Polynomial System Solving in the Real Case

(Solving Zero-dimensional Systems <u>in practice</u>)

F. Rouillier

`Fabrice.Rouillier@inria.fr`

SPACES Project - INRIA / University of Paris VI

RUR : a naive algorithm

- (1) compute $d = rank(q_1)$
- (2) find $t \in \mathcal{T} = \{Y_1 + iY_2, \ldots + i^{n-1}Y_n \ , \ i = 1 \ldots nd(d-1)/2\}$ such that $degree(\overline{PolChar(m_t)}) = d$
- (3) compute the $Trace(m_{X_j t^i})$ for $i = 1 \ldots d$ and $j = 1 \ldots n$
- construct the RUR

In practice, one guess a separating t modulo p (steps (1) and (2)), and check after the full computation that the computed set is a RUR :

- $\{g_t, g_{t,1}, g_{t,Y_1}, \ldots, g_{t,Y_n}\}$ is a RUR iff $g_t(t) \in I_K$ and $h_j = g_{t,1}(t)Y_j - g_{t,Y_j} \in \sqrt{I_K}$.
- $h_j \in \sqrt{I_K}$ iff $rank(q_{h_j}) = 0$ iff $Trace(m_{h_j w_i}) = 0 \ , \ \forall i = 1 \ldots D$.

Another trick is that $Trace(m_{t^i})$ is exactly the i-th Newton sum of g_t (Stickelberger) : all the polynomials of the RUR can be easily computed once knowing the $Trace(m_{Y_j t^i})$

Dimension 0 : back to the shape lemma

When I is radical and Y_1 is separating V_C, one can compute the RUR associated with Y_1, and we have an "equivalent" system :

$$g_{Y_1}(Y_1)$$
$$g_{Y_1,1}(Y_1)Y_2 - g_{Y_1,Y_2}(Y_1)$$
$$\vdots$$
$$g_{Y_1,1}(Y_1)Y_n - g_{Y_n,Y_2}(Y_1)$$

One can deduce a lexicographic Gröbner basis from a RUR

Dimension 0 : back to the shape lemma

When I is radical and Y_1 is separating V_C, one can compute the RUR associated with Y_1, and we have an "equivalent" system :

$$
\begin{array}{l}
g_{Y_1}(Y_1) \\
Y_2 - g_{Y_1,1}(Y_1)^{-1} g_{Y_1,Y_2}(Y_1) \; mod \; g_{Y_1}(Y_1) \\
\vdots \\
Y_n - g_{Y_1,1}(Y_1)^{-1} g_{Y_n,Y_2}(Y_1) \; mod \; g_{Y_1}(Y_1)
\end{array}
$$

This computation induces, in general, a growth of coefficients such that the coefficients of the RUR are smaller than those of the lexicographic Gröbner basis

Consider the inequalities

Let $F_j \in K[Y_1, \ldots, Y_n]$.

What are the roots of V_C where $F_j > 0$?

$g_{t,F_j}(T) = \sum_{i=0}^{d-1} Trace(m_{F_j t^i}) H_{d-i-1}(g_t)(T)$, then $F_j(\alpha) = \frac{g_{t,F_j}(t(\alpha))}{g_{t,1}(t(\alpha))}$.

In particular the sign (also the value) of F_j at a zero of V_C can be computed by studying the value of $\frac{g_{t,F_j}}{g_{t,1}}$ at a zero of g_t.

If $F_j = \sum_{k=0}^{D} a_k \omega_k$ then $Trace(m_{F_j t^i}) = \sum_{k=0}^{D} a_k Trace(m_{t^i \omega_k})$ and the computation of g_{t,F_j} can be cone using $O(D^2)$ arithmetic operations.

The full simplification (reduction to univariate problems) of our system can be done using $O(D^3 + (n+l)D^2$ arithmetic operations.

Triangular sets

A triangular set is a set of polynomials with the following shape :

$$\begin{cases} t_1(X_1) \\ t_2(X_1, X_2) \\ \vdots \\ t_n(X_1, \ldots, X_n) \end{cases}$$

(the t_i may be identically zero).

Triangular sets : basic definitions

For $p \in K[X_1, \ldots, X_n] \setminus K$, we denote by $\mathrm{mvar}(p)$ (and we call *main variable* of p) the greatest variable appearing in p w.r.t. a fixed lexicographic ordering.

Notations :

- h_i the leading coefficient of t_i (when $t_i \neq 0$ is seen as a univariate polynomial in its main variable), and $h = \Pi_{i=1, t_i \neq 0}^{n} h_i$.
- $\mathrm{sat}(T) =< T >: h^\infty = \{p \in K[X_1, \ldots, X_n] \mid \exists m \in \mathbb{N},\ h^m p \in \langle T \rangle\}$;
- $\overline{\mathcal{V}(T) \setminus \mathcal{V}(h)} = \mathcal{V}(sat(T))$ (elementary property of localization).

A triangular set $T = (t_1, \ldots, t_n) \subset K[X_1, \ldots, X_n]$ is said to be *regular* if $\forall i \in \{1, \ldots, n\}$, such that $t_i \neq 0$, the initial h_i does not belong to any associated prime ideal of $\mathrm{sat}(t_1, \ldots, t_{i-1}) \bigcap K[X_1, \ldots, X_{i-1}]$.

Triangular sets : representation of a variety

One may naturally "compute"

$$\overline{V(< T >) \setminus V(h)} = V(sat(< T >))$$

but the full study of $V(< T >)$ requires additional computations.

If T is regular, then $sat(T)$ is equidimensional (elementary property of localization).

It is always possible to represent an algebraic variety as the union of varieties defined as zeroes of regular triangular sets

$$V_C = \bigcup_i V(\mathrm{sat}(T_i))$$

but this do not give a straightforward representation (need to compute $\mathrm{sat}(T_i)$).

Triangular sets in the zero-dimensional case : lextriangular

Start from a Lexicographic Gröbner basis :

$$
\begin{array}{l}
f_1(Y_1) \\
f_2(Y_1, Y_2) \\
\vdots \\
f_{k_2}(Y_1, Y_2) \\
f_{k_2+1}(Y_1, Y_2, Y_3) \\
\vdots \\
f_{k_{n-1}}(Y_1, \ldots, Y_n) \\
f_{k_{n-1}+1}(Y_1, \ldots, Y_n) \\
\vdots \\
f_{k_n}(Y_1, \ldots, Y_n)
\end{array}
$$

Triangular sets in the zero-dimensional case : lextriangular

Start from a Lexicographic Gröbner basis :

$f_1(Y_1)$
$f_2(Y_1, Y_2)$
$\vdots$
$f_{k_2}(Y_1, Y_2)$
$f_{k_2+1}(Y_1, Y_2, Y_3)$
$\vdots$
$f_{k_{n-1}}(Y_1, \ldots, Y_n)$
$f_{k_{n-1}+1}(Y_1, \ldots, Y_n)$
$\vdots$
$f_{k_n}(Y_1, \ldots, Y_n)$

The triangular set extracted from the Lex. G. basis is not necessarily regular.

- if $< LC(f_2, Y_2), f_1 > \neq < 1 >$, split into two systems : $< G, LC(f_2, Y_2) >$, and $G : LC(f_2, Y_2)$ and follow with the same strategy.
- other else, do the same with f_{k_2+1} and Y_3.

and so on ...

Triangular sets in the zero-dimensional case : lextriangular

Start from a Lexicographic Gröbner basis :

$f_1(Y_1)$
$f_2(Y_1, Y_2)$
$\vdots$
$f_{k_2}(Y_1, Y_2)$
$f_{k_2+1}(Y_1, Y_2, Y_3)$
$\vdots$
$f_{k_{n-1}}(Y_1, \ldots, Y_n)$
$f_{k_{n-1}+1}(Y_1, \ldots, Y_n)$
$\vdots$
$f_{k_n}(Y_1, \ldots, Y_n)$

The triangular set extracted from the Lex. G. basis is not necessarily regular.

- if $< LC(f_2, Y_2), f_1 > \neq < 1 >$, split into two systems : $< G, LC(f_2, Y_2) >$, and $G : LC(f_2, Y_2)$ and follow with the same strategy.
- other else, do the same with f_{k_2+1} and Y_3.

and so on ...

Due to the choice of the polynomials, the computed T_i are lexicographic Gröbner basis. In particular, $< G_i >= sat(T_i)$.

Triangular sets in the zero-dimensional case : lextriangular

Start from a Lexicographic Gröbner basis :

$f_1(Y_1)$
$f_2(Y_1, Y_2)$
$\vdots$
$f_{k_2}(Y_1, Y_2)$
$f_{k_2+1}(Y_1, Y_2, Y_3)$
$\vdots$
$f_{k_{n-1}}(Y_1, \ldots, Y_n)$
$f_{k_{n-1}+1}(Y_1, \ldots, Y_n)$
$\vdots$
$f_{k_n}(Y_1, \ldots, Y_n)$

The triangular set extracted from the Lex. G. basis is not necessarily regular.

- if $< LC(f_2, Y_2), f_1 > \neq < 1 >$, split into two systems : $< G, LC(f_2, Y_2) >$, and $G : LC(f_2, Y_2)$ and follow with the same strategy.
- other else, do the same with f_{k_2+1} and Y_3.

and so on ...

Due to the choice of the polynomials, the computed T_i are lexicographic Gröbner basis. In particular, $< G_i >= sat(T_i)$.
Due to the equidimentionality of $sat(T)$, when T is regular, this method can easily be generalized to the positive dimensional case (Safey El Din's thesis).

Computational Strategies

Let's try on some examples ...

Used Software :

- Maple 8 user interface
- Gb (J.C. Faugère) [external] - Gröbner basis computations
- RS (F. Rouillier) [external] - RUR - Real Roots of zero-dimensional systems and univariate polynomials

Available at `http;//spaces.lip6.fr`

MuPAD versions in progress.

Algorithms performances

Empirical measures of performances :

- A means at least "average" compared with Gb implementation of algorithm F4 (Faugère) for computing DRL Gröbner bases;
- B means "slower" but may be reasonable;
- C means "very slow";

- Buchberger Algorithm for DRL G. Basis (Gb) :C;
- F4 Algorithm for Lex G. Basis (Gb) :C;
- FGLM on a DRL G. Basis (Gb) :B for low degree and small coefficients, otherelse C in shape lemma case, maybe B for some non shape lemma cases.
- RUR on any G. Basis (RS) : A in shape lemma case for reasonable degrees, B in non shape lemma case for reasonable degrees, C for high degrees;
- Lextriangular (Gb) : A
- Real Root isolation (RS) :A.