INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

The Lazy Hermite Reduction

Manuel Bronstein

N° 3562

November 1998

THÈME 2

Rapport de recherche

ISSN 0249-6399

The Lazy Hermite Reduction

Manuel Bronstein

Thème 2 — Génie logiciel
et calcul symbolique
Projet Safir

Rapport de recherche n° 3562 — November 1998 — 13 pages

Abstract: The Hermite reduction is a symbolic integration technique that reduces algebraic functions to integrands having only simple affine poles [1, 2, 8]. While it is very effective in the case of simple radical extensions, its use in more general algebraic extensions requires the precomputation of an integral basis, which makes the reduction impractical for either multiple algebraic extensions or complicated ground fields. In this paper, we show that the Hermite reduction can be performed without *a priori* computation of either a primitive element or integral basis, computing the smallest order necessary for a particular integrand along the way.

Key-words: symbolic integration, algebraic fonctions, integral closure

Unité de recherche INRIA Sophia Antipolis
2004, route des Lucioles, B.P. 93, 06902 Sophia Antipolis Cedex (France)
Téléphone : 04 92 38 77 77 - International : +33 4 92 38 77 77 — Fax : 04 92 38 77 65 - International : +33 4 92 38 77 65

La réduction d'Hermite paresseuse

Résumé : La réduction d'Hermite est une méthode utilisée en intégration formelle pour ramener les fonctions algébriques à des intégrands n'ayant que des pôles simples dans le plan affine [1, 2, 8]. Alors que cette méthode fonctionne bien dans le cas d'extensions radicales, elle a besoin de calculer une base des entiers dans le cas de fonctions algébriques plus générales, ce qui la rend difficile à mettre en œuvre pour des intégrands faisant intervenir plusieurs fonctions algébriques ou bien lorsque le corps des constantes est compliqué. Nous montrons dans ce rapport que la réduction d'Hermite est possible sans connaissance préalable d'une base des entiers.

Mots-clés : intégration formelle, fonctions algébriques, clôture intégrale

1 Preliminaries

We recall in this section some terminology and results from [2, 4, 6, 7] that will be needed in the main algorithm. Let R be an integral domain, K its quotient field and E a finitely generated algebraic extension of K. An element $\alpha \in E$ is called *integral over* R if there is a *monic* polynomial $p \in R[X]$ such that $p(\alpha) = 0$. The set

$$\mathcal{O}_R = \{\alpha \in E \text{ such that } \alpha \text{ is integral over } R\}$$

is called the *integral closure of* R *in* E. It is a subring of E, and if R is a Dedekind domain and E is separable over K, then $\mathcal{O}_R$ is a finitely generated torsion-free R-module [7] and any R-submodule of $\mathcal{O}_R$ is then finitely generated. A basis of E over K that generates $\mathcal{O}_R$ over R is called an *integral basis.*

Let now k be a differential field of characteristic 0 with derivation $'$. An element t in a differential extension of k is called a *monomial over* k if t is transcendental over k and $t' \in k[t]$, which implies that both $k[t]$ and $k(t)$ are closed under differentiation. We say that $p \in k[t]$ is *normal (with respect to $'$)* if $\gcd(p, p') = 1$, and *special (with respect to $'$)* if $\gcd(p, p') = p$. Factors and products of specials are special, and factors and least common multiples of normals are normal. Note that normal polynomials are squarefree. Conversely, for $p \in k[t]$ squarefree, let $p_s = \gcd(p, p')$ and $p_n = p/p_s$. Then, p_s is special and p_n is normal.

Definition 1 *For any $p \in k[t]$, the* normal part of p, *denoted p^*, is the product of all the irreducible normal factors of p.*

The normal part can be computed as follows: let $p = p_1 p_2^2 \dots p_m^m$ be a squarefree factorization of p, $p_{i,s} = \gcd(p_i, p_i')$ and $p_{i,n} = p_i/p_{i,s}$. Then, $p^* = p_{1,n} \cdots p_{m,n}$. In contrast with the case of polynomials, the derivatives of integral algebraic functions can have denominators (e.g. $d\sqrt{x}/dx$), so we need some results about the denominators of such derivatives.

Lemma 1 *Let t be a monomial over k, E be a finitely generated algebraic extension of $k(t)$ and $(w_1, \dots, w_n)$ be an integral basis. Then, there are nonzero normal polynomials $p_1, \dots, p_n \in k[t]$ such that $p_i w_i' \in \mathcal{O}_{k[t]}$ for each i.*

Proof. This is a consequence of Propositions 1.18 and 1.19 of [2], and the proofs of the results of that section remain valid for curves over arbitrary monomial extensions. □

Lemma 2 *Let t be a monomial over k and E be a finitely generated algebraic extension of $k(t)$. Then, for any $w \in \mathcal{O}_{k[t]}$ and for any $p \in k[t]$, if $pw' \in \mathcal{O}_{k[t]}$, then $p^* w' \in \mathcal{O}_{k[t]}$, where p^* is the normal part of p.*

Proof. Let $(w_1, \dots, w_n)$ be an integral basis, $p_1, \dots, p_n$ be the normal polynomials of Lemma 1 and $q = \operatorname{lcm}(p_1, \dots, p_n) \neq 0$. Then, q is normal and $qw_i' \in \mathcal{O}_{k[t]}$ for each i. Let $w \in \mathcal{O}_{k[t]}$ and write $w = \sum_{i=1}^n a_i w_i$ with $a_i \in k[t]$. Then,

$$qw' = \sum_{i=1}^n (qa_i' w_i + a_i q w_i') \in \mathcal{O}_{k[t]}$$

which implies that

$$w' = \frac{1}{d}\sum_{i=1}^{n} b_i w_i$$

where $d, b_1, \ldots, b_n \in k[t]$, $d \mid q$ and $\gcd(d, b_1, \ldots, b_n) = 1$. Let $p \in k[t]$ be such that $pw' \in \mathcal{O}_{k[t]}$. If $p = 0$, then $p^* = 0$, so $p^* w' \in \mathcal{O}_{k[t]}$. Otherwise, we have

$$pw' = \frac{p}{d}\sum_{i=1}^{n} b_i w_i \in \mathcal{O}_{k[t]}$$

so $d \mid pb_i$ for each i. Since $\gcd(d, b_1, \ldots, b_n) = 1$, this implies that $d \mid p$, hence that $d \mid p^*$ since d is normal. Therefore,

$$p^* w' = \frac{p^*}{d}\sum_{i=1}^{n} b_i w_i \in \mathcal{O}_{k[t]}\,.$$

□

Lemma 3 *Let t be a monomial over k, E be a finitely generated algebraic extension of $k(t)$ and $f \in E$. If there exist an integer $m > 0$ and a normal polynomial $p \in k[t]$ such that $p^m f \in \mathcal{O}_{k[t]}$ and $p^m f' \in \mathcal{O}_{k[t]}$, then $p^{m-1} f \in \mathcal{O}_{k[t]}$.*

Proof. Suppose that $p^m f \in \mathcal{O}_{k[t]}$ and $p^m f' \in \mathcal{O}_{k[t]}$, but that $p^{m-1} f \notin \mathcal{O}_{k[t]}$. Then there is a k-place μ of E with order function ν such that $\nu(p^{m-1} f) < 0$. Since $p^m f \in \mathcal{O}_{k[t]}$, $0 \le \nu(p^m f) = \nu(p) + \nu(p^{m-1} f)$, so $\nu(p) > 0$, which implies that $\nu(f) < 0$. Since p is normal, by Lemma 1.7 of [2], whose proof remain valid for curves over arbitrary monomial extensions, $\nu(f') = \nu(f) - \nu(p)$, so $\nu(p^m f') = m\nu(p) + \nu(f') = \nu(p^{m-1} f) < 0$, in contradiction with our hypothesis. Therefore, $p^{m-1} f \in \mathcal{O}_{k[t]}$. □

2 Extending a Module

Let R be a Euclidean domain, K its quotient field, V a finite-dimensional vector space over K with basis $(w_1, \ldots, w_n)$ and $M_w = Rw_1 + \cdots + Rw_n$ the module generated by $(w_1, \ldots, w_n)$. Let $w \in V$ and $M = Rw + M_w$ be the module generated by $(w, w_1, \ldots, w_n)$. We describe in this section an algorithm for computing a generating set $(m_1, \ldots, m_n)$ of M over R.

Since $(w_1, \ldots, w_n)$ generates V over K, we can write

$$w = \frac{1}{d}(a_1 w_1 + \cdots + a_n w_n)$$

where $d, a_1, \ldots, a_n \in R$ and $d \neq 0$. This implies that M is the submodule of $R(1/d)w_1 + \cdots + R(1/d)w_n$ generated by $w_1, \ldots, w_n, w$, *i.e.* by the rows of

$$\mathcal{M} = \begin{pmatrix} d & & & \\ & d & & \\ & & \ddots & \\ & & & d \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$$

Using Hermitian row reduction, we can zero out the last row of $\mathcal{M}$, obtaining a matrix of the form

$$\mathcal{N} = \begin{pmatrix} b_{1,1} & b_{1,2} & \cdots & b_{1,n} \\ b_{2,1} & b_{2,2} & \cdots & b_{2,n} \\ \vdots & \vdots & & \vdots \\ b_{n,1} & b_{n,2} & \cdots & b_{n,n} \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

with $b_{ij} \in R$. A generating set for M over R is then given by

$$m_i = \frac{1}{d} \sum_{j=1}^{n} b_{ij} w_j \quad \text{for } 1 \leq i \leq n\,.$$

3 Suitable Bases

Let k be a differential field of characteristic 0 with derivation $'$, t a monomial over k, $R = k[t]$, $K = k(t)$, E a finitely generated algebraic extension of K and $\mathcal{O}$ the integral closure of R in E. Given any vector-space basis $(w_1, \ldots, w_n)$ of E over K, let $f_{ij} \in K$ be such that

$$w_i' = \sum_{j=1}^{n} f_{ij} w_j \quad \text{for } 1 \leq i \leq n \tag{1}$$

and $F_w \in R$ be the least common multiple of the denominators of all the f_{ij}'s. We say that $(w_1, \ldots, w_n)$ is *suitable* if F_w is normal and $w_i \in \mathcal{O}$ for each i.

Let $(w_1, \ldots, w_n)$ be any vector-space basis of E over K. We describe in this section an algorithm for transforming it into a suitable basis. By multiplying each w_i by a suitable power of the leading coefficient of a polynomial annihilating it, we can assume that $w_i \in \mathcal{O}$ for each i. Let then $\mathcal{O}_w = Rw_1 + \ldots + Rw_n$, the $f_{ij}'s$ be given by (1), and $F_i \in R$ be the least common multiple of the denominators of $f_{i1}, \ldots, f_{in}$ for each i. F_w is then the least common multiple of $F_1, \ldots, F_n$. Suppose that F_w is not normal. Then, one of the F_i's, say F_1, is not normal, so let F_1^* be its normal part and $F_1^\dagger = F_1/F_1^*$, which is not a unit in R. We have,

$$F_1 w_1' = \sum_{j=1}^{n} A_j w_j$$

for $A_1,\ldots,A_n \in R$ with $\gcd(A_1,\ldots,A_n,F_1)=1$. By Lemma 2, $F_1^* w_1' \in \mathcal{O}$. But

$$F_1^* w_1' = \frac{1}{F_1^\dagger}\sum_{j=1}^n A_j w_j\,,$$

which is not in $\mathcal{O}_w$ since $\gcd(A_1,\ldots,A_n,F_1^\dagger)=1$. Let $M = RF_1^* w_1' + \mathcal{O}_w$ and $(b_1,\ldots,b_n)$ be a generating set for M over R, obtained by the algorithm of Section 2. Since $M \subseteq \mathcal{O}$, the b_i's are integral over R, so we can replace the basis $(w_1,\ldots,w_n)$ by $(b_1,\ldots,b_n)$ and repeat this process. Since this process produces a submodule of $\mathcal{O}$ that is stricly larger than $\mathcal{O}_w$, it computes a suitable basis in a finite number of iterations.

4 The Lazy Reduction

With the notation as in the previous section, let $(w_1,\ldots,w_n)$ be a suitable basis for E over K, the $f_{ij}'s$ be given by (1), F_w be the least common multiple of the denominators of all the f_{ij}'s, and $\mathcal{M}_w$ be the n by n matrix with entry $F_w f_{ij}$ at row i and column j. Let $f \in E^*$ and write

$$f = \frac{A_1 w_1 + \cdots A_n w_n}{D}$$

where $D, A_1,\ldots,A_n \in k[t]$ and $\gcd(A_1,\ldots,A_n,D)=1$. Let $D = d_1 d_2^2 \ldots d_{m+1}^{m+1}$ be a squarefree factorization of D, $d_{i,s} = \gcd(d_i, d_i')$ and $U_i = d_i/d_{i,s}$ for each i, $S = d_{1,s}d_{2,s}^2 \cdots d_{m+1,s}^{m+1}$, $U = U_1 U_2^2 \cdots U_m^m$ and $V = U_{m+1}$. Then,

$$D = SUV^{m+1}$$

where S is special, V and all the squarefree factors of U are normal, and $\gcd(U,V)=1$. Let $G_w = F_w/\gcd(F_w,UV)$. Note that $G_w \mid F_w \mid G_w UV$. In addition, $\gcd(G_w,V)=1$ by construction, and since the basis is suitable, F_w, and therefore G_w, are normal.

Consider the following linear system in $k[t]/(V)$:

$$\left(\frac{G_w UV}{F_w}\mathcal{M}_w^t - mG_w UV' I_n\right)\begin{pmatrix}B_1\\B_2\\\vdots\\B_n\end{pmatrix} = G_w S^{-1}\begin{pmatrix}A_1\\A_2\\\vdots\\A_n\end{pmatrix} \tag{2}$$

where $\mathcal{M}_w^t$ is the transpose of $\mathcal{M}_w$, I_n is the n by n identity matrix, and S^{-1} is the inverse of S modulo V. The classical Hermite reduction (where the w_i's form an integral basis) proceeds by computing a solution of (2) in $k[t]/(V)$ and using it to reduce the poles of the integrand. We first show that even with only a suitable basis, any solution in $k[t]/(V)$ does reduce the poles of the integrand.

Theorem 1 *For any solution* $(B_1, \ldots, B_n)$ *of (2) in* $k[t]/(V)$*,*

$$f = \left(\frac{\sum_{i=1}^n B_i w_i}{V^m}\right)' + \frac{\sum_{i=1}^n C_i w_i}{SG_w UV^m} \tag{3}$$

where

$$C_i = \frac{G_w A_i}{V} - SG_w UB_i' + m\frac{SG_w UV' B_i}{V} - \sum_{j=1}^m SG_w U f_{ji} B_j \quad \in k[t]\,. \tag{4}$$

Proof. From (4) and using that $f_{ij} = \mathcal{M}_{w,ij}/F_w$, we get

$$\begin{aligned} V\begin{pmatrix} C_1 \\ C_2 \\ \vdots \\ C_n \end{pmatrix} &= G_w \begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ A_n \end{pmatrix} - SUVG_w \begin{pmatrix} B_1' \\ B_2' \\ \vdots \\ B_n' \end{pmatrix} \\ &\quad + \left(mSG_w UV' I_n - \frac{SG_w UV}{F_w}\mathcal{M}_w^t\right)\begin{pmatrix} B_1 \\ B_2 \\ \vdots \\ B_n \end{pmatrix}. \end{aligned}$$

Since $F_w \mid G_w UV$, the right hand side is in $k[t]^n$, so $VC_i \in k[t]$ for each i. Reducing the above modulo V and using that the B_i's are a solution of (2) in $k[t]/(V)$, and that the B_i' are in $k[t]$ since t is a monomial over k, we obtain

$$V\begin{pmatrix} C_1 \\ C_2 \\ \vdots \\ C_n \end{pmatrix} \equiv G_w \begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ A_n \end{pmatrix} - SUVG_w \begin{pmatrix} B_1' \\ B_2' \\ \vdots \\ B_n' \end{pmatrix} - G_w \begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ A_n \end{pmatrix} \equiv 0 \pmod{V}$$

hence that $C_i \in k[t]$ for each i. The proof of (3) follows by a straightforward calculation, putting the right hand side over a common denominator, and using (4) to replace VC_i:

$$\begin{aligned} &\left(\frac{\sum_{i=1}^n B_i w_i}{V^m}\right)' + \frac{\sum_{i=1}^n C_i w_i}{SG_w UV^m} \\ &= \frac{\sum_{i=1}^n (SG_w UVB_i' - mSG_w UV' B_i + VC_i) w_i + SG_w UVB_i w_i'}{SG_w UV^{m+1}} \\ &= \frac{\sum_{i=1}^n \left(G_w A_i - \sum_{j=1}^m SG_w UV f_{ji} B_j\right) w_i + \sum_{j=1}^n SG_w UVB_i f_{ij} w_j}{SG_w UV^{m+1}} \\ &= \frac{\sum_{i=1}^n G_w A_i}{SG_w UV^{m+1}} = f\,. \end{aligned}$$

□

There remains to study under which circumstances the system (2) has a solution in $k[t]/(V)$.

Lemma 4 *Let*
$$S_i = SUV^{m+1}\left(\frac{w_i}{V^m}\right)' \quad \textit{for } 1 \le i \le n\,. \tag{5}$$
If there are $Q, T_1, \dots, T_n \in k[t]$ *such that* $\gcd(Q, V) = 1$ *and*
$$\sum_{i=1}^n A_i w_i = \frac{1}{Q}\sum_{i=1}^n T_i S_i$$
then (2) has a solution in $k[t]/(V)$.

Proof. Suppose that $Q\sum_{i=1}^n A_i w_i = \sum_{i=1}^n T_i S_i$ for some $Q, T_1, \dots, T_n \in k[t]$. Since
$$\begin{aligned} S_i &= SUV^{m+1}\left(\frac{w_i}{V^m}\right)' = SUV^{m+1}\left(\frac{w_i{}'}{V^m} - m w_i \frac{V'}{V^{m+1}}\right) \\ &= S\left(\frac{UV}{F_w}\sum_{j=1}^n f_{ij} w_j - mUV' w_i\right) \end{aligned}$$
equating the coefficients of each w_i yields
$$S\left(\frac{G_w UV}{F_w}\mathcal{M}_w^t - mG_w UV' I_n\right)\begin{pmatrix} T_1 \\ T_2 \\ \vdots \\ T_n \end{pmatrix} = QG_w\begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ A_n \end{pmatrix}.$$
If $\gcd(Q, V) = 1$, then $(T_1 Q^{-1}, \dots, T_n Q^{-1})$ is a solution in $k[t]/(V)$ of (2), where Q^{-1} is the inverse of Q modulo V. □

Lemma 5 *Let* $A, B \in k[t]$ *with* B *normal,* $(w_1, \dots, w_n)$ *be a basis for* E *over* K *such that* $w_i \in \mathcal{O}$ *for* $1 \le i \le n$, $m > 0$ *be an integer, and*
$$R_i = AB^{m+1}\left(\frac{w_i}{B^m}\right)' \quad \textit{for } 1 \le i \le n\,.$$
Then, for any $T_1, \dots, T_n \in k[t]$,
$$\frac{1}{B}\sum_{i=1}^n T_i R_i \in \mathcal{O} \Rightarrow \frac{A}{B}\sum_{i=1}^n T_i w_i \in \mathcal{O}\,.$$

Proof. Suppose that $B^{-1}\sum_{i=1}^n T_i R_i \in \mathcal{O}$ and let
$$w = \frac{A}{B}\sum_{i=1}^n T_i w_i \quad \text{and} \quad h = wB^{1-m}\,.$$

We have

$$\begin{aligned} B^m h' &= B^m \left(\sum_{i=1}^n \frac{AT_i w_i}{B^m}\right)' = B^m \sum_{i=1}^n AT_i \left(\frac{w_i}{B^m}\right)' + \sum_{i=1}^n (AT_i)' w_i \\ &= \frac{1}{B} \sum_{i=1}^n T_i R_i + \sum_{i=1}^n (AT_i)' w_i \quad \in \mathcal{O}\,. \end{aligned}$$

Since $B^m h = Bw = A_n \sum_{i=1}^n T_i w_i \in \mathcal{O}$, it follows from Lemma 3 that $w = B^{m-1} h \in \mathcal{O}$. □

Lemma 6 *Let $A, B \in k[t]$ with B normal, $(w_1, \dots, w_n)$ be a basis for E over K such that $w_i \in \mathcal{O}$ for $1 \le i \le n$, $m > 0$ be an integer, and*

$$R_i = AB^{m+1} \left(\frac{w_i}{B^m}\right)' \quad \textit{for } 1 \le i \le n\,.$$

Then, for any $T_1, \dots, T_n \in k[t]$ and any $C \in k[t]$ such that $C \mid B$,

$$\frac{1}{C} \sum_{i=1}^n T_i R_i \in \mathcal{O} \Rightarrow \frac{A(B/C)}{C} \sum_{i=1}^n T_i w_i \in \mathcal{O}\,.$$

Proof. Suppose that $C^{-1} \sum_{i=1}^n T_i R_i \in \mathcal{O}$ and let $D = B/C$,

$$w = \frac{AD}{C} \sum_{i=1}^n T_i w_i \quad \text{and} \quad r_i = (AD) C^{m+1} \left(\frac{w_i}{C^m}\right)' \text{ for } 1 \le i \le n\,.$$

We have

$$R_i = AD^{m+1} C^{m+1} \left(\frac{w_i}{C^m} \frac{1}{D^m}\right)' = ADC^{m+1} \left(\frac{w_i}{C^m}\right)' - mD'CAw_i$$

so $r_i = R_i + mD'CAw_i$, which implies that

$$\frac{1}{C} \sum_{i=1}^n T_i r_i = \frac{1}{C} \sum_{i=1}^n T_i R_i + mAD' \sum_{i=1}^n T_i w_i \in \mathcal{O}\,.$$

Since C is a factor of B, it is normal, so $w \in \mathcal{O}$ by Lemma 5. □

We can now extend the module $k[t]w_1 + \cdots + k[t]w_n$ whenever the system (2) has no solution in $k[t]/(V)$.

Theorem 2 *Suppose that $m > 0$ and that $\{S_1, \dots, S_n\}$ as given by (5) are linearly dependent over $k(t)$, and let $T_1, \dots, T_n \in k[t]$ be not all 0 and such that $\sum_{i=1}^n T_i S_i = 0$. Then,*

$$w = \frac{SU}{V} \sum_{i=1}^n T_i w_i \in \mathcal{O}\,.$$

Furthermore, if $\gcd(T_1, \dots, T_n) = 1$, then $w \notin \mathcal{O}_w = k[t]w_1 + \cdots + k[t]w_n$.

Proof. Since $V^{-1}\sum_{i=1}^n T_i S_i = 0 \in \mathcal{O}$, Lemma 5 applied to $A = SU$ and $B = V$ implies that $w \in \mathcal{O}$. If $\gcd(T_1, \dots, T_n) = 1$, then V cannot divide all the SUT_i's, so $w \notin \mathcal{O}_w$ since $(w_1, \dots, w_n)$ is a basis for E over $k(t)$. □

Theorem 3 *Suppose that $m > 0$ and that $\{S_1, \dots, S_n\}$ as given by (5) are linearly independent over $k(t)$, and let $Q, T_1, \dots, T_n \in k[t]$ be such that*

$$\sum_{i=1}^m A_i w_i = \frac{1}{Q}\sum_{i=1}^n T_i S_i \,.$$

Then,

$$w = \frac{SU(V/\gcd(V,Q))}{\gcd(V,Q)}\sum_{i=1}^n T_i w_i \in \mathcal{O}\,.$$

Furthermore, if $\gcd(Q, T_1, \dots, T_n) = 1$ and (2) has no solution in $k[t]/(V)$, then $w \notin \mathcal{O}_w = k[t]w_1 + \cdots + k[t]w_n$.

Proof. Let $G = \gcd(V, Q)$. Then,

$$\frac{1}{G}\sum_{i=1}^n T_i S_i = \frac{Q}{G}\sum_{i=1}^n A_i w_i \in \mathcal{O}\,,$$

so by Lemma 6 applied to $A = SU$, $B = V$ and $C = G$, we have $w \in \mathcal{O}$. If the system (2) has no solution in $k[t]/(V)$, then $\deg(G) > 0$ by Lemma 4. Furthermore, if $\gcd(Q, T_1, \dots, T_n) = 1$, then G cannot divide all the $SU(V/G)T_i$'s, so $w \notin \mathcal{O}_w$ since $(w_1, \dots, w_n)$ is a basis for E over $k(t)$. □

The lazy reduction algorithm follows from Theorems 1, 2 and 3: if $m = 0$, then $D = SU_1$, where S is special and U_1 is normal. Otherwise, we solve the system

$$\sum_{i=1}^n A_i w_i = \sum_{i=1}^n h_i S_i$$

for $h_1, \dots, h_n \in k(t)$. Any solution in $k(t)$ whose denominators are coprime with V is a solution of (2) in $k[t]/(V)$ as shown in the proof of Lemma 4. In that case, (3) reduces integrating f to a new integrand whose denominator divides SG_wUV^m. If the above equation has no solution in $k(t)$ whose denominators are coprime with V, then either the S_i's are linearly dependent over $k(t)$ or there is a solution whose denominator has a nontrivial common factor with V, so either Theorem 2 or 3 produces $w \in \mathcal{O}$ such that $w \notin \mathcal{O}_w$, and the algorithm of Section 2 produces a new basis $b_1, \dots, b_n$ for the submodule $k[t]w + \mathcal{O}_w$ of $\mathcal{O}$. We make that basis suitable with the algorithm of Section 3, express f in the new basis and continue the reduction process. In both of the above cases, the integrand after the reduction step has an expression whose denominator has stricly less zeroes of multiplicity

$m+1$ than before the reduction step (it has none when the system has a solution), so after finitely many reduction steps, we have produced a new basis made of integral elements, and a new integrand, whose denominator with respect to that basis is the product of a special and a normal polynomial. This is the same result obtained by the Hermite reduction (with an integral basis) as presented in [1, 2, 8].

Conclusions

We have presented a lazy Hermite reduction for which each reduction step uses only rational operations and performs Gaussian or Hermitian elimination on a matrices of sizes n by n or $n+1$ by n, while computing an integral basis requires Hermitian elimination on matrices of sizes n^2 by n, so the lazy reduction is expected to cost $\mathcal{O}(n^3)$ operations in $k(t)$ as compared to $\mathcal{O}(n^4)$ for computing rationally an integral basis. In the case of pure algebraic functions, this yields a complete algorithm for determinining whether the integral of an algebraic function is itself an algebraic function. The natural direction in which to extend this work is to ask whether the complete algebraic integration algorithm can be performed rationally without computing an integral basis. Since Propositions 2.4 and 2.5 of [2] do not depend on an integral basis, the inner resultant in Proposition 2.6 can be replaced by the norm from $E[z]$ to $K[z]$, yielding a polynomials whose roots are nonzero rational multiples of the residues of the integrand at all the normal affine places, so divisors for the logarithmic parts can be computed. The remaining problems are representing such divisors and testing them for principality, and I am not aware of any rational algorithm for solving those problems that avoid desingularizing the curve in some way. Another interesting direction would be to generalize the Hermite reduction (and its lazy variant) to solve equations of the form $y'+fy=g$ in a finitely generated algebraic extension of $k(t)$, as was done for the transcendental case in [5]. This could yield a better algorithm than the reduction to a linear differential system in $k(t)$ [3].

References

[1] Laurent Bertrand. *Calcul Symbolique des Intégrales Hyperelliptiques.* Thèse de doctorat, Université de Limoges, Mathématiques, 1995.

[2] Manuel Bronstein. On the integration of elementary functions. *Journal of Symbolic Computation*, 9(2):117–173, February 1990.

[3] Manuel Bronstein. The Risch differential equation on an algebraic curve. In Stephen Watt, editor, *Proceedings of ISSAC'91*, pages 241–246. ACM Press, 1991.

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

[5] James Harold Davenport. The Risch differential equation problem. *SIAM Journal on Computing*, 15:903–918, 1986.

[6] Serge Lang. *Algebra.* Addison Wesley, Reading, Massachusetts, 1970.

[7] M. Pohst and H. Zassenhaus. *Algorithmic algebraic number theory.* Cambridge University Press, Cambridge, 1989.

[8] Barry Trager. *On the integration of algebraic functions.* PhD thesis, MIT, Computer Science, 1984.

Contents

Unité de recherche INRIA Sophia Antipolis
2004, route des Lucioles - B.P. 93 - 06902 Sophia Antipolis Cedex (France)

Unité de recherche INRIA Lorraine : Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - B.P. 101 - 54602 Villers lès Nancy Cedex (France)
Unité de recherche INRIA Rennes : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex (France)
Unité de recherche INRIA Rhône-Alpes : 655, avenue de l'Europe - 38330 Montbonnot St Martin (France)
Unité de recherche INRIA Rocquencourt : Domaine de Voluceau - Rocquencourt - B.P. 105 - 78153 Le Chesnay Cedex (France)

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, B.P. 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399