Effective Nullstellensatz and Generalized Bézout identities

André GALLIGO (U.C.A., INRIA, LJAD, France)

JNCF, CIRM
February 2019.

Abstract

Among recent results on effective Hilbert's Nullstellensatz:

- Z. Jelonek (Inventiones mathematicae, 2005)
- C. d'Andrea, T. Krick and M. Sombra (A. S. ENS, 2013) "[DKS:13]".

I will present our curent work with Z. Jelonek, for finding effective versions of sharp elimination processes.

Hilbert Nullstellensatz

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

do not share any root in $\mathbb{C}^n$ if and only if there exist $g_1, \ldots, g_s \in \mathbb{C}[x_1, \ldots, x_n]$ such that:

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

- Assuming $deg(f_i) \leq d$. If the degrees of the $f_i g_i$, is bounded by D, one finds the g_i by solving a linear system of size about sD^n.
- The coefficients of the g_i belong to the field of coefficients of the f_i, (e.g. $\mathbb{Q}$).

Brief History: Upper bound D for the degrees

- Hermann, 1923: $D = 2(2d)^{2^{n-1}}$.
- Brownawell, 1987: $D = n^2 d^n$, in characteristic 0.
- Caniglia-Galligo-Heintz, 1988: $D = d^{n(n+3)/2}$.
- Kollar, 1988: $D = max(d, 3)^n$.
- Fitchas-Giusti-Smietanski, 1995: $D = d^{cn}$, for a constant c. (Using Straight-Line Programs).
- Sabia-Solerno, Sombra, 1995-97: Improvements for $d = 2$.
- Jelonek, 2005: $D = d^n$, for $s \leq n$.
- C. d'Andrea, T. Krick and M. Sombra, 2013: Parametric and arithmetic versions.

Elimination and Bézout identities

Let $\mathbb{K}$ be an algebraically closed field.

- When $V(f_1, \ldots, f_s)$ is of dimension 0 in $\mathbb{K}^n$, Z. Jelonek established in 2005, an elimination theorem. We generalize this result as follows.
- Assume $V(f_1, \ldots, f_s)$ has dimension q in $\mathbb{K}^n$; $deg(f_1) \geq \ldots \geq deg(f_s)$.
- There exist $g_1, \ldots, g_s \in \mathbb{C}[x]$ and a non-zero polynomial $\phi(x_{n-q}, \ldots, x_n)$, such that:

$$\phi = g_1 f_1 + \ldots + g_s f_s;$$

$$deg(g_i f_i) \leq [deg(f_1) \ldots deg(f_{n-q-1})] deg(f_n).$$

- We first prove it in generic coordinates, then we use a deformation argument.

Perron's theorem

Jelonek type approaches rely on generalizations of Perron's theorem. Here, we will use one proved in [DKS:13].
Let k be an arbitrary field and consider the groups of variables $t = \{t_1, \ldots, t_p\}$ and $x = \{x_1, \ldots, x_n\}$.

Generalized Perron Theorem:

Let $Q_1, \ldots, Q_{n+1} \in k[t, x] \setminus k[t]$.
$d = (d_1, ..., d_{n+1}),\ h = (h_1, \ldots, h_{n+1})$. Then there exists

$$E = \sum_{a \in N^{n+1}} \alpha_a y^a \in k[t][y_1, \ldots, y_{n+1}] \setminus \{0\}$$

satisfying $E(Q_1, \ldots, Q_{n+1}) = 0$ and such that, for all $a \in supp(E)$, we have

1) $< d, a > \leq (\prod_{i=1}^{n+1} d_j)$.
2) $deg(\alpha_a) + < h, a > \leq (\prod_{i=1}^{n+1} d_j)(\sum_{l=1}^{n+1} \frac{h_l}{d_l})$.

Main Construction

$I = (f_1, \ldots, f_s) \subset \mathbb{K}[x_1, \ldots, x_n]$ is an ideal, of dimension $q < n$.

- Take $F_{n-q} = f_s$ and $F_i = \sum_{j=i}^{s} \alpha_{ij} f_j$ for $i = 1, ..., n-q-1$, where α_{ij} are sufficiently general. Take $J = (F_1, ..., F_{n-q})$, deg $F_{n-q} = d_s$, deg $F_i = d_i$ for $i \leq n-q-1$, $dim V(J) = q$.
- $$\Phi : \mathbb{K}^n \times \mathbb{K} \ni (x, z) \rightarrow (F_1(x)z, \ldots, F_{n-q}(x)z, x) \in \mathbb{K}^{n-q} \times \mathbb{K}^n$$
  is a (non-closed) embedding outside the set $V(J) \times \mathbb{K}$.
- $\Gamma = \mathrm{cl}(\Phi(\mathbb{K}^n \times \mathbb{K}))$ is an affine sub-variety of dimension $n+1$ of $\mathbb{K}^{2n-q}$. Let $\pi : \Gamma \rightarrow \mathbb{K}^{n+1}$ be a generic projection and define $\Psi := \pi \circ \Phi$.
- In the generic coordinates X, we get $\Psi(X, z) =$
  $$(zF_1 + \ell_0(x), zF_2 + X_1 \ldots, zF_{n-q} + X_{n-q-1}, X_{n-q}, \ldots, X_n).$$

Continued

- By this genericity, the image of the projection

$$\pi' : V(J) \ni X \mapsto (X_{n-q}, \ldots, X_n) \in \mathbb{K}^{q+1}$$

is an hypersurface S, let $\phi'(X_{n-q}, \ldots, X_n) = 0$ describe S.
- $\Psi = (\Psi_1, \ldots, \Psi_{n-q}, X_{n-q}, \ldots, X_n) : \mathbb{K}^n \times \mathbb{K} \to \mathbb{K}^{n+1}$ is finite outside the set $V(J) \times \mathbb{K}$.
- Hence, the set of non-properness of Ψ is contained in

$$S = \{T = (T_1, \ldots, T_{n-q}, X_{n-q}, \ldots, X_n) \in \mathbb{K}^{n+1} : \phi'(X) = 0\}.$$

- Now, we apply to Ψ, Perron's theorem with $\mathbb{L} = \mathbb{K}(z)$.
- There exists a non-zero polynomial
$W(T_1, \ldots, T_{n+1}) \in \mathbb{L}[T_1, \ldots, T_{n+1}]$ such that
$W(\Psi_1, \ldots, \Psi_{n+1}) = 0$
with the expected degree inequalities.

End of proof

- There is a non-zero minimal poynomial $\tilde{W} \in \mathbb{K}[T_1, \ldots, T_{n+1}, Y]$ such that
  (a) $\tilde{W}(\Psi_1(x, z), \ldots, \Psi_{n+1}(x, z), z) = 0$,
  (b) $\deg_T \tilde{W}(T_1^{d_1}, T_2^{d_2}, \ldots, T_{n-q}^{d_{n-q}}, T_{n-q+1}, \ldots, T_{n+1}, Y) \leq d_s \prod_{j=1}^{n-q-1} d_j$,
- The $Y-$leading coefficient $b_0(T)$ of $\tilde{W}$ satisfies $\{T : b_0(T) = 0\} \subset S$, hence $b_0(T)$ depends only on coordinates $T_{n-q+i+1} = X_{n-q+i}$, for $0 \leq i \leq q$.
- We now develop (a) in z and get $E(X, z) = 0$.
  The $z-$leading coefficient $B(X)$ in E, is obtained either from $b_0(X_{n-q}, ..., X_n)$ or from terms corresponding to products, containing at least one of $T_i, i < n$, hence containing at least one of F_i.
- The Bézout identity follows from the fact that this coefficient $B(X)$ vanishes identically. $\square$

Getting rid of the coordinates change

- We first establish a parametric version: We replace the field $\mathbb{K}$ by the algebraic closure of the fraction field of $k[t]$, where k is an infinite field, following [DKS:13].
- Then, we use the following generic change of coordinates and its inverse.

$$X_i = x_i + t \sum_{j=i+1}^{n} a_{i,j} x_j \; ; \; x_i = X_i + t \sum_{j=i+1}^{n} b_{i,j}(t) X_j.$$

- Set $\bar{F}_j(X,t) = F_j(x)$. Notice that t divises $\bar{F}_j(X,t) - F_j(X)$.
- After simpliflications, we have,

$$b_0(X_{n-q}, ..., X_n, t) = \sum_{j=1}^{n-q} G_j(X,t) \bar{F}_j(X,t).$$

Continuation

- We cannot exclude the possibility of a remaining factor t^p in the left hand, side with $p > 0$.
  So we need to perform several reduction steps.
- Let $b_0(X,t)) = t^p(\phi(x) + t\phi_1(x,t))$. Setting $t = 0$, we obtain a non trivial relation $0 = \sum_{j=1}^{s} G_j(x,0)F_j(x)$.
- Apply a change of coordinates to this relation to get $0 = \sum_{j=1}^{s} \bar{H}_j(X,t)\bar{F}_j(X,t)$.
- The $x-$degree of $G_j(x,0)$ is bounded by the $X-$degree of $G_j(X,t)$, and is equal to the $X-$degree of $\bar{H}_j(X,t)$.
- Now, $\sum_{j=1}^{n-q}(G_j(X,t) - \bar{H}_j(X,t))\bar{F}_j(X,t)$ vanishes for $t = 0$, hence admits a factor t.
  We simplify the two sides of the previous equality by t, so $t^{p-1}(\phi(x) + t\phi_1(x,t)) = \sum_{j=1}^{s}(G_j(X,t) - \bar{H}_j(X,t))\bar{F}_j(X,t)$.
  □