Solving Systems of Polynomial Equations with Symmetries Using SAGBI-Gröbner Bases

Jean-Charles Faugère
Sajjad Rahmany

SALSA Research Team

Issac 2009

Problem

Solving by **exact method** the polynomial system:

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \vdots \\ f_m(x_1, \ldots, x_n) = 0 \end{cases} \quad \text{with } f_i \in R = \mathbb{K}[x_1, \ldots, x_n]$$

Problem

Solving by **exact method** the polynomial system:

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \vdots \\ f_m(x_1, \ldots, x_n) = 0 \end{cases} \quad \text{with } f_i \in R = \mathbb{K}[x_1, \ldots, x_n]$$

NP-hard even when $\mathbb{K} = \mathbb{K}_2$

☞ Try to identify families of systems which are easier to solve:

Problem

Solving by **exact method** the polynomial system:

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \vdots \\ f_m(x_1, \ldots, x_n) = 0 \end{cases} \quad \text{with } f_i \in R = \mathbb{K}[x_1, \ldots, x_n]$$

☞ Try to identify families of systems which are easier to solve:

- Sparse/Structured systems
- Systems s.t. the set of solutions is left invariant by the action of a finite group.

Problem

Solving by **exact method** the polynomial system:

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \vdots \\ f_m(x_1, \ldots, x_n) = 0 \end{cases} \quad \text{with } f_i \in R = \mathbb{K}[x_1, \ldots, x_n]$$

☞ Try to identify families of systems which are easier to solve:

In this talk: sub problem of the previous case

- f_i is invariant by the action of a finite subgroup G of $\mathfrak{S}_n$.

Cyclic n

Well known benchmark is the cyclic n problem.

G. Björk.
Functions of modulus 1 on $\mathbf{Z}_n$, whose Fourier transforms have constant modulus, and "cyclic n-roots".
In J.S. Byrnes and J.F. Byrnes, editor, *Recent Advances in Fourier Analysis and its Applications*, volume 315 of *Ser. C: Math. Phys. Sci., Kluwer*, pages 131–140. NATO Adv. Sci. Inst., 1989.

Example (Cyclic 5)

Consider the cyclic 5 problem:

$$\begin{cases} f_1 = x_1 + x_2 + x_3 + x_4 + x_5 \\ f_2 = x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1 \\ f_3 = x_1x_2x_3 + x_2x_3x_4 + x_3x_4x_5 + x_4x_5x_1 + x_5x_1x_2 \\ f_4 = x_1x_2x_3x_4 + x_2x_3x_4x_5 + x_3x_4x_5x_1 + x_4x_5x_1x_2 + x_5x_1x_2x_3 \\ f_5 = x_1x_2x_3x_4x_5 - 1 \end{cases}$$

Gröbner bases destroy the symmetries

Computations: Gröbner basis, Triangular sets, . . .

Destroy the symmetries of the system instead of using them !

Gröbner bases destroy the symmetries

Computations: Gröbner basis, Triangular sets, ...

Destroy the symmetries of the system instead of using them !

Example (Cyclic 5)

A lexicographic Gröbner basis of the ideal generated by the cyclic 5 problem contains the univariate polynomial:

$$h(x_1) = x_1^{15} + 122x_1^{10} - 122x_1^5 - 1$$

which is *not invariant* by the cyclic group.

Related Works

Computing the Gröbner basis in invariants rings:

☞ Using the primary and secondary invariants to reformulate the problem.

B.Sturmfels.
Algorithms in Invariant Theory.
Springer-Verlag, Wien,New York, 1993.

A.Colin.
Solving a system of algebraic equations with symmetries.
Pure and applied algebra, 117-118:195–215, 1997.

Related Works

Computing the Gröbner basis in invariants rings:

☞ Using the primary and secondary invariants to reformulate the problem.

- B.Sturmfels.
- A.Colin.

Difficult to compute the **generating set** of invariants rings !

Example (Cyclic *n*)

Group	cardinality of the generating set	CPU
cyclic 7	48	1.3 s
cyclic 8	65	1478 s

Cardinality and CPU time of generating sets of the invariant rings (Magma 2-14)

Related Works

☞ Using the primary and secondary invariants to reformulate the problem.

The resulting system is very often **much difficult** to solve than the original system !

Example (Cyclic n)

Resulting system cyclic 5 problem: 17 equations and 17 variables.

Experimental Fact:

Untractable when $n > 6$.

Reynolds operator

$R = \mathbb{K}[x_1, \ldots, x_n]$ and R^G is the ring of invariant polynomials.

Definition

Let G be a finite group. The Reynolds operator of G is the map $\Re : R \longrightarrow R^G$ defined by the formula

$$\overline{\Re}(f) = \sum_{A \in G} f(A.X) \quad \text{and} \quad \Re(f) = \frac{\overline{\Re}(f)}{\mid G \mid}.$$

Reynolds operator

$R = \mathbb{K}[x_1, \ldots, x_n]$ and R^G is the ring of invariant polynomials.

Definition

Let G be a finite group. The Reynolds operator of G is the map $\Re : R \longrightarrow R^G$ defined by the formula

$$\overline{\Re}(f) = \sum_{A \in G} f(A.X) \quad \text{and} \quad \Re(f) = \frac{\overline{\Re}(f)}{\mid G \mid}.$$

Proposition

Let $\Re$ be the Reynolds operator of the finite matrix group G.

(a) *$\Re$ is $\mathbb{K}$-linear in f : $\Re(cf + g) = c\Re(f) + \Re(g)$*

(b) *If $f \in R$, then $\Re(f) \in R^G$.*

(c) *If $f \in R^G$, then $\Re(f) = f$.*

Reynolds operator

$R = \mathbb{K}[x_1, \ldots, x_n]$ and R^G is the ring of invariant polynomials.

Definition

Let G be a finite group. The Reynolds operator of G is the map $\Re : R \longrightarrow R^G$ defined by the formula

$$\overline{\Re}(f) = \sum_{A \in G} f(A.X) \quad \text{and} \quad \Re(f) = \frac{\overline{\Re}(f)}{\mid G \mid}.$$

Lemma

We fix $<$ a monomial ordering.
Every $f \in R^G$ can be written uniquely as $f = \sum_\alpha c_\alpha \Re(t_\alpha)$, where $c_\alpha \in \mathbb{K}$ and $t_\alpha \in LT_<(R^G)$.

Reynolds operator

Example (Cyclic n)

Let G be the cyclic group generated by $\{(1,2,3,4,5)\}$. Consider $f = x_1x_2x_3+x_2x_3x_4+x_3x_4x_5+x_4x_5x_1+x_5x_1x_2+3x_1+3x_2+3x_3+3x_4+3x_5$ wrt lex order $x_1 > x_2 > x_3 > x_4 > x_5$.

$$f = \Re(f) = \overline{\Re}(x_1x_2x_3) + 3\,\overline{\Re}(x_1)$$

Very compact representation !