Computing an Integral Basis for an Algebraic Function Field

Mark van Hoeij
Florida State University

joint with Mike Stillman, Cornell University

Georgia Tech meeting on Algebraic Geometry for Applications

April 11, 2015

Algorithms

1. Round 2, round 4. Works for number fields and function fields. Implemented in several computer algebra systems.
2. Puiseux expansions. Works if there is no wild ramification (includes function fields of char 0 and char $p >> 0$). Implemented in Maple's algcurves package.
3. Montes algorithm. Number fields and function fields. Magma implementation can be downloaded online.
4. Frobenius based method. Designed for function field of small prime characteristic p. Implemented in Macaulay.

Applications

Consider the following number field:

$K = \mathbb{Q}[x]/(98818x^6 - 800756x^5 + 3495803x^4 - 8505211x^3 + 15375943x^2 - 17721960x + 7848261)$

There is an algorithm, POLRED, that can size-reduce this to

$K \cong \mathbb{Q}[x]/(x^6 - 5x^4 - 21x^3 - 23x^2 - 12x - 2)$

A key step is the computation of an *integral basis*.

Applications

Let $L = \mathbb{Q}(x)[y]/(f)$ be the function field of the algebraic curve $C \subset P^2$ defined by:

$$f = y^4 + (-4x^2 + 2x + 2)y^3 + (8x^4 - 7x^3 - 2x^2 - 2x + 1)y^2 + (-12x^6 + 9x^5 + 4x^4 + x^3 - 2x^2)y + 9x^8 - 9x^7 + 3x^6 - 6x^5 + 4x^4$$

Then: $L \cong \mathbb{Q}(u)[v]/(\tilde{f})$

where $\tilde{f} = 3v^2 + 4u^3 + 24u + 1$.

How to find such size-reduction? Again, *integral basis* is key.

Applications

$L = \mathbb{Q}(x)[y]/(\text{large equation}) = \{\text{functions on } C\}$, want to find:

$L \cong \mathbb{Q}(u)[v]/(\text{small equation})$.

The main step is to find two functions $g, h \in L$ of low degree (then construct an isomorphism with $g, h \mapsto u, v$).

Functions of low degree are functions $C \to P^1$ with few poles (counting with multiplicity).

To find those, we need an *integral basis*. If $A \subset C$ denote:
$\mathcal{O}_A = \{g \in L \mid \text{ no poles in } A\}$

We can compute low-degree functions from a basis for $\mathcal{O}_A$ and a basis for $\mathcal{O}_{A^c}$.

Places on Curves

If P is a *regular point* on a curve C defined over $\mathbb{C}$, then one can *evaluate* functions $g \in L$ at the point P, and the result is an element of $P^1(\mathbb{C}) = \mathbb{C} \bigcup \{\infty\}$.

One can also compute the *valuation* of g at the point P:

- $v_P(g) > 0$ when g has a root of that order at P
- $v_P(g) = \infty$ when $g = 0$
- $v_P(g) < 0$ when g has a pole of that order at P
- $v_P(g) = 0$ when $g(P) \notin \{0, \infty\}$.

$v_P(g) \geqslant 0$ means that g has no pole at P.

Places and Valuations

A discrete valuation on L is an onto map $v : L \to \mathbb{Z} \bigcup \{\infty\}$ with

- $g = 0 \iff v(g) = \infty$
- $v(gh) = v(g) + v(h)$
- $v(g + h) \geqslant \min(v(g), v(h))$ for all functions $g, h \in L$.

A *non-singular point* P corresponds to a valuation $v_P : L \to \mathbb{Z} \bigcup \{\infty\}$.

A singular point can correspond to several valuations (g could go to 0 on one branch of a double-point and not on the other).

Places = "points on desingularized curve".

Each *place* P corresponds precisely to one valuation v_P.

Places and Valuations

Let $L := \mathbb{F}_p(x)[y]/(f)$ and

$A := \{\text{finite places}\} = \{P \text{ with } v_P(x) \geqslant 0\}$

First consider functions in $\mathbb{F}_p(x) \subset L$ with no poles in A:

$$\{g \in \mathbb{F}_p(x) \mid v_P(g) \geqslant 0 \text{ for all } P \in A\}$$

This is the ring $\mathbb{F}_p[x]$, and so:

$$\mathcal{O}_A := \{g \in L \mid v_P(g) \geqslant 0 \text{ for all } P \in A\}$$

is a $\mathbb{F}_p[x]$-module.

This module is free ($\mathbb{F}_p[x]$ is a PID) so it has a basis $b_1, \ldots, b_n$.

Integral basis and singularities

$L = \mathbb{F}_p(x)[y]/(f)$ and $A = \{\text{finite places}\}$

$$\mathcal{O}_A = \{g \in L \mid v_P(g) \geqslant 0 \text{ for all } P \in A\}$$

is the *integral closure* of $\mathbb{F}_p[x]$ in L
(the elements of L that satisfy a monic equation over $\mathbb{F}_p[x]$).

Assume $f \in \mathbb{F}_p[x, y]$ is monic in y. Then (starting point):

$$B := \{1, y, y^2, \ldots, y^{n-1}\} \subset \mathcal{O}_A.$$

B is a basis of $\mathcal{O}_A \iff f$ has no singularities in A.

Integral basis and singularities

Assume f monic in y, so $\mathbb{F}[x,y] \subseteq \mathcal{O}_A$

If $g \in \mathcal{O}_A$ and d is the smallest polynomial in $\mathbb{F}_p[x]$ for which $d \cdot g \in \mathbb{F}[x,y]$ then d is the *denominator* of g.

α is a root of a denominator of an element of $\mathcal{O}_A$
$\iff$
α is the x-coordinate of a singular point
$\implies$
α is a root of multiplicity $\geqslant 2$ of the discriminant $\mathrm{Res}_y(f, \frac{\partial f}{\partial y})$

Step 1: Square-free factor the discriminant. Then determine all irreducible factors of multiplicity $\geqslant 2$. These are the only factors that can appear in a denominator.

Local integral basis

For d irreducible with $d^2|\text{disc}$ we need a *local integral basis*:

a basis of all $g \in \mathcal{O}_A$ whose denominator is a power of d.

Basic overview (for notational convenience take $d = x$):

1. $b_1, \ldots, b_n := 1, y, \ldots, y^{n-1}$.
2. Find, if it exists (if not, then done), an $\mathbb{F}_p$-linear combination s of $b_1, \ldots, b_n$ for which $s/x \in \mathcal{O}_A$.
3. Replace a suitable b_i by s/x.
4. Back to step 2.

Main task: step 2.

Matrix of a basis

Start: $B = b_1, \ldots, b_n = 1, y, \ldots, y^{n-1}$.

Let M_B be the n by n matrix over $\mathbb{F}_p(x)$ for which

$$\begin{pmatrix} b_1^p \\ \vdots \\ b_n^p \end{pmatrix} = M_B \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$

Lemma: If M_B has entries in $\mathbb{F}_p[x]$ then $b_1, \ldots, b_n \in \mathcal{O}_A$.

Proof: If there is a pole in A among $b_1, \ldots, b_n$ then the pole order for $b_1^p, \ldots, b_n^p$ must be higher!
(that contradicts M_B having entries in $\mathbb{F}_p[x]$).

Linear algebra

$$\begin{pmatrix} b_1^p \\ \vdots \\ b_n^p \end{pmatrix} = M_B \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$

Goal: find $c_1, \ldots, c_{k-1} \in \mathbb{F}_p$ such that

$$\frac{b_k - (c_1 b_1 + \cdots + c_{k-1} b_{k-1})}{x} \in \mathcal{O}_A$$

Idea: $b \mapsto b^p$ is an $\mathbb{F}_p$-linear, so an equivalent problem is to use matrix M_B to search for $c_1, \ldots, c_{k-1} \in \mathbb{F}_p$ such that

$$b_k^p - (c_1 b_1^p + \cdots + c_{k-1} b_{k-1}^p)$$

is divisible by x^p. $\implies$ $\mathbb{F}_p$-linear equations for the c_i.

Algorithm (stated locally for the factor x)

1. Construct M_B for $B := 1, y, \ldots, y^{n-1}$.
2. Read off linear equations for the c_i. If no solution: local basis is done.
3. If there is a solution, then replace b_k by $b_k - (c_1 b_1 + \cdots + c_{k-1} b_{k-1})$ and adjust M_B accordingly (with elementary row and column operations).
4. Replace b_k by b_k / x and adjust M_B accordingly (multiply the k'th column by x, and divide the k'th row by x^p).
5. Return to step 2.

The algorithm is almost the same for $\mathbb{F}_q$ with $q = p^s$, except that one obtains *twisted-linear* equations. These are turned into ordinary $\mathbb{F}_q$-linear equations with the inverse of the Frobenius.

Algorithm (treating all factors of the discriminant)

- To treat the next multiplicity $\geqslant 2$ factor of the discriminant one does not need to recompute M_B;
  simply continue with the last M_B.
- The "factor at infinity":

  For the application of finding low-degree functions, it is important to normalize $b_1, \ldots, b_n$ at infinity. This means: minimize the pole orders of $b_1, \ldots, b_n$ in A^c (they have no poles in A).
  This is almost the same as the local algorithm at $x = 0$, except that this time the linear equations come from the highest powers of x in M_B instead of the lowest powers of x.