Solving polynomial equations by decomposition of algebraic varieties

Gabriela Jeronimo

Departamento de Matemática
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires

DEFINITIONS AND NOTATION

$\mathbb{K}$ denotes a field with char$(\mathbb{K}) = 0$ and $\overline{\mathbb{K}}$ is an algebraic closure of $\mathbb{K}$.

If $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$, $V(f_1, \ldots, f_s)$ is the affine variety

$$\{x \in \mathbb{A}^n(\overline{\mathbb{K}}) : f_1(x) = 0, \ldots, f_s(x) = 0\}.$$

Equidimensional decomposition

Any algebraic variety $V \subset \mathbb{A}^n$ (or $\mathbb{P}^n$) can be uniquely decomposed in a minimal way as

$$V = \bigcup_{r=0}^{n} V_r,$$

where, for every $0 \leq r \leq n$, $V_r = \emptyset$ or V_r is r-equidimensional.

$V_0, \ldots, V_n$ are the *equidimensional components* of V.

THE PROBLEM

Given $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$ defining a variety

$$V := V(f_1, \ldots, f_s) \subset \mathbb{A}^n,$$

obtain *algorithmically* the equidimensional decomposition

$$V = \bigcup_{r=0}^{n} V_r,$$

that is, provide a characterization for each of the equidimensional components $V_0, \ldots, V_n$ of V.

ALGORITHMS

Assume $\mathbb{K}$ is an effective field.

- *Input data:* Polynomials defining the variety V

- *Instructions:* Arithmetic operations and comparisons ($=$ or $\neq$)

- *Output:* A description of each equidimensional component of V

Complexity: Number of instructions.

DESCRIBING EQUIDIMENSIONAL VARIETIES

An equidimensional variety $V \subset \mathbb{A}^n$ can be described in different ways:

- *Polynomial defining equations:*
  $V = V(f_1, \dots, f_s)$

- *Geometric resolution:*
  A generic "parametric" description of V.

- *Chow form:*
  A *single* multivariate polynomial containing all the relevant information about V.

The precise definitions will be given later.

FIRST ALGORITHMS FOR EQUIDIMENSIONAL DECOMPOSITION

$V = V(f_1, \ldots, f_s) \subset \mathbb{A}^n$ (or $\mathbb{P}^n$), deg $f_i \leq d$.

- A. Chistov - D.Y. Grigor'ev (1983)
- M. Giusti - J. Heintz (1991)
  (*well parallelizable*)

Complexities: $(sd^{n^2})^{O(1)}$.

Remarks

- Both algorithms compute the equidimensional components V_r recursively, from $r = n, \ldots, 0$.

- They yield polynomial defining equations for the equidimensional components.

- Each polynomial is represented by the vector of its coefficients.

FURTHER PROBLEM

Construction of an algorithm with complexity *polynomial* in sd^n (input size).

Some ideas to solve this problem partially:

- Changing the data structure used to encode polynomials
- Probabilistic algorithms

ENCODING POLYNOMIALS

Let $f \in \mathbb{K}[x_1, \ldots, x_n]$

- *Dense form:*

  Vector of the coefficients of f in a prefixed order of monomials.

  Size: number of coefficients of f.

- *Straight-line program (slp):*

  Program whose instructions are $+, -, \cdot$, which enables to evaluate f at any given point $a \in \mathbb{K}^n$.

  Size (*length* of the slp):
  $L =$ number of instructions

- *Mixed representation*:

  In dense form with respect to certain variables and the coefficients by slp's.

PROBABILISTIC ALGORITHMS

The algorithm works under certain genericity conditions depending on parameters whose values are chosen randomly.

Additional operation allowed: random choice of a parameter from a prefixed finite set.

For each random choice, there is a non-zero polynomial whose non-vanishing leads to a correct computation.

The error probability of the algorithm can be estimated by means of the following result (Schwartz, 1980):

> Let $f \in \mathbb{K}[x_1, \ldots, x_n]$ be a non-zero polynomial. Then, if $\Gamma \subset \mathbb{K}$ is a finite set, we have for a randomly chosen $a \in \Gamma^n$:
>
> $$\text{Prob}(f(a) = 0) \leq \frac{\deg(f)}{\#\Gamma}.$$

COMPUTING EQUATIONS IN POLYNOMIAL TIME

Theorem (G. J.- J. Sabia, 2000)

Let $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$ with $\deg f_i \leq d$ for $1 \leq i \leq s$, and let

$$V = V(f_1, \ldots, f_s) = \bigcup_{r=0}^{n} V_r \subset \mathbb{A}^n.$$

Then, there is a probabilistic algorithm which computes the equidimensional decomposition of V within complexity $(sd^n)^{O(1)}$.

For every $0 \leq r \leq \dim V$, the algorithm yields a set of $n+1$ polynomials of degrees bounded by $\deg(V_r)$ defining V_r.

Remark Output and intermediate results are encoded by slp's.

GEOMETRIC RESOLUTIONS

Let $V \subset \mathbb{A}^n$ be an equidimensional variety with $\dim V = r$ and $\deg V = D$.

Assume that $\#\Big(V \cap V(x_1, \ldots, x_r)\Big) = D$. Set

$K := \mathbb{K}(x_1, \ldots, x_r)$, $\quad A := K \otimes_{\mathbb{K}[x_1,\ldots,x_r]} \mathbb{K}[V]$.

A *geometric resolution* of V is defined by:

- a linear form ℓ which is a primitive element of $K \hookrightarrow A$.
- the minimal polynomial $p \in \mathbb{K}[x_1, \ldots, x_r][t]$ of ℓ in A (monic in t).
- a polynomial $\rho \in \mathbb{K}[x_1, \ldots, x_r] - \{0\}$ and polynomials $v_{r+1}, \ldots, v_n \in \mathbb{K}[x_1, \ldots, x_r][t]$ with $\deg v_i \leq D - 1$ such that

$$\rho\, x_i = v_i(\ell) \quad \text{in } A \text{ for } i = r+1, \ldots, n.$$

OTHER PROBABILISTIC ALGORITHMS

(1) M. Elkadi - B. Mourrain (1999).
Complexity: $sd^{O(n^2)}$ (dense encoding).

(2) G. Lecerf (2000).
Complexity: $(sd^n L)^{O(1)}$ (slp's).

Remarks

- In (1), a *non-minimal* decomposition of V is obtained, and no probability considerations are made.

- Both algorithms compute *geometric resolutions* describing the equidimensional components.

- In (2), the input is encoded by a slp of length L.

CHOW FORM OF AN EQUIDIMENSIONAL VARIETY

Let $V \subset \mathbb{P}^n$ be an equidimensional *projective* variety definable over $\mathbb{K}$ with $\dim V = r$. For $i = 0, \dots r$, let

$$\begin{aligned} U_i &:= (U_{i0}, U_{i1}, \dots, U_{in}) \\ L_i(U_i, x) &:= U_{i0}x_0 + U_{i1}x_1 + \cdots + U_{in}x_n. \end{aligned}$$

The *Chow form* of V is the unique —up to scalar factors— squarefree polynomial $\mathcal{F}_V \in \mathbb{K}[U_0, \dots, U_r]$ verifying

$$V \cap \{L_0(u_0, x) = 0, \dots, L_r(u_r, x) = 0\} \neq \emptyset$$
$$\Updownarrow$$
$$\mathcal{F}_V(u_0, \dots, u_r) = 0$$

The Chow form of an equidimensional *affine* variety is the Chow form of its projective closure.

Remarks

- $\deg_{U_i} \mathcal{F}_V = \deg V \quad \forall\, 0 \le i \le r$
- $V = \bigcup_{i=1}^{t} C_i$ (irr. dec.) $\Rightarrow \mathcal{F}_V = \prod_{i=1}^{t} \mathcal{F}_{C_i}$

Examples

- $V = \mathbb{P}^n$, $\mathcal{F}_V(U_0, \ldots, U_n) = \det(U_{ij})_{\substack{0 \le i \le n \\ 0 \le j \le n}}$
- $V = \{p_1, \ldots, p_D\} \subset \mathbb{P}^n$,

$$\mathcal{F}_V(U_0) = \prod_{1 \le j \le D} L_0(U_0, p_j).$$

Remark

An equidimensional projective variety $V \subset \mathbb{P}^n$ is uniquely determined by its Chow form:

$$\xi \in V$$
$$\Updownarrow$$
$$L_i(u_i, \xi) = 0 \ \forall\, 0 \le i \le r \Rightarrow \mathcal{F}_V(u_0, \ldots, u_r) = 0$$

If V is a *projective* or *affine* variety, it is possible to derive equations for V from $\mathcal{F}_V$.

COMPUTING CHOW FORMS

$V = V(f_1, \dots, f_s) \subset \mathbb{P}^n$, deg $f_i \le d$:

- T. Krick (1990), L. Caniglia (1990).
  V equidimensional.
  Complexity: $(sd)^{n^{O(1)}}$.

- M. Giusti - J. Heintz (1991).
  $V = \bigcup_{r=0}^{n} V_r$ equid. decomposition.
  Computation of $\mathcal{F}_{V_0}, \dots, \mathcal{F}_{V_n}$ within complexity $(sd)^{n^{O(1)}}$.

Dense encoding $\Rightarrow$ Complexity $\ge d^{n^2}$

Using straight-line programs

- S. Puddu - J. Sabia (1998)
  V irreducible.
  Complexity: $(sd^{nr})^{O(1)}$, if $r = \dim V$.

- G. J. - S. Puddu - J. Sabia (2001)
  Computation of $\mathcal{F}_{V_r}$, where $r = \dim V$.
  Complexity: $(sd^n)^{O(1)}$.

Remarks

- All these algorithms are *deterministic*.

- Effective quantifier elimination applied to:

$$\exists\, x \in \mathbb{P}^n : f_1(x) = 0 \wedge \cdots \wedge f_s(x) = 0 \wedge L_0(u_0, x) = 0 \wedge \cdots \wedge L_r(u_r, x) = 0$$

BETTER COMPLEXITY BOUNDS

Theorem (G. J.-T. Krick-J. Sabia-M. Sombra, 2002)

Let $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$ be polynomials with $\deg(f_i) \leq d$ $(1 \leq i \leq s)$ encoded by slp's of length L, and let

$$V = V(f_1, \ldots, f_s) = \bigcup_{r=0}^{n} V_r \subset \mathbb{A}^n.$$

There is a probabilistic algorithm which computes slp's of length $s(nd^n)^{O(1)}L$ encoding the Chow forms $\mathcal{F}_{V_0}, \ldots, \mathcal{F}_{V_n}$ within complexity $s(nd^n)^{O(1)}L$.

Auxiliary result (algorithm $\mathbf{ChowForm}$)

$V \subset \mathbb{A}^n$ equidimensional, $\dim V = r$.
Assume that $Z := V \cap V(x_1, \ldots, x_r)$ is a 0-dimensional variety with $\deg V$ points.

There is a *deterministic* algorithm which computes a slp encoding $\mathcal{F}_V$ from

- a geometric resolution of Z and
- a system of local equations $f_1, \ldots, f_{n-r} \in \mathbb{K}[x_1, \ldots, x_n]$ of V at Z.

Complexity and length of the output slp:

$$(n\, d \deg V)^{O(1)} L$$

if $\deg f_i \leq d$ ($1 \leq i \leq n-r$) and $f_1, \ldots, f_{n-r}$ are encoded by slp's of length L.

Sketch of the main algorithm ($\mathrm{EquiDec}$)

1. Input preparation (random).
   - $n+1$ linear combinations of $f_1, \ldots, f_s$
   - linear change of variables

   New polynomials: $f_1, \ldots, f_{n+1}$.

   For $r = 0, \ldots, n$:

$$\begin{array}{rcl} V(f_1, \ldots, f_{n-r}) & = & W_r \cup V_r \cup \cdots \cup V_n \\ W_{r+1} \cap V(f_{n-r}) & = & W_r \cup V_r \cup V_r' \quad \text{with } V_r' \subset V \end{array}$$

2. Computing Chow forms of a non-minimal decomposition

   For $r = n-1, \ldots, 0$ compute:
   - $\mathcal{F}_{W_{r+1}} := \mathbf{ChowForm}(GR_{r+1}, f_1, \ldots, f_{n-r})$
   - $\mathcal{F}_{W_{r+1} \cap V(f_{n-r})} := \mathbf{Inter}(\mathcal{F}_{W_{r+1}}, f_{n-r})$
   - $\mathcal{F}_{V_r \cup V_r'} := \mathbf{Sep}_1(W_{r+1} \cap V(f_{n-r}), f_{n-r+1})$
   - $GR_r :=$ geometric resolution of $W_r \cap V(x_1, \ldots, x_r)$.

3. Cleaning spurious components

   For $r = n-2, \ldots, 0$ compute:
   - $G_r \in \mathbb{K}[x_1, \ldots, x_n]$ verifying $V_r' \subset V(G_r)$ and $\dim(V_r \cap V(G_r)) < r$.
   - $\mathcal{F}_{V_r} := \mathbf{Sep}_2(\mathcal{F}_{V_r \cup V_r'}, G_r)$

CHOW FORMS VS. GEOMETRIC RESOLUTIONS

Let $V \subset \mathbb{A}^n$ be an r-equidimensional variety and let $Z := V \cap V(x_1, \ldots, x_r)$.

Assume that $\dim Z = 0$, $\deg Z = \deg V$ and ℓ is a linear form separating the points in Z.

Chow form → Geometric resolution:

Let $e_0 := (1, 0, \ldots, 0)$, $c_0 :=$ coefficients of ℓ and

$$P := \mathcal{F}_V(U_0 - T_0 e_0, \ldots, U_r - T_r e_0)$$

In $A := \mathbb{K}(x_1, \ldots, x_r) \otimes_{\mathbb{K}[x_1, \ldots, x_r]} \mathbb{K}[V]$, we have:

- $p(t) := P(c_0, e_1, \ldots, e_r)(t, x_1, \ldots, x_r)$ is the minimal polynomial of ℓ
- for $i = 1, \ldots, n$, the polynomial $w_i := \partial P / \partial U_{0i}(c_0, e_1, \ldots, e_r)(t, x_1, \ldots, x_r)$ verifies $p'(\ell) x_i = w_i(\ell)$

This enables to derive a geometric resolution of V within complexity polynomial in n, $\deg V$ and the length of a slp encoding $\mathcal{F}_V$.

Geometric resolution $\to$ Chow form:

- Obtain a geometric resolution of Z by specialization of the geometric resolution of V.
- Compute a system of local equations of V at Z (eliminating polynomials of generic linear forms)
- Apply algorithm $\mathbf{ChowForm}$

This procedure computes $\mathcal{F}_V$ within complexity polynomial in n, $\deg V$ and the length of a slp encoding the geometric resolution of V.

Corollary From the complexity viewpoint, Chow forms and geometric resolutions are *equivalent* representations of an equidimensional variety.

GEOMETRIC DEGREE OF A POLYNOMIAL SYSTEM

How can we identify particular instances of the problem which can be solved faster than the general case?

Giusti et al. (1998) introduced a parameter δ associated with the system in the complexity estimates of 0-dimensional system solving.

Let $f_1, \dots, f_s \in \mathbb{K}[x_1, \dots, x_n]$.

Consider new variables $(T_{ij})_{1 \le i \le n,\, 1 \le j \le s}$ and polynomials

$$\widehat{f}_i := \sum_{j=1}^{s} T_{ij}\, f_j \qquad i = 1, \dots, n$$

The *geometric degree of the system* $f_1, \dots, f_s$ can be defined as

$$\delta := \max\{\deg V(\widehat{f}_1, \dots, \widehat{f}_\ell) : 1 \le \ell \le n\}$$

Remark If $\deg(f_i) \le d$, by Bézout inequality $\delta \le d^n$, but it can be considerably smaller.

EXPECTED COMPLEXITY

EquiDec is a *bounded probability algorithm* (error probability $< \frac{1}{4}$ on any input).
Its complexity on a given input γ can be seen as a random variable $C(\gamma)$ with finite sample set.

Expected complexity of the algorithm := expectation of the random variable C.

If $V = V(f_1, \ldots, f_s) \subset \mathbb{A}^n$, where $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$ satisfy:

- $\deg f_i \leq d$ for $1 \leq i \leq s$,
- they are encoded by slp's of length L,
- δ is the geometric degree of the system,

EquiDec computes $\mathcal{F}_{V_0}, \ldots, \mathcal{F}_{V_n}$ within expected complexity

$$s(nd\delta)^{O(1)}L.$$

AN APPLICATION: COMPUTATION OF SPARSE RESULTANTS

Let $\mathcal{A} \subset (\mathbb{N}_0)^n$ be a finite set containing $\{0, e_1, \ldots, e_n\}$.

Vol($\mathcal{A}$) := normalized volume of the convex hull of $\mathcal{A}$ in $\mathbb{R}^n$.

Theorem (G. J.-T. Krick-J. Sabia-M. Sombra, 2002)

There is a probabilistic algorithm which computes a scalar multiple of the $\mathcal{A}$-resultant within (expected) complexity $(n\,\mathrm{Vol}(\mathcal{A}))^{O(1)}$.

This follows from the fact that the $\mathcal{A}$-resultant $\mathrm{Res}_{\mathcal{A}}$ is the Chow form of the toric variety associated with $\mathcal{A}$.