Théorème des zéros et preuves en Coq

Loïc Pottier
Projet Marelle
INRIA Sophia Antipolis

Bases de Gröbner

- Polynômes à plusieurs indéterminées: $R[X_1,\ldots,X_s]$
- Ordre total sur les monômes (degré, lexico,…):
  x^3 > x^2*y > x*y^2 > y^3 > x^2 > x*y > y^2 > x > y > 1
- Division par X^a-R: remplacer partout où X^a par R:
  x^2*y divisé par x^2+1 donne –y
  mais divisé par x*y-1 donne x
- Base de Gröbner = famille de polynômes telle que les restes des divisions par cette famille sont uniques.
- {x^2+1, x*y-1} n'est pas une base de Gröbner

Algorithme de Buchberger

- Complétion: ajouter de nouveaux polynômes (S-polynômes) et les diviser.

- Ex: y*(x^2+1) – x*(x*y-1)

  = x+y

  puis x^2+1 – x*(x+y)

  = -x*y+1 qui se divise et donne le reste y^2+1

- {x^2+1,x*y-1,x+y,y^2+1} est une base de Gröbner.

Digression: bases de Gröbner et triangulation de Delaunay.

4.2 Delaunay triangulation

A triangulation of the set of points $a_1, ..., a_n$ of $\mathbb{Z}^d$ is said "regular" iff there exists a vector w of $\mathbb{R}^n$ such that this triangulation is obtained as the projection of the lower convex envelop of the points $(a_1, w_1), ..., (a_n, w_n)$ of $\mathbb{R}^{d+1}$.
A theorem of Sturmfels [10] gives relations between regular triangulations of $a_1, ..., a_n$ and the Gröbner bases of the toric ideal I.
Suppose that the points $a_1, ..., a_n$ are in an affine hyperplane and generate $\mathbb{Z}^d$. Let Δ_w be the triangulation defined by $w \in \mathbb{R}^n$. Let I_Δ be the ideal generated by the monomials $X_{\sigma_1}...X_{\sigma_p}$ where $\{\sigma_1, ..., \sigma_p\}$ is not a face of Δ_w (the Stanley-Reisner ideal of Δ_w) .

Theorem 7 ([10]) *I_Δ is the radical of $in_w(I)$*

The Delaunay triangulation is regular, as obtained with the vector $(||a_1||^2, ..., ||a_n||^2)$. Then, a consequence of the theorem is:

Corollary 1 *Let $w = (||a_1||^2, ..., ||a_n||^2)$, then a Gröbner basis of I for $<_w$ gives the Delaunay triangulation of $a_1, ..., a_n$.*

Théorème
(Pottier 92 via un théorème de Sturmfels):

Étant donnés des points $a_1,\ldots,a_n$ de $\mathbb{N}^m$,
dans un même hyperplan,
G une base de Gröbner de l'idéal

$$(X^{a_1}-Y_1,\ldots,X^{a_n}-Y_n,\ TX_1\ldots X_mY_1\ldots Y_n-1)$$

pour l'ordre où Y_i a le poids $||a_i||^2$ et $X>Y$,
Alors *les monômes initiaux de G (et leurs multiples) forment les non-faces de la triangulation de Delaunay de* $a_1,\ldots,a_n$

Malheureusement, ça rame trop ☹...

The complexity of this computation depends directly from the degree of the Gröbner basis, bounded by $(1+na)^d$ where a is the maximum coordinate of the a_is. We cannot *a priori* compete with specialized algorithms for Delaunay triangulation (which have however a theoretical complexity of the same order), but we can expect to interpret them in the context of polynomials.

Example:

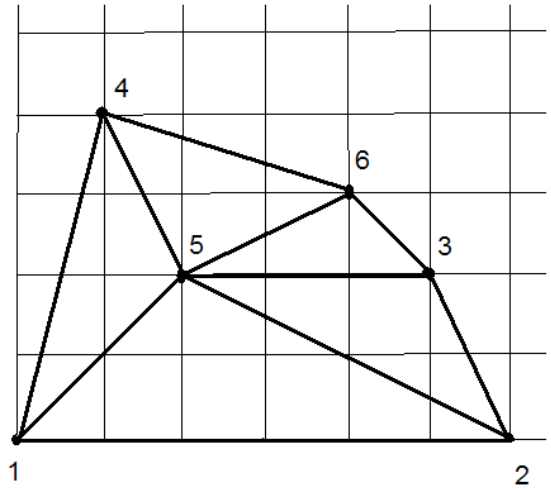
Let $a_1 = (0,0,1), a_2 = (6,0,1), a_3 = (5,2,1), a_4 = (1,4,1), a_5 = (2,2,1), a_6 = (4,3,1)$ in the plane identified to $\{z = 1\}$ in $\mathbb{R}^3$.

Computations with softwares Macaulay [1] or bastat [9], give a Gröbner basis for I with initial monomials

$\{X_1^2X_6^6, X_1X_2X_6^6, X_1X_3^2, X_1X_3X_4, X_2^2X_6^6, X_3^6X_4^2, X_2X_4, X_3^5X_4^3, X_3^4X_4^2X_5\}$

and then $I_\Delta = (X_1X_6, X_1X_3, X_2X_6, X_3X_4, X_2X_4)$,

the Delaunay triangulation is $\Delta = \{\{1,2,5\},\{1,4,5\},\{2,3,5\},\{3,5,6\},\{4,5,6\}\}$.



Egalités polynomiales

But: prouver automatiquement en coq des buts de la forme

$P_1=0$

...

$P_n=0$

==========

$P=0$

Où $P_1,\ldots,P_n,P$ sont des polynômes à plusieurs indéterminées

Exemple

x:R
y:R
H: x^2+1=0

H0: x*y-1=0

==========

x+y=0

Remarque: x+y = y*(x^2+1) -x*(x*y-1)

Théorème des zéros de Hilbert (Nullstellensatz)

Soient $P_1,\ldots,P_n$,P des polynômes de $C[X_1,\ldots,X_s]$

alors

$P_1=0,\ldots,P_n=0 \Rightarrow P=0$

<=>

il existe $r,Q_1,\ldots,Q_n$ tels que

$P^r = Q_1*P_1+\ldots+Q_nP_n$

(autrement dit P^r est dans l'idéal engendré par P_1, $\ldots,P_n$)

Comment calculer $r,Q_1,\ldots,Q_n$?

Une possibilité: bases de Gröbner.

Calcul du théorème des zéros

On construit pas à pas la base de Gröbner en calculant le reste de la division de P à chaque nouveau polynôme ajouté dans la base.

S'il est nul, on a presque gagné:

$P = Q'_1 * P_1 + \ldots + Q'_n P_n + Q_{n+1} * P_{n+1} + \ldots + Q_{n+m} P_{n+m}$

Mais $P_{n+1},\ldots,P_{n+m}$ s'expriment en fonction de $P_1,\ldots,P_n$

D'où $P = Q_1 * P_1 + \ldots + Q_n P_n$

Sinon, on essaie avec P^2, P^3, etc

En Coq

- Procédure externe (ocaml) pour calculer les $Q_1,\ldots,Q_n$
- Vérification de $P= Q_1*P_1+\ldots+Q_nP_n$ par la tactique Ring.
- Bien plus rapide que de calculer une base de Gröbner complète avec un outil externe (F4, FGB)

Exemple: géométrie

I milieu de CD