Real roots of systems of polynomial equations and inequations or inequalities

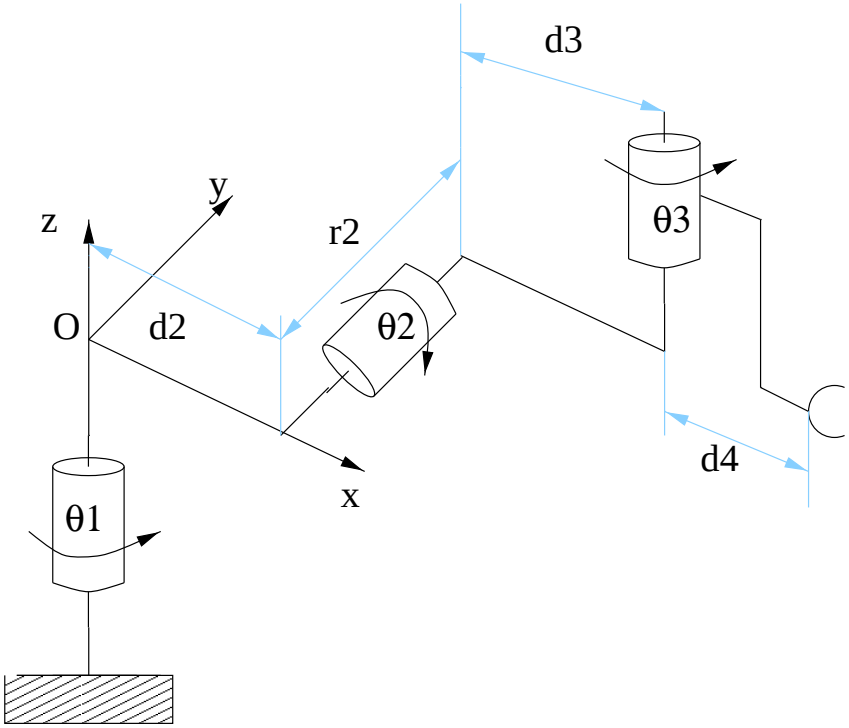
Using Exact Computations

Fabrice Rouillier

SALSA (INRIA) project and CALFOR (LIP6) team

Paris, France

A challenge



For which design parameters these kind of robot can change of posture without crossing a singularity ?

$\Rightarrow$ Deciding if a univariate polynomial p of degree 4 has triple roots or not.

The coefficients depends on 2 indeterminates ρ, z and on 3 parameters d_4, d_3, r_2 : we have to solve a parametric system depending on 3 indeterminates and 3 parameters.

The system $(p, \partial p/\partial t, \partial^2 p/\partial t^2)$

[1 + 8 t r2 d4^3 + 8 t r2 d4 + 8 t r2^3 d4 + 4 d4 d3 r2^2 − 4 t^4 d4 d3 r2^2 − 4 t^4 d4 d3 r3^2 + 4 t^4 d4 d3 rho^
2 + 4 t^4 d4 d3 z^2 − 16 t^3 r2 d3 d4^2 + 8 t^3 r2 d4 d3^2 + 8 t^3 r2 d4 r3^2 − 8 t^3 r2 d4 rho^2 − 8 t^
3 r2 d4 z^2 + 8 t r2 d4 r3^2 − 8 t r2 d4 rho^2 − 8 t r2 d4 z^2 + 16 t r2 d3 d4^2 + 6 d4^2 d3^2 + 4 d4 d3^3 +
4 d4^3 d3 + 2 rho^2 z^2 − 2 rho^2 d3^2 − 2 rho^2 d4^2 − 2 rho^2 r2^2 − 2 rho^2 r3^2 − 2 z^2 d3^2 − 2 z^
2 d4^2 − 2 z^2 r2^2 − 2 z^2 r3^2 + 2 d3^2 r2^2 + 2 d3^2 r3^2 + 2 d4^2 r2^2 + 2 d4^2 r3^2 + 2 r2^2 r3^2 −
2 t^4 rho^2 + 2 t^4 z^2 − 2 t^4 d3^2 − 2 t^4 d4^2 + 2 t^4 r2^2 − 2 t^4 r3^2 + t^4 rho^4 + t^4 z^4 + t^4 d3^
4 + t^4 d4^4 + t^4 r2^4 + t^4 r3^4 − 2 rho^2 + 2 z^2 − 2 d3^2 − 2 d4^2 + 2 r2^2 − 2 r3^2 + t^4 + 2 t^2 +
rho^4 + z^4 − 4 d4 d3 + 4 d4 d3 r3^2 − 4 d4 d3 rho^2 − 4 d4 d3 z^2 + 6 t^4 d4^2 d3^2 − 4 t^4 d4 d3^3 − 4 t^
4 d4^3 d3 + 2 t^4 rho^2 z^2 − 2 t^4 rho^2 d3^2 − 2 t^4 rho^2 d4^2 − 2 t^4 rho^2 r2^2 − 2 t^4 rho^2 r3^2 −
2 t^4 z^2 d3^2 − 2 t^4 z^2 d4^2 − 2 t^4 z^2 r2^2 − 2 t^4 z^2 r3^2 + 2 t^4 d3^2 r2^2 + 2 t^4 d3^2 r3^2 + 2 t^
4 d4^2 r2^2 + 2 t^4 d4^2 r3^2 + 2 t^4 r2^2 r3^2 + 4 t^4 d4 d3 + 8 t^3 r2 d4 + 8 t^3 r2 d4^3 + 8 t^3 r2^3 d4 +
d3^4 + d4^4 + r2^4 + r3^4 − 4 t^2 rho^2 + 4 t^2 z^2 − 4 t^2 d3^2 + 12 t^2 d4^2 + 4 t^2 r2^2 − 4 t^2 r3^2 +
2 t^2 rho^4 + 2 t^2 z^4 + 2 t^2 d3^4 + 2 t^2 d4^4 + 2 t^2 r2^4 + 2 t^2 r3^4 + 8 t r2 d4 d3^2 − 4 t^2 d4^2 d3^
2 + 4 t^2 rho^2 z^2 − 4 t^2 rho^2 d3^2 − 4 t^2 rho^2 d4^2 − 4 t^2 rho^2 r2^2 − 4 t^2 rho^2 r3^2 − 4 t^2 z^
2 d3^2 − 4 t^2 z^2 d4^2 − 4 t^2 z^2 r2^2 − 4 t^2 z^2 r3^2 + 4 t^2 d3^2 r2^2 + 4 t^2 d3^2 r3^2 + 20 t^2 d4^
2 r2^2 + 4 t^2 d4^2 r3^2 + 4 t^2 r2^2 r3^2, t − 4 t^3 d4 d3 r2^2 − 4 t^3 d4 d3 r3^2 + 4 t^3 d4 d3 rho^2 + 4 t^
3 d4 d3 z^2 − 12 t^2 r2 d3 d4^2 + 6 t^2 r2 d4 d3^2 + 6 t^2 r2 d4 r3^2 − 6 t^2 r2 d4 rho^2 − 6 t^2 r2 d4 z^2 +
2 r2 d4 + 2 r2^3 d4 + t^3 + 4 r2 d3 d4^2 + 2 r2 d4 d3^2 + 2 r2 d4 r3^2 − 2 r2 d4 rho^2 − 2 r2 d4 z^2 + 2 r2 d4^
3 + 2 t^3 z^2 − 2 t^3 d3^2 − 2 t^3 d4^2 + 2 t^3 r2^2 − 2 t^3 r3^2 + t^3 rho^4 + t^3 z^4 + t^3 d3^4 + t^3 d4^

$$4 + t\hat{}3\ r2\hat{}4 + t\hat{}3\ r3\hat{}4 - 2\ t\ \mathrm{rho}\hat{}2 + 2\ t\ z\hat{}2 - 2\ t\ d3\hat{}2 + 6\ t\ d4\hat{}2 + 2\ t\ r2\hat{}2 - 2\ t\ r3\hat{}2 + t\ \mathrm{rho}\hat{}4 + t\ z\hat{}4 +$$
$$t\ d3\hat{}4 + t\ d4\hat{}4 + t\ r2\hat{}4 + t\ r3\hat{}4 + 6\ t\hat{}3\ d4\hat{}2\ d3\hat{}2 - 4\ t\hat{}3\ d4\ d3\hat{}3 - 4\ t\hat{}3\ d4\hat{}3\ d3 + 2\ t\hat{}3\ \mathrm{rho}\hat{}2\ z\hat{}2 - 2\ t\hat{}$$
$$3\ \mathrm{rho}\hat{}2\ d3\hat{}2 - 2\ t\hat{}3\ \mathrm{rho}\hat{}2\ d4\hat{}2 - 2\ t\hat{}3\ \mathrm{rho}\hat{}2\ r2\hat{}2 - 2\ t\hat{}3\ \mathrm{rho}\hat{}2\ r3\hat{}2 - 2\ t\hat{}3\ z\hat{}2\ d3\hat{}2 - 2\ t\hat{}3\ z\hat{}2\ d4\hat{}2 -$$
$$2\ t\hat{}3\ z\hat{}2\ r2\hat{}2 - 2\ t\hat{}3\ z\hat{}2\ r3\hat{}2 + 2\ t\hat{}3\ d3\hat{}2\ r2\hat{}2 + 2\ t\hat{}3\ d3\hat{}2\ r3\hat{}2 + 2\ t\hat{}3\ d4\hat{}2\ r2\hat{}2 + 2\ t\hat{}3\ d4\hat{}2\ r3\hat{}2 + 2\ t\hat{}$$
$$3\ r2\hat{}2\ r3\hat{}2 + 4\ t\hat{}3\ d4\ d3 + 6\ t\hat{}2\ r2\ d4 + 6\ t\hat{}2\ r2\ d4\hat{}3 + 6\ t\hat{}2\ r2\hat{}3\ d4 - 2\ t\ d4\hat{}2\ d3\hat{}2 + 2\ t\ \mathrm{rho}\hat{}2\ z\hat{}2 -$$
$$2\ t\ \mathrm{rho}\hat{}2\ d3\hat{}2 - 2\ t\ \mathrm{rho}\hat{}2\ d4\hat{}2 - 2\ t\ \mathrm{rho}\hat{}2\ r2\hat{}2 - 2\ t\ \mathrm{rho}\hat{}2\ r3\hat{}2 - 2\ t\ z\hat{}2\ d3\hat{}2 - 2\ t\ z\hat{}2\ d4\hat{}2 - 2\ t\ z\hat{}2\ r2\hat{}$$
$$2 - 2\ t\ z\hat{}2\ r3\hat{}2 + 2\ t\ d3\hat{}2\ r2\hat{}2 + 2\ t\ d3\hat{}2\ r3\hat{}2 + 10\ t\ d4\hat{}2\ r2\hat{}2 + 2\ t\ d4\hat{}2\ r3\hat{}2 + 2\ t\ r2\hat{}2\ r3\hat{}2 - 2\ t\hat{}3\ \mathrm{rho}\hat{}$$
$$2,\ 1 + 12\ t\ r2\ d4\hat{}3 - 12\ t\hat{}2\ d4\hat{}3\ d3 - 12\ t\hat{}2\ d4\ d3\hat{}3 + 12\ t\ r2\ d4 + 12\ t\ r2\hat{}3\ d4 + 12\ t\ r2\ d4\ r3\hat{}2 -$$
$$12\ t\ r2\ d4\ \mathrm{rho}\hat{}2 - 12\ t\ r2\ d4\ z\hat{}2 - 24\ t\ r2\ d3\ d4\hat{}2 - 12\ t\hat{}2\ d4\ d3\ r2\hat{}2 - 12\ t\hat{}2\ d4\ d3\ r3\hat{}2 - 2\ d4\hat{}2\ d3\hat{}2 +$$
$$2\ \mathrm{rho}\hat{}2\ z\hat{}2 - 2\ \mathrm{rho}\hat{}2\ d3\hat{}2 - 2\ \mathrm{rho}\hat{}2\ d4\hat{}2 - 2\ \mathrm{rho}\hat{}2\ r2\hat{}2 - 2\ \mathrm{rho}\hat{}2\ r3\hat{}2 - 2\ z\hat{}2\ d3\hat{}2 - 2\ z\hat{}2\ d4\hat{}2 - 2\ z\hat{}$$
$$2\ r2\hat{}2 - 2\ z\hat{}2\ r3\hat{}2 + 2\ d3\hat{}2\ r2\hat{}2 + 2\ d3\hat{}2\ r3\hat{}2 + 10\ d4\hat{}2\ r2\hat{}2 + 2\ d4\hat{}2\ r3\hat{}2 + 2\ r2\hat{}2\ r3\hat{}2 - 2\ \mathrm{rho}\hat{}2 + 2\ z\hat{}$$
$$2 - 2\ d3\hat{}2 + 6\ d4\hat{}2 + 2\ r2\hat{}2 - 2\ r3\hat{}2 + 3\ t\hat{}2 + \mathrm{rho}\hat{}4 + z\hat{}4 + d3\hat{}4 + d4\hat{}4 + r2\hat{}4 + r3\hat{}4 - 6\ t\hat{}2\ \mathrm{rho}\hat{}2 +$$
$$6\ t\hat{}2\ z\hat{}2 - 6\ t\hat{}2\ d3\hat{}2 - 6\ t\hat{}2\ d4\hat{}2 + 6\ t\hat{}2\ r2\hat{}2 - 6\ t\hat{}2\ r3\hat{}2 + 3\ t\hat{}2\ \mathrm{rho}\hat{}4 + 3\ t\hat{}2\ z\hat{}4 + 3\ t\hat{}2\ d3\hat{}4 + 3\ t\hat{}$$
$$2\ d4\hat{}4 + 3\ t\hat{}2\ r2\hat{}4 + 3\ t\hat{}2\ r3\hat{}4 + 12\ t\ r2\ d4\ d3\hat{}2 + 18\ t\hat{}2\ d4\hat{}2\ d3\hat{}2 + 6\ t\hat{}2\ \mathrm{rho}\hat{}2\ z\hat{}2 - 6\ t\hat{}2\ \mathrm{rho}\hat{}2\ d3\hat{}2 -$$
$$6\ t\hat{}2\ \mathrm{rho}\hat{}2\ d4\hat{}2 - 6\ t\hat{}2\ \mathrm{rho}\hat{}2\ r2\hat{}2 - 6\ t\hat{}2\ \mathrm{rho}\hat{}2\ r3\hat{}2 - 6\ t\hat{}2\ z\hat{}2\ d3\hat{}2 - 6\ t\hat{}2\ z\hat{}2\ d4\hat{}2 - 6\ t\hat{}2\ z\hat{}2\ r2\hat{}2 -$$
$$6\ t\hat{}2\ z\hat{}2\ r3\hat{}2 + 6\ t\hat{}2\ d3\hat{}2\ r2\hat{}2 + 6\ t\hat{}2\ d3\hat{}2\ r3\hat{}2 + 6\ t\hat{}2\ d4\hat{}2\ r2\hat{}2 + 6\ t\hat{}2\ d4\hat{}2\ r3\hat{}2 + 6\ t\hat{}2\ r2\hat{}2\ r3\hat{}2 +$$
$$12\ t\hat{}2\ d4\ d3 + 12\ t\hat{}2\ d4\ d3\ \mathrm{rho}\hat{}2 + 12\ t\hat{}2\ d4\ d3\ z\hat{}2]$$

For specializations of the parameters : Solving zero-dimensional systems

Low level algorithms (implemented in C - RS software):

- (RSU) Real Roots of univariate polynomials (Descartes' based method) - Rouillier/Zimmermann 2003 : all the roots are isolated with interval with rational bounds. Memory optimal version + use of floating point arithmetics.

- (RSZD) Zero-dimensional Systems : from a Gröbner basis (Faugère F4/F5) or a triangular sets (ex : Aubry, Lazard, Moreno 1999) reduce the problem to a univariate one (Rouillier 1999, 2004) :

$$(f_t(T) = 0, \underbrace{X_1 = g_1(T)/g(T), ..., X_n = g_n(T)/g(T)}_{\text{coordinates}}, \underbrace{\mu = m(T)/g(T)}_{\text{multiplicity}},$$
$$[\underbrace{p_1 = h_1(T)/g(T), ..., p_s = h_s(T)/g(T)}_{\text{evaluation of polynomials at the roots}}])$$

  - preserves the real roots and multiplicities

Dimension Zero : 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)

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

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

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

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

$\dim(K[Y]/I_K)$=$\dim(C[Y]/I_C)$=number of complex zeroes of I_C counted with multiplicities.

Dimension Zero : "compute" $K[Y]/I_K$

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 $h \in K[Y]$

$$\begin{array}{rccc} m_h\colon & C[Y]/I_C & \longrightarrow & C[Y]/I_C \\ & p & \longmapsto & p\,h \end{array}$$

Thm : 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 $\mathcal{B}_<(G) = \{w_1, ...w_D\}$

If $N\,F_<(h, G) = \sum_{i=1}^{D} a_i w_i$ with $a_i \in K$ (G reduced), let us denote by $\vec{h} = [a_1, ...a_D]$, and by M_h the matrix of m_h with respect to $\mathcal{B}_<(G)$.

Then

$$M_h = [\overrightarrow{h\,w_1}, ..., \overrightarrow{h\,w_D}]^T$$

can explicitly be computed.

Dimension 0 : use of Stickelberger's 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 $Y_1 < Y_i \; i = 1...n$ has always the following shape (shape position):

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

Computing the complex/real roots of the system is in this case equivalent to solving $f(Y_1) = 0$

Dimension 0 : shape lemma

Suppose I radical.

Let $\mathcal{T} = \{Y_1 + i\, Y_2, \ldots + i^{n-1} Y_n\ ,\ i = 1 \ldots n\ D(D-1)/2\}$. There exists $t \in \mathcal{T}$ s.t. $\alpha \neq \beta \in V_C \Rightarrow t(\alpha) \neq t(\beta)$.

Sickelberger $\Rightarrow$ $f(T) = Char Pol(m_t)$ is square-free.

Also, the system can be "re-written":

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

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

Dimension 0 : Hermite

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

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

Thm :

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

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:

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

Numerical "Solve" is difficult

Dimension 0 : the general case - RUR

For $t \in K[X_1, .., X_n]$ let us define

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

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:

$$H_i(f)(T) = \sum_{j=0}^{i} a_{i-j} T^i \text{ if } f = \sum_{j=0}^{D} a_i T^i.$$

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, if t is separating $(t(\alpha) \neq t(\beta), \forall \beta \neq \alpha \in \mathcal{V}(I_K))$: $p(\alpha) = \frac{g_{t,p}(t(\alpha))}{g_{t,1}(t(\alpha))}$

Dimension 0 : the RUR

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

When t is separating $\mathcal{V}(\mathcal{I})$, this is a Rational Univariate Representation.

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 $g_{t,Y_i}/g_{t,1}(Y_i)$ 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: such a costly computation can be optimized since $\frac{g_t{}'}{g_{t,1}}(t(\alpha)) = \mu(\alpha)$

RUR : a simple algorithm

- (1) compute $d = rank(q_1)$
- (2) find $t \in \mathcal{T} = \{Y_1 + i\,Y_2, ... + i^{n-1}Y_n\ ,\ i = 1...n\,d(d-1)/2\}$ such that $degree(\overline{PolChar(m_t)}) = d$
- (3) compute the $Trace(m_{X_j t^i})$ for $i = 1...d$ and $j = 1...n$
- compte the RUR from (3)

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:

- $\{g_t,\ g_{t,1},\ g_{t,Y_1},\ ...,\ g_{t,Y_n}\}$ 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 $Trace(m_{h_j w_i}) = 0\ ,\ \forall i = 1...D$.

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

Extending the RUR

Given $v_1, ..., v_s \in \mathbb{Q}[X_1, ..., X_n]$, what is the sign of v_i at $\alpha \in \boldsymbol{V}(I)$?

Naive solutions :

- subs$(X_i = \frac{g_{t,X_i}(T)}{g_{t,1}(T)}, v_i)$ mod f_t and then solves the univariate problem

  terrible computations !

- use interval/floating point arithmetic

  difficult to detect 0 !

Our proposal : RUR of $I' = < T_i - \mathrm{NF}(v_i, G_X), G_{<X} >$

- $\frac{\mathbb{Q}[T_1, ..., T_s, X_1, ..., X_n]}{\mathrm{I}}$ has the same monomial basis than $\frac{\mathbb{Q}[X_1, ..., X_n]}{G_{<X}}$

- RUR+$O(s\,D^2)$ operations $\Rightarrow v_i(\alpha) = \frac{g_{t,T_i}(t(\alpha))}{g_{t,1}(t(\alpha))}$

  $(g_{t,v_j}(T) = \sum_{i=0}^{d-1} Trace(m_{v_j t^i}) H_{d-i-1}(g_t)(T))$

Solving systems with parameters ???

$$\mathcal{E} = \{p_1, ..., p_r\}, \mathcal{F} = \{f_1, ..., f_l\}, \text{ with } p_i, f_i \in \mathbb{Q}[U, X]$$

$$U = U_1, ..., U_d \Rightarrow \textbf{parameters}$$

$$X = X_{d+1}, ..., X_n \Rightarrow \textbf{ indeterminates}$$

$$\mathcal{C} = \{x \in \mathbb{C}^n, p_1 = 0, ..., p_r = 0, f_1 \neq 0, ..., f_s \neq 0\}$$

$$\mathcal{S} = \{x \in \mathbb{R}^n, p_1 = 0, ..., p_r = 0, f_1 > 0, ..., f_s > 0\}$$

End users's queries

- Formal expression (rational parametrizations) ?
- Number of roots w.r.t. the parameters' values ?
- Topology ?

The cylindrical Algebraic Decomposition (Collins - 1975)

Given a set of polynomials (in $\mathbb{Q}[X_1, ..., X_n]$), the CAD computes a partition of the ambiant space ($\mathbb{R}^n$) into cells such that in cell, all the polynomials have a constant sign.

Recursive with respect to the variables.

The basic principle is to study the values of $[X_2, ..., X_n]$ where the number of real solutions of $f \in \mathbb{Q}[X_1, ..., X_n]$ varies.

CAD : the projection step (2)

For each polynomial : $f \in \mathcal{S}_1 \subset \mathbb{Q}[X_1][X_2, ..., X_n]$, find conditions over $[X_2, ..., X_n]$ such that the number of real roots may change :

the projection of points at infinity (zeroes of $\mathrm{LC}(f, X_1)$)

the critical values of the projection w.r.t. X_1 (discriminant of f w.r.t X_1)

For each couple $(f, g) \in \mathcal{S}_1 \subset \mathbb{Q}[X_1][X_2, ..., X_n]$ compute the projection of the intersection $\boldsymbol{V}(f) \cap \boldsymbol{V}(g)$: resultant(f, g) w.r.t. X_1.

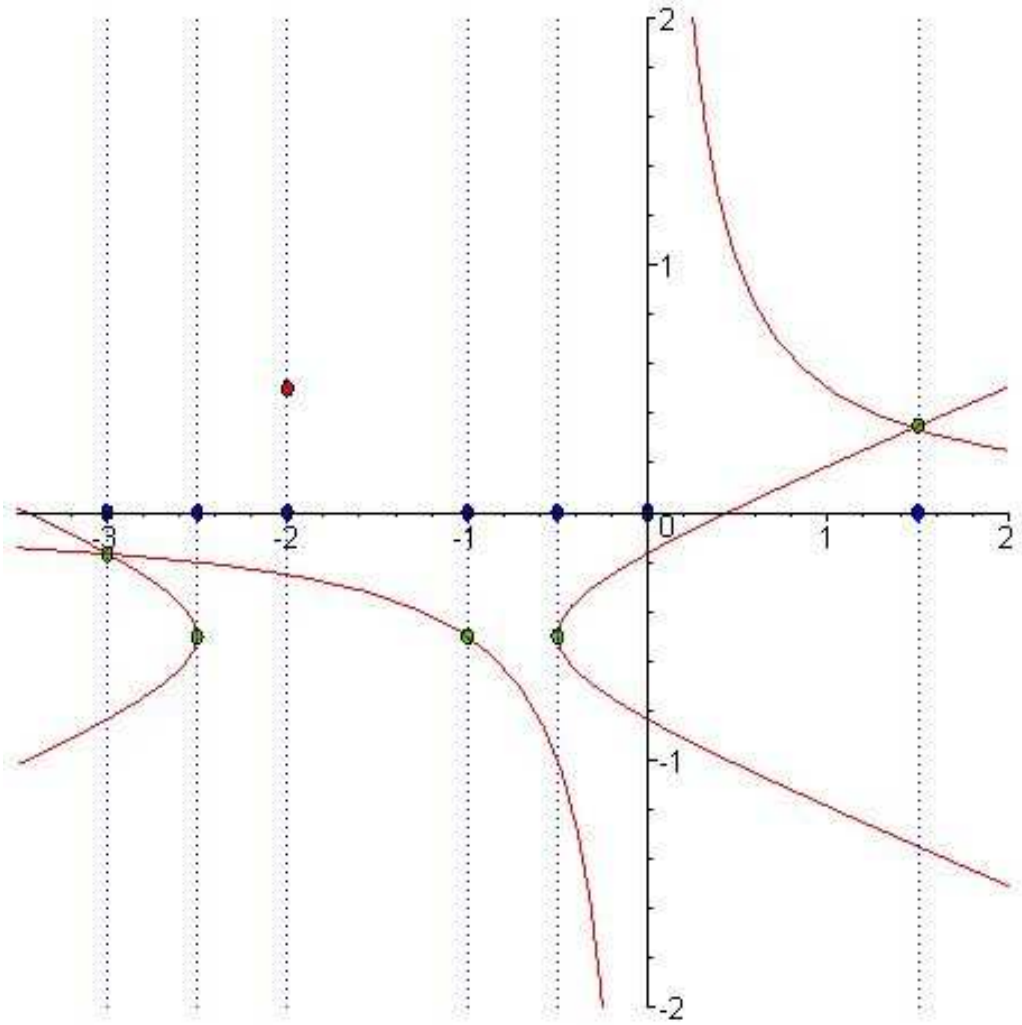
$\Rightarrow$ this generates a set $\mathcal{S}_2$ of polynomials in $\mathbb{Q}[X_2, ..., X_n]$

Then apply the same projection recursively to $\mathcal{S}_2, \mathcal{S}_3, ..., \mathcal{S}_{n-1}$.

At the end of the projection step, you have :

- $\mathcal{S}_i \subset \mathbb{Q}[X_i, ..., X_n]$ induces a partition of $\mathbb{R}^i$ if we consider $V(\mathcal{S}_i)$ and the union of cells (simply connected components) that do not meet any $V(f)$, $f \in \mathcal{S}_i$.
- Over each element of the above partition, the polynomials of S_{i-1} have a constant sign.

CAD : an example



CAD : the lifting step

Using the CAD, the cells are described recursively by the polynomials sets $\mathcal{S}_i$, and the CAD computes one point on each cell by the following process : by specializing the variables by the coordinates of the simple points, one then computes the sign condition described by the cell.

Start with $S_n \subset \mathbb{Q}[X_n]$: the cells of $\mathbb{R}$ "adapted" to $\mathcal{S}_{n-1}$ are the points of $\boldsymbol{V}(\mathcal{S}_n)$ and the intervals betwee them. We define the set of sample points as $\boldsymbol{V}(S_n)$ and one point in each interval.

For each sample point, we specialize the X_n coordinate of the polynomials of $\mathcal{S}_{n-1}$, and do the same : we then obtain sample points in $\mathbb{R}^2$.

Why not using directly CAD for our problem ?

- Projection step is double exponential in the number of variables.
- Lifting step need to work with algebraic numbers
- Computes to much information (do not take care of equalities)

In practice, for our problem, the CAD generates more than 500 000 cells

$\Rightarrow$ the output is not usable by the end-user.

Solving ???

Notation : $\Pi_U : \mathbb{C}^n \longrightarrow \mathbb{C}^d$ the canonical proj. on the parameters' space.

Mathematical answers :

- **Geometry (local)** : $\mathcal{U}$ s.t. $\Pi_U^{-1}(\mathcal{U}) \cap \mathcal{C}$ is an analytic covering of $\mathcal{U}$.
- **Algebra (global)** : I_W s.t. $\mathcal{U} \subset (\Pi_U(\mathcal{C}) \setminus \boldsymbol{V}(I_W))$ is an A.C. of $\mathcal{U}$.

Examples :

- CAD : I_W generated by the polynomials of the projection step;
- Comprehensive Gröbner based methods : specializations' defects;
- Rational parametrizations : projections' defects.

Remark : all these algorithms depend on arbitrary choices $\Rightarrow$ different I_W.

Define and compute a "minimal" $\boldsymbol{I_W}$, describe $\boldsymbol{\Pi_U(\mathcal{C}) \setminus V(I_W)}$

Discriminant Varieties

Definition 1. $\delta = \dim(\overline{\Pi_U(\mathcal{C})}), \phi_u : U \longrightarrow u$

An algebraic variety W is a discriminant variety of $\mathcal{C}$ w.r.t. Π_U iff:

- *W is contained in $\overline{\Pi_U(\mathcal{C})} = \overline{\Pi_U(\bar{\mathcal{C}})}$;*
- *$W = \overline{\Pi_U(\mathcal{C})}$ iff $\Phi_u(\mathcal{C})$ is infinite or empty for almost all $u \in \overline{\Pi_U(\mathcal{C})}$;*
- *The connected components $\mathcal{U}_1, ...\mathcal{U}_k$ of $\overline{\Pi_U(\mathcal{C})} \setminus W$ are analytic submanifolds of dimension δ (If $\overline{\Pi_U(\mathcal{C})}$ is connected, there is only one component).*
- *For $i = 1...k$, $(\Pi_U^{-1}(\mathcal{U}_i) \bigcap \mathcal{C}, \Pi_U)$ is an analytic covering of $\mathcal{U}_i$.*

The minimal discriminant variety

Notation : $W_D = W_{sc} \cup W_c \cup W_\infty \cup W_{\mathcal{F}} \cup W_{sing}$ with

- W_{sd} the Zariski closure of the projection of the irreducible components of $\overline{\mathcal{C}}$ of dimension less than δ;
- W_c the Zariski closure of the critical values of Π_U;
- $W_{\mathcal{F}}$ the Zariski closure of the projection of the intersection of $\overline{\mathcal{C}}$ with the zero set of $\prod_{i=1}^{s} f_i$;
- W_{sing} the singular locus of Π.
- W_∞ the set of points $u \in \Pi_U$ such that $\Pi_U^{-1}(\mathcal{U}) \cap \overline{\mathcal{C}}$ is not compact for any compact neighborhood $\mathcal{U}$ of u in Π;

Thm (Lazard/Rouillier 2004): W_D is **the** smallest discriminant variety associated to $\mathcal{C}$ w.r.t. Π_U.

Using Discriminant Varieties

The "real" version of the minimal discriminant variety should be a semi-algebraic set.

Over each connected component of $\Pi_U(\mathcal{S}) \setminus (W_D \cap \mathbb{R}^d)$:

- the number of real roots is locally constant;
- the sheets are locally diffeomorphic to the comp.

For using the discriminant variety, one can

- Compute one point on each C.C. + solving a zero-dimensional system : qualitative information
- Compute a "partial" CAD adapted to the polynomials defining the discriminant variety : full information

"Straightforward" Computations

Notation:

- $<_U$ (resp. $<_X$) : a DRL ordering w.r.t. to U (resp. X);
- $<_{U,X}$ (block) elimination ordering s.t. $U_i <_{U,X} X_j$, $\forall U_i \in U, \forall X_j \in X$;
- G a Gröbner basis w.r.t. $<_{U,X}$.

Basic Tools :

- $G \cap \mathbb{Q}[U]$ is a Gröbner basis of $< G > \cap \mathbb{Q}[U]$ w.r.t. U

  $\rightarrow$ deduce I_U s.t. $\boldsymbol{V}(I_U) = \overline{\Pi_U(\mathcal{C})}$

- δ can efficiently be computed from G
- $(I + < Tf - 1 >) \cap \mathbb{Q}[U, X] = I\colon f^\infty$ and $\boldsymbol{V}(I\colon f^\infty) = \overline{\boldsymbol{V}(I) \setminus \boldsymbol{V}(f)}$

  $\rightarrow$ compute $I_{\mathcal{F}}$ s.t. $\boldsymbol{V}(I_{\mathcal{F}}) = W_{\mathcal{F}}$

W_∞

Theorem 2. ***(Lazard/Rouillier 2004-2005)***

Let G be a reduced Gröbner basis w.r.t. $<_{U,X}$ of any ideal I such that $\boldsymbol{V}(I) = \bar{\mathcal{C}}$.

We define $\mathcal{E}_i^\infty = \{L\, C_{<_X}(g) \quad | \quad g \in G \quad , \quad \exists m \geq 0, \quad L\, M_{<_X}(g) = X_i^m\}$, and $\mathcal{E}_0 = G \bigcap \mathbb{Q}[U]$. Then:

- *$\mathcal{E}_0$ is a Gröbner basis of $I \bigcap \mathbb{Q}[U]$ w.r.t. $<_U$ and $\mathcal{E}_0 \subset \mathcal{E}_i^\infty$ for $i = d+1 \ldots n$;*
- *$\mathcal{E}_i^\infty$ is a Gröbner basis of some ideal $I_i^\infty \subset \mathbb{Q}[U]$ w.r.t. $<_U$;*
- $W_\infty = \bigcup_{i=d+1}^{n} \boldsymbol{V}(I_i^\infty)$.

Nothing to compute when G is known !

c, sing, sd

The main computational problems :

- Jacobian criteria are independant from the equations in the case of a radical and equi-dimensional ideals. In such cases $W_c = \boldsymbol{V}(I + \mathrm{Jac}_X^{n-\delta}(\mathcal{E}))$ and $W_{\mathrm{sing}} = \boldsymbol{V}(I \cap \mathbb{Q}[U] + \mathrm{Jac}_U^{d-\delta}(I \cap \mathbb{Q}[U]))$.

- In the general case, the jacobian criteria

  $\rightarrow$ may give too much points (non radical ideals, embeeded components)

  $\rightarrow$ may give varieties of dimension δ (non radical ideals)

- We want to avoid as most as possible to compute a decomposition of the ideal into radical and/or equi-dimensional components (avoid also primary decompositions)

Usual situations

- **(1)** $r = \sharp\mathcal{E} = n - \delta$ and **(2)** $< \phi_u(I) >$ is radical for almost all $u \in \Pi_U(\mathcal{C})$

  $\rightarrow$ in applications, specializations of the system are often solvable using basic numerical methods (Newton);

- **(3)** $\overline{\Pi_U(\mathcal{C})} = \mathbb{C}^d$

  $\rightarrow$ taking parameters' values in a Zariski closed strict subset of $\mathbb{C}^d$ does not make sence in many applications.

One can not suppose a priori and even in practice, that $I(\overline{\mathcal{C}})$ is radical or equidimensional or both.

$\rightarrow$ artefacts from modelizations (from rational fractions to polynomials, changes of coordinates like $t = \tan(\alpha/2)$, etc.) often introduce primary but not prime components of arbitrary dimensions.

If I is any ideal such that $\boldsymbol{V}(I) = \overline{\mathcal{C}}$,

(2) $\Rightarrow$ primary comp. Q of I s.t. $\dim(Q) = \dim(Q \cap \mathbb{Q}[U]) = \delta$ are prime.

If $\dim(\boldsymbol{V}(I)) = \delta$, **(1)** $\Rightarrow \boldsymbol{V}(I)$ is equi-dimensional but $\not\Rightarrow I$ is equi-dimensional.

Tricks for usual situations

The condition (1) ($r = \sharp\mathcal{E} = n - \delta$) is easy to detect.

The condition (3) ($\overline{\Pi_U(\mathcal{C})} = \mathbb{C}^d$) can be checked (Gröbner basis for $<_{U,X}$)

Remark : (3) $\Rightarrow W_{\text{sing}} = \emptyset$.

One can "guess" the condition (2) ($< \phi_u(I) >$ is radical for almost all $u \in \Pi_U(\mathcal{C})$), by specializing the system using an arbitrary $(u_1, ..., u_d) \in \Pi_U(\mathcal{C})$.

- if $u \notin W_D$, (2) is fulfilled iff $\phi_u(\mathcal{C})$ is zero-dimensional and radical
- $\dim((I + \text{Jac}_X^{n-\delta}(\mathcal{E}) \cap \mathbb{Q}[U]) < \delta \Rightarrow$ (2) is fulfilled

Proposition (Lazard/Rouillier 2004): Suppose **(1) and (2)**

- if Q is an embeeded component of I, then $\boldsymbol{V}(Q) \subset W_\infty$.
- $\boldsymbol{V}(I + \text{Jac}_X^{n-\delta}(\mathcal{E})) \cup W_\infty = W_c \cup W_\infty$

Back to our application

There exists a full general algorithm for computing discriminant varieties, but in ourcase, we are in a "usual" situation (can be automatically detected).

We only have to compute :

- $W_D = W_\infty \cup W_c$

Since :

- $\overline{\Pi_U(\mathcal{C})} = \mathbb{C}^d$ (detected on the Gröbner basis)
- $\mathcal{E} = n - d$ (detected counting the equations)
- $\mathcal{F} \subset \mathbb{Q}[U_1, ..., U_d]$ (detected reading the equations)
- $< \mathcal{E} > = \sqrt{< \mathcal{E} >}$ (detected when computing W_c)

$W_\infty \cup W_c$ induces an optimal partition of the parameter's space

About the discriminant variety

The discriminant variety is an optimal object (at least in the complex case);

It can efficiently be computed with an adaptative algorithm;

There exists a Maple implementation (G. Moroz) using Gb (Faugère) RS (Rouillier) RAGlib (Safey El Din);

It can replace the polynomials computed by a partial CAD after $n - \delta$ projection steps.

Work in progress :

- precise complexity : we know from Grigoriev an Vorobjov (ISSAC 2001) that the algorithm is single exponential;
- lasy decompositions for the general case. We currently test the capabilities of the RAGlib (M. Safey El Din);
- recursive use to describe all the solutions;
- computation of the cell decomposition of a semi-algebraic set ($\neq$ cell decomposition of $\mathbb{R}^n$ adapted to a set of polynomials).

Using the discriminant variety

Over each connected component of $\Pi_U(\mathcal{S}) \setminus (W_D \cap \mathbb{R}^d)$:

- the number of real roots is locally constant;
- the sheets are locally diffeomorphic to the conn. comp.

For using the discriminant variety, one can

- Compute one point on each C.C. + solving a zero-dimensional system : qualitative information
- Compute a "partial" CAD adapted to the polynomials defining the discriminant variety : full information

Partial CAD : computes only the cells of higher dimension (do not describe the solutions over W_D in our case).

Does not make sence in practice to study the solutions over an algebraic set : in our case the parameters are design parameters, one can not construct a robot whose parameters verify an algebraic relation (manufacture errors ...).

Algorithm : remove all the computations with algebraic numbers !

The final computation

We started with a system $\mathcal{S}$ in $\mathbb{Q}[U_1, ..., U_d][X_{d+1}, ..., X_n]$;

We computed $W_d \subset \mathbb{C}^d$ (defined by polynomials in $\mathbb{Q}[U_1, ..., U_d]$;

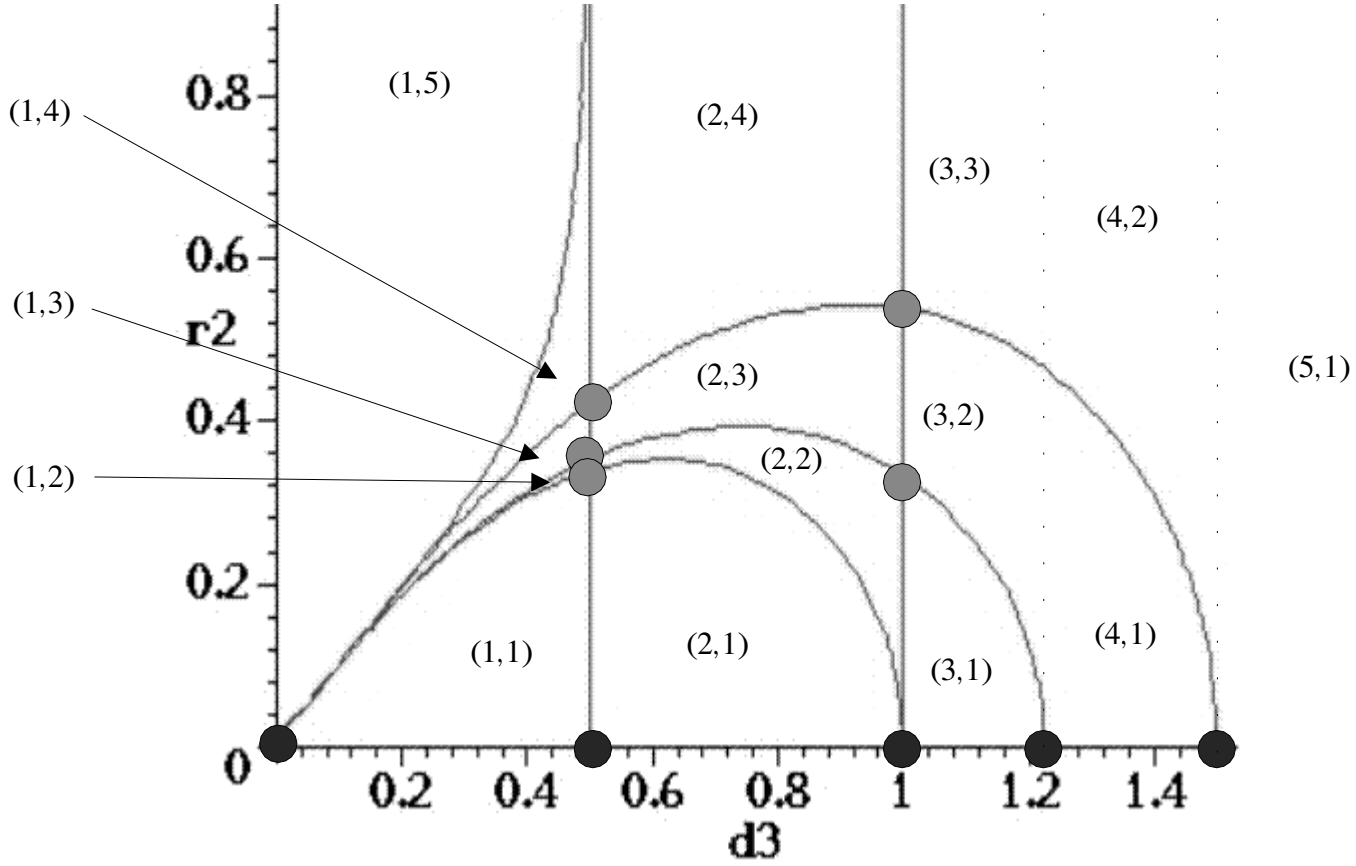
We described all the cells of maximal dimension of $\mathbb{C}^d \setminus W_D$;

We now want to characterize all the possible solutions : given a cell in $\mathbb{C}^d \setminus W_D$ (a sample point $(u_1, ..., u_d)$), how much solutions has the system over the cell : substitute U_i by $u_i, i = 1...d$ in the system and solve it.

We know, by definition of W_D than $\mathcal{S}_{U_i=u_i, i=1...d}$ has a finite number of complex solutions.

The full classification

After the first partial CAD projection step, we got :



The full classification

Solving the zero-dimensional systems over the cells of dimension 3, we obtain :

$(d_3, r_2) \setminus d_4$	1	2	3	4	5	6	7
(1,1)	0	0	4	4	2	0	0
(1,2)	0	4	4	4	2	0	0
(1,3)	0	4	4	4	2	0	0
(1,4)	0	4	4	2	2	0	0
(1,5)	0	4	4	2	0	0	0
(2,1)	0	0	4	4	2	2	0
(2,2)	0	4	4	4	2	2	0
(2,3)	0	4	4	4	2	2	0
(2,4)	0	4	4	2	2	2	0
(3,1)	0	4	4	4	2	2	4
(3,2)	0	4	4	4	2	2	4
(3,3)	0	4	4	2	2	2	4
(4,1)	0	4	4	4	2	2	4
(4,2)	0	4	4	2	2	2	4
(5,1)	0	4	4	2	2	2	4