Computing Riemann–Roch spaces via Puiseux expansions

Elena Berardini

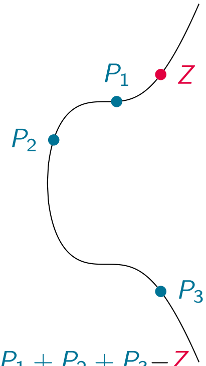
with S. Abelard (Thales), A. Couvreur (Inria), G. Lecerf (LIX)

Projet funded by the Agence de l'Innovation de Défense

Journées Nationales de Calcul Formel
1 mars 2022

Riemann–Roch spaces of curves

A divisor on a curve $\mathcal{C}$: $D = \sum_{P \in \mathcal{C}} n_P P,\ n_P \in \mathbb{Z}$



D=$P_1 + P_2 + P_3 - Z$

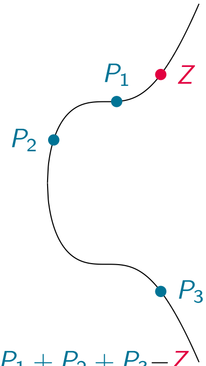
The **Riemann–Roch space** $L(D)$ is the space of functions $\frac{G}{H} \in \mathbb{K}(\mathcal{C})$ such that:

- if $n_P < 0$ then P must be a zero of G (of multiplicity $\geqslant -n_P$)
- if $n_P > 0$ then P can be a zero of H (of multiplicity $\leqslant n_P$)
- G/H has no other poles outside the points P with $n_P > 0$

Here: Z must be a zero of G, the P_i can be zeros of H

Riemann–Roch spaces of curves

A divisor on a curve $\mathcal{C}$: $D = \sum_{P \in \mathcal{C}} n_P P,\ n_P \in \mathbb{Z}$



The **Riemann–Roch space** $L(D)$ is the space of functions $\frac{G}{H} \in \mathbb{K}(\mathcal{C})$ such that:

- if $n_P < 0$ then P must be a zero of G (of multiplicity $\geqslant -n_P$)
- if $n_P > 0$ then P can be a zero of H (of multiplicity $\leqslant n_P$)
- G/H has no other poles outside the points P with $n_P > 0$

Here: Z must be a zero of G, the P_i can be zeros of H

Riemann–Roch Theorem $\rightsquigarrow$ dimension of $L(D) = \deg D + 1 - g$

where the degree of a divisor is $\deg D = \sum_P n_P \deg(P)$

Toy example

Let $\mathcal{C} = \mathbb{P}^1$, $P = [0:1]$ and $Q = [1:1]$. Let $D = P - Q$, then

$$f \in L(D) \iff \begin{cases} \text{f has a zero of order at least 1 at } Q \\ \text{f can have a pole of order at most 1 at } P \\ \text{f has not other poles outside } P \end{cases}$$

Toy example

Let $\mathcal{C} = \mathbb{P}^1$, $P = [0 : 1]$ and $Q = [1 : 1]$. Let $D = P - Q$, then

$$f \in L(D) \iff \begin{cases} \text{f has a zero of order at least 1 at } Q \\ \text{f can have a pole of order at most 1 at } P \\ \text{f has not other poles outside } P \end{cases}$$

$f = \frac{X-1}{X}$ is a solution

Toy example

Let $\mathcal{C} = \mathbb{P}^1$, $P = [0:1]$ and $Q = [1:1]$. Let $D = P - Q$, then

$$f \in L(D) \iff \begin{cases} \text{f has a zero of order at least 1 at } Q \\ \text{f can have a pole of order at most 1 at } P \\ \text{f has not other poles outside } P \end{cases}$$

$$f = \frac{X-1}{X} \text{ is a solution}$$

$$g = 0, \deg D = 0 \xrightarrow[\text{Theorem}]{\text{Riemann–Roch}} \dim L(D) = \deg D + 1 - g = 1$$

$$\rightarrow f \text{ generates the space of solutions}$$

Toy example

Let $\mathcal{C} = \mathbb{P}^1$, $P = [0:1]$ and $Q = [1:1]$. Let $D = P - Q$, then

$$f \in L(D) \iff \begin{cases} \text{f has a zero of order at least 1 at } Q \\ \text{f can have a pole of order at most 1 at } P \\ \text{f has not other poles outside } P \end{cases}$$

$$f = \frac{X-1}{X} \text{ is a solution}$$

$$g = 0, \deg D = 0 \xrightarrow[\text{Theorem}]{\text{Riemann–Roch}} \dim L(D) = \deg D + 1 - g = 1$$

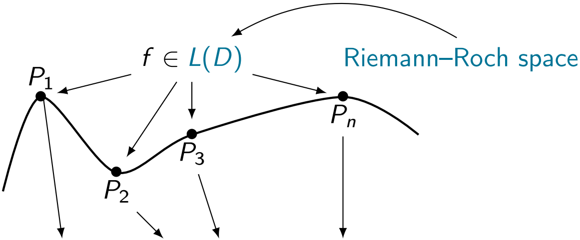
$\rightarrow f$ generates the space of solutions

⚠ no explicit method to compute a basis of $L(D)$

How do we solve the problem in general?

Riemann–Roch spaces: for what?

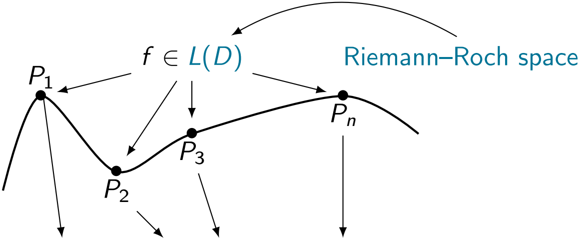
- Construction of algebraic geometry codes from curves



$$C((P_i)_i, D) := \{(f(P_1), f(P_2), f(P_3), \ldots, f(P_n)) \mid f \in L(D)\}$$

Riemann–Roch spaces: for what?

- Construction of algebraic geometry codes from curves



$$C((P_i)_i, D) := \{(f(P_1), f(P_2), f(P_3), \ldots, f(P_n)) \mid f \in L(D)\}$$

- Arithmetic operations on Jacobians of curves[1]

[1] K. Khuri-Makdisi, Mathematics of Computations, 2007

Riemann–Roch problem: state of the art

Geometric Method:
(Brill–Noether theory∼1874)

- Goppa, Le Brigand–Risler (80's)
- Huang–Ierardi (90's)
- Khuri–Makdisi (2007)
- Le Gluher–Spaenlehauer (2018)
- Abelard–Couvreur–Lecerf (2020)

Arithmetic Method:
(Ideals in function fields)

- Hensel–Landberg (1902)
- Coates (1970)
- Davenport (1981)
- Hess (2001)

Riemann–Roch problem: state of the art

Geometric Method:
(Brill–Noether theory∼1874)

- Goppa, Le Brigand–Risler (80's)
- Huang–Ierardi (90's)
- Khuri–Makdisi (2007)
- Le Gluher–Spaenlehauer (2018)
- Abelard–Couvreur–Lecerf (2020)

Arithmetic Method:
(Ideals in function fields)

- Hensel–Landberg (1902)
- Coates (1970)
- Davenport (1981)
- Hess (2001)

Ordinary/nodal curves:	Las Vegas algorithm computing $L(D)$ in sub–quadratic time
Non–ordinary curves:	⚠ no explicit complexity exponent

Brill–Noether method

Notations:

- $(H) = \sum_{P \in \mathcal{C}} \mathrm{ord}_P(H) P$ – divisor of the zeros of H with multiplicity
- $D \geqslant D' \rightsquigarrow D - D' = \sum n_P P$ with $n_P \geqslant 0 \; \forall P$ ($D - D'$ is *effective*)

Brill–Noether method

Notations:

- $(H) = \sum_{P \in \mathcal{C}} \mathrm{ord}_P(H) P$ – divisor of the zeros of H with multiplicity
- $D \geqslant D' \rightsquigarrow D - D' = \sum n_P P$ with $n_P \geqslant 0 \; \forall P$ ($D - D'$ is *effective*)

Description of $L(D)$ for $\mathcal{C} : F(X, Y, Z) = 0$ a plane projective curve.

The non–zero elements are of the form $\frac{G_i}{H}$ where

- *H satisfies $(H) \geqslant D$*
- *H vanishes at any singular point of $\mathcal{C}$ with ad hoc multiplicity*
- $\deg G_i = \deg H$, *G_i prime with F and $(G_i) \geqslant (H) - D$*

Brill–Noether method

Notations:

- $(H) = \sum_{P \in \mathcal{C}} \mathrm{ord}_P(H)P$ – divisor of the zeros of H with multiplicity
- $D \geqslant D' \rightsquigarrow D - D' = \sum n_P P$ with $n_P \geqslant 0 \ \forall P$ ($D - D'$ is *effective*)

Description of $L(D)$ for $\mathcal{C} : F(X, Y, Z) = 0$ a plane projective curve.

The non–zero elements are of the form $\frac{G_i}{H}$ where

- *H satisfies $(H) \geqslant D$*
- *H vanishes at any singular point of $\mathcal{C}$ with ad hoc multiplicity*
- $\deg G_i = \deg H$, *G_i prime with F and $(G_i) \geqslant (H) - D$*

How do we manage singular points?

Brill–Noether method

Notations:

- $(H) = \sum_{P \in \mathcal{C}} \mathrm{ord}_P(H)P$ – divisor of the zeros of H with multiplicity
- $D \geqslant D' \rightsquigarrow D - D' = \sum n_P P$ with $n_P \geqslant 0$ $\forall P$ ($D - D'$ is *effective*)

Description of $L(D)$ for $\mathcal{C} : F(X, Y, Z) = 0$ a plane projective curve.

The non–zero elements are of the form $\frac{G_i}{H}$ where

- *H satisfies $(H) \geqslant D$*
- *H vanishes at any singular point of $\mathcal{C}$ with ad hoc multiplicity*
- $\deg G_i = \deg H$, *G_i prime with F and $(G_i) \geqslant (H) - D$*

How do we manage singular points?

✓ the adjoint divisor $\mathcal{A}$ "encodes" the singular points of $\mathcal{C}$ with their multiplicities

Brill–Noether method

Notations:

- $(H) = \sum_{P \in \mathcal{C}} \mathrm{ord}_P(H)P$ – divisor of the zeros of H with multiplicity
- $D \geqslant D' \rightsquigarrow D - D' = \sum n_P P$ with $n_P \geqslant 0\ \forall P$ ($D - D'$ is *effective*)

Description of $L(D)$ for $\mathcal{C} : F(X, Y, Z) = 0$ a plane projective curve.

The non–zero elements are of the form $\frac{G_i}{H}$ where

- *H satisfies $(H) \geqslant D$*
- *H satisfies $(H) \geqslant \mathcal{A}$ (we say that "H is adjoint to the curve")*
- $\deg G_i = \deg H$, *G_i prime with F and $(G_i) \geqslant (H) - D$*

How do we manage singular points?

✓ the adjoint divisor $\mathcal{A}$ "encodes" the singular points of $\mathcal{C}$ with their multiplicities

Brill–Noether method

Notations:

- $(H) = \sum_{P \in \mathcal{C}} \mathrm{ord}_P(H) P$ – divisor of the zeros of H with multiplicity
- $D \geqslant D' \rightsquigarrow D - D' = \sum n_P P$ with $n_P \geqslant 0\ \forall P$ ($D - D'$ is *effective*)

Description of $L(D)$ for $\mathcal{C} : F(X, Y, Z) = 0$ a plane projective curve.

The non–zero elements are of the form $\frac{G_i}{H}$ where

- *H satisfies $(H) \geqslant D$*
- *H satisfies$(H) \geqslant \mathcal{A}$*
- $\deg G_i = \deg H$, *G_i prime with F and $(G_i) \geqslant (H) - D$*

How do we manage singular points?

✓ the adjoint divisor $\mathcal{A}$ "encodes" the singular points of $\mathcal{C}$ with their multiplicities

How do we represent divisors?

Brill–Noether method

Notations:

- $(H) = \sum_{P \in \mathcal{C}} \mathrm{ord}_P(H) P$ – divisor of the zeros of H with multiplicity
- $D \geqslant D' \rightsquigarrow D - D' = \sum n_P P$ with $n_P \geqslant 0 \ \forall P$ ($D - D'$ is *effective*)

Description of $L(D)$ for $\mathcal{C} : F(X, Y, Z) = 0$ a plane projective curve.

The non–zero elements are of the form $\frac{G_i}{H}$ where

- *H satisfies $(H) \geqslant D$*
- *H satisfies $(H) \geqslant \mathcal{A}$*
- $\deg G_i = \deg H$, *G_i prime with F and $(G_i) \geqslant (H) - D$*

How do we manage singular points?

✓ the adjoint divisor $\mathcal{A}$ "encodes" the singular points of $\mathcal{C}$ with their multiplicities

How do we represent divisors?

series expansions of multi–set representations $((P_i)_i, n_i)$ $\rightsquigarrow$ operations on divisors with negligible cost

Sketch of the algorithm

Input

$\mathcal{C} : F(X, Y, Z) = 0$ a plane curve of degre δ, D a smooth divisor.

Step 1 : Compute the adjoint divisor $\mathcal{A}$

Step 2 : Compute the common denominator H

Step 3 : Compute $(H) - D$

Step 4 : Compute the numerators G_i (similar to Step 2)

Output

A basis of the Riemann–Roch space $L(D)$ in terms of H and the G_i.

Sketch of the algorithm

Input

$\mathcal{C} : F(X, Y, Z) = 0$ a plane curve of degre δ, D a smooth divisor.

Step 1 : Compute the adjoint divisor $\mathcal{A}$

Step 2 : Compute the common denominator H

Step 3 : Compute $(H) - D$ ✓ $\leftarrow \tilde{O}(\delta^2 + \deg D)$

Step 4 : Compute the numerators G_i (similar to Step 2)

Output

A basis of the Riemann–Roch space $L(D)$ in terms of H and the G_i.

Sketch of the algorithm

Input

$\mathcal{C} : F(X, Y, Z) = 0$ *a plane curve of degre* δ, D *a smooth divisor.*

Step 1 : Compute the adjoint divisor $\mathcal{A}$

Step 2 : Compute the common denominator H

Step 3 : Compute $(H) - D$ ✓ $\leftarrow \tilde{O}(\delta^2 + \deg D)$

Step 4 : Compute the numerators G_i (similar to Step 2)

Output

A basis of the Riemann–Roch space $L(D)$ *in terms of* H *and the* G_i.

Warm up: adjoint divisor in the ordinary case

Definition

Let $P \in \mathrm{Sing}(\mathcal{C})$. The local adjoint divisor is

$$\mathcal{A}_P = -\sum_{\mathcal{P}|P} \mathrm{val}_{\mathcal{P}} \left(\frac{dx}{F_y(x,y,1)} \right) \mathcal{P}.$$

Warm up: adjoint divisor in the ordinary case

Definition

Let $P \in \mathrm{Sing}(\mathcal{C})$. The local adjoint divisor is

$$\mathcal{A}_P = -\sum_{\mathcal{P}|P} \mathrm{val}_{\mathcal{P}} \left(\frac{dx}{F_y(x,y,1)} \right) \mathcal{P}.$$

Let $P \in \mathrm{Sing}(\mathcal{C})$ ordinary of multiplicity m, wlog $P = (0:0:1)$. Then F locally factorises as

$$F(x,y,1) = u(x,y) \prod_{i=1}^{m} (y - \varphi_i(x))$$

with $u \in \overline{\mathbb{K}}[[x,y]]$ invertible, $\varphi_i(x) \in x\overline{\mathbb{K}}[[x]]$ and $\varphi_i'(0) \neq \varphi_j'(0)$.

Warm up: adjoint divisor in the ordinary case

Definition

Let $P \in \mathrm{Sing}(\mathcal{C})$. The local adjoint divisor is

$$\mathcal{A}_P = -\sum_{\mathcal{P}|P} \mathrm{val}_{\mathcal{P}}\left(\frac{dx}{F_y(x,y,1)}\right)\mathcal{P}.$$

Let $P \in \mathrm{Sing}(\mathcal{C})$ ordinary of multiplicity m, wlog $P = (0:0:1)$. Then F locally factorises as

$$F(x,y,1) = u(x,y)\prod_{i=1}^{m}(y - \varphi_i(x))$$

with $u \in \overline{\mathbb{K}}[[x,y]]$ invertible, $\varphi_i(x) \in x\overline{\mathbb{K}}[[x]]$ and $\varphi_i'(0) \neq \varphi_j'(0)$.

Germ of the curve parametrized by $\varphi_i(x)$ $\longleftrightarrow$ place $\mathcal{P}_i$ in the functions field $\overline{\mathbb{K}}(\mathcal{C})$

Warm up: adjoint divisor in the ordinary case

Definition

Let $P \in \mathrm{Sing}(\mathcal{C})$. The local adjoint divisor is

$$\mathcal{A}_P = -\sum_{\mathcal{P}|P} \mathrm{val}_{\mathcal{P}}\left(\frac{dx}{F_y(x,y,1)}\right)\mathcal{P}.$$

Let $P \in \mathrm{Sing}(\mathcal{C})$ ordinary of multiplicity m, wlog $P = (0:0:1)$. Then F locally factorises as

$$F(x,y,1) = u(x,y)\prod_{i=1}^{m}(y-\varphi_i(x))$$

with $u \in \overline{\mathbb{K}}[[x,y]]$ invertible, $\varphi_i(x) \in x\overline{\mathbb{K}}[[x]]$ and $\varphi_i'(0) \neq \varphi_j'(0)$.

Germ of the curve parametrized by $\varphi_i(x)$	$\longleftrightarrow$	place $\mathcal{P}_i$ in the functions field $\overline{\mathbb{K}}(\mathcal{C})$

The *local adjoint divisor* becomes

$$\mathcal{A}_P = (m-1)\sum_{i=1}^{m}\mathcal{P}_i.$$

Adjoint condition via Puiseux series

Let $F \in \mathbb{K}[x, y]$ be absolutely irreducible, monic in y and of degree d in y. $F \in \mathbb{K}((x))[y]$ has d distinct roots in $\overline{\mathbb{K}}\langle\langle x\rangle\rangle$, $\varphi_1, \ldots, \varphi_d$, and writes as

$$F = \prod_{i=1}^{d}(y - \varphi_i) = \prod_{i=1}^{d}\left(y - \sum_{j=n}^{\infty}\beta_{i,j}x^{j/e_i}\right).$$

Adjoint condition via Puiseux series

Let $F \in \mathbb{K}[x, y]$ be absolutely irreducible, monic in y and of degree d in y. $F \in \mathbb{K}((x))[y]$ has d distinct roots in $\overline{\mathbb{K}}\langle\langle x\rangle\rangle$, $\varphi_1, \dots, \varphi_d$, and writes as

$$F = \prod_{i=1}^{d}(y - \varphi_i) = \prod_{i=1}^{d}\left(y - \sum_{j=n}^{\infty}\beta_{i,j}x^{j/e_i}\right).$$

We fix φ of degree e, ζ a primitive e-th root of unity. For $0 \leqslant k < e$ we can construct other e Puiseux series by replacing $x^{1/e}$ with $\zeta^k x^{1/e}$.

Adjoint condition via Puiseux series

Let $F \in \mathbb{K}[x, y]$ be absolutely irreducible, monic in y and of degree d in y. $F \in \mathbb{K}((x))[y]$ has d distinct roots in $\overline{\mathbb{K}}\langle\langle x \rangle\rangle$, $\varphi_1, \ldots, \varphi_d$, and writes as

$$F = \prod_{i=1}^{d}(y - \varphi_i) = \prod_{i=1}^{d}\left(y - \sum_{j=n}^{\infty} \beta_{i,j} x^{j/e_i}\right).$$

We fix φ of degree e, ζ a primitive e-th root of unity. For $0 \leqslant k < e$ we can construct other e Puiseux series by replacing $x^{1/e}$ with $\zeta^k x^{1/e}$. They are all equivalent and represented by...

Definition

A Rational Puiseux Expansion (RPE) is a pair $(X(t), Y(t)) = \left(\gamma t^e, \sum_{j=n}^{\infty} \beta_j t^j\right)$ *such that* $F(X(t), Y(t)) = 0$.

Adjoint condition via Puiseux series

Let $F \in \mathbb{K}[x, y]$ be absolutely irreducible, monic in y and of degree d in y. $F \in \mathbb{K}((x))[y]$ has d distinct roots in $\overline{\mathbb{K}}\langle\langle x \rangle\rangle$, $\varphi_1, \ldots, \varphi_d$, and writes as

$$F = \prod_{i=1}^{d}(y - \varphi_i) = \prod_{i=1}^{d}\left(y - \sum_{j=n}^{\infty}\beta_{i,j}x^{j/e_i}\right).$$

We fix φ of degree e, ζ a primitive e-th root of unity. For $0 \leqslant k < e$ we can construct other e Puiseux series by replacing $x^{1/e}$ with $\zeta^k x^{1/e}$. They are all equivalent and represented by...

Definition

A Rational Puiseux Expansion (RPE) is a pair $(X(t), Y(t)) = \left(\gamma t^e, \sum_{j=n}^{\infty}\beta_j t^j\right)$ *such that* $F(X(t), Y(t)) = 0$.

Rational Puiseux Expansion of $F(x, y, 1)$	$\longleftrightarrow$	places of $\overline{\mathbb{K}}(\mathcal{C})$ in the chart $z = 1$

Adjoint condition via Puiseux series

Let $F \in \mathbb{K}[x, y]$ be absolutely irreducible, monic in y and of degree d in y. $F \in \mathbb{K}((x))[y]$ has d distinct roots in $\overline{\mathbb{K}}\langle\langle x \rangle\rangle$, $\varphi_1, \ldots, \varphi_d$, and writes as

$$F = \prod_{i=1}^{d}(y - \varphi_i) = \prod_{i=1}^{d}\left(y - \sum_{j=n}^{\infty}\beta_{i,j}x^{j/e_i}\right).$$

We fix φ of degree e, ζ a primitive e-th root of unity. For $0 \leqslant k < e$ we can construct other e Puiseux series by replacing $x^{1/e}$ with $\zeta^k x^{1/e}$. They are all equivalent and represented by...

Definition

A Rational Puiseux Expansion (RPE) is a pair $(X(t), Y(t)) = \left(\gamma t^e, \sum_{j=n}^{\infty}\beta_j t^j\right)$ *such that* $F(X(t), Y(t)) = 0$.

Rational Puiseux Expansion of $F(x, y, 1)$ $\longleftrightarrow$ places of $\overline{\mathbb{K}}(\mathcal{C})$ in the chart $z = 1$

⚠ the RPE are often defined over an extension of $\mathbb{K}$.
It is an algorithmic question to take the minimal extension of the field.

The adjoint divisor

Let $P \in \mathrm{Sing}(\mathcal{C})$ ~~ordinary~~, wlog $P = (0 : 0 : 1)$. Then F locally factorises as

$$F(x, y, 1) = u(x, y) \prod_{i=1}^{m} (y - \varphi_i(x))$$

with $u \in \mathbb{K}[[x, y]]$ invertible and φ_i Puiseux series of $F \in \overline{\mathbb{K}}[[x]][y]$.

The adjoint divisor

Let $P \in \mathrm{Sing}(\mathcal{C})$ ~~ordinary~~, wlog $P = (0:0:1)$. Then F locally factorises as

$$F(x, y, 1) = u(x, y) \prod_{i=1}^{m} (y - \varphi_i(x))$$

with $u \in \mathbb{K}[[x, y]]$ invertible and φ_i Puiseux series of $F \in \overline{\mathbb{K}}[[x]][y]$.

$\{\varphi_1, \ldots, \varphi_m\}$ $\rightsquigarrow$ RPEs/places $(X_i(t), Y_i(t))$
$i \in \{1, \ldots, s\}$, $s \leqslant m$

The adjoint divisor

Let $P \in \mathrm{Sing}(\mathcal{C})$ ~~ordinary~~, wlog $P = (0:0:1)$. Then F locally factorises as

$$F(x,y,1) = u(x,y)\prod_{i=1}^{m}(y-\varphi_i(x))$$

with $u \in \mathbb{K}[[x,y]]$ invertible and φ_i Puiseux series of $F \in \overline{\mathbb{K}}[[x]][y]$.

$\{\varphi_1,\ldots,\varphi_m\}$ $\rightsquigarrow$ RPEs/places $(X_i(t), Y_i(t))$
$i \in \{1,\ldots,s\}$, $s \leqslant m$

The local adjoint divisor becomes

$$\mathcal{A}_P = -\sum_{\mathcal{P}|P} \mathrm{val}_t\left(\frac{et^{e-1}}{F_y(X(t),Y(t),1)}\right)\mathcal{P}.$$

The adjoint divisor

Let $P \in \mathrm{Sing}(\mathcal{C})$ ~~ordinary~~, wlog $P = (0:0:1)$. Then F locally factorises as

$$F(x,y,1) = u(x,y)\prod_{i=1}^{m}(y-\varphi_i(x))$$

with $u \in \mathbb{K}[[x,y]]$ invertible and φ_i Puiseux series of $F \in \overline{\mathbb{K}}[[x]][y]$.

$\{\varphi_1,\ldots,\varphi_m\}$ $\rightsquigarrow$ RPEs/places $(X_i(t), Y_i(t))$, $i \in \{1,\ldots,s\}$, $s \leqslant m$

The local adjoint divisor becomes

$$\mathcal{A}_P = -\sum_{\mathcal{P}|P} \mathrm{val}_t\left(\frac{et^{e-1}}{F_y(X(t),Y(t),1)}\right)\mathcal{P}.$$

In practice: algorithm for computing Puiseux series[2]

$\rightsquigarrow \mathcal{A}$ computed with $\tilde{O}(\delta^3)$ operations

[2] A. Poteaux et M. Weimann, Annales Herni Lebesgue, 2021

Sketch of the algorithm

Input

$\mathcal{C} : F(X, Y, Z) = 0$ *a plane curve of degree* δ, D *a smooth divisor* .

Step 1 : Compute the adjoint divisor $\mathcal{A}$ ✓ $\leftarrow \tilde{O}(\delta^3)$

Step 2 : Compute the common denominator H

Step 3 : Compute $(H) - D$ ✓ $\leftarrow \tilde{O}(\delta^2 + \deg D)$

Step 4 : Compute the numerators G_i (similar to Step 2)

Output

A basis of the Riemann–Roch space $L(D)$ *in terms of* H *and the* G_i.

Sketch of the algorithm

Input

$\mathcal{C} : F(X, Y, Z) = 0$ a plane curve of degree δ, D a smooth divisor .

Step 1 : Compute the adjoint divisor $\mathcal{A}$ ✓ $\leftarrow \tilde{O}(\delta^3)$

Step 2 : Compute the common denominator H

Step 3 : Compute $(H) - D$ ✓ $\leftarrow \tilde{O}(\delta^2 + \deg D)$

Step 4 : Compute the numerators G_i (similar to Step 2)

Output

A basis of the Riemann–Roch space $L(D)$ in terms of H and the G_i.

Find a denominator in practice

Classical linear algebra

Let $d := \deg H$.

$$\text{Condition } (H) \geqslant \mathcal{A} + D$$

$\rightsquigarrow$ linear system with $\deg \mathcal{A} + \deg D \sim \delta^2 + \deg D$ equations

$\rightsquigarrow$ Gauss elimination costs

$$\tilde{O}((d\delta + \delta^2 + \deg D)^\omega) \text{ operations in } \mathbb{K}$$

Find a denominator in practice

Classical linear algebra

Let $d := \deg H$.

$$\text{Condition } (H) \geqslant \mathcal{A} + D$$

$\rightsquigarrow$ linear system with $\deg \mathcal{A} + \deg D \sim \delta^2 + \deg D$ equations

$\rightsquigarrow$ Gauss elimination costs

$$\tilde{O}((d\delta + \delta^2 + \deg D)^\omega) \text{ operations in } \mathbb{K}$$

How big is d?

We showed that $d = \left\lceil \frac{(\delta-1)(\delta-2)+\deg D}{\delta} \right\rceil$ is enough

$\rightsquigarrow$ denominator computed with $\tilde{O}((\delta^2 + \deg D)^\omega)$ operations in $\mathbb{K}$

Second method: structured linear algebra

Condition $(H) \geqslant \mathcal{A}$

$$\rightsquigarrow \mathrm{val}_t(H(X(t), Y(t), 1) \geqslant \mathrm{val}_t\left(\frac{et^{e-1}}{F_y(X(t), Y(t), 1)}\right)$$

(similar equations for the condition $(H) \geqslant D$)

The space of polynomials $H(x, y, 1)$ that satisfy these conditions is a $\mathbb{K}[x]$–module

$\rightsquigarrow$ Computing a basis[3] costs $\tilde{O}((\delta^2 + \deg D)^\omega)$ operations

[3] C.-P. Jeannerod, V. Neiger, É. Schost et G. Villard, J. Symbolic Comput. 2017

Second method: structured linear algebra

Condition $(H) \geqslant \mathcal{A}$

$$\rightsquigarrow \mathrm{val}_t(H(X(t), Y(t), 1) \geqslant \mathrm{val}_t \left(\frac{et^{e-1}}{F_y(X(t), Y(t), 1)} \right)$$

(similar equations for the condition $(H) \geqslant D$)

The space of polynomials $H(x, y, 1)$ that satisfy these conditions is a $\mathbb{K}[x]$–module

$\rightsquigarrow$ Computing a basis[3] costs $\tilde{O}((\delta^2 + \deg D)^\omega)$ operations

Same complexity exponent but...

Advantages:

- better complexity exponent on algebraically closed fields
- potential improvement in the futur

[3] C.-P. Jeannerod, V. Neiger, É. Schost et G. Villard, J. Symbolic Comput. 2017

Sketch of the algorithm

Input

$\mathcal{C} : F(X, Y, Z) = 0$ *a plane curve of degree* δ, D *a smooth divisor .*

Step 1 : Compute the adjoint divisor $\mathcal{A}$ ✓ $\leftarrow \tilde{O}(\delta^3)$

Step 2 : Compute the common denominator H ✓ $\leftarrow \tilde{O}((\delta^2 + \deg D)^\omega)$

Step 3 : Compute $(H) - D$ ✓ $\leftarrow \tilde{O}(\delta^2 + \deg D)$

Step 4 : Compute the numerators G_i (similar to Step 2)

Output

A basis of the Riemann–Roch space $L(D)$ *in terms of* H *and the* G_i*.*

Sketch of the algorithm

Input

$\mathcal{C} : F(X, Y, Z) = 0$ a plane curve of degree δ, D a smooth divisor .

Step 1 : Compute the adjoint divisor $\mathcal{A}$ ✓ $\leftarrow \tilde{O}(\delta^3)$

Step 2 : Compute the common denominator H ✓ $\leftarrow \tilde{O}((\delta^2 + \deg D)^\omega)$

Step 3 : Compute $(H) - D$ ✓ $\leftarrow \tilde{O}(\delta^2 + \deg D)$

Step 4 : Compute the numerators G_i ✓ $\leftarrow \tilde{O}((\delta^2 + \deg D)^\omega)$

Output

A basis of the Riemann–Roch space $L(D)$ in terms of H and the G_i.

Theorem (Abelard, B., Couvreur, Lecerf – preprint 2021)

The previous algorithm computes $L(D)$ with $\tilde{\mathcal{O}}((\delta^2 + \deg D)^\omega)$ operations in $\mathbb{K}$.

What to take away?

1. Brill–Noether method $\rightsquigarrow$ necessary and sufficient conditions on G and H such that $G/H \in L(D)$
2. Puiseux series $\rightsquigarrow$ management of *non–ordinary* singular points of the curve
3. Linear Algebra $\rightsquigarrow$ Computing H and G in practice

What to take away?

1. Brill–Noether method $\rightsquigarrow$ necessary and sufficient conditions on G and H such that $G/H \in L(D)$
2. Puiseux series $\rightsquigarrow$ management of *non–ordinary* singular points of the curve
3. Linear Algebra $\rightsquigarrow$ Computing H and G in practice

Main result

Las Vegas algorithm computing $L(D)$ with $\tilde{\mathcal{O}}((\delta^2 + \deg D)^\omega)$ operations.

Future questions

- Computing Riemann–Roch spaces of non–ordinary curves in positive “small” characteristic
- Implementing the algorithm
- Improving the complexity exponent in the non–ordinary case (sub–quadratic?)

Future questions

- Computing Riemann–Roch spaces of non–ordinary curves in positive "small" characteristic
- Implementing the algorithm
- Improving the complexity exponent in the non–ordinary case (sub–quadratic?)

Merci de votre attention !

Questions? e.berardini@tue.nl