Computing Riemann–Roch spaces for Algebraic Geometry codes

Elena Berardini
Eindhoven University of Technology

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

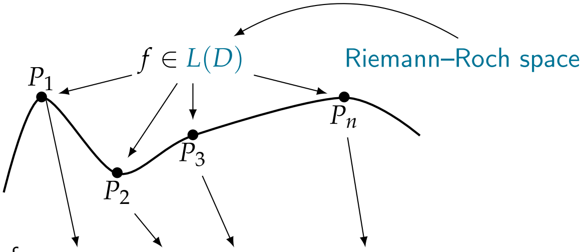
Project funded by the Agence de l'Innovation de Défense

EuroTechPostdoc2 Programme
Excellence in Science and Technology

Journées Codes et Cryptographie
11^{th} April 2022
Hendaye

Riemann–Roch spaces: for what?

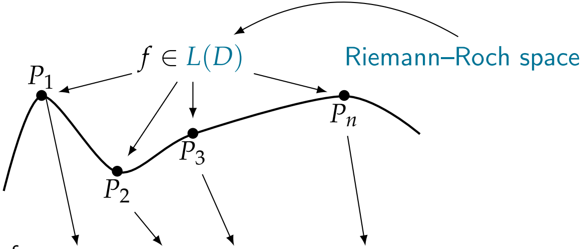
- Construction of Algebraic Geometry codes from curves (see previous talk):



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

Riemann–Roch spaces: for what?

- Construction of Algebraic Geometry codes from curves (see previous talk):



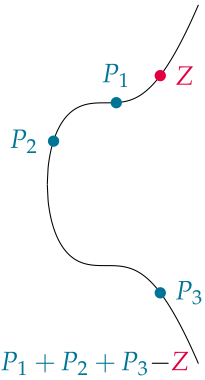
$$C((P_i)_i, D) \overset{\text{def}}{=} \{(f(P_1), f(P_2), f(P_3), \ldots, f(P_n)) \mid f \in L(D)\}$$

- Arithmetic operations on Jacobians of curves.

  📕 K. Khuri–Makdisi, Mathematics of Computations, 2007.

Riemann–Roch spaces: definition

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



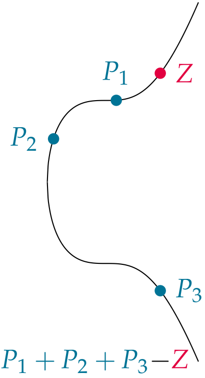
The **Riemann–Roch space** $L(D)$ is the space of functions $\frac{G}{H}$ in the function field of $\mathcal{C}$ such that:

- 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: definition

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 the function field of $\mathcal{C}$ 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 $\deg D = \sum_P n_P \deg(P)$.

Riemann–Roch space: toy example

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

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

Riemann–Roch space: toy example

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

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

$$\left.\begin{array}{r} \text{Denominator } H \text{ passes through } P: H(X,Y) \equiv 0 \mod X \\ \text{Numerator } G \text{ passes through } Q: G(X,Y) \equiv 0 \mod X-1 \end{array}\right\} \Rightarrow f = \frac{X-1}{X} \text{ is a solution.}$$

Riemann–Roch space: toy example

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

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

$$\left.\begin{array}{r} \text{Denominator } H \text{ passes through } P : H(X,Y) \equiv 0 \mod X \\ \text{Numerator } G \text{ passes through } Q : G(X,Y) \equiv 0 \mod X-1 \end{array}\right\} \Rightarrow f = \frac{X-1}{X} \text{ is a solution.}$$

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

$$\Rightarrow f \text{ generates the space of solutions.}$$

Riemann–Roch space: toy example

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

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

$$\left.\begin{array}{r} \text{Denominator } H \text{ passes through } P : H(X,Y) \equiv 0 \mod X \\ \text{Numerator } G \text{ passes through } Q : G(X,Y) \equiv 0 \mod X-1 \end{array}\right\} \Rightarrow f = \frac{X-1}{X} \text{ is a solution.}$$

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

$\Rightarrow f$ 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 problem: state of the art

Geometric Method:
(Brill–Noether theory$\sim$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)

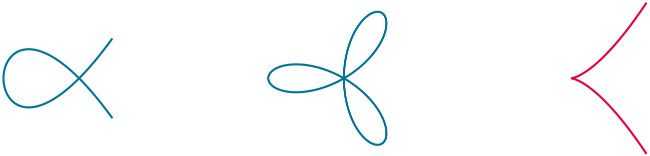
- Goppa, Le Brigand–Risler (80's)
- Huang–Ierardi (90's)
- Khuri–Makdisi (2007)
- Le Gluher–Spaenlehauer (2018)
- Abelard–Couvreur–Lecerf (2020)

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 in a nutshell

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*),
- We can alway write $D = D_+ - D_-$ with D_+, D_- effective divisors.

Brill–Noether method in a nutshell

Notations:

- $(H) = \sum_{P \in \mathcal{C}} \operatorname{ord}_P(H)P$ – 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*),
- We can alway write $D = D_+ - D_-$ with D_+, D_- effective divisors.

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 in a nutshell

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*),
- We can alway write $D = D_+ - D_-$ with D_+, D_- effective divisors.

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 deal with singular points?

Brill–Noether method in a nutshell

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*),
- We can alway write $D = D_+ - D_-$ with D_+, D_- effective divisors.

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 deal with singular points?

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

Brill–Noether method in a nutshell

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*),
- We can alway write $D = D_+ - D_-$ with D_+, D_- effective divisors.

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 deal with singular points?

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

Brill–Noether method in a nutshell

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*),
- We can alway write $D = D_+ - D_-$ with D_+, D_- effective divisors.

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 deal with 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 in a nutshell

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*),
- We can alway write $D = D_+ - D_-$ with D_+, D_- effective divisors.

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 deal with 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 with negligible cost.

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 $\mathcal{A}$.

Step 2 Compute the common denominator H.

Step 3 Compute $(H) - D$.

Step 4 Compute the numerators G_i.

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 $\mathcal{A}$.

Step 2 Compute the common denominator H.

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

Step 4 Compute the numerators G_i.

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 $\mathcal{A}$.

Step 2 Compute the common denominator H.

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

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 $\mathcal{A}$.

Step 2 Compute the common denominator H.

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

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.

The adjoint divisor via Puiseux series

Definition

Let $P \in \mathrm{Sing}(\mathcal{C})$. *The local adjoint divisor is* $\mathcal{A}_P = -\sum_{\mathcal{P}|P} \mathrm{val}_{\mathcal{P}}\left(\frac{dx}{F_y(x,y,1)}\right)\mathcal{P}$.

The adjoint divisor via Puiseux series

Definition

Let $P \in \mathrm{Sing}(\mathcal{C})$. The local adjoint divisor is $\mathcal{A}_P = -\sum_{\mathcal{P}|P} \mathrm{val}_{\mathcal{P}} \left(\frac{dx}{F_y(x,y,1)} \right) \mathcal{P}$.

Ordinary case: local factorisation of F allows writing of $\mathcal{A}_P$ in a convenient manner. $\mathcal{A}_P = (m-1) \sum_{i=1}^{m} \mathcal{P}_i$

The adjoint divisor via Puiseux series

Definition

Let $P \in \operatorname{Sing}(\mathcal{C})$. The local adjoint divisor is $\mathcal{A}_P = -\sum_{\mathcal{P}|P} \operatorname{val}_{\mathcal{P}} \left(\frac{dx}{F_y(x,y,1)} \right) \mathcal{P}$.

Ordinary case: local factorisation of F allows writing of $\mathcal{A}_P$ in a convenient manner. $\mathcal{A}_P = (m-1)\sum_{i=1}^{m} \mathcal{P}_i$
Non–ordinary case: the nice local factorisation does not hold ⇝ need to find another tool.

The adjoint divisor via Puiseux series

Definition

Let $P \in \mathrm{Sing}(\mathcal{C})$. *The local adjoint divisor is* $\mathcal{A}_P = -\sum_{\mathcal{P}|P} \mathrm{val}_{\mathcal{P}}\left(\frac{dx}{F_y(x,y,1)}\right)\mathcal{P}$.

Ordinary case: local factorisation of F allows writing of $\mathcal{A}_P$ in a convenient manner. $\mathcal{A}_P = (m-1)\sum_{i=1}^{m}\mathcal{P}_i$
Non–ordinary case: the nice local factorisation does not hold ⇝ Puiseux series!

The adjoint divisor via Puiseux series

Definition

Let $P \in \mathrm{Sing}(\mathcal{C})$. The local adjoint divisor is $\mathcal{A}_P = -\sum_{\mathcal{P}|P} \mathrm{val}_{\mathcal{P}}\left(\frac{dx}{F_y(x,y,1)}\right)\mathcal{P}$.

Ordinary case: local factorisation of F allows writing of $\mathcal{A}_P$ in a convenient manner. $\mathcal{A}_P = (m-1)\sum_{i=1}^{m}\mathcal{P}_i$
Non–ordinary case: the nice local factorisation does not hold ⇝ Puiseux series!

Let $P \in \mathrm{Sing}(\mathcal{C})$, w.l.o.g. $P = (0:0:1)$. 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 the φ_i are the Puiseux series of $F \in \overline{\mathbb{K}}[[x]][y]$.

The adjoint divisor via Puiseux series

Definition

Let $P \in \operatorname{Sing}(\mathcal{C})$. The local adjoint divisor is $\mathcal{A}_P = -\sum_{\mathcal{P}|P} \operatorname{val}_{\mathcal{P}}\left(\frac{dx}{F_y(x,y,1)}\right)\mathcal{P}$.

Ordinary case: local factorisation of F allows writing of $\mathcal{A}_P$ in a convenient manner. $\mathcal{A}_P = (m-1)\sum_{i=1}^{m}\mathcal{P}_i$
Non–ordinary case: the nice local factorisation does not hold $\rightsquigarrow$ Puiseux series!

Let $P \in \operatorname{Sing}(\mathcal{C})$, w.l.o.g. $P = (0:0:1)$. 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 the φ_i are the Puiseux series of $F \in \overline{\mathbb{K}}[[x]][y]$.

$\{\varphi_1, \ldots, \varphi_m\}$

The adjoint divisor via Puiseux series

Definition

Let $P \in \operatorname{Sing}(\mathcal{C})$. The local adjoint divisor is $\mathcal{A}_P = -\sum_{\mathcal{P}|P} \operatorname{val}_{\mathcal{P}} \left(\frac{dx}{F_y(x,y,1)} \right) \mathcal{P}$.

Ordinary case: local factorisation of F allows writing of $\mathcal{A}_P$ in a convenient manner. $\mathcal{A}_P = (m-1)\sum_{i=1}^{m} \mathcal{P}_i$
Non–ordinary case: the nice local factorisation does not hold ⇝ Puiseux series!

Let $P \in \operatorname{Sing}(\mathcal{C})$, w.l.o.g. $P = (0:0:1)$. Then F locally factorises as

$$F(x,y,1) = u(x,y)\prod_{i=1}^{m}(y - \varphi_i(x)) = u(x,y)\prod_{i=1}^{s}\prod_{k=1}^{e_i}\left(y - \sum_{j=n}^{\infty}\beta_{i,j}(\zeta_i^k (x/\gamma_i)^{1/e_i})^j\right)$$

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

$\{\varphi_1,\dots,\varphi_m\} \xrightarrow[\text{root of unity}]{\zeta_i \text{ a } e_i\text{–th primitive}}$ Rational Puiseux Expansions $(X_i(t), Y_i(t))_{i\in\{1,\dots,s\}}$ of $F(x,y,1)$

The adjoint divisor via Puiseux series

Definition

Let $P \in \operatorname{Sing}(\mathcal{C})$. The local adjoint divisor is $\mathcal{A}_P = -\sum_{\mathcal{P}|P} \operatorname{val}_{\mathcal{P}}\left(\frac{dx}{F_y(x,y,1)}\right)\mathcal{P}$.

Ordinary case: local factorisation of F allows writing of $\mathcal{A}_P$ in a convenient manner. $\mathcal{A}_P = (m-1)\sum_{i=1}^{m}\mathcal{P}_i$

Non–ordinary case: the nice local factorisation does not hold ⇝ Puiseux series!

Let $P \in \operatorname{Sing}(\mathcal{C})$, w.l.o.g. $P = (0:0:1)$. Then F locally factorises as

$$F(x,y,1) = u(x,y)\prod_{i=1}^{m}(y-\varphi_i(x)) = u(x,y)\prod_{i=1}^{s}\prod_{k=1}^{e_i}\left(y - \sum_{j=n}^{\infty}\beta_{i,j}(\zeta_i^k(x/\gamma_i)^{1/e_i})^j\right)$$

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

$\{\varphi_1,\dots,\varphi_m\} \xrightarrow[\text{root of unity}]{\zeta_i \text{ a } e_i\text{–th primitive}}$ Rational Puiseux Expansions $(X_i(t),Y_i(t))_{i\in\{1,\dots,s\}}$ of $F(x,y,1)$ $\longleftrightarrow$ Places of $\overline{\mathbb{K}}(\mathcal{C})$ in the chart $z=1$

The adjoint divisor via Puiseux series

Definition

Let $P \in \operatorname{Sing}(\mathcal{C})$. The local adjoint divisor is $\mathcal{A}_P = -\sum_{\mathcal{P}|P} \operatorname{val}_{\mathcal{P}}\left(\frac{dx}{F_y(x,y,1)}\right)\mathcal{P}$.

Ordinary case: local factorisation of F allows writing of $\mathcal{A}_P$ in a convenient manner. $\mathcal{A}_P = (m-1)\sum_{i=1}^{m} \mathcal{P}_i$
Non–ordinary case: the nice local factorisation does not hold ⇝ Puiseux series!

Let $P \in \operatorname{Sing}(\mathcal{C})$, w.l.o.g. $P = (0:0:1)$. Then F locally factorises as

$$F(x,y,1) = u(x,y)\prod_{i=1}^{m}(y-\varphi_i(x)) = u(x,y)\prod_{i=1}^{s}\prod_{k=1}^{e_i}\left(y-\sum_{j=n}^{\infty}\beta_{i,j}(\zeta_i^k(x/\gamma_i)^{1/e_i})^j\right)$$

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

$\{\varphi_1,\dots,\varphi_m\} \xrightarrow[\text{root of unity}]{\zeta_i \text{ a } e_i\text{–th primitive}}$ Rational Puiseux Expansions $(X_i(t),Y_i(t))_{i\in\{1,\dots,s\}}$ of $F(x,y,1)$ $\longleftrightarrow$ Places of $\overline{\mathbb{K}}(\mathcal{C})$ in the chart $z=1$

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

The adjoint divisor via Puiseux series

Definition

Let $P \in \mathrm{Sing}(\mathcal{C})$. *The local adjoint divisor is* $\mathcal{A}_P = -\sum_{\mathcal{P}|P} \mathrm{val}_{\mathcal{P}}\left(\frac{dx}{F_y(x,y,1)}\right)\mathcal{P}$.

Ordinary case: local factorisation of F allows writing of $\mathcal{A}_P$ in a convenient manner. $\mathcal{A}_P = (m-1)\sum_{i=1}^{m}\mathcal{P}_i$
Non–ordinary case: the nice local factorisation does not hold ⇝ Puiseux series!

Let $P \in \mathrm{Sing}(\mathcal{C})$, w.l.o.g. $P = (0:0:1)$. Then F locally factorises as

$$F(x,y,1) = u(x,y)\prod_{i=1}^{m}(y - \varphi_i(x)) = u(x,y)\prod_{i=1}^{s}\prod_{k=1}^{e_i}\left(y - \sum_{j=n}^{\infty}\beta_{i,j}(\zeta_i^k(x/\gamma_i)^{1/e_i})^j\right)$$

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

$\{\varphi_1,\dots,\varphi_m\} \xrightarrow[\text{root of unity}]{\zeta_i \text{ a } e_i\text{–th primitive}}$ Rational Puiseux Expansions $(X_i(t),Y_i(t))_{i\in\{1,\dots,s\}}$ of $F(x,y,1)$ $\longleftrightarrow$ Places of $\overline{\mathbb{K}}(\mathcal{C})$ in the chart $z=1$

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

A. Poteaux and 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 $(H) - D$. ✓ $\leftarrow \tilde{O}((\delta^2 + \deg D)^2)$

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 $(H) - D$. ✓ $\leftarrow \tilde{O}((\delta^2 + \deg D)^2)$

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

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 $\tilde{O}((\deg(H)\delta + \delta^2 + \deg D_+)^\omega)$ operations in $\mathbb{K}$.

Find a denominator in practice: classical linear algebra

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 $\tilde{O}((\deg(H)\delta + \delta^2 + \deg D_+)^\omega)$ operations in $\mathbb{K}$.

How big is $\deg(H)$?

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

$\rightsquigarrow$ denominator computed with $\tilde{O}((\delta^2 + \deg D_+)^\omega)$ operations[1] in $\mathbb{K}$.

[1] $2 \leqslant \omega \leqslant 3$ is a feasible exponent for linear algebra.

Find a denominator in practice: classical linear algebra

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 $\tilde{O}((\deg(H)\delta + \delta^2 + \deg D_+)^\omega)$ operations in $\mathbb{K}$.

How big is $\deg(H)$?

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

$\rightsquigarrow$ denominator computed with $\tilde{O}((\delta^2 + \deg D_+)^\omega)$ operations[1] in $\mathbb{K}$.

Second method:

structured linear algebra $\rightsquigarrow$ same complexity exponent but hope for future improvements.

(see the paper)

[1] $2 \leqslant \omega \leqslant 3$ is a feasible exponent for linear algebra.

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 $(H) - D$. ✓ $\leftarrow \tilde{O}((\delta^2 + \deg D)^2)$

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 $(H) - D$. ✓ $\leftarrow \tilde{O}((\delta^2 + \deg D)^2)$

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 📖 Journal of Complexity 2022)

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

What to take away?

0. Implementation of AG codes ⇝ need of computing Riemann–Roch space $L(D)$.
1. Brill–Noether method ⇝ necessary and sufficient conditions on G and H such that $G/H \in L(D)$.
2. Puiseux series ⇝ handling the *non–ordinary* singular points of the curve.
3. Linear Algebra ⇝ computing H and G in practice.

What to take away?

0. Implementation of AG codes ⇝ need of computing Riemann–Roch space $L(D)$.
1. Brill–Noether method ⇝ necessary and sufficient conditions on G and H such that $G/H \in L(D)$.
2. Puiseux series ⇝ handling the *non–ordinary* singular points of the curve.
3. Linear Algebra ⇝ computing H and G in practice.

Main result

We can compute Riemann–Roch spaces of any plane curve with a good complexity exponent.

Future questions

- Computing Riemann–Roch spaces of non–ordinary curves in positive "small" characteristic.
  Main obstacle: find an alternative tool to Puiseux series.

Future questions

- Computing Riemann–Roch spaces of non–ordinary curves in positive "small" characteristic.

  Main obstacle: find an alternative tool to Puiseux series.

- Implementing the algorithm.

Future questions

- Computing Riemann–Roch spaces of non–ordinary curves in positive “small” characteristic.
  Main obstacle: find an alternative tool to Puiseux series.

- Implementing the algorithm.

- Improving the complexity exponent in the non–ordinary case.
  (Sub–quadratic as in the ordinary case?)
  Main obstacle: linear algebra.

Future questions

- Computing Riemann–Roch spaces of non–ordinary curves in positive “small” characteristic.
  Main obstacle: find an alternative tool to Puiseux series.

- Implementing the algorithm.

- Improving the complexity exponent in the non–ordinary case.
  (Sub–quadratic as in the ordinary case?)
  Main obstacle: linear algebra.

- Can we develop a "Brill–Noether" theory for computing Riemann–Roch spaces of surfaces?

Future questions

- Computing Riemann–Roch spaces of non–ordinary curves
  in positive "small" characteristic.
  Main obstacle: find an alternative tool to Puiseux series.

- Implementing the algorithm.

- Improving the complexity exponent in the non–ordinary case.
  (Sub–quadratic as in the ordinary case?)
  Main obstacle: linear algebra.

- Can we develop a "Brill–Noether" theory
  for computing Riemann–Roch spaces of surfaces?

Future questions

- Computing Riemann–Roch spaces of non–ordinary curves in positive “small” characteristic.
  Main obstacle: find an alternative tool to Puiseux series.
- Implementing the algorithm.
- Improving the complexity exponent in the non–ordinary case.
  (Sub–quadratic as in the ordinary case?)
  Main obstacle: linear algebra.
- Can we develop a "Brill–Noether" theory for computing Riemann–Roch spaces of surfaces?

Thank you for your attention!

Questions? e.berardini@tue.nl