Elimination Techniques for the Computation of the Ideal of a Smooth Algebraic Variety

Gabriela Jeronimo

Departamento de Matemática, FCEyN,
Universidad de Buenos Aires
CONICET - Argentina

On the number of equations defining a variety

$\mathbb{K}$:= algebraically closed field with $\mathrm{char}(\mathbb{K}) = 0$

(Kronecker, 1882) Every affine algebraic variety $V \subset \mathbb{A}^n$ can be defined as the set of common zeros of $n+1$ polynomials in $\mathbb{K}[x_1, \ldots, x_n]$. Moreover:

$$\text{If } V = V(f_1, \ldots, f_s) \text{ with } f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n], \text{ then}$$

$$\exists g_1, \ldots, g_{n+1} \in \mathbb{K}[x_1, \ldots, x_n] \text{ such that } V = V(g_1, \ldots, g_{n+1}) \text{ with}$$

$$g_i = \sum_{j=1}^{s} \lambda_{ij} f_j \quad (\lambda_{ij} \in \mathbb{K}) \quad \text{for every } 1 \leq i \leq n+1.$$

Idea of a proof:

Construct recursively, for $i = 1, \ldots, n+1$, linear combinations $g_1, \ldots, g_{n+1}$ of $f_1, \ldots, f_s$ such that each irreducible component of $W_i := V(g_1, \ldots, g_i)$ not contained in V has dimension $n - i$.
In particular, $W_{n+1} = V$.

- Take one point $p_C \notin V$ in each irreducible component C of W_{i-1} not contained in V.

- Choose $g_i = \sum_{j=1}^{s} \lambda_{ij} f_j$ so that $g_i(p_C) \neq 0 \; \forall \, p_C$. When taking $W_i := W_{i-1} \cap V(g_i)$, the dimension of each irreducible component not contained in V drops.

- The condition $g_i(p_C) \neq 0$ is obtained by choosing λ_{ij} such that $\prod_C (\sum_{j=1}^{s} \lambda_{ij} f_j(p_C)) \neq 0$ (non-zero polynomial in the λ_{ij}'s).

The degree of an affine variety

Crucial in order to obtain upper bounds for the degrees of equations defining a variety $V \subset \mathbb{A}^n$.

(Heintz, 1983) If $V \subset \mathbb{A}^n$ is irreducible with $\dim V = k$,

$$\deg V = \max\{D \in \mathbb{N} : \exists\, H_1, \dots, H_k \subset \mathbb{A}^n \text{ affine hyperplanes with } \#(V \cap H_1 \cap \cdots \cap H_k) = D\}$$

For an arbitrary affine variety $V \subset \mathbb{A}^n$, $\deg V$ is the sum of the degrees of the irreducible components of V.

A degree upper bound for defining equations

(Heintz, 1983) Let $V \subset \mathbb{A}^n$ be an algebraic variety. Then:

$\exists\ f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$ with $\deg(f_i) \leq \deg(V)$ for $i = 1, \ldots, s$, such that $V = V(f_1, \ldots, f_s)$.

Idea of the proof:

- For every $p \notin V$, $\exists\, f_p \in \mathbb{K}[x_1, \ldots, x_n]$ such that $f_p(\xi) = 0$ $\forall\, \xi \in V$ and $f_p(p) \neq 0$.
- f_p is the defining equation of the image of V under a linear projection and so, $\deg(f_p) \leq \deg(V)$.

Theorem *Every affine algebraic variety $V \subset \mathbb{A}^n$ can be defined by $n+1$ polynomials with degrees bounded by $\deg V$.*

A refinement of Kronecker's bound

(Storch, 1972; Eisenbud and Evans, 1975) Every affine algebraic variety $V \subset \mathbb{A}^n$ can be defined by n polynomials.

Remarks:

- This bound is optimal (consider the case when $\dim V = 0$).
- No upper bound on the degrees of the polynomials is given.

The ideal of an algebraic variety

$V \subset \mathbb{A}^n$ an affine algebraic variety. Denote

$$I(V) = \{f \in \mathbb{K}[x_1, \ldots, x_n] : f(\xi) = 0 \; \forall \xi \in V\}.$$

Problem 1.

Determine whether there exists a system of generators of $I(V)$ with 'few' polynomials of 'low' degree.

Problem 2.

Given $g_1, \ldots, g_s \in \mathbb{K}[x_1, \ldots, x_n]$ such that $V = V(g_1, \ldots, g_s)$, compute a set of generators for $I(V)$.

Zero-dimensional varieties

Let $V \subset \mathbb{A}^n$, $\dim V = 0$ (finite set).

(Shape Lemma) $\exists\, \ell \in \mathbb{K}[x_1, \ldots, x_n]$ a linear form with

$$\ell(\xi) \neq \ell(\xi') \text{ for } \xi, \xi' \in V,\ \xi \neq \xi'.$$

Assume ℓ depends on x_1. Then, there are univariate polynomials $p_1, \ldots, p_n$ with $\deg p_1 = \deg V$ and $\deg p_i < \deg V$ for $i = 2, \ldots, n$ such that

$$I(V) = (p_1(\ell), x_2 - p_2(\ell), \ldots, x_n - p_n(\ell)).$$

If $f_1 := p_1(\ell)$, $f_i := x_i - p_i(\ell)$ for $i = 2, \ldots, n$,

$$I(V) = (f_1, \ldots, f_n) \text{ and } \deg f_i \leq \deg V.$$

An example due to Macaulay

(Macaulay, 1916) $\forall\, m \in \mathbb{N}$, $\exists\, V_m \subset \mathbb{A}^3$ curve such that $I(V_m)$ cannot be generated by less than m polynomials.

Corollary. For $V \subset \mathbb{A}^n$, there is no general upper bound depending only on n for the number of polynomials in a generator set of $I(V)$.

Estimates under additional assumptions

(Kumar, 1978; Sathaye, 1978)

Let $V \subset \mathbb{A}^n$ be an affine variety such that $I(V)$ is locally complete intersection. Then, $I(V)$ can be generated by n polynomials.

Not clear how to obtain degree estimates.

(Mumford, 1970; Seidenberg, 1975)

Let $V \subset \mathbb{A}^n$ be a smooth irreducible variety. Then $I(V)$ can be generated by polynomials with degrees bounded by $\deg V$.

No non-trivial upper bound for the number of generators.

The main problem

Can the number and the degrees of the polynomials in a generating set of $I(V)$ be controlled *simultaneously* under certain assumptions on V?

In this talk:

Positive answer for smooth equidimensional affine varieties.

Number and degree of ideal generators

Theorem 1. *(Blanco-J. -Solernó)*

Let $V \subset \mathbb{A}^n$ *be a smooth equidimensional algebraic variety. Set*

$$m := (n - \dim V)(1 + \dim V)$$

Then, there exist $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$ *with* $\deg f_i \leq \deg V$ *for* $i = 1, \ldots, m$ *such that*

$$I(V) = (f_1, \ldots, f_m).$$

Basic ingredients of the proof

- Local-global principle, which enables us to look for generators of the ideal locally at any of the points of the variety.
- Linear projections to obtain polynomials in the ideal $I(V)$.
- A Jacobian criterion for a system of polynomials to be local generators of the ideal at a given point.

Regular points and smooth varieties

Assume that:

- $V \subset \mathbb{A}^n$ is an equidimensional algebraic variety.
- $I(V) = (f_1, \ldots, f_m) \subset \mathbb{K}[x_1, \ldots, x_n]$.
- $J := \left(\frac{\partial f_i}{\partial x_j}\right)_{\substack{1\le i\le m\\ 1\le j\le n}}$ is the associated Jacobian matrix.

V is *smooth at a point* $p \in V$ (and p is a *regular point* of V) if $\operatorname{rank} J(p) = n - \dim V$.

V is *smooth* if it is smooth at every $p \in V$.

From now on, we assume $V \subset \mathbb{A}^n$ smooth equidimensional.

Linear projections

Let $V \subset \mathbb{A}^n$ be an equidimensional variety and let $k := \dim(V)$.

For $h = (h_1, \ldots, h_{k+1}) \in (\mathbb{A}^{n+1})^{k+1}$, let

$$\begin{array}{rcl} \ell_{h_j} & \in & \mathbb{K}[x_1, \ldots, x_n] \quad j = 1, \ldots, k+1 \\ \ell_{h_j} & := & h_{j0} + h_{j1}x_1 + \cdots + h_{jn}x_n \end{array}$$

and let

$$\begin{array}{rcl} \pi_h : \mathbb{A}^n & \to & \mathbb{A}^{k+1} \\ x & \mapsto & (\ell_{h_1}(x), \ldots, \ell_{h_{k+1}}(x)). \end{array}$$

Consider the image

$$\pi_h(V) \subset \mathbb{A}^{k+1}.$$

Polynomials of low degrees in $I(V)$

$\exists\ U_0 \subset (\mathbb{A}^{n+1})^{k+1}$ Zariski dense open set such that $\forall\, h \in U_0$, $\pi_h(V)$ is a hypersurface.

Then, for $h \in U_0$ we have

$$\pi_h(V) = \{y \in \mathbb{A}^{k+1} : f_h(y) = 0\} \subset \mathbb{A}^{k+1},$$

where f_h is square-free and $\deg f_h = \deg \pi_h(V) \le \deg V$.

$$\Rightarrow f_h^* := f_h(\ell_{h_1}, \ldots, \ell_{h_{k+1}}) \in I(V)$$

$$\deg f_h^* \le \deg V$$

A condition for local generators

For every $p \in \mathbb{A}^n$, we denote

$$\mathcal{O}_{p,\mathbb{A}^n} := \{f/g : f, g \in \mathbb{K}[x_1, \ldots, x_n],\ g(p) \neq 0\}.$$

(Mumford, 1970) If $p \in V$ is a regular point and $f_1, \ldots, f_t \in I(V)$, the following conditions are equivalent:

- $T_{p,V} = \bigcap_{i=1}^{t} T_{p,V(f_i)}$
- $I(V)\mathcal{O}_{p,\mathbb{A}^n} = (f_1, \ldots, f_t)\mathcal{O}_{p,\mathbb{A}^n}$

Local generators of low degrees

- For every regular point $p \in V$, $\exists\, \mathcal{U}_p \neq \emptyset$, Zariski open, such that $\forall\, h \in \mathcal{U}_p$, $\{f_h^*(x) = 0\}$ is a hypersurface smooth at p.

Lemma. Let $p \in V$ be a regular point. Then, if $\mathcal{U}_p$ is as above,

$$I(V)\mathcal{O}_{p,\mathbb{A}^n} = (f_h^* : h \in \mathcal{U}_p)\mathcal{O}_{p,\mathbb{A}^n}.$$

$\Rightarrow I(V)\mathcal{O}_{p,\mathbb{A}^n}$ is generated by polynomials of degrees bounded by $\deg V$.

Moreover, for a generic choice of $h^{(1)}, \ldots, h^{(n-k)} \in \mathcal{U}_p$, we have

$$I(V)\mathcal{O}_{p,\mathbb{A}^n} = (f_{h^{(1)}}^*, \ldots, f_{h^{(n-k)}}^*)\mathcal{O}_{p,\mathbb{A}^n}.$$

Existence of generators of $I(V)$ of low degrees

Thus, we recover the result in *(Mumford, 1970; Seidenberg, 1975; Catanese, 1992)*:

Proposition. Let $V \subset \mathbb{A}^n$ be a smooth equidimensional variety. Then

$$I(V) = (f_h^* : h \in U_0),$$

$U_0 \subset (\mathbb{A}^{n+1})^{k+1}$ is a Zariski dense open set. In particular, $I(V)$ can be generated by polynomials of degrees bounded by $\deg V$.

Choosing ‘few’ generators

Lemma. Let $V \subset \mathbb{A}^n$ be a k-equidimensional smooth variety and let $f_1, \ldots, f_s \in I(V)$ such that

- $V(f_1, \ldots, f_s) = V \cup Z$, with $Z = \emptyset$ or equidimensional,
- $(f_1, \ldots, f_s)\mathcal{O}_{p,\mathbb{A}^n} = I(V)\mathcal{O}_{p,\mathbb{A}^n}$ $\forall\, p \in V - Y$, for an equidim. subvariety $Y \subset V$.

Then $\exists\, h^{(1)}, \ldots, h^{(n-k)} \in (\mathbb{A}^{n+1})^{k+1}$ such that

- $V\left(f_1, \ldots, f_s, f^*_{h^{(1)}}, \ldots, f^*_{h^{(n-k)}}\right) = V \cup Z'$, where $Z' = \emptyset$ or equidim. with $\dim Z' = \dim Z - (n-k)$,
- $(f_1, \ldots, f_s, f^*_{h^{(1)}}, \ldots, f^*_{h^{(n-k)}})\mathcal{O}_{p,\mathbb{A}^n} = I(V)\mathcal{O}_{p,\mathbb{A}^n}$ $\forall\, p \in V - Y'$, where $Y' = \emptyset$ or $Y' \subset V$ equidim. with $\dim Y' = \dim Y - 1$.

Idea of the proof:

- Take $\{p_1, \ldots, p_r\} \subset V$ containing one point in each irreducible component of the set Y of 'bad points' (= points at which the given polynomials do not generate $I(V)$ locally).

- Choose recursively $h^{(1)}, \ldots, h^{(n-k)}$ so that

  (i) $f^*_{h^{(1)}}, \ldots, f^*_{h^{(n-k)}}$ generate $I(V)\mathcal{O}_{p_i,\mathbb{A}^n}$ $\forall\, 1 \leq i \leq r$,

  (ii) $Z \cap V(f^*_{h^{(1)}}, \ldots, f^*_{h^{(l)}}) = \emptyset$ or equidimensional with dimension $\dim Z - l$ for $l = 1, \ldots, n-k$.

- Condition (i) above implies that the dimension of the set of 'bad points' drops.

A recursive construction based on the previous lemma:

- Choose a family of $n-k$ linear projections such that their associated defining polynomials generate $I(V)$ locally at the points of a Zariski dense open set of V.
- By choosing $k+1$ different families of $n-k$ projections, reduce the set of 'bad points' successively from $k-1$ to -1.

$\exists\ h^{(1)},\ldots,h^{(m)} \in (\mathbb{A}^{n+1})^{k+1}$, with $m := (n-k)(k+1)$, such that

$$I(V) = \left(f^*_{h^{(1)}},\ldots,f^*_{h^{(m)}}\right).$$

Computing generators of $I(V)$

Problem. *Given* $g_1, \ldots, g_s \in \mathbb{K}[x_1, \ldots, x_n]$ *with* $V = V(g_1, \ldots g_s)$, *compute* $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$ *such that* $I(V) = (f_1, \ldots, f_m)$.

Nullstellensatz $\Rightarrow$ this is equivalent to

$$I = (g_1, \ldots, g_s) \rightsquigarrow \sqrt{I} = (f_1, \ldots, f_m)$$

There are effective procedures solving this task in the general case *(Gianni-Trager-Zacharias, 1988; Eisenbud-Huneke-Vasconcelos, 1992; Krick-Logar, 1992;...)*

Complexities: At least doubly exponential.

Our result on the computation of $I(V)$

Theorem 2. *(Blanco-J. -Solernó)*

Let $g_1, \ldots, g_s \in \mathbb{K}[x_1, \ldots, x_n]$ *such that* $V = V(g_1, \ldots, g_s) \subset \mathbb{A}^n$ *is smooth equidimensional with* $0 < \dim V < n - 1$.

Assume that $\deg g_i \leq d$ *and that* $g_1, \ldots, g_s$ *are encoded by slp's of length* L. *Set* $m := (n - \dim V)(\dim V + 1)$.

Then, there is a probabilistic algorithm which computes polynomials $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$ *such that* $I(V) = (f_1, \ldots, f_m)$ *within complexity* $s(nd^n)^{O(1)}L$.

Basic ingredients

- Our upper bound for the number of generators.
- Fast computation of eliminating polynomials using Chow forms.

The Chow form of an equidimensional variety

$V \subset \mathbb{A}^n$ a k-equidimensional variety; $\overline{V} \subset \mathbb{P}^n$ its projective closure.

$(H_1, \ldots, H_{k+1})$ sets of new indeterminates and, for $j = 1, \ldots, k+1$,

$$L_j := H_{j0}\, x_0 + H_{j1}\, x_1 + \cdots + H_{jn}\, x_n.$$

The *Chow form* of V is the unique (up to scalar factors) square-free polynomial $\mathcal{F} \in \mathbb{K}[H_1, \ldots, H_{k+1}]$ satisfying

$$\mathcal{F}(h_1, \ldots, h_{k+1}) = 0$$

$$\Updownarrow$$

$$\overline{V} \cap \{L_1(h_1, x) = 0, \ldots, L_{k+1}(h_{k+1}, x) = 0\} \neq \emptyset$$

Eliminating polynomials and Chow forms

Lemma. Let $e := (1, 0, \ldots, 0) \in \mathbb{K}^{n+1}$ and $(h_1, \ldots, h_k) \in (\mathbb{K}^{n+1})^k$ such that $\mathcal{F}(h_1, \ldots, h_k, e) \neq 0$. Then, for every $h_{k+1} \in \mathbb{K}^{n+1}$,

$$\widehat{f}_h := \mathcal{F}(h_1 - y_1 e, \ldots, h_{k+1} - y_{k+1} e) \in \mathbb{K}[y_1, \ldots, y_{k+1}]$$

satisfies

$$\pi_h(V) = \{y \in \mathbb{A}^{k+1} : \widehat{f}_h(y) = 0\},$$

where $\pi_h : \mathbb{A}^n \to \mathbb{A}^{k+1}$, $\pi_h(x) = (\ell_{h_1}(x), \ldots, \ell_{h_{k+1}}(x))$.

Moreover, there is an open set $\mathcal{U}_0 \subset (\mathbb{A}^{n+1})^{k+1}$ such that $\widehat{f}_h$ is square-free and so, $f_h^* = f_h(\ell_{h_1}, \ldots, \ell_{h_{k+1}})$ can be obtained as

$$f_h^* = \mathcal{F}\left(h_1 - \ell_{h_1} e, \ldots, h_{k+1} - \ell_{h_{k+1}} e\right)$$

$$\forall\, h := (h_1, \ldots, h_{k+1}) \in \mathcal{U}_0$$

The algorithm

INPUT: $g_1, \ldots, g_s \in \mathbb{K}[x_1, \ldots, x_n]$ such that
$V = V(g_1, \ldots, g_s) \subset \mathbb{A}^n$ is k-equidim. and smooth.

1. Compute the Chow form $\mathcal{F}$ of V.
2. Choose $m := (n-k)(k+1)$ elements $h^{(1)}, \ldots, h^{(m)} \in (\mathbb{A}^{n+1})^{k+1}$ at random with coordinates in $\{1, \ldots, C(N)\}$ for an appropriate $C(N) \in \mathbb{N}$.
3. For $i = 1, \ldots, m$, compute

$$f_i := \mathcal{F}\big(h_1^{(i)} - \ell_{h_1^{(i)}} e, \ldots, h_{k+1}^{(i)} - \ell_{h_{k+1}^{(i)}} e\big).$$

OUTPUT: $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$ such that
$I(V) = (f_1, \ldots, f_m)$ with error probability $\leq 1/N$.

Complexity estimates

Assume that the input is given by:

- s polynomials $g_1, \ldots, g_s \in \mathbb{K}[x_1, \ldots, x_n]$
- $\deg g_i \leq d$, $L(g_i) \leq L$ for every $1 \leq i \leq s$.

Complexity of computing an slp for the Chow form of V *(J. -Krick-Sabia-Sombra, 2003)*: $s(nd^n)^{O(1)}L$.

The algorithm computes slp's of length $s(nd^n)^{O(1)}L$ encoding $f_1, \ldots, f_m$.

Remark. If δ is the *geometric degree* of the input system, $\exists$ a system of generators for $I(V)$ that can be encoded by slp's of length $s(nd\delta)^{O(1)}L$.

Happy 60th birthday Joos!