Algebraic Approaches for Constraint Solving

Yosuke Sato
Tokyo University of Science

Today's talk

Algebraic tools for exact(symbolic) solutions of various constraints

(1) Gröbner bases in polynomial rings

- over complex numbers(algebraically closed fields)
- over sets(boolean rings,Von Neumann regular rings)

(2) More advanced tools

- Quantifier Eliminations
- Parametric Gröbner bases

Contents of the talk

(1) Polynomial ideals and Gröbner bases

- breaf introduction -

(2) Applications of Gröbner bases in constraint solving

・ complex numbers and real numbers

・ set constraints

(3) Polynomial constraints over real numbers

・ Quantifier eliminations(QE) - breaf review -

・ CAD(Cylindrical Algebraic Decomposition)

(4) Polynomial constraints with parameters

・ CGB(Comprehensive Gröbner Bases)

(5) Available Softwares

Polynomial ideals and Gröbner bases

$K[\bar{X}]$: a polynomial ring over a field K with variables

$$\bar{X} = X_1, \ldots, X_n$$

$I = \{h_1(\bar{X})(f_1(\bar{X}) + \cdots + h_k(\bar{X}) f_k(\bar{X}) | h_i(\bar{X}) \in K[\bar{X}]\}$:

I is called a polynomial ideal generated by polynomials $f_1(\bar{X}), \ldots, f_k(\bar{X})$.

I is denoted by $Id(f_1(\bar{X}), \ldots, f_k(\bar{X}))$.

$\{f_1(\bar{X}), \ldots, f_k(\bar{X})\}$ is called a basis of I.

Important fact

If $Id(f_1(\bar{X}), \ldots, f_k(\bar{X})) = Id(g_1(\bar{X}), \ldots, g_l(\bar{X}))$, the systems of equations:

$$\begin{cases} f_1(\bar{X}) & = 0 \\ & \vdots \\ f_k(\bar{X}) & = 0 \end{cases} \qquad \begin{cases} g_1(\bar{X}) & = 0 \\ & \vdots \\ g_l(\bar{X}) & = 0 \end{cases}$$

have the same solutions.

Example.

$$f_1(s,x,y,z) = 3*x^2 + 2*y*z - 2*x*s$$
$$f_2(s,x,y,z) = x*z - y*s$$
$$f_3(s,x,y,z) = x*y - z - z*s$$
$$f_4(s,x,y,z) = x^2 + y^2 + z^2 - 1$$

$$g_1(s,x,y,z) = s - \frac{3}{2}*x - \frac{3}{2}*y*z - \frac{167616}{3835}*z^6 + \frac{36717}{590}*z^4 - \frac{134419}{7670}*z^2$$
$$g_2(s,x,y,z) = x^2 + y^2 + z^2 - 1$$
$$g_3(s,x,y,z) = x*y - \frac{19584}{3835}*z^5 + \frac{1999}{295}*z^3 - \frac{6403}{3835}*z$$
$$g_4(s,x,y,z) = x*z + y*z^2 - \frac{1152}{3835}*z^5 - \frac{108}{295}*z^3 + \frac{2556}{3835}*z$$
$$g_5(s,x,y,z) = y^3 + y*z^2 - y - \frac{9216}{3835}*z^5 + \frac{906}{295}*z^3 - \frac{2562}{3835}*z$$
$$g_6(s,x,y,z) = y^2*z - \frac{6912}{3835}*z^5 + \frac{827}{295}*z^3 - \frac{3839}{3835}*z$$
$$g_7(s,x,y,z) = y*z^3 - y*z - \frac{576}{59}*z^6 + \frac{1605}{118}*z^4 - \frac{453}{118}*z^2$$
$$g_8(s,x,y,z) = z^7 - \frac{1763}{1152}*z^5 + \frac{655}{1152}*z^3 - \frac{11}{288}*z$$

$$Id(f_1, f_2, f_3, f_4) = Id(g_1, g_2, g_3, g_4, g_5, g_6 \cdot g_7, g_8)$$

Gröbner bases

A Gröbner basis of an ideal I is a basis of I which has nice properties.

One of the most important properties

Let G be a Gröbner basis of an ideal I in a polynomial ring $K[\bar{X},\bar{Y}]$ with variable $\bar{X} = X_1,\ldots,X_m$ and $\bar{Y} = Y_1,\ldots,Y_n$ with a term order such that $\bar{X} >> \bar{Y}$. Then $G \cap K[\bar{Y}]$ becomes a Gröbner basis of the ideal $I \cap K[\bar{Y}]$ in $K[\bar{Y}]$.

Example.

$$f_1(s,x,y,z) = 3*x^2+2*y*z-2*x*s$$
$$f_2(s,x,y,z) = x*z-y*s$$
$$f_3(s,x,y,z) = x*y-z-z*s$$
$$f_4(s,x,y,z) = x^2+y^2+z^2-1$$

$$g_1(s,x,y,z) = s-\frac{3}{2}*x-\frac{3}{2}*y*z-\frac{167616}{3835}*z^6 +\frac{36717}{590}*z^4-\frac{134419}{7670}*z^2$$
$$g_2(s,x,y,z) = x^2+y^2+z^2-1$$
$$g_3(s,x,y,z) = x*y-\frac{19584}{3835}*z^5+\frac{1999}{295}*z^3-\frac{6403}{3835}*z$$
$$g_4(s,x,y,z) = x*z+y*z^2-\frac{1152}{3835}*z^5-\frac{108}{295}*z^3+\frac{2556}{3835}*z$$
$$g_5(s,x,y,z) = y^3+y*z^2-y-\frac{9216}{3835}*z^5+\frac{906}{295}*z^3-\frac{2562}{3835}*z$$
$$g_6(s,x,y,z) = y^2*z-\frac{6912}{3835}*z^5+\frac{827}{295}*z^3-\frac{3839}{3835}*z$$
$$g_7(s,x,y,z) = y*z^3-y*z-\frac{576}{59}*z^6+\frac{1605}{118}*z^4-\frac{453}{118}*z^2$$
$$g_8(s,x,y,z) = z^7-\frac{1763}{1152}*z^5+\frac{655}{1152}*z^3-\frac{11}{288}*z$$

$$Id(f_1,f_2,f_3,f_4) = Id(g_1,g_2,g_3,g_4,g_5,g_6{\cdot}g_7,g_8)$$

$\{g_1,g_2,g_3,g_4,g_5,g_6,g_7,g_8\}$ is a Gröbner basis of $Id(f_1,f_2,f_3,f_4)$ with a term order $s>x>y>z$

Applications of Gröbner bases in constraint solving

1. Systems of polynomial equations over real numbers and complex numbers.

<u>Case 1</u>: The system of polynomial equations has only finite number of solutions over complex numbers.

We can solve it using Gröbner bases as the previous example for both of real numbers and complex numbers.

<u>Key fact</u>(Extension Theorem)
Let I be a polynomial ideal in a polynomial ring $K[\bar{X}, \bar{Y}]$ over an algebraically closed field K such that $I \cap K[\bar{Y}]$ is 0-dimensional. Let $\bar{a}$ be a solution of $I \cap K[\bar{Y}]$, i.e. $f(\bar{a}) = 0$ for any polynomial $f(\bar{Y}) \in I \cap K[\bar{Y}]$. Then we can extend $\bar{a}$ to a whole solution of I, i.e. there exists $\bar{b}$ such that $f(\bar{b}, \bar{a}) = 0$ for any polynomial $f(\bar{X}, \bar{Y})$ $\in I$.

Case 2: The system of polynomial equations has infinitely many solutions over complex numbers.

Extension Theorem does not hold.

We need further sophisticated tools.

(1) When we are interested in solutions over real numbers, we need **Quantifier Elimination**.

(2) When we are interested in solutions over complex numbers, we need **Comprehensive Gröbner bases**.

2. Constraints over Sets and Elements

Important fact 1(Boolean Ring)

Let S be a class of sets.
Define the addition $+$ and the multiplication $\cdot$ by

$$a + b = (a \cap \tilde{}\, b) \cup (\tilde{}\, a \cap b)$$
$$a \cdot b = a \cap b$$

($\tilde{}\, x$ denotes the complement of x.)

Then S becomes a commutative ring with identity $1 =$ 'the whole set' and $0 =$ 'the empty set'. S is called a boolean ring of sets.

Important fact 2(Boolean Gröbner Bases)

We can construct Gröbner bases in polynomial rings over boolean rings.

Important facts 3(Extension Theorem)

We can always exdend partial solutions to whole solutions.

These facts enable us to have **Set Constraint Solver** bases on boolean Gröbner bases.

Computation example

unknown 24 set variables:

$a, b, c, d, j, ja, jo, k, kl, kh, ko, we, ma, ol, md, yn, n1, n2, n3, n4, n5, n6, n7, n8$

unknown 18 element variables:

$x1, x2, x3, x4, x5, x6, x7, x8, x9, x10, y1, y2, y3, y4, y5, y6, y7, y8$

Our solver compute a boolean Gröbner basis in the polynomial ring

$$S[a, b, c, d, j, ja, jo, k, kl, kh, ko, we, ma, ol, md, yn, n1, n2, n3, n4, n5, n6, n7, n8, x1, x2, x3, x4, x5, x6, x7, x8, x9, x10, y1, y2, y3, y4, y5, y6, y7, y8].$$

Quantifier eliminations(QE)

Example 1.
$\exists X(X^2 + A * X + B = 0) \iff A^2 - 4 * B \geq 0$

Example 2.
Solve the equation
$(3 * X + 4 * Y - 1)^2 + (2 * X - 7 * Y - 5)^2 = 0.$
We can not apply Gröbner bases computation for such problems.
QE can handle such problems.
$\exists X((3 * X + 4 * Y - 1)^2 + (2 * X - 7 * y - 5)^2 = 0)$

Example 3.

Compute the envelope of the family of circles $\{(x-t)^2+(y-t^2)^2-4|t \in \mathbf{R}\}$.

$$\begin{aligned} F &= (x-t)^2+(y-t^2)^2-4 \\ \frac{\partial}{\partial t}F &= -2*(x-t)-4*t*(y-t^2) \end{aligned}$$

The envelope consists of all points (x,y) such that there exists a real number t such that $F = \frac{\partial}{\partial t}F = 0$

Comprehensive Gröbner Bases(CGB)

Example

$$\begin{cases} a * x + y^2 - 1 &= 0 \\ y^3 - 1 &= 0 \end{cases}$$

$Id(a * x + y^2 - 1, y^3 - 1)$ is not 0-dimentional.
$(Id(a * x + y^2 - 1, y^3 - 1) \cap \mathbf{C}[a] = \{0\}.)$
In this example a can be considered as a parameter.
We can not use a standard Gröbner basis computation.

Definition
Let $F = \{f_1(\bar{A}, \bar{X}), \ldots, f_k(\bar{A}, \bar{X})\}$ be a set of polynomials in $K[\bar{A}, \bar{X}]$.
A set $G = \{g_1(\bar{A}, \bar{X}), \ldots, g_l(\bar{A}, \bar{X})\}$ of polynomials in $K[\bar{A}, \bar{X}]$ is called a comprehensive Gröbner basis of F if $\{g_1(\bar{a}, \bar{X}), \ldots, g_l(\bar{a}, \bar{X})\}$ becomes a Gröbner basis of $Id(f_1(\bar{a}, \bar{X}), \ldots, f_k(\bar{a}, \bar{X}))$ for any elements $\bar{a}$ of K.

Widely used Softwares

Gröbner bases

- RISA/ASIR
  http://www.arir.org
- Singular
  http://www.singular.uni-kl.de

Quantifier Elimination

- QEPCAD
  (Quantifier Elimination by Partial Cylindrical Algebraic Decomposition)
  http://www.cs.usna.edu/ qepcad/B/QEPCAD.html
- Mathematica(after version 5.0)
- Redlog in Reduce

Comprehensive Gröbner bases

- CGB in Reduce