Codes géométriques sur les courbes et les surfaces

Elena Berardini

Séminaire de Théorie des Nombres
Laboratoire de Mathématiques Nicolas Oresme
25 février 2022

Sommaire

Qu'est que c'est un code (linéaire) ?

Un outil pour transmettre et stocker des données.

Propriété : détection et correction des erreurs qui se produisent pendant la transmission/le stockage.

Qu'est que c'est un code (linéaire) ?

Un outil pour transmettre et stocker des données.

Propriété : détection et correction des erreurs qui se produisent pendant la transmission/le stockage.

Un $\mathbb{F}_q$–sous espace vectoriel de $\mathbb{F}_q^n$ (codes linéaires).

Trois paramètres :

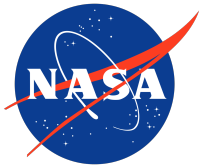
- **n**, la longueur ;
- **k**, la dimension ;
- **d**, la distance minimale.

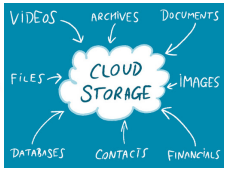
Taux de transmission : k/n
Détecte jusqu'à $d-1$ erreurs
Corrige jusqu'à $\lfloor \frac{d-1}{2} \rfloor$ erreurs.

Qu'est que c'est un code (linéaire) ?

Un outil pour transmettre et stocker des données.

Propriété : détection et correction des erreurs qui se produisent pendant la transmission/le stockage.





Un $\mathbb{F}_q$–sous espace vectoriel de $\mathbb{F}_q^n$ (codes linéaires).

Trois paramètres :

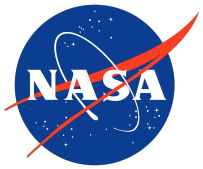
- **n**, la longueur ;
- **k**, la dimension ;
- **d**, la distance minimale.

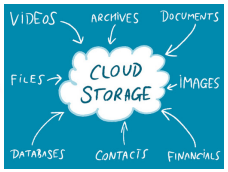
Taux de transmission : k/n
Détecte jusqu'à $d-1$ erreurs
Corrige jusqu'à $\lfloor \frac{d-1}{2} \rfloor$ erreurs.

Qu'est que c'est un code (linéaire) ?

Un outil pour transmettre et stocker des données.

Propriété : détection et correction des erreurs qui se produisent pendant la transmission/le stockage.





OBJECTIF : encoder le plus de données possible et détecter et corriger le plus d'erreurs possible !

Un $\mathbb{F}_q$–sous espace vectoriel de $\mathbb{F}_q^n$ (codes linéaires).

Trois paramètres :

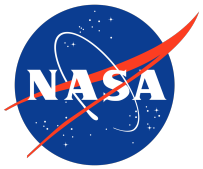
- **n**, la longueur ;
- **k**, la dimension ;
- **d**, la distance minimale.

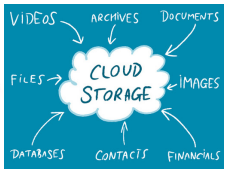
Taux de transmission : k/n
Détecte jusqu'à $d-1$ erreurs
Corrige jusqu'à $\lfloor \frac{d-1}{2} \rfloor$ erreurs.

Qu'est que c'est un code (linéaire) ?

Un outil pour transmettre et stocker des données.

Propriété : détection et correction des erreurs qui se produisent pendant la transmission/le stockage.





OBJECTIF : encoder le plus de données possible et détecter et corriger le plus d'erreurs possible !

Un $\mathbb{F}_q$–sous espace vectoriel de $\mathbb{F}_q^n$ (codes linéaires).

Trois paramètres :

- **n**, la longueur ;
- **k**, la dimension ;
- **d**, la distance minimale.

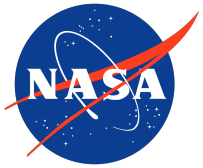
Taux de transmission : k/n
Détecte jusqu'à $d-1$ erreurs
Corrige jusqu'à $\lfloor \frac{d-1}{2} \rfloor$ erreurs.

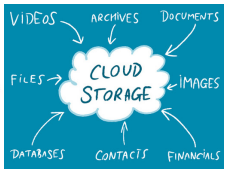
OBJECTIF : avoir **k** et **d** aussi grands que possible !

Qu'est que c'est un code (linéaire) ?

Un outil pour transmettre et stocker des données.

Propriété : détection et correction des erreurs qui se produisent pendant la transmission/le stockage.





OBJECTIF : encoder le plus de données possible et détecter et corriger le plus d'erreurs possible !

Un $\mathbb{F}_q$–sous espace vectoriel de $\mathbb{F}_q^n$ (codes linéaires).

Trois paramètres :

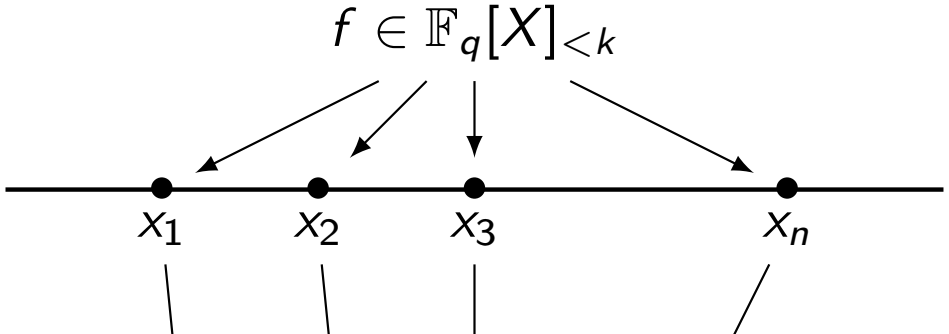
- **n**, la longueur ;
- **k**, la dimension ;
- **d**, la distance minimale.

Taux de transmission : k/n
Détecte jusqu'à $d-1$ erreurs
Corrige jusqu'à $\lfloor \frac{d-1}{2} \rfloor$ erreurs.

OBJECTIF : avoir **k** et **d** aussi grands que possible !

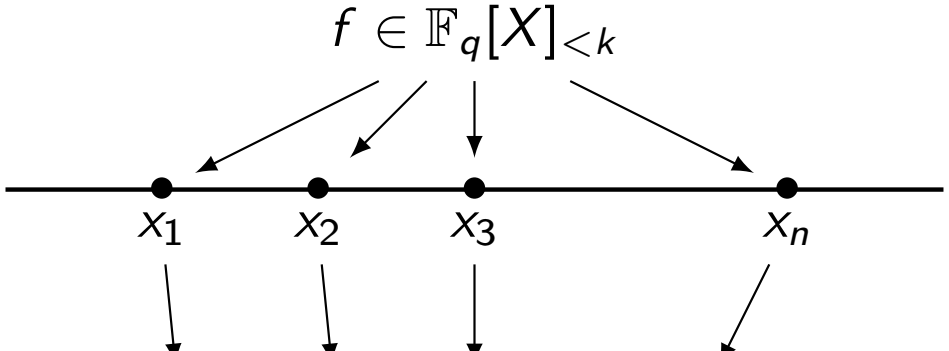
Borne de Singleton : $k+d \leqslant n+1$.
$\rightsquigarrow$ compromis entre redondance et capacité de correction d'erreurs.

Codes de Reed–Solomon...



$$\mathrm{RS}_k(\mathbf{x}) := \{(f(x_1), f(x_2), f(x_3), \ldots, f(x_n)) \mid f \in \mathbb{F}_q[X]_{<k}\}$$

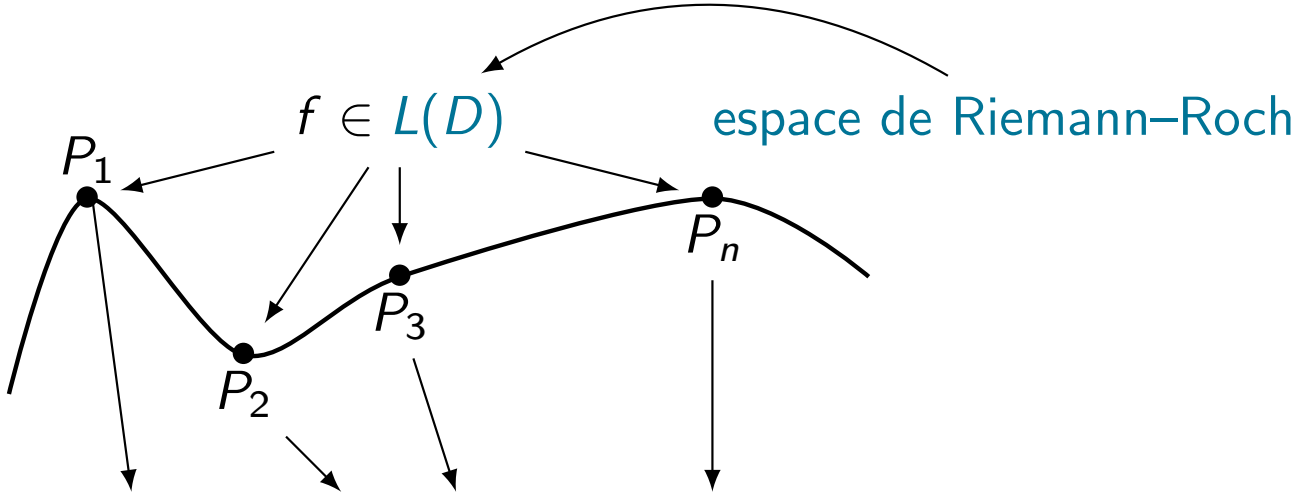
Codes de Reed–Solomon...



$$\mathrm{RS}_k(\mathbf{x}) := \{(f(x_1), f(x_2), f(x_3), \ldots, f(x_n)) \mid f \in \mathbb{F}_q[X]_{<k}\}$$

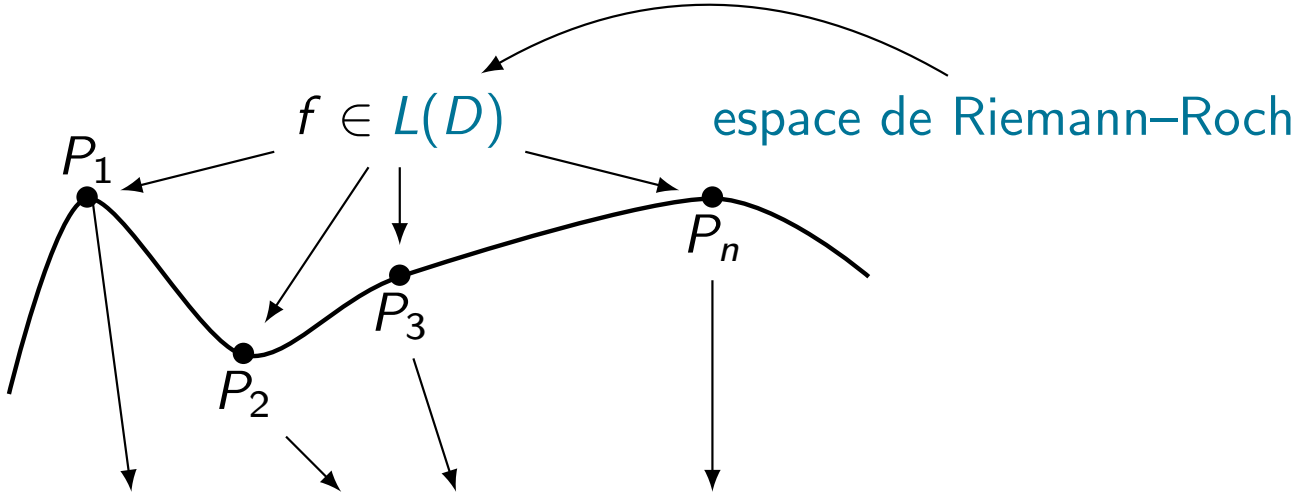
- ✓ Paramètres optimaux : $k + d = n + 1$ (codes MDS)
- ✓ Algorithme de décodage efficace (Berlekamp, 1968)
- ✓ Operations sur les données
- ⚠ Incovenient : $n \leqslant q$

...et codes géométriques (codes AG)



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

...et codes géométriques (codes AG)

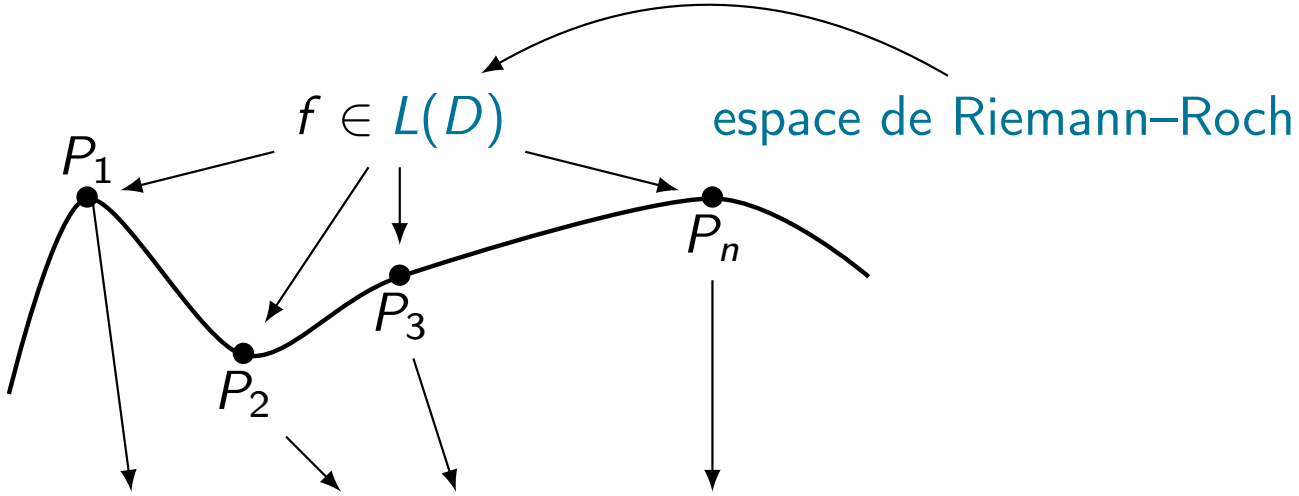


$$C((P_i)_i, D) := \{(f(P_1), f(P_2), f(P_3), \ldots, f(P_n)) \mid f \in L(D)\}$$

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

Dimension : $\dim L(D) \rightsquigarrow$ théorème de Riemann–Roch

...et codes géométriques (codes AG)



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

Longueur : $|\#\mathcal{C}(\mathbb{F}_q) - (q+1)| \leq g\lfloor 2\sqrt{q}\rfloor$
Dimension : $\dim L(D) \rightsquigarrow$ théorème de Riemann–Roch

Proposition

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

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

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

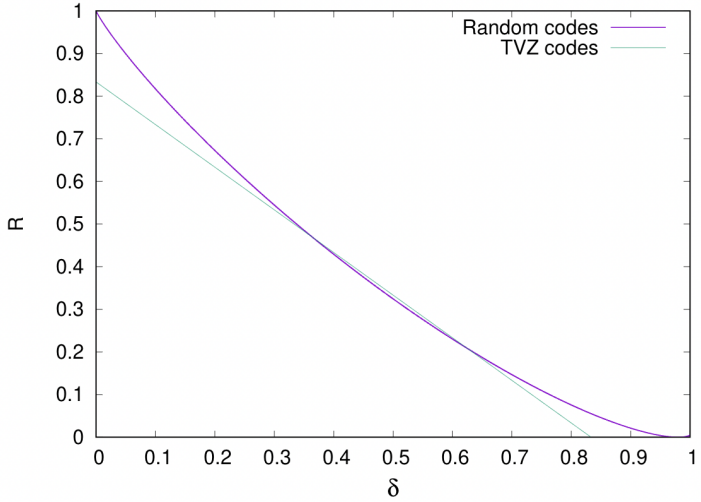
Bref histoire des codes géométriques

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

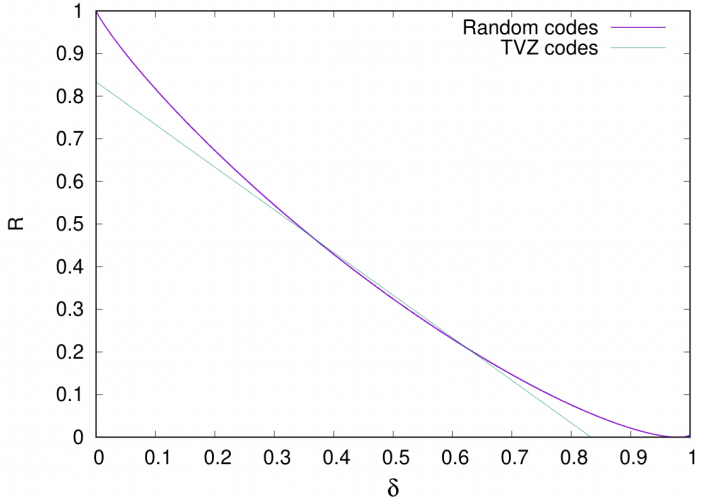
1982 : Tsfasman, Vlăduț et Zink utilisent les codes AG pour dépasser la borne de Gilbert–Varshamov



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



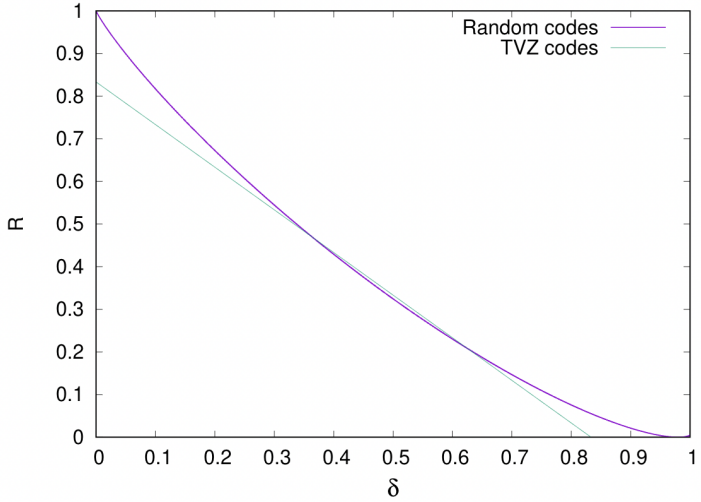
XXs : des different familles de courbes sont étudiées afin d'obtenir des codes AG avec des bons paramètres

$\hookrightarrow$ 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

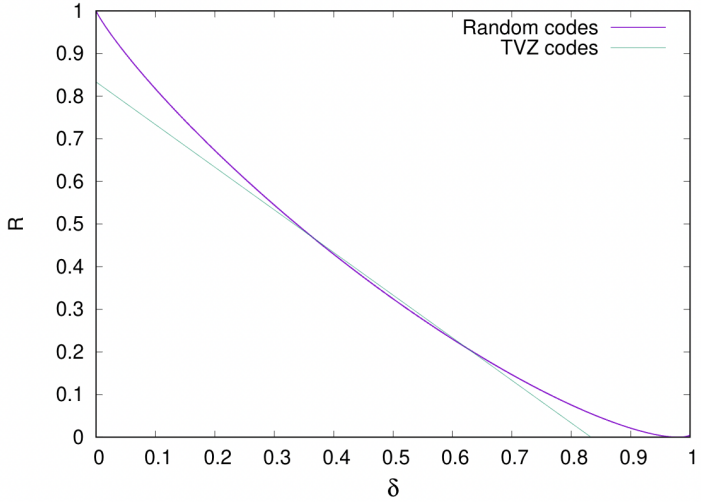
↪ on utilise souvent les courbes dont les espaces de Riemann–Roch sont déjà connus (*e.g.* courbes Hermitiennes)

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

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



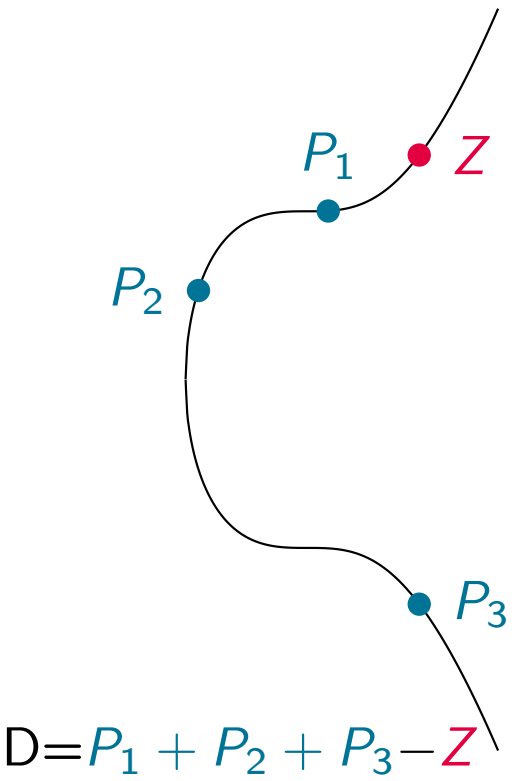
XXs : des different familles de courbes sont étudiées afin d'obtenir des codes AG avec des bons paramètres

↪ 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 ⇝ besoin de calculer les espaces de Riemann–Roch

Espaces de Riemann–Roch de courbes

Diviseurs sur une courbe $\mathcal{C}$: $D = \sum_{P \in \mathcal{C}} n_P P,\ n_P \in \mathbb{Z}$



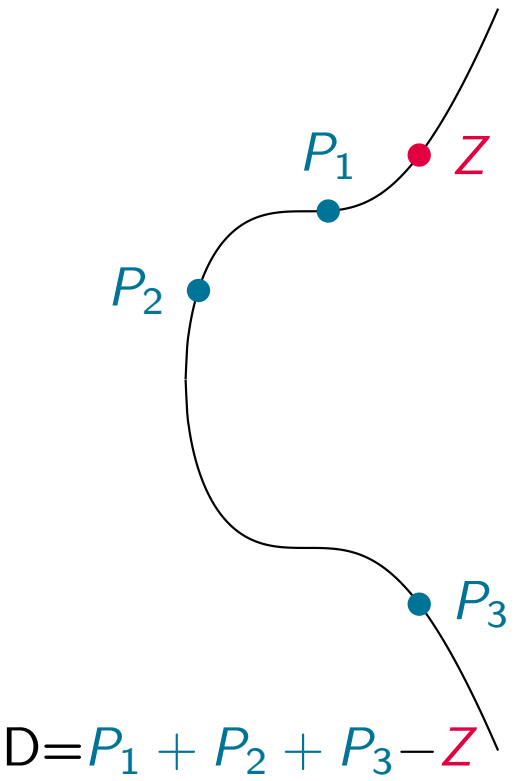
L'**espace de Riemann–Roch** $L(D)$ est l'espace de toutes les fonctions de la forme $\frac{G}{H} \in \mathbb{K}(\mathcal{C})$ telles que :

- si $n_P < 0$ alors P doit être un zéro de G (de multiplicité $\geqslant -n_P$)
- si $n_P > 0$ alors P peut être un zéro of H (de multiplicité $\leqslant n_P$)
- 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 de courbes

Diviseurs sur une courbe $\mathcal{C}$: $D = \sum_{P \in \mathcal{C}} n_P P,\ n_P \in \mathbb{Z}$



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 $\geqslant -n_P$)
- si $n_P > 0$ alors P peut être un zéro of H (de multiplicité $\leqslant n_P$)
- 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 $\rightsquigarrow \dim L(D) = \deg D + 1 - g$

Exemple jouet

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

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

Exemple jouet

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

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

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

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

$$\rightarrow f \text{ engendre l'espace des solutions}$$

Exemple jouet

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

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

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

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

$$\rightarrow f \text{ engendre l'espace des solutions}$$

⚠ on n'a pas une méthode explicite pour calculer une base de $L(D)$
Comment résoudre le problème en général?

Problème de Riemann–Roch : état de l'art

Méthode géométrique :
(Théorie de Brill–Noether ∼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 ∼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 : Algorithme Las Vegas qui calcule $L(D)$ en $\tilde{\mathcal{O}}((\delta^2 + \deg D)^{\frac{\omega+1}{2}})$ operations[1]

Courbes non–ordinaires : ⚠ aucun exposant de complexité explicite

[1] $2 \leqslant \omega \leqslant 3$ est un exposant faisable pour l'algèbre linéaire ($\omega = 2.373$)

Méthode de Brill–Noether

Notations :

- $(H) = \sum_{P \in \mathcal{C}} \mathrm{ord}_P(H) P$ – diviseur de zéros de H avec multiplicité
- $D \geqslant D' \rightsquigarrow D - D' = \sum n_P P$ avec $n_P \geqslant 0 \ \forall P$ ($D - D'$ est *effectif*)

Méthode de Brill–Noether

Notations :

- $(H) = \sum_{P \in \mathcal{C}} \mathrm{ord}_P(H) P$ – diviseur de zéros de H avec multiplicité
- $D \geqslant D' \rightsquigarrow D - D' = \sum n_P P$ avec $n_P \geqslant 0 \ \forall P$ ($D - D'$ est *effectif*)

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 $(H) \geqslant D$*
- *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 $(G_i) \geqslant (H) - D$*

Méthode de Brill–Noether

Notations :

- $(H) = \sum_{P \in \mathcal{C}} \mathrm{ord}_P(H) P$ – diviseur de zéros de H avec multiplicité
- $D \geqslant D' \rightsquigarrow D - D' = \sum n_P P$ avec $n_P \geqslant 0 \ \forall P$ ($D - D'$ est *effectif*)

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 $(H) \geqslant D$*
- *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 $(G_i) \geqslant (H) - D$*

Comment gérer les points singuliers ?

Méthode de Brill–Noether

Notations :

- $(H) = \sum_{P \in \mathcal{C}} \mathrm{ord}_P(H)P$ – diviseur de zéros de H avec multiplicité
- $D \geqslant D' \rightsquigarrow D - D' = \sum n_P P$ avec $n_P \geqslant 0 \ \forall P$ ($D - D'$ est *effectif*)

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 $(H) \geqslant D$*
- *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 $(G_i) \geqslant (H) - D$*

Comment gérer les points singuliers ?

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

Méthode de Brill–Noether

Notations :

- $(H) = \sum_{P \in \mathcal{C}} \mathrm{ord}_P(H)P$ – diviseur de zéros de H avec multiplicité
- $D \geqslant D' \rightsquigarrow D - D' = \sum n_P P$ avec $n_P \geqslant 0 \ \forall P$ ($D - D'$ est *effectif*)

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

Comment gérer les points singuliers ?

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

Méthode de Brill–Noether

Notations :

- $(H) = \sum_{P \in \mathcal{C}} \mathrm{ord}_P(H)P$ – diviseur de zéros de H avec multiplicité
- $D \geqslant D' \rightsquigarrow D - D' = \sum n_P P$ avec $n_P \geqslant 0 \ \forall P$ ($D - D'$ est *effectif*)

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 $(H) \geqslant D$*
- *H satisfait$(H) \geqslant \mathcal{A}$*
- $\deg G_i = \deg H$, *G_i copremier avec F et $(G_i) \geqslant (H) - D$*

Comment gérer les points singuliers ?

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

Comment gérer les diviseurs ?

Méthode de Brill–Noether

Notations :

- $(H) = \sum_{P \in \mathcal{C}} \mathrm{ord}_P(H) P$ – diviseur de zéros de H avec multiplicité
- $D \geqslant D' \rightsquigarrow D - D' = \sum n_P P$ avec $n_P \geqslant 0 \ \forall P$ ($D - D'$ est *effectif*)

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 $(H) \geqslant D$*
- *H satisfait$(H) \geqslant \mathcal{A}$*
- $\deg G_i = \deg H$, *G_i copremier avec F et $(G_i) \geqslant (H) - D$*

Comment gérer les points singuliers ?

$\rightsquigarrow$ 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

$\mathcal{C} : F(X, Y, Z) = 0$ *une courbe plane de degré* δ, 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

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

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

Étape 2 : Calcul du dénominateur commun H

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

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

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

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

Étape 2 : Calcul du dénominateur commun H

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

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.

Échauffement: diviseur d'adjonction dans le cas ordinaire

Définition

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

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

Échauffement: diviseur d'adjonction dans le cas ordinaire

Définition

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

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

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

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

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

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

Soit $P \in \mathrm{Sing}(\mathcal{C})$ 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 parametré 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 $\overline{\mathbb{K}}\langle\langle x \rangle\rangle$, $\varphi_1, \ldots, \varphi_d$, 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 $\overline{\mathbb{K}}\langle\langle x \rangle\rangle$, $\varphi_1, \ldots, \varphi_d$, 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 φ de degré e, ζ une racine primitive e-ème de l'unité. Pour $0 \leqslant k < e$ 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 $\overline{\mathbb{K}}\langle\langle x \rangle\rangle$, $\varphi_1, \ldots, \varphi_d$, 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 φ de degré e, ζ une racine primitive e-ème de l'unité. Pour $0 \leqslant k < e$ on peut construire autres e séries de Puiseux en remplaçant $x^{1/e}$ par $\zeta^k x^{1/e}$. Elles sont toutes équivalentes et représentées par...

Définition

Une Expansion de Puiseux Rationnelle est un couple $(X(t), Y(t)) = \left(\gamma t^e, \sum_{j=n}^{\infty} \beta_j t^j\right)$ *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 $\overline{\mathbb{K}}\langle\langle x \rangle\rangle$, $\varphi_1, \ldots, \varphi_d$, 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 φ de degré e, ζ une racine primitive e-ème de l'unité. Pour $0 \leqslant k < e$ on peut construire autres e séries de Puiseux en remplaçant $x^{1/e}$ par $\zeta^k x^{1/e}$. Elles sont toutes équivalentes et représentées par...

Définition

Une Expansion de Puiseux Rationnelle est un couple $(X(t), Y(t)) = \left(\gamma t^e, \sum_{j=n}^{\infty} \beta_j t^j\right)$ *tel que* $F(X(t), Y(t)) = 0$

Expansions de Puiseux Rationnelles de $F(x, y, 1)$	$\longleftrightarrow$	places de $\overline{\mathbb{K}}(\mathcal{C})$ dans la carte $z = 1$

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 $\overline{\mathbb{K}}\langle\langle x \rangle\rangle$, $\varphi_1, \ldots, \varphi_d$, 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 φ de degré e, ζ une racine primitive e-ème de l'unité. Pour $0 \leqslant k < e$ on peut construire autres e séries de Puiseux en remplaçant $x^{1/e}$ par $\zeta^k x^{1/e}$. Elles sont toutes équivalentes et représentées par...

Définition

Une Expansion de Puiseux Rationnelle est un couple $(X(t), Y(t)) = \left(\gamma t^e, \sum_{j=n}^{\infty} \beta_j t^j\right)$ *tel que* $F(X(t), Y(t)) = 0$

Expansions de Puiseux Rationnelles de $F(x, y, 1)$	$\longleftrightarrow$	places de $\overline{\mathbb{K}}(\mathcal{C})$ dans la carte $z = 1$

⚠ 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 $P \in \mathrm{Sing}(\mathcal{C})$ ~~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 φ_i series de Puiseux de $F \in \overline{\mathbb{K}}[[x]][y]$.

Le diviseur d'adjonction

Soit $P \in \mathrm{Sing}(\mathcal{C})$ ~~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 φ_i series de Puiseux de $F \in \overline{\mathbb{K}}[[x]][y]$.

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

Le diviseur d'adjonction

Soit $P \in \mathrm{Sing}(\mathcal{C})$ ~~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 φ_i series de Puiseux de $F \in \overline{\mathbb{K}}[[x]][y]$.

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

Le diviseur d'adjonction local devient

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

Le diviseur d'adjonction

Soit $P \in \mathrm{Sing}(\mathcal{C})$ ~~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 φ_i series de Puiseux de $F \in \overline{\mathbb{K}}[[x]][y]$.

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

Le diviseur d'adjonction local devient

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

Dans la pratique : algorithme pour les séries de Puiseux [2]

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

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

Sketch de l'algorithme

Input

$\mathcal{C} : F(X, Y, Z) = 0$ *une courbe plane de degré* δ, 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

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

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

$\mathcal{C} : F(X, Y, Z) = 0$ *une courbe plane de degré* δ, 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

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

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.

Trouver un dénominateur en pratique

Soit $d = \deg H$.

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

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

$\rightsquigarrow$ l'élimination de Gauss coûte

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

Trouver un dénominateur en pratique

Soit $d = \deg H$.

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

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

$\rightsquigarrow$ l'élimination de Gauss coûte

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

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 $\mathbb{K}$

Trouver un dénominateur en pratique

Soit $d = \deg H$.

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

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

$\rightsquigarrow$ l'élimination de Gauss coûte

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

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

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

$\rightsquigarrow$ structure de $\mathbb{K}[x]$-module

Sketch de l'algorithme

Input

$\mathcal{C} : F(X, Y, Z) = 0$ *une courbe plane de degré* δ, 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 $(H) - D$ ✓ $\leftarrow \tilde{O}(\delta^2 + \deg D)$

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

$\mathcal{C} : F(X, Y, Z) = 0$ *une courbe plane de degré* δ, 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 $(H) - D$ ✓ $\leftarrow \tilde{O}(\delta^2 + \deg D)$

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* $\mathbb{K}$.

Quoi retenir ?

0. Codes AG sur les courbes $\rightsquigarrow$ besoin de calculer de manière efficace les espaces de Riemann–Roch $L(D)$
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 (structurée) $\rightsquigarrow$ calcul de H et G en pratique

Quoi retenir ?

0. Codes AG sur les courbes $\rightsquigarrow$ besoin de calculer de manière efficace les espaces de Riemann–Roch $L(D)$
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 (structurée) $\rightsquigarrow$ calcul de H et G en pratique

Théorème

Algorithme de type Las Vegas qui calcule $L(D)$ en $\tilde{\mathcal{O}}((\delta^2 + \deg D)^\omega)$ opérations.

Codes géométriques : des courbes aux surfaces

	Courbes	Surfaces
Diviseurs	sommes de points	sommes de courbes

Espace de Riemann–Roch associé à un diviseur sur une surface
= fonctions avec conditions sur leurs zéros et pôles

Codes géométriques : des courbes aux surfaces

	Courbes	Surfaces
Diviseurs	sommes de points	sommes de courbes

Espace de Riemann–Roch associé à un diviseur sur une surface
= fonctions avec conditions sur leurs zéros et pôles
$\rightsquigarrow$ *construction de codes à partir de surfaces !*

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

Codes géométriques : des courbes aux surfaces

	Courbes	Surfaces
Diviseurs	sommes de points	sommes de courbes

Espace de Riemann–Roch associé à un diviseur sur une surface
= fonctions avec conditions sur leurs zéros et pôles
$\rightsquigarrow$ *construction de codes à partir de surfaces !*

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

Pourquoi s'intéresser aux codes sur les surfaces ?

Nombre de points rationnels : $O(q^2)$ / *surface VS* $O(q)$ / *courbe*
$\rightsquigarrow$ *codes de même longueur sur des corps finis plus petit*

Applications : constructions de codes localement recouvrables/decodables

Intérêt mathématique : nouvelles questions mathématiques qui se posent

Étude des paramètres

Longueur : bornée par le nombre de points rationnels sur la surface

Dimension : $\dim L(D) \rightsquigarrow$ théorème de Riemann–Roch pour les surfaces
⚠ Ne donne pas une méthode effective pour calculer une base de $L(D)$!

Distance minimale :

Définition

Soit C un code de longueur n. Soit $z(c)$ le nombre des coordonnées nulles d'un mot du code $c \in C$. La distance minimale de C est

$$d := n - \max\{z(c) | \, c \in C \setminus \{0\}\}.$$

Outils de géométrie algébrique $\rightsquigarrow$ borne pour la distance minimale

Méthode

Mots du code : $(f(P_1), \ldots, f(P_n))$, pour $f \in L(D)$.

Soit $(f)_+ = \sum_{\mathrm{ord}_{\mathcal{C}}(f)>0} \mathrm{ord}_{\mathcal{C}}(f)\mathcal{C}$ (i.e. les zéros de f sont sur $\mathcal{C}$) et

$$Z(f) := \text{nombre de points rationnels sur } (f)_+$$

$Z(f) \geqslant \#$ zéros de $(f(P_1), \ldots, f(P_n))$, d'où

$$d \geqslant n - \max_{f \in L(D)\setminus\{0\}} Z(f)$$

borne sup pour $Z(f) \Rightarrow$ borne inf pour la distance minimale

Méthode

Mots du code : $(f(P_1), \ldots, f(P_n))$, pour $f \in L(D)$.

Soit $(f)_+ = \sum_{\mathrm{ord}_{\mathcal{C}}(f)>0} \mathrm{ord}_{\mathcal{C}}(f)\mathcal{C}$ (i.e. les zéros de f sont sur $\mathcal{C}$) et

$$Z(f) := \text{nombre de points rationnels sur } (f)_+$$

$Z(f) \geqslant \#$ zéros de $(f(P_1), \ldots, f(P_n))$, d'où

$$d \geqslant n - \max_{f \in L(D)\setminus\{0\}} Z(f)$$

borne sup pour $Z(f) \Rightarrow$ borne inf pour la distance minimale

$$\boxed{Z(f) \leqslant \sum_{i=1}^{k} \#\mathcal{C}_i(\mathbb{F}_q)}$$

La géométrie algébrique entre en jeu

Borner k :

- Avec la théorie de l'intersection sur les surfaces.

Borner $\#\mathcal{C}(\mathbb{F}_q)$:

- Différentes bornes existent déjà et peuvent être utilisées dans ce contexte (*e.g.* borne de Serre–Weil).
- Borne plus fine pour $\#\mathcal{C}(\mathbb{F}_q)$ pour les courbes sur une surface donnée $\rightsquigarrow$ borne plus fine pour la distance minimale[3].

[3] E. Berardini et J. Nardi, preprint 2021

La géométrie algébrique entre en jeu

Borner k :

- Avec la théorie de l'intersection sur les surfaces.

Borner $\#\mathcal{C}(\mathbb{F}_q)$:

- Différentes bornes existent déjà et peuvent être utilisées dans ce contexte (*e.g.* borne de Serre–Weil).
- Borne plus fine pour $\#\mathcal{C}(\mathbb{F}_q)$ pour les courbes sur une surface donnée $\rightsquigarrow$ borne plus fine pour la distance minimale[3].

La borne pour d dépend des invariants de la surface

$\downarrow$

Informations sur quelles surfaces donnent des bons codes, *e.g.*

✓ Surfaces abéliennes sans courbes irréductibles de genre petit[4]
✓ Surfaces fibrées sur une courbe de base avec peu de points rationnels[5]

[3] E. Berardini et J. Nardi, preprint 2021
[4] Y. Aubry, E. Berardini, F. Herbaut et M. Perret, Finite Fields Appl. 70 (2021)
[5] Y. Aubry, E. Berardini, F. Herbaut et M. Perret, Contemp. Maths. AMS (2021)

Questions futures

Calcul d'espaces de Riemann–Roch de courbes.

- Implementer l'algorithme (en cours)
- Calculer les espaces de Riemann–Roch de courbes non–ordinaires en caractéristique positive "petite" (en cours)
- Améliorer l'exposant de complexité dans le cas non–ordinaire (sous–quadratique ?)

Questions futures

Calcul d'espaces de Riemann–Roch de courbes.

- Implementer l'algorithme (en cours)
- Calculer les espaces de Riemann–Roch de courbes non–ordinaires en caractéristique positive "petite" (en cours)
- Améliorer l'exposant de complexité dans le cas non–ordinaire (sous–quadratique ?)

Dimension supérieure.

- Obtenir une borne plus fine pour le nombre de points rationnels d'une courbe sur une surface de $\mathbb{P}^n$ donnée (fait pour $n = 3$, en cours pour $n > 3$)
- Appliquer les méthodes développées à l'étude de codes géométriques à partir de variétés de 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.

- Implementer l'algorithme (en cours)
- Calculer les espaces de Riemann–Roch de courbes non–ordinaires en caractéristique positive "petite" (en cours)
- Améliorer l'exposant de complexité dans le cas non–ordinaire (sous–quadratique ?)

Dimension supérieure.

- Obtenir une borne plus fine pour le nombre de points rationnels d'une courbe sur une surface de $\mathbb{P}^n$ donnée (fait pour $n = 3$, en cours pour $n > 3$)
- Appliquer les méthodes développées à l'étude de codes géométriques à partir de variétés de 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