Computation of the Integral Basis of an Algebraic Function Field and Application to the Parametrization of Algebraic Curves

Mark van Hoeij
University of Nijmegen

June 7, 1995

[summary by Laurent Bertrand]

Abstract

A new algorithm [1] for computing an integral basis of an algebraic function field is presented. This algorithm is then applied to the computation of parametrizations of algebraic curves of genus zero [2].

1. Computation of the integral basis

Let L be an algebraically closed field of characteristic zero and x be transcendental over L. Let y be algebraic over $L(x)$ with minimal polynomial f of degree n with respect to y. We suppose that y is integral over $L[x]$, so f is monic over $L[x]$. Let C be the algebraic curve defined by the equation

$$f(X,Y)=0$$

and let $L(C)$ be the function field

$$L(C)=L(x,y)=L(X)[Y]/(f(X,Y)).$$

A function of $L(C)$ is called *integral* if it satisfies a monic irreducible polynomial with coefficients in $L[x]$. The integral closure Θ of $L[x]$ in $L(C)$ is the set of all integral functions. It is also the set of all functions with no finite pole, and it is a free module of rank n over $L[x]$. An *integral basis* is then a set $\{b_0,\ldots,b_{n-1}\}$ of elements of $L(C)$ such that

$$\Theta = L[x]b_0+\cdots+L[x]b_{n-1}.$$

The algorithm presented here computes an integral basis with all its elements in $K(x,y)$ where K is a given subfield of L containing all the coefficients of f.

1.1. Algorithm. The algorithm can be described as follows. We look for an integral basis of the form $\{b_0,\ldots,b_{n-1}\}$ such that b_i is a polynomial of degree i in y with coefficients in $K(x)$. Moreover b_0 can be chosen equal to 1. The integral basis is computed step by step. Suppose that

$$\{b_0,\ldots,b_{d-1}\}$$

have been computed, then we compute b_d such that

$$L[x]b_0+\cdots+L[x]b_d=\{a\in\Theta : \deg(a)\le d\}$$

and $\deg(b_d)=d$ as follows:

(1) let b_d be yb_{d-1};

(2) let $V = \{a \in \Theta : \deg(a) \leq d\} \setminus L[x]b_0 + \cdots + L[x]b_d$;
while $V \neq \emptyset$ do
  (a) choose $a \in V$ such that $a = (a_0b_0 + \cdots + a_db_d)/k$ with $a_0, \ldots, a_d$ and k in $K[x]$ and $a_d = 1$;
  (b) substitute b_d by a.

In order to compute an element a satisfying the conditions of (a), the author applies the result saying that $x - \alpha$ appears in the denominator k if and only if C has a singularity on the line $x = \alpha$. After that, for computing the a_i's, Puiseux expansions are used and also bounds for these expansions and for the degree of the denominator. The issue is the resolution of a linear system.

2. Application to the parametrization of algebraic curves

Here f is supposed to be irreducible of degree n with respect to y. The curve C is the projective algebraic curve defined by f. Let F be the homogenization of f. It means that $F(X,Y,Z)$ is the polynomial of smallest degree such that $f = F(X,Y,1)$. A parameter p is a function generating $L(C)$, i.e., every function in $L(C)$ can be written as a rational funtion in p. It is in fact a function with only one pole which is of order 1 on C. A parametrization of C is a pair $(X(t), Y(t))$ of rational functions such that $f\,(X(t), Y(t)) = 0$ and $L\,(X(t), Y(t)) = L(t)$.

Curves allowing parametrizations are called rational curves. They are in fact curves of genus 0. The aim of this algorithm is to compute when it is possible a parametrization of a given curve, using the algorithm for computing an integral basis presented before.

2.1. Algorithm. The algorithm for computing a parametrization is the following:

(1) Compute a parameter p;
(2) Express x and y as rational functions in p.

For the computation of a parameter, divide the projective plane in two disjoint parts A and B. Compute a function P with only one pole of multiplicity 1 in $A \cap C$. Then compute a function Q with no pole in $A \cap C$ and such that $P + Q$ has no pole in $B \cap C$. (For that, the computation of an integral basis is used). Then a parameter is $P + Q$.

The last thing to do is to express x and y as rational functions in p by computing appropriated resultants.

The computation of integral basis can also be used to compute the genus of a curve or the Weierstrass normal form of a curve of genus 1, see [1, 3].

Bibliography

[1] van Hoeij (Mark). – An algorithm for computing an integral basis in an algebraic function field. *Journal of Symbolic Computation*, vol. 18, 1994, pp. 353–363.

[2] van Hoeij (Mark). – Computing parametrizations of rational algebraic curves. In *Symbolic and Algebraic Computation*. ACM, pp. 187–190. – New York, 1994. Proceedings ISSAC'94, Oxford, England.

[3] van Hoeij (Mark). – An algorithm for computing the Weierstrass normal form. In *Symbolic and Algebraic Computation*. ACM. – ACM Press, 1995. Proceedings ISSAC'95, Montreal, Canada.