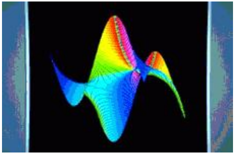
On the Complexity of Gröbner Basis Computation for Regular and Semi-Regular Systems

Bruno Salvy
Bruno.Salvy@inria.fr

Algorithms Project, Inria



Joint work with Magali Bardet & Jean-Charles Faugère

September 21st, 2006

I Introduction

Don't Expect the Worst

Complexity for m equations, degree d, n variables:

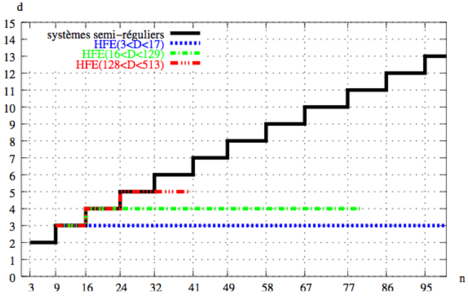
- worst case: $2^{2^{O(n)}}$ [Mayr-Meyer82, Möller-Mora84]
- generically: $m^{O(1)}d^{O(n)}$ [Lazard83, Giusti84]

Questions:

1. how small can be the exponent in $d^{O(n)}$?
2. what about overdetermined systems? does the extra information help?

Motivation from Cryptography

Wanted: Solutions in $\mathbb{F}_2$ of a system in $\mathbb{F}_2[x_1, \dots, x_n]$.
Possible approach: add the equations $x_i^2 - x_i = 0 \rightarrow$ overdetermined system.
Faugère-Joux 2003: break the HFE challenge thanks to a small regularity:



$\rightarrow$ How do these stairs grow?

Setting for the Talk

- homogeneous system $f_1 = \cdots = f_m = 0$
- in $k[x_1, \ldots, x_n]$, with char $k = 0$;
- $\deg f_1 = \cdots = \deg f_m = d$;
- system regular if $m \leq n$; semi-regular if $n \leq m$;
- coordinates in simultaneous Noether position wrt the system;
- all bases are computed for the degree reverse lexicographical order (grevlex).

See the forthcoming article for extensions to

1. formulæ with $d_i = \deg f_i$ and $d_1 \leq \cdots \leq d_m$;
2. non-homogeneous systems;
3. $k = \mathbb{F}_2$.

Starting Point: the Macaulay Matrix $\mathcal{M}_D$

all multiples of the f_i of degree D

$$\begin{matrix} m_1 f_1 \\ \vdots \\ m_k f_1 \\ m_2 f_2 \\ \vdots \\ m_k f_m \end{matrix} \begin{pmatrix} \\ \\ \\ \\ \\ \\ \end{pmatrix}$$

Columns indexed by monomials of degree D (sorted by $\prec$)

For D large enough

Buchberger's algorithm	$\leftrightarrow$	(Structured) Gaussian elimination
Reductions to 0	$\leftrightarrow$	"Useless" lines
Algorithm F_5 [Faugère 02]	$\leftrightarrow$	Construct matrices by increasing degrees avoiding useless lines coming from $f_i f_j = f_j f_i$.

Linear Algebra and its Complexity

Proposition (General Upper Bound)

The number of operations in k required to compute the GB up to degree D is bounded by

$$O\left(mD\binom{n+D-1}{D}^{\omega}\right),$$

$2 \leq \omega \leq 3$ *is the complexity of matrix product.*

Strassen: $\omega < 2.81$; Coppersmith-Winograd: $\omega < 2.376$.

Needed: bounds on D.

Regular system: $D \leq n(d-1)+1$ [Macaulay]

$$\Rightarrow \text{bound} \approx \left(\frac{d^d}{(d-1)^{d-1}}\right)^{\omega n}$$

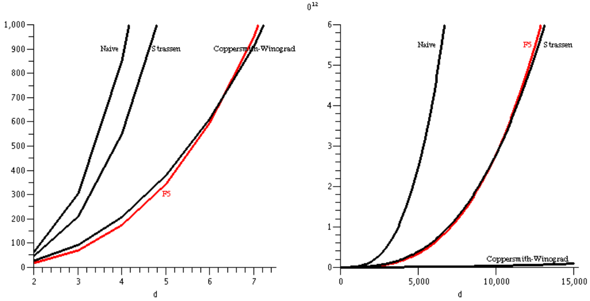
F_5 for Regular Systems in Simultaneous Noether Position

Theorem (BaFaSa06, $m = n$)

F_5 computes the GB in at most

$$A(d)^n n(C + O(1/n)) \text{ operations in } k, \qquad n \to \infty,$$

with $A(d)$ root of a simple polynomial of degree $2d - 1$.



Quantifies how F_5 exploits the structure of the Macaulay matrix.

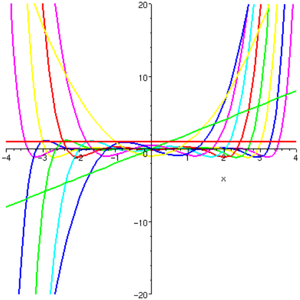
Semi-Regular Systems in Simultaneous Noether Position I.

Theorem (BaFaSa06, $m = n + k$ $(k \geq 1)$)

$$D \leq i_{reg} = \frac{d-1}{2}m - \alpha_k \sqrt{\frac{d^2-1}{6}}\sqrt{m} + \cdots, \qquad n \to \infty,$$

α_k largest root of kth Hermite polynomial.

Quantifies the gain brought by the extra equations.



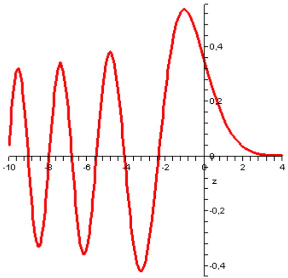
Semi-Regular Systems in Simultaneous Noether Position II.

Theorem (BaFaSa06, $m = [\alpha n]$ $(\alpha > 1)$)

$$D \leq i_{reg} = \phi_d(\alpha)m + a_1\psi_d(\alpha)m^{1/3} + \cdots, \qquad n \to \infty$$

a_1 largest root of the Airy function, ϕ_d & ψ_d algebraic,

$$\phi_d(\alpha) = \frac{d-1}{2} - \sqrt{\frac{d^2-1}{3}}(\alpha-1)^{1/2} + \cdots, \quad \alpha \to 1.$$



II Regular Systems

Hilbert: Function, Polynomial, Series

$$\mathcal{I}^{(m)} := \langle f_1, \dots, f_m \rangle$$

- Hilbert Function:

$$\mathrm{HF}_{\mathcal{I}^{(m)}}(d) := (\dim k[x_1, \dots, x_n]/\mathcal{I}^{(m)})_d.$$

- Using the Macaulay matrix $\mathcal{M}_d$:

$$\mathrm{HF}_{\mathcal{I}^{(m)}}(d) = \#\mathrm{cols}(\mathcal{M}_d) - \mathrm{rank}(\mathcal{M}_d).$$

- For d large enough, this is a polynomial.
- The first such d is called the index of regularity ($i_{\mathrm{reg}}(\mathcal{I}^{(m)})$).
- Hilbert series:

$$H_{\mathcal{I}^{(m)}}(z) := \sum_{d\geq 0} \mathrm{HF}_{\mathcal{I}^{(m)}}(d) z^d = \frac{P(z)}{(1-z)^\delta}.$$

Regular Systems

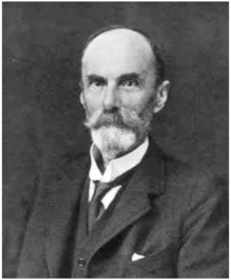
Definition ($(f_1, \dots, f_m)$ regular)

For all $i = 1, \dots, m$, f_i is not a zero-divisor in $k[x_1, \dots, x_n]/\mathcal{I}^{(i-1)}$.

$$\Leftrightarrow (k[x_1, \dots, x_n]/\mathcal{I}^{(i-1)})_d \xrightarrow{f_i \cdot} (k[x_1, \dots, x_n]/\mathcal{I}^{(i-1)})_{d+d_i} \text{ injective } \forall d \geq 0$$

$$\Leftrightarrow \boxed{\mathrm{HF}_{\mathcal{I}^{(i)}}(d + d_i) = \mathrm{HF}_{\mathcal{I}^{(i-1)}}(d + d_i) - \mathrm{HF}_{\mathcal{I}^{(i-1)}}(d) \text{ for all } d}$$

$$\Leftrightarrow H_{\mathcal{I}^{(m)}}(z) = \frac{\prod_{j=1}^{m}(1 - z^{d_j})}{(1 - z)^n}.$$



Index of regularity: $\displaystyle\sum_{i=1}^{m}(d_i - 1) + 1.$

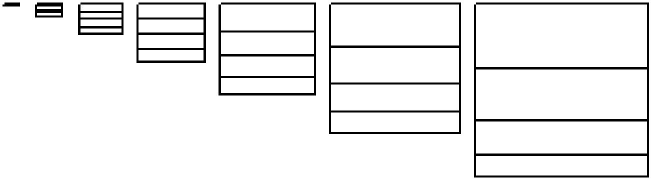
F_5 for Regular Systems

Proposition (Faugère02)

For regular systems, F_5 constructs matrices $\tilde{\mathcal{M}}_d^{(i)}$ such that

$$\#cols(\tilde{\mathcal{M}}_d^{(i)}) - \#rows(\tilde{\mathcal{M}}_d^{(i)}) = \mathrm{HF}_{\mathcal{I}^{(i)}}(d).$$

No reduction to 0 at all!



Example: $n = m = 4, d = 3$

Noether Position

Definition ($(x_1, \dots, x_m)$ in Noether position wrt $(f_1, \dots, f_m)$)

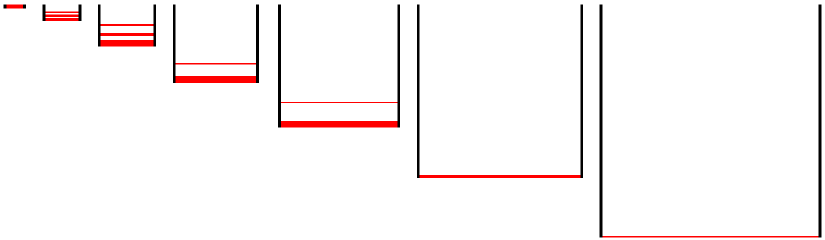
1. Their canonical images in $k[x_1, \dots, x_n]/\langle f_1, \dots, f_m \rangle$ are algebraic integers over $k[x_{m+1}, \dots, x_n]$;
2. $k[x_{m+1}, \dots, x_n] \cap \langle f_1, \dots, f_m \rangle = \langle 0 \rangle$.

Definition (Simultaneous Noether position)

For $i = 1, \dots, m$, $(x_1, \dots, x_i)$ in Noether position wrt $(f_1, \dots, f_i)$.

$\Rightarrow$ the leading terms of the elements of the grevlex GB do not depend on $x_{m+1}, \dots, x_n$.

Shape of a Gröbner Basis I

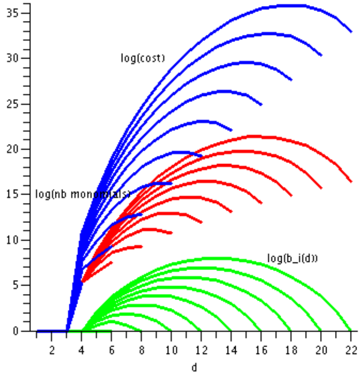


Theorem (new?)

$(x_1, \dots, x_n)$ in simultaneous Noether position. G_i reduced Gröbner basis of $(f_1, \dots, f_i)$, $1 \le i \le m$. The number of polynomials of degree d in $G_i \setminus G_{i-1}$ is bounded by $b_d^{(i)}$, where

$$B_i(z) = \sum_{d=0}^{\infty} b_d^{(i)} z^d = z^{d_i} \prod_{k=1}^{i-1} \frac{1 - z^{d_k}}{1 - z}.$$

Shape of a Gröbner Basis II



Number of operations for F_5 bounded by

$$\sum_{i=1}^{m} \sum_{d=d_i}^{i_{\mathrm{reg}}} b_d^{(i)} \binom{n+d-1}{d} \binom{i+d-1}{d}$$

III Semi-Regular Systems

Definition

Regular systems cannot be overdetermined.

Definition ($(f_1, \dots, f_m)$ semi-regular ($m \geq n$))

$$\mathrm{HF}_{\mathcal{I}^{(i)}}(d) = \mathrm{HF}_{\mathcal{I}^{(i-1)}}(d) - \mathrm{HF}_{\mathcal{I}^{(i-1)}}(d - d_i), \quad d_i \leq d < i_{\mathrm{reg}}(\mathcal{I}^{(m)})$$

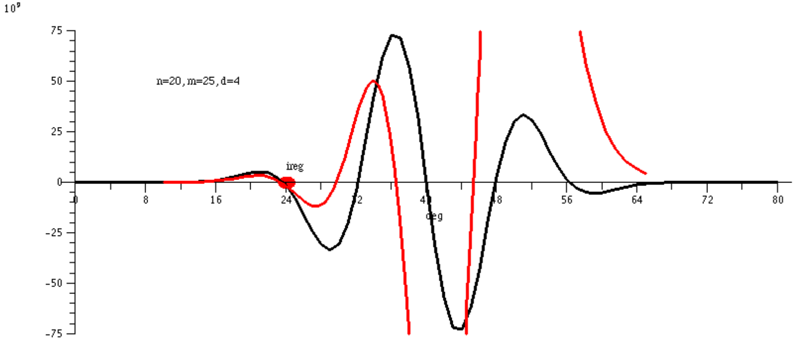
Proposition (Hilbert Series)

$$H_{\mathcal{I}^{(m)}}(z) = \left[\frac{\prod_{j=1}^{m}(1 - z^{d_j})}{(1-z)^n}\right].$$

Notation:

$$\left[\sum_{i\geq 0} a_i z^i\right] = \sum_{i\geq 0} b_i z^i, \quad \text{with} \quad b_i = \begin{cases} a_i & \text{if } a_j > 0 \text{ for } 0 \leq j \leq i \\ 0 & \text{otherwise.} \end{cases}$$

Asymptotics of the Index of Regularity

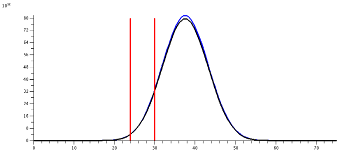


Approach:

1. Compute an asymptotic approximation of the coefficient sequence in the neighborhood of the 0;
2. find its smallest zero.

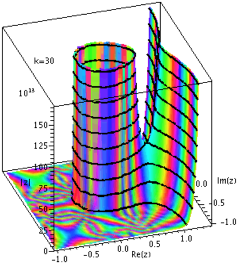
Few More Equations than Unknowns

$$\frac{\prod_{j=1}^{m}(1-z^{d_j})}{(1-z)^n} = (1-z)^{m-n}\underbrace{\prod_{j=1}^{m}\frac{1-z^{d_j}}{1-z}}_{F(z)}.$$



Coefficients of $F(z)$ approximated well by the saddle-point method.

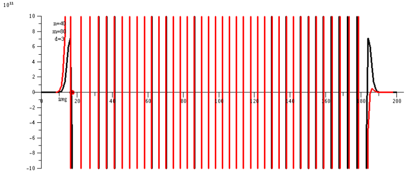
Cauchy: $[z^k]F(z) = \frac{1}{2i\pi}\oint F(z)\frac{dz}{z^{k+1}}\ \frac{(1-z)^{m-n}}{z^{k+1}}$



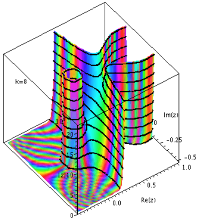
1. Saddle-point: $F'(\rho)=0$;
2. Locally:
   $F(z) \approx F(\rho)e^{-\lambda u^2}(1-\rho-iu)^{m-n}$;
3. coeff $\approx \frac{F(\rho)}{2\pi}\underbrace{\int_{-\infty}^{\infty} e^{-\lambda u^2}(1-\rho-iu)^{m-n}\,du}_{\frac{\sqrt{\pi}}{2^k\sqrt{\lambda}^{k+1}}H_{m-n}((1-\rho)\sqrt{\lambda})}$.

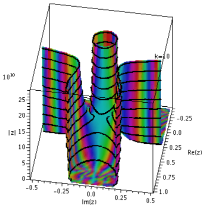
Even More Equations

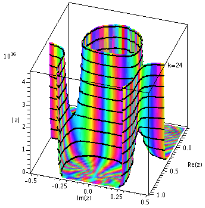
$$\frac{1}{2i\pi}\oint \frac{(1-z^d)^{\alpha n}}{(1-z)^n z^{k+1}}\,dz$$



Small k Transition Larger k





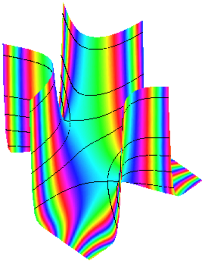


The coalescence of saddle-points is captured by the Airy function.

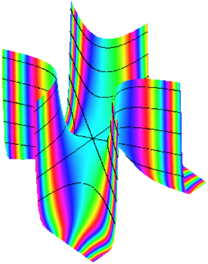
Coalescent Saddle-Points [Chester-Friedman-Ursell 57]

Capture both saddle-points by a cubic change of variables.
Leads to uniform asymptotic expansions involving

$$\mathrm{Ai}(z) = \frac{1}{2i\pi} \int_{\infty e^{-i\pi/3}}^{\infty e^{i\pi/3}} e^{t^3/3 - zt}\, dt.$$



Airy $z \neq 0$,
two neighboring saddle-points



Airy $z = 0$
A double saddle-point