Symbolic Computation of Hyperelliptic Integrals and Arithmetic in the Jacobian

Laurent Bertrand
Université de Limoges

June 7, 1995

[summary by Gaétan Haché]

1. Introduction

The interest of this talk is the integration of hyperelliptic functions. The technique used for such integration follows the usual pattern for the integration of algebraic function developed by R. H. Risch, B. M. Trager, J. H. Davenport and a representation of divisors over hyperelliptic curves due to D. G. Cantor. For example, we want to compute the integral

$$\int_2^3 \frac{3x^5 - x + 2}{(x^2 - x^5 - x + 1)\sqrt{x^5 + x - 1}}\, dx. \tag{1}$$

If the exact value of this integral is needed, then one normally computes a primitive. In this case it is equal to

$$\log\left(\frac{x + \sqrt{x^5 + x - 1}}{x - \sqrt{x^5 + x - 1}}\right).$$

If we set

$$y^2 = x^5 + x - 1, \tag{2}$$

then one can consider the integral

$$\int \frac{3x^5 - x + 2}{(x^2 - x^5 - x + 1)y}\, dx$$

over the algebraic function field of the affine curve

$$\mathcal{C} = \{(a, b) \in \mathbb{A}^2(\mathbb{C}) : b^2 - a^5 - a + 1 = 0\}.$$

2. Integration over function field of curves

The general setup is the following. Let K be a field of characteristic 0, $\overline{K}$ an algebraic closure of K and $F \in K[x, y]$ an absolutely irreducible polynomial (that is F is irreducible over $\overline{K}$). We consider the function field

$$K(\mathcal{C}) = K(x)[y]/\langle F \rangle$$

where $\mathcal{C}$ is the curve defined by $F(x, y) = 0$.

Definition 1. A function H is said to be an *elementary primitive* of $h \in K(\mathcal{C})$ if $H' = h$ and if H can be written from functions of $K(\mathcal{C})$ using combinations of logarithms, exponentials and algebraic expressions.

In the previous example

$$h = \frac{3x^5 - x + 2}{(x^2 - x^5 - x + 1)y},$$

the curve has for equation

$$y^2 - x^5 - x + 1 = 0$$

and h has for elementary primitive

$$\log\left(\frac{x+y}{x-y}\right).$$

We want to answer the following questions:

(1) Does a function $h \in K(\mathcal{C})$ have an elementary primitive $H = \int h\,dx$ over K ?
(2) If so, what is this primitive?

Risch have shown that if H is an elementary primitive over K then

$$H = v_0 + \sum_{i=1}^{k} c_i \log(v_i) \tag{3}$$

where $v_0 \in K(\mathcal{C})$, $c_i \in \overline{K}$ and $v_i \in \overline{K}(\mathcal{C})$. The algebraic part v_0 is computed using Hermite's algorithm and the logarithmic part is done using Risch's algorithm.

Following is a short history of integration of algebraic functions.

1833: Liouville's principle; gives the form of the elementary primitive;
1872: Hermite's algorithm; allows the computation of the algebraic part;
1970: Risch's algorithm; allows the computation of the logarithmic part. Needs arithmetic over divisors of function fields and principality test;
1981–1984: Davenport and Trager algorithms; first implementable algorithms.

3. Special case: hyperelliptic curves

In his thesis, B. Trager gives an algorithm which solves the previous questions in the general cases. The work of L. Bertrand studies the case where $\mathcal{C}$ has genus $g \geq 2$ (hyperelliptic) and $K(\mathcal{C})$ is a quadratic extension of $K(x)$ with $x \in K(\mathcal{C})$ transcendental over K. Let L be the function field of genus g of the curve $\mathcal{C}$ defined by the equation

$$y^2 = f(x) \tag{4}$$

where $f(x)$ is square free of degree m. In this case, the computation of the logarithmic part of the primitive is reduced to the computation of the primitive of the following type

$$\int \omega \qquad \text{where} \qquad \omega = \frac{P(x)}{Q(x)y}\,dx$$

with $P, Q \in K[x]$ such that $\gcd(Q', Q) = \gcd(P, Q) = \gcd(f, Q) = 1$. To the differential ω is associated some zero degree divisors $D_1, D_2, \ldots, D_k$ over the normalized of the affine curve $\mathcal{C}$ defined by (4). A necessary condition for the primitive to be elementary is that all these divisors are torsion divisors, that is there exist m_i, $(i = 1, \ldots, k)$, such that $m_i D_i$ are principal. Then the functions $v_i \in K(\mathcal{C})$ such that $(v_i) = n_i D_i$ are candidates to verify (3).

4. Representation of divisors

For quadratic extensions, L. Bertrand has developed an algorithm which is much more efficient than Trager's one. This is because the test of principality is greatly improved by the use of a simpler representation of divisors over such quadratic extensions. Following is an overview of such representations. Two cases are considered:

- $m = 2g + 1$ and $\mathcal{C}$ has a unique point at infinity;
- $m = 2g + 2$ and $\mathcal{C}$ has exactly two points at infinity.

Case $m = 2g + 1$. Any divisor D of degree 0 may be written

$$D = \sum_{i=1}^{k} n_i P_i - \sum_{i=1}^{k} n_i P_\infty. \tag{5}$$

It is represented by two polynomials

$$[a(x), b(x)]$$

where

- $a(x) = \prod_{i=1}^{k} (x - x_i)^{n_i}$;
- for all i, $\nu_P(y - b(x)) \geq n_i$;
- $\deg b < \deg a$.

Case $m = 2g + 2$. Any divisor D of degree 0 may be written

$$D = \sum_{i=1}^{k} n_i P_i + n_{\infty+} P_{\infty+} + n_{\infty-} P_{\infty-}$$

with $\sum_{i=1}^{k} n_i + n_{\infty+} + n_{\infty-} = 0$ and the representation of D is given by

$$[a(x), b(x), \delta]$$

where a and b are defined in the same manner as in the case $m = 2g + 1$ and where $\delta = n_{\infty+} - n_{\infty-}$.

5. Arithmetic in the Jacobian

To test if a divisor D is a torsion divisor, one computes the order of D in the Jacobian over several well chosen finite prime fields (note that over finite fields, any zero degree divisor is a torsion divisor since the Jacobian of the curve is finite). Using the outcome of these order computation, one can decide if the divisor D is a torsion divisor or not.

The computation of the order of a divisor is done by performing a principality test of lD for $l = 1, 2, \ldots$ until we find l such that lD is principal. To do so in an efficient way, fast arithmetic computation over the Jacobian is needed. Following is an overview of how it is done using the representation of divisors by two polynomials (for more details see [1]). Let D be a divisor represented by $[a, b]$. Then $-D = [a, -b] - (a)$. Let D_1 and D_2 be two divisors represented by $[a_1, b_1]$ and $[a_2, b_2]$ respectively. Then

$$D_1 + D_2 = \left[\frac{a_1 a_2}{d^2}, \frac{h_1 a_1 b_2 + h_2 a_2 b_1 + h_3(b_1 b_2 + f)}{d} \mod a \right] + (d) \tag{6}$$

where

$$d = \gcd(a_1, a_2, b_1 + b_2) = h_1 a_1 + h_2 a_2 + h_3(b_1 + b_2).$$

A notion of reduced divisor is considered and the principality test relies on a theorem stating that a reduced divisor D is principal if and only if $D = [1, 0]$. Using the arithmetic over the Jacobian, one can compute for any divisor D an equivalent reduced divisor D_0, that is such that $D = D_0 + (h)$ for some function $h \in K(\mathcal{C})$. In the case where $m = 2g + 2$, a similar notion of reduced divisor is used, and a reduced divisor D is principal if and only if $D = [1, 0, 0]$.

Bibliography

[1] Cantor (D. G.). – Computing in the Jacobian of an hyperelliptic curve. *Mathematics of Computation*, vol. 48, n° 177, 1987.