

# *Calcul d'espaces de Riemann–Roch pour les codes géométriques*

Elena Berardini

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

Projet financé par l'Agence de l'Innovation de Défense



Séminaire Calcul Formel  
10 mars 2022

*I. Introduction aux codes géométriques (motivation)*

*II. Introduction aux espaces de Riemann–Roch*

*III. Calcul d'espaces de Riemann–Roch*

*IV. Questions futures*

## Codes linéaires : des codes de Reed–Solomon...

Code linéaire :  $\mathbb{F}_q$ -sous espace vectoriel de  $\mathbb{F}_q^n$

$[n, k, d]$ -code : code de longueur  $n$ , dimension  $k$  et distance minimale  $d$

**Borne de Singleton** :  $k + d \leq n + 1$

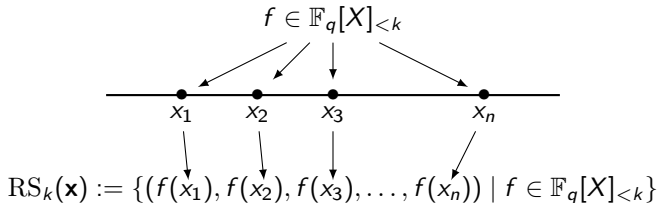
## Codes linéaires : des codes de Reed–Solomon...

Code linéaire :  $\mathbb{F}_q$ -sous espace vectoriel de  $\mathbb{F}_q^n$

$[n, k, d]$ -code : code de longueur  $n$ , dimension  $k$  et distance minimale  $d$

**Borne de Singleton** :  $k + d \leq n + 1$

**Codes de Reed–Solomon (codes RS) :**



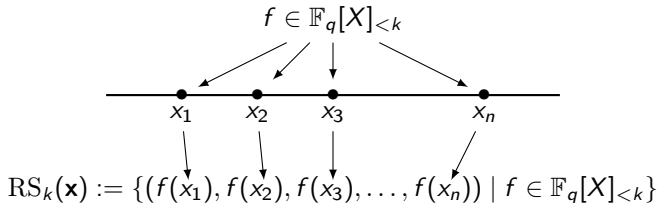
## Codes linéaires : des codes de Reed–Solomon...

Code linéaire :  $\mathbb{F}_q$ -sous espace vectoriel de  $\mathbb{F}_q^n$

$[n, k, d]$ -code : code de longueur  $n$ , dimension  $k$  et distance minimale  $d$

**Borne de Singleton** :  $k + d \leq n + 1$

**Codes de Reed–Solomon (codes RS) :**



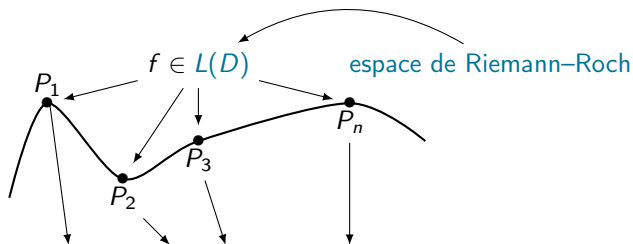
✓ Paramètres optimaux :  $k + d = n + 1$  (codes MDS)

✓ Algorithme de décodage efficace (Berlekamp, 1968)

✓ Opérations sur les données

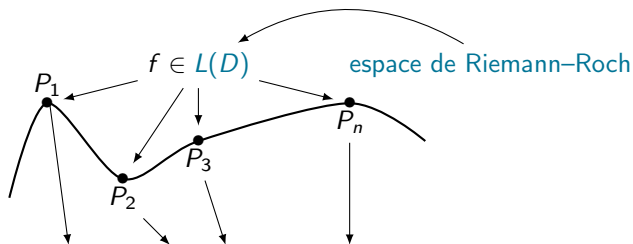
⚠ Inconvénient :  $n \leq q$

...aux codes géométriques (codes AG)



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

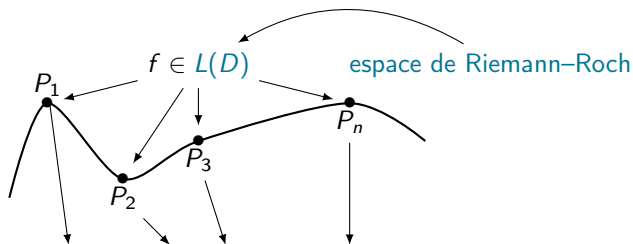
...aux codes géométriques (codes AG)



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

Longueur :  $|\#C(\mathbb{F}_q) - (q + 1)| \leq g \lfloor 2\sqrt{q} \rfloor$

## ...aux codes géométriques (codes AG)



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

Longueur :  $|\#\mathcal{C}(\mathbb{F}_q) - (q + 1)| \leq g \lfloor 2\sqrt{q} \rfloor$

### Proposition

Les paramètres  $[n, k, d]$  des codes géométriques satisfont

$$n + 1 - g \leq k + d \leq n + 1.$$

$\rightsquigarrow$  les codes AG sont à distance  $g$  de l'optimalité



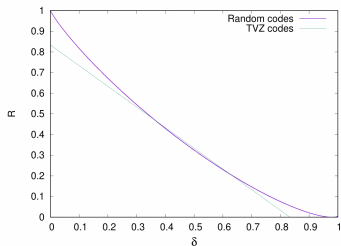
## *Bref histoire des codes géométriques*

*1981:* Goppa introduit les codes AG sur les courbes algébriques

## Bref histoire des codes géométriques

1981: Goppa introduit les codes AG sur les courbes algébriques

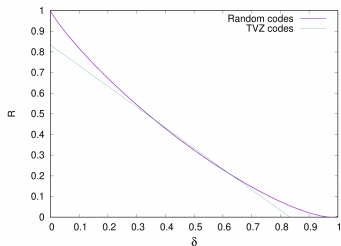
1982: Tsfasman, Vlăduț et Zink utilisent les codes AG pour dépasser la borne de Gilbert–Varshamov



## Bref histoire des codes géométriques

1981: Goppa introduit les codes AG sur les courbes algébriques

1982: Tsfasman, Vlăduț et Zink utilisent les codes AG pour dépasser la borne de Gilbert–Varshamov



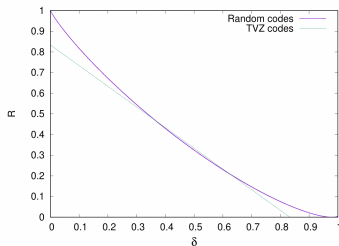
$XX_s$  : des different familles de courbes sont étudiées afin d'obtenir des codes AG avec des bons paramètres

↪ on utilise souvent les courbes dont les espaces de Riemann–Roch sont déjà connus (e.g. courbes Hermitiennes)

## Bref histoire des codes géométriques

1981: Goppa introduit les codes AG sur les courbes algébriques

1982: Tsfasman, Vlăduț et Zink utilisent les codes AG pour dépasser la borne de Gilbert–Varshamov



*XXs* : des different familles de courbes sont étudiées afin d'obtenir des codes AG avec des bons paramètres

↪ on utilise souvent les courbes dont les espaces de Riemann–Roch sont déjà connus (e.g. courbes Hermitiennes)

*XXIs* : les codes AG sont utilisés dans des nouvelles applications en théorie de l'information

# Espaces de Riemann–Roch : les codes AG et au-delà

Les codes AG interviennent dans le

- ▶ Partage de Secret <sup>1</sup>
- ▶ Calcul Vérifiable <sup>2</sup>
- ▶ autres applications

↪ besoin de calculer les espaces de Riemann–Roch de courbes

---

<sup>1</sup>R. Cramer, M. Rambaud et C. Xing, Crypto 2021

<sup>2</sup>S. Bordage et J. Nardi, preprint 2020

# Espaces de Riemann–Roch : les codes AG et au-delà

Les codes AG interviennent dans le

- ▶ Partage de Secret <sup>1</sup>
- ▶ Calcul Vérifiable <sup>2</sup>
- ▶ autres applications

↪ besoin de calculer les espaces de Riemann–Roch de courbes

Utile aussi pour...

- ▶ Operations arithmétiques sur les Jacobiennes de courbes<sup>3</sup>
- ▶ Intégration symbolique<sup>4</sup>

---

<sup>1</sup>R. Cramer, M. Rambaud et C. Xing, Crypto 2021

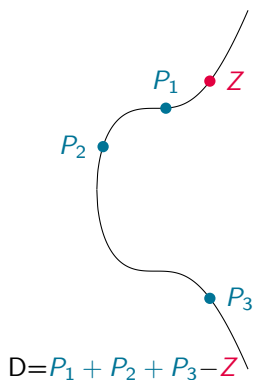
<sup>2</sup>S. Bordage et J. Nardi, preprint 2020

<sup>3</sup>K. Khuri-Makdisi, Mathematics of Computations, 2007

<sup>4</sup>J.H. Davenport, Intern. Symp. on Symbolic et Algebraic Manipulation, 1979

# Espaces de Riemann–Roch

Un **diviseur** sur une courbe  $\mathcal{C}$  c'est :  $D = \sum_{P \in \mathcal{C}} n_P P, n_P \in \mathbb{Z}$



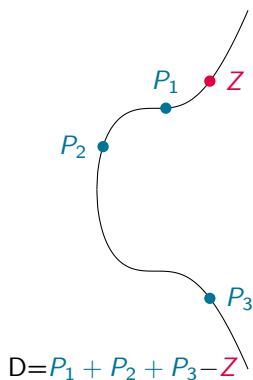
L'**espace de Riemann–Roch**  $L(D)$  est l'espace de toutes les fonctions de la forme  $\frac{G}{H} \in \mathbb{K}(\mathcal{C})$  telles que :

- ▶ si  $n_P < 0$  alors  $P$  **doit être un zéro** de  $G$  (de multiplicité  $\geq -n_P$ )
- ▶ si  $n_P > 0$  alors  $P$  **peut être un zéro** of  $H$  (de multiplicité  $\leq n_P$ )
- ▶  $G/H$  n'a pas **d'autres pôles** en dehors des points  $P$  avec  $n_P > 0$

**Ici** :  $Z$  doit être un zéro de  $G$ , les  $P_i$  peuvent être des zéros de  $H$

# Espaces de Riemann–Roch

Un **diviseur** sur une courbe  $\mathcal{C}$  c'est :  $D = \sum_{P \in \mathcal{C}} n_P P, n_P \in \mathbb{Z}$



L'**espace de Riemann–Roch**  $L(D)$  est l'espace de toutes les fonctions de la forme  $\frac{G}{H} \in \mathbb{K}(\mathcal{C})$  telles que :

- ▶ si  $n_P < 0$  alors  $P$  **doit être un zéro** de  $G$  (de multiplicité  $\geq -n_P$ )
- ▶ si  $n_P > 0$  alors  $P$  **peut être un zéro** of  $H$  (de multiplicité  $\leq n_P$ )
- ▶  $G/H$  n'a pas **d'autres pôles** en dehors des points  $P$  avec  $n_P > 0$

**Ici** :  $Z$  doit être un zéro de  $G$ , les  $P_i$  peuvent être des zéros de  $H$

**Théorème de Riemann–Roch**  $\rightsquigarrow \dim L(D) = \deg D + 1 - g$

où le **degré** d'un diviseur est  $\deg D = \sum_P n_P$



## Exemple jouet

Soit  $\mathcal{C} = \mathbb{P}^1$ ,  $P = [0 : 1]$  et  $Q = [1 : 1]$ . Soit  $D = P - Q$ , alors

$$f \in L(D) \iff \begin{cases} f \text{ a un zéro d'ordre au moins 1 en } Q \\ f \text{ peut avoir un p\^ole d'ordre au plus 1 en } P \\ f \text{ n'a pas d'autres p\^oles en dehors de } P \end{cases}$$

## Exemple jouet

Soit  $C = \mathbb{P}^1$ ,  $P = [0 : 1]$  et  $Q = [1 : 1]$ . Soit  $D = P - Q$ , alors

$$f \in L(D) \iff \begin{cases} f \text{ a un zéro d'ordre au moins 1 en } Q \\ f \text{ peut avoir un p\^ole d'ordre au plus 1 en } P \\ f \text{ n'a pas d'autres p\^oles en dehors de } P \end{cases}$$

$$f = \frac{X-1}{X} \text{ est une solution}$$

## Exemple jouet

Soit  $C = \mathbb{P}^1$ ,  $P = [0 : 1]$  et  $Q = [1 : 1]$ . Soit  $D = P - Q$ , alors

$$f \in L(D) \iff \begin{cases} f \text{ a un zéro d'ordre au moins 1 en } Q \\ f \text{ peut avoir un p\^ole d'ordre au plus 1 en } P \\ f \text{ n'a pas d'autres p\^oles en dehors de } P \end{cases}$$

$$f = \frac{X-1}{X} \text{ est une solution}$$

$$g = 0, \deg D = 0 \xrightarrow[\text{Riemann-Roch}]{\text{Th\^eor\^eme de}} \dim L(D) = \deg D + 1 - g = 1$$

$\rightarrow f$  engendre l'espace des solutions

## Exemple jouet

Soit  $C = \mathbb{P}^1$ ,  $P = [0 : 1]$  et  $Q = [1 : 1]$ . Soit  $D = P - Q$ , alors

$$f \in L(D) \iff \begin{cases} f \text{ a un zéro d'ordre au moins 1 en } Q \\ f \text{ peut avoir un p\^ole d'ordre au plus 1 en } P \\ f \text{ n'a pas d'autres p\^oles en dehors de } P \end{cases}$$

$f = \frac{X-1}{X}$  est une solution

$$g = 0, \deg D = 0 \xrightarrow[\text{Riemann-Roch}]{\text{Th\^eor\^eme de}} \dim L(D) = \deg D + 1 - g = 1$$

$\rightarrow f$  engendre l'espace des solutions

### Strat\egie

D\^enominateur  $H$  passe par  $P$ :  $H(X, Y, 1) \equiv 0 \pmod{X}$

Num\^erateur  $G$  passe par  $Q$ :  $G(X, Y, 1) \equiv 0 \pmod{X-1}$

On retrouve la solution :  $\frac{X-1}{X}$ .

## *Problème de Riemann–Roch : état de l'art*

### **Méthode géométrique :**

(Théorie de Brill–Noether  $\sim 1874$ )

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

### **Méthode arithmétique :**

(Idéaux dans de corps de fonctions)

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

# Problème de Riemann–Roch : état de l'art

## Méthode géométrique :

(Théorie de Brill–Noether  $\sim 1874$ )

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

## Méthode arithmétique :

(Idéaux dans de corps de fonctions)

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

Courbes

ordinaires/nodales :

Courbes

non-ordinaires :

Algorithme Las Vegas qui calcule  $L(D)$  en temps sous-quadratique

⚠ aucun exposant de complexité explicite



# Plan d'attaque

## 1. Méthode de Brill–Noether

↪

conditions nécessaires et suffisantes sur  $G$  et  $H$  pour que  $G/H \in L(D)$

## 2. Séries de Puiseux

↪

gestion des points singuliers  
*non-ordinaires* de la courbe

## 3. Algèbre linéaire

↪

calcul de  $H$  et  $G$  en pratique

# Plan d'attaque

1. Méthode de Brill–Noether  $\rightsquigarrow$  conditions nécessaires et suffisantes sur  $G$  et  $H$  pour que  $G/H \in L(D)$
2. Séries de Puiseux  $\rightsquigarrow$  gestion des points singuliers *non-ordinaires* de la courbe
3. Algèbre linéaire  $\rightsquigarrow$  calcul de  $H$  et  $G$  en pratique

## Resultat principal

Algorithme de type Las Vegas qui calcule  $L(D)$  en  $\tilde{O}(((\deg C)^2 + \deg D_+)^{\omega})$  opérations<sup>5</sup>.



---

<sup>5</sup> $2 \leq \omega \leq 3$  est un exposant faisable pour l'algèbre linéaire ( $\omega = 2.373$ )



## Notations et hypothèses

$\mathcal{C} : F(x, y, z) = 0$  – courbe plane,  $F$  absolument irréductible de degré  $\delta$

$\text{Sing}(\mathcal{C})$  – les points singuliers de  $\mathcal{C}$ , supposés dans la carte affine  $z = 1$

$(H) = \sum_{P \in \mathcal{C}} \text{ord}_P(H)P$  – diviseurs de zéros de  $H$  avec multiplicité

$D \geq D' \rightsquigarrow D - D' = \sum n_P P$  avec  $n_P \geq 0 \forall P$  ( $D - D'$  est effectif)

On peut écrire  $D = D_+ - D_-$  avec  $D_+$  et  $D_-$  effectifs

## Notations et hypothèses

$\mathcal{C} : F(x, y, z) = 0$  – courbe plane,  $F$  absolument irréductible de degré  $\delta$

$\text{Sing}(\mathcal{C})$  – les points singuliers de  $\mathcal{C}$ , supposés dans la carte affine  $z = 1$

$(H) = \sum_{P \in \mathcal{C}} \text{ord}_P(H)P$  – diviseurs de zéros de  $H$  avec multiplicité

$D \geq D' \rightsquigarrow D - D' = \sum n_P P$  avec  $n_P \geq 0 \forall P$  ( $D - D'$  est effectif)

On peut écrire  $D = D_+ - D_-$  avec  $D_+$  et  $D_-$  effectifs

$\mathbb{K}$  – corps parfait (caractéristique nulle ou positive)

$\mathbb{K}[[x]]$  – anneau de séries entières en  $x$

$\mathbb{K}((x))$  – corps de séries de Laurent

$\overline{\mathbb{K}}\langle\langle x \rangle\rangle$  – corps de séries de Puiseux

## Notations et hypothèses

$\mathcal{C} : F(x, y, z) = 0$  – courbe plane,  $F$  absolument irréductible de degré  $\delta$

$\text{Sing}(\mathcal{C})$  – les points singuliers de  $\mathcal{C}$ , supposés dans la carte affine  $z = 1$

$(H) = \sum_{P \in \mathcal{C}} \text{ord}_P(H)P$  – diviseurs de zéros de  $H$  avec multiplicité

$D \geq D' \rightsquigarrow D - D' = \sum n_P P$  avec  $n_P \geq 0 \forall P$  ( $D - D'$  est effectif)

On peut écrire  $D = D_+ - D_-$  avec  $D_+$  et  $D_-$  effectifs

$\mathbb{K}$  – corps parfait (caractéristique nulle ou positive)

$\mathbb{K}[[x]]$  – anneau de séries entières en  $x$

$\mathbb{K}((x))$  – corps de séries de Laurent

$\overline{\mathbb{K}}\langle\langle x \rangle\rangle$  – corps de séries de Puiseux

⚠ bien définies en caractéristique 0 ou positive "grande"

## Méthode de Brill–Noether

*Description de  $L(D)$  pour  $C : F(X, Y, Z) = 0$  courbe plane projective.*

*Les éléments non-nuls sont de la forme  $\frac{G_i}{H}$  où*

- ▶  *$H$  satisfait  $(H) \geq D_+$*
- ▶  *$H$  s'annule en tout point singulier de  $C$  avec multiplicité ad hoc*
- ▶  *$\deg G_i = \deg H$ ,  $G_i$  copremier avec  $F$  et  $(G_i) \geq (H) - D$*

# Méthode de Brill–Noether

Description de  $L(D)$  pour  $C : F(X, Y, Z) = 0$  courbe plane projective.

Les éléments non-nuls sont de la forme  $\frac{G_i}{H}$  où

- ▶  $H$  satisfait  $(H) \geq D_+$
- ▶  $H$  s'annule en tout point singulier de  $C$  avec multiplicité ad hoc
- ▶  $\deg G_i = \deg H$ ,  $G_i$  copremier avec  $F$  et  $(G_i) \geq (H) - D$

Comment gérer les points singuliers ?

# Méthode de Brill–Noether

Description de  $L(D)$  pour  $\mathcal{C} : F(X, Y, Z) = 0$  courbe plane projective.

Les éléments non-nuls sont de la forme  $\frac{G_i}{H}$  où

- ▶  $H$  satisfait  $(H) \geq D_+$
- ▶  $H$  s'annule en tout point singulier de  $\mathcal{C}$  avec multiplicité ad hoc
- ▶  $\deg G_i = \deg H$ ,  $G_i$  copremier avec  $F$  et  $(G_i) \geq (H) - D$

Comment gérer les points singuliers ?

- ✓ le diviseur d'adjonction  $\mathcal{A}$  "contient" les points singuliers de  $\mathcal{C}$  avec leurs multiplicités

# Méthode de Brill–Noether

Description de  $L(D)$  pour  $\mathcal{C} : F(X, Y, Z) = 0$  courbe plane projective.

Les éléments non-nuls sont de la forme  $\frac{G_i}{H}$  où

- ▶  $H$  satisfait  $(H) \geq D_+$
- ▶  $H$  satisfait  $(H) \geq \mathcal{A}$  (on dira que " $H$  est adjoint à la courbe")
- ▶  $\deg G_i = \deg H$ ,  $G_i$  copremier avec  $F$  et  $(G_i) \geq (H) - D$

Comment gérer les points singuliers ?

- ✓ le diviseur d'adjonction  $\mathcal{A}$  "contient" les points singuliers de  $\mathcal{C}$  avec leurs multiplicités

# Méthode de Brill–Noether

Description de  $L(D)$  pour  $\mathcal{C} : F(X, Y, Z) = 0$  courbe plane projective.

Les éléments non-nuls sont de la forme  $\frac{G_i}{H}$  où

- ▶  $H$  satisfait  $(H) \geq D_+$
- ▶  $H$  satisfait  $(H) \geq \mathcal{A}$
- ▶  $\deg G_i = \deg H$ ,  $G_i$  copremier avec  $F$  et  $(G_i) \geq (H) - D$

Comment gérer les points singuliers ?

✓ le diviseur d'adjonction  $\mathcal{A}$  "contient" les points singuliers de  $\mathcal{C}$  avec leurs multiplicités

Comment gérer les diviseurs ?



# Méthode de Brill–Noether

Description de  $L(D)$  pour  $\mathcal{C} : F(X, Y, Z) = 0$  courbe plane projective.

Les éléments non-nuls sont de la forme  $\frac{G_i}{H}$  où

- ▶  $H$  satisfait  $(H) \geq D_+$
- ▶  $H$  satisfait  $(H) \geq \mathcal{A}$
- ▶  $\deg G_i = \deg H$ ,  $G_i$  copremier avec  $F$  et  $(G_i) \geq (H) - D$

Comment gérer les points singuliers ?

✓ le diviseur d'adjonction  $\mathcal{A}$  "contient" les points singuliers de  $\mathcal{C}$  avec leurs multiplicités

Comment gérer les diviseurs ?

expansions en séries de  
representations multi-set  $((P_i)_i, n_i)$

$\rightsquigarrow$

opérations sur les diviseurs  
avec coût négligeable

## Sketch de l'algorithme

### Input

$C : F(X, Y, Z) = 0$  une courbe plane projective,  $D$  un diviseur lisse.

**Étape 1 :** Calcul du diviseur d'adjonction  $\mathcal{A}$

**Étape 2 :** Calcul du dénominateur commun  $H$

**Étape 3 :** Calcul de  $(H) - D$

**Étape 4 :** Calcul des numérateurs  $G_i$  (proche de l'étape 2)

### Output

Une base de l'espace de Riemann–Roch  $L(D)$  en termes de  $H$  et des  $G_i$ .

## Sketch de l'algorithme

### Input

$C : F(X, Y, Z) = 0$  une courbe plane projective,  $D$  un diviseur lisse.

**Étape 1 :** Calcul du diviseur d'adjonction  $\mathcal{A}$

**Étape 2 :** Calcul du dénominateur commun  $H$

**Étape 3 :** Calcul de  $(H) - D \checkmark \leftarrow \tilde{O}((\delta^2 + \deg D_+)^2)$

**Étape 4 :** Calcul des numérateurs  $G_i$  (proche de l'étape 2)

### Output

Une base de l'espace de Riemann–Roch  $L(D)$  en termes de  $H$  et des  $G_i$ .

## Sketch de l'algorithme

### Input

$C : F(X, Y, Z) = 0$  une courbe plane projective,  $D$  un diviseur lisse.

**Étape 1 :** Calcul du diviseur d'adjonction  $\mathcal{A}$

**Étape 2 :** Calcul du dénominateur commun  $H$

**Étape 3 :** Calcul de  $(H) - D \checkmark \leftarrow \tilde{O}((\delta^2 + \deg D_+)^2)$

**Étape 4 :** Calcul des numérateurs  $G_i$  (proche de l'étape 2)

### Output

Une base de l'espace de Riemann–Roch  $L(D)$  en termes de  $H$  et des  $G_i$ .

## Échauffement: diviseur d'adjonction dans le cas ordinaire

### Définition

Soit  $P \in \text{Sing}(C)$ . Le *diviseur d'adjonction local* est

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

## Échauffement: diviseur d'adjonction dans le cas ordinaire

### Définition

Soit  $P \in \text{Sing}(\mathcal{C})$ . Le *diviseur d'adjonction local* est

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

Soit  $P \in \text{Sing}(\mathcal{C})$  **ordinaire** de multiplicité  $m$ , wlog  $P = (0 : 0 : 1)$ . Alors  $F$  se factorise localement comme

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

avec  $u \in \overline{\mathbb{K}}[[x, y]]$  inversible,  $\varphi_i(x) \in x\overline{\mathbb{K}}[[x]]$  et  $\varphi'_i(0) \neq \varphi'_j(0)$ .

# Échauffement: diviseur d'adjonction dans le cas ordinaire

## Définition

Soit  $P \in \text{Sing}(\mathcal{C})$ . Le *diviseur d'adjonction local* est

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

Soit  $P \in \text{Sing}(\mathcal{C})$  **ordinaire** de multiplicité  $m$ , wlog  $P = (0 : 0 : 1)$ . Alors  $F$  se factorise localement comme

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

avec  $u \in \overline{\mathbb{K}}[[x, y]]$  inversible,  $\varphi_i(x) \in x\overline{\mathbb{K}}[[x]]$  et  $\varphi'_i(0) \neq \varphi'_j(0)$ .

Germe de courbe  
paramétré par  $\varphi_i(x)$   $\longleftrightarrow$  place  $\mathcal{P}_i$  dans le corps  
de fonctions  $\overline{\mathbb{K}}(\mathcal{C})$

## Échauffement: diviseur d'adjonction dans le cas ordinaire

### Définition

Soit  $P \in \text{Sing}(\mathcal{C})$ . Le *diviseur d'adjonction local* est

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

Soit  $P \in \text{Sing}(\mathcal{C})$  **ordinaire** de multiplicité  $m$ , wlog  $P = (0 : 0 : 1)$ . Alors  $F$  se factorise localement comme

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

avec  $u \in \overline{\mathbb{K}}[[x, y]]$  inversible,  $\varphi_i(x) \in x\overline{\mathbb{K}}[[x]]$  et  $\varphi'_i(0) \neq \varphi'_j(0)$ .

Germe de courbe  
paramétré par  $\varphi_i(x)$   $\longleftrightarrow$  place  $\mathcal{P}_i$  dans le corps  
de fonctions  $\overline{\mathbb{K}}(\mathcal{C})$

Le *diviseur d'adjonction local* devient

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



## *La condition d'adjonction via les séries de Puiseux*

Soit  $F \in \mathbb{K}[x, y]$  absolument irréductible, unitaire en  $y$  et de degré  $d$  en  $y$ .  $F \in \mathbb{K}((x))[y]$  admet  $d$  racines distinctes dans  $\overline{\mathbb{K}}\langle\langle x \rangle\rangle$ ,  $\varphi_1, \dots, \varphi_d$ , et s'écrit

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

## La condition d'adjonction via les séries de Puiseux

Soit  $F \in \mathbb{K}[x, y]$  absolument irréductible, unitaire en  $y$  et de degré  $d$  en  $y$ .  $F \in \mathbb{K}((x))[y]$  admet  $d$  racines distinctes dans  $\overline{\mathbb{K}}\langle\langle x \rangle\rangle$ ,  $\varphi_1, \dots, \varphi_d$ , et s'écrit

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

On fixe  $\varphi$  de degré  $e$ ,  $\zeta$  une racine primitive  $e$ -ème de l'unité. Pour  $0 \leq k < e$  on peut construire autres  $e$  séries de Puiseux en remplaçant  $x^{1/e}$  par  $\zeta^k x^{1/e}$ .

## La condition d'adjonction via les séries de Puiseux

Soit  $F \in \mathbb{K}[x, y]$  absolument irréductible, unitaire en  $y$  et de degré  $d$  en  $y$ .  $F \in \mathbb{K}(\!(x)\!) [y]$  admet  $d$  racines distinctes dans  $\overline{\mathbb{K}}\langle\langle x \rangle\rangle$ ,  $\varphi_1, \dots, \varphi_d$ , et s'écrit

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

On fixe  $\varphi$  de degré  $e$ ,  $\zeta$  une racine primitive  $e$ -ème de l'unité. Pour  $0 \leq k < e$  on peut construire autres  $e$  séries de Puiseux en remplaçant  $x^{1/e}$  par  $\zeta^k x^{1/e}$ . Elles sont équivalentes et représentées par...

### Définition

Une **Expansion de Puiseux Rationnelle** est un couple

$$(X(t), Y(t)) = \left( t^e, \sum_{j=n}^{\infty} \beta_j t^j \right) \text{ tel que } F(X(t), Y(t)) = 0$$

## La condition d'adjonction via les séries de Puiseux

Soit  $F \in \mathbb{K}[x, y]$  absolument irréductible, unitaire en  $y$  et de degré  $d$  en  $y$ .  $F \in \mathbb{K}(\!(x)\!) [y]$  admet  $d$  racines distinctes dans  $\overline{\mathbb{K}}\langle\langle x \rangle\rangle$ ,  $\varphi_1, \dots, \varphi_d$ , et s'écrit

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

On fixe  $\varphi$  de degré  $e$ ,  $\zeta$  une racine primitive  $e$ -ème de l'unité. Pour  $0 \leq k < e$  on peut construire autres  $e$  séries de Puiseux en remplaçant  $x^{1/e}$  par  $\zeta^k x^{1/e}$ . Elles sont équivalentes et représentées par...

### Définition

Une **Expansion de Puiseux Rationnelle** est un couple

$$(X(t), Y(t)) = \left( t^e, \sum_{j=n}^{\infty} \beta_j t^j \right) \text{ tel que } F(X(t), Y(t)) = 0$$

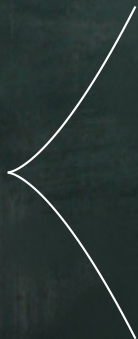
Expansions de Puiseux  
Rationnelles de  $F(x, y, 1)$



places de  $\overline{\mathbb{K}}(\mathcal{C})$  dans la  
carte  $z = 1$

Exemple

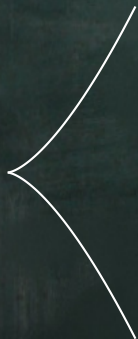
$$C : y^2 - x^3 = 0 \text{ dans la carte } z = 1$$



## Exemple

$\mathcal{C} : y^2 - x^3 = 0$  dans la carte  $z = 1$

$(0, 0)$  unique point singulier, non ordinaire



## Exemple

$\mathcal{C} : y^2 - x^3 = 0$  dans la carte  $z = 1$

$(0, 0)$  unique point singulier, non ordinaire

Séries de Puiseux :  $(y - x^{3/2})(y + x^{3/2}) = 0$

## Exemple

$\mathcal{C} : y^2 - x^3 = 0$  dans la carte  $z = 1$

$(0, 0)$  unique point singulier, non ordinaire

Séries de Puiseux :  $(y - x^{3/2})(y + x^{3/2}) = 0$

(Unique) RPE :  $(X(t), Y(t)) = (t^2, t^3)$



## Exemple

$\mathcal{C} : y^2 - x^3 = 0$  dans la carte  $z = 1$

$(0, 0)$  unique point singulier, non ordinaire

Séries de Puiseux :  $(y - x^{3/2})(y + x^{3/2}) = 0$

(Unique) RPE :  $(X(t), Y(t)) = (t^2, t^3)$

⚠ les RPE sont souvent définies sur une extension de  $\mathbb{K}$ .

C'est une question algorithmique de prendre l'extension minimale du corps.

## *Le diviseur d'adjonction*

Soit  $P \in \text{Sing}(C)$  ordinaire, wlog  $P = (0 : 0 : 1)$ . Alors  $F$  se factorise localement comme

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

avec  $u \in \mathbb{K}[[x, y]]$  inversible et  $\varphi_i$  series de Puiseux de  $F \in \overline{\mathbb{K}}[[x]][y]$ .

## Le diviseur d'adjonction

Soit  $P \in \text{Sing}(C)$  ordinaire, wlog  $P = (0 : 0 : 1)$ . Alors  $F$  se factorise localement comme

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

avec  $u \in \mathbb{K}[[x, y]]$  inversible et  $\varphi_i$  series de Puiseux de  $F \in \overline{\mathbb{K}}[[x]][y]$ .

$\{\varphi_1, \dots, \varphi_m\} \rightsquigarrow$  séries de Puiseux Rationnels/places  $(X_i(t), Y_i(t))$   
 $i \in \{1, \dots, s\}, s \leq m$

## Le diviseur d'adjonction

Soit  $P \in \text{Sing}(C)$  ordinaire, wlog  $P = (0 : 0 : 1)$ . Alors  $F$  se factorise localement comme

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

avec  $u \in \mathbb{K}[[x, y]]$  inversible et  $\varphi_i$  series de Puiseux de  $F \in \overline{\mathbb{K}}[[x]][y]$ .

$\{\varphi_1, \dots, \varphi_m\} \rightsquigarrow$  séries de Puiseux Rationnels/places  $(X_i(t), Y_i(t))$   
 $i \in \{1, \dots, s\}, s \leq m$

Le diviseur d'adjonction local devient

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

## Le diviseur d'adjonction

Soit  $P \in \text{Sing}(\mathcal{C})$  ordinaire, wlog  $P = (0 : 0 : 1)$ . Alors  $F$  se factorise localement comme

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

avec  $u \in \mathbb{K}[[x, y]]$  inversible et  $\varphi_i$  séries de Puiseux de  $F \in \overline{\mathbb{K}}[[x]][y]$ .

$\{\varphi_1, \dots, \varphi_m\} \rightsquigarrow$  séries de Puiseux Rationnels/places  $(X_i(t), Y_i(t))$   
 $i \in \{1, \dots, s\}, s \leq m$

Le diviseur d'adjonction local devient

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

Dans la pratique : algorithme pour les séries de Puiseux <sup>6</sup>

$\rightsquigarrow \mathcal{A}$  calculé avec  $\tilde{O}(\delta^3)$  opérations

---

<sup>6</sup>A. Poteaux et M. Weimann, Annales Henni Lebesgue, 2021

## Exemple

$\mathcal{C} : y^2 - x^3 = 0$  dans la carte  $z = 1$

$(0, 0)$  unique point singulier, non ordinaire

Séries de Puiseux :  $(y - x^{3/2})(y + x^{3/2}) = 0$

(Unique) RPE :  $(X(t), Y(t)) = (t^2, t^3)$

Condition d'ajonction

$$\text{val}_t \left( \frac{et^{e-1}}{F_y(X(t), Y(t), 1)} \right) =$$

$$\text{val}_t \left( \frac{2t}{2t^3} \right) = \text{val}_t \left( \frac{1}{t^2} \right) = -2$$

$H$  adjoint  $\iff \text{val}_t H(t^2, t^3) \geq 2$



## Sketch de l'algorithme

### Input

$\mathcal{C} : F(X, Y, Z) = 0$  une courbe plane projective,  $D$  un diviseur lisse.

**Étape 1 :** Calcul du diviseur d'adjonction  $\mathcal{A} \checkmark \leftarrow \tilde{O}(\delta^3)$

**Étape 2 :** Calcul du dénominateur commun  $H$

**Étape 3 :** Calcul de  $(H) - D \checkmark \leftarrow \tilde{O}((\delta^2 + \deg D_+)^2)$

**Étape 4 :** Calcul des numérateurs  $G_i$  (proche de l'étape 2)

### Output

Une base de l'espace de Riemann–Roch  $L(D)$  en termes de  $H$  et des  $G_j$ .

## Sketch de l'algorithme

### Input

$C : F(X, Y, Z) = 0$  une courbe plane projective,  $D$  un diviseur lisse.

**Étape 1 :** Calcul du diviseur d'adjonction  $\mathcal{A} \checkmark \leftarrow \tilde{O}(\delta^3)$

**Étape 2 :** Calcul du dénominateur commun  $H$

**Étape 3 :** Calcul de  $(H) - D \checkmark \leftarrow \tilde{O}((\delta^2 + \deg D_+)^2)$

**Étape 4 :** Calcul des numérateurs  $G_i$  (proche de l'étape 2)

### Output

Une base de l'espace de Riemann–Roch  $L(D)$  en termes de  $H$  et des  $G_j$ .



# Trouver le dénominateur en pratique

*Algèbre linéaire classique*

Soit  $d := \deg H$ .

Condition  $(H) \geq \mathcal{A} + D_+$

$\rightsquigarrow$  système linéaire avec  $\deg \mathcal{A} + \deg D_+ \sim \delta^2 + \deg D_+$  équations

$\rightsquigarrow$  l'élimination de Gauss coûte

$\tilde{O}((d\delta + \delta^2 + \deg D_+)^\omega)$  opérations sur  $\mathbb{K}$

# Trouver le dénominateur en pratique

Algèbre linéaire classique

Soit  $d := \deg H$ .

Condition  $(H) \geq \mathcal{A} + D_+$

$\rightsquigarrow$  système linéaire avec  $\deg \mathcal{A} + \deg D_+ \sim \delta^2 + \deg D_+$  équations

$\rightsquigarrow$  l'élimination de Gauss coûte

$\tilde{O}((d\delta + \delta^2 + \deg D_+)^\omega)$  opérations sur  $\mathbb{K}$

**Quelle taille a  $d$ ?**

On montre que  $d = \left\lceil \frac{(\delta-1)(\delta-2) + \deg D_+}{\delta} \right\rceil$  est suffisant

$\rightsquigarrow$  dénominateur calculé avec  $\tilde{O}((\delta^2 + \deg D_+)^\omega)$  opérations sur  $\mathbb{K}$

## Deuxième méthode : algèbre linéaire structurée

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

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

(équations similaires pour la condition  $(H) \geq D_+$  )

L'espace des polynômes  $H(x, y, 1)$  qui satisfont ces conditions est un  $\mathbb{K}[x]$ -module

$\rightsquigarrow$  calculer une base coûte  $\tilde{O}((\delta^2 + \deg D_+)^\omega)$  opérations <sup>7</sup>

---

<sup>7</sup>C.-P. Jeannerod, V. Neiger, É. Schost et G. Villard, Journal of Symbolic Computation, 2017

## Deuxième méthode : algèbre linéaire structurée

Condition  $(H) \geq A$

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

(équations similaires pour la condition  $(H) \geq D_+$ )

L'espace des polynômes  $H(x, y, 1)$  qui satisfont ces conditions est un  $\mathbb{K}[x]$ -module

$\rightsquigarrow$  calculer une base coûte  $\tilde{O}((\delta^2 + \deg D_+)^\omega)$  opérations <sup>7</sup>

Même exposant de complexité mais...

Avantages :

- ▶  $\tilde{O}((\delta^2 + \deg D_+)^{\frac{\omega+1}{2}})$  sur les corps algébriquement clos
- ▶ améliorations possibles dans le futur

---

<sup>7</sup>C.-P. Jeannerod, V. Neiger, É. Schost et G. Villard, Journal of Symbolic Computation, 2017

## Sketch de l'algorithme

### Input

$C : F(X, Y, Z) = 0$  une courbe plane de degré  $\delta$ ,  $D$  un diviseur lisse.

**Étape 1 :** Calcul du diviseur d'adjonction  $\mathcal{A} \checkmark \leftarrow \tilde{O}(\delta^3)$

**Étape 2 :** Calcul du dénominateur commun  $H \checkmark \leftarrow \tilde{O}((\delta^2 + \deg D_+)^{\omega})$

**Étape 3 :** Calcul de  $(H) - D \checkmark \leftarrow \tilde{O}((\delta^2 + \deg D_+)^2)$

**Étape 4 :** Calcul des numérateurs  $G_i$  (proche de l'étape 2)

### Output

Une base de l'espace de Riemann–Roch  $L(D)$  en termes de  $H$  et des  $G_i$ .

## Sketch de l'algorithme

### Input

$C : F(X, Y, Z) = 0$  une courbe plane de degré  $\delta$ ,  $D$  un diviseur lisse.

**Étape 1 :** Calcul du diviseur d'adjonction  $\mathcal{A}$  ✓  $\leftarrow \tilde{O}(\delta^3)$

**Étape 2 :** Calcul du dénominateur commun  $H$  ✓  $\leftarrow \tilde{O}((\delta^2 + \deg D_+)^{\omega})$

**Étape 3 :** Calcul de  $(H) - D$  ✓  $\leftarrow \tilde{O}((\delta^2 + \deg D_+)^2)$

**Étape 4 :** Calcul des numérateurs  $G_i$  ✓  $\leftarrow \tilde{O}((\delta^2 + \deg D_+)^{\omega})$

### Output

Une base de l'espace de Riemann–Roch  $L(D)$  en termes de  $H$  et des  $G_i$ .

*Théorème (Abelard, B., Couvreur, Lecerf – preprint 2021)*

L'algorithme présenté calcule  $L(D)$  en  $\tilde{O}((\delta^2 + \deg D_+)^{\omega})$  opérations en  $\mathbb{K}$ .

## Questions futures

Calcul d'espaces de Riemann–Roch de courbes.

- ◇ Calcul d'espaces de Riemann–Roch de courbes non-ordinaires en caractéristique positive “petite”



## Questions futures

Calcul d'espaces de Riemann–Roch de courbes.

- ◇ Calcul d'espaces de Riemann–Roch de courbes non-ordinaires en caractéristique positive “petite”  
**Obstacle** : trouver un outil alternatif aux séries de Puiseux





## Questions futures

Calcul d'espaces de Riemann–Roch de courbes.

- ◇ Calcul d'espaces de Riemann–Roch de courbes non-ordinaires en caractéristique positive “petite”  
**Obstacle** : trouver un outil alternatif aux séries de Puiseux
- ◇ Calcul d'espaces de Riemann–Roch associés à des diviseurs non lisses



## Questions futures

### Calcul d'espaces de Riemann–Roch de courbes.

- ◇ Calcul d'espaces de Riemann–Roch de courbes non-ordinaires en caractéristique positive “petite”  
**Obstacle** : trouver un outil alternatif aux séries de Puiseux
- ◇ Calcul d'espaces de Riemann–Roch associés à des diviseurs non lisses
- ◇ Implementation de l'algorithme



## Questions futures

### Calcul d'espaces de Riemann–Roch de courbes.

- ◇ Calcul d'espaces de Riemann–Roch de courbes non-ordinaires en caractéristique positive “petite”  
**Obstacle** : trouver un outil alternatif aux séries de Puiseux
- ◇ Calcul d'espaces de Riemann–Roch associés à des diviseurs non lisses
- ◇ Implementation de l'algorithme
- ◇ Améliorer l'exposant de complexité dans le cas non-ordinaire (sous-quadratique ?)



## Questions futures

### Calcul d'espaces de Riemann–Roch de courbes.

- ◇ Calcul d'espaces de Riemann–Roch de courbes non-ordinaires en caractéristique positive “petite”  
**Obstacle** : trouver un outil alternatif aux séries de Puiseux
- ◇ Calcul d'espaces de Riemann–Roch associés à des diviseurs non lisses
- ◇ Implementation de l'algorithme
- ◇ Améliorer l'exposant de complexité dans le cas non-ordinaire (sous-quadratique ?)  
**Obstacle** : algèbre linéaire



## Questions futures

### Calcul d'espaces de Riemann–Roch de courbes.

- ◇ Calcul d'espaces de Riemann–Roch de courbes non-ordinaires en caractéristique positive “petite”  
**Obstacle** : trouver un outil alternatif aux séries de Puiseux
- ◇ Calcul d'espaces de Riemann–Roch associés à des diviseurs non lisses
- ◇ Implementation de l'algorithme
- ◇ Améliorer l'exposant de complexité dans le cas non-ordinaire (sous-quadratique ?)  
**Obstacle** : algèbre linéaire



### Dimension supérieure.

- ◇ Peut-on développer des techniques type "Brill–Noether" pour le calcul d'espaces de Riemann–Roch de surfaces ?

## Questions futures

### Calcul d'espaces de Riemann–Roch de courbes.

- ◇ Calcul d'espaces de Riemann–Roch de courbes non-ordinaires en caractéristique positive “petite”  
**Obstacle** : trouver un outil alternatif aux séries de Puiseux
- ◇ Calcul d'espaces de Riemann–Roch associés à des diviseurs non lisses
- ◇ Implementation de l'algorithme
- ◇ Améliorer l'exposant de complexité dans le cas non-ordinaire (sous-quadratique ?)  
**Obstacle** : algèbre linéaire



### Dimension supérieure.

- ◇ Peut-on développer des techniques type "Brill–Noether" pour le calcul d'espaces de Riemann–Roch de surfaces ?



**Merci de votre attention !**

Des questions ? [e.berardini@tue.nl](mailto:e.berardini@tue.nl)