# Genus computation of global function fields

Jens-Dietrich Bauch

Universitat Autònoma de Barcelona

**SEMINARI DE TEORIA DE NOMBRES**

28 de gener 2013, Barcelona

# Genus

**Theorem**

Let $F/k$ be a global function field. The genus $g$ of $F$ satisfies:

$$g = 1 - n - \left|[\mathcal{O}_F : A[\theta]]\right| + \left|[\mathcal{O}_{F,\infty} : A_\infty[\theta_\infty]]\right| + C_f\, n(n-1)/2$$

# Function fields

$k$ finite field

$A := k[t], \quad K := k(t), \quad$ where $t$ is an indeterminate

$v_\infty : K \to \mathbb{Z} \cup \{\infty\}$ discrete valuation at $\infty$

$A_\infty = k[t^{-1}]_{(t^{-1})}$ valuation ring of $v_\infty$

# Function fields

$k$ finite field

$A := k[t], \quad K := k(t), \quad$ where $t$ is an indeterminate

$v_\infty : K \to \mathbb{Z} \cup \{\infty\}$ discrete valuation at $\infty$

$A_\infty = k[t^{-1}]_{(t^{-1})}$ valuation ring of $v_\infty$

$f(t,x) = x^n + a_1(t)x^{n-1} + \cdots + a_n(t) \in A[x]$ irreducible separable

$F := K[x]/(f(t,x))$ algebraic function field over $k$ of degree $n$

$\mathbb{P}_F$ set of all **places** of $F/k$

$v_P : F \to \mathbb{Z} \cup \{\infty\}$ discrete valuation, which is zero on $k^*$

$\deg P = \dim_k k_P$, where $k_P$ is the residue class field of $v_P$

# Divisors

$\mathcal{D}_F$ free abelian group generated by $\mathbb{P}_F$

$D = \sum_{P \in \mathbb{P}_F} a_P \cdot P$ divisor of $F$

$\deg D := \sum_{P \in \mathbb{P}_F} a_P \cdot \deg P$

$(z) := \sum_{P \in \mathbb{P}_F} v_P(z) \cdot P$ principal divisor of $z \in F^*$

$\mathcal{L}(D) := \{a \in F^* \mid (a) \geq -D\} \cup \{0\}$ Riemann-Roch space of $D$

$\dim D := \dim_k \mathcal{L}(D)$

$g := \max\{\deg D - \dim D + 1 \mid D \in \mathcal{D}_F\}$ genus of $F$

# Genus

Let $F/k$ be a global function field. The genus $g$ of $F$ satisfies:

$$g = 1 - n - \left|[\mathcal{O}_F : A[\theta]]\right| + \left|[\mathcal{O}_{F,\infty} : A_\infty[\theta_\infty]]\right| + C_f\, n(n-1)/2$$

# Maximal orders

$\mathcal{O}_F := \mathrm{Cl}(A, F)$ **finite maximal order**

$\theta \in F$ root of $f(t, x) = x^n + a_1(t)x^{n-1} + \cdots + a_n(t)$, so that $F = k(t, \theta)$

$A[\theta]$ **finite equation order** of $f$

# Maximal orders

$\mathcal{O}_F := \mathrm{Cl}(A, F)$ **finite maximal order**

$\theta \in F$ root of $f(t,x) = x^n + a_1(t)x^{n-1} + \cdots + a_n(t)$, so that $F = k(t,\theta)$

$A[\theta]$ **finite equation order** of $f$

$\mathcal{O}_{F,\infty} := \mathrm{Cl}(A_\infty, F)$ **infinite maximal order**

$C_f := \max\{\lceil \deg a_i(t)/i \rceil \mid 1 \leq i \leq n\}$

$f_\infty(t^{-1}, x) := t^{-nC_f} f(t, t^{C_f} x) \in k[t^{-1}, x] \subset A_\infty[x]$

# Maximal orders

$\mathcal{O}_F := \mathrm{Cl}(A, F)$ **finite maximal order**

$\theta \in F$ root of $f(t,x) = x^n + a_1(t)x^{n-1} + \cdots + a_n(t)$, so that $F = k(t,\theta)$

$A[\theta]$ **finite equation order** of $f$

$\mathcal{O}_{F,\infty} := \mathrm{Cl}(A_\infty, F)$ **infinite maximal order**

$C_f := \max\{\lceil \deg a_i(t)/i \rceil \mid 1 \leq i \leq n\}$

$f_\infty(t^{-1}, x) := t^{-nC_f} f(t, t^{C_f} x) \in k[t^{-1}, x] \subset A_\infty[x]$

$\theta_\infty := \theta / t^{C_f}$ satisfies $f_\infty(t^{-1}, \theta_\infty) = 0$, so that $F = k(t^{-1}, \theta_\infty)$

$A_\infty[\theta_\infty]$ **infinite equation order** of $f_\infty$

# Genus

**Theorem**

Let $F/k$ be a global function field. The genus $g$ of $F$ satisfies:

$$g = 1 - n - \left|[\mathcal{O}_F : A[\theta]]\right| + \left|[\mathcal{O}_{F,\infty} : A_\infty[\theta_\infty]]\right| + C_f\, n(n-1)/2$$

# Indices of modules

## Definition

Let $M$ and $M'$ be two free $A$-modules (or $A_\infty$-modules) of rank $n$. The **index** $[M : M']$ is the class of $\det(T)$ in $K^*/k^*$, where $T \in \mathrm{GL}_n(K)$ is a transition matrix between a basis of $M'$ and a basis of $M$.

$v_\infty([M : M'])$ and $v_{p(t)}([M : M'])$ are uniquly defined integers.

# Indices of modules

## Definition

Let $M$ and $M'$ be two free $A$-modules (or $A_\infty$-modules) of rank $n$. The **index** $[M : M']$ is the class of $\det(T)$ in $K^*/k^*$, where $T \in \mathrm{GL}_n(K)$ is a transition matrix between a basis of $M'$ and a basis of $M$.

$v_\infty([M : M'])$ and $v_{p(t)}([M : M'])$ are uniquly defined integers.

We are interested in $v_{p(t)}([\mathcal{O}_F : A[\theta]])$ and $v_\infty([\mathcal{O}_{F,\infty} : A_\infty[\theta_\infty]])$

# The Montes algorithm

## Montes algorithm

**INPUT**

– Defining polynomial $f(t, x)$ of a global function field $F/k$
– An irreducible polynomial $p(t) \in A$

# The Montes algorithm

## Montes algorithm

**INPUT**

– Defining polynomial $f(t, x)$ of a global function field $F/k$
– An irreducible polynomial $p(t) \in A$

**OUTPUT**

– The non-negative integer $\text{ind}_{p(t)} := v_{p(t)}([\mathcal{O}_F : A[\theta]])$

# The Montes algorithm

## Montes algorithm

**INPUT**

– Defining polynomial $f(t,x)$ of a global function field $F/k$

– An irreducible polynomial $p(t) \in A$

**OUTPUT**

– The non-negative integer $\mathrm{ind}_{p(t)} := v_{p(t)}([\mathcal{O}_F : A[\theta]])$

We may apply the Montes algorithm to $f_\infty(t^{-1},x)$ and the irreducible polynomial $1/t$ of $A_\infty$. We obtain analogous the value of the integer

$$\mathrm{ind}_\infty := v_\infty([\mathcal{O}_{F,\infty} : A_\infty[\theta_\infty]]).$$

# Lattices

$| \, | : K \to \{-\infty\} \cup \mathbb{Z}, \quad |g| := -v_\infty(g), \quad$ degree function

# Lattices

$| \ | : K \to \{-\infty\} \cup \mathbb{Z}, \ \ |g| := -v_\infty(g), \ \ \text{degree function}$

## Definition

Let $E$ be a finite dimensional $K$-vector space. A **norm** on $E$ is a mapping $\| \ \| : E \longrightarrow \{-\infty\} \cup \mathbb{R}$ satisfying:

1. $\|x + y\| \leq \max\{\|x\|, \|y\|\}$, for all $x, y \in E$
2. $\|ax\| = |a| + \|x\|$, for all $a \in K$, $x \in E$
3. $\|x\| = -\infty$ if and only if $x = 0$.

# Lattices

$| \ | : K \to \{-\infty\} \cup \mathbb{Z}, \ \ |g| := -v_\infty(g), \ \ \text{degree function}$

## Definition

Let $E$ be a finite dimensional $K$-vector space. A **norm** on $E$ is a mapping $\| \ \| : E \longrightarrow \{-\infty\} \cup \mathbb{R}$ satisfying:

1. $\|x + y\| \leq \max\{\|x\|, \|y\|\}$, for all $x, y \in E$
2. $\|ax\| = |a| + \|x\|$, for all $a \in K$, $x \in E$
3. $\|x\| = -\infty$ if and only if $x = 0$.

## Definition

A **lattice** $L$ over $A$ is an $A$-submodule of full rank of $E$ equipped with a **norm** such that

$$\dim_k\{x \in L \mid \|x\| \leq r\} < \infty, \ \text{for each } r \in \mathbb{R}.$$

# Reduced bases, orthonormal bases and determinant

## Definition

A $K$-basis $\mathcal{B} = \{b_1, \ldots, b_n\}$ of $(E, \| \ \|)$ is **reduced** if
$$\|a_1 b_1 + \cdots + a_n b_n\| = \max_{1 \leq i \leq n} \{\|a_i b_i\|\}, \quad \forall\, a_1, \ldots, a_n \in A.$$

A reduced basis of $E$ is **orthonormal** if $-1 < \|b\| \leq 0, \ \forall b \in \mathcal{B}$.

Let $L$ be a lattice in $E$. The **determinant** $d(L) \in K^*/A_\infty^*$ is the determinant of the transition matrix from any basis of $L$ to any orthonormal basis of $E$.

# Reduced bases, orthonormal bases and determinant

## Definition

A $K$-basis $\mathcal{B} = \{b_1, \ldots, b_n\}$ of $(E, \| \ \|)$ is **reduced** if

$$\|a_1 b_1 + \cdots + a_n b_n\| = \max_{1 \leq i \leq n} \{\|a_i b_i\|\}, \quad \forall\, a_1, \ldots, a_n \in A.$$

A reduced basis of $E$ is **orthonormal** if $-1 < \|b\| \leq 0, \ \forall b \in \mathcal{B}$.

Let $L$ be a lattice in $E$. The **determinant** $d(L) \in K^*/A_\infty^*$ is the determinant of the transition matrix from any basis of $L$ to any orthonormal basis of $E$.

## Theorem

1. Every lattice admits a reduced basis.
2. If $\mathcal{B} = \{b_1, \ldots, b_n\}$ is a reduced basis of $L$, then
$$|d(L)| = \sum_{1 \leq i \leq n} \lceil \|b_i\| \rceil.$$

# Riemann-Roch theory and lattices

Consider $(F, \| \ \|)$ with the norm:

$$\|z\| = -\min_{P \in \mathbb{P}_\infty} \{v_P(z)/e(P/\infty)\}.$$

$(\mathcal{O}_F, \| \ \|)$ is a lattice.

# Riemann-Roch theory and lattices

Consider $(F, \| \ \|)$ with the norm:

$$\|z\| = -\min_{P \in \mathbb{P}_\infty} \{v_P(z)/e(P/\infty)\}.$$

$(\mathcal{O}_F, \| \ \|)$ is a lattice.

**Theorem**

Let $\mathcal{B} := \{b_1, \ldots, b_n\}$ be a reduced basis of $\mathcal{O}_F$. Then,

$$\dim(\mathcal{L}(0)) = \sum_{\lceil \|b_i\| \rceil \leq 0} (-\lceil \|b_i\| \rceil + 1).$$

# Riemann-Roch theory and lattices

Consider $(F, \| \ \|)$ with the norm:

$$\|z\| = -\min_{P \in \mathbb{P}_\infty} \{v_P(z)/e(P/\infty)\}.$$

$(\mathcal{O}_F, \| \ \|)$ is a lattice.

**Theorem**

Let $\mathcal{B} := \{b_1, \ldots, b_n\}$ be a reduced basis of $\mathcal{O}_F$. Then,

$$\dim(\mathcal{L}(0)) = \sum_{\lceil \|b_i\| \rceil \leq 0} (-\lceil \|b_i\| \rceil + 1).$$

In particular, $\left|d(\mathcal{O}_F)\right| = g + n - 1$.

# Riemann-Roch theory and lattices

Consider $(F, \| \ \|)$ with the norm:

$$\|z\| = -\min_{P \in \mathbb{P}_\infty} \{v_P(z)/e(P/\infty)\}.$$

$(\mathcal{O}_F, \| \ \|)$ is a lattice.

**Theorem**

Let $\mathcal{B} := \{b_1, \ldots, b_n\}$ be a reduced basis of $\mathcal{O}_F$. Then,

$$\dim(\mathcal{L}(0)) = \sum_{\lceil \|b_i\| \rceil \leq 0} (-\lceil \|b_i\| \rceil + 1).$$

In particular, $\left|d(\mathcal{O}_F)\right| = g + n - 1$.

$$\left|d(\mathcal{O}_F)\right| = -\left|[\mathcal{O}_F : A[\theta]]\right| + \left|[\mathcal{O}_{F,\infty} : A_\infty[\theta_\infty]]\right| + C_f n(n-1)/2$$

# Genus

**Theorem**

Let $F/k$ be a global function field. The genus $g$ of $F$ satisfies:

$$g = 1 - n - \left|[\mathcal{O}_F : A[\theta]]\right| + \left|[\mathcal{O}_{F,\infty} : A_\infty[\theta_\infty]]\right| + C_f\, n(n-1)/2$$

# Computation of the genus

**INPUT**

A global function field $F/k$ with defining polynomial $f$ of degree $n$.

**OUTPUT**

The genus $g$ of $F$.

**1.** $f_\infty \leftarrow t^{-C_f n} f(t, t^{C_f} x)$

**2.** FiniteIndex $\leftarrow 0$

**3.** Factorize $\mathrm{Disc}(f)$ in $A$

**4.** FOR all irreducible polynomials $p(t) \in A$ with $v_{p(t)}(\mathrm{Disc}(f)) \geq 2$ DO

$\quad \mathrm{ind}_{p(t)} \leftarrow \texttt{Montes}(f, p(t))$

$\quad \mathrm{FiniteIndex} \leftarrow \mathrm{FiniteIndex} + |p(t)| \cdot \mathrm{ind}_{p(t)}$

**5.** $\mathrm{ind}_\infty \leftarrow \texttt{Montes}(f_\infty, 1/t)$

**6.** **return** $1 - n - \mathrm{FiniteIndex} - \mathrm{ind}_\infty + C_f n(n-1)/2$

# Numerical tests

$$f = (x + p(t) + \cdots + p(t)^r)^n + p(t)^k \in \mathbb{F}_{37}[t, x]$$

| $g$ | $p(t)$ | $n$ | $k$ | $r$ | I.C. | Algo | Magma |
|---|---|---|---|---|---|---|---|
| 0 | $t$ | 5 | 7 | 10 | 0.0 | 0.02 | 0.39 |
| 22 | $t^3 + 2$ | 23 | 30 | 10 | 8.08 | 8.31 | 66289.34 |
| 0 | $t + 1$ | 77 | 163 | 20 | 265.4 | 267.91 | – |

# Numerical tests

$$f = (x + p(t) + \cdots + p(t)^r)^n + p(t)^k \in \mathbb{F}_{37}[t, x]$$

| $g$ | $p(t)$ | $n$ | $k$ | $r$ | I.C. | Algo | Magma |
|---|---|---|---|---|---|---|---|
| 0 | $t$ | 5 | 7 | 10 | 0.0 | 0.02 | 0.39 |
| 22 | $t^3 + 2$ | 23 | 30 | 10 | 8.08 | 8.31 | 66289.34 |
| 0 | $t + 1$ | 77 | 163 | 20 | 265.4 | 267.91 | – |

$$f = (\prod_{\alpha \in \mathbb{F}_3} (x + t\alpha)^m + t(t^2 + 1)^k)^m + t(t^2 + 1)^{3mk} \in \mathbb{F}_3[t, x]$$

| $g$ | $\deg(f)$ | $k$ | $m$ | I.C. | Algo | Magma |
|---|---|---|---|---|---|---|
| 50 | 12 | 2 | 2 | 0.01 | 0.05 | 0.82 |
| 528 | 48 | 5 | 4 | 1.13 | 3.96 | 1322.08 |
| 1136 | 75 | 7 | 5 | 9.0 | 37.9 | 15961.82 |
| 1198 | 147 | 1 | 7 | 2.60 | 80.3 | – |

# Numerical tests

$$f = (x^{l-1} + \cdots + x + 1)^m + t^k \in \mathbb{F}_q[t, x]$$

| $g$ | $q$ | $\deg f$ | $m$ | $l$ | $k$ | I.C. | Algo | Magma |
|---|---|---|---|---|---|---|---|---|
| 6 | 101 | 8 | 4 | 3 | 13 | 0.00 | 0.01 | 0.10 |
| 0 | 13 | 42 | 7 | 7 | 13 | 0.01 | 0.17 | 292.9 |
| 2 | 3 | 260 | 13 | 21 | 2 | 0.02 | 0.82 | – |
| 36 | 13 | 420 | 21 | 21 | 5 | 1.45 | 3.81 | – |

# Runtime

**Theorem**

Let $F/k$ be a function field over the finite field $k$ with $q$ elements and with defining polynomial $f$ of degree $n$. Then, the algorithm needs at most

$$O(n^{5+\epsilon} C_f^{2+\epsilon} \log(q))$$

operations in $k$ to determine the genus of $F$.