Computing the genus of plane curves with cubic complexity in the degree

Adrien Poteaux[⋆] and Martin Weimann[✈]

⋆: CRIStAL - University of Lille

✈: GAATI - University of French Polynesia

July 16-20, 2019

ACA, Montreal

1. Genus

Genus

Definition

The ***genus*** *of an irreducible algebraic curve C is the dimension of the space of regular 1-forms on a smooth projective curve birational to C.*

- Main birational invariant of curves
- Characterizes rational curves ($g = 0$)
- Topology of Riemann surfaces ($g =$ number of handles)

$g = 0$ $g = 1$ $g = 2$

- Abel-Jacobi map $C \to \mathbb{C}^g/\Lambda$
- Canonical embedding $C \to \mathbb{P}^{g-1}$
- Hasse-Weil bounds (rational points over finite fields)

Main result

- C a **plane curve** of degree d over a perfect field $\mathbb{K}$ of **characteristic zero or greater than d**.

Theorem (Poteaux-Weimann '18)

We can compute the genus of C with $\tilde{\mathcal{O}}(d^3)$ arithmetic operations over $\mathbb{K}$.

- Improves $\tilde{\mathcal{O}}(d^7)$ of Bauch'12 (all characteristic) and $\tilde{\mathcal{O}}(d^5)$ of Poteaux-Rybowicz '15.

- Case $\mathbb{K} = \mathbb{Q}$. Monte-Carlo algorithm with *bit complexity* $\tilde{\mathcal{O}}(d^3 \log(h))$.

Strategy

1. Consider the completion $\mathcal{C} \subset \mathbb{P}^1 \times \mathbb{P}^1$ and the finite morphism

$$\begin{array}{cccc} \pi : & \mathcal{C} & \to & \mathbb{P}^1 \\ & (x, y) & \mapsto & x \end{array}$$

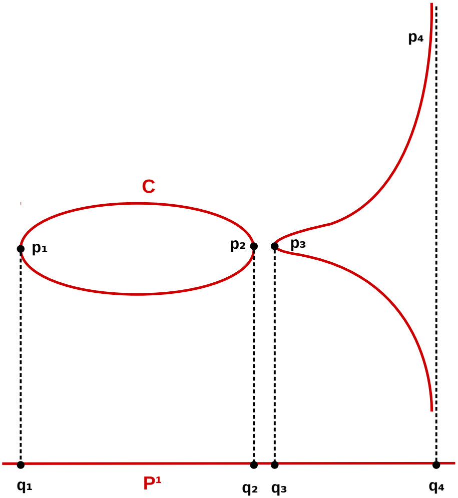
2. For all **critical** places $q \in \mathbb{P}^1$ and all places $p \in \mathcal{C}$ above q, compute :
   - Index of ramification e_p
   - Residual degree f_p

3. Apply the **Riemann-Hurwitz formula**

$$g = 1 - d_y + \frac{1}{2} \sum_q \deg(q) \sum_{p|q} f_p(e_p - 1)$$

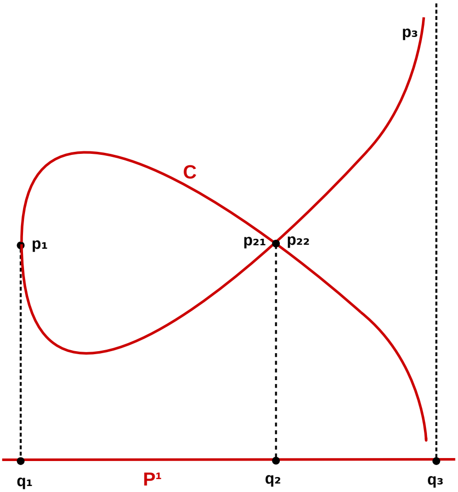
- **Main task : step 2**

$F(x, y) = y^2 - x(x-1)(x+1)$



$$\mathbf{g(C) = 1 - d_y + \frac{1}{2}\left((e_1 - 1) + (e_2 - 1) + (e_3 - 1) + (e_4 - 1)\right) = 1}$$

$F(x, y) = y^2 - x(x-1)^2$



$$g(C) = 1 - d_y + \frac{1}{2}\left((e_1 - 1) + (e_{21} - 1) + (e_{22} - 1) + (e_3 - 1)\right) = 0$$

2. A fast algorithm of Newton-Puiseux type

Rational Puiseux Expansions (above 0)

Bijective correspondence between :

- **Places** $p_1, \ldots, p_\rho$ of $\mathcal{C}$ above 0.
- **Irreducible factors** $F_1, \ldots F_\rho$ of F in $\mathbb{K}[[x]][y]$.
- **Rational Puiseux expansions** $R_1, \ldots, R_\rho$ of F above 0 :

$$R_i(T) = (\mu_i T^{e_i}, S_i(T)) \ \in \mathbb{K}_i((T))^2,$$

with e_i the index of ramification and $f_i = [\mathbb{K}_i : \mathbb{K}]$ the residual degree.

Remark

The set $(e_i, f_i)_{i=1,\ldots,\rho}$ depends only on the **singular parts** of the RPE's (suitable truncation).

Fast computation of Puiseux expansions

Denote $\delta = val_x(Res_y(F, F_y))$.

Theorem (Poteaux-Weimann '18)

Singular parts of all RPE's above 0 *within* $\tilde{\mathcal{O}}(\delta d_y)$.

Corollary

Singular parts of all RPE's above all critical places within $\tilde{\mathcal{O}}(d^3)$.

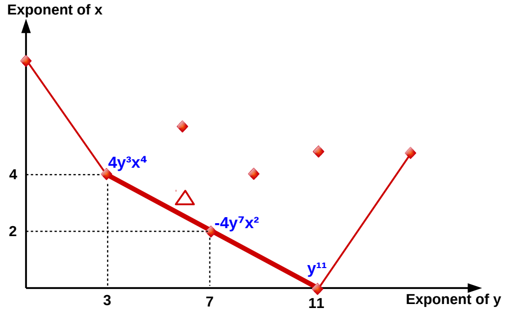
Proof of Corollary:

1. Critical places identify with prime factors q of $R = Res_y(F, F_y)$ (special care at infinity).
2. Apply previous theorem above each q. Sum over q gives $\tilde{\mathcal{O}}(\deg(R) d_y) \subset \tilde{\mathcal{O}}(d^3)$.
3. Do not factorize R (too costly) ! Use *square-free* factors and rely on dynamic evaluation.

Definition

1. *The **Newton polygon** $\mathcal{N}(F)$ is the lower convex hull of the set of exponents of F.*
2. *To each edge $\Delta \in \mathcal{N}(F)$ is attached a **characteristic polynomial** $\Phi_\Delta \in \mathbb{K}[z]$.*

$$F(x,y) = x^9 - y^6x^6 - 2y^{11}x^5 + y^{15}x^5 + y^8x^4 + \mathbf{y^{11} - 4y^7x^2 + 4y^3x^4}$$



$$F_{|\Delta} = \mathbf{y^{11} - 4y^7x^2 + 4y^3x^4} = y^3x^4 \underbrace{\left(\left(\frac{y^2}{x}\right)^4 - 4\left(\frac{y^2}{x}\right)^2 + 4\right)}_{\Phi_\Delta(z) = z^4 - 4z^2 + 4 = (z-2)^2}$$

Algorithm (Poteaux-Rybowic '15, variant of Duval '89)

*For **each edge** $\Delta = (q,m)$ of $\mathcal{N}(F)$ and **each prime factor** ϕ of Φ_Δ:*

1. $G \leftarrow F(\alpha x^q, x^m(y+\beta))$ *for some* $\alpha, \beta \in \mathbb{K}[z]/(\phi(z))$ ***(Puiseux transform)***
2. $H \leftarrow$ *Weierstrass polynomial of* G ***(Hensel lifting)***
3. $F \leftarrow H(x, y-c)$, *with* $c = \text{coeff}(H, y^{d_H-1})/d_H$ ***(Abhyankhar's trick)***
4. *Update the involved RPE*
   - *If* $F = y$ *: singular part is computed.*
   - *Else : recursive call on* F ***(Primitive elements)***

- $\rho \log(\delta)$ recursive calls
- Sharp truncation bounds
- Dynamic evaluation
- Primitive elements

$\Longrightarrow$ Complexity $\tilde{\mathcal{O}}(d^2\delta)$

Divide and conquer

Proposition

- *Truncation mod x^δ allows to compute **all** RPE's.*
- *Truncation mod $x^{2\delta/d_y}$ allows to compute at least **half** of the RPE's.*

Algorithm (Poteaux-Weimann '18)

1. *Use previous algo with precision $2\delta/d_y$ to compute at least half of the RPEs of F.*
2. *Let G be the corresponding factor of F. Compute $F = GH \mod x^{2\delta/d_y}$.*
3. *Compute $F = GH \mod x^\delta$ (generalized Hensel's lifting).*
4. *Recursive call on $H \mod x^\delta$.*

$$d_y(H) \leq d_y/2 \quad \Longrightarrow \quad \mathcal{O}(\log(d_y)) \text{ recursive calls} \quad \Longrightarrow \quad \text{Complexity } \tilde{\mathcal{O}}(\delta d_y)\ !$$

Fast factorization in $\mathbb{K}[[x]][y]$

- Suppose that $F \in \mathbb{K}[[x]][y]$ has irreducible factors $F_1, \ldots, F_\rho \in \mathbb{K}[[x]][y]$.

Theorem (Poteaux-Weimann '18)

Let $n \in \mathbb{N}$. We can compute the F_i's modulo x^n within $\tilde{\mathcal{O}}(d_y(\delta + n))$.

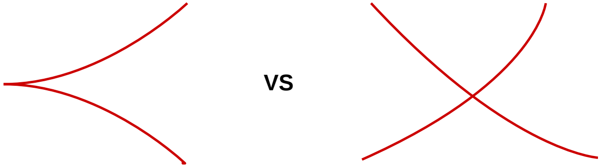
- **Proof :** Fast computation of RPE's and generalized multifactor hensel lifting.
- **Application :** Fast factorization in $\mathbb{K}[x, y]$ by recombination of the F_i's (Weimann '17)

Corollary

Irreducibility test in $\mathbb{K}[[x]][y]$ within $\tilde{\mathcal{O}}(d_y\delta)$.

- **Faster irreducibility test ?** Hopeless using Newton-Puiseux type algorithm...

Faster irreducibility test



Theorem (Poteaux-Weimann '19)

Irreducibility test in $\mathbb{K}[[x]][y]$ *with complexity* $\tilde{\mathcal{O}}(\delta)$.

- Algorithm **quasi-linear** in the size of the input
- Computes also the **equisingularity class** of the germ $(F, 0)$
- Generalizes Abhyankhar's criterion : uses **approximate roots**.

Proposition (Abhyankhar '89)

Assume F monic and let N dividing d_y. There exists a unique monic polynomial $\psi \in \mathbb{K}[[x]][y]$ such that F has ψ-adic expansion

$$F = \psi^N + a_{N-2}\psi^{N-2} + a_{N-3}\psi^{N-3} + \cdots + a_0.$$

*We call ψ the $\mathbf{N^{th}}$**-approximate root** of F.*

Algorithm (Poteaux-Weimann '19)

1. $N \leftarrow d_y$
2. *While $N > 1$:*
   1. $\psi \leftarrow N^{th}$*-approximate root*
   2. *Compute the ψ-adic Newton polygon. If not straight : Return **False***
   3. *Compute the ψ-adic characteristic polynomial. If not prime power : Return **False***
   4. $N \leftarrow N/q\deg(\phi)$ $\quad$ *($q\deg(\phi) \geq 2$)*
3. *Return **True**.*

Computations mod $x^{2\delta/d_y}$ $\Longrightarrow$ Total cost : $\tilde{\mathcal{O}}(\delta)$!

3. Last slide...

1. **Fast computation of RPE's** with various applications:
   - Desingularization of plane curves (genus, equisingularity classes, etc.)
   - Factorization in $\mathbb{K}[[x]][y]$ and $\mathbb{K}[x,y]$
   - Integral basis of function fields (Van Hoeij algorithm)
   - Regular differentials and adjoint polynomials (jacobian, parametrization)
2. **Quasi-optimal irreducibility test** in $\mathbb{K}[[x]][y]$.
3. **Ongoing research:**
   - Use approximate roots for factorization in $\mathbb{K}[[x]][y]$
     (easier implementation and better practical behaviour)
   - Generalization over local rings of arbitrary characteristic
     (try to improve the $\tilde{\mathcal{O}}(d\delta^2)$ of Guardia-Montes-Nart '08)
   - Implementation.