Polynomial System Solving in the Real Case

(Zero-dimensional Systems)

F. Rouillier

Fabrice.Rouillier@inria.fr

SPACES Project - INRIA / University of Paris VI

Notations and results from the last course

Notations

$K \subset K'$ are ordered fields, R the real closure of K' and C the algebraic closure of R. In practice, we consider $K = \mathbb{Q}$, $R = \mathbb{R}$ and $C = \mathbb{C}$.

A semi-algebraic system will be denoted by

$$\mathcal{S} = \{E_1 = 0, \ldots E_s = 0, F_1 > 0, \ldots F_l > 0\},$$

where $E_i, F_i \in K[Y_1, \ldots, Y_n]$

The main ideal of $K[Y_1, \ldots Y_n]$ associated to $\mathcal{S}$:

$$I_K =< E_1, \ldots E_s >$$

The main variety of $\mathcal{S}$: $V_C = \mathcal{V}(I_C) \subset C^n$. We define also $V_R = V_C \bigcap R^n$.

Gröbner bases : a minimal set of definitions

A Gröbner basis G of I w.r.t. any admissible monomial ordering $<$, is a set of generators of I such that $\exists$ a K-linear function (Normal Form) $NF_<(.,G) : K[Y_1,\ldots Y_n] \longrightarrow K[Y_1,\ldots Y_n]$ s.t.

$$NF_<(p,G) = 0 \Leftrightarrow p \in I$$

An admissible monomial ordering is a total well-ordering (compatible with the multiplication) on the monomials of $K[Y_1,\ldots,Y_n]$.

$LM_<(p)$ (leading monomial) , $LC_<(p)$ (leading coefficient), $LT_<(p) = LC_<(p)LM_<(p)$ (leading term).

The $NF_<$ function "generalizes" the Euclidian division for univariate polynomials.

Gröbner bases : definition of monomial orderings

The main used monomial orderings are :
Lexicographic orderings

$$Y_1^{\alpha_1} \cdot \ldots \cdot Y_n^{\alpha_n} <_{Lex} Y_1^{\beta_1} \cdot \ldots \cdot Y_n^{\beta_n} \Leftrightarrow \exists i_0 \leq n \ , \begin{cases} \alpha_i = \beta_i \ , \ \forall i = 1 \ldots i_0 - 1, \\ \alpha_{i_0} < \beta_{i_0} \end{cases}$$

Degree Reverse Lexicographic orderings

$$Y_1^{\alpha_1} \cdot \ldots \cdot Y_n^{\alpha_n} <_{DRL} Y_1^{\beta_1} \cdot \ldots \cdot Y_n^{\beta_N} \Leftrightarrow Y^{\left((\sum_k \beta_k), \beta_n, \ldots, \beta_1\right)} <_{Lex} Y^{\left((\sum_k \alpha_k), \alpha_n, \ldots, \alpha_1\right)}$$

Block Orderings
Let $<_1$ (resp. $<_2$) be an admissible ordering on $U = Y_1, \ldots, Y_d$ (resp. $X = Y_{d+1}, \ldots, Y_n$), we define $<$ on $[Y_1, \ldots, Y_n]$

$$U^m X^l < U^p X^q \Leftrightarrow ((X^l <_2 X^q) \ or \ (X^l = X^q \ and \ U^m <_1 U^p))$$

Zero Dimensional Systems

Dimension 0 : check !

Let G a Gröbner basis of I for any admissible monomial ordering $<$.

Known result : $\sharp V_C < \infty \Leftrightarrow C[Y]/I_C$ is a finite dimensional C-vector space

($\Leftrightarrow K[Y]/I_K$ is a finite dimensional K-vector space $\Leftrightarrow I_K$ has dimension $0 \Leftrightarrow I_C$ has dimension 0)

Dimension 0 : check !

Let G a Gröbner basis of I for any admissible monomial ordering $<$.

Known result : $\sharp V_C < \infty \Leftrightarrow C[Y]/I_C$ is a finite dimensional C-vector space

($\Leftrightarrow K[Y]/I_K$ is a finite dimensional K-vector space $\Leftrightarrow I_K$ has dimension $0 \Leftrightarrow I_C$ has dimension 0)

I has dimension 0 iff $\forall i = 1 \ldots n, \exists g \in G, \exists n_i \in \mathbb{N}^* \; : \; LM_<(g) = Y^{n_i}$

Dimension 0 : check !

Let G a Gröbner basis of I for any admissible monomial ordering $<$.

Known result : $\sharp V_C < \infty \Leftrightarrow C[Y]/I_C$ is a finite dimensional C-vector space

($\Leftrightarrow K[Y]/I_K$ is a finite dimensional K-vector space $\Leftrightarrow I_K$ has dimension $0 \Leftrightarrow I_C$ has dimension 0)

I has dimension 0 iff $\forall i = 1 \ldots n, \exists g \in G, \exists n_i \in \mathbb{N}^* \ : \ LM_<(g) = Y^{n_i}$

$\Rightarrow$ Since $C[Y]/I_C$ is a finite dimensional C-vector space,
$\forall i = 1 \ldots n, \exists D_i \in \mathbb{N}$, $1, Y_i, \ldots, Y_i^{D_i}$ are C-linearly dependents in $C[Y]/I_C$. Also $\exists P_i \neq 0 \in C[Y_i] \bigcap I$. In particular $NF_<(P_i, G) = 0$.

Dimension 0 : check !

Let G a Gröbner basis of I for any admissible monomial ordering $<$.

Known result : $\sharp V_C < \infty \Leftrightarrow C[Y]/I_C$ is a finite dimensional C-vector space

($\Leftrightarrow K[Y]/I_K$ is a finite dimensional K-vector space $\Leftrightarrow I_K$ has dimension $0 \Leftrightarrow I_C$ has dimension 0)

I has dimension 0 iff $\forall i = 1 \ldots n, \exists g \in G, \exists n_i \in \mathbb{N}^* \ : \ LM_<(g) = Y^{n_i}$

$\Leftarrow$ If $\forall i = 1 \ldots n, \exists g \in G, n_i \in \mathbb{N}^* \ : \ LM_<(g) = Y^{n_i}$, then $p \in C[Y]/I_C$ is a linear combination of monomials in the form $Y_1^{m_1} \ldots Y_n^{m_n}$ with $m_i < n_i$ and so $C[Y]/I_C$ is a finite dimensional C-vector space.

Dimension 0 : check !

Let G a Gröbner basis of I for any admissible monomial ordering $<$.

Known result : $\sharp V_C < \infty \Leftrightarrow C[Y]/I_C$ is a finite dimensional C-vector space

($\Leftrightarrow K[Y]/I_K$ is a finite dimensional K-vector space $\Leftrightarrow I_K$ has dimension $0 \Leftrightarrow I_C$ has dimension 0)

I has dimension 0 iff $\forall i = 1 \dots n, \exists g \in G, \exists n_i \in \mathbb{N}^* \ : \ LM_<(g) = Y^{n_i}$

If $\mathcal{S} \subset K[Y]$ then $G \in K[Y]$.

The dimension of the K-vector space (resp. C-vector space) $K[Y]/I_K$ (resp. $C[Y]/I_C$) is the number of complex zeroes of I_C counted with multiplicities.

Dimension 0 : computing $K[Y]/I_K$

A monomial basis of the K-vector space $K[Y]/I_K$ can be read on a Gröbner basis G of I_K (for any monomial ordering) :

$$\mathcal{B}_<(I_K) = \{m \in M[Y] \ : NF_<(m, G) = m\}$$

This is the set of all the possible monomials $m \in K[Y]$ that can not be reduced by $NF_<(., G)$, or equivalently such that $\nexists g \in G$ such that $LM_<(g)$ divides m.

Dimension 0 : multiplication maps

Let $h \in K[Y]$

$$\begin{array}{cccc} m_h : & C[Y]/I_C & \longrightarrow & C[Y]/I_C \\ & \overline{p} & \longmapsto & \overline{ph} \end{array}$$

(Stickelberger) The eigenvalues of m_h are exactly the $h(\alpha)$, $\alpha \in V_C$ with respective multiplicities the multiplicity of α (dimension of $(C[Y]/I_C)_\alpha$).

Suppose G is a Gröbner basis of I for $<$ and that $\mathcal{B}_<(G) = \{w_1, \ldots w_D\}$

If $NF_<(h, G) = \sum_{i=1}^{D} a_i w_i$ with $a_i \in K$ (uniquely defined if G is reduced), let denote $\overrightarrow{h} = [a_1, \ldots a_D]$, and by M_h the matrix of m_h with respect to $\mathcal{B}_<(G)$.

Then

$$M_h = [\overrightarrow{hw_1}, \ldots, \overrightarrow{hw_D}]^T$$

can explicitly be computed.

Dimension 0 : applications of Stickelberger theorem

The eigenvalues of m_{Y_i} are exactly the i-th coordinates of all the points of V_C.

If I is radical and if $Y_1(\alpha) \neq Y_1(\beta) \forall \alpha \neq \beta \in V_C$, then a Gröbner basis for any lexicographic ordering such that $Y_1 < Y_i \; i = 1 \ldots n$ has always the following shape :

$$\begin{cases} f(Y_1) = 0 \\ Y_2 = f_2(Y_1) \\ \vdots \\ Y_n = f_n(Y_1) \end{cases}$$

When a Gröbner basis has this shape, the system is said to be in shape position.

Computing the complex/real roots of the system is now equivalent to solve $f(Y_1) = 0$

Dimension 0 : shape lemma

Suppose I radical.

Let $\mathcal{T} = \{Y_1 + iY_2, \ldots + i^{n-1}Y_n \;,\; i = 1 \ldots nD(D-1)/2\}$. There exists $t \in \mathcal{T}$ s.t. $\alpha \neq \beta \in V_C \Rightarrow t(\alpha) \neq t(\beta)$.
Sickelberger $\Rightarrow f(T) = CharPol(m_t)$ is square-free.

Also, the system can be re-written :

$$\left\{\begin{array}{l} f(T) = 0 \\ Y_2 = f_2(T) \\ \vdots \\ Y_n = f_n(T) \end{array}\right.$$

Computing the complex/real roots of the system is now equivalent to solve $f(T) = 0$

Dimension 0 : Hermite's quadratic form

For $h \in K[Y]$, let define :

$$\begin{array}{rcll} q_p : & K[Y]/I_K & \longrightarrow & K \\ & f & \longmapsto & Trace(m_{hp^2}) \end{array}$$

- $rank(q_p) = \sharp\{y \in V_C \ : \ p(y) \neq 0\}$
- $sig(q_p) = \sharp\{y \in V_R \ : \ p(y) > 0\} - \sharp\{y \in V_R \ : \ p(y) < 0\}$.

In particular, the rank (resp. signature) of q_1 give the number of distinct complex (resp. real) roots of $\mathcal{S}$.

Application : P separates V_C iff $degree(\overline{CharPol(m_p)}) = rank(q_1)$

Dimension 0 : the general case - Lex. G. Basis

The general shape of the Lexicographic Gröbner basis is the following :

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

Dimension 0 : the general case - Lex. G. Basis

The general shape of the Lexicographic Gröbner basis is the following :

$f_1(Y_1)$

$f_2(Y_1, Y_2)$

$\vdots$

$f_{k_2}(Y_1, Y_2)$

$f_{k_2+1}(Y_1, Y_2, Y_3)$

$\vdots$

$f_{k_{n-1}+1}(Y_1, \ldots, Y_n)$

$\vdots$

$f_{k_n}(Y_1, \ldots, Y_n)$

Proof : since I_K has dimension 0, then $I_K \bigcap K[Y_i] \neq \emptyset \; \forall i = 1 \ldots n$. If $p \in I_K \bigcap K[Y_i]$, then $NF_{<_{lex}}(p, G) = 0$ and in particular $\exists g \in G$ s.t. $LM_{<_{lex}}(g) = Y_i^{n_i}$, and consequently $g \in K[Y_1, \ldots, Y_i]$.

Dimension 0 : the general case - Lex. G. Basis

The general shape of the Lexicographic Gröbner basis is the following :

$f_1(Y_1)$

$f_2(Y_1, Y_2)$

$\vdots$

$f_{k_2}(Y_1, Y_2)$

$f_{k_2+1}(Y_1, Y_2, Y_3)$

$\vdots$

$f_{k_{n-1}+1}(Y_1, \ldots, Y_n)$

$\vdots$

$f_{k_n}(Y_1, \ldots, Y_n)$

Proof : since I_K has dimension 0, then $I_K \bigcap K[Y_i] \neq \emptyset \; \forall i = 1 \ldots n$. If $p \in I_K \bigcap K[Y_i]$, then $NF_{<_{lex}}(p, G) = 0$ and in particular $\exists g \in G$ s.t. $LM_{<_{lex}}(g) = Y_i^{n_i}$, and consequently $g \in K[Y_1, \ldots, Y_i]$.

$G \bigcap K[X_1, \ldots, X_i]$ is a lex. G. Basis of $G \bigcap K[X_1, \ldots, X_i]$

Dimension 0 : the general case - Lex. G. Basis

The general shape of the Lexicographic Gröbner basis is the following :

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

Proof : since I_K has dimension 0, then $I_K \bigcap K[Y_i] \neq \emptyset \; \forall i = 1 \ldots n$. If $p \in I_K \bigcap K[Y_i]$, then $NF_{<_{lex}}(p, G) = 0$ and in particular $\exists g \in G$ s.t. $LM_{<_{lex}}(g) = Y_i^{n_i}$, and consequently $g \in K[Y_1, \ldots, Y_i]$.

$G \bigcap K[X_1, \ldots, X_i]$ is a lex. G. Basis of $G \bigcap K[X_1, \ldots, X_i]$

Numerical "Solve" is difficult

Dimension 0 : FGLM Algorithm

Let G a G. Basis for any ordering $<_1$. One want to compute the G. Basis of $< G >$ for an ordering $<_2$.

The basic principle is simple : consider all the possible monomials in increasing order for $<_2$ as vectors w.r.t $\mathcal{B}_{<_1}(G_{<1})$, detect the linear combinations (polynomials of the new G. Basis : $G_{<_2}$), stop when $\forall i = 1 \ldots n \exists n_i \in \mathbb{N}^* \exists g \in G_{<_2} \; : \; LM_{<2}(g) = Y_i^{n_i}$

Dimension 0 : FGLM Algorithm

Let G a G. Basis for any ordering $<_1$. One want to compute the G. Basis of $< G >$ for an ordering $<_2$.

The basic principle is simple : consider all the possible monomials in increasing order for $<_2$ as vectors w.r.t $\mathcal{B}_{<_1}(G_{<1})$, detect the linear combinations (polynomials of the new G. Basis : $G_{<_2}$), stop when $\forall i = 1 \ldots n \exists n_i \in \mathbb{N}^* \exists g \in G_{<_2} \ : \ LM_{<2}(g) = Y_i^{n_i}$

---

compute $\overrightarrow{1}, \overrightarrow{Y_1}, \ldots, \overrightarrow{Y_1^d}$ and stop when a linear dependence is founded.

Dimension 0 : FGLM Algorithm

Let G a G. Basis for any ordering $<_1$. One want to compute the G. Basis of $< G >$ for an ordering $<_2$.

The basic principle is simple : consider all the possible monomials in increasing order for $<_2$ as vectors w.r.t $\mathcal{B}_{<_1}(G_{<1})$, detect the linear combinations (polynomials of the new G. Basis : $G_{<_2}$), stop when $\forall i = 1 \ldots n \exists n_i \in \mathbb{N}^* \exists g \in G_{<_2} \; : \; LM_{<2}(g) = Y_i^{n_i}$

$f_1(Y_1)$

Dimension 0 : FGLM Algorithm

Let G a G. Basis for any ordering $<_1$. One want to compute the G. Basis of $< G >$ for an ordering $<_2$.

The basic principle is simple : consider all the possible monomials in increasing order for $<_2$ as vectors w.r.t $\mathcal{B}_{<_1}(G_{<1})$, detect the linear combinations (polynomials of the new G. Basis : $G_{<_2}$), stop when $\forall i = 1 \ldots n \exists n_i \in \mathbb{N}^* \exists g \in G_{<_2} \; : \; LM_{<2}(g) = Y_i^{n_i}$

$f_1(Y_1)$

follow with $\overrightarrow{Y_2}, \overrightarrow{Y_1 Y_2}, \ldots, \overrightarrow{Y_1^{d-1} Y_2}$ and stop when a linear dependence is founded.

Dimension 0 : FGLM Algorithm

Let G a G. Basis for any ordering $<_1$. One want to compute the G. Basis of $< G >$ for an ordering $<_2$.

The basic principle is simple : consider all the possible monomials in increasing order for $<_2$ as vectors w.r.t $\mathcal{B}_{<_1}(G_{<1})$, detect the linear combinations (polynomials of the new G. Basis : $G_{<_2}$), stop when $\forall i = 1 \ldots n \exists n_i \in \mathbb{N}^* \exists g \in G_{<_2} \; : \; LM_{<2}(g) = Y_i^{n_i}$

$f_1(Y_1)$

$f_2(Y_1, Y_2)$

$\vdots$

Dimension 0 : FGLM Algorithm

Let G a G. Basis for any ordering $<_1$. One want to compute the G. Basis of $< G >$ for an ordering $<_2$.

The basic principle is simple : consider all the possible monomials in increasing order for $<_2$ as vectors w.r.t $\mathcal{B}_{<_1}(G_{<1})$, detect the linear combinations (polynomials of the new G. Basis : $G_{<_2}$), stop when $\forall i = 1 \ldots n \exists n_i \in \mathbb{N}^* \exists g \in G_{<_2} \ : \ LM_{<2}(g) = Y_i^{n_i}$

$f_1(Y_1)$

$f_2(Y_1, Y_2)$

$\vdots$

follow multiplying by Y_2 up to finding $g \in G_{<_2}$ such that $LM_{<_2}(g) = Y_2^{n_2}$

Dimension 0 : FGLM Algorithm

Let G a G. Basis for any ordering $<_1$. One want to compute the G. Basis of $< G >$ for an ordering $<_2$.

The basic principle is simple : consider all the possible monomials in increasing order for $<_2$ as vectors w.r.t $\mathcal{B}_{<_1}(G_{<1})$, detect the linear combinations (polynomials of the new G. Basis : $G_{<_2}$), stop when $\forall i = 1 \ldots n \exists n_i \in \mathbb{N}^* \exists g \in G_{<_2} \; : \; LM_{<2}(g) = Y_i^{n_i}$

$$f_1(Y_1)$$
$$f_2(Y_1, Y_2)$$
$$\vdots$$
$$f_{k_2}(Y_1, Y_2)$$

Dimension 0 : FGLM Algorithm

Let G a G. Basis for any ordering $<_1$. One want to compute the G. Basis of $< G >$ for an ordering $<_2$.

The basic principle is simple : consider all the possible monomials in increasing order for $<_2$ as vectors w.r.t $\mathcal{B}_{<_1}(G_{<1})$, detect the linear combinations (polynomials of the new G. Basis : $G_{<_2}$), stop when $\forall i = 1 \ldots n \exists n_i \in \mathbb{N}^* \exists g \in G_{<_2} \;:\; LM_{<2}(g) = Y_i^{n_i}$

$$f_1(Y_1)$$

$$f_2(Y_1, Y_2)$$

$$\vdots$$

$$f_{k_2}(Y_1, Y_2)$$

Apply the same process iteratively with $Y_3, \ldots, Y_n$

Dimension 0 : FGLM Algorithm

Let G a G. Basis for any ordering $<_1$. One want to compute the G. Basis of $< G >$ for an ordering $<_2$.

The basic principle is simple : consider all the possible monomials in increasing order for $<_2$ as vectors w.r.t $\mathcal{B}_{<_1}(G_{<1})$, detect the linear combinations (polynomials of the new G. Basis : $G_{<_2}$), stop when $\forall i = 1 \ldots n \exists n_i \in \mathbb{N}^* \exists g \in G_{<_2} \ : \ LM_{<2}(g) = Y_i^{n_i}$

$f_1(Y_1)$

$f_2(Y_1, Y_2)$

$\vdots$

$f_{k_2}(Y_1, Y_2)$

$f_{k_2+1}(Y_1, Y_2, Y_3)$

$\vdots$

$f_{k_n}(Y_1, \ldots, Y_n)$

Apply the same process iteratively with $Y_3, \ldots, Y_n$

Dimension 0 : the general case - RUR

Let $t \in \mathcal{T}$ s.t. $\alpha \neq \beta \in V_C \Rightarrow t(\alpha) \neq t(\beta)$.

Let $g_t(T) = CharPol(m_t) = \prod_{\alpha \in V_C} (T - t(\alpha))^{\mu(\alpha)}$.

We denote by $\overline{f}$ the square-free part of $f \in K[T]$ and by $H_i(f)$ the i-th Horner's polynomial associated to f : $H_i(f)(T) = \sum_{j=0}^{i} a_{i-j} T^i$ if $f = \sum_{j=0}^{D} a_i T^i$.

For $p \in K[Y]$, if $d = degree(\overline{f})$ and $g_{t,p}(T) = \sum_{i=0}^{d-1} Trace(m_{pt^i}) H_{d-i-1}(g_t)(T)$, then $p(\alpha) = \frac{g_{t,p}(t(\alpha))}{g_{t,1}(t(\alpha))}$.

"Proof" : since $Trace(m_p) = \sum_{\alpha \in V_C} \mu(\alpha) p(\alpha)$, then

$$g_{t,p}(T) = \sum_{\alpha \in V_C} \mu(\alpha) p(\alpha) \prod_{\beta \in V_C, \beta \neq \alpha} (T - t(\beta))$$

Dimension 0 : the general case - RUR

Let $t \in \mathcal{T}$ s.t. $\alpha \neq \beta \in V_C \Rightarrow t(\alpha) \neq t(\beta)$.
Let $g_t(T) = CharPol(m_t) = \prod_{\alpha \in V_C} (T - t(\alpha))^{\mu(\alpha)}$.

We denote by $\overline{f}$ the square-free part of $f \in K[T]$ and by $H_i(f)$ the i-th Horner's polynomial associated to f : $H_i(f)(T) = \sum_{j=0}^{i} a_{i-j} T^i$ if $f = \sum_{j=0}^{D} a_i T^i$.

For $p \in K[Y]$, if $d = degree(\overline{f})$ and
$g_{t,p}(T) = \sum_{i=0}^{d-1} Trace(m_{pt^i}) H_{d-i-1}(g_t)(T)$, then $p(\alpha) = \frac{g_{t,p}(t(\alpha))}{g_{t,1}(t(\alpha))}$.

A one-to-one correspondence :

$$\begin{array}{ccc} \mathcal{V}(I_K) & \longrightarrow & \mathcal{V}(g_t) \\ (\alpha_1, \ldots, \alpha_n) & \longrightarrow & t(\alpha_1, \ldots, \alpha_n) \\ \left(\frac{g_{t,Y_1}(\beta)}{g_{t,1}(\beta)}, \ldots, \frac{g_{t,Y_n}(\beta)}{g_{t,1}(\beta)} \right) & \longleftarrow & \beta \end{array}$$

Dimension 0 : the Rational Univariate Representation

$\{g_t, g_{t,1}, g_{t,Y_1}, \ldots, g_{t,Y_n}\}$ is the Rational Univariate Representation of V_C associated to t.

Note that $g_{t,1} = \overline{g_t'}$. In particular g_t and $g_{t,1}$ are coprime.

Solving the system through the RUR means :

- solving the univariate polynomial g_t
- evaluating/studying the rational functions $g_{t,Y_i}/g_{t,1}$ at the roots of g_t.

Since the RUR has coefficients in K, it preserves the real roots.

By construction, it “preserves” the multiplicities. In particular, a square-free decomposition of g_t would decompose the zeroes w.r.t. the multiplicities.

Remark : this costly computation can be avoid since

$$\frac{\overline{g_t}'}{g_{t,1}}(t(\alpha)) = \mu(\alpha)$$

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 $Trace(m_{Y_j t^i})$