Affine varieties:
Degree, Height and Complexity

Martín Sombra

Departamento de Matemática
Universidad Nacional de La Plata
La Plata, Argentina

Mathematical Sciences Research Institute
Berkeley, USA

- Degree of varieties

- Height of varieties

- Arithmetic Nullstellensatz

- Distance between varieties

- Complexity of varieties

Nullstellensatz *(Hilbert 1893)*

$f_1, \ldots, f_s \in \mathbb{Q}[x_1, \ldots, x_n]$ polynomials

$V(f_1, \ldots, f_s) := \{x \in \mathbb{C}^n : f_1 = 0, \ldots, f_s = 0\} = \emptyset$

$\iff \quad \exists\, g_1, \ldots, g_s \in \mathbb{Q}[x_1, \ldots, x_n]$ st

$$1 = g_1 f_1 + \cdots + g_s f_s$$

$V_i := V(f_i) := \{x \in \mathbb{C}^n : f_i(x) = 0\} \subseteq \mathbb{C}^n$

$$\cap_i V_i = \emptyset$$

Zariski closed sets with empty intersection

$\psi_i := g_i f_i$ algebraic partition of 1

- $1 = \Sigma_i\, \psi_i$
- $\psi_i \equiv 0$ in V_i

Eg.

$$f_1 := x^3, f_2 := 2 - x\,y^2$$

$$y^6 f_1 + (x^2y^4 + 2xy^2 + 4)f_2 = 8$$

Problems

- Degree and height bounds for the Nullstellensatz (Arithmetic Nullstellensatz):

  Find

  $g_1, \ldots, g_s \in \mathbb{Z}[x_1, \ldots, x_n], \;\; a \in \mathbb{Z} - \{0\}$ st

  $$a = g_1 f_1 + \cdots + g_s f_s$$

  $\deg g_i \leq$ **?** $\qquad h(a), \;\; h(g_i) \leq$ **?**

- Separation of varieties $V, \; W \subseteq \mathbb{C}^n$ varieties defined over $\mathbb{Q}$ st $V \cap W = \emptyset$

  $$\mathrm{dist}(V, W) \geq \textbf{?}$$

Degree of varieties

k field

$V \subseteq \mathbb{A}^n(\overline{k})$ equidimensional affine variety of dimension r

$$\deg V := \#(V \cap E)$$

E generic affine space of dimension $n - r$

$V = \cup_i V_i$ equidimensional decomposition

(V_i equidimensional variety of dimension i)

$$\deg V = \sum_i \deg V_i$$

- $\deg V \geq 1$

- $f \in k[x_1, \ldots, x_n]$ square–free polynomial

  $\Rightarrow \quad \deg V(f) = \deg f$

- $\dim V = 0 \quad \Rightarrow \quad \deg V = \# V$

Bézout inequality

Heintz–Sieveking 77
Fulton–MacPherson–Lazarsfeld 80

$V, W \subseteq \mathbb{A}^n$ affine variety. Then

$$\deg V \cap W \leq \deg V \cdot \deg W$$

Cor. *(Bézout 1764)*

$f_1, \ldots, f_n \in k[x_1, \ldots, x_n]$
st $\dim V(f_1, \ldots, f_n) = 0$. Then

$$\# V(f_1, \ldots, f_n) \leq \prod_i \deg f_i$$

Height of varieties

Height of a polynomial

$f = \Sigma_i\, a_i x^i \in \mathbb{Z}[x_1, \ldots, x_n] \;\Rightarrow\; h(f) := \log(\max_i |a_i|)$

Weil height

$V \subseteq \mathbb{A}^n$ $\mathbb{Q}$–variety of dimension 0

$$w(V) := \sum_{\xi \in V} h(\xi)$$

For $\xi \in \mathbb{Z}^n$, $h(\xi) = \log(\max_i |\xi_i|)$

Problem

Define a *height* $h(V)$ of a $\mathbb{Q}$-variety $V \subseteq \mathbb{A}^n(\mathbb{C})$ st

- For $f \in \mathbb{Z}[x_1, \ldots, x_n]$ primitive square–free polynomial.

$$h(V(f)) = h(V)$$

- $\dim V = 0 \;\Rightarrow\; h(V) = w(V)$
- $h(V \cap W) \leq$ **?** (Arithmetic Bézout inequality)

Chow form

$X \subseteq \mathbb{P}^n$ equidimensional projective $\mathbb{Q}$–variety of dimension r

$u_i := (u_{i,1}, \ldots, u_{i,n+1})$ groups of variables

$f_X \in \mathbb{Z}[u_1, \ldots, u_{r+1}]$ *Chow form* of X

Primitive polynomial in $(r+1)(n+1)$ variables

For $V \subseteq \mathbb{A}^n$ (affine variety) we define

$$f_V := f_{\overline{V}}$$

where $\overline{V} \subseteq \mathbb{P}^n$ projective closure of V

Defn. *(Philippon 95)*
V equidimensional affine $\mathbb{Q}$–variety

$$h(V) := \int_{S_n^{r+1}} \log |f_V| \; \mu_n^{r+1} + \Big(\sum_{i=1}^{n} 1/2\, i\Big) \deg V$$

S_n unit sphere $\{|z_1|^2 + \cdots + |z_n|^2 = 1\}$ in $\mathbb{C}^n$
μ invariant measure over S_n of total mass 1

(Alternative Mahler measure of f_V)

$V = \cup_i V_i$ equidimensional decomposition

$$h(V) = \sum_i h(V_i)$$

Definition of h via Chow form:
Weil 50, Nesterenko 77, Philippon 86

via arithmetic intersection theory:
Faltings 91, Bost–Gillet–Soulé 94

Equivalence between both points of view:
Soulé 91, Philippon 91

Properties *(Bost–Gillet–Soulé 94, Philippon 95)*

- $h(V) \geq 0$

- $f = \Sigma_i \, a_i \, x^i \in \mathbb{Z}[x_1, \ldots, x_n]$ primitive square–free polynomial $\Rightarrow$

  $$|h(V(f)) - h(f)| \leq 4\,(n+1)\log(n+1)\deg f$$

- $V \subseteq \mathbb{A}^n$ $\mathbb{Q}$–variety of dimension 0

  $$|h(V) - w(V)| \leq \log(n+1)\deg V$$

- Arithmetic Bézout inequality

  $V, W \subseteq \mathbb{A}^n(\mathbb{C})$ arithmetic varieties

  $$h(V \cap W) \leq \deg(W) \cdot h(V) + \deg(V) \cdot h(W) + c(n)\,\deg(V) \cdot \deg(W)$$

Extension *(S. 98)*
h extends to the case of a PF–field k (field with product formula):

$V \subseteq \mathbb{A}^n$ equidimensional k–variety

$$h(V) := \sum_{v \in S_k} \lambda_v \, m(\sigma_v(f_V)) + \sum_{v \in M_k - S_k} \lambda_v \log |f_V|_v$$

M_k proper set of absolute values over k

S_k subset of archimedian absolute values

λ_v multiplicities

m alternative Mahler measure

Basic examples of PF-fields

- number fields
- $K(t_1, \ldots, t_m)$ function fields

For $P \in K[t_1, \ldots t_m][x_1, \ldots, x_n]$

$$h(P) := \deg_t P$$

Allows to consider varieties defined by a parametric system of equations

Thm. *(Arithmetic Bézout inequality, general case)*

k PF–field
V, $W \subseteq \mathbb{A}^n$ k–varieties $\Rightarrow$

$$h(V \cap W) \;\leq\; c_1(n)\,(\deg V \cdot \deg W)^8 (h(V) + h(W)) \\ + c_2(n)\,(\deg V \cdot \deg W)^9$$

More generally $V_1, \ldots, V_l \subseteq \mathbb{A}^n$ k–varieties

δ_i degree of V_i, $\quad \delta := \Pi_i\, \delta_i \quad \Rightarrow$

$$h(V_1 \cap \cdots \cap V_l) \leq c_1(n)\,\delta^8 \sum_i h(V_i) + c_2(n)\,\delta^9$$

Cor.

$f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ polynomials st
$V := V(f_1, \ldots, f_s) \subseteq \mathbb{A}^n$ is 0-dimensional
$\deg f_i \leq d, \quad h(f_i) \leq h$

$$w(V) \leq c_3(n)\, d^{8\,n}\, h + c_4(n)\, d^{9\,n}$$

$w(V)$ Weil height of V

Thm.

$F := \{F_{r+1}, \ldots, F_n\} \subseteq \mathbb{Z}[x_1, \ldots, x_n]$
reduced complete intersection

$V := V(F) \subseteq \mathbb{A}^n$ and $\deg V = \delta$

$\pi : W \to \mathbb{A}^r,\ x \mapsto (x_1, \ldots, x_r)$
linear and separable linear projection

$0 \in \mathbb{A}^r$ non–ramified

$$h(V) \le c_1(n)\, \delta^5\, h(\pi^{-1}(0)) + c_2(n)\, \delta^7$$

ie the height of a complete intersection variety is polinomially equivalent to the height of the fiber $\pi^{-1}(0)$

Other aspects:

- Height of a product of varieties
- Height of the image of a morphism
- Height of the inverse of a birrational morphism $\varphi : V \to \mathbb{A}^r$

Interpretation of h

$\dim V = 0$ then $\dim_k k[V] \leq \deg V$

$\deg V$ controls the algebraic parameters

Which is the rol of h ?

Geometric solution *(Kronecker 1882)*

V equidimensional $\mathbb{Q}$–variety of dimension r

$\pi : V \to \mathbb{A}^{r+1}$ generic linear projection

$\Rightarrow \ \overline{\pi(V)} \subseteq \mathbb{A}^{r+1}$ hypersurface birrational to V

$\pi^{-1} : \overline{\pi(V)} \to V$ weak parametrization of V

Output of the symbolic algorithms for multivariate polynomial equation solving

Eg.

$C := V(x^2 - y, z - xy) \subseteq \mathbb{A}^3$ rational normal curve of degree 3

$\pi : \mathbb{A}^3 \to \mathbb{A}^2$ defined by $(x, y, z) \mapsto (x, y)$

- $\overline{\pi(C)} = V(x^2 - y)$
- $\pi^{-1}(x, y) := (x, y, xy)$

$p \in k[y_1, \ldots, y_{r+1}]$ equation of $\overline{\pi(V)}$

$v_i/\rho \in k(y_1, \ldots, y_{r+1})$ st

$$\pi^{-1} = (v_1/\rho, \ldots, v_n/\rho)$$

We have $\deg p \leq \deg V$, $\deg \rho, \deg v_i \leq 2\,(\deg V)^2$

Defn.
Height of a variety (via a geometric solution) *(Giusti–Heintz–Pardo et al. 96)*

$$\eta(V) := h(\pi^{-1}) = h(p, v_1, \ldots, v_n, \rho)$$

$\eta(V)$ bounds the *bit length* of the integers in the elimination algorithms

Thm.

η is polynomially equivalent to h

$$\eta(V) \leq c_1\,\delta^4 h(V) + c_2\,\delta^6$$
$$h(V) \leq c_3\,\delta^{12}\,\eta(V) + c_4\,\delta^{13}$$

Arithmetic Nullstellensatz

k field

$f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ st $V(f_1, \ldots, f_s) = \emptyset$

$\Rightarrow \quad \exists g_1, \ldots, g_s \in k[x_1, \ldots, x_n]$ st

$$1 = g_1 f_1 + \cdots + g_s f_s$$

$\deg f_i \leq d \quad \Rightarrow \quad \deg g_i \leq$ **?**

- $\deg g_i f_i \leq \deg g + 2\,(1 + d^2 + \cdots + d^{2^{n-1}})$

  (Hermann 1926)

- $\mathrm{char}\,(k) = 0 \quad \Rightarrow \quad \deg g_i f_i \leq 3n^2 d^n$

  (Brownawell 87)

- $\deg g_i f_i \leq d^{n^2}$ *(Caniglia–Galligo–Heintz 88)*

- $\deg f_i\, g_i \leq \max\{3, d\}^n$

  (Kollár 88, Fitchas–Galligo 90)

Thm.

$f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ st $V(f_1, \ldots, f_s) = \emptyset$
$d_i := \deg f_i$ st $d_1 \geq \cdots \geq d_s$. Then

$$\deg g_i f_i \;\leq\; 2\, d_s \, \Pi_{j=1}^{\min\{n,s\}-1} d_j \leq 2\, d^n$$

$\deg g_i f_i \leq \max\{3, d\}^n$ optimal for $d \geq 3$

Best previous upper bound for $\deg f_i = 2$
(Sabia–Solernó 95)

$$\deg g_i f_i \leq n\, 2^{n+2}$$

We obtain

$$\deg g_i f_i \leq 2^{n+1}$$

$f_1, \ldots, f_s \in \mathbb{Z}[x_1, \ldots, x_n]$ without common zeros in $\mathbb{C}^n$

$\Rightarrow \quad a \in \mathbb{Z} - \{0\}$ and $g_1, \ldots, g_s \in \mathbb{Z}[x_1, \ldots, x_n]$ st

$$a = g_1 f_1 + \cdots + g_s f_s$$

Problem

$\deg f_i \leq d \quad h(f_i) \leq h$

$$\Rightarrow \quad \deg g_i \leq \quad \mathbf{?}, \quad h(a), h(g_i) \leq \quad \mathbf{?}$$

Previous results

$$h(a), h(g_i) \leq d^{n^2}\, h$$

by Cramer's rule

$$\deg g_i \leq d^{c\,n} \qquad h(a), h(g_i) \leq \kappa(n)\, d^{8n+5} h$$

c constant, $\kappa(n)$ hyper–exponential on n *(Berenstein–Yger 91)*

$$\deg g_i \leq d^{c_1 n} \qquad h(a), h(g_i) \leq d^{c_2 n} h$$

$c_1,\ c_2 \leq 35$ constants *(Krick–Pardo 94)*

Thm. *(Arithmetic Nullstellensatz over complete intersection varieties)*

$F_{r+1}, \ldots, F_n \in \mathbb{Z}[x_1, \ldots, x_n]$ reduced complete intersection

$V := V(F) \subseteq \mathbb{A}^n$ variety of dimension r and degree δ

$f_1, \ldots, f_s \in \mathbb{Z}[x_1, \ldots, x_n]$ polynomials without common zeros in V

$d := \max_i \deg f_i, \;\; h := \max_i h(f_i)$

$D := \max_i \deg F_i, \;\; H := \max_i h(F_i)$

$\Rightarrow \;\exists a \in \mathbb{Z} - \{0\}$ and $g_1, \ldots, g_s \in \mathbb{Z}[x_1, \ldots, x_n]$ st

- $a \equiv g_1 f_1 + \cdots + g_s f_s \mod (F_{r+1}, \ldots, F_n)$
- $\deg g_i \le 5\, n^2\, D\, d^{2\, r}\, \delta^2$
- $h(a),\, h(g_i) \le c(n)\, D^2 (d^r\, \delta)^{12} (h + H + h(V) + \; d^r\, \delta)$

Distance between varieties

$V \subseteq \mathbb{A}^n(\mathbb{C})$ 0–dimensional variety defined over $\mathbb{Q}$

$\log ||V|| := \log(\max_{\xi \in V} ||\xi||) \leq h(V) + \log(n+1) \deg V$

ie the height of V bounds its distance to the origin

Problem:

For $V, W \subseteq \mathbb{A}^n$ $\mathbb{Q}$–varieties st $V \cap W = \emptyset$ give a lower bound for the distance between V and W

Prop.

$V, W \subseteq \mathbb{A}^n$ $\mathbb{Q}$–varieties st $V \cap W = \emptyset$ and $\dim W = 0$

$$\log(\mathrm{dist}(V, W)) \\ \leq -c(n) \left(\deg V \cdot \deg W (h(V) + h(W)) + 4 \log(n+1)\right)$$

Distance function

$$\operatorname{dist}_\alpha(V,W) := \inf\{||p-q|| : \\ p \in V,\ q \in W,\ \ \log||p||,\ \log||q|| \le \alpha\}$$

Thm.

$V, W \subseteq \mathbb{A}^n$ $\mathbb{Q}$–varieties st $V \cap W = \emptyset$

$r := \dim V, \ \ s := \dim W$

V, W reduced complete intersection varieties of

$f := \{f_1, \dots, f_{n-r}\}$

$g := \{g_1, \dots, g_{n-s}\} \subseteq \mathbb{Z}[x_1, \dots, x_n]$ resp.

$d := \deg f, \quad h := h(f), \quad \delta := \deg V$

$D := \deg g, \quad H := h(g)$

$\Rightarrow$

$$\log(\operatorname{dist}_\alpha(V,W)) \\ \ge -c(n)\, d^2\, D^{12\,r+2}\, \delta^{12}(h + H + h(V) + D^r\,\delta + \log\alpha)$$

for $\alpha > 0$

Conj.

V, $W \in \mathbb{A}^n$ $\mathbb{Q}$–varieties st $V \cap W = \emptyset$

Then there exist $F \in I(V)$, $G \in I(W)$ st

- $1 = F + G$
- $\deg F, \deg G \leq \deg V \cdot \deg W$
- $m(F), m(G) \leq \deg V \cdot h(W) + \deg W \cdot h(V)$
  $+c(n) \deg V \cdot \deg W$

Effective partition of 1

Implies

$$\log(\mathrm{dist}_\alpha(V, W)) \geq -(\deg V \cdot h(W) + \deg W \cdot h(V) \\ +(c(n) + 2\,n + \log \alpha) \deg V \cdot \deg W)$$

Complexity of a variety

Let $f \in \mathbb{Z}[x_1, \dots, x_n]$ polynomial
Γ straight–line program (slp) for f is

$$\Gamma := \{a_1, \dots, a_L\} \subseteq \mathbb{Z}[x_1, \dots, x_n]$$

st $a_i = 1,\ x$ or $a_i = a_j * a_k$ with $* = +, -, \cdot$
and $j,\ k < i$, and $a_L = f$

$$L(f) = \text{length } (\Gamma)$$

complexity of computing f

Eg.

$f := (x+1)^4$

$\Rightarrow\ \Gamma := \{1,\ x,\ x{+}1,\ (x{+}1)\cdot(x{+}1),\ (x{+}1)^2\cdot(x{+}1)^2\}$

is a slp for f

$L(f) = 5$

$f = \Sigma_i \, a_i x^i \in \mathbb{Z}[x_1, \ldots, x_n]$

$\deg f = d, \quad h(f) = h$

$$\Rightarrow \quad L(f) \leq (d^n \, h)^{O(1)}$$

but... $L(f)$ can be quite smaller in some cases

Eg.

$L(x^{2^n}) = O(n)$

Defn.

For $V \subseteq \mathbb{A}^n$ equidimensional variety
the *complexity* of V is defined as

$$L(V) := L(f_V)$$

For $V \subseteq \mathbb{A}^n$ variety
$V = \cup_i V_i$ equidimensional descomposition

$$L(V) := \sum_i L(V_i)$$

Thm.

$V \subseteq \mathbb{A}^n$ equidimensional variety
$\dim V = r \qquad \deg V = \delta$
$\pi : V \to \mathbb{A}^{r+1}$ generic linear projection

$\Rightarrow \quad L(V)$ is polynomially equivalent to $L(\pi^{-1})$

$$L(\pi^{-1}) \ \leq (n\,\delta\,L(V))^{O(1)}$$
$$L(V) \leq (n\,\delta V\,L(\pi^{-1}))^{O(1)}$$

Thm. *(Computational Bézout inequality)*

V, $W \subseteq \mathbb{A}^n$ $\mathbb{Q}$–varieties

$$L(V \cap W) \leq (n \deg V \deg W \, L(V) \, L(W))^{O(1)}$$

More generally

$V_1, \ldots, V_l \subseteq \mathbb{A}^n$ $\mathbb{Q}$–varieties

δ_i degree of V_i $\quad \delta := \Pi_i \, \delta_i$

$$L(V_1 \cap \cdots \cap V_l) \leq (n \, \delta \sum_i L(V_i))^{O(1)}$$

The slp for the Chow form of (each of the components of) $\cap_i V_i$ can be computed in time

$$(n \, \delta \sum_i L(V_i))^{O(1)}$$

Cor.

$f_1, \ldots, f_s \in \mathbb{Z}[x_1, \ldots, x_n]$ st

$V := V(f_1, \ldots, f_s) \subseteq \mathbb{A}^n$ is 0-dimensional

$\deg f_i \leq d, \;\; h(f_i) \leq h$

$\Rightarrow$ the system of equations

$$f_1 = 0, \ldots, f_n = 0$$

can be solved in time $(n \, d^n \, h)^{O(1)}$