Lifting and Recombination Techniques for Absolute Factorization

Grégoire Lecerf

CNRS UMI 2615

J.-V. Poncelet Mathematics Laboratory

Independant University of Moscow

Joint work with Guillaume Chèze

Definition

Let $\mathbb{K}$ be a field.
Let $F \in \mathbb{K}[x_1, \ldots, x_n]$.

The absolute factorization of F is its factorization in $\bar{\mathbb{K}}[x_1, \ldots, x_n]$.

Example: $y^2 - 2x^2 = (y + \sqrt{2}x)(y - \sqrt{2}x)$.

To avoid confusion, the factorization over $\mathbb{K}$ is called the rational factorization.

Motivations

- Absolute primary decomposition of ideals and modules [Decker, Pfister, recent implementation in `Singular`].
- Decomposition of the smooth locus of a Zariski closed set into path-connected components $\rightsquigarrow$ applications in kinematics [Sommese, Verschelde, Wampler, 2004].
- Early use in symbolic integration [Trager, 1984].
- Resolution of linear differential equations [Singer, Ulmer, 1997], [Bronstein, 2001].
- Explicit estimates on the number of solutions of systems of equations over finite fields, [Cafure, Matera, 2005]: use of Bertini's irreducibility theorem.

Usual Representation of the Absolute Factorization

The absolutely irreducible factors of $F \in \mathbb{K}[x_1, \ldots, x_n]$ are written $F_1, \ldots, F_r$, and are represented by $\{(q_1, \mathsf{F}_1), \ldots, (q_s, \mathsf{F}_s)\}$, such that:

- $q_i \in \mathbb{K}[z] \setminus \mathbb{K}$, monic, squarefree.
- $\mathsf{F}_i \in \mathbb{K}[x_1, \ldots, x_n, z]$, with $\deg_z(\mathsf{F}_i) \leq \deg(q_i) - 1$.
- $\deg(\mathsf{F}_i(x_1, \ldots, x_n, \alpha))$ is independant of the root α of q_i.
- $\{F_1, \ldots, F_r\} = \cup_{i=1}^{s} \{\mathsf{F}_i(x_1, \ldots, x_n, \alpha) \mid q_i(\alpha) = 0\}$.

Such a representation is called irredundant if $\sum_{i=1}^{s} \deg(q_i) = r$.

☞ No unicity!

☞ There is a cheap way to compute an irredundant representation from any redundant one.

Examples

Example 1. If $F \in \mathbb{K}[x]$ is squarefree then we can take $s := 1$, $q_1(z)$ as the monic part of $F(z)$ and $\mathsf{F}_1(x, z) := x - z$.

Example 2. If $\mathbb{K} := \mathbb{Q}$ and $F := y^2 - 2x^2$ then we can take $s := 1$, $q_1(z) := z^2 - 2$, $\mathsf{F}_1(x, y, z) := y - zx$.

☞ Observe that F and q_1 are irreducible over $\mathbb{Q}$.

Absolute and Rational Factorizations

Assume that the representation is irredundant.

Remark 1. For all i, $P_i := \mathrm{Res}_z(q_i(z), \mathsf{F}_i(x_1, \ldots, x_n, z)) \in \mathbb{K}[x_1, \ldots, x_n]$ is a factor of F, and its absolute factorization can be represented by (q_i, F_i).

Remark 2. P_i is irreducible if and only if q_i is irreducible.

$\rightsquigarrow$ The rational factorization of F can thus be computed from the irreducible factors of $q_1, \ldots, q_s$ by arithmetic operations in $\mathbb{K}$ alone.

History

Exponential Time "Algorithms".

- E. Noether, 1922: the absolute factorization problem is a purely rational problem. The proof based on elimination theory.
  $\rightsquigarrow$ Noether's irreducibility forms.

- Schmidt, 1976: first quantitative analysis of Noether's results.

First Breakthrough.

- Heintz, Sieveking, 1981: absolute irreducibility test in time polynomial in the number of variables.

  ☞ Crucial idea = use Bertini's irreducibility theorem to reduce the problem to 2 variables:

  The intersection of an irreducible hypersurface by a "generic" plane is an irreducible curve.

Absolute Primality of Polynomials is Decidable in Random Polynomial Time in the Number of Variables

Joos Heintz and Malte Sieveking

Abstract. Let F be a n-variate polynomial with $\deg F = d$ over an infinite field k_0. Absolute primality of F can be decided randomly in time polynomial in n and exponential in d^5 and determinalistically in time exponential in $d^6 + n^2 d^3$.

“Polynomial Time” Algorithms.

Underlined = complexity analysis done for bivariate polynomials.

Trager, 1984

Dicrescenzo, Duval, 1984

Kaltofen, 1985

von zur Gathen, 1985

Ruppert, 1986

Dvornicich, Traverso, 1987

Bajaj, Canny, Garrity, Warren, 1989

Duval, 1990

Sasaki *et al.*, 1991-1993

Kaltofen, 1995: cubic time!

Ragot, 1997

Ruppert, 1999

Cormier, Singer, Ulmer, Trager, 2002

Galligo, Rupprecht, 2002

Coreless, Galligo, *et al.*, 2002

Rupprecht, 2004

Bronstein, Trager, 2003

Gao, 2003: almost quadratic time!

Sommese, Verschelde, Wampler, 2004

Chèze, Galligo, 2004

Chèze, Lecerf, 2005: sub-quadratic!

Complexity Issues

► $\mathcal{O}(d^\omega)$ = cost for multiplying two $d \times d$ matrices ($2 \leq \omega \leq 3$).

Until [Gao, 2003] absolute factorization was known to be much more expensive than rational factorization.

Even Gao's algorithm is much slower than the fastest known algorithms for rational factorization: $\tilde{\mathcal{O}}(d^4)$ versus $\tilde{\mathcal{O}}(d^\omega)$ [Bostan, Lecerf, Salvy, Schost, Wiebelt, 2004].

☞ Our new algorithm reduces this gap: we can now compute the absolute factorization in $\tilde{\mathcal{O}}(d^{(\omega+3)/2})$.

☞ The two costs are now asymptocaly equivalent when $\omega = 3$.

☞ Remark that we discard the cost of one univariate factorization in degree d in the rational factorization algorithm.

About Rational Factorization

So far, the fastest known factorization algorithms are based on the lifting and recombination technique introduced in [Zasshaus, 1969]: [Bostan, Lecerf, Salvy, Schost, Wiebelt, 2004], [Lecerf, 2005 (Math. Comp. and MEGA)].

Input: $F \in \mathbb{K}[x_1, \ldots, x_n, y]$ square-free.

Output: the irreducible rational factors of F.

Normalization hypothesis:

$$\deg_y(F) = \deg(F) =: d \quad \text{and} \quad \mathrm{Res}_y\left(\frac{\partial F}{\partial y}, F\right)(0, \ldots, 0) \neq 0.$$

Lifting and recombination technique:

1. Factor $F(0, \ldots, 0, y)$ in $\mathbb{K}[y]$.
2. Lift the factors to a certain precision $(x_1, \ldots, x_n)^\sigma$.
3. Find out how the lifted factors recombine into the rational factors.

$\rightsquigarrow$ Can we benefit of this technique for absolute factorization?

[Gao, 2003]

"In practice rational factorization of most polynomials can be computed efficiently using Hensel lifting.[...] Absolute factorization is fundamental in computation in commutative algebra, algebraic geometry and number theory. Here Hensel lifting technique seems no longer applicable."

- ☞ It is true that the construction of the splitting field of $F(0, \ldots, 0, y)$ is in general too expensive!
- ☞ The only known exception concerns $\mathbb{K} = \mathbb{Q}$. Numerical computations can be performed in $\mathbb{C}$: Sasaki, Galligo, Chèze,...

Our “Absolute Lifting and Recombination” Technique

1. Compute the absolute factorization of $F(0, \dots, 0, y)$.
2. Lift the absolute factorization to a certain precision $(x_1, \dots, x_n)^\sigma$.
3. Find out how the lifted factors recombine.

☞ Step 1 costs nothing.

☞ We need to detail steps 2 and 3.

Assumptions:

- $F \in \mathbb{K}[x, y]$.
- F is monic in y and $\deg_y(F) = \deg(F) = d$.
- $\mathrm{Res}\left(F(0, y), \frac{\partial F}{\partial y}(0, y)\right) \neq 0$.

☞ Not restrictive!

Lifting Step

Let $f(y) := F(0, y)$ and $\mathbb{A} := \mathbb{K}[y]/(f(y))$.
$(f(z), y - z)$ represents the absolute factorization of $f(y)$.

Let φ denote the residue class of y in $\mathbb{A}$. Then there exists a unique series $\phi \in \mathbb{A}[[x]]$ such that:

- $\phi - \varphi \in (x)$,
- $F(x, \phi) = 0$.

ϕ can be approximated to any precision (x^σ) by means of Newton's operator.

$\rightsquigarrow$ $(f(z), y - \phi(z, x))$ represents the factorization of $F(x, y)$ seen in $\bar{\mathbb{K}}[[x]][y]$.

☞ For efficiency, we use Paterson and Stockmeyer's evaluation scheme [1973].

Recombination Step

It divides into:

- Linear System Solving,
- Absolute Partial Fraction Decomposition.

Linear System Solving

From ϕ computed to the precision (x^σ), we construct the following linear system where $\hat{\mathfrak{F}} := F/\mathfrak{F} \in \mathbb{A}[[x]][y]$ and $\mathfrak{F} := y - \phi$:

$$
\begin{aligned}
L_\sigma := \Big\{ &((\ell_1, \ldots, \ell_d), G, H) \in \mathbb{K}^d \times \mathbb{K}[x,y]_{d-1} \times \mathbb{K}[x,y]_{d-1} \mid \\
&G - \sum_{i=1}^{d} \ell_i \,\mathrm{coeff}\left(\hat{\mathfrak{F}} \frac{\partial \mathfrak{F}}{\partial y}, \varphi^{i-1}\right) \in (x,y)^\sigma, \\
&H - \sum_{i=1}^{d} \ell_i \,\mathrm{coeff}\left(\hat{\mathfrak{F}} \frac{\partial \mathfrak{F}}{\partial x}, \varphi^{i-1}\right) \in (x,y)^\sigma + (x^{\sigma-1}) \Big\}.
\end{aligned}
$$

Let $\sigma = 2d$ if $\mathrm{char}(\mathbb{K}) = 0$ or $> d(d-1)$, otherwise let $\sigma = d(d-1)+1$.

Theorem.

$$\bar{\mathbb{K}} \otimes L_\sigma = \left\langle \left(\mu_i, \frac{F}{F_i}\frac{\partial F_i}{\partial y}, \frac{F}{F_i}\frac{\partial F_i}{\partial x} \right) \mid i \in \{1, \ldots, r\} \right\rangle,$$

where $\mu_i := (\mathrm{Tr}_0(F_i(0, y)), \ldots, \mathrm{Tr}_{d-1}(F_i(0, y)))$.

☞ The proof is based on the first algebraic de Rham cohomology group of the complementary of $F = 0$ (as for Gao's algorithm).

☞ For efficiency reasons we compute a basis of $\pi(L_\sigma)$, defined as the projection of L_σ to $\mathbb{K}^d$.

Absolute Partial Fraction Decomposition

For any $((\ell_1,\ldots,\ell_d),G,H)\in L_\sigma$, the previous theorem implies that:

$$\frac{G}{F}=\sum_{i=1}^{r}\rho_i\frac{\frac{\partial F_i}{\partial y}}{F_i},\qquad \text{with } \rho_i\in\bar{\mathbb{K}}.$$

For almost all G, the ρ_i are pairwise distinct, and thus $F_1,\ldots,F_r$ can be directly obtained from the partial fraction decomposition of G/F:

1. Let $Q(z)=\mathrm{Res}_y\left(F(0,y),z\frac{\partial F}{\partial y}(0,y)-G(0,y)\right)$.
2. The set of roots of Q is $\{\rho_1,\ldots,\rho_r\}$, and $F_i=\gcd\left(F,\rho_i\frac{\partial F}{\partial y}-G\right)$.

☞ The partial fraction decomposition of G/F can be computed with the classical Rothstein-Trager of Lazard-Rioboo-Trager algorithms.

Example

$\mathbb{K} := \mathbb{Q}$, $F := y^4 + (2x+14)y^2 - 7x^2 + 6x + 47$.

$f := y^4 + 14y^2 + 47$, with $\sigma := 2\deg(F) = 8$, we obtain:

$$\begin{aligned}\phi = \varphi &- \left(\frac{13}{94}\varphi^3 + \frac{44}{47}\varphi\right)x + \left(\frac{39}{8836}\varphi^3 + \frac{199}{17672}\varphi\right)x^2 \\ &- \left(\frac{4745}{1661168}\varphi^3 + \frac{15073}{830584}\varphi\right)x^3 \\ &+ \cdots - \left(\frac{26241896109}{1037564150708224}\varphi^3 + \frac{76656876747}{518782075354112}\varphi\right)x^7 + \mathcal{O}(x^8).\end{aligned}$$

A possible basis of $\pi(L_\infty)$ is $(1,0,0,0)$, $(0,0,1,0)$. We take $G := (2x+1)y$, and the partial fraction decomposition gives us the absolute factorization $(z^2 - 1/32, y^2 + (1-16z)x - 8z + 7)$.

Main Complexity Results

Assume $\mathbf{char}(\mathbb{K}) = 0$ of $\mathbf{char}(\mathbb{K}) > d(d-1)$.

$\mathsf{M}(d)$ = cost for multiplying two polynomials in degree d.
$\mathcal{O}(d^\omega)$ = cost for multiplying two $d \times d$ matrices.

Theorem. Cost of the absolute factorization:

- $\mathcal{O}(d^3 \mathsf{M}(d) \log(d))$ or $\tilde{\mathcal{O}}(d^4)$ arithmetic operations in $\mathbb{K}$ deterministically.
- $\mathcal{O}(d^{(\omega+3)/2} + d^{3/2}\mathsf{M}(d)(\mathsf{M}(d)^2/d^2 + \log(d)))$ or $\tilde{\mathcal{O}}(d^{(\omega+3)/2})$ arithmetic operations in $\mathbb{K}$, with a Las Vegas probabilistic algorithm.

☞ These algorithms do not use rational factorization, hence do not depend on the base field.

☞ Discarding one univariate factorization in degree d, the rational factorization costs [Bostan *et al.*, 2004], [Lecerf, 2005]:

- $\mathcal{O}(d^{\omega+1})$, deterministically,
- $\mathcal{O}(d^\omega)$, probabilistically $\rightsquigarrow$ the overhead is much less than d.

Timings

$\mathbb{K} := \mathbb{Z}/754974721\mathbb{Z}$, F irreducible with r absolutely irreducible factors.

MAGMA V2.11-14 on a 1.8 GHz Pentium M processor.

d	$r=1$	$r=2$	$r=2^{\lfloor \log_2(d)/2 \rfloor}$	$r=d/2$	$r=d$
8	0.08 s	0.03 s	0.03 s	0.03 s	0.02 s
16	0.41 s	0.20 s	0.18 s	0.17 s	0.12 s
32	2.36 s	1.55 s	2.96 s	1.42 s	0.78 s
64	18.8 s	21.0 s	21.8 s	20.5 s	15.8 s
128	147 s	175 s	170 s	179 s	119 s
256	1239 s	1423 s	1419 s	1520 s	973 s

$\leadsto$ Reflects well the cost in $\tilde{\mathcal{O}}(d^3)$.

☞ These computations were previously out of reach.

Sharp Bertini's Theorem in the Normalized Case

- $\mathrm{char}(\mathbb{K}) = 0$ or $\mathrm{char}(\mathbb{K}) \geq d(d-1)+1$.
- $F \in \mathbb{K}[x_1, \ldots, x_n, y]$ is irreducible.
- S is a finite subset of $\mathbb{K}$.

Normalization hypothesis:

$$\deg_y(F) = \deg(F) =: d \quad \text{and} \quad \mathrm{Res}_y\left(\frac{\partial F}{\partial y}, F\right)(0, \ldots, 0) \neq 0.$$

Upper bound: $|\{(a_1, \ldots, a_n) \in S^n \mid F(a_1 x, \ldots, a_n x, y) \text{ is reducible}\}|$

$$\leq \tfrac{1}{8}(3d-1)(5d-3)|S|^{n-1}.$$

Lower bound: $\mathbb{K} := \mathbb{C}$, $F := y^d + x_1^{d-1} y - x_2^{d-1} - 1$. Let S be the set of roots of $z^{d(d-1)} - 1$.
$|\{(a_1, \ldots, a_n) \in S^n \mid F(a_1 x, \ldots, a_n x, y) \text{ is reducible}\}| = S^n$.

$\rightsquigarrow$ $|S| \gg d^2$ is necessary and sufficient to reach small probabilities of failure.

Quantitative Version of Bertini's Irreducibility Theorem

▶ $P \in \mathbb{K}[v_1, \ldots, v_n]$ is irreducible of total degree d.

Problem: for a finite subset S of $\mathbb{K}$, upper bound the density of points $(a, b, c) \in (S^n)^3$ for which $P(a_1 x + b_1 y + c_1, \ldots, a_n x + b_n y + c_n)$ is reducible.

- Hilbert (1892) (before Bertini): the density tends to 0 for large S.
- Heintz & Sieveking (1981), Kaltofen (1982): use in computer algebra.
- von zur Gathen (1985): $9^{d^2}/|S|$.
- Bajaj, Canny, Garrity & Warren (1993): $d^4/|S|$, when $\mathbb{K} = \mathbb{C}$.
- Kaltofen (1995): $2d^4/|S|$, when $\mathbb{K}$ is perfect.
- Gao (2003): $2d^3/|S|$, when $\mathrm{char}(\mathbb{K}) = 0$ or $\geq 2d^2$.
- Chèze (2004): $d^3/|S|$, when $\mathrm{char}(\mathbb{K}) = 0$ or $\geq d(d-1)+1$.
- Lecerf (2005): $\frac{23}{8}d^2/|S|$, when $\mathrm{char}(\mathbb{K}) = 0$ or $\geq d(d-1)+1$.

Further Work

- Unified approach to factorizations: rational, absolute, over an algebraic extension and over the splitting field of a given univariate polynomial (in preparation).
- Improve the “small characteristic” case.
- Improve the “sparse” case, via analytic factorization.