Lifting and Recombination Techniques for Absolute Factorization

G. CHEZE

Laboratoire J.-A. Dieudonné,

Université de Nice Sophia-Antipolis

FRANCE

Joint work with

G. LECERF

DEFINITION

Definition : Let $\mathbb{K}$ be a commutative field, and $F(X,Y) \in \mathbb{K}[X,Y]$.
The absolute factorization of F is the irreducible factorization over the algebraic closure $\overline{\mathbb{K}}$ of $\mathbb{K}$.
The rational factorization is the factorization in $\mathbb{K}[X,Y]$.

Motivation

- **Effective Algebraic Geometry.** Chistov/Grigoriev 84.
- **Kinematics.** Sommese/Verschelde/Wampler 04.
- **Linear Differential Equation Solving.** Singer/Ulmer 97.
- **Symbolic Integration.** Rothstein 76, Trager 76, Lazard/Rioboo 90.

Related Works

Symbolic-Numeric methods ($\mathbb{K} = \mathbb{Q}$) :

- **Bajaj/Canny/Garrity/Warren 93** : Find the connected component of $\mathcal{V}(F)$.
- **Sasaki 01** : zero sums.
- **Corless/Galligo/Kotsireas/Watt 02, Galligo/Rupprecht 02** : monodromy , and zero sums.
- **Sommese/Verschelde/Wampler 02** : monodromy and homotopy continuation.
- **Gao/Kaltofen/May/Yang/Zhi 04** : approximate absolute factorization.
- **Chèze 04** : monodromy, zero sums and LLL.

Related Works

Symbolic methods :

- **Trager 85, Kaltofen 85, Traverso/Dvornicich 89** : reduction to compute in an algebraic extension of $\mathbb{K}$.
- **Ruppert 86, 99** : closed forms.
- **Duval 91, Ragot 97** : integral basis.
- **Cormier/Singer/Trager/Ulmer 02** : differential operators.
- **Gao 03** : closed forms (probabilistic algorithm, $\tilde{\mathcal{O}}(d^5)$).

- **Lecerf 04** : rational factorization algorithm following a “lifting and recombination “ scheme (recombination probabilistic algorithm $\tilde{\mathcal{O}}(d^\omega)$; deterministic algorithm $\tilde{\mathcal{O}}(d^{\omega+1})$).

RELATED WORKS

Symbolic methods :

• **Trager 85, Kaltofen 85, Traverso/Dvornicich 89** : reduction to compute in an algebraic extension of $\mathbb{K}$

• **Ruppert 86, 99** : closed forms.

• **Duval 91, Ragot 97** : integral basis.

• **Cormier/Singer/Trager/Ulmer 02** : differential operators.

• **Gao 03** : closed forms (probabilistic algorithm, $\tilde{\mathcal{O}}(d^4)$).

• **Lecerf 04** : rational factorization algorithm following a “lifting and recombination “ scheme (recombination probabilistic algorithm $\tilde{\mathcal{O}}(d^\omega)$; deterministic algorithm $\tilde{\mathcal{O}}(d^{\omega+1})$).

Notations

Hypothesis (H) **:** $\begin{cases} (i)\ \ \deg_Y(F) = \deg(F) = d; \\ (ii)\ \mathrm{Res}_Y\left(F, \dfrac{\partial F}{\partial Y}\right)(0) \neq 0. \end{cases}$

Hypothesis (C) **:** $\mathbb{K}$ has caracteristic 0 or at least $d(d-1)+1$.

Gao's Theorem

THEOREM [S. Gao]. Let

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

Under hypothesis (C) and (H), we have :

1. $\dim_{\mathbb{K}} E = r$, where r is the number of absolute irreducible factors.
2. $(G_i, H_i) = \left(\hat{F}_i \dfrac{\partial F_i}{\partial X}, \hat{F}_i \dfrac{\partial F_i}{\partial Y}\right)$ is basis of $E \otimes \overline{\mathbb{K}}$, where $\hat{F}_i = \displaystyle\prod_{j=1, j\neq i}^{r} F_i$.

How to find an absolute factor

THEOREM. Let $G = \sum_{i=1}^{r} c_i G_i$, where all the c_i are distincts, $g(Y) = G(0, Y)$, $f(Y) = F(0, Y)$, and $\delta = \mathrm{Disc}(f)$.

Then we have :

1. $\mathrm{Res}_Y(f, zf' - g(Y)) = \delta q^{d/r}$, where $q(z) = \prod_{i=1}^{r}(z - c_i)$.
2. $F_1 = \gcd(F, c_1 \dfrac{\partial F}{\partial Y} - G)$.

Gao's Algorithm

Input : $F(X,Y) \in \mathbb{K}[X,Y]$
Output : Irreducible factors of F in $\overline{\mathbb{K}}[X,Y]$

Overview :

1. Compute a basis of E. (Solve a linear system with $O(d^2)$ unknowns).
2. Pick a random element (G,H) in E. Set $g(Y) = G(0,Y)$.
3. Compute the squarefree part of q of $\mathrm{Res}_Y(f, zf' - g)$.
   If $\deg q \leq r - 1$ then go to step 2.
4. For each factor $q_i(z) \in \mathbb{K}[z]$ of q,
   compute $F_i = \gcd(F, \alpha_i \dfrac{\partial F}{\partial Y} - G)$ where α_i is a root of q_i.

Lecerf's rational factorization theorem

We have : $F = \prod_{j=1}^{t} \mathfrak{F}_j$, where $\mathfrak{F}_j$ is irreducible in $\mathbb{K}[[X]][Y]$.

We want : $F = F_1 \cdots F_r$, where F_i is irreducible in $\mathbb{K}[X,Y]$.

1. $F_i = \prod_{j=1}^{t} \mathfrak{F}_j^{\mu_{F_i,j}}$, where $\mu_{F_i} \in \{0,1\}^t$.

LECERF'S RATIONAL FACTORIZATION THEOREM

We have : $F = \prod_{j=1}^{t} \mathfrak{F}_j$, where $\mathfrak{F}_j$ is irreducible in $\mathbb{K}[[X]][Y]$.

We want : $F = F_1 \cdots F_r$, where F_i is irreducible in $\mathbb{K}[X,Y]$.

1. $F_i = \prod_{j=1}^{t} \mathfrak{F}_j^{\mu_{F_i,j}}$, where $\mu_{F_i} \in \{0,1\}^t$.

2. $G_i = \hat{F}_i \frac{\partial F_i}{\partial Y} = \sum_{j=1}^{t} \mu_{F_i,j} \frac{\partial \mathfrak{F}_j}{\partial Y} \hat{\mathfrak{F}}_i$, where $\hat{\mathfrak{F}}_i = \prod_{k=1, k\neq i} \mathfrak{F}_k$.

$(H_i = \sum_{j=1}^{t} \mu_{F_i,j} \frac{\partial \mathfrak{F}_j}{\partial X} \hat{\mathfrak{F}}_j)$.

Lecerf's rational factorization theorem

We have : $F = \prod_{j=1}^{t} \mathfrak{F}_j$, where $\mathfrak{F}_j$ is irreducible in $\mathbb{K}[[X]][Y]$.

We want : $F = F_1 \cdots F_r$, where F_i is irreducible in $\mathbb{K}[X,Y]$.

1. $F_i = \prod_{j=1}^{t} \mathfrak{F}_j^{\mu_{F_i,j}}$, where $\mu_{F_i} \in \{0,1\}^t$.

2. $G_i = \hat{F}_i \dfrac{\partial F_i}{\partial Y} = \sum_{j=1}^{t} \mu_{F_i,j} \dfrac{\partial \mathfrak{F}_j}{\partial Y} \hat{\mathfrak{F}}_i$, where $\hat{\mathfrak{F}}_i = \prod_{k=1, k\neq i} \mathfrak{F}_k$.

$\left(H_i = \sum_{j=1}^{t} \mu_{F_i,j} \dfrac{\partial \mathfrak{F}_j}{\partial X} \hat{\mathfrak{F}}_j\right)$.

3. $$R_{\sigma}^{\mathbb{K}} = \left\{ (\mu, G, H) \in \mathbb{K}^t \times (\mathbb{K}[X,Y]_{d-1})^2 \mid \quad G = \sum_{j=1}^{t} \mu_j \frac{\partial \mathfrak{F}_j}{\partial Y} \hat{\mathfrak{F}}_i \mod (X,Y)^{\sigma}, \right.$$
$$\left. H = \sum_{j=1}^{t} \mu_j \frac{\partial \mathfrak{F}_j}{\partial Y} \hat{\mathfrak{F}}_j \mod (X,Y)^{\sigma} + (X)^{\sigma-1} \right\}.$$

LECERF'S RATIONAL FACTORIZATION THEOREM

THEOREM [Lec04]. If the hypotheses (C) and (H) are satisfied, and $\sigma \geq 2d$ then :

1. $\dim_{\mathbb{K}} R_\sigma^{\mathbb{K}} = r$.
2. $R_\sigma^{\mathbb{K}} = Span_{\mathbb{K}}(\mu_{F_i}, \hat{F}_i \frac{\partial F_i}{\partial Y}, \hat{F}_i \frac{\partial F_i}{\partial Y})$.

ABSOLUTE FACTORIZATION

Notations :

- $F(X,Y) \in \mathbb{K}[X,Y]$,
- $F = F_1 \cdots F_r$, where F_i is irreducible in $\overline{\mathbb{K}}[X,Y]$.

THEOREM. If the hypotheses (C) and (H) are satisfied, and $\sigma \geq 2d$ then :

1. $\dim_{\overline{\mathbb{K}}} R_\sigma^{\overline{\mathbb{K}}} = r$, where r is the number of absolute irreducible factors.
2. $R_\sigma^{\overline{\mathbb{K}}} = Span_{\overline{\mathbb{K}}}(\mu_{F_i}, \hat{F}_i \dfrac{\partial F_i}{\partial Y}, \hat{F}_i \dfrac{\partial F_i}{\partial Y})$.

A $\mathbb{K}$ vector space

- $\mathbb{A} = \dfrac{\mathbb{K}[Y]}{(F(0,Y))}$, φ is the canonical image of Y in $\mathbb{A}$.
- $\phi(X) \in \mathbb{A}[[X]]$ and satisfy $F(X, \phi(X)) = 0$,
- $\mathfrak{F}(X,Y) = Y - \phi(X) \in \mathbb{A}[[X]][Y]$,
- $\hat{\mathfrak{F}}(X,Y) = \dfrac{F(X,Y)}{Y - \phi(X)} \in \mathbb{A}[[X]][Y]$,

A $\mathbb{K}$ VECTOR SPACE

- $$A_{\sigma} = \Big\{ (\tau, G, H) \in \mathbb{K}^d \times (\mathbb{K}[X,Y]_{d-1})^2 \mid$$
$$G = \sum_{j=1}^{d} \tau_j \mathrm{coef}(\hat{\mathfrak{F}} \frac{\partial \mathfrak{F}}{\partial Y}, \varphi^{i-1}) \mod (X,Y)^{\sigma},$$
$$H = \sum_{j=1}^{d} \tau_j \mathrm{coef}(\hat{\mathfrak{F}} \frac{\partial \mathfrak{F}}{\partial X}, \varphi^{i-1}) \mod (X,Y)^{\sigma} + (X)^{\sigma-1} \Big\}.$$

A KEY INGREDIENT

THEOREM. There is a $\overline{\mathbb{K}}$ isomorphism between $A_\sigma \otimes \overline{\mathbb{K}}$ and $R_\sigma^{\overline{\mathbb{K}}}$.

COROLLARY. If the hypotheses (C) and (H) are satisfied, and $\sigma \geq 2d$ then :

1. $\dim_{\mathbb{K}} A_\sigma = r$, where r is the number of absolute irreducible factors.
2. $A_\sigma \otimes \overline{\mathbb{K}} = Span_{\overline{\mathbb{K}}}(\tau_i, \hat{F}_i \dfrac{\partial F_i}{\partial Y}, \hat{F}_i \dfrac{\partial F_i}{\partial X})$.

The algorithm

Hypotheses : (C) and (H) are satisfied.

Input : $F(X,Y) \in \mathbb{K}[X,Y]$.
Output : Irreducible factors of F in $\overline{\mathbb{K}}[X,Y]$.

Overview :
1. Compute $\phi(X) \mod X^{2d}$.
2. Compute $\pi_{\mathbb{K}^d}(A_\sigma)$ for $\sigma \geq 2d$ (Solve a linear system with d unknowns).
3. Deduce $G = \sum_{i=1}^{d} \lambda_i \hat{F}_i \dfrac{\partial F_i}{\partial Y} \in Span_{\overline{\mathbb{K}}}(G_1, \ldots, G_r)$.
4. Conclude as in Gao's algorithm.

Main Complexity Results

THEOREM.

- Under Hypothesis (C), if F is irreducible in $\mathbb{K}[X,Y]$ then the absolute factorization can be obtained within $\tilde{\mathcal{O}}(d^{(\omega+3)/2})$ arithmetic operations in $\mathbb{K}$ with a probabilistic algorithm, where ω is the linear algebra exponent, $(2 \leq \omega \leq 3)$.
- Under Hypothesis (C), if F is irreducible in $\mathbb{K}[X,Y]$ then the absolute factorization can be obtained within $\tilde{\mathcal{O}}(d^4)$ arithmetic operations in $\mathbb{K}$ with a deterministic algorithm.

Remark : Gao's probabilistic algorithm has a complexity in $\tilde{\mathcal{O}}(d^4)$.

Conclusion

• New algorithms (probabilistic and deterministic) with a better complexity than the previous ones.

• **Work in progress :**

– Absolute irreducibility test using the Newton's polytope of F.

– Practical comparison between this symbolic algorithm and the algorithm [Che 04] when $\mathbb{K} = \mathbb{Q}$.