Computing integral bases of algebraic function fields

Simon Abelard

LIX, École Polytechnique
Institut Polytechnique de Paris

March 5, 2020

Algebraic function fields, integral bases

Algebraic function fields

Consider a plane curve $\mathcal{C}$ over perfect field K of equation $f(x, y) = 0$.
View $f \in K[x][y]$, monic of degree n, squarefree.
Function field $K(\mathcal{C}) = \mathrm{Frac}\,(K[x, y]/\langle f(x, y)\rangle)$.

Algebraic function fields, integral bases

Algebraic function fields

Consider a plane curve $\mathcal{C}$ over perfect field K of equation $f(x, y) = 0$.
View $f \in K[x][y]$, monic of degree n, squarefree.
Function field $K(\mathcal{C}) = \mathrm{Frac}\,(K[x, y]/\langle f(x, y)\rangle)$.

Integral elements

A function $g \in K(\mathcal{C})$ is integral (over $K[x]$) if there is a monic polynomial $\mu \in K[x][y]$ such that $\mu(g(x, y)) = 0$.

Algebraic function fields, integral bases

Algebraic function fields

Consider a plane curve $\mathcal{C}$ over perfect field K of equation $f(x, y) = 0$.
View $f \in K[x][y]$, monic of degree n, squarefree.
Function field $K(\mathcal{C}) = \mathrm{Frac}\,(K[x, y]/\langle f(x, y)\rangle)$.

Integral elements

A function $g \in K(\mathcal{C})$ is integral (over $K[x]$) if there is a monic polynomial $\mu \in K[x][y]$ such that $\mu(g(x, y)) = 0$.

Example: $1, y, \ldots, y^{n-1}$ are integral elements.
When f irreducible, integral elements form a $K[x]$-module of rank n.
A $K[x]$-basis of this module is an **integral basis**.

Motivations

- Originally: symbolic integration (Trager, 1984).
- Precomputing integral closures in Hess' algorithm for Riemann–Roch spaces (2001).
  (Geometric error-correcting codes, and arithmetic in Jacobians)
- Reduction of function fields (van Hoeij–Novocin, 2005).

Motivations

- Originally: symbolic integration (Trager, 1984).
- Precomputing integral closures in Hess' algorithm for Riemann–Roch spaces (2001).
  (Geometric error-correcting codes, and arithmetic in Jacobians)
- Reduction of function fields (van Hoeij–Novocin, 2005).

The following equations

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

and $h(u,v) = 3v^2 + 4u^3 + 24u + 1$ define isomorphic function fields.

Algorithms for integral bases

Algorithms updating a candidate basis until a criterion is met:

- Trager's algorithm (1984), criterion from commutative algebra. (A function field analogue of the Round 2 algorithm)
- Van Hoeij's algorithm (1995) using Puiseux series for integrality.

In both families, updating the candidate relies on linear algebra.

Algorithms for integral bases

Algorithms updating a candidate basis until a criterion is met:

- Trager's algorithm (1984), criterion from commutative algebra. (A function field analogue of the Round 2 algorithm)
- Van Hoeij's algorithm (1995) using Puiseux series for integrality.

In both families, updating the candidate relies on linear algebra.

Montes' algorithm: devised for number fields, very different approach.

Algorithms for integral bases

Algorithms updating a candidate basis until a criterion is met:

- Trager's algorithm (1984), criterion from commutative algebra. (A function field analogue of the Round 2 algorithm)
- Van Hoeij's algorithm (1995) using Puiseux series for integrality.

In both families, updating the candidate relies on linear algebra.

Montes' algorithm: devised for number fields, very different approach.

Many algorithms but very few complexity bounds in literature.
Algorithms are compared through runtimes over ad hoc examples.
No consensus, no guiding rules on which algorithm to use.

A few projects

Exploit significant contributions of computer algebra since the 90's:

- Puiseux series (characteristic $\geq n$).
  (Poteaux, Rybowicz, Weimann)
- Structured linear algebra.
  (Dumas, Giorgi, Jeannerod, Neiger, Schost, Villard and many more)

A few projects

Exploit significant contributions of computer algebra since the 90's:

- Puiseux series (characteristic $\geq n$).
  (Poteaux, Rybowicz, Weimann)
- Structured linear algebra.
  (Dumas, Giorgi, Jeannerod, Neiger, Schost, Villard and many more)

Give more precise bounds in particular cases:

- case of few singularities?
- case of low multiplicities?

A few projects

Exploit significant contributions of computer algebra since the 90's:

- Puiseux series (characteristic $\geq n$).
  (Poteaux, Rybowicz, Weimann)
- Structured linear algebra.
  (Dumas, Giorgi, Jeannerod, Neiger, Schost, Villard and many more)

Give more precise bounds in particular cases:

- case of few singularities?
- case of low multiplicities?

Provide criteria to choose which algorithm based on input features.

A few projects

Exploit significant contributions of computer algebra since the 90's:

- Puiseux series (characteristic $\geq n$).
  (Poteaux, Rybowicz, Weimann)
- Structured linear algebra.
  (Dumas, Giorgi, Jeannerod, Neiger, Schost, Villard and many more)

Give more precise bounds in particular cases:

- case of few singularities?
- case of low multiplicities?

Provide criteria to choose which algorithm based on input features.

First step: complexity analysis.

Contributions

Complexity bounds

Denote $\delta = \deg \mathrm{Disc}(f)$. So far (work in progress!):

- Trager's algorithm needs $O(n^{\omega+3}\delta)$ field operations.
- Van Hoeij's algorithm needs $\widetilde{O}\left(n^{\omega+2}\delta + n^5 + n^2 d_x\right)$ field ops, $\oplus$ factorization of $\mathrm{Disc}(f)$, time $O(\delta^{1.5}\log q + \delta \log^2 q)$ over $\mathbb{F}_q$.
- Böhm et al. in $\widetilde{O}\left(n^3\delta + n^5 + n^2 d_x\right)$, and one factorization of degree δ ? (speculative)

Particular cases: adapt strategy in case of few singularities.

Overview of van Hoeij's algorithm

There is an integral basis of the form $\left(1, \frac{Q_1(x,y)}{\Delta_1(x)}, \ldots, \frac{Q_{n-1}(x,y)}{\Delta_{n-1}(x)}\right)$ where:

- the Q_i's are in $K[x, y]$ monic in y and of degree i in y
- the Δ_i's are square factors of $\mathrm{Disc}(f) = \mathrm{Res}_y\left(f, \frac{\partial f}{\partial y}\right)$

Overview of van Hoeij's algorithm

There is an integral basis of the form $\left(1, \frac{Q_1(x,y)}{\Delta_1(x)}, \ldots, \frac{Q_{n-1}(x,y)}{\Delta_{n-1}(x)}\right)$ where:

- the Q_i's are in $K[x,y]$ monic in y and of degree i in y
- the Δ_i's are square factors of $\mathrm{Disc}(f) = \mathrm{Res}_y\left(f, \frac{\partial f}{\partial y}\right)$

Principle of van Hoeij's algorithm

Incrementally build an integral basis $(1, b_1, \ldots, b_{n-1})$
For each irreducible ϕ such that $\phi^2 | \mathrm{Disc}(f)$
  While $d \leq n-1$
    Set $b_d = y b_{d-1}$ (first guess for b_d)
    Are there $a_0, \ldots, a_{d-1}$ in $K[x]$ with $\frac{y^d + \sum_{i=0}^{d-1} a_i(x) b_i(x,y)}{\phi(x)}$ integral?
      If so, this becomes our new b_d and we repeat
      If not, increment d (i.e. we did not find a better b_d)

Puiseux series and integrality

Puiseux series and valuation

Puiseux expansions of f at $x = \alpha$: $\rho_i(x) = \sum_{j \geq 0} \rho_{i,j}(x - \alpha)^{j/\tau}$.
The n expansions ρ_i satisfy $f(x, y) = \prod_{i=1}^{n}(y - \rho_i(x))$.
Define valuations: for $b \in K(x)[y]$ $v_i(b) = \mathrm{val}(b(x, \rho_i(x)))$.
(val gives the smallest exponent with non-zero coefficient.)

Puiseux series and integrality

Puiseux series and valuation

Puiseux expansions of f at $x = \alpha$: $\rho_i(x) = \sum_{j \geq 0} \rho_{i,j}(x - \alpha)^{j/\tau}$.
The n expansions ρ_i satisfy $f(x, y) = \prod_{i=1}^{n}(y - \rho_i(x))$.
Define valuations: for $b \in K(x)[y]$ $v_i(b) = \mathrm{val}(b(x, \rho_i(x)))$.
(val gives the smallest exponent with non-zero coefficient.)

Theorem: b is (locally) integral iff for any $1 \leq i \leq n$, $v_i(b) \geq 0$.

Puiseux series and integrality

Puiseux series and valuation

Puiseux expansions of f at $x = \alpha$: $\rho_i(x) = \sum_{j \geq 0} \rho_{i,j}(x - \alpha)^{j/\tau}$.
The n expansions ρ_i satisfy $f(x, y) = \prod_{i=1}^{n}(y - \rho_i(x))$.
Define valuations: for $b \in K(x)[y]$ $v_i(b) = \mathrm{val}(b(x, \rho_i(x)))$.
(val gives the smallest exponent with non-zero coefficient.)

Theorem: b is (locally) integral iff for any $1 \leq i \leq n$, $v_i(b) \geq 0$.

Back to van Hoeij's algorithm

View $a_0, \ldots, a_{d-1}$ as unknowns, pick α a root of ϕ.
Valuative conditions:

$$\forall j, \quad v_j\left(\frac{y^d + \sum_{i=0}^{d-1} a_i b_i}{x - \alpha}\right) \geq 0,$$

Give a linear system of $\leq n^2$ equations in d variables, solve it in $K(\alpha)$.

An example: $f(x, y) = y^2 - x^3$ over $\mathbb{Q}$.

Only singularity is $(0, 0)$ and $\mathrm{Disc}(f) = -4x^3$ so $\phi(x) = x$.
Puiseux expansions at 0 : $\rho_1 = x^{3/2}$ and $\rho_2 = -x^{3/2}$.

An example: $f(x, y) = y^2 - x^3$ over $\mathbb{Q}$.

Only singularity is $(0, 0)$ and $\mathrm{Disc}(f) = -4x^3$ so $\phi(x) = x$.
Puiseux expansions at 0 : $\rho_1 = x^{3/2}$ and $\rho_2 = -x^{3/2}$.

Step 1: $d = 1$, first guess $b_1 = y$

Is there $a_0 \in \mathbb{Q}$ such that $b = \frac{y - a_0}{x}$ is integral?
We have $b(x, \rho_1) = x^{1/2} - a_0/x$ and $b(x, \rho_2) = -x^{1/2} - a_0/x$.
Both have positive valuation iff $a_0 = 0$ so we update $b_1 = y/x$.

An example: $f(x,y) = y^2 - x^3$ over $\mathbb{Q}$.

Only singularity is $(0,0)$ and $\mathrm{Disc}(f) = -4x^3$ so $\phi(x) = x$.
Puiseux expansions at 0 : $\rho_1 = x^{3/2}$ and $\rho_2 = -x^{3/2}$.

Step 1: $d = 1$, first guess $b_1 = y$

Is there $a_0 \in \mathbb{Q}$ such that $b = \frac{y - a_0}{x}$ is integral?
We have $b(x, \rho_1) = x^{1/2} - a_0/x$ and $b(x, \rho_2) = -x^{1/2} - a_0/x$.
Both have positive valuation iff $a_0 = 0$ so we update $b_1 = y/x$.

Step 2: $d = 1$, first guess $b_1 = y/x$

Repeat: is there $a_0 \in \mathbb{Q}$ such that $b = \frac{y/x - a_0}{x}$ is integral?
We have $b(x, \rho_1) = x^{-1/2} - a_0/x$ and $b(x, \rho_1) = -x^{-1/2} - a_0/x$.
The valuation of both is at best $-1/2 < 0$, we cannot divide further.

An example: $f(x,y) = y^2 - x^3$ over $\mathbb{Q}$.

Only singularity is $(0,0)$ and $\mathrm{Disc}(f) = -4x^3$ so $\phi(x) = x$.
Puiseux expansions at 0 : $\rho_1 = x^{3/2}$ and $\rho_2 = -x^{3/2}$.

Step 1: $d = 1$, first guess $b_1 = y$

Is there $a_0 \in \mathbb{Q}$ such that $b = \frac{y - a_0}{x}$ is integral?
We have $b(x, \rho_1) = x^{1/2} - a_0/x$ and $b(x, \rho_2) = -x^{1/2} - a_0/x$.
Both have positive valuation iff $a_0 = 0$ so we update $b_1 = y/x$.

Step 2: $d = 1$, first guess $b_1 = y/x$

Repeat: is there $a_0 \in \mathbb{Q}$ such that $b = \frac{y/x - a_0}{x}$ is integral?
We have $b(x, \rho_1) = x^{-1/2} - a_0/x$ and $b(x, \rho_1) = -x^{-1/2} - a_0/x$.
The valuation of both is at best $-1/2 < 0$, we cannot divide further.

Conclusion: $(1, y/x)$ is an integral basis.

Complexity analysis

For simplicity, $K = \mathbb{F}_q$ has characteristic $> n$.
Notation $d_x = \deg_x f$ and $\delta = \deg \mathrm{Disc}(f) \leq 2nd_x$.
Complexity in base field operations.

- Input size: f consists of $O(nd_x)$ field elements.
- Output size: $O(n^2\delta)$ field elements.
  (n basis elements, y-degree $\leq n$, x-degree $\leq \delta \leq 2nd_x$).

Complexity analysis

For simplicity, $K = \mathbb{F}_q$ has characteristic $> n$.
Notation $d_x = \deg_x f$ and $\delta = \deg \mathrm{Disc}(f) \leq 2nd_x$.
Complexity in base field operations.

- Input size: f consists of $O(nd_x)$ field elements.
- Output size: $O(n^2\delta)$ field elements.
  (n basis elements, y-degree $\leq n$, x-degree $\leq \delta \leq 2nd_x$).
- Factoring discriminant: $\widetilde{O}(\delta^{1.5} \log q + \delta \log^2 q)$ bit operations.
- Computing Puiseux expansions at all singularities: $\widetilde{O}(n^2 d_x + n^5)$.
  (Poteaux-Weimann, Kung-Traub)

Complexity analysis

For simplicity, $K = \mathbb{F}_q$ has characteristic $> n$.
Notation $d_x = \deg_x f$ and $\delta = \deg \mathrm{Disc}(f) \leq 2nd_x$.
Complexity in base field operations.

- Input size: f consists of $O(nd_x)$ field elements.
- Output size: $O(n^2\delta)$ field elements.
  (n basis elements, y-degree $\leq n$, x-degree $\leq \delta \leq 2nd_x$).
- Factoring discriminant: $\widetilde{O}(\delta^{1.5} \log q + \delta \log^2 q)$ bit operations.
- Computing Puiseux expansions at all singularities: $\widetilde{O}(n^2 d_x + n^5)$.
  (Poteaux-Weimann, Kung-Traub)
- One iteration for a factor ϕ: $\widetilde{O}(n^{\omega+1} \deg \phi)$.
- Final CRT: $\widetilde{O}(n^2\delta)$.

Complexity analysis

For simplicity, $K = \mathbb{F}_q$ has characteristic $> n$.
Notation $d_x = \deg_x f$ and $\delta = \deg \mathrm{Disc}(f) \leq 2nd_x$.
Complexity in base field operations.

- Input size: f consists of $O(nd_x)$ field elements.
- Output size: $O(n^2\delta)$ field elements.
  (n basis elements, y-degree $\leq n$, x-degree $\leq \delta \leq 2nd_x$).
- Factoring discriminant: $\widetilde{O}(\delta^{1.5} \log q + \delta \log^2 q)$ bit operations.
- Computing Puiseux expansions at all singularities: $\widetilde{O}(n^2 d_x + n^5)$.
  (Poteaux-Weimann, Kung-Traub)
- One iteration for a factor ϕ: $\widetilde{O}(n^{\omega+1} \deg \phi)$.
- Final CRT: $\widetilde{O}(n^2\delta)$.
- Overall: $\widetilde{O}\left(n^{\omega+2}\delta + n^2 d_x + n^5\right)$ field operations
  Plus one factorization of a degree-δ polynomial.

Improving the case of low multiplicities:

For simplicity, assume only singularity is $(0,0)$.
Integral basis elements are 1, $b_1 = \frac{Q_1(x,y)}{x^{e_1}}, \ldots, b_{n-1} = \frac{Q_{n-1}(x,y)}{x^{e_{n-1}}}$.
The e_i's are necessarily non-decreasing (if b_k is integral, so is yb_k).

Improving the case of low multiplicities:

For simplicity, assume only singularity is $(0,0)$.
Integral basis elements are 1, $b_1 = \frac{Q_1(x,y)}{x^{e_1}}, \ldots, b_{n-1} = \frac{Q_{n-1}(x,y)}{x^{e_{n-1}}}$.
The e_i's are necessarily non-decreasing (if b_k is integral, so is yb_k).

Idea: compute a b_i without knowing all the previous b_j's.
For $i > j$ if $e_i = e_j$ then for $j \leq k \leq i$, $b_k = y^{k-j} b_j$.
Use dichotomy to locate indices j such that $e_j > e_{j-1}$.

Example: for nodal curves, just find the first e_i equal to 1.

Improving the case of low multiplicities:

For simplicity, assume only singularity is $(0,0)$.
Integral basis elements are 1, $b_1 = \frac{Q_1(x,y)}{x^{e_1}}, \ldots, b_{n-1} = \frac{Q_{n-1}(x,y)}{x^{e_{n-1}}}$.
The e_i's are necessarily non-decreasing (if b_k is integral, so is yb_k).

Idea: compute a b_i without knowing all the previous b_j's.
For $i > j$ if $e_i = e_j$ then for $j \leq k \leq i$, $b_k = y^{k-j} b_j$.
Use dichotomy to locate indices j such that $e_j > e_{j-1}$.

Example: for nodal curves, just find the first e_i equal to 1.

Drawback: not knowing all the previous b_j's increase the cost.

Advantage: in the extreme case where multiplicities are constant,
Saves a factor $\widetilde{O}(n)$ on the number of systems to solve.

Case of few singularities, high multiplicities

For simplicity, assume only singularity is $(0, 0)$.
Integral basis elements are 1, $b_1 = \frac{Q_1(x,y)}{x^{e_1}}$, ..., $b_{n-1} = \frac{Q_{n-1}(x,y)}{x^{e_{n-1}}}$.

Case of few singularities, high multiplicities

For simplicity, assume only singularity is $(0, 0)$.
Integral basis elements are 1, $b_1 = \frac{Q_1(x,y)}{x^{e_1}}, \ldots, b_{n-1} = \frac{Q_{n-1}(x,y)}{x^{e_{n-1}}}$.

Idea: Instead of iteratively dividing by x, find e_k using binary search.
Drawback: Less systems to solve, but each system is much bigger.

Case of few singularities, high multiplicities

For simplicity, assume only singularity is $(0, 0)$.
Integral basis elements are 1, $b_1 = \frac{Q_1(x,y)}{x^{e_1}}$, ..., $b_{n-1} = \frac{Q_{n-1}(x,y)}{x^{e_{n-1}}}$.

Idea: Instead of iteratively dividing by x, find e_k using binary search.
Drawback: Less systems to solve, but each system is much bigger.

No improvement over the general bound even if only one singularity.
Possible improvement in terms run time remains to be checked.

Further improvement

Böhm et al. (2015) split using branches instead of points.
i.e. factor $f(x, y)$ in $K[[x]][y]$.

Further improvement

Böhm et al. (2015) split using branches instead of points.
i.e. factor $f(x, y)$ in $K[[x]][y]$.

Drawback: work in $K[[x]][y]/\langle f(x, y)\rangle$ instead.

Advantage: f irreducible so Puiseux series are conjugate.
Compute numerators from products of Puiseux series truncation.

Further improvement

Böhm et al. (2015) split using branches instead of points.
i.e. factor $f(x, y)$ in $K[[x]][y]$.

Drawback: work in $K[[x]][y]/\langle f(x, y)\rangle$ instead.

Advantage: f irreducible so Puiseux series are conjugate.
Compute numerators from products of Puiseux series truncation.

A HNF is computed to fall back to triangular form

$$\left(1, \frac{Q_1(x, y)}{d_1(x)}, \ldots, \frac{Q_{n-1}(x, y)}{d_{n-1}(x)}\right),$$

where the Q_i's are **polynomials**.

Comparisons and prospective

Recall $\delta = \deg \mathrm{Disc}(f)$. So far we have:

- Trager in $O(n^{\omega+3}\delta)$. (but quite pessimistic estimate)
- Van Hoeij in $\widetilde{O}\left(n^{\omega+2}\delta + n^5 + n^2 d_x\right)$,
  and one factorization of degree δ.
- Böhm et al. in $\widetilde{O}\left(n^3\delta + n^5 + n^2 d_x\right)$,
  and one factorization of degree δ ? (speculative)

Future work

- Push complexity analysis further.
- Investigate particular cases, provide guidelines.
- Experiments: run-times do not match theory.
  (Puiseux series may become the bottleneck in practice.)

Thank you !