + xt + yt))^{-1}.$$

The computation of an annihilating operator for  $\text{res}_{x,y} f(x, y, \frac{t}{x^3y})$  is completed in about 4.5 seconds by our new approach. The other techniques need at least twice as long and up to 500 seconds. In this example, the telescoper has order 6 and coefficients of degree 15. On the other hand, computing an annihilating operator for  $\text{res}_{x,y} f(x, y, \frac{t}{x^2y^2})$  takes about half an hour using the reduction based approach, while all other approaches all need less than 90 seconds. Here the telescoper has order 4 and coefficients of degree 11.

**Acknowledgement.** We thank the referees for their careful reading and their valuable suggestions.

## REFERENCES

- [1] <http://www.algebra.uni-linz.ac.at/people/mkauers/lazyhermite/>.
- [2] Niels H. Abel. *Œuvres complètes. Tome I*. Éditions Jacques Gabay, Sceaux, 1992. Edited and with a preface by L. Sylow and S. Lie, Reprint of the second (1881) edition.
- [3] Simon Abelard. On the complexity of computing integral bases of function fields. In *Proc. CASC'20*, pages 42–62, 2020.
- [4] Shreeram S. Abhyankar. Historical ramblings in algebraic geometry and related algebra. *Amer. Math. Monthly*, 83(6):409–448, 1976.
- [5] Gert Almkvist and Doron Zeilberger. The method of differentiating under the integral sign. *J. Symbolic Comput.*, 10:571–591, 1990.
- [6] Janko Böhm, Wolfram Decker, Santiago Laplagne, and Gerhard Pfister. Computing integral bases via localization and Hensel lifting. *J. Symb. Comput.*, 2020.
- [7] Alin Bostan, Shaoshi Chen, Frédéric Chyzak, and Ziming Li. Complexity of creative telescoping for bivariate rational functions. In *Proc. of ISSAC'10*, pages 203–210, 2010.
- [8] Alin Bostan, Shaoshi Chen, Frédéric Chyzak, Ziming Li, and Guoce Xin. Hermite reduction and creative telescoping for hyperexponential functions. In *Proc. of ISSAC'13*, pages 77–84, 2013.
- [9] Alin Bostan, Frédéric Chyzak, Pierre Lairez, and Bruno Salvy. Generalized Hermite reduction, creative telescoping and definite integration of D-finite functions. In *Proc. of ISSAC'18*, pages 95–102, 2018.
- [10] Alin Bostan, Frédéric Chyzak, Mark van Hoeij, Manuel Kauers, and Lucien Pech. Hypergeometric expressions for generating functions of walks with small steps in the quarter plane. *European Journal of Combinatorics*, 61:242–275, 2017.
- [11] Alin Bostan, Pierre Lairez, and Bruno Salvy. Creative telescoping for rational functions using the Griffiths-Dwork method. In *Proc. of ISSAC'13*, pages 93–100, 2013.
- [12] Manuel Bronstein. Integration of elementary functions. *J. Symbolic Comput.*, 9(2):117–173, 1990.
- [13] Manuel Bronstein. The lazy Hermite reduction. Technical Report 3562, INRIA, 1998.
- [14] Manuel Bronstein. Symbolic integration tutorial. ISSAC'98, 1998.
- [15] Manuel Bronstein. *Symbolic Integration I: Transcendental Functions*. Springer-Verlag, Berlin, 2005.
- [16] Shaoshi Chen, Hui Huang, Manuel Kauers, and Ziming Li. A modified Abramov-Petkovsek reduction and creative telescoping for hypergeometric terms. In *Proc. of ISSAC'15*, pages 117–124, 2015.
- [17] Shaoshi Chen, Manuel Kauers, and C. Koutschan. Reduction-based creative telescoping for algebraic functions. In *Proc. of ISSAC'16*, pages 175–182, 2016.
- [18] Shaoshi Chen, Manuel Kauers, and Michael F. Singer. Telescopers for rational and algebraic functions via residues. In *Proc. of ISSAC'12*, pages 130–137, 2012.
- [19] Shaoshi Chen, Mark van Hoeij, Manuel Kauers, and Christoph Koutschan. Reduction-based creative telescoping for fuchsian D-finite functions. *J. Symb. Comput.*, 85:108–127, 2018.
- [20] Frédéric Chyzak. Gröbner bases, symbolic summation and symbolic integration. In *Gröbner Bases and Applications*. Cambridge University Press, 1997.
- [21] Frédéric Chyzak. An extension of Zeilberger’s fast algorithm to general holonomic functions. *Discrete Mathematics*, 217:115–134, 2000.
- [22] James H. Davenport. *On the Integration of Algebraic Functions*, volume 102 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, 1981.
- [23] Keith O. Geddes, Stephen R. Czapor, and George Labahn. *Algorithms for Computer Algebra*. Kluwer, 1992.
- [24] Charles Hermite. Sur l’intégration des fractions rationnelles. *Ann. Sci. École Norm. Sup. (2)*, 1:215–218, 1872.
- [25] Christoph Koutschan. *Advanced Applications of the Holonomic Systems Approach*. PhD thesis, Johannes Kepler University, 2009.
- [26] Christoph Koutschan. A fast approach to creative telescoping. *Mathematics in Computer Science*, 4(2–3):259–266, 2010.
- [27] Christoph Koutschan. HolonomicFunctions (User’s Guide). Technical Report 10-01, RISC Report Series, University of Linz, Austria, January 2010.
- [28] Christoph Koutschan. Creative telescoping for holonomic functions. In *Computer Algebra in Quantum Field Theory: Integration, Summation and Special Functions*, Texts and Monographs in Symbolic Computation, pages 171–194. Springer, 2013.
- [29] George Labahn, Vincent Neiger, and Wei Zhou. Fast, deterministic computation of the hermite normal form and determinant of a polynomial matrix. *J. of Complexity*, 42:44–71, 2017.
- [30] Pierre Lairez. Computing periods of rational integrals. *Mathematics of Computation*, 85:1719–1752, 2016.
- [31] Jesper Lützen. *Joseph Liouville 1809–1882: master of pure and applied mathematics*, volume 15 of *Studies in the History of Mathematics and Physical Sciences*. Springer-Verlag, New York, 1990.
- [32] Ju. I. Manin. Algebraic curves over fields with differentiation. *Izv. Akad. Nauk SSSR. Ser. Mat.*, 22:737–756, 1958.
- [33] Robin Pemantle and Mark C. Wilson. Twenty combinatorial examples of asymptotics derived from multivariate generating functions. *SIAM Review*, 50(2):199–272, 2008.
- [34] Emile Picard. Sur les périodes des intégrales doubles et sur une classe d’équations différentielles lineaires. *Annales scientifiques de l’E.N.S.*, 50:393–395, 1933.
- [35] Robert H. Risch. The solution of the problem of integration in finite terms. *Bull. Amer. Math. Soc.*, 76:605–608, 1970.
- [36] Joseph F. Ritt. *Integration in Finite Terms. Liouville’s Theory of Elementary Methods*. Columbia University Press, New York, N. Y., 1948.
- [37] Joseph F. Ritt. *Differential Algebra*. American Mathematical Society Colloquium Publications, Vol. XXXIII. American Mathematical Society, New York, N. Y., 1950.
- [38] Marc Rybowicz. An algorithms for computing integral bases of an algebraic function field. In *Proc. of ISSAC'91*, page 157–166, 1991.
- [39] Barry M. Trager. *Integration of Algebraic Functions*. PhD thesis, MIT, 1984.
- [40] Joris van der Hoeven. Constructing reductions for creative telescoping. *Applicable Algebra in Engineering, Communication and Computing*, pages 1–28, 2020.
- [41] Mark van Hoeij. An algorithm for computing an integral basis in an algebraic function field. *Journal of Symbolic Computation*, 18(4):353–363, 1994.
- [42] Doron Zeilberger. A holonomic systems approach to special functions identities. *J. Comput. Appl. Math.*, 32:321–368, 1990.
- [43] Doron Zeilberger. The method of creative telescoping. *J. Symbolic Comput.*, 11(3):195–204, 1991.