The Lazy Hermite Reduction

Manuel Bronstein
INRIA, Sophia Antipolis

May 4, 1998

[summary by Grégoire Lecerf]

Abstract

The Hermite reduction is a symbolic integration technique that reduces algebraic functions to integrands having only simple affine poles [1, 2, 7]. 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 work, Manuel Bronstein shows 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.

1. Preliminaries

We recall in this section some terminology and results from [2, 4, 6] 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 ring and a finitely generated R-module. A basis of E over K that generates $\mathcal{O}_R$ over R is called an *integral basis.* Any submodule of $\mathcal{O}_R$ is finitely generated over R.

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.

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 $d, a1, \ldots, a_n \in R$ 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

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

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

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

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

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

The cost of this computation is $O(n^3)$ operations in $k[t]$.

3. I-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 $f_{i,j} \in K$ be such that

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

and $F_w \in R$ be the least common multiple of the denominators of all the $f_{i,j}$'s.

Definition 1. With the above notations, we say that $(w_1, \ldots, w_n)$ is an *I-basis* if F_w is normal and $w_i \in \mathcal{O}$ for each i.

For any vector-space basis of E over K we have an algorithm for transforming it into an I-basis within $O(n^3)$ operations in $k(t)$.

4. The Lazy Reduction

With the notations as in the previous section, let $(w_1, \ldots, w_n)$ be an I-basis for E over K, the $f_{i,j}$'s be given by (1), F_w be the least common multiple of the denominators of all the $f_{i,j}$'s, and $\mathcal{M}_w$ be the n by n matrix with entry $F_w f_{i,j}$ 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 $D = d_1 d_2^2 \cdots d_{m+1}^{m+1}$ 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 an I-basis, F_w, and therefore G_w, are normal.

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

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

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. Even with an I-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 $k[t]/(V)$,*

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

where

$$C_i = \frac{G_w A_i}{V} - S G_w U B_i' + m \frac{S G_w U V' B_i}{V} - \sum_{j=1}^m S G_w U f_{j,i} B_j \qquad \in k[t]. \tag{4}$$

It remains to study under which circumstances the system (2) has a solution in $k[t]/(V)$: we show that, whenever the system has no solution, we can extend the module $k[t]w_1 + \cdots + k[t]w_n$. Let

$$S_i = SUV^{m+1}\left(\frac{w_i}{V^m}\right)', \quad \text{for} \quad 1 \le i \le n. \tag{5}$$

Theorem 2. *Suppose that $m > 0$ and that $\{S_1, \ldots, S_n\}$ as given by (5) are linearly independent over $k(t)$, and let $T_1, \ldots, T_n \in k[T]$ be not all zero 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 $\gcd(T_1, \ldots, T_n) = 1$, *then $w \notin \mathcal{O}_w = k[t]w_1 + \cdots k[t]w_n$.*

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

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

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* $w \notin \mathcal{O}_w = k[t]w_1 + \cdots + k[t]w_n$.

The lazy reduction algorithm follows from Theorems 1, 2, and 3: if $m = 0$, then $D = SU_1$, where S is special and U_i 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 $k[t]/(V)$. 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 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 transform that basis into an I-basis, 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 strictly less zeroes of multiplicity $m + 1$ than before (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 as obtained by the Hermite reduction (with an integral basis) as presented in [1, 2, 7].

Conclusion

We have presented a lazy Hermite reduction for which each reduction step uses only rational operations and performs Gaussian or Hermitian elimination on matrices of size 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 $O(n^3)$ operations in $k(t)$ as compared to $O(n^4)$ for computing rationally an integral basis. In the case of pure algebraic functions, this yields a complete algorithm for determining 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. 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].

Bibliography

[1] Bertrand (Laurent). – *Calcul Symbolique des Intégrales Hyperelliptiques.* – PhD thesis, Université de Limoges, Mathématiques, 1995.

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

[3] Bronstein (Manuel). – The Risch differential equation on an algebraic curve. In Watt (Stephen) (editor), *Symbolic and algebraic computation.* pp. 241–246. – New York, 1991. Proceedings of ISSAC'91, Bonn, Germany.

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

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

[6] Lang (Serge). – *Algebra.* – Addison Wesley, Reading, Massachussets, 1970.

[7] Trager (Barry). – *On the integration of algebraic functions.* – PhD thesis, MIT, Computer Science, 1984.