

# A propos du calcul des polynômes de Darboux

G. Chèze

Institut de Mathématiques de Toulouse

Séminaire Algo

# Plan

- 1 Comment en arriver là
- 2 Polynômes de Darboux
- 3 La courbe extatique
- 4 Questions

## Définition

Soit  $P(X, Y) \in \mathbb{Q}[X, Y]$ .

La **factorisation absolue** de  $P$  est la décomposition en irréductibles de  $P$  dans  $\overline{\mathbb{Q}}[X, Y]$ , où  $\overline{\mathbb{Q}}$  est la clôture algébrique de  $\mathbb{Q}$ .

La **factorisation rationnelle** est la factorisation dans  $\mathbb{Q}[X, Y]$ .

**Exemple :**

$$\begin{aligned} P(X, Y) &= Y^4 + 2Y^2X + 14Y^2 - 7X^2 + 6X + 47 \\ &= \left( Y^2 + (2\sqrt{2} + 1)X + \sqrt{2} + 7 \right) \left( Y^2 + (-2\sqrt{2} + 1)X - \sqrt{2} + 7 \right) \end{aligned}$$

## Théorème (W. Ruppert, 1986)

Soit  $f \in \mathbb{Q}[X, Y]$  un polynôme sans facteurs carrés de degré  $d$ .  
On considère :

$$E = \left\{ (G, H) \in (\mathbb{Q}[X, Y]_{\leq d-1})^2 \mid \frac{\partial}{\partial X} \left( \frac{G}{f} \right) = \frac{\partial}{\partial Y} \left( \frac{H}{f} \right) \right\}.$$

alors :

$$\dim_{\mathbb{Q}} E = r,$$

où  $r$  est le nombre de facteurs absolument irréductibles de  $f$ .

⇒ Algorithmes de Gao, Lecerf, C-Lecerf.

# Décomposition

## Définition

Soit  $f(X, Y)/g(X, Y) \in \mathbb{Q}(X, Y)$ ,  
 $f/g$  est **décomposable** lorsque  $f/g$  peut s'écrire :

**$f/g = u(h) = u \circ h$** , avec  $u \in \mathbb{Q}(T)$ ,  **$\deg u \geq 2$** , et  $h \in \mathbb{Q}(X, Y)$ .

Exemple :

$$\frac{f}{g}(X, Y) = \frac{X^2 + XY + 3Y^2}{Y^2} = \left(\frac{X}{Y}\right)^2 + \left(\frac{X}{Y}\right) - 3.$$

$$u(T) = T^2 + T - 3, \quad h(X, Y) = \frac{X}{Y}.$$

- 1 Gutiérrez-Rubio-Sevilla (2001),  $\tilde{O}(2^d)$ .  
Polynômes presque séparés :  
 $f(X, Y)g(U, V) - g(X, Y)f(U, V)$ .  
(C.  $\Rightarrow \tilde{O}(d^{2n+\omega-1})$ )
- 2 Moulin-Ollagnier (2004),  $\tilde{O}(d^{\omega \cdot n})$ .  
Polynômes de Darboux.
- 3 C. (2009),  $\tilde{O}(d^n)$ .  
Spectre d'une fraction rationnelle.

- 1 Gutiérrez-Rubio-Sevilla (2001),  $\tilde{O}(2^d)$ .

Polynômes presque séparés :

$$f(X, Y)g(U, V) - g(X, Y)f(U, V).$$

$$(C. \Rightarrow \tilde{O}(d^{2n+\omega-1}))$$

- 2 Moulin-Ollagnier (2004),  $\tilde{O}(d^{\omega \cdot n})$ .

Polynômes de Darboux.

- 3 C. (2009),  $\tilde{O}(d^n)$ .

Spectre d'une fraction rationnelle.

- 1 Gutiérrez-Rubio-Sevilla (2001),  $\tilde{O}(2^d)$ .  
Polynômes presque séparés :  
 $f(X, Y)g(U, V) - g(X, Y)f(U, V)$ .  
(C.  $\Rightarrow \tilde{O}(d^{2n+\omega-1})$ )
- 2 Moulin-Ollagnier (2004),  $\tilde{O}(d^{\omega \cdot n})$ .  
Polynômes de Darboux.
- 3 C. (2009),  $\tilde{O}(d^n)$ .  
Spectre d'une fraction rationnelle.

## Définition

$$D = A(X, Y)\partial_X + B(X, Y)\partial_Y,$$

où  $\deg A, \deg B \leq d$ , et  $\|A\|_\infty, \|B\|_\infty \leq \mathcal{H}$ .

## Définition

Soit  $f \in \mathbb{C}[X, Y]$ . On dit que  $f$  est un **polynôme de Darboux** pour  $D$  s'il existe  $g \in \mathbb{C}[X, Y]$  tel que :

$$D(f) = g.f.$$

On dit que  $g$  est le **cofacteur** de  $f$ .

Notation :  $g = \text{cof}(f)$ .

Etude des solutions de

$$(*) \begin{cases} \dot{X} = A(X, Y), \\ \dot{Y} = B(X, Y), \end{cases} \quad \text{avec } A(X, Y), B(X, Y) \in \mathbb{Q}[X, Y].$$

**On cherche  $\mathcal{F}$  tel que  $\mathcal{F}(X(t), Y(t)) = c$ .**

On dit que  $\mathcal{F}$  est une **intégrale première**.

## Définition

*$\mathcal{F}$  est une intégrale première signifie  $D(\mathcal{F}) = 0$ .*

## Proposition

Soit  $f = f_1 \cdot f_2$  où  $f_1, f_2$  sont premiers entre eux.

$f$  est un polynôme de *Darboux*.



$f_1$  et  $f_2$  sont des polynômes de *Darboux*.

De plus  $\text{cof}(f) = \text{cof}(f_1) + \text{cof}(f_2)$ .

## Proposition

$$D(p/q) = 0 \iff \text{cof}(p) = \text{cof}(q)$$

Remarque :

$$\text{cof}(p) = \text{cof}(q) \Rightarrow \text{cof}(\lambda p + \mu q) = \text{cof}(p) = \text{cof}(q).$$

$p/q \in \mathbb{C}(X, Y)$  intégrale première  $\Rightarrow \infty$  polynômes de Darboux.

## Proposition

$$D(p/q) = 0 \iff \text{cof}(p) = \text{cof}(q)$$

Remarque :

$\text{cof}(p) = \text{cof}(q) \Rightarrow \text{cof}(\lambda p + \mu q) = \text{cof}(p) = \text{cof}(q)$ .

$p/q \in \mathbb{C}(X, Y)$  intégrale première  $\Rightarrow \infty$  polynômes de Darboux.

# Théorème de Darboux

## Théorème

Soient  $A, B \in \mathbb{Z}[X, Y]$ ,  $D = A\partial_X + B\partial_Y$ .

Soient  $f_1, \dots, f_m \in \mathbb{C}[X, Y]$  des polynômes de Darboux irréductibles de  $D$ .

Si  $m \geq d(d+1)/2 + 2$ , alors il existe  $n_i \in \mathbb{Z}$  tels que :

$$f = \prod_{i=1}^m f_i^{n_i} \text{ est une intégrale première.}$$

Dans ce cas il existe une *infinité* de polynômes de Darboux.

## Méthode :

- 1 Trouver  $d(d+1)/2 + 2$  polynômes de Darboux irréductibles.
- 2 Résoudre  $\sum_i n_i \text{cof}(f_i) = 0$ , avec  $n_i \in \mathbb{Z}$ .
- 3 Rendre  $f = \prod_i f_i^{n_i} \in \mathbb{C}(X, Y)$ .

Preuve :  $\text{cof}(f) = \sum_i n_i \text{cof}(f_i) = 0$ .

## Méthode :

- 1 Trouver  $d(d+1)/2 + 2$  polynômes de Darboux irréductibles.
- 2 Résoudre  $\sum_i n_i \text{cof}(f_i) = 0$ , avec  $n_i \in \mathbb{Z}$ .
- 3 Rendre  $f = \prod_i f_i^{n_i} \in \mathbb{C}(X, Y)$ .

Preuve :  $\text{cof}(f) = \sum_i n_i \text{cof}(f_i) = 0$ .

# Comment obtenir une intégrale première

On cherche  $R$  un **facteur intégrant** :

$$\partial_X(RA) = -\partial_Y(RB) \iff D(R) = -\operatorname{div}(A, B) \cdot R.$$

$$\mathcal{F} = \int RBdX - RAdY \text{ est une intégrale première.}$$

Preuve :

$$\begin{aligned}(\mathcal{F}(X(t), Y(t)))' &= A\partial_X\mathcal{F} + B\partial_Y\mathcal{F} \\ &= A\partial_X \int RBdX - RAdY \\ &\quad + B\partial_Y \int RBdX - RAdY \\ &= -A \int \partial_X(RA)dY + B \int \partial_Y(RB)dX \\ &= 0\end{aligned}$$

# Méthode de Prelle-Singer

**Idée :** Chercher un “polynôme” de Darboux ayant pour cofacteur  $-\operatorname{div}(A, B)$  en résolvant :

$$\sum_i n_i \operatorname{cof}(f_i) = -\operatorname{div}(A, B).$$

$\Rightarrow R = \prod_i f_i^{n_i}$  est un facteur intégrant,  $R \in \mathbb{C}(X, Y)^{1/K}$ .

Seuls les  $f_i$  irréductibles sont utiles.

**Idée :** Chercher un “polynôme” de Darboux ayant pour cofacteur  $-\operatorname{div}(A, B)$  en résolvant :

$$\sum_i n_i \operatorname{cof}(f_i) = -\operatorname{div}(A, B).$$

$\Rightarrow R = \prod_i f_i^{n_i}$  est un facteur intégrant,  $R \in \mathbb{C}(X, Y)^{1/K}$ .

**Seuls les  $f_i$  irréductibles sont utiles.**

# Méthode de Prelle-Singer

**Idée :** Chercher un polynôme de Darboux ayant pour cofacteur  $-\operatorname{div}(A, B)$  en résolvant :

$$\sum_i n_i \operatorname{cof}(f_i) = -\operatorname{div}(A, B).$$

$\Rightarrow R = \prod_i f_i^{n_i}$  est un facteur intégrant,  $R \in \mathbb{C}(X, Y)^{1/K}$ .

## Théorème (Prelle-Singer, 1983)

(\*) possède une intégrale première élémentaire.



Il existe un facteur intégrant  $R(X, Y) \in \mathbb{C}(X, Y)^{1/K}$ .

# Méthode des coefficients indéterminés

**Objectif** : Trouver les polynômes de Darboux de degré  $\leq N$ .

**Méthode** : Résolution du **système polynomial** :  $D(f) = g.f$ ,  
où les coefficients de  $g$  et  $f$  sont indéterminés.

**Problèmes** :

- 1 Comment borner  $N$  a priori ?
- 2 Le système polynomial est de degré 2, avec  $\mathcal{O}((d + N)^2)$  équations et  $\mathcal{O}(d^2 + N^2)$  variables.  
**Pas de structure simple à exploiter !**

# Méthode des coefficients indéterminés

**Objectif** : Trouver les polynômes de Darboux de degré  $\leq N$ .

**Méthode** : Résolution du **système polynomial** :  $D(f) = g.f$ ,  
où les coefficients de  $g$  et  $f$  sont indéterminés.

## Problèmes :

- 1 Comment borner  $N$  a priori ?
- 2 Le système polynomial est de degré 2, avec  $\mathcal{O}((d + N)^2)$  équations et  $\mathcal{O}(d^2 + N^2)$  variables.  
**Pas de structure simple à exploiter !**

# Méthode des coefficients indéterminés

**Objectif** : Trouver les polynômes de Darboux de degré  $\leq N$ .

**Méthode** : Résolution du **système polynomial** :  $D(f) = g.f$ ,  
où les coefficients de  $g$  et  $f$  sont indéterminés.

**Problèmes** :

- 1 Comment borner  $N$  a priori ?
- 2 Le système polynomial est de degré 2, avec  $\mathcal{O}((d + N)^2)$  équations et  $\mathcal{O}(d^2 + N^2)$  variables.

**Pas de structure simple à exploiter !**

## Problème :

$X^n - Y^{n+1}$  est un polynôme de Darboux irréductible de

$$D = (n + 1)X\partial_X + nY\partial_Y.$$



On ne peut pas borner  $N$  en fonction de  $d$ .

# Nombre exponentiel de solutions

## Proposition

Soit

$$D = (\partial_Y \mathcal{F}) \partial_X - (\partial_X \mathcal{F}) \partial_Y, \text{ où } \mathcal{F}(X, Y) = Y \prod_{i=1}^{d-1} (X + i) + X.$$

La dérivation  $D$  possède **au moins**  $2^{d-1} + 1$  **polynômes de Darboux** de degré  $\leq d$ .

Preuve :  $(X + i)$  Darboux  $\Rightarrow \prod_i (X + i)$  Darboux.

**Problème : Recombinaison des facteurs irréductibles.**

# Nombre exponentiel de solutions

## Proposition

Soit

$$D = (\partial_Y \mathcal{F}) \partial_X - (\partial_X \mathcal{F}) \partial_Y, \text{ où } \mathcal{F}(X, Y) = Y \prod_{i=1}^{d-1} (X + i) + X.$$

La dérivation  $D$  possède **au moins**  $2^{d-1} + 1$  **polynômes de Darboux** de degré  $\leq d$ .

Preuve :  $(X + i)$  Darboux  $\Rightarrow \prod_i (X + i)$  Darboux.

**Problème : Recombinaison des facteurs irréductibles.**

# Nombre exponentiel de solutions

## Proposition

Soit

$$D = (\partial_Y \mathcal{F}) \partial_X - (\partial_X \mathcal{F}) \partial_Y, \text{ où } \mathcal{F}(X, Y) = Y \prod_{i=1}^{d-1} (X + i) + X.$$

La dérivation  $D$  possède **au moins**  $2^{d-1} + 1$  **polynômes de Darboux** de degré  $\leq d$ .

Preuve :  $(X + i)$  Darboux  $\Rightarrow \prod_i (X + i)$  Darboux.

**Problème : Recombinaison des facteurs irréductibles.**

## Définition

Soit  $D$  une dérivation, la *Nième courbe extatique* de  $D$ ,  $\mathcal{E}_{\mathcal{B},N}(D)$ , est le polynôme

$$\mathcal{E}_{\mathcal{B},N}(D) = \det \begin{pmatrix} v_1 & v_2 & \cdots & v_l \\ D(v_1) & D(v_2) & \cdots & D(v_l) \\ \vdots & \vdots & \cdots & \vdots \\ D^{l-1}(v_1) & D^{l-1}(v_2) & \cdots & D^{l-1}(v_l) \end{pmatrix},$$

où  $\mathcal{B} = \{v_1, v_2, \dots, v_l\}$  est une base de  $\mathbb{C}[X, Y]_{\leq N}$ ,  
 $l = (N+1)(N+2)/2$ , and  $D^k(v_i) = D(D^{k-1}(v_i))$ .

## Proposition

Soient  $\mathcal{B}$  et  $\mathcal{B}'$  deux bases de  $\mathbb{C}[X, Y]_{\leq N}$ .

$$\mathcal{E}_{\mathcal{B}, N}(D) = c \cdot \mathcal{E}_{\mathcal{B}', N}(D),$$

où  $c \in \mathbb{C}$ .

**Notation :**  $\mathcal{E}_N(D) := \mathcal{E}_{\mathcal{B}, N}(D)$ , où  $\mathcal{B}$  est la base monomiale.

## Proposition (Pereira, 2001)

*Les polynômes de Darboux de degré  $\leq N$  sont des facteurs de  $\mathcal{E}_N(D)$ .*

Exemple :

$$D = -2X^2\partial_X + (1 - 4XY)\partial_Y$$

$$\Rightarrow \mathcal{E}_1(D) = YX^4.$$

$D(X) = -2X.X \Rightarrow X$  est un polynome de Darboux.

$D(Y) = 1 - 4XY \Rightarrow Y$  n'est pas un polynôme de Darboux.

Soit  $f$  un polynôme de Darboux de degré  $\leq N$ .  
Prendre une base telle que  $v_1 = f$ .

$$\begin{aligned}D(f) &= g_1 f, \\D^2(f) &= D(g_1 f) = (g_1^2 + D(g_1))f = g_2 f, \\D^{l-1}(f) &= g_{l-1} f,\end{aligned}$$

où  $g_1, g_2, \dots, g_{l-1}$  sont des polynômes.  
Donc  $f$  est un facteur de  $\mathcal{E}_N(D)$ .

## Proposition (Pereira, 2001)

$$\mathcal{E}_N(D) = 0 \text{ et } \mathcal{E}_{N-1}(D) \neq 0$$



*D a une intégrale première rationnelle de degré N.*

↑).  $D$  a une intégrale première  $p/q \in \mathbb{C}(X, Y)$ .

$D$  a une infinité de polynômes de Darboux de degré  $N : \lambda p + \mu q$ .

$\mathcal{E}_N(D)$  a une infinité de facteurs non triviaux de degré  $N$ .

$\mathcal{E}_N(D) = 0$ .

# L'algorithme

## Lagutinskii-Pereira's algorithm

**Input :**  $D = A(X, Y)\partial_X + B(X, Y)\partial_Y$ , et  $N \in \mathbb{N}$ .

**Output :**  $S$  l'ensemble de **tous les polynômes de Darboux irréductibles** de  $D$  de degré  $\leq N$  ou “ $\infty$  de Darboux”.

- 1  $S = \{\}$ .
- 2 Calculer  $\mathcal{E}_N(D)$ .
- 3 Si  $\mathcal{E}_N(D) = 0$  alors Rendre “ $\infty$  de Darboux ” sinon aller à l'étape 4.
- 4 Calculer  $f_1, \dots, f_m$  les facteurs absolument irréductibles de degré  $\leq N$  de  $\mathcal{E}_N(D)$ .
- 5 Pour  $i := 1, \dots, m$  faire : Si  $\gcd(f_i, D(f_i)) = f_i$  alors ajouter  $f_i$  à  $S$ .
- 6 Rendre  $S$ .

## Lagutinskii-Pereira's algorithm

**Input :**  $D = A(X, Y)\partial_X + B(X, Y)\partial_Y$ , et  $N \in \mathbb{N}$ .

**Output :**  $S$  l'ensemble de **tous les polynômes de Darboux irréductibles** de  $D$  de degré  $\leq N$  ou “ $\infty$  de Darboux”.

- 1  $S = \{\}$ .
- 2 Calculer  $\mathcal{E}_N(D)$ .
- 3 Si  $\mathcal{E}_N(D) = 0$  alors Rendre “ $\infty$  de Darboux ” sinon aller à l'étape 4.
- 4 Calculer  $f_1, \dots, f_m$  les facteurs absolument irréductibles de degré  $\leq N$  de  $\mathcal{E}_N(D)$ .
- 5 Pour  $i := 1, \dots, m$  faire : Si  $\gcd(f_i, D(f_i)) = f_i$  alors ajouter  $f_i$  à  $S$ .
- 6 Rendre  $S$ .

# Complexité : Définitions.

- **Complexité algébrique.**

$\mathbb{K}$  est un corps commutatif, on compte les opérations arithmétiques :  $+$ ,  $-$ ,  $\times$ ,  $\div$ .

- **Complexité binaire.**

On compte le nombre d'opérations sur les bits.

Complexité binaire  $\leq$  Complexité algébrique  $\times$  Taille des objets manipulés.

$$\text{Taille}(f(X, Y)) = \deg(f)^2 \cdot \log(\|f\|_\infty).$$

# Complexité : Définitions.

- **Complexité algébrique.**

$\mathbb{K}$  est un corps commutatif, on compte les opérations arithmétiques :  $+$ ,  $-$ ,  $\times$ ,  $\div$ .

- **Complexité binaire.**

On compte le nombre d'opérations sur les bits.

Complexité binaire  $\leq$  Complexité algébrique  $\times$  Taille des objets manipulés.

$$\text{Taille}(f(X, Y)) = \deg(f)^2 \cdot \log(\|f\|_\infty).$$

## Théorème

Soit  $D = A(X, Y)\partial_X + B(X, Y)\partial_Y$  telle que  $A(X, Y), B(X, Y) \in \mathbb{Z}[X, Y]$ ,  $\deg A \leq d$ ,  $\deg B \leq d$ ,  $\|A\|_\infty \leq \mathcal{H}$ ,  $\|B\|_\infty \leq \mathcal{H}$  et  $A, B$  sont premiers entre eux.

- 1 On peut décider s'il existe un nombre fini de polynômes de Darboux irréductibles de degré  $\leq N$  de manière déterministe avec  $\mathcal{O}\left((dN \log(\mathcal{H}))^{\mathcal{O}(1)}\right)$  bit-operations.
- 2 Si le nombre de polynômes de Darboux irréductibles de degré  $\leq N$  est fini alors nous pouvons tous les calculer de manière déterministe avec  $\mathcal{O}\left((dN \log(\mathcal{H}))^{\mathcal{O}(1)}\right)$  bit-operations.

## Théorème

Soit  $D = A(X, Y)\partial_X + B(X, Y)\partial_Y$  telle que  $A(X, Y), B(X, Y) \in \mathbb{Z}[X, Y]$ ,  $\deg A \leq d$ ,  $\deg B \leq d$ ,  $\|A\|_\infty \leq \mathcal{H}$ ,  $\|B\|_\infty \leq \mathcal{H}$  et  $A, B$  sont premiers entre eux.

- 1 On peut décider s'il existe un nombre fini de polynômes de Darboux irréductibles de degré  $\leq N$  de manière déterministe avec  $\mathcal{O}\left((dN \log(\mathcal{H}))^{\mathcal{O}(1)}\right)$  bit-operations.
- 2 Si le nombre de polynômes de Darboux irréductibles de degré  $\leq N$  est fini alors nous pouvons tous les calculer de manière déterministe avec  $\mathcal{O}\left((dN \log(\mathcal{H}))^{\mathcal{O}(1)}\right)$  bit-operations.

- 1  $\deg \mathcal{E}_N(D) \leq \mathcal{O}(dN^4),$
- 2  $\|\mathcal{E}_N(D)\|_\infty \leq \left(2N^2\mathcal{H}(N^2(d-1) + N)^3\right)^{N^4},$
- 3  $\text{Taille}(\mathcal{E}_N(D)) \in \mathcal{O}\left((dN \log(\mathcal{H}))^{\mathcal{O}(1)}\right).$

## Problème :

$\mathcal{E}_N(D) = 0 \Rightarrow$  Pas de facteurs à calculer !

## Définition

Soit  $D$  une dérivation,  $\mathcal{E}_{N,0}(D)$ , est le polynôme  $\mathcal{E}_{\mathcal{B}_0,N}(D)$  où  $\mathcal{B}_0$  est la base monomiale de  $\mathbb{C}[X, Y]_{\leq N} \cap \{P(0,0) = 0\}$ .

# Propriétés de $\mathcal{E}_{N,0}(D)$

## Proposition

Soit  $p/q \in \mathbb{Q}(X, Y)$  une intégrale première de  $D$  indécomposable tel que  $\deg(p/q) = N$ .

- 1 On a  $\mathcal{E}_{N,0}(D) \neq 0$  dans  $\mathbb{Q}[X, Y]$ .
- 2 Si on pose  $(\lambda_0, \mu_0) = (-q(0,0), p(0,0))$  alors  $\lambda_0 p + \mu_0 q$  est un facteur de  $\mathcal{E}_{N,0}(D)$ .

Rappel :  $\text{cof}(\lambda_0 p + \mu_0 q) = \text{cof}(p) = \text{cof}(q)$ .

## Lemme

$$\begin{aligned}\mathcal{L}_g : \mathbb{Q}[X, Y]_{\leq N} &\longrightarrow \mathbb{Q}[X, Y]_{\leq N+d-1} \\ f &\longmapsto D(f) - g.f\end{aligned}$$

Si  $D$  a une intégrale première  $p/q \in \mathbb{Q}(X, Y)$  telle que  $\deg(p/q) \leq N$  et  $g$  est le cofacteur de  $p$  et  $q$  alors  $\dim_{\mathbb{Q}} \ker \mathcal{L}_g = 2$  et si  $\{\tilde{p}, \tilde{q}\}$  est une base de  $\ker \mathcal{L}_g$  alors  $\tilde{p}/\tilde{q}$  est une intégrale première de  $D$ .

# L'algorithme

## Algorithm Rat-First-Int

Input :  $D = A(X, Y)\partial_X + B(X, Y)\partial_Y$ ,  $N \in \mathbb{N}$ .

Output : Une intégrale première rationnelle de degré  $\leq N$  ou "YEN-NA-PAS".

- 1 Calculer  $\mathcal{E}_N(D)$ .
- 2 Si  $\mathcal{E}_N(D) \neq 0$  alors Rendre "YEN-NA-PAS" sinon aller à l'étape 3.
- 3 Calculer le plus petit entier  $n$  tel que  $\mathcal{E}_n(D) = 0$  et  $\mathcal{E}_{n-1}(D) \neq 0$ .
- 4 Calculer  $\mathcal{E}_{n,0}(D)$ .
- 5 Trouver le facteur irréductible de degré  $n$  qui est un polynôme de Darboux.
- 6 Calculer son cofacteur :  $g$ .
- 7 Calculer une base  $\{\tilde{p}, \tilde{q}\}$  de  $\ker \mathcal{L}_g$ .
- 8 Rendre  $\tilde{p}/\tilde{q}$ .

# L'algorithme

## Algorithm Rat-First-Int

Input :  $D = A(X, Y)\partial_X + B(X, Y)\partial_Y$ ,  $N \in \mathbb{N}$ .

Output : Une intégrale première rationnelle de degré  $\leq N$  ou “YEN-NA-PAS”.

- 1 Calculer  $\mathcal{E}_N(D)$ .
- 2 Si  $\mathcal{E}_N(D) \neq 0$  alors Rendre “YEN-NA-PAS” sinon aller à l'étape 3.
- 3 Calculer le plus petit entier  $n$  tel que  $\mathcal{E}_n(D) = 0$  et  $\mathcal{E}_{n-1}(D) \neq 0$ .
- 4 Calculer  $\mathcal{E}_{n,0}(D)$ .
- 5 Trouver le facteur irréductible de degré  $n$  qui est un polynôme de Darboux.
- 6 Calculer son cofacteur :  $g$ .
- 7 Calculer une base  $\{\tilde{p}, \tilde{q}\}$  de  $\ker \mathcal{L}_g$ .
- 8 Rendre  $\tilde{p}/\tilde{q}$ .

## Algorithm Rat-First-Int

Input :  $D = A(X, Y)\partial_X + B(X, Y)\partial_Y$ ,  $N \in \mathbb{N}$ .

Output : Une intégrale première rationnelle de degré  $\leq N$  ou “YEN-NA-PAS”.

- 1 Calculer  $\mathcal{E}_N(D)$ .
- 2 Si  $\mathcal{E}_N(D) \neq 0$  alors Rendre “YEN-NA-PAS” sinon aller à l'étape 3.
- 3 Calculer le plus petit entier  $n$  tel que  $\mathcal{E}_n(D) = 0$  et  $\mathcal{E}_{n-1}(D) \neq 0$ .
- 4 Calculer  $\mathcal{E}_{n,0}(D)$ .
- 5 Trouver le facteur irréductible de degré  $n$  qui est un polynôme de Darboux.
- 6 Calculer son cofacteur :  $g$ .
- 7 Calculer une base  $\{\tilde{p}, \tilde{q}\}$  de  $\ker \mathcal{L}_g$ .
- 8 Rendre  $\tilde{p}/\tilde{q}$ .

## Théorème

Soit  $D = A(X, Y)\partial_X + B(X, Y)\partial_Y$  telle que  
 $A(X, Y), B(X, Y) \in \mathbb{Z}[X, Y]$ ,  $\deg A \leq d$ ,  $\deg B \leq d$ ,  $\|A\|_\infty \leq \mathcal{H}$ ,  
 $\|B\|_\infty \leq \mathcal{H}$  et  $A, B$  sont premiers entre eux.

- 1 On peut décider s'il existe une intégrale première rationnelle de degré  $\leq N$  avec  $\mathcal{O}\left((dN \log(\mathcal{H}))^{O(1)}\right)$  bit-operations.
- 2 S'il existe une intégrale première rationnelle de degré  $\leq N$  alors nous pouvons la calculer de manière déterministe avec  $\mathcal{O}\left((dN \log(\mathcal{H}))^{O(1)}\right)$  bit-operations.

## Théorème

Soit  $D = A(X, Y)\partial_X + B(X, Y)\partial_Y$  telle que  
 $A(X, Y), B(X, Y) \in \mathbb{Z}[X, Y]$ ,  $\deg A \leq d$ ,  $\deg B \leq d$ ,  $\|A\|_\infty \leq \mathcal{H}$ ,  
 $\|B\|_\infty \leq \mathcal{H}$  et  $A, B$  sont premiers entre eux.

- 1 On peut décider s'il existe une intégrale première rationnelle de degré  $\leq N$  avec  $\mathcal{O}\left((dN \log(\mathcal{H}))^{\mathcal{O}(1)}\right)$  bit-operations.
- 2 S'il existe une intégrale première rationnelle de degré  $\leq N$  alors nous pouvons la calculer de manière déterministe avec  $\mathcal{O}\left((dN \log(\mathcal{H}))^{\mathcal{O}(1)}\right)$  bit-operations.

# Questions

# Comment calculer des solutions Liouvilliennes

## Théorème (Singer, 1992)

$$\begin{cases} \dot{X} = A(X, Y), \\ \dot{Y} = B(X, Y). \end{cases} \quad \text{a une intégrale première Liouvillienne}$$

ssi

$$\begin{cases} \dot{X} = B(X, Y), \\ \dot{Y} = -A(X, Y), \end{cases} \quad \text{a un facteur intégrant de la forme :}$$

$$R = \exp \int U dX + V dY, \quad \text{avec } U, V \in \mathbb{K}(X, Y) \text{ et } \partial_Y U = \partial_X V.$$

## Théorème

Soient  $f = f_1^{e_1} \cdots f_r^{e_r}$ ,  $U = \frac{U_1}{f}$ ,  $V = \frac{V_1}{f}$ , tels que :  $\partial_Y U = \partial_X V$ ,  
alors

$$\begin{cases} U = \sum_i c_i \partial_X \log f_i + \partial_X \left( \frac{P}{Q} \right) \\ V = \sum_i c_i \partial_Y \log f_i + \partial_Y \left( \frac{P}{Q} \right) \end{cases}$$

# Le théorème de Christopher, 1999

Singer, 1992

$$\Rightarrow R = \exp \int U dX + V dY, \text{ avec } U, V \in \mathbb{K}(X, Y) \text{ et } \partial_Y U = \partial_X V.$$

Ruppert, 1986

$$\Rightarrow R = \exp \int \sum_i c_i \partial_X \log f_i + \partial_X \left( \frac{P}{Q} \right) dX + \sum_i c_i \partial_Y \log f_i + \partial_Y \left( \frac{P}{Q} \right) dY$$

$$\Rightarrow R = \prod_i f_i^{c_i} \exp \left( \frac{P}{Q} \right).$$

Lien facteur exponentiel, et courbe extatique dans  
Christopher-Llibre-Pereira, 2007...

# Le théorème de Christopher, 1999

Singer, 1992

$$\Rightarrow R = \exp \int U dX + V dY, \text{ avec } U, V \in \mathbb{K}(X, Y) \text{ et } \partial_Y U = \partial_X V.$$

Ruppert, 1986

$$\Rightarrow R = \exp \int \sum_i c_i \partial_X \log f_i + \partial_X \left( \frac{P}{Q} \right) dX + \sum_i c_i \partial_Y \log f_i + \partial_Y \left( \frac{P}{Q} \right) dY$$

$$\Rightarrow R = \prod_i f_i^{c_i} \exp \left( \frac{P}{Q} \right).$$

Lien facteur exponentiel, et courbe extatique dans  
Christopher-Llibre-Pereira, 2007...

## Définition

On dit que  $R \in \mathbb{Q}[X, Y]$  est un *facteur intégrant inverse* lorsque :

$$D(R) = \operatorname{div}(A, B).R.$$

## Proposition (Giacomini-Llibre-Viano, 1996)

*Les cycles limites algébriques d'un champ de vecteur polynomial correspondant à  $D$  sont des facteurs de  $R$ .*

## Proposition

*R est un facteur intégrant inverse*

$$A\partial_x R + B\partial_y R = \operatorname{div}(A, B)R$$

$$\partial_x \left( \frac{A}{R} \right) = \partial_y \left( \frac{B}{R} \right).$$

⇒ Peut on calculer  $R$  avec la même complexité que celle de la factorisation absolue ?

## Proposition

*R est un facteur intégrant inverse*

$$A\partial_x R + B\partial_y R = \operatorname{div}(A, B)R$$

$$\partial_x \left( \frac{A}{R} \right) = \partial_y \left( \frac{B}{R} \right).$$

⇒ Peut on calculer  $R$  avec la même complexité que celle de la factorisation absolue ?