Effective Hilbert's Nullstellensatz

Carlos D'Andrea

cdandrea@ub.edu

http://carlos.dandrea.name

David Hilbert (1862-1943)

Nullstellensatz

German: “theorem of zeros,” or more literally,

“zero-locus-theorem”

Hilbert's Nullstellensatz

(from Wikipedia)

is a theorem which makes precise a fundamental relationship between the geometric and algebraic sides of algebraic geometry, an important branch of mathematics. It relates algebraic sets to ideals in polynomial rings over algebraically closed fields. The theorem was first proved by David Hilbert, after whom it is named.

Ingredients of Hilbert's Nullstellensatz

- The field of complex numbers $\mathbb{C}$
- A sequence of polynomials

  $f_1, \ldots, f_s \in \mathbb{C}[x_1, \ldots, x_n]$
- An algebraic variety in $\mathbb{C}^n$:

  $V(f_1, \ldots, f_s) := \{x \in \mathbb{C}^n : f_i(x) = 0, i = 1, \ldots, s\}$

Hilbert's Nullstellensatz

(weak version)

$$V(f_1, \ldots, f_s) = \emptyset$$

$$\Updownarrow$$

$$\exists g_1, \ldots, g_s \in \mathbb{C}[x_1, \ldots, x_n]$$

such that

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

The Nullstellensatz in Linear Algebra

$$(*)\begin{cases} f_1(x_1,\ldots,x_n) &= 0 \\ \vdots & \vdots \\ f_s(x_1,\ldots,x_n) &= 0 \end{cases}$$

with $f_i(x_1,\ldots,x_n) = a_{i1}x_1 + \ldots + a_{in}x_n + a_{i(n+1)}$

$$a_{ij} \in \mathbb{C}$$

$$A := \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} & a_{1(n+1)} \\ a_{21} & a_{22} & \dots & a_{2n} & a_{2(n+1)} \\ \vdots & \vdots & \dots & \vdots & \vdots \\ a_{s1} & a_{s2} & \dots & a_{sn} & a_{s(n+1)} \end{pmatrix}$$

$\text{rank}(A_{s,n}) < \text{rank}(A_{s,n+1}) \iff$ the system does not have solutions

Nullstellensatz for Linear Systems

$$\text{rank}(A_{s,n}) < \text{rank}(A_{s,n+1})$$

$$\Updownarrow$$

there exist $\lambda_1, \ldots, \lambda_s \in \mathbb{C}$ such that

$$\lambda_1 f_1(x_1, \ldots, x_n) + \ldots + \lambda_s f_s(x_1, \ldots, x_n) = 1$$

Univariate Nullstellensatz

(Euclidean algorithm)

$$f_1, \ldots, f_s \in \mathbb{C}[x_1]$$

$$f := \gcd(f_1, \ldots, f_s)$$

$$f = g_1 f_1 + \ldots + g_s f_s$$

$$V(f_1, \ldots, f_s) = V(f)$$

$$V(f) = \emptyset \iff f \in \mathbb{C} \setminus \{0\}$$

Effective Hilbert's Nullstellensatz

(degrees bound)

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

$$V(f_1, \ldots, f_s) = \emptyset$$

$$\Updownarrow$$

$$\exists D = D(s, n, d) \in \mathbb{N},\ g_1, \ldots, g_s \in \mathbb{C}[x_1, \ldots, x_n]$$

with $\deg(g_i) \leq D$ and

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

Nullstellensatz

Algebraic Geometry

↓

Commutative Algebra

Effective Nullstellensatz

Algebraic Geometry

↓

Commutative Algebra

↓

Linear Algebra!

Effective Hilbert's Nullstellensatz

(Arithmetic version)

$a \in \mathbb{Z},\ h(a) := \log\left(|a|\right)$

$(h(0) := -\infty)$

$f(x) = \sum_{j=0}^{d} a_j x^j \in \mathbb{Z}[x]$

$h(f) := \max\{h(a_0), \ldots, h(a_d)\}$

Effective Hilbert's Nullstellensatz

(height bound)

$$f_1, \ldots, f_s \in \mathbb{Z}[x_1, \ldots, x_n],\ h(f_i) \leq h_0$$

$$V(f_1, \ldots, f_s) = \emptyset$$

$$\Updownarrow$$

$$\exists H_0 = H_0(h_0, d, s, n) \in \mathbb{R},\ a \in \mathbb{Z}_{\neq 0},$$

$$g_1, \ldots, g_s \in \mathbb{Z}[x_1, \ldots, x_n]$$

with $h(a),\ h(g_i) \leq H_0$ and

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

Effective Hilbert's Nullstellensatz

(Arithmetic-geometric version)

$$f_1, \ldots, f_s \in \mathbb{Z}[x_1, \ldots, x_n],\ \deg(f_i) \leq d,\ h(f_i) \leq h_0$$

$$V(f_1, \ldots, f_s) = \emptyset$$

$$\Updownarrow$$

$$\exists D \in \mathbb{N},\ H_0 \in \mathbb{R},\ a \in \mathbb{Z} \neq 0,$$

$$g_1, \ldots, g_s \in \mathbb{Z}[x_1, \ldots, x_n]$$

with $\deg(g_i) \leq D,\ h(a),\ h(g_i) \leq H_0$ and

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

Applications

- Number Theory
- Theoretical Computer Science
- Diophantine Geometry
- Problems over finite fields

Effective Univariate Nullstellensatz

$\Updownarrow$

Effective Euclidean algorithm

$f_1, \ldots, f_s \in \mathbb{Z}[x_1],\ \deg(f_i) \leq d,\ h(f_i) \leq h_0$

$f := \gcd(f_1, \ldots, f_s)$

$f = g_1 f_1 + \ldots + g_s f_s$

$\deg(g_i) \leq d - 1$

$h(f),\ h(g_i f_i) \leq 3d \log(d+1) + 6dh + \log(4)$

Effective Hilbert's Nullstellensatz

(degree bound)

- $D \leq 2(2d)^{2^{n-1}}$ (G. Hermann, 1926)
- $D \leq \min\{n, s\} n d^{\min\{n,s\}} + \min\{n, s\} d$ (Brownawell, 1987)
- $D \leq 2^{n^2}$ over any field (Caniglia-Galligó-Heintz, 1988)
- $\deg(g_i f_i) \leq \max\{3, d\}^n$ (Kollär 1988)

A lower bound

(Masser & Philippon)

$f_1 := x_1^d,\ f_2 := x_1 x_n^{d-1} - x_2^d, \ldots$

$f_{n-1} := x_{n-2} x_n^{d-1} - x_{n-1}^d,\ f_n := 1 - x_{n-1} x_n^{d-1}$

$V(f_1, \ldots, f_n) = \emptyset$

$(x_1, \ldots, x_n) \mapsto (t^{d^{n-1}-1}, \ldots, t^{d-1}, t^{-1})$

shows $\deg(g_1 f_1) \geq d^n$

Effective Hilbert's Nullstellensatz

(height-degree bound)

- $H_0 \leq sd^{n^2}(h_0 + \log\, s + d)$ (Cramer rule over the best degree bound)
- $D \leq (2n+1)d^n,\ H_0 \leq \lambda(n)d^{8n+3}(h_0 + \log\, s + d\log\, d)$ with $\lambda(n) = \mathcal{O}(e^n)$ (Berenstein-Yger, 1991)
- $D \leq (nd)^{cn},\ H_0 \leq (nc)^{cn}(h_0 + \log\, s + d)$ with $c \leq 35$ (Krick-Pardo, 1996)
- $D \leq (2n+1)d^n,\ H_0 \leq \lambda(n)d^{4n+2}(h_0 + \log\, s + d\log\, d)$ with $\lambda(n) = \mathcal{O}(e^n)$ (Berenstein-Yger, 1999)

Effective Hilbert's Nullstellensatz

(height-degree bound)

$D \leq 4nd^n,\ H_0 \leq$

$4n(n+1)d^n(h_0 + \log\ s + (n+7)\log(n+1)d)$

(Krick-Pardo-Sombra 2001)

$\deg(g_i f_i) \leq d^{\min\{s,n+1\}},\ h(g_i) + h(f_i) \leq$

$d^{n-1}(h_0 + c(n,s)d)$ with

$c(n,s) \leq (5n+11)\log(n+2) + (2n+1)\log^+(s-n)$

(D-Krick-Sombra, 2009)

A lower bound

$f_1 := Hx_1^d,\ f_2 := x_1x_n^{d-1} - Hx_2^d, \ldots$

$f_{n-1} := x_{n-2}x_n^{d-1} - Hx_{n-1}^d,\ f_n := H - x_{n-1}x_n^{d-1}$

$(x_1, \ldots, x_n) \mapsto$

$(H^{1+d+\ldots+d^{n-1}}t^{d^{n-1}-1}, \ldots, Ht^{d-1}, t^{-1})$

shows $\deg(g_1f_1) \geq d^n$ and

$h(a) \geq h_0(1 + d + d^2 + \ldots + d^{n-1})$

Mathematical Tools

- Elimination theory “a la Gröbner” (double exponential bounds)
- Intersection and Elimination Theory in projective space (Brownawell, Kollär)
- Arithmetic IET + duality theory in Gorenstein Algebras (Krick-Pardo-Sombra)
- Geometric Elimination in multiprojective spaces (Jelonek)
- Arithmetic and Geometric Elimination in multiprojective spaces (D-Krick-Sombra)

Nullstellensatz “a la Jelonek”

On the effective Nullstellensatz

(Invent. Math. 162 (2005) 1–17)

Effective version of *Perron’s Theorem*

Effective Implicitization of hypersurfaces

Effective Nullstellensatz

Geometric Perron's Theorem

(1927)

$q_1, \ldots, q_{n+1} \in \mathbb{C}[x_1, \ldots, x_n]$ with $\deg(q_i) \leq d_i$

There exists a nontrivial $E \in \mathbb{C}[y_1, \ldots, y_{n+1}]$ with

$E(q_1, \ldots, q_{n+1}) = 0$ and

$$\deg\left(E(T_1^{d_1}, \ldots, T_{n+1}^{d_{n+1}})\right) \leq \prod_{j=1}^{n+1} d_j$$

Extended by Jelonek (2005) to general varieties

Arithmetic-Geometric Perron

(D-Krick-Sombra)

$q_1, \ldots, q_{n+1} \in \mathbb{Z}[x_1, \ldots, x_n]$ with $\deg(q_i) \leq d_i,\ h(q_i) \leq h_i$

There exists a nontrivial $E = \sum_{a \in \mathbb{N}^{n+1}} \alpha_a y^a \in \mathbb{Z}[y_1, \ldots, y_{n+1}]$ with

$E(q_1, \ldots, q_{n+1}) = 0$ and, if $\alpha_a \neq 0,\ a = (a_1, \ldots, a_{n+1})$,

$$\sum_{i=1}^{n+1} a_i d_i \leq \prod_{j=1}^{n+1} d_j$$

$$h(E) + \sum_{i=1}^{n+1} a_i h_i \leq \left(\prod_{j=1}^{n+1} d_j\right) \left((n+1)\log(n+2) + \sum_{i=1}^{n+1} \frac{h_i}{d_i} \right)$$

AG Perron for rational functions

(D-Krick-Sombra)

$p_1, q_1, \ldots, p_{n+1}, q_{n+1} \in \mathbb{Z}[x_1, \ldots, x_n]$ with

$\max\{\deg(p_i), \deg(q_i)\} \leq d_i,\ \log(|p_i| + |q_i|) \leq h_i$

There exists a nontrivial $E \in \mathbb{Z}[y_1, \ldots, y_{n+1}]$ with

$E\left(\frac{p_1}{q_1}, \ldots, \frac{p_{n+1}}{q_{n+1}}\right) = 0$ and

$$\deg_{y_i}(E) \leq \prod_{j \neq i} d_j,\ h(E) \leq \sum_{j=1}^{n+1} \left(\prod_{i \neq j} d_j\right)(h_i + \log(2))$$

Example

$$\frac{p_1}{q_1} = \frac{x^{d_1}}{m_1(x+1)^{d_1}}, \quad \frac{p_2}{q_2} = \frac{(x+1)^{d_2}}{m_2\, x^{d_2}}$$

$$E = m_1^{d_2} m_2^{d_1} y_1^{d_2} y_2^{d_1} - 1$$

- $\deg_{y_1}(E) = d_2$
- $\deg_{y_2}(E) = d_1$
- $h(E) = h_1 d_2 + h_2 d_1$

Parametric Nullstellensatz

$\mathbb{F} = k(t_1, \ldots, t_p)$, k any field

$f_1, \ldots, f_s \in k[t_1, \ldots, t_p, x_1, \ldots, x_n]$, such that $V_{\overline{\mathbb{F}}^n}(f_1, \ldots, f_s) = \emptyset$

There exist $\alpha \in k[t_1, \ldots, t_p]_{\neq 0}$, $g_1, \ldots, g_s \in k[t_1, \ldots, t_p, x_1, \ldots, x_n]$ such that

$$\boxed{\alpha(t) = g_1(t, x) f_1(t, x) + \ldots + g_s(t, x) f_s(t, x)}$$

Effective Parametric Nullstellensatz

(D-Krick-Sombra)

(previous results by Smietanski 1993)

$$h_i := \deg_t(f_i),\ d_i := \deg_x(f_i)$$

$$d_1 \geq d_2 \geq \dots$$

Then

- $\deg_x(g_i f_i) \leq \prod_{j=1}^{\min\{s,n+1\}} d_j$
- $\deg_t(\alpha),\ \deg_t(g_i f_i) \leq \left(\prod_{j=1}^{\min\{s,n+1\}} d_j\right) \sum_{k=1}^{s} \frac{h_k}{d_k}$

Example: the Sylvester Resultant

- $f_1 = t_0 + t_1 x + t_2 x^2 + \ldots + t_{d_1} x^{d_1}$
- $f_2 = t_{d_1+1} + t_{d_1+2} x + t_2 x^2 + \ldots + t_{d_1+d_2+1} x^{d_2}$
- $\mathbb{F} = k(t_0, \ldots, t_{d_1+d_2+1})$
- $\alpha(t) = \text{Resultant}(f_1, f_2, x) = g_1(t,x) f_1 + g_2(t,x) f_2$
- $\deg_t(\alpha),\ \deg_t(g_i f_i) = d_1 + d_2$
- $\deg_x(g_i f_i) = d_1 + d_2 - 1 \leq d_1 d_2$

Parametric Perron's Theorem

(D-Krick-Sombra)

$q_1, \ldots, q_{n+1} \in k[t_1, \ldots, t_p, x_1, \ldots, x_n]$ with

$\deg_x(q_i) \leq d_i,\ \deg_t(q_i) \leq h_i$

There exists a nontrivial

$E = \sum_{a \in \mathbb{N}^{n+1}} \alpha_a(t) y^a \in k[t_1, \ldots, t_p, y_1, \ldots, y_{n+1}]$ with

$E(q_1, \ldots, q_{n+1}) = 0$ and, if $\alpha_a \neq 0,\ a = (a_1, \ldots, a_{n+1})$,

- $\sum_{i=1}^{n+1} a_i d_i \leq \prod_{j=1}^{n+1} d_j$
- $\deg_t(E) + \sum_{i=1}^{n+1} a_i h_i \leq \left(\prod_{j=1}^{n+1} d_j\right) \sum_{i=1}^{n+1} \frac{h_i}{d_i}$

Parametric Perron for rational functions

(D-Krick-Sombra)

$p_1, q_1, \ldots, p_{n+1}, q_{n+1} \in k[t_1, \ldots, t_p, x_1, \ldots, x_n]$ with
$\max\{\deg_x(p_i), \deg_x(q_i)\} \leq d_i,\ \max\{\deg_t(p_i), \deg_t(q_i)\} \leq h_i$

There exists a nontrivial $E \in k[t_1, \ldots, t_p, y_1, \ldots, y_{n+1}]$
with $E\left(\frac{p_1}{q_1}, \ldots, \frac{p_{n+1}}{q_{n+1}}\right) = 0$ and

$$\deg_{y_i}(E) \leq \prod_{j \neq i} d_j,\ \deg_t(E) \leq \sum_{j=1}^{n+1} \left(\prod_{i \neq j} d_j\right)\ (h_i)$$

Example

- $g_1, g_2 \in k[t],\ \deg_t(g_i) = h_i$
- $\frac{p_1}{q_1} = \frac{x^{d_1}}{g_1(x+1)^{d_1}},\ \frac{p_2}{q_2} = \frac{(x+1)^{d_2}}{g_2\, x^{d_2}}$

$$E = g_1^{d_2} g_2^{d_1} y_1^{d_2} y_2^{d_1} - 1$$

- $\deg_{y_1}(E) = d_2,\ \deg_{y_2}(E) = d_1$
- $h(E) = h_1 d_2 + h_2 d_1$

Further Effective Nullstellensatz

- Strong Nullstellensatz

  (Jelonek 2005, D-Krick-Sombra 2009)

- Nullstellensatz over varieties

  (Jelonek 2005, D-Krick-Sombra 2009)

- Nullstellensatz for arbitrary ideals

  (Kollär 1999)

- Sparse effective Nullstellensatz

  (Sombra 1999, Krick-Pardo-Sombra 2001)

UNIVERSITAT DE BARCELONA

Moltes Gràcies...